INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

RESILIENCE TO HIGH CONSEQUENCE CASCADING FAILURES OF CRITICAL INFRASTRUCTURE NETWORKS

Institute for Homeland Security

Sam Houston State University

Arthur Mouco, PhD
Benjamin L. Ruddell, PhD, PE
Susan Ginsburg, Esq.
Criticality Sciences, Inc.

Resilience to High Consequence Cascading Failures of Critical Infrastructure Networks

Arthur Mouco, PhD

Benjamin L. Ruddell, PhD, PE

Susan Ginsburg, Esq.

Criticality Sciences, Inc.

Abstract

Critical infrastructure networks such as telecommunications, power, water, natural gas, diesel, transportation, and cyber networks are interdependent with one another, forming a vast and dauntingly complex web of institutions and physical systems that must be engineered and secured for reliability. No single utility operator, engineering consultant, emergency management organization, financial institution, or local, regional or other government entity is capable of understanding, monitoring, or managing the whole system. Yet, failures are unavoidable, and when those failures cascade through the network the result may be high-consequence cascading "catastrophes" or Black Swan events. In one recent and tragic example, the February 13–17, 2021 Winter Storm Uri in Texas initiated a failure in the natural gas production system that cascaded first to the natural gas power generation system and then to the wider ERCOT power system, the water distribution system, and the petrochemical industry of Texas. No single system operator was responsible, and yet the consequences – including fatalities, recovery challenges, regulatory attention, and extreme costs – are everyone's problem. As networked interdependencies grow, the likelihood of cascading failures has increased accordingly, necessitating technical solutions tailored to this problem. This report introduces the basic principles of interdependent critical infrastructure networks and reviews approaches for analyzing and mitigating the vulnerability of the network to make it resilient. Resilience and reliability in critical infrastructures are complementary and orthogonal. In resilient networks, the inevitable failures due to "all hazards" stay small and don't become catastrophes.

Summary

1. The Resilience Challenge

Resilience can be defined as the ability of a system to absorb, cope, and restore from a disturbance, as well as adapt itself, learning from past disturbances [1]. Moreover, resilience can be associated with the capacity of a system to resist and recover from the impacts of all kinds of failure events, including low probability, high consequence (LPHC) events that often dominate total system risk. LPHC events are the "black swan" events – catastrophic scale events that were not forecast or prepared for in advance of them happening and are considered impossible to predict: the Northeast Blackout, the Fukushima nuclear disaster, and Winter Storm Uri are notorious examples.

LPHC events on engineered network systems, such as power, telecommunication, water, gas, and cyber networks are usually associated with cascading failures. A cascade failure happens when a failure on one or a few parts of the system spreads to other parts, progressively spreading to the system or multiple systems with extreme consequences. This may happen within a single utility – the Colonial Pipeline failure is an example – and it may also happen across sectors. Critical infrastructure systems that keep cities alive and allow populations to thrive are interdependent, as illustrated in Figure 1. Gas delivery, power delivery, communication services, and water delivery are all examples of infrastructures that can, while interrupted during a failure, spread failures on other critical infrastructures and significantly impact society. LPHC events are likely to cause cascading failures and, ultimately, long-term interruption of services with severe consequences to the population and economy, as well as the utility itself. In financial terms, the consequences are both direct (money lost for service not supplied) and indirect (community impacts, legal liability, fines, and reputational damage). Therefore, the practical challenge of resilience for engineers is to keep failures small, and with their emergency management partners, also to recover quickly.

Figure 1 – Interdependent Critical Infrastructure Networks in a City.

Because critical infrastructures are not independent and cannot function alone for an extended period, systems interdependencies in critical infrastructure must be considered when analyzing resilience [2]. The impacts of the Uri storm in Texas in 2021 provide a real example of the effects of failures in interdependent critical infrastructure systems. In that event, failures propagated between power, gas, and water systems generated a death toll of 151 and severe economic consequences, to the order of U$ 155 billion, as shown in [3] and [4]. Systems interdependencies can propagate cascade failures and must be evaluated, as shown in Figure 2.

Why is interdependent network resilience analysis not a standard feature of reliability engineering and regulatory policy today? Three reasons stand out. One reason is that operations engineering tends to utilize single-sector physically-based models for design and optimization, but physically-based models of multi-sector interdependent infrastructure systems remain in their infancy. Such models are fundamentally challenging and costly to construct and to validate due to the variety and scale of the physics, institutions, regulations, and data sources involved, and also the high computational cost associated with them.

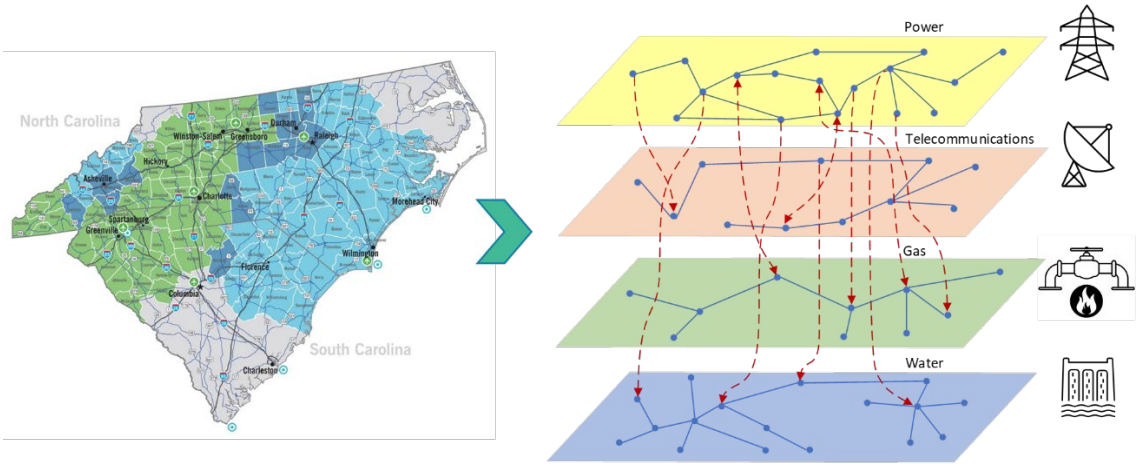

Figure 2 - System Interdependencies

A second reason is that network fragilities stemming from network interdependencies tend to be hidden from any single sector's systems operators, and also to regulatory agencies that focus on one sector of critical infrastructure. Critical infrastructure operations tend to be much better prepared to mitigate vulnerabilities within their own sector and systems operations than they are to absorb vulnerabilities originating from interdependent networked systems. However, what you can't see can hurt you, because failures in other networked systems can easily cascade to create major failures in your system.

A third reason why resilience remains an unsolved problem is that current methods of failure and risk analysis focus more on reliability than resilience (even when the word

"resilience" is thrown around). Built into engineering reliability analysis, failure analysis generally considers risk as the possibility of a failure event occurring multiplied by the consequence of that event. Risk can be calculated as a function of different consequences – such as loss of lives, financial, societal, and reputational – and the probability of a failure event happening [5]. The standard methods to mitigate risks are to define the likelihood and consequences of threats and failures in the system using historically observed threat and failure data. These historically experienced risks are then built into engineering models to simulate failure risk. Those simulations, used extensively in critical infrastructure management and constituting the backbone of engineering reliability analysis, require accurate and detailed physics-based network models along with accurate characterization of the probability of the threats facing the system.

This type of failure analysis works well for reliability in the face of routine threats but works poorly for resilience to rare, unpredictable, and catastrophic threats- and also works poorly for cascading failures once they obey a different set of risk principles and physics. Reliability is, by definition, the ability to be trustworthy or perform consistently well. Reliability is generally accepted as the characteristic of an asset expressed by the probability that it will perform a required function under stated conditions for a stated period [5]. Investing in reliability to prevent failures caused by routine threats does not guarantee resilience during LPHC events. As an illustration, Figure 3 presents a photograph of Manhattan, New York during the 2003 Northeast Blackout that affected 55 million people in eight US states and parts of Canada, with electric power being lost for anywhere from a few hours to several days. This LPHC event started with a single software bug in the alarm system that prevented operators from quickly becoming aware of an overload on a high-voltage transmission line and, following human error, a manageable problem developed into a large-scale blackout [6].

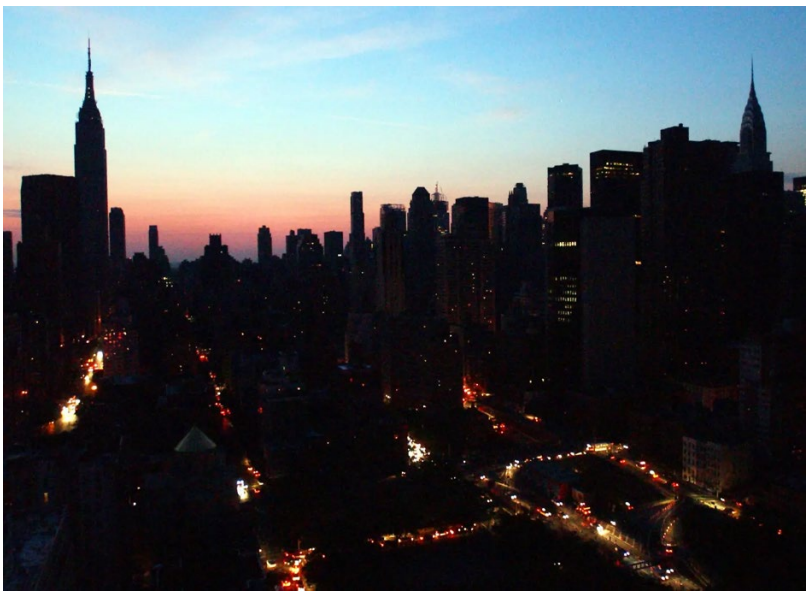

Figure 3 – New York City, 2003 Northeast Blackout (Frank Franklin II/Associated Press)

Black Swan events with their uncertainty and extreme features are more common than we expect, and they seem to have become more frequent in the 21st century. Climate factors are associated with some of the most notable events affecting critical infrastructure in recent decades. The consequences of extreme weather events, such as hurricanes, storms, and floods, are increasing in severity, leading to community and ecological challenges in every region of the United States [7]. It may be that globalized and interdependent networks along with climate change have made Black Swans more common, or it may be that we are only now beginning to appreciate their prevalence as we collect systematic failure data for the first time in human history. Regardless, they cause extreme damage to critical infrastructure, resulting in loss of life, generating severe social impacts, extreme financial burdens, legal liability, national security compromises, and reputational damage. For all these reasons, it has become paramount to adopt a methodology to increase critical infrastructure systems resilience, identify critical assets associated with such failures and mitigate those risks so that failures due to unforeseen disruptions are kept small and recovery can be rapid.

