Robustness and Extensibility in Infrastructure Systems

Daniel A. Eisenberg[1]*, Thomas P. Seager[1], Margaret M. Hinrichs[1], Yeowon Kim[2], Ben A. Wender[3], Samuel Markolf[1], John E. Thomas[1], Mikhail V. Chester[1], David L. Alderson[4], Jeryang Park[5], Ying-Cheng Lai[6], Igor Linkov[7], Susan Spierre Clark[8], and David Woods[9]

[1]School of Sustainable Engineering and the Built Environment, Arizona State University, Tempe, AZ, USA
[2]School of Sustainability, Arizona State University, Tempe, AZ, USA
[3]United States National Academy of Sciences, Washington D.C., USA
[4]Operations Research Department, Naval Postgraduate School, Monterey, CA, USA
[5]School of Urban and Civil Engineering, Hongik University, Seoul, South Korea
[6]School of Electrical, Computer, and Energy Engineering, Arizona State University, Tempe, AZ, USA
[7]United States Army Corps of Engineers – Engineer Research and Development Center, Environmental Laboratory, Concord, MA, USA
[8]RENEW Institute, University of Buffalo, Buffalo, NY, USA
[9]Department of Integrated Systems Engineering, The Ohio State University, Columbus, OH, USA

*Corresponding Author: daeisenb@asu.edu

Abstract
Resilient infrastructure research has produced a myriad of conflicting definitions and analytic frameworks, highlighting the difficulty of creating a foundational theory that informs disciplines as diverse as business, engineering, ecology, and disaster risk reduction. Nevertheless, there is growing agreement that resilience is a desirable property for infrastructure systems – i.e., that more resilience is always better. Unfortunately, this view ignores that a single concept of resilience is insufficient to ensure effective performance under diverse stresses. Scholarship in resilience engineering has identified at least four irreducible resilience concepts, including: rebound, robustness, graceful extensibility, and sustained adaptability. In this paper, we clarify the meaning of the word resilience and its use, explain the advantages of the pluralistic approach to advancing resilience theory, and expound two of the four conceptual understandings: robustness and graceful extensibility. Furthermore, we draw upon examples in electric power, transportation, and water systems that illustrate positive and negative cases of resilience in infrastructure management and crisis response. The following conclusions result: 1) robustness and extensibility are different strategies for resilience that draw upon different system characteristics, 2) neither robustness nor extensibility can prevent all hazards, and 3) while systems can perform both strategies simultaneously, their drawbacks are different.

Keywords
Infrastructure; Resilience; Resilience Engineering; Electric Power Systems; Water Systems; Transportation Systems

1. Introduction

Prior to Holling's (1973) seminal publication, the word "resilience" was used in few scientific settings – notably, in materials science to describe elastic deformation under stress, and in psychiatry and psychology to describe the characteristics of individuals that allow them to recover from psychological trauma (Alexander 2013). These understandings of the word are analogous and consistent with the etymological roots of its original verb form, *to resile*, meaning "to return to a former position" (Alexander 2013), which is sometimes interpreted as "to bounce back" (e.g., Meerow, Newell, & Stults, 2016). Building upon Holling's work, this understanding persists in the natural sciences through groups like the Resilience Alliance, which describes resilience as "the capacity of a social-ecological system to absorb or withstand perturbations and other stressors such that the system remains within the same regime, essentially maintaining its structure and functions" (C. S. Holling 1973; Holling and Gunderson 2002; Walker et al. 2004; Alliance 2017). More recently, usage of resilience has increased exponentially across various disciplines (Rose 2017) with each new adoption resulting in efforts to redefine its meaning to fit the purposes of broad applications like business, sustainability, and disaster risk reduction (Hosseini, Barker, and Ramirez-Marquez 2016). For example, the United States National Academy of Sciences now defines disaster resilience as "the ability to plan and prepare for, absorb, recover from, and adapt to adverse events" (NAS 2012), where the United Nations defines disaster resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions," (UNISDR 2012). Both definitions draw upon the retrospective concept of returning to a former position through a process of recovery, but also include future and present temporal perspectives that seek to minimize hazardous outcomes in the first place. Holling's work expanded "resilience" from simple (material elasticity) and individual (psychology) applications to *complex* systems. Accommodating these new applications, understandings of the word resilience itself were made more complex.

In ecology, resilience is a descriptive term that does not suggest one system state is better than any other. By contrast, in psychology, business, engineering, and other disciplines resilience is a normative term that largely suggests a preference for the status quo. The difference is most evident in contrasting the incorporation of recovery into the definitions of disaster resilience. To ecologists, recovery processes were dubbed "engineering resilience" (Gallopín 2006) to segregate them from socio-ecological perspectives, despite this misnomer ignoring *technological* systems in the Resilience Alliance's canonical definition. Still, the distinction is of critical importance as the dominant view in design disciplines such as engineering, architecture, and urban planning is that resilience is a *good* thing that successful systems do, need, or have when faced with adversity (Haimes 2009), suggesting more resilience is always better. This view is also evident in psychology, psychiatry, management, sustainability, and disaster risk reduction where resilience is the result of enacting *positive* coping capacities to better manage hazards and risks (Meerow, Newell, and Stults 2016). However, the original verb *resile* is not meant to evoke success. Rather, it has pejorative connotations, as in reneging on a commitment or retreating from a prior position (Alexander 2013). The positive perspectives of resilience which now dominate research overlook this pejorative definition and may limit theoretical progress by also overlooking possible ways systems cope with change.

