Reliability Engineering and System Safety 175 (2018) 19–23

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Short communication

Resilience science, policy and investment for civil infrastructure

T.P. Bostick[a], E.B. Connelly[b,c], J.H. Lambert[b], I. Linkov[c,*]

[a] *53rd Chief of Engineers, US Army Corps of Engineers and George Washington University, Washington, DC, USA*
[b] *University of Virginia, Charlottesville, VA, USA*
[c] *Environmental Laboratory, US Army Engineer Research and Development Center, Vicksburg, MS, USA*

ARTICLE INFO

Keywords:
Resilience
Policy
Cost-effective
Recover
Investment
Infrastructure

ABSTRACT

The 2017 Atlantic hurricane season resulted in nearly US $200 billion in disruption across the Caribbean and several US states. Several seeming knockout blows to communities will challenge the wisdom and affordability of *resilience* paradigms that have shaped policy and investment for civil works since Hurricanes Katrina and Sandy. With extensive involvement of the public and lawmakers, mid-Atlantic US cities, New Orleans, and nearby coastal communities ultimately, and mostly successfully, opted to use pre-2005 civil works as the blueprint for future investment. Should options of returning to pre-event normalcy be considered for these latest devastated communities? What would gain and what will suffer? While there is continuing priority and commitment for infrastructure systems to be resilient, the theory, science and methodologies to do so will certainly be tested by recent events. Adoption of a resilience strategy by government agencies requires the wisdom of the emerging science of resilience as never before. We describe economic motivations for implementing resilience assessment and management in damaged communities and large scale complex systems. We describe the latest understood principles of resilience that drive a decision framework. We call for examination of risk-based policymaking and investment decisions by the science of resilience.

1. The challenges of risk assessment and management

Hurricane Katrina and Hurricane Sandy transformed US national priorities in the last decade. Hurricanes Harvey, Irma, and Maria will either continue the transformation or lead to yet-unimagined and unprecedented innovation and policy change. The environmental movement of the 1960s, the energy crises of the 1970s, dismantling of a global superpower in the 1980s–1990s, new global terrorism in the 2000s and 2010s, and the Great Recession of 2007–2009 are just a few to which national and global strategic plans have had to re-align. Each spurred a new social, economic, or environmental reality in the United States and required a paradigm shift to adequately adapt. Increasingly, there is recognition that climate change and other emerging hazards that threaten national civil infrastructure represent yet another shift in reality to which we must adapt. This shift if from risk-based management to resilience-based management. After Superstorm Sandy, President Obama directed leaders at every level to focus on climate change adaptation and resilience in our communities, and further defined resilience as “the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions” (Executive Order 13,653 [11]). Sandy called attention to the fact that we face a wide range of probable futures for which we cannot necessarily prepare, and yet from which we might need to be prepared to recover and adapt. The integration of resilience demands holistic treatment of systems, which is appropriate for the complexity of our modern systems. Research in the fields of risk analysis and decision theory currently aims to develop methodologies to assess resilience and ultimately facilitate much needed changes in long-held policies and practices [1], specifically cost-benefit analyses in which the main benefit is quantified risk reduction.

Infrastructure systems