A final important contributing factor to the resilience challenge is the primary focus in recent decades on increasing efficiency within individual systems. It has become clear that maximizing efficiency under routine operating conditions can decrease the system's resilience to unexpected high-consequence events [8]. This factor creates an unfortunate “race to the bottom” or “tragedy of the commons” in an unregulated competitive marketplace where less resilient operations outcompete more resilient operations on short term cost and price. Resilience is therefore a regulatory challenge, in addition to a technical problem.

The power transmission system fully reflects the gap in resilience considerations. The power system is an essential infrastructure for the operation of fundamental societal functions. All other critical infrastructures depend on continuous electrical energy availability [1, 2], making the power grid among the “most critical” of infrastructures. The push for efficiency was translated into new methodologies to operate the system close to its capacity. Investments in system asset expansion are being postponed in exchange for additional monitoring and more flexible procedures, relying on state-of-the-art simulations using digital twins and pre-defined reliability criteria. Those new procedures allowed flexibility in real-time operation limits. However, this means that there is less margin for error, whether traceable to humans or models, a combination of both, or to other factors. More importantly, the system is less robust to respond to unpredicted failures and prone to cascade failures caused by black swans.

Engineering models to prevent failure in power systems center on achieving reliability. They do so by simulating the loss of any single asset on the system at a time representing failures of known intensity, duration, and frequency. This reliability methodology is well established for power systems planning and real-time operation,

commonly cited as the “N-1” criteria. N-1 is sometimes extended to N-k when expanded to combinations of failures. Power systems reliability is also expressed in two terms: adequacy and security. Adequacy is the balance between generation and load, and security is the ability of the system to respond to disturbances and transients. Those disturbances, usually frequent and associated with single asset failure, have relatively good statistical predictability. The standard measures to increase reliability mainly focus on preventing component failure by hardening assets against known hazards and preventive maintenance. From the financial perspective, reliability methodology leads to a cost/benefit analysis to address known types of events that can lead to expected revenue losses, planned recovery and new prevention requirements.

Unlike frequent or at least relatively predictable events with consequences that can be anticipated, LPHC events on the power grid are usually associated with extreme weather, such as hurricanes, ice storms and floods, and increasingly forest fires. They can also be initiated by cascading failures from other infrastructure systems, accidents, physical attacks by insiders, domestic attackers, or external adversaries, cyber-attacks, electromagnetic pulses, or failures in multiple internal computing and control networks. Those so-called black swans in power systems have low-frequency occurrence (e.g. years to decades), extremely low predictability, and present extreme costs and burdens to utilities and society [9, 10]. As discussed, LPHC events present elevated risks of loss of life, legal liability (insured and non-insured), and extended asset damage for the utilities that may lead to bankruptcy. A critical aspect of power grid resilience is the capacity to restore service quickly after LPHC events. There is reason to believe that LPHC events drive total risk and cost in critical infrastructure systems, and that building resilience to LPHC events simultaneously enhances resilience to routine failures.

Resilience to rare and severe events is the weak point in the predominant power engineering reliability paradigm. Despite all developments in technology, protection systems, availability of accurate models, and processing power for reliability and resilience simulation analysis, the frequency of power outages in the US has been increasing in the last decades. As shown in Figure 4, created from data provided in [11], the overall frequency of outages with energy interruption in the last decades is still increasing, as well as the number of people affected by those interruptions (over 2% growth on average). Resilience has therefore become a prerequisite for reliability.

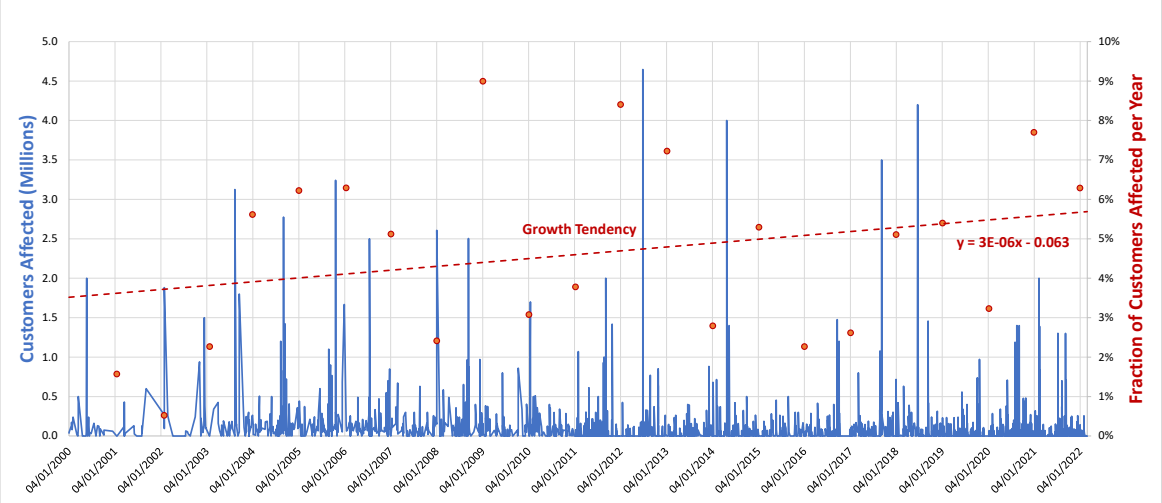

Figure 4 - US Power Outages [12]. The number of customers affected by outages (blue) and the fraction of customers affected per year (red) are both increasing over time in the United States, despite increasing investment in protection, modeling, maintenance, and more advanced technology for the grid. This may be due to increases in LPHC cascades.

2. Resilience Definitions and Metrics

Resilience has many definitions, from its historical, foundational meaning tied to the dynamics of life itself and the natural environment, to features of organizations and human psychology, to process definitions and practical engineering metrics that are being brought into the forefront of the design and operation of critical infrastructure. Resilience is fundamentally an adaptive learning process undertaken by societies and organizations. Resilience can be technically measured using standard threat-specific risk metrics (e.g. RAMCAP and similar), or with quantification of the "three R's" of robustness, recovery, and resistance. Resilience can and must be approached using both threat-specific and all-hazard techniques. In Table 1 are presented some resilience definitions from energy sector entities [13]. Note that there is still not a standard (sectoral or cross-sectoral) definition of resilience in place. These definitions have a shared common element: focusing on enhancing infrastructure systems to not only operate reliably under normal conditions, but also adapt, withstand, and more rapidly recover from a growing number of LPHC events.

Table 1 - Several Definitions of Resilience from Energy Sector Entities

Authority / Publishing Entity	Definition
National Association of Regulatory Utility Commissioners (NARUC)	"Robustness and recovery characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event."
Federal Energy Regulatory Commission (FERC)	"The ability to withstand and reduce the magnitude and/or duration of disruptive

	events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event."
Presidential Policy Directive Critical Infrastructure Security and Resilience (PPD)	"The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."
National Renewable Energy Laboratory (NREL)	"The ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions through adaptable and holistic planning and technical solutions."
Electric Power Research Institute (EPRI)	"In the context of the power system, resiliency includes the ability to harden the system against— and quickly recover from— high-impact, low frequency events."
PJM Interconnection	"Resilience, in the context of the bulk electric system, relates to preparing for, operating through and recovering from a high-impact, low-frequency event. Resilience is remaining reliable even during these events."
National Academies of Sciences, Engineering, and Medicine (NASEM)	"Resilience is not just about lessening the likelihood that that these outages will occur. It is also about limiting the scope and impact of outages when they do occur, restoring power rapidly afterwards, and learning from these experiences to better deal with the events in the future."
National Governors Association (NGA) / National Association of State Energy Officials (NASEO)	"The ability to withstand disasters better, respond effectively, and recover more quickly and to a more improved state."

2.1. Resilience is an Adaptive Learning Process

The concept of a resilient system is based on ecological theory developed decades ago in the 1960's. Underlying all technical definitions of resilience is the foundation of an effective adaptive learning process, based upon observations about how life thrives in nature.

All organizations, public and private, can enhance their resilience by building the capacity to adapt to disruptive events. Organizational resilience is the ability to bounce

back from crises, but this ability is based on proactive preparation and adaptive capacity. Literature describes four key capabilities that underpin organizational resilience: anticipation, monitoring, responding, and learning [14].

Anticipation centers on the ability to perceive and correctly respond to risk. Risk perception is influenced by various factors, including organizational culture, leadership, and external influences. Organizations with robust accounting systems and proactive risk assessment mechanisms are better equipped to identify and respond to risks effectively. Integrating risk perception and accounting practices is vital for enhancing the resilience of organizations in the face of uncertainties and challenges [15]. Building the technical capacity of an organization to accurately measure risk is a key part of its adaptive learning cycle supporting resilience.

Successful resilience planning also requires a shift in mindset from reactive practices to proactive strategies that integrate people, natural and technical processes, and economic considerations. In addition to risk assessment, collaboration, stakeholder engagement, and adaptive management are necessary to building in resilience to our collective infrastructure. The resilience planning process requires integrating diverse knowledge systems, promoting learning and experimentation as well as adapting existing governance structures to new needs [16].

Two well established examples of resilience defined as an adaptive learning process are the “OODA Loop” and the “RAAG” or Resilience Analysis Grid [17, 18]. The emphasis of these definitions is that effective resilience is created by accelerating the learning cycle wherein we (1) accurately sense what is happening around us, (2) learn based on how well our previous decisions are performing, (3) anticipate what will happen next, and (4) take adaptive action based on what we anticipate will happen. The faster and better we complete this adaptive learning cycle, the more resilient we are. In the context of critical infrastructure, data collection and transparency are the key to (1); science and honest debate are the key to (2); science and engineering are the keys to (3), and engineering and leadership are the keys to (4).

Whereas engineering and operations professionals are trained to isolate and control a system, to keep it from changing and to protect it from shocks, the ecological systems definition emphasizes social, economic, and environmental change as the structure of the system adapts to maintain its basic functions. The literature on social-ecological resilience [19, 20] proposes a shift in perspective to recognize the dynamic and interconnected nature of social-ecological systems. Key elements of resilience include the ability to absorb disturbances, adapt to change, and transform when necessary, and the importance of understanding the interactions and feedback loops between social and ecological components in shaping system resilience.

The engineering and operations management communities are just beginning to explore the implications of ecological resilience for their work [21]. The standard engineering approach to resilience through hardening and redundancy is an efficient way to handle routine shocks that are well understood, but when shocks and changes are large and unexpected (e.g. Black Swans), the ecological systems resilience concept is more relevant. It is paramount for planning, engineering, and operations professionals to gain the perspective that their daily work toward the implementation of cost-effective and reliable systems exists in the context of a larger adaptive socio-ecological system that sets the rules guiding daily decisions. But when big shocks or changes happen in the system, those rules should and will change as the larger ecological system adapts and learns. What happens to your finely tuned operations when the system breaks and the rules change- for example, when the Colorado River ran out of water in 2022, when the insurance companies pulled out of California and Florida to avoid covering fires and hurricanes, or when the power went out for Texas water utilities during Winter Storm Uri? Ecological resilience and adaptive learning cycles are a deeper resilience that underpin and shape technical engineering and operations resilience.