The idea that resilience might be both positive *and* negative is resurrected here to provide greater clarity and illustrative examples to two particular concepts of resilience important to infrastructure systems: robustness and extensibility. In particular, this paper describes how robustness and extensibility concepts guide different activities to maintain infrastructure services under stress while simultaneously being the reason infrastructure services may be lost. To establish a foundational theory of resilience that is broadly generalizable, resilience research must realize the differences between concepts that only become clear when discussing both their desirable and undesirable qualities (Mochizuki et al. 2017). In our view, resilience research must shift from identifying which concept is superior to identifying use of both in practice and how to facilitate switching between them when needed. In this paper, we expound upon robustness and extensibility and draw upon examples in electric power, water management, and transportation systems to illustrate their positive and negative implications for infrastructure management and crisis response.

1.1 Risk and Resilience in Infrastructure Systems

Improving the resilience of infrastructure systems is meant to protect them from unforeseen and unknown threats, yet confusion remains over what resilient infrastructure is. "Resilience" entered the civil protection lexicon through materials science, medicine, psychology, social science, and ecology and has recently become a popular word describing the ability of infrastructure components and systems to handle adversity (Park et al. 2013; Eisenberg, Park, Bates, et al. 2014; Linkov et al. 2014). In the context of infrastructure, resilience is generally associated with the design of built systems and actions that ensure the provision of services like mobility, energy, and water when faced with threats (Francis and Bekera 2013; Bruneau et al. 2003). Even with broad consensus on the need to maintain the structure and function of built systems, literature reviews seeking to condense the growing number of research articles into specific definitions, metrics, methods, and applications continue to produce conflicting views. Resilience is often likened to divergent concepts like risk (Park et al. 2013; Park, Seager, and Rao 2011), reliability (Pettersen and Schulman 2015), sustainability (Seager 2008), adaptive capacity (Eisenberg, Park, Kim, et al. 2014), and transformation (Amir and Kant 2017). Confusion is further amplified as numerous research articles and policy documents from influential organizations discuss infrastructure resilience (e.g., TRB 2011) or use resilience in their title (e.g., Wang et al. 2015) but fail to be informed by a mature theoretical understanding of resilience that can be broadly applied.

Part of the reason that resilience is so difficult to apply in infrastructure systems is that the word itself occupies an awkward position in the English language. Although "resilience" is used as a noun, the most popular definitions describe it as a *capacity to act* – which makes resilience an action or property that systems *perform*, like a verb, rather than a property that a system *has*, like a noun. Table 1 compares different forms of the words "risk" and "resilience" to further illustrate this point. While both risk and resilience work well as abstract nouns, only risk works as a quantifiable noun. This may explain some of the difficulty that researchers have coming up with quantifiable, concrete measures of resilience for infrastructure. On the other hand, the action verb form of risk is a poor choice, whereas the word resile, although obscure, is nonetheless proper and useful. Risk works well as a linking or helping verb, but resile does not. The ways in which we can use these words in English creates constraints around the ways we think about them for infrastructure design and management. We can see that both risk and resilience can be used in noun and verb forms, but that risk works better as an objective, quantifiable noun and helping verb, whereas resilience works better as an action verb. We should think of infrastructure resilience not just in the *capacity* to act, but *in the action itself.* Consequentially, the tools and methods for measuring and addressing infrastructure risks are not appropriate for resilience, as these two related concepts are fundamentally different.

Table 1 | Comparison of the noun and verb forms of risk and resilience

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

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

Infrastructure resilience as a verb endorses designing built systems with beneficial properties such as diversity (Ahern 2011) or efficiency (Fiksel 2003) to maintain service provision, as well as systems that have the capacity to *switch between* these properties. Major resilience research efforts across disciplines promote the need for an array of beneficial system properties that influence infrastructure failure response (see Kim et al., 2017 for a more comprehensive list of properties). However, designing built systems with beneficial qualities like efficient failure response systems is often in conflict with increasing the diversity of response options, as too many different technologies or decision-makers may inhibit timely crisis response (Roege et al. 2014). In contrast, efficient systems may fail in unknown and unforeseen situations that require a diversity of failure response options to maintain service provision (Fiksel 2003). Neither approach is perfect nor resilient. That is, resilience would neither be found in infrastructure systems that emphasize efficiency nor diversity, but rather in systems with a capacity to deploy efficiency in some scenarios and diversity in others. We refer to the act of designing infrastructure systems to have some combination of efficient, diverse, or otherwise beneficial properties as pursuing different *resilience strategies*. The shift from focusing on system properties to resilience strategies is important because any single strategy can help maintain a continuity of needs in the present, but if practiced forever may eventually fail. A theory of resilience therefore cannot promise complete protection of built systems and services against all adverse events, but it could reveal the benefits and limitations of different adaptive strategies in practice. The verb resile in this context refers to need to switch between strategies when current practices are found to be impractical or dangerous, e.g., when efficiency trumps diversity, or vice versa.

1.2 Concepts of Resilience for Infrastructure Systems

We build upon work in the subdiscipline of "resilience engineering" to realize how different resilience strategies may be implemented in infrastructure systems. Resilience engineering has a large and growing body of literature with roots in system safety and organizational theory relevant to the design and management of infrastructure (Jackson and Ferris 2012; Seager et al. 2017). In general, authors within the subdiscipline share consistent views of resilience as an action systems *do,* rather than a property they have (e.g., Hollnagel, 2014; Hollnagel, Woods, & Leveson, 2007; Madni & Jackson, 2009). Still, the subdiscipline has more than three decades of development and debate that contrast different strategies to engineer systems to handle unknown and unforeseen events (Righi, Saurin, and Wachs 2015; Le Coze 2015; Haavik et al. 2016). Recently, four concepts of resilience extant in the literature were distinguished that can form the basis for resilience strategies in infrastructure systems (Woods 2015; Seager et al. 2017):