The adaptive learning process driving critical infrastructure resilience includes customs and traditions, government law and regulation, engineering design standards, monitoring and data collection, transparency with performance data, and the policies and actions of people and organizations including, for example, the federal government, major industry organizations, utilities, and individuals. The technical definitions and metrics of resilience are tools to support the adaptive learning cycle by measuring and helping to improve resilience. Resilience's many technical measures and definitions include measures of the system's reliability, its ability to resist damage from a hazard, and its ability to quickly recover from damage.

2.2. Technical Metrics for Resilience: RAMCAP R=TVC, the "Three R's", and All-Hazard metrics

Stakeholder engagement, community preparedness, and effective governance are all required to enhance resilience through adaptive learning [22,23,24,25]. But making this process work requires technically accurate metrics to operationalize. This includes technically accurate financial measurement of risk and of mitigation so that investments in resilience can be financed and weighed against competing priorities.

Engineering and operations management professionals do not yet have all the needed tools in hand. The current focus is on measuring and managing disruptions to systems using three classes of technical metrics, the "three R's" [26]: resistance to change, robustness to a wide range of hazards and recovery or reorganization time after a shock.

Performance on the first two R's is typically measured using the RAMCAP (Risk Analysis and Management for Critical Asset Protection) risk-based performance process (Risk = Threat x Vulnerability x Consequence), and the third R is typically the domain of operations and of emergency management professionals who measure recovery in terms of cost and time to restore functions after a disruption. This approach to resilience is already widely implemented under the rubric of "reliability". Much of current research seeks to advance the state of reliability by modeling a wider variety of hazards and interdependencies between more types of infrastructures.

Department of Energy (DOE) and Department of Defense (DOD) funded institutions, as well as elements of the Department of Homeland Security and Department of Commerce, have created and published definitions of resilience, as presented in Section 2.4.4. These definitions have similarities, but there is no consensus in the scientific, engineering, or financial communities on how to define resilience in the context of critical infrastructure, especially for practical purposes of cost-based engineering metrics. The most widely accepted metric for hazard-specific risk measurement and engineering is RAMCAP. The American Society of Mechanical Engineers (ASME) developed the method now known at RAMCAP Plus, that is widely used today by critical infrastructure organizations like utilities and their engineers. This hazards-based approach catalogs historically observed hazards and their consequences data along with models of future hazards to specify design requirements for the intensity, duration, and frequency of threats that the system should be designed to resist. Robust design and operations solutions that cost-effectively handle a wide range of threats are preferred over those that require highly precise threat predictions, that only address a narrow spectrum of threats, or that are costly. For example, it is cost-effective for a civil engineer to design a bridge that withstands the expected loads from rush hour traffic and from the expected intensities of storms and earthquakes, but it is not cost-effective or feasible for the engineer to anticipate a contractor parking all the construction equipment to overload a single support beam; this black swan event was the bridge collapse in Minneapolis, MN in 2007.

The RAMCAP approach is effective and efficient for engineering resilience via resistance to and recovery from common hazards, but robustness to a wide range of hazards is a limitation of RAMCAP. Several features of today's security landscape for critical infrastructure limit RAMCAP's usefulness for achieving deep and broad resilience. "Knightian Unknowns" represent unknown, unknowable, or unusually severe hazards for which accurate anticipation is impossible based on historical data. "Nonstationarity" [27] refers to a future that will not reliably look like the past – even for well-observed historical hazards such as coastal flooding, that is worsening over time. Asymmetric adversarial threats that manifest themselves as rare or unknown hazards as the adversary actively seeks "soft" targets within a system, have become increasingly important since Al Qaeda's September 11th, 2001 attacks. For all these reasons, RAMCAP is insufficient by itself as a

basis for critical infrastructure systems resilience. (see detailed discussion of RAMCAP in Section 2.4 below).

Whether Black Swans originate due to extreme weather, cyber features, and/or adversary attacks, the sheer complexity and scale of interdependent systems also may both trigger and worsen an initial disruption. An all-hazards methodology to measure resilience must also consider interdependent vulnerabilities among critical infrastructure systems and the possibility of cascade failures propagating from one system to another, whether internally or across sectors. As portrayed in Figure 2, most critical infrastructures have interdependencies and can be affected by multiple systems, with cascades spreading from one system to another, internally and externally.

Understanding the consequences and impacts of the failure events is as fundamental for determining investment in resilience mitigation as assessing the system propensity to cascade failure. Direct financial consequences are easily identified during failure events, usually associated with lost revenue, repair, and immediate recovery cost. However, utilities may be exposed to many indirect consequences – loss of life, morbidity, legal liability, reputation damage, uninsured liabilities, that can generate tremendous costs and damage, possibly leading to bankruptcy and/or imposition of new regulatory requirements. The population that the utility serves as well as the utility itself may suffer losses that go well beyond what may be captured by the authority to fund mitigation represented in existing rate and other financial processes.

Due to the hazards-oriented limitations of RAMCAP and similar, engineering and operations resilience must be complemented with “all-hazards” approaches to resilience that rely on different assumptions and do not require accurate anticipation of the intensity, duration, or frequency of a hazard to achieve resilient outcomes. For example, engineers and operators can create a diversity of options by arranging for multiple decorrelated systems or sources [28] to increase the probability that adequate adaptive options will remain available after an unanticipated threat impacts the system. Moreover, engineers and operators can achieve resilience by focusing on designing systems that resist “cascading failure” through the system’s network regardless of the cause of the original failure, keeping the consequences of failure localized and small, instead of focusing exclusively on resisting the primary failure caused by a specific kind of threat [29]. For example, an all-hazards design for the Minneapolis MN bridge would have resulted in the contractor’s overloading equipment falling into the river when the beam failed, but that would not have taken down the entire bridge in a cascading collapse. Or, an all-hazards design would have recovered the damage of the failed beam quickly enough to prevent the failure of the rest of the bridge. An all-hazard approach assumes the failure of critical system components, and then proceeds to develop engineering and operations solutions to limit the spread of the damage and contain overall consequences of the failure.

The hazard-specific and all-hazard approaches have complementary advantages, and when used together these approaches yield systems that are both very efficient in their resistance to common hazards while also providing robust resilience to unanticipated hazards. The hazards-agnostic approaches bring an important dose of perspective and technical humility to bear on the problem of resilience. We need both hazard-specific and all-hazard technical metrics in order to build resilient systems.

2.3. From Reliability to Resilience

Reliable service is the central goal of critical infrastructure systems and their operators and reliability performance is measured and regulated in most jurisdictions (and by most supplier service contracts). However, reliability in the face of unexpected and severe events requires resilience. Resilience supports and improves reliability under extraordinary circumstances, but reliability may not support and improve resilience under extraordinary circumstances. “Uptime” under routine operating conditions including routine threats is a common measurement of reliability. Consequence (or risk) created by failure is a better measure of resilience. In other words, reliability focuses on minimizing service failures, and resilience focuses on minimizing the consequence (or risk) created by service failures. Reliability is focused on routine circumstances, and resilience on extraordinary circumstances. If a utility operator is forced to choose one metric, choose resilience, because risk is the more fundamental measurement, and because the catastrophic life-and-death consequences of major failures in critical infrastructures outweigh the inconvenience of routine outages. Fortunately, we may pursue both reliability and resilience, and the two complement each other. Figure 5 provides a table comparing reliability and resilience.

	RELIABILITY	RESILIENCE
Timeframe	• Daily (statistical predictability)	• Decades (unpredictable "Black Swans")
Costs	• Lost revenue • Contractual costs • Repair • Recovery • Prevention	• Loss of life • Extreme costs • Uninsured liability • Bankruptcy • Reputational injury • Prosecution • Political and regulatory response
Focus	• Asset failure • Hardening against anticipated hazards • Preventative maintenance and replacement • Limited customer differentiation • Annual budgeting	• Critical function failure • Mitigation for unanticipated events • Containing and recovering cascading failures • Critical customer protection and recovery • Variable budgeting
Metrics	• Well established quantitative standards • Each sector measures its own performance • Service reliability metrics • Asset service life & optimal replacement schedule • Reliability ROI for Capital and Rate Planning	• **Emerging quantitative standards** • **System interdependency analysis** • **Cascade risk and resilience scoring** • **Interdependent system resilience mitigation & optimization** • **Critical customer & recovery order planning** • **Resilience ROI for Capital Improvement and Rate Planning**

Figure 5 - Reliability VS Resilience

2.4. Resilience Standards in Use Today

2.4.1. American Society of Mechanical Engineers (ASME): Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus Process, or R=TVC)

The American Society of Mechanical Engineers (ASME) program called RAMCAP is in widespread use as a set of updated standards for risk and resilience assessment in critical infrastructure systems. These standards are in reality a process to provide a framework for assessing and improving the resilience of these systems to disruptions. The standards themselves are not primarily quantitative; instead, they are designed to be flexible and adaptable to the specific needs of individual systems by providing a systematic approach for identifying vulnerabilities, assessing risks, and implementing measures to improve resilience.

The ASME RAMCAP standards are divided into three main categories: assessment, design, and operation. The *assessment* standards provide a process for identifying the potential vulnerabilities and risks to a system, and for evaluating the current level of resilience. The *design* standards provide guidance on how to design systems that are more resilient to disruptions, including guidelines for selecting materials and components, and for implementing redundancy and diversity. The *operation* standards provide guidance on how to operate and maintain systems to ensure they remain resilient over time.

Importantly, the standards cover a variety of different types of disruptions, including natural hazards, cyber threats, and human-caused events, whether accidental or adversarial. They also address the importance of considering the entire lifecycle of a system, from design and construction, through operation and maintenance, to eventual decommissioning.

While the ASME RAMCAP standards are not embodied in law or regulation and are voluntary, they are widely recognized and used in the power industry as a best practice for resilience. As we will discuss below, the water industry has also adapted RAMCAP for its needs through its J100 resilience standard. RAMCAP standards are designed to be flexible and adaptable to the specific needs of different types of systems and organizations, and provide a systematic approach for identifying vulnerabilities, assessing risks, and implementing measures to improve resilience.

In summary, the ASME RAMCAP resilience standards provide a framework for assessing and improving the resilience of critical infrastructure systems to disruptions, by providing guidelines for identifying vulnerabilities, assessing risks, and implementing measures to improve resilience. These standards are widely recognized and used in the industry as a best practice for resilience and provide a systematic approach to improve the resilience of different types of systems and organizations.