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

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

2. Robustness as a Resilience Strategy

Robustness as a resilience strategy emphasizes active buffering and dynamic reallocation of resources in response to known hazards and in accordance with explicit protocols, policies, or procedures, while accepting the inevitability that surprises may lead to catastrophic losses. For example, highway rules sometimes allow travel in shoulder lanes during periods of peak travel or inclement weather, called "hard shoulder running" (Buckeye 2012; Chun and Fontaine 2016). Under ordinary conditions travel in the roadway shoulder would be prohibited, with the space at the side of the road reserved for emergency and broken-down vehicles. However, during times expected to be peak travel periods, some rules designate the shoulders for travel, increasing the capacity of the roadway and mitigating the likelihood of traffic jams. While this policy is adaptive in the sense that it deploys the capacity of the roadway shoulder only when the normal travel lanes would be overwhelmed, this dynamic reallocation of resources also leaves the highway system vulnerable to massive congestion. Without a shoulder, crashes or breakdowns will cause even greater impacts to traffic given that response vehicles (e.g., police, tow trucks) will be delayed without a clear path by which to reach the site of the emergency.

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

Still, pursuing robustness exclusively for infrastructure protection will never ensure a continuity of services to all hazards. It emphasizes threat identification as the first and foremost step prior to any design actions. Nonetheless, any attempt to prevent one type of failure may increase the likelihood and damages experienced from others (Alderson and Doyle 2010). When robustness fails, it typically is because reallocation of resources results in sudden and catastrophic collapse when system loads become overwhelming, or the system encounters unexpected stressors for which no contingency exists.

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

2.1 Designing Robust Infrastructure Systems

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

Even when using linear models and simple equations, calculating the flow of resources like electricity, water, data, and traffic is a demanding task. The most effective robust designs consider all aspects of future hazards and system dynamics, including how system losses propagate in many different operational scenarios. Computers can complete these tasks flawlessly in fractions of time. This characteristic difference in precision and throughput between technology and people can be further expanded to suggest that technology will outperform people when completing any complex task with explicit rules such as driving (Fagnant and Kockelman 2015) and games like Go (Lee et al. 2016). Each of these systems epitomizes robustness by averting anticipated hazards through well-defined tasks and by experiencing difficulty when managing situations with ill-defined rules. Because technologies have the throughput and precision to ensure robustness and lack the fallibility of humans in well-defined scenarios, robustness is largely a technological hazard prevention strategy,

Although computerized systems epitomize robust operations, robust approaches to resilience can also be carried out by people when conforming to prescribed responses to known threats. For example, generation-load dispatch in power grids can be optimized to reduce the probability of losses to unusual weather, rare and novel threats like geomagnetic disturbances (Lu et al. 2017), and hurricanes (Pasqualini 2017). To realize these adaptive actions, sensor information is used to update operational protocols and reliable human responses. Robustness enhancing policies include N-k reliability standards that require operations of N interconnected infrastructures to survive k failures without reduction in service constraints. The standard for electric power grids is N-1 reliability (Corporation 2014), where systems are designed to continue functioning after the loss of any single infrastructure, but is not necessarily guaranteed for a larger number of failures. Similar thresholds exist in infrastructure operations, including limits on the number of system errors allowed to occur and their impact on customer access to services (Roe and Schulman 2012). Thus, robustness requires explicit contingency policies that demand reliable human actions.

2.2 Tradeoffs of Pursuing Robustness in Infrastructure Systems

Robustness has limitations for managing inconceivable threats that may prove disastrous. Improving a system to handle a known threat can increase the likelihood that other threats will cause greater damages, as has been demonstrated in control theory (Alderson and Doyle 2010). This tradeoff exists when implementing any of the adaptive robustness strategies described above in infrastructure systems – redesigning the interactions among built components, changing operational methods, and developing regulatory thresholds for ordinary operations – where tradeoffs exist even among robustness strategies themselves. In complex systems, this is referred to as the conservation of fragility (Doyle et al. 2005; Alderson and Doyle 2010) and is most pronounced in systems highly optimized to few, specific threats. The more robustness is pursued to increase the resilience of infrastructure, the greater the risk that catastrophic failures can occur from unforeseen events.

In some cases, robust contingency plans remain underdeveloped because rare events are misunderstood as inconceivable – even when they are well within the imagination of infrastructure operators and managers. The near-breaching of the Oroville Dam in California serves an important case of imagined catastrophes being realized. In 2005, several environmental groups expressed concern that allowing high water levels to overtop a secondary (i.e., emergency) spillway may cause significant damage to the dam, surrounding power plants, fisheries, communities, and waterways (Sierra Club, 2005). Although infrastructure managers refuted this vision by claiming the safety of the dam and reservoir control would not be compromised in the event of an emergency spillway discharge (FERC, 2006), a surge of rain and melting snow pack in February 2017 combined with a structural failure of the main spillway overwhelmed the capacity of existing operating procedures to ensure the safety of downstream communities. The realization of events outside operational routine and thresholds demonstrate the potential drawbacks of robust infrastructure management (FERC, 2006).

3. Extensibility as a Resilience Strategy

An extensible infrastructure system seeks the same outcome as a robust system, which is to prevent loss of services by protecting the system against hazards. However, extensible infrastructure systems achieve protection in a contradictory way to robustness – by defying rules and protocols rather than shoring them up. Events like Deepwater Horizon and the Fukushima Daiichi Meltdown were exacerbated into disasters by built systems working (and failing) in known ways and people following the rules to manage them (Park et al., 2011). Seminal works by Perrow (1984) and Hollnagel et al. (2014) argue that these events are caused by characteristically different stressors from faults or disruptions, called *surprises,* that cannot be anticipated *a priori*. However, even where hazards are pre-conceived, contingencies plans will fail in the face of complexity, as a sufficient number of simultaneous disruptions, feedback loops, or maladaptive responses can result in "normal accidents" (Perrow 1984) that amplify consequences beyond any previous expectations.

Following the rules and norms established for the operation and management of these cascading, unforeseen scenarios may only exacerbate damages (Hollnagel and Goteman 2004). In these cases, extensibility is needed to break established systems, norms, rules, or expectations to arrest failures. Thus, we define extensibility in infrastructure systems as the adaptive modification of existing system structures and functions to prevent losses resulting from surprise.

In contrast to the United Airlines example of robustness failure, the actions of Captain Sullivan in the case of US Airways 1549 after dual engine failure exemplify abandoning robustness in favor of extensibility. According to Capt. Sullivan's testimony and after action findings, it was only by departing from established procedures that the pilots were able to land the plane in the Hudson river without a single loss of life (NTSB, 2010). While the crew was trained in emergency procedures for engine failure, these procedures assumed cruising altitude and never anticipated total loss of engine thrust at a low altitude so soon after takeoff. The resulting checklists for dual engine failure included many more checks than the pilots had time to complete prior to emergency landing (NTSB, 2010). In this event, following the explicit rules prior to ditching may have led to catastrophe by slowing decision-making processes. Instead, the pilots extended response protocols by skipping several recommended tasks and improvising a safe response.

3.1 Designing Extensible Infrastructure Systems

Extensibility requires that infrastructure systems have controls that can be turned on, shut down, modified, or moved to arrest surprising threats. These controls allow human discretion. For example, modern office buildings increasingly use motion detectors to control lights and faucets, thereby avoiding the waste associated with lighting unoccupied rooms or running water into empty sinks. However, almost all modern office occupants have experienced the frustration of having the automatic light switches turn off accidentally, or the frustration of waving their hands in front of an automatic faucet in an attempt to get running water. Manual light switches and faucets are the consumer analog of circuit breakers in power systems (Chen, Wang, and ton 2017), activated floodways in streamflow management systems (Park et al. 2013), and ad hoc communication networking devices (Loo, Mauri, and Ortiz 2012). Although these systems are sometimes used for normal infrastructure operations--e.g., in power distribution systems and roadway management--they enable humans to respond to surprises by opening and closing paths for service flow, allowing infrastructure to function beyond designed thresholds, and switching on and off backup resources.

Extensibility is engineered into various infrastructure systems through the use of human-in-the-loop systems that enable people to rearrange physical dependencies, system operation, and management processes. These systems are evident in control rooms where operators manipulate the structure and function of built systems. For example, all major factories and plants use supervisory control and data acquisition systems (SCADA) to collect and display real-time data on the function of working infrastructure (e.g., a turbine) and enable operators to modify infrastructure working conditions (e.g., is the turbine on or off). A common operator practice is to disregard information these systems display as SCADA systems are notorious for calculating and displaying unrealistic system errors (Schulman et al. 2004), many of which are either benign, or if acted upon, would increase the possibility of a disruption to critical services . In response, operators must identify and ignore these errors, or in certain cases, actively generate them (Roe and Schulman 2012) to maintain continuous service provision. Assuming that there is no prescribed way in which SCADA errors are ignored or initiated, control room operators are practicing infrastructure extensibility by applying their own expert heuristics to unpredictable circumstances.

Infrastructure policies that promote extensibility use imprecise language in support of context-specific implementation. Designing extensible infrastructure systems requires that people associated with infrastructure operations and management have the ability to influence and redirect service provision. While policies for robust solutions assign explicit thresholds and roles for infrastructure providers, extensible policies have “strategic ambiguity” (Davenport and Leitch 2005) to empower people to act on their own volition. For example, military doctrine has now adopted the principal of “commander’s intent” that allow for ingenuity and adaptation in the field (Shattuck and Woods 2000). The commander’s intent gives high level, strategic direction, but remains ambiguous in the specific tactics or pathways that may be used to achieve the intent. Similarly, standards for developing and maintaining manufacturing robots utilize ambiguous language, using the term “justifiable trust” for the necessary amount of trust the technological system is meant to display to the human operators that work with them (Eder, Harper, and Leonards 2014). The ambiguous nature of this term is purposeful to force a broad interpretation of trust across many manufacturing industries and foster systems with flexible approaches to sociotechnical safety. This ambiguity supports extensibility by requiring infrastructure providers to continuously manage shifting interpretations of trust across their respective industries similar to shifting international politics surrounding nuclear and cyber warfare (Libicki 2011).

3.2 Tradeoffs of Pursuing Extensibility in Infrastructure Systems

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

We refer to these processes collectively as “decompensation”: when a sociotechnical system exhausts its extensibility in a way that jeopardizes other hazard prevention activities (Woods and Branlat 2011). An example of decompensation in infrastructure systems comes from roadway management. Deployable traffic control equipment can be used to create a detour around accidents for the safety of local drivers. While this detour exists, the use of equipment may increase the risk of a major traffic jam as other accidents and crisis situations cannot be detoured because traffic control equipment is already committed. In this example, the road system may experience a brittle failure (sudden, large traffic jam) as the routine activity (detour) is unavailable when extensible resources (traffic control equipment) are committed to other activities (working at cross purposes).