The ASME RAMCAP defines “risk” as a product of the likelihood of a threat attacking a system asset (a probability), the vulnerability of that system component to that threat (a probability), and the proximate consequences of the failure of that component due to that threat (or, R=TVC). Risk is therefore expressed as an expected loss due to a specific threat, using the same units as the consequence, e.g. dollars or lives lost.

Risk = Threat x Vulnerability x Consequence

Resilience is broadly defined as the ability to function through an attack or natural event or the speed at which an asset can return to virtually full function (or a substitute function or asset provided) [30]. Resilience as a concept is still being formalized. Some prefer to measure resilience using time, from time of event until return to full function, but this ignores partial service denial (severity), which is generally much more common than complete loss of function, and the value of the services denied. For the purposes of the RAMCAP Plus process, resilience is defined in different ways for the asset owner and community, respectively.

- From the narrow or “direct” perspective of the system asset’s operator, the consequences are limited to a combination of lost revenue, legal liabilities, recovery costs, reputational costs, and regulatory fines. From the broad or “total”, societal” perspective, consequences additionally include public morbidity and mortality, lost revenue and income by businesses and their employees, security failures and crimes, and long term losses from foregone economic development.

Some key definitions follow: **Lost revenue** – the product of the duration of service denial (in days), the extent of service denial (in units of service denied per day) and the price (in dollars per unit, estimated at pre-event levels), which are all essential parts of estimating the owner's financial loss.

- **Lost Economic Activity in the Community** – the amount of decrease in the loss of output to direct customers and the indirect losses (multiplier effect) throughout the economy of a given region due to denial of service. It is estimated as a function of the asset's lost revenue and the duration of the service denial using an economic model. One application used a static application of basic regional economic data and an input-output table, modified to reflect the resilience of the respective business sectors.
- **Threat** – Any indication, circumstance or event with the potential to cause the loss of, or damage to, an asset or population. In the case of terrorism risk, threat is based on the analysis of the intention and capability of an adversary to undertake actions detrimental to an asset or population and the attractiveness of the asset or population relative to alternative assets or populations. In the case of natural hazards, threat refers to the historical frequency of the specific natural event to which the asset(s) may be subjected. In both cases, threat is summarized as the likelihood the event will occur.
- **Vulnerability** – Any weakness in an asset or infrastructure's design, implementation or operation that can be exploited by an adversary or contribute to functional failure in a natural disaster. Such weaknesses can occur in building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings or operational and personnel practices. In risk analysis, vulnerabilities are usually summarized as the conditional probability that, given an attack or natural event, the estimated consequences will ensue, i.e., the attack will succeed or the natural event will cause the estimated damage.
- **Consequence** – The outcome of an event occurrence, including immediate, short and long-term, direct and indirect losses and effects. Loss may include human fatalities and injuries, financial and economic damages and environmental impacts, which can generally be estimated in quantitative terms. Consequences may also include less tangible and less quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness or military readiness or other impacts.

2.4.2. National Institute of Standards and Technology (NIST): Interdependent Networked Community Resilience Modeling Environment (IN-CORE)

According to The National Institute for Standards and Technology (NIST), resilience refers to the ability of a system, community, or organization to prepare for, withstand, and rapidly recover from disruptions. This includes the ability to anticipate, absorb, adapt to, and/or rapidly recover from the effects of an adverse event, while maintaining the continuity of essential functions.

NIST sees resilience as important because disruptions can have significant negative impacts on individuals, communities, and organizations. These impacts can include loss of life, property damage, economic disruption, and more. By building resilience, we can reduce the likelihood and severity of these impacts and minimize the overall disruption caused by an event. NIST sees resilience not as a one-time or static state, but rather as a continuous process of adaptation and improvement in a world where unexpected disruptions may occur swiftly and with major impact. In NIST's view, organizations, communities, and systems need to be constantly assessing and updating their resilience plans and strategies in response to changing risks and vulnerabilities.

Resilience, according to this approach, has three main components: preparedness, response, and recovery. *Preparedness* involves taking steps to anticipate and mitigate the potential impacts of disruptions. This can include processes like risk assessments, emergency planning, and training. *Response* involves taking action during and immediately after a disruption to minimize the impacts and protect lives and property. *Recovery* refers to the process of returning to normal operations after a disruption. This can include things like restoring damaged infrastructure, providing aid to affected individuals, and conducting after-action reviews to learn from the event and improve future preparedness and response.

NIST sees effective community resilience metrics as addressing two key questions:

- How can community leaders know how resilient their community is?
- And how can they know if their decisions and investments to improve resilience are making a significant difference?

NIST defined in [31] its community resilience metrics. Currently, NIST accepts a wide variety of community resilience approaches as valid: descriptive or quantitative; based on interviews, expert opinion, engineering analysis, or making use of pre-existing datasets; presented as an overall score or as a set of separately reported scores across physical, economic, social, and environmental dimensions. NIST has concluded that time to recovery of function is the most important resilience metric to be employed, because other resilience methods are insufficiently validated.

Noting the variety of approaches to resilience in use, the National Academies Committee on Increasing National Resilience to Hazards and Disasters and the Committee on Science, Engineering, and Public Policy in 2021 evaluated seventeen approaches to measuring various aspects of resilience. The authors concluded that none of the seventeen existing methodologies satisfactorily addressed both of the two basic questions posed by NIST noted above. One of the report's six main recommendations therefore is the development of a "national resilience scorecard, from which communities can then develop their own, tailored scorecards".

Other recent reviews of hazard risk reduction and resilience make similar recommendations for flexible scorecards [32] that permit a tailorable or locally relevant scorecard, concluding that a single prescriptive scorecard may not be appropriate for the wide range of US communities, from small agriculture communities to large industrial cities.

NIST and its partners from 12 universities, led by Colorado State University, established the Community Resilience Center of Excellence [33]. The objective is to accelerate the development of system-level models to support community resilience decision-making. A dynamic platform was developed to support resilience analysis based on research, development, and modeling relating to communities. The Interdependent Networked Community Resilience Modeling Environment (IN-CORE) is an open-source software platform that incorporates a risk-based approach to decision-making, enabling quantitative comparisons of alternative resilience strategies [34]. IN-CORE allows users to optimize community disaster resilience planning and post-disaster recovery strategies intelligently, using available data and physics-based models of inter-dependent physical systems combined with socio-economic systems.

2.4.3. National Academies

The National Academies (NA), non-profit institutions providing expert advice publicly, including the National Academy of Sciences, the National Academy of Engineering, and the National Academy of Medicine, established a program on Risk, Resilience, and Extreme Events (Resilient America) in 2014. NA founded the Resilient America program after the National Research Council's 2012 publication of the report "Disaster resilience: A national imperative".

FEMA in 2020 asked Resilient America to convene a committee on hazard mitigation and resilience-applied research topics as part of its efforts to reduce the immense human and financial toll of extreme events. NA released a consensus study report in 2022 defining resilience as "The ability to prepare and plan for, absorb, recover from, and more

successfully adapt to adverse events." [35]. To prepare this report NA engaged with the academic, public, and private sectors at national and local levels to achieve the following goals:

- Increase understanding of complex risks and extreme events in a changing environment, and the exposure of communities, infrastructure, and natural systems to these threats.
- Investigate and strengthen attributes of equitable, resilient systems and communities, including their interconnections and interdependencies.
- Test, communicate, and strengthen implementation of equitable strategies for adapting to changing risks and robust recovery from disruptions.
- Share accessible science and data for strengthening resilience and adaptive action, including policies, tools, best practices, and metrics.
- Connect and facilitate partnerships among scientists, data providers, practitioners, and decision makers.

The National Academy of Engineering hosted a workshop in October 2022: "Creating A Sustainable National Electric Infrastructure While Maintaining Reliability and Resiliency of the Grid". Several ISOs, transmission companies and power utilities participated, and a report was released afterwards. Some of the recommendations include:

- New tools are necessary for integrated resource and T&D planning and investment prioritization.
- The creation of grid resilience standards is necessary.
- Probabilistic assessments are necessary to account for LPHC event impacts on power grids.

2.4.4. Department of Energy (DOE): Voluntary Action Program for Resilience (VARP)

Drawing on the work of its associated national laboratories, the U.S. Department of Energy has adopted a definition of resilience that applies to a wide range of critical infrastructure sectors, including energy, transportation, and telecommunications, as well as the built environment and other essential systems. The DOE places a particular emphasis on the importance of energy resilience, highlighting the central role of energy systems in supporting critical infrastructure and enabling economic growth and development.

DOE defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions through adaptable and holistic planning and technical solutions." This definition emphasizes the importance of anticipating and adapting to changing conditions, as well as the need for a holistic and integrated approach to resilience that includes both planning and technical solutions. It also emphasizes the importance of rapid recovery from disruptions, which requires the ability to quickly assess and respond to the impacts of disruptive events. Collaboration among stakeholders, effective risk management and planning, and the integration of advanced technologies and tools are all paramount, as is incorporating resilience into long-term planning and decision-making processes.

To help communities and organizations build resilience to the impacts of natural and man-made hazards, DOE launched Voluntary Action Program for Resilience (VARP) as a voluntary program in 2016. VARP provides a framework for communities and organizations to assess their current level of resilience, identify areas for improvement, and develop and implement plans and strategies to enhance their resilience. The program is designed to be flexible and adaptable to the unique needs and priorities of different communities and organizations, and to encourage innovation and collaboration in the resilience planning process.

VARP participants may include local governments, businesses, academic institutions, and community groups. Participants commit to following a set of core principles for resilience planning, including:

- Collaboration: Participants agree to collaborate with other stakeholders in the resilience planning process, including other organizations, community groups, and government agencies.
- Assessment: Participants agree to conduct a comprehensive assessment of their current level of resilience, including an analysis of their risks, vulnerabilities, and capabilities.
- Planning: Participants agree to develop and implement plans and strategies to enhance their resilience, based on the results of their assessment.
- Monitoring and Evaluation: Participants agree to monitor and evaluate the effectiveness of their resilience plans and strategies, and to make adjustments as needed.

DOE's VARP is a resource for communities and organizations seeking to build resilience to a wide range of hazards, including natural disasters, cybersecurity threats, and other disruptive events.

2.4.5. Cyber Resilience

Cyber security and cyber resilience, including relating to Supervisory Control and Data Acquisition systems (SCADA) and the interface of cyber and physical operating systems generally, has become an urgent topic due to the potential of cyber threats to manifest as Black Swans [36]. A US Executive Order (EO) issued in May 2021 declared key themes in cybersecurity strategy and foundational ideas linked to the need for greater resilience [37]. The objective is to identify opportunities to enhance, measure, and sustain long-term resilience against the impacts of malicious cyber activity, at the entity level and systemic level, including continuity of the economy. The EO is expected to be implemented through cyber security strategy performance goals issued in 2023 [38,39].