Not all extensibility is “graceful”. Where decompensation results in a degradation of performance, a system may be extended in ways that management may fail to recognize – even in the face of overwhelming evidence. For example, evidence of decompensation can be found in “near misses” (Woods 2006), when catastrophic failure was narrowly avoided through some human ingenuity and adaptation. However, people may misinterpret the lesson from the near miss as evidence that they are more robust than they really are, rather than interpreting the near miss as evidence of decompensation. The ongoing water quality crisis in Flint, Michigan emphasizes the danger of overlooking near misses. In 2014, the decision for the City of Flint to change water sources from Detroit to the Flint River extended distribution systems to convey water with historically worse water quality (Masten, Davies, and McElmurry 2016). Subsequent discovery of pathogens and corrosive chemicals in city water led to a series of boil water warnings and attempts by local residents to switch water sources again, this time away from the Flint River (Zahran, McElmurry, and Sadler 2017). Attempts to change water sources were rebuked by government officials believing corrective actions taken by the Michigan Department of Environmental Quality to treat

Flint River water were effective (Pulido 2016). This failure to recognize decompensation exacerbated the initial extensibility of built systems to use a new water source and human actions to continually correct mounting issues. Eventually, the failure to act upon early issues regarding E coli and corrosion exposed residents to water with Legionnaires disease (Masten, Davies, and McElmurry 2016) and an unsafe concentration of lead (Zahran, McElmurry, and Sadler 2017).

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

4. Comparison of Robustness and Graceful Extensibility for Infrastructure Systems

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

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

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

Robustness and extensibility in infrastructure systems require distinct implementation strategies. Summarized in Tables 2 and 3 is a non-exhaustive list of ways in which both strategies can be implemented in infrastructure systems with specific examples for electric power, transportation, and water systems. This list is based upon well-known approaches used by infrastructure designers, operators, and managers to maintain the structure and function of built systems and provides a new organization of these strategies based on robustness and extensibility. Rows within the tables compare robustness and extensibility strategies across different infrastructure systems. For example, manual switchgear in power systems offers equivalent control over power flow as deployable traffic equipment in roadways and activated floodways in flood control systems (Table 3). Cells across Tables 2 and 3 offer comparison between robustness and extensibility strategies in practice. For example, using automated flow regulating devices is a robustness strategy to flood management that is built directly into the water infrastructure system (Table 2). Likewise, activated floodways that must be opened or destroyed to control floodwaters could be extensible infrastructures built into the system wherever operating rules require expert judgment for their actuation. Both flood control infrastructures provide the same services, but in characteristically different ways.

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

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

None of the strategies in Table 2 for designing robust built systems, operational protocols, and/or policies preclude those in Table 3 for gracefully extensible systems. In other words, infrastructure systems can and are designed to have a redundancy of options that support both robust and extensible hazard prevention strategies. One example would be an activated infrastructure that has both automatic systems to prevent known failures and human activated systems to enable extensibility such as some microgrids in power systems that have automatic and on-site control systems. However, few infrastructure components or systems are designed for this form of optionality, making it difficult to fund redundancy among strategies. In current infrastructure operations and management environments with limited time and money, infrastructure providers will be faced with choosing to employ one strategy or the other.

Table 2 | Robust infrastructure implementation strategies

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

Note: sources for table contents – [1](NAS 2017), [2](Markolf et al. 2017; Meyer and Weigel 2011; Meyer et al. 2011; TRB 2011), *and* [3](FEMA 2013; Balcazar 2012; Le Dinh et al. 2007; Dawson et al. 2011; Park et al. 2013).

Table 3 | Extensible infrastructure implementation strategies

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

Note: sources for table contents – [1](NAS 2017), [2](Fawcett et al. 2015; ITS International 2017; SMART Motorway Tunnel 2017; Markolf et al. 2017)*, and* [3](Park et al. 2013; Ahern 2011; Dawson et al. 2011; Le Dinh et al. 2007; Balcazar 2012; FEMA 2013)

5. Conclusion

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

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

Acknowledgements

This material is based upon work supported by the National Science Foundation (NSF) (grant #1311230 & 1441352). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

Ahern, Jack. 2011. “From Fail-Safe to Safe-to-Fail: Sustainability and Resilience in the New Urban World.” Landscape and Urban Planning 100 (4). Elsevier B.V.: 341–43. doi:10.1016/j.landurbplan.2011.02.021.

Alderson, David L., and John C. Doyle. 2010. “Contrasting Views of Complexity and Their Implications For Network-Centric Infrastructures.” IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 40 (4): 839–52. doi:10.1109/TSMCA.2010.2048027.

Alexander, D.E. 2013. “Resilience and Disaster Risk Reduction: An Etymological Journey.” Natural Hazards Earth System Sciences 13 (11): 2707–16. doi:10.5194/nhess-13-2707-2013.

Amir, Sulfikar, and Vivek Kant. 2017. “Sociotechnical Resilience: A Preliminary Concept.” Risk Analysis 0 (0). doi:10.1111/risa.12816.

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

Bruneau, Michel, Stephanie E. Chang, Ronald T. Eguchi, George C. Lee, Thomas D. O’Rourke, Andrei M. Reinhorn, Masanobu Shinozuka, Kathleen Tierney, William A. Wallace, and Detlof Von Winterfeldt. 2003. “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities.” Earthquake Spectra 19 (4): 733–52. doi:10.1193/1.1623497.

Buckeye, Kenneth R. 2012. “Innovations on Managed Lanes in Minnesota.” Public Works Management & Policy 17 (2): 152–69. doi:10.1177/1087724X11430001.

Chen, Chen, Jianhui Wang, and Dan Ton. 2017. “Modernizing Distribution System Restoration to Achieve Grid Resiliency Against Extreme Weather Events: An Integrated Solution.” Proceedings of the IEEE 105 (7). doi:10.1109/JPROC.2017.2684780.