The Executive Order states something fundamental to all considerations of critical infrastructure resilience: metrics are needed because investments in resilience can be expensive, with benefits that may be realized only intermittently because “black swan” events are unusual, making it return on such investments difficult to calculate. This can make resilience investment an uphill battle in the context of budgeting, capital raises, and rate applications [40]. For this reason, a viable strategy for resilience requires more than predictions about hazards and identification of vulnerabilities; it also requires decision frameworks for understanding what can and should be made resilient, how resources should be allocated, and, most importantly, an ability to quantify the value of investments in terms of resilience over time.

2.4.6. Department of Homeland Security (DHS): Cybersecurity and Infrastructure Agency (CISA) and Federal Emergency Management Agency (FEMA): Resilience Analysis and Planning Tool (RAPT)

The Department of Homeland Security (DHS) oversees two agencies increasingly relevant to resilience. DHS’ Cybersecurity and Infrastructure Security Agency (CISA) with its National Risk Management Center, and its Federal Emergency Management Agency (FEMA), share a common definition of resilience as the ability to prepare for, withstand, and rapidly recover from disruptions [41]. This definition highlights the key components of resilience, which include the ability to anticipate potential disruptions, prepare for them in advance, and quickly adapt and recover when they do occur. In the context of emergency management and national security, resilience refers to the ability of individuals, communities, and critical systems and infrastructure to withstand and recover from natural or man-made disasters and to ensure the continuity of essential services during and after disruptions. This includes not only physical systems such as power grids and

transportation networks, but also social systems such as communities and organizations. Both anticipatory mitigation for low probability high consequence events and well-instituted emergency management procedures are essential to ensure resilience in the face of potential disasters.

FEMA has developed the Resilience Analysis and Planning Tool (RAPT), a web-based software to help communities assess their resilience to natural and man-made hazards and plan for future events. RAPT provides a standardized framework for communities to identify and evaluate their risks, capabilities, and vulnerabilities, and to develop plans and strategies to enhance their resilience. RAPT focuses primarily on the assessment and planning phases of the resilience process and, as with the DOE tools, requires significant time, effort, and resources to use effectively, including the collection and analysis of data, stakeholder engagement, and the development of resilience plans and strategies. This may be a challenge for communities with limited resources or expertise.

2.4.7. American Water Works Association (AWWA) and Water Environment Foundation (WEF): Water Resilience Framework (J100)

The Water Resilience Framework J100 is a voluntary standard that emerged out of RAMCAP in response to the requirement of a risk and resilience analysis set forth in the federal American Water Infrastructure Act of 2018. The American Water Works Association (AWWA) and the Water Environment Federation (WEF) developed J100 through the Joint Committee on Water Utility Resilience, established in 2015 to help water utilities better understand and prepare for the impacts of natural and man-made hazards, and to promote the development of more resilient water systems. J100 defines resilience in the water sector as "the ability of a water system to adapt to changing conditions and to withstand and recover from disruptions, stresses, and acute events."

The J100 framework recognizes that disruptions and stresses are inevitable and that water systems must be able to adapt and respond effectively to these challenges to maintain their essential functions and services. The standard highlights the importance of adaptability and the ability to withstand and recover from various defined threats – potential disruptions, stresses, and acute events, such as droughts, floods, power outages, chemical spills, and cyber-attacks. It requires utilities to define threat-asset pairs, for example, a flood in relation to a particular pump station, and then to prioritize risks in terms of threats and asset vulnerabilities, for purposes of mitigation and emergency preparedness.

J100 is an assessment process that focuses on building capacity and capabilities that enable water systems to respond effectively to a range of known potential disruptions and stresses. J100 is being continuously updated, most recently in 2021 and has recently introduced the idea of addressing risk from interdependencies in water systems.

2.4.8. CIGRE Working Group C4.47

CIGRE is a global professional power engineering community committed to the collaborative development and sharing of end-to-end power system expertise. CIGRE Working Group C4.47 has defined resilience as the "ability of an electrical system to prepare for, absorb, recover from and adapt to a disturbance, while maintaining its essential functions, structure, and identity" [1]. This definition emphasizes the ability of the power system to not only withstand and recover from disruptions but also to adapt and evolve to changing conditions over time.

CIGRE Working Group C4.47's definition of resilience includes several key components, such as the importance of maintaining the essential functions of the power system, the need to preserve the overall structure and identity of the system, and the requirement for effective preparation, absorption, and recovery from disruptions. This definition highlights the importance of a holistic and system-level approach to resilience in the electric power system context, including the integration of advanced technologies and tools, effective risk management and planning, and collaboration among stakeholders. Figure 6 presents a graphical description of CIGRE´s resilience definition for power systems disturbances.

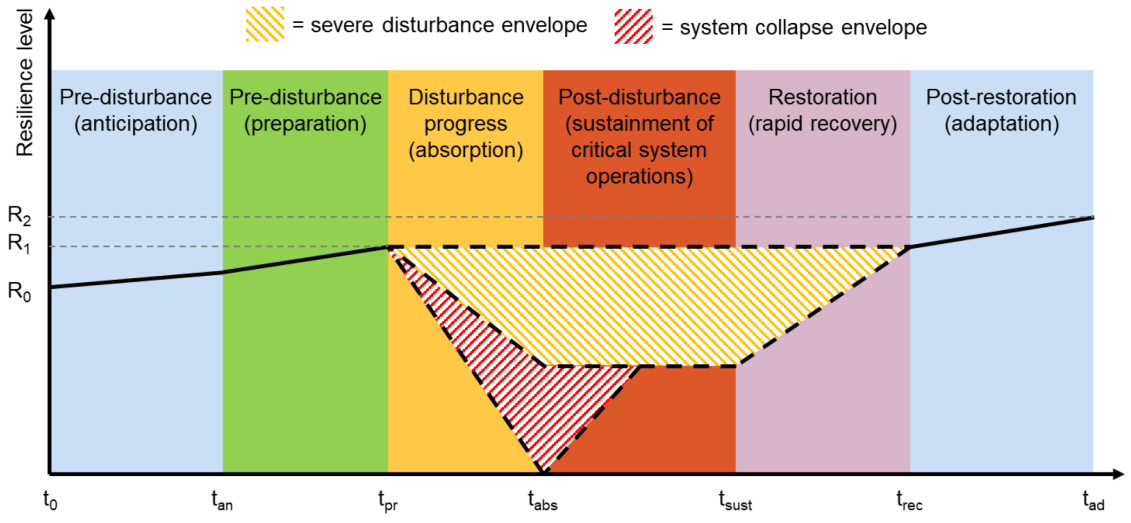

Figure 6 - CIGRE WG C4.47 Resilience Trapezoid [1]

2.4.9. The Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE), the electrical sector's leading professional organization, does not have a single definition of resilience, rather the organizations members apply the concept of resilience differently to a wide range of fields and applications. However, in the context of the IEEE's work related to electric power systems, the organization has developed a definition of resilience that focuses on the ability of the power system to withstand and recover from disruptions.

According to the IEEE, resilience in the electric power system context is "the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event" [42]. This definition emphasizes the need for effective planning and preparation, as well as the ability of the power system to adapt to changing conditions over time.

The IEEE's definition of resilience includes several key components, such as the importance of maintaining essential functions and services during disruptions, the need for effective response and recovery, and the importance of collaboration among stakeholders. This definition highlights the importance of a holistic and system-level approach to resilience in the electric power system context, including the integration of advanced technologies and tools, effective risk management and planning, and collaboration among stakeholders. Figure 7 presents a graphical description of IEEE´s resilience definition for power systems disturbances.

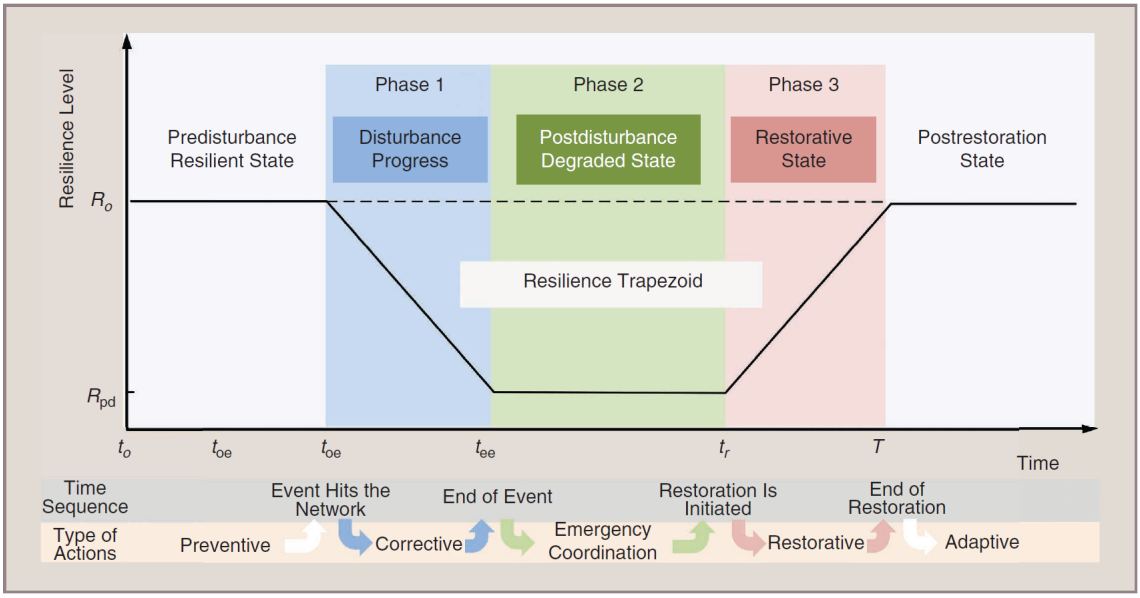

Figure 7 - IEEE Time Varying Resilience Multi-Phase Trapezoid [42]

2.4.10. Eastern Interconnection Planning Collaborative (EIPC)

The Eastern Interconnection Planning Collaborative (EIPC) is a collaboration among electric utilities, their regulatory agencies (ISO's and RTO's), and other stakeholders in the Eastern Interconnection region of the United States. EIPC is one of three major power grids in North America [43], together with the Electric Reliability Council of Texas (ERCOT), and the Western Electricity Coordinating Council (WECC). The EIPC has developed a definition of resilience for the electric power sector and the Eastern Interconnection region.

According to the EIPC, resilience is "the ability of the Eastern Interconnection to prepare for, withstand, and recover from high impact, low frequency events that could cause significant disruption to the electricity system and to the broader economy." Such events might include severe weather events, cyber-attacks, physical attacks, or other disruptive events that could cause widespread power outages.