Chun, Pil Jin, and Michael D. Fontaine. 2016. “Evaluation of the Impact of the I-66 Active Traffic Management System.” Virginia Transportation Research Councail (VRTC) Report. Accessed July 2017. http://www.virginiadot.org/vtrc/main/online_reports/pdf/17-r5.pdf

Davenport, S, and S Leitch. 2005. “Circuits of Power in Practice: Strategic Ambiguity as Delegation of Authority.” Organization Studies 26 (11): 1603–23. doi:10.1177/0170840605054627.

Dawson, Richard J., Tom Ball, Jonathan Werritty, Alan Werritty, Jim W. Hall, and Nicolas Roche. 2011. “Assessing the Effectiveness of Non-Structural Flood Management Measures in the Thames Estuary under Conditions of Socio-Economic and Environmental Change.” Global Environmental Change 21 (2). Elsevier Ltd: 628–46. doi:10.1016/j.gloenvcha.2011.01.013.

Doyle, John C, David L Alderson, Lun Li, Steven Low, Matthew Roughan, Stanislav Shalunov, Reiko Tanaka, and Walter Willinger. 2005. “The ‘robust yet Fragile’ nature of the Internet.” Proceedings of the National Academy of Sciences of the United States of America 102 (41): 14497–502. doi:10.1073/pnas.0501426102.

Eder, Kerstin, Chris Harper, and Ute Leonards. 2014. “Towards the Safety of Human-in-the-Loop Robotics: Challenges and Opportunities for Safety Assurance of Robotic Co-Workers’.” Proceedings - IEEE International Workshop on Robot and Human Interactive Communication 2014–Octob (October): 660–65. doi:10.1109/ROMAN.2014.6926328.

Eisenberg, Daniel A., Jeryang Park, Dongwhan Kim, and Thomas P. Seager. 2014. “Resilience analysis of critical infrastructure systems requires integration of multiple analytical techniques.” Urban Sustainability and Resilience (USAR) Conference. London, U.K. Accessed July 2017. https://figshare.com/articles/Resilience_analysis_of_critical_infrastructure_systems_requires_integration_of_multiple_analytical_techniques/3085810

Eisenberg, Daniel A, Jeryang Park, Matthew E Bates, Cate Fox-lent, Thomas P Seager, and Igor Linkov. 2014. “Resilience Metrics: Lessons from Military Doctrines.” The Solutions Journal. https://www.thesolutionsjournal.com/article/resilience-metrics-lessons-from-military-doctrines/

Transportation Research Board (TRB) Special Task Force on Climate Change and Energy. 2011. "Adapting Transportation to the Impacts of Climate Change: State of Practice 2011." Transportation Research Circular. Washington, DC. http://onlinepubs.trb.org/onlinepubs/circulars/ec152.pdf.

Fagnant, Daniel J., and Kara Kockelman. 2015. "Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations." Transportation Research Part A: Policy and Practice 77. Elsevier Ltd: 167–81. doi:10.1016/j.tra.2015.04.003.

Fawcett, William, Ignacio Robles Urquijo, Hannes Krieg, Martin Hughes, Lars Mikalsen, and Óscar Ramón Ramos Gutiérrez. 2015. "Cost and Environmental Evaluation of Flexible Strategies for a Highway Construction Project under Traffic Growth Uncertainty." Journal of Infrastructure Systems 21 (3): 5014006. doi:10.1061/(ASCE)IS.1943-555X.0000230.

Federal Emergency Management Agency (FEMA). 2013. "Mitigation Ideas: A Resource for Reducing Risk to Natural Hazards." Accessed July 2017. https://www.fema.gov/ar/media-library/assets/documents/30627

Federal Energy Regulatory Commission (FERC). 2006. "Office of Energy Projects Emergency Spillway Re-Evaluation."

Fiksel, Joseph. 2003. "Designing Resilient, Sustainable Systems." Environmental Science & Technology 37 (23): 5330–39.

Francis, Royce, and Behailu Bekera. 2013. "A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems." Reliability Engineering and System Safety 121. Elsevier: 90–103. doi:10.1016/j.ress.2013.07.004.

Friends of the River Sierra Club South Yuba River Citizens League (Sierra Club). 2005. "Motion to intervene."

Gallopín, Gilberto C. 2006. "Linkages between Vulnerability, Resilience, and Adaptive Capacity." Global Environmental Change 16 (3): 293–303. doi:10.1016/j.gloenvcha.2006.02.004.

Haavik, Torgeir K, Stian Antonsen, Ragnar Rosness, and Andrew Hale. 2016. "HRO and RE: A Pragmatic Perspective." Safety Science. The Authors. doi:10.1016/j.ssci.2016.08.010.

Haimes, Yacov Y. 2009. "On the Complex Definition of Risk: A Systems-Based Approach." Risk Analysis 29 (12): 1647–54. doi:10.1111/j.1539-6924.2009.01310.x.

Holling, C. S. 1973. "Resilience and Stability of Ecological Systems." Annual Review of Ecology and Systematics 4: 1–23.

Holling, C. S., and Lance H. Gunderson. 2002. "Resilience and Adaptive Cycles." In Panarchy: Understanding Transformations in Human and Natural Systems, 25–62. Island Press.

Hollnagel, Erik. 2014. "Resilience Engineering and the Built Environment." Building Research & Information 42 (2). Taylor & Francis: 221–28. doi:10.1080/09613218.2014.862607.

Hollnagel, Erik, and Örjan Goteman. 2004. "The Functional Resonance Accident Model." Proceedings of Cognitive System Engineering in Process Plant, 155–61. http://82.94.179.196/bookshelf/books/403.pdf.

Hollnagel, Erik, David D. Woods, and Nancy Leveson. 2007. Resilience Engineering: Concepts and Precepts. Ashgate Publishing Ltd.

Hosseini, Seyedmohsen, Kash Barker, and Jose E. Ramirez-Marquez. 2016. "A Review of Definitions and Measures of System Resilience." Reliability Engineering & System Safety 145. Elsevier: 47–61. doi:10.1016/j.ress.2015.08.006.