The EIPC's definition of resilience also emphasizes the importance of both preparing for and responding to such events. This includes taking steps to enhance the power system's resilience, such as through the use of advanced technologies, improved planning and coordination among stakeholders, and investments in infrastructure and equipment. It also includes having effective response and recovery plans in place, which can help to minimize the impacts of disruptive events and facilitate a rapid return to normal operations.

2.4.11. Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI) defines resilience, in the context of power systems, as "the ability to harden the system against - and quickly recover from - high-impact, low-frequency events" [44]. Such LPHC events can threaten lives, disable communities, and devastate generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines and other fuel transport and telecommunications. Some examples of such events are severe weather or natural events (hurricanes and consequent flooding, tornadoes, earthquakes and consequent tsunamis, wildfires, ice storms, etc.), severe geomagnetic disturbances, cyber-attacks, physical attacks, coordinated cyber and/or physical attacks, electromagnetic pulse (EMP), high-altitude EMP, intentional electromagnetic interference attacks and pandemics.

EPRI defines resiliency as described above but also acknowledges diverse definitions of resilience associated with different systems, areas of actuation and interdependencies, including in the context of climate preparedness and resiliency.

EPRI has developed a Resilient System Investment Framework (RSIF). The objective of this framework is to help transmission planners assess the impacts and consequences resulting from LPHC contingency events on their systems. RSIF is based on the Siemens PTI PSS®E – a software system – which is intended to apply and solve extreme contingency events for a given power flow case, evaluating the resulting impacts to determine possible paths of cascading failures and the associated consequences. RSIF thus can determine the risk of adverse system impacts emanating from the extreme contingency event analyzed.

2.4.12. NetResilience

Resilience engineering literature for critical infrastructure systems does not make available a standard scientific definition and related industry guidelines for objective resilience metrics, especially metrics that consider critical infrastructure as an interconnected set of systems. One company is filling this gap by providing a new scientific method to evaluate resilience, using an objective scale to show risk of cascade failures that engineers can use to make improvements in system resilience, and relating this resilience score to dollar values that estimate the risk exposure of a system to LPHC events for use in cost-benefit analysis and capital planning[1].

This supplies a standardized methodology to evaluate resilience against LPHC events in critical infrastructure. The technique is based on engineering analysis, network sciences, and probabilistic measures, observing asset-to-asset risk in independent systems (e.g. power grid) or interconnected, interdependent systems (e.g. power grid and gas distribution or water distribution and connected SCADA and power supply). This provides utilities and other organizations including industrial sites and communities with a real measure of the system resilience considering all-hazard and LPHC events. The score is an intuitive zero to ten scale as presented in Figure 8. This methodology and metrics are discussed in [12] with an example of a large-scale power system's resilience analysis.

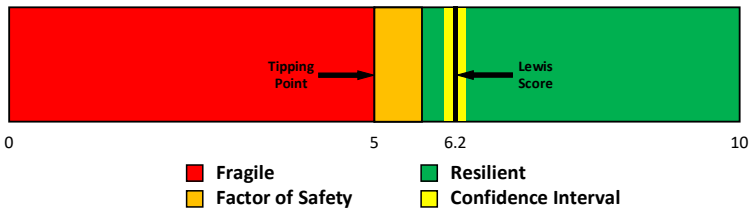

Figure 8 - Lewis Score℠ [12]. Networked systems with a status below the score of "5" (in red) tend to propagate and exacerbate initial failures to create high-consequence cascading failures. A Lewis Score℠ that is confidently above this "tipping point" at 5 indicates that a networked system tends to suppress cascades, containing failures to the immediate vicinity and consequences of the primary failure, and avoiding high consequence failure.

[1] https://www.critsci.com/

This method identifies critical assets – assets critical specifically for risk of cascade failures – and proposes mitigation options and recovery order, also optimizing these investments and providing benchmark comparisons to the Lewis Score^{SM} and a financial risk measure for LPHC events. The methodology focuses on hardening and/or reconfiguring the system against cascade failures caused by unpredictable black swans. It recommends budget allocation opportunities that increase the system's resilience against LPHC cascade failures, avoiding the severe consequences caused by such events, and showing how these reduce financial risk to the utility and their customers.

The risk measurement for financial exposure to loss from extreme events like Winter Storm Uri, is called maximum probable loss (MPL Risk^{SM}). MPL Risk^{SM} is a statistic of the consequence distribution estimated for all possible cascading failure events in the system. It is a function of the exceedance probability for cascade failure and marginal consequence, as presented in Figure 9. It provides a value for the most likely cascade failure with the highest consequence (direct and/or indirect) in a given system.

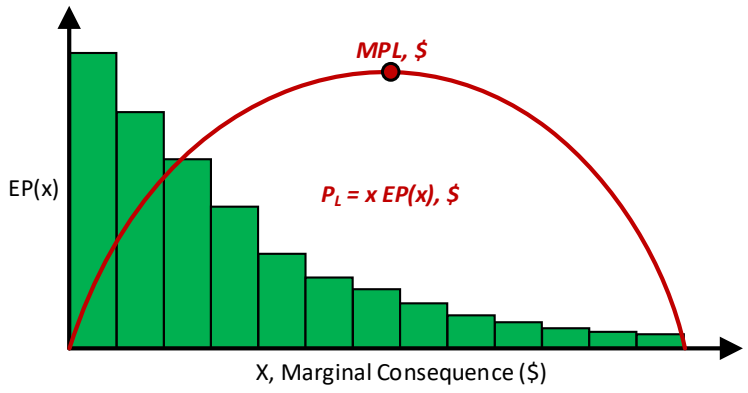

Figure 9 - Maximum Probable Loss (MPL RIsk^{SM}) [12], an essential statistic of a complex networked system's expected failure consequence distribution. MPL Risk^{SM} indicates a level of risk that is both relatively severe and also relatively common. MPL Risk^{SM} has units of expected loss, such as dollars ($) or lives lost.

3. How Can Stakeholders Cooperatively Mitigate Cascading Failure Risk?

To achieve resilience at community, regional and national scale, and beyond, and reduce the consequences of potentially catastrophic events– whether in operations, money, the natural and built environment, or life and health -- multiple stakeholders must develop a common understanding of catastrophic risk and how to mitigate it. These stakeholders include: engineering and operations personnel involved in designing and running the systems; emergency managers who maintain coordination and recovery

capacity for utilities and engage with governmental emergency personnel and others in the private sector; finance and insurance professionals who determine budgets, investments, and insurance; regulators who set rates and standards and monitor or enforce compliance; public officials at the local, State and federal levels directing or regulating utilities and promoting resilience; and researchers who drive progress in utilities and their supporting engineering companies, universities and governmental and nonprofit institutions.

Today these groups jointly create and manage day to day reliability in engineered systems including power, water, and telecommunications. To enable proper allocation of resilience investments, it is essential to augment reliability with resilience to large scale cascading failures by using a straightforward resilience metric to quantify the level of resilience in a given system that all stakeholders can agree upon. That method must apply to all hazards, including human threats, and must evaluate interdependent critical infrastructure.

The method described here, using a Lewis Score^{SM} and risk metrics, takes advantage of network science, a relatively new concept, to solve problems of interdependency, and uses probability science to address black swan risk. The use of network science to evaluate power systems' resilience to cascading failure has been discussed in the literature [29, 45], but has received far less attention than the standard power engineering paradigm. The network-based approach would typically employ the (interdependent) network topology, and among other features a mathematical approach to identify the critical assets on the system which tend to contribute to cascading system failures. Cascading failure probabilities are empirically determined, as are the direct (to the utility) and total (societal) consequences of critical infrastructure failure.

For larger and more complicated networked systems, interdependent systems can be modeled together using network science far more feasibly and simply with the probabilistic and topological approach than with the physics-based engineering modeling approach [46, 47]. Nevertheless, the network approach has both advantages and disadvantages compared to the physics-based modelling approach. Interdependency of systems is one element that favors the simpler and more flexible network approach. Overall, the network approach provides a largely complementary and orthogonal view into interdependent network resilience; it can be used to critique and corroborate the standard engineering approach, adding robustness and confidence when used in tandem. The system is greater than the sum of its parts, so analysis of the interdependent networks yields fundamentally different and superior resilience findings [48].

The following example, presented in [12], demonstrated the network resilience method for a major national power transmission system- in this case, the Brazilian interconnected system. The Brazilian transmission system supplies the entire nation of Brazil and has approximately 170,000 km of high-voltage transmission lines, as seen in

Figure 10. It has 176 GW of installed generation capacity and attends to a population of roughly 213 million. This system is heavily dependent on renewable generation, with approximately 86 % of its energy matrix based on hydro, wind, solar, and biomass generation.

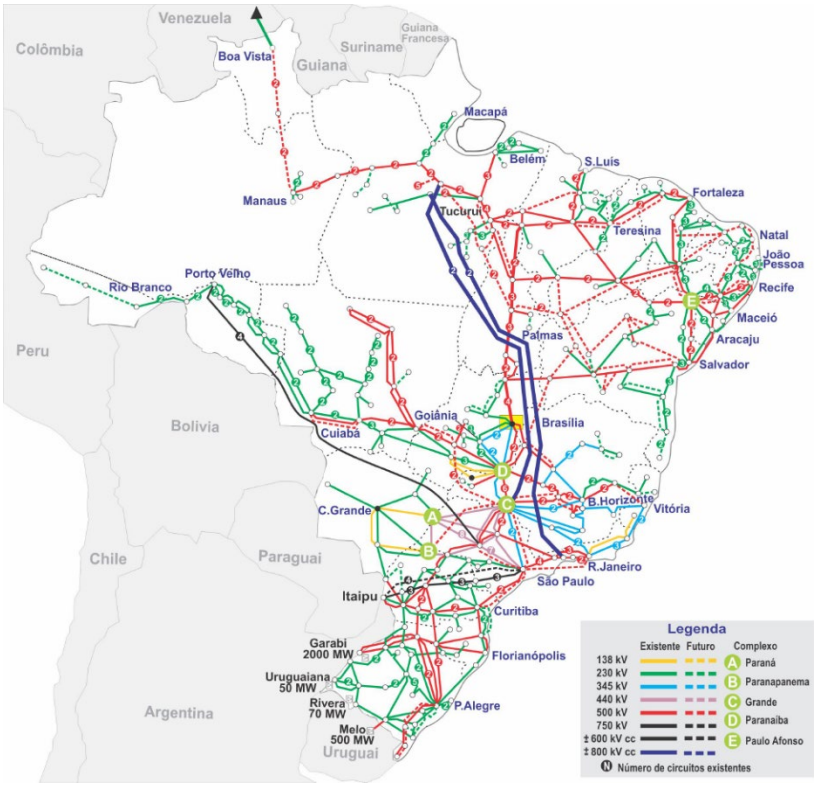

Figure 10 - Brazilian Interconnected System [12].

Software and advanced computing enable the estimation of cascading failures extent and severity for all possible primary failure initiation events, resulting in a distribution of consequences (US$/h) for many thousands of simulated failures, along with statistical results for the tendency of each network component to participate in LPHC cascading failures. The probability of cascading failures between components- a key input to the system is directly estimated from historical failure data of the same Brazilian system. The consequences of failure are calculated based on the load and generation connected to all substations on a typical day, and the cost per hour of service failure is based on the highest energy cost observed in 2021 for the Brazilian system energy market.

The method provides a cost per hour for the likely cascade failure with the highest direct consequence (loss of revenue), as well as a static risk representing the direct loss per hour to the system operator for a complete service failure in Brazil, without taking into account the broader societal consequences. The simulation found a maximum

probable loss (MPL Risk[SM]) from cascading failure events of US $12.5 million per hour, which is roughly one-quarter of the static risk of US $55.8 million per hour.

This method also measures the system's resilience to cascading failure events using the Lewis Score[SM] normalized scale. The Lewis Score[SM] ranges from zero to ten and has a "tipping point" of five. Below this tipping point any random failure on the network has the tendency to "blow up" into a LPHC event and the network is "fragile". Above the tipping point the network tends to naturally suppress the spread of failures, so consequences stay small and the network is "resilient". Simulations on the Brazilian system estimate its Lewis Score[SM] as 6.2, so the Brazilian Interconnection is resilient to cascading failure events. However, that score as well as MPL Risk[SM] could still be significantly improved by restructuring the network topology and hardening critical assets that tend to disproportionately participate in LPHC cascading failure events, as indicated in Figure 11.

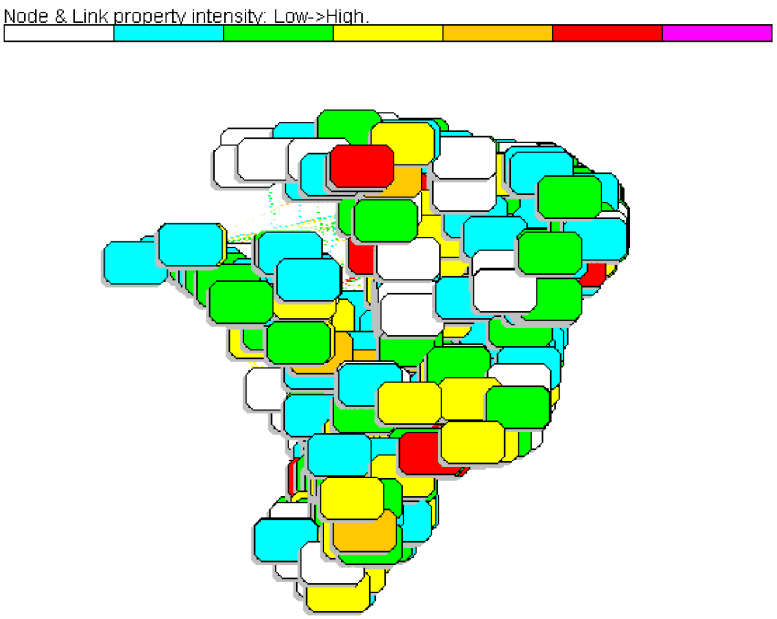

Figure 11 - Critical Assets Heat Map for the Brazilian Power Transmission System [12].

Utilities and communities, and larger regional systems, such as ERCOT, EIPC and WECC, as well as the nation and its regional partners, can benefit from application of an objective resilience methodology. As shown above, many federal agencies are exploring and developing resilience and related security approaches to the challenges of interdependency, Black Swan events, and cascading failures.

At the utility level, it is important for each stakeholder to take charge of their own resilience procedures. For example, local public utility authorities whether municipal or

investor owned, can obtain their own internal measurements, and use these to inform their own engineering and investment priorities. They can also collaborate to look at systems at a larger scale, for example, combining assessments by a university and its surrounding locality or among co-owned water, power, and/or gas providers Engineers will benefit from an identification of critical assets for cascade failures and relevant mitigation; financial planners can use financial risk metrics to evaluate the cost-benefits of mitigation for internal and external financial purposes; and emergency managers can use recovery times associated with LPHC events as a baseline for process improvements, for understanding risk faced by critical customers, and for risk mitigation through resource and recovery order planning. Those focused on energy transition can treat grid resilience as a tool to support that process and well as protect consumer populations.

4. Conclusions

This report discusses resilience standards for interconnected critical infrastructure, especially focused on power systems. It also discusses approaches to resilience established and embraced by related institutions, funded by the DOE and DOD, as well as elements of the Department of Homeland Security and Department of Commerce.

A probabilistic based resilience standard for the industry is deemed necessary for regulation and standardization. The ideal solution would effectively handle interdependent network failures, mitigate unpredictable "Black Swan" events (i.e. all-hazard failures), establish clear guidance on whether or not a network is adequately resilient, and would have a theoretical basis that is orthogonal and complementary to the dominant power systems engineering and modelling approach, that could be extended for water and other critical infrastructure systems. The presented method and the Lewis Score^{SM} satisfy these criteria by providing practical, robust measurement for resilience to LPHC events, including an objective cascade resilience score, maximum probable financial loss, critical asset identification and prioritized mitigation for capital improvement planning, emergency management, and rate applications. Collectively, these provide a new toolset to augment day to day reliability with resilience to unanticipated, large-scale events.

5. Appendix

5.1. Definitions of Resilience in Selected US National Laboratories

US national laboratories associated with the DOE and DOD have recognized a need for resilience solutions for energy and defense infrastructure especially because of climate related disasters and grid related technical challenges associated with distributed energy. The focus of these national laboratories is less on community resilience and more on resilience approaches for energy and defense infrastructure, including a parallel focus on cyber infrastructure and to a lesser extent water infrastructure. In their approaches to the problem, some of the laboratories have proposed resilience methods for general use based on their definitions. We have noted those below.

5.1.1. Sandia National Laboratories

According to the Sandia National Laboratories, sponsored by DOE, Resilience is defined as "the ability to adapt to changing conditions and withstand and rapidly recover from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [49]. This can refer to physical systems, such as infrastructure, or social systems, such as communities or organizations. In the context of national security and emergency management, resilience refers to the ability of individuals, communities, and critical systems to withstand and recover from natural or man-made disasters.

Sandia National Laboratories has developed resilience metrics for the electric power system [50], following a Presidential policy directive defining the energy sector as a uniquely critical infrastructure [51], recognizing that most essential societal functions taken for granted are dependent on energy infrastructure. Communications, transportation, industrial production, banking and finance, and almost every aspect of modern life relies on energy availability and the continuous operation of the electrical power grid. Sandia's proposed approach creates a correlation to associate different consequence categories with specific resilience metrics, dividing them into direct and indirect consequences, as shown in Table 1.

Table 1 - Consequence Categories VS Resilience Metrics from [51]

	Consequence Category	Resilience Metric
Direct	Electrical Service	Cumulative customer-hours of outages Cumulative customer energy demand not served Average number (or percentage) of customers experiencing outage during a specified time period
	Critical Electrical Service	Cumulative critical customer-hours of outages Critical customer energy demand not served Average number (or percentage) of critical loads that experience an outage
	Restoration	Time to recovery Cost of recovery
	Monetary	Loss of utility revenue Cost of grid damages (e.g. repair or replace lines, transformers) Cost of recovery Avoided outage cost
Indirect	Community Function	Critical services without power (e.g., hospitals, fire stations, police stations) Critical services without power for more than N hours (e.g., N > hours of back up fuel requirement)
	Monetary	Loss of assets and perishables Business interruption costs Impact on Gross Municipal Product (GMP) or Gross Regional Product (GRP)
	Other critical assets	Key production facilities without power Key military facilities without power

5.1.2. Idaho National Laboratory

The Idaho National Laboratory (INL), sponsored by DOE, defines resilience as "the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions" [52]. This definition highlights the key components of resilience – the ability to anticipate potential disruptions, prepare for them in advance, and quickly adapt and recover when they do occur. INL's focus is the resilience of critical infrastructure and systems, such as energy, transportation, and communications systems, to ensure the continuity of essential services during and after disruptions.

INL has developed an All-Hazards Analysis (AHA) framework [53] for use critical infrastructure organizations. AHA is a dynamic analysis framework that identifies dependencies and associated risks. The intention is to enable threat discovery and related decision support by providing decision-makers and emergency managers with a comprehensive view of interconnected infrastructure systems.

AHA offers an optimized framework to collect, store, analyze, and visualize critical infrastructure information. It uses a function-based approach to present information as nodes (infrastructure) and links (dependency relationships). AHA can learn to blend general and facility dependency profiles with new information and changes in network structures; this is intended to support modeling and analysis of consequences relating to threats and risks on an infrastructure and sector basis.

INL has also developed a methodology for cyber resilience that is commercializing with partners. The concept is a consequence-driven, cyber-informed engineering (CCE)

methodology. CCE was developed because engineering methods traditionally used in the water and other critical infrastructure sectors do not adequately account for cyber-risk and "bolt-on" cybersecurity solutions designed for information technology systems do not work well for digital ICS. CCE's goal is to improve Industrial Control Systems (ICS) cyber-resilience and reduce the potential for severe consequences and threats in cyber-enabled sabotage [54].

5.1.3. Argonne National Laboratory

The Argonne National Laboratory, sponsored by DOE, presents two aspects of the definition of resilience, one that considers only "after the adverse event" and the second one that also considers "before the adverse event," including assets, resistance, protection, anticipation, and preparedness. An accepted definition for resilience "after the adverse event" is "the capacity of a system to absorb disturbance, undergo change, and retain essentially the same function, structure, identity, and feedbacks." Regarding also "before the adverse event," an accepted definition is the ability to minimize the costs of a disaster, to return to a state as good as or better than the status quo ante, and to do so in the shortest feasible time. Resistance is used to mean the ability to withstand a hazard without suffering much harm. Resilience in this paper will include resistance but will also include the ability to recover after suffering harm from a hazard [55].

5.1.4. Lincoln National Laboratory

A proper definition of Resilience from Lincoln National Laboratory (LNL), sponsored by DOD, could not be found. However, LNL has performed a study evaluating and applying a resilience framework to military installations for the DOD [56]. According to the DOD guidance [57], resilience is defined as "the ability to prepare for and recover from energy disruptions that impact mission assurance on military installations." In the LNL study, availability and reliability were the key metrics to measure different energy resilience solutions and ensure continuous critical mission operations.