ITS Interational. 2017. "HDR Predicts an Adaptable and Flexible Future for Roadways." Accessed July 2017. http://www.itsinternational.com/categories/charging-tolling/features/hdr-predicts-an-adaptable-and-flexible-future-for-roadways/.

Jackson, Scott, and Timothy L J Ferris. 2012. "Resilience Principles for Engineered Systems." Systems Engineering 16 (2): 152–64. doi:10.1002/sys.

Le Coze, Jean Christophe. 2015. "Vive La Diversite! High Reliability Organisation (HRO) and Resilience Engineering (RE)." Safety Science. Elsevier Ltd. doi:10.1016/j.ssci.2016.04.006.

Le Dinh, Tuan, Wen Hu, Pavan Sikka, Peter Corke, Leslie Overs, and Stephen Brosnan. 2007. “Design and Deployment of a Remote Robust Sensor Network: Experiences from an Outdoor Water Quality Monitoring Network.” Proceedings - Conference on Local Computer Networks, LCN, 799–806. doi:10.1109/LCN.2007.49.

Lee, Chang Shing, Mei Hui Wang, Shi Jim Yen, Ting Han Wei, I. Chen Wu, Ping Chiang Chou, Chun Hsun Chou, Ming Wan Wang, and Tai Hsiung Yan. 2016. “Human vs. Computer Go: Review and Prospect.” IEEE Computational Intelligence Magazine 11 (3): 67–72. doi:10.1109/MCI.2016.2572559.

Libicki, Martin C. 2011. “The Strategic Uses of Ambiguity in Cyberspace.” Military and Strategic Affairs 3 (3): 3–10.

Linkov, Igor, Todd Bridges, Felix Creutzig, Jennifer Decker, Cate Fox-Lent, Wolfgang Kröger, James H. Lambert, et al. 2014. “Changing the Resilience Paradigm.” Nature Climate Change 4 (6). Nature Publishing Group: 407–9. doi:10.1038/nclimate2227.

Loo, Jonathan, Jaime Lloret Mauri, and Jesús Hamilton Ortiz. 2012. Mobile Ad Hoc Networks: Current and Future Trends. CRC Press. https://books.google.com/books?hl=en&lr=&id=k-zRBQAAQBAJ&oi=fnd&pg=PP1&dq=%22Networks+of+Networks%22+AND+%22Review%22&ots=aiqLlt2jtB&sig=8Mjx9_Dw7SB6qxCr4SNDsmnCpnQ#v=onepage&q=%22Networks of Networks%22 AND %22Review%22&f=false.

Lu, M., H. Nagarajan, E. Yamangil, R. Bent, and S. Backhaus. 2017. “Optimal Transmission Line Switching under Geomagnetic Disturbances,” 1–8. http://arxiv.org/abs/1701.01469.

Madni, A M, and S Jackson. 2009. “Towards a Conceptual Framework for Resilience Engineering.” IEEE Systems Journal 3 (2): 181–91. doi:10.1109/JSYST.2009.2017397.

Markolf, Samuel A., Christopher Hoehne, Andrew Fraser, Mikhail V. Chester, and B. Shane Underwood. 2017. “Transportation Resilience to Climate Change and Extreme Weather Events – Beyond Risk and Robustness.” Transport Policy in review. doi:10.3724/SP.J.1258.2011.00882.

Masten, Susan J., Simon H. Davies, and Shawn P. McElmurry. 2016. “Flint Water Crisis: What Happened and Why?” Journal - American Water Words Association 108 (12): 21–34.

Meerow, Sara, Joshua P. Newell, and Melissa Stults. 2016. “Defining Urban Resilience: A Review.” Landscape and Urban Planning 147. Elsevier B.V.: 38–49. doi:10.1016/j.landurbplan.2015.11.011.

Meyer, Michael D., and Brent Weigel. 2011. “Climate Change and Transportation Engineering: Preparing for a Sustainable Future.” Journal of Transportation Engineering 137 (6): 393–403. doi:10.1061/(ASCE)TE.

Meyer, Michael D, Michael Flood, Chris Dorney, Ken Leonard, Robert Hyman, and Joel Smith. 2011. “Climate Change and the Highway System: Impacts and Adaptation Approaches.” http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP20-83(05)_Task2-3SynthesisReport.pdf%5Cnpapers2://publication/uuid/0083F5C0-7F6B-489B-9CA6-09483C006F11%5Cnhttp://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP20-83(05)_Task2-3SynthesisReport.pdf%5Cnhttp://f.

Mochizuki, Junko, Adriana Keating, Wei Liu, Stefan Hochrainer-Stigler, and Reinhard Mechler. 2017. “An Overdue Alignment of Risk and Resilience? A Conceptual Contribution to Community Resilience.” Disasters. doi:10.1111/disa.12239.

National Academy of Science (NAS) Committee on Enhancing the Resilience of the Nation’s Electric Power Transmission and Distribution System. 2017. Enhancing the Resilience of the Nation’s Electricity System. doi:10.17226/24836.

National Academy of Sciences (NAS) Committee on Increasing National Resilience to Hazards and Disasters. 2012. Disaster Resilience: A National Imperative. The National Academies Press.

National Transportation Safety Board (NTSB). 2010. “Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River US Airways Flight 1549 Airbus A320-214, N106US.” Accident Report. doi:NTSB/AAR-10/03.

North American Electric Reliability Corporation (NERC). 2014. “Standard TPL-001-4 — Transmission System Planning Performance Requirements.” Accessed July 2017. http://www.nerc.com/files/tpl-001-4.pdf

Park, J, T P Seager, P S C Rao, M Convertino, and I Linkov. 2013. “Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems.” Risk Analysis 33 (3): 356–67. doi:10.1111/j.1539-6924.2012.01885.x.