5.1.5. Pacific Northwest National Laboratory

Pacific Northwest National Laboratory (PNNL), sponsored by DOE, defines resilience as the ability of a system, organization, or community to prepare for, withstand, adapt to, and recover from disruptions, whether they are acute shocks or chronic stresses. PNNL just released a report to define a framework for quantitative evaluation of resilience solutions to determine the value of resilience for a particular site [58]. The report uses a broader definition of resilience, applied by the Federal Energy Management Program's

Technical Resilience Navigator (TRN): “the ability to anticipate, prepare for, and adapt to changing conditions and to withstand, respond to, and recover rapidly from disruptions through adaptable and holistic planning and technical solutions”. The TRN is a free software that helps organizations manage the risk to critical missions from disruptions in energy and water services. It provides a systematic approach to identifying energy and water resiliency gaps and developing and prioritizing solutions that reduce risk.

6. References

[1] S. Skarvelis-Kazakos, R. Moreno, I. Dobson, M. Panteli, P. Mancarella, A. Jin, I. Linkov, M. Papic, R. Dhrochand, C. Kumar, C. Mak, “Resilience of interdependent critical infrastructure”, Electra, Feb 2022, CIGRE C4.47 working group report.

[2] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 21(6), 11-25.

[3] Busby, Joshua W., et al. “Cascading risks: Understanding the 2021 winter blackout in Texas.” Energy Research & Social Science 77 (2021): 102106.

[4] Glazer, Yael R., et al. “Winter Storm Uri: A Test of Texas’ Water Infrastructure and Water Resource Resilience to Extreme Winter Weather Events.” Journal of Extreme Events (2021): 2150022.

[5] Čepin, M. (2011). Assessment of power system reliability: methods and applications. Springer Science & Business Media.

[6] Power Grid International Website. Retrieved May 23, 2023, from https://www.power-grid.com/executive-insight/13-years-after-the-northeast-black-of-2003-changed-grid-industry-still-causes-fear-for-future/#gref

[7] U.S. Climate Resilience Toolkit, “Understand Exposure”, July 28, 2022, https://toolkit.climate.gov/steps-to-resilience/understand-exposure.

[8] Markolf, Samuel A., et al. "Balancing efficiency and resilience objectives in pursuit of sustainable infrastructure transformations." Current Opinion in Environmental Sustainability 56 (2022): 101181.

[9] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini and A. Sargolzaei, “Toward a Consensus on the Definition and Taxonomy of Power System Resilience,” in IEEE Access, vol. 6, pp. 32035-32053, 2018, doi: 10.1109/ACCESS.2018.2845378.

[10] E. Ciapessoni, D. Cirio, A. Pitto, M. Panteli, M. Van Harte, C. Mak, “Defining power system resilience”, Electra, Oct 2019, CIGRE C4.47 reference paper.

[11] US Department of Energy (DOE) Annual Summary. Retrieved May 17, 2022, from https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

[12] Mouco, A., et al. “Resilience of Power Grids to Catastrophic Cascading Failures “Proc. CIGRE US National Committee 2022 Grid of the Future Symposium, 2022.

[13] National Association of Regulatory Utility Commissioners (NARUC). (2023). Energy Resilience Reference Guide. https://pubs.naruc.org/pub/1C098515-1866-DAAC-99FB-3FBA6FA3AB0B

[14] Duchek, S. (2020) “Organizational resilience: a capability-based conceptualization”. Business Research, 1, 215.

[15] Tallaki, M. & Bracci, E. (2021) “Risk perception, accounting, and resilience in public sector organizations: A case study analysis” Journal of Risk and Financial Management, 14(1), 4.

[16] Sellberg, M. M., Ryan, P., Borgström, S. T., Norström, A. V., & Peterson, G. D. (2018). “From resilience thinking to resilience planning: Lessons from practice”. Journal of Environmental Management, 217, 906-918.

[17] Enck, Robert E. "The OODA loop." Home Health Care Management & Practice 24.3 (2012): 123-124.

[18] Ljunberg, D. & Lundh, V. (2013). “Resilience Engineering within ATM - Development, adaption, and application of the Resilience Analysis Grid (RAG)”. University of Linköping, LiU-ITN-TEK-G--013/080--SE.

[19] Folke, C. (2006). “Resilience: The emergence of a perspective for social-ecological systems analyses”. Global Environmental Change-Human and Policy Dimensions, 16(3), 253-267.

[20] Copeland, S., Comes, T., Bach, S., Nagenborg, M., Schulte, Y., & Doorn, N. (2020). “Measuring social resilience: Trade-offs, challenges and opportunities for indicator models in transforming societies”. International Journal of Disaster Risk Reduction, 51.

[21] Folke, C. et al. “Regime shifts, resilience, and biodiversity in ecosystem management”. Annu. Rev. Ecol. Evol. Syst. 35, 557–581 (2004).

[22] Axtell, Richard. “The Resilience Phenomena: What Does It Mean for Critical Infrastructure Systems Such As Water Utilities?” 2023. National University, Doctoral Dissertation.

[23] Shin, S., Lee, S., Judi, D. R., Parvania, M., Goharian, E., McPherson, T., & Burian, S. J. (2018). “A systematic review of quantitative resilience measures for water infrastructure systems” Water, 10(2), 164.

[24] Wilby, R. L. (2020). “Resilience viewed through the lens of climate change and water management”. Water, 12(9), 2510.

[25] Pagano, A., Pluchinotta, I., Giordano, R., & Fratino, U. (2018). “Integrating “Hard” and “Soft” infrastructural resilience assessment for water distribution systems”. Complexity, 2018.

[26] Allen, C.R., Angeler, D.G., Chaffin, B.C., Twidwell, D. and Garmestani, A., 2019. Resilience reconciled. Nature sustainability, 2(10), pp.898-900.

[27] Milly, P.C., Betancourt, J., Falkenmark, M., Hirsch, R.M., Kundzewicz, Z.W., Lettenmaier, D.P. and Stouffer, R.J., 2008. Stationarity is dead: Whither water management?. Science, 319(5863), pp.573-574.

[28] Gomez, M., Mejia, A., Ruddell, B.L. and Rushforth, R.R., 2021. Supply chain diversity buffers cities against food shocks. Nature, 595(7866), pp.250-254.

[29] Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

[30] ASME Innovative Technologies Institute LLC. All Hazards Risk and Resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach. 1st ed., ASME, 2009. p. 160.

[31] McAllister, Therese P. “Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume II.” (2016).

[32] United Nations Office for Disaster Risk Reduction (UNISDR 2012) Making Cities Resilient Report 2012: My City is Getting Ready! A Global Snapshot of How Local Governments Reduce Disaster Risk, Second Edition, October, The United Nations Office for Disaster Risk Reduction (UNISDR).

[33] NIST Center of Excellence & IN-CORE. Retrieved February 18, 2023 from https://www.nist.gov/community-resilience/center-excellence

[34] Interdependent Networked Community Resilience Modeling Environment (IN-CORE). Retrieved February 18, 2023 from http://resilience.colostate.edu/in_core/

[35] National Academies of Sciences, Engineering, and Medicine. "Resilience for Compounding and Cascading Events." (2022).

[36] Danzig, Richard. Surviving on a diet of poisoned fruit: Reducing the National Security Risks of America's Cyber Dependencies. Center for a New American Security, 2014.

[37] The White House, “Executive Order on Improving the Nation’s Cybersecurity”, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[38] U.S. Department of Commerce, National Institute of Standards and Technology (NIST), May 12, 2022, https://www.nist.gov/system/files/documents/2022/07/11/Report%20to%20President%20-%20Improving%20the%20Nations%20Cybersecurity.pdf

[39] Cybersecurity & Infrastructure Security Agency – CISA. Retrieved September 16, 2023 from https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[40] U.S. Government Accountability Office, Electricity Grid Resilience (Washington, DC: March 2021), https://www.gao.gov/assets/gao-21-346.pdf.

[41] US Department of Homeland Security. Retrieved January 19, 2023 from https://www.dhs.gov/topics/resilience

[42] Moreno, R., Panteli, M., Mancarella, P., Rudnick, H., Lagos, T., Navarro, A., … Araneda, J. C. (2020). From Reliability to Resilience: Planning the Grid Against the Extremes. IEEE Power and Energy Magazine, 18(4), 41–53.

[43] Eastern Interconnection Planning Collaborative (EIPC). Retrieved February 18, 2023 from https://eipconline.com/

[44] EPRI. "Electric Power System Resiliency: Challenges and Opportunities." (2016): 56.

[45] Bernabeu, E., K. Thomas, and Y. Chen. "Cascading Trees & Power System Resiliency." 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). IEEE, 2018.

[46] Barabási, Albert-László. "Network science." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 371.1987 (2013): 20120375.

[47] Lewis, Ted G. "Network science." New Jersey: Wiley and Sons 10 (2009): 9780470400791.

[48] Ouyang, Min. "Review on modeling and simulation of interdependent critical infrastructure systems." Reliability engineering & System safety 121 (2014): 43-60.

[49] Watson, Jean-Paul, et al. “Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States.” Sandia national laboratories, albuquerque, nm (united states), tech. rep (2014).

[50] Vugrin, Eric D., Andrea R. Castillo, and Cesar Augusto Silva-Monroy. Resilience Metrics for the Electric Power System: A Performance-Based Approach. No. SAND2017-1493. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2017.

[51] Obama B., Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, Washington, DC: 2013.

[52] Culler, Megan Jordan, et al. “Distributed Wind Resilience Metrics for Electric Energy Delivery Systems: Comprehensive Literature Review.” (2021).

[53] Idaho National Laboratory, All Hazards Analysis Framework website. Retrieved February 18, 2023 from https://inl.gov/ics-aha/

[54] Groves, Daniel A., et al. "Engineering Cyber–Physical Resilience." Journal: American Water Works Association 113.4 (2021).

[55] Carlson, J. L., et al. Resilience: Theory and Application. No. ANL/DIS-12-1. Argonne National Lab.(ANL), Argonne, IL (United States), 2012.

[56] Judson, Nicholas, et al. Application of a resilience framework to military installations: A methodology for energy resilience business case decisions. MIT Lincoln Laboratory Lexington United States, 2016.

[57] Department of Defense Instruction 4170.11, 2016. Installation Energy Management, Department of Defense. Available from: http://www.dtic.mil/whs/directives/corres/pdf/417011p.pdf.

[58] Weimar, Mark R. Framework for Quantitative Evaluation of Resilience Solutions: An Approach to Determine the Value of Resilience for a Particular Site. No. PNNL-28776. Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2022.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Mouco, A. & Ruddell, B. L., Ginsburg, S. (2023) Resilience to High Consequence Cascading Failures of Critical Infrastructure Networks. (Report No. IHS/CR-2023-1015). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/5R2H6