Park, Jeryang, Thomas P Seager, and P Suresh C Rao. 2011. “Lessons in Risk- versus Resilience-Based Design and Management.” Integrated Environmental Assessment and Management 7 (3): 396–99. doi:10.1002/ieam.228.

Pasqualini, Donatella. 2017. “Resilient Grid Operational Strategies.” http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-17-21753.

Perrow, Charles. 1984. “Normal Accidents: Living With High-Risk Technologies.” Princeton University Press.

Pettersen, Kenneth A., and Paul R. Schulman. 2015. “Drift, Adaptation, Resilience and Reliability: Toward an Empirical Clarification.” Safety Science. Elsevier Ltd. doi:10.1016/j.ssci.2016.03.004.

Pizam, Abraham. 2017. “The Practice of Overbooking: Lessons Learned from United Airlines Flight 3411.” International Journal of Hospitality Management 64. Elsevier Ltd: 94–95. doi:10.1016/j.ijhm.2017.05.005.

Pulido, Laura. 2016. “Flint, Environmental Racism, and Racial Capitalism.” Capitalism Nature Socialism 27 (3). Taylor & Francis: 16. doi:10.1080/10455752.2016.1213013.

Resilience Alliance (RA). 2017. “Resilience.” Accessed July 2017. https://www.resalliance.org/resilience.

Righi, Angela Weber, Tarcisio Abreu Saurin, and Priscila Wachs. 2015. “A Systematic Literature Review of Resilience Engineering: Research Areas and a Research Agenda Proposal.” Reliability Engineering & System Safety 141. Elsevier: 142–52. doi:10.1016/j.ress.2015.03.007.

Roe, Emery, and Paul R. Schulman. 2012. “Toward a Comparative Framework for Measuring Resilience in Critical Infrastructure Systems.” Journal of Comparative Policy Analysis: Research and Practice 14 (2): 114–25. doi:10.1080/13876988.2012.664687.

Roege, Paul E., Zachary a. Collier, James Mancillas, John a. McDonagh, and Igor Linkov. 2014. “Metrics for Energy Resilience.” Energy Policy 72 (September). Elsevier: 249–56. doi:10.1016/j.enpol.2014.04.012.

Rose, Adam. 2017. “Defining Resilience Across Disciplines.” In Defining and Measuring Economic Resilience from a Societal, Environmental and Security Perspective. Integrated Disaster Risk Management., 19–27. Springer Singapore. doi:10.1007/978-981-10-1533-5_3.

Schulman, Paul, Emery Roe, Michel Van Eeten, and Mark De Bruijne. 2004. “High Reliability and the Management of Critical Infrastructures.” Journal of Contingencies and Crisis Management 12 (1): 14–28.

Seager, Thomas P. 2008. “The Sustainability Spectrum and the Sciences of Sustainability.” Business Strategy and the Environment 453 (September): 444–53. doi:10.1002/bse.

Seager, Thomas P., Susan Spierre-Clark, Daniel A. Eisenberg, John E. Thomas, Margaret M. Hinrichs, Ryan Kofron, Camilla Jensen, Lauren R. McBurnett, Marcus Snell, and David L. Alderson. 2017. “Resdesigning Resilient Infrastructure Research.” In Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, edited by Igor Linkov and Jose Palma-Olivera. Springer.

Shattuck, Lawrence G., and David D. Woods. 2000. “Communication of Intent in Military Command and Control Systems.” In The Human in Command: Exploring the Modern Military Experience, 279–92. Springer.

United Nations International Strategy for Disaster Reduction (UNISDR) and World Meteorological Organization (WMO). 2012. “Disaster Risk and Resilience.” http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/3_disaster_risk_resilience.pdf.

Walker, Brian, C S Holling, Stephen R Carpenter, and Ann Kinzig. 2004. “Resilience , Adaptability and Transformability in Social – Ecological Systems.” Ecology and Society 9 (2).

Wang, Yezhou, Student Member, Chen Chen, Jianhui Wang, Senior Member, and Ross Baldick. 2015. “Research on Resilience of Power Systems Under Natural Disasters — A Review” 31 (2): 1–10.

SMART Motorway Tunnel. 2017. “What Is SMART?” Accessed July 2017. http://smarttunnel.com.my/smart/what-is-smart/.

Woods, David D. 2006. “Incidents - Markers of Resilience or Brittleness?” Resilience Engineering : Concepts and Precepts, 69–75. http://www.loc.gov/catdir/toc/ecip0518/2005024896.html.

Woods, David D. 2015. “Four Concepts for Resilience and the Implications for the Future of Resilience Engineering.” Reliability Engineering and System Safety 141. Elsevier: 5–9. doi:10.1016/j.ress.2015.03.018.

Woods, David D., and Matthieu Branlat. 2011. “Basic Patterns in How Adaptive Systems Fail.” In Resilience Engineering in Practice: A Guidebook, 127–44. Ashgate.

Yeowon Kim, Daniel A. Eisenberg, Emily N. Bondank, Mikhail V. Chester, Giuseppe Mascaro, and B. Shane Underwood. 2017. “Fail-Safe and Safe-to-Fail Adaptation: Decision-Making for Urban Flooding under Climate Change.” Climatic Change *in review*.

Zahran, Sammy, Shawn P. McElmurry, and Richard C. Sadler. 2017. “Four Phases of the Flint Water Crisis: Evidence from Blood Lead Levels in Children.” Environmental Research 157 (February). Elsevier Inc.: 160–72. doi:10.1016/j.envres.2017.05.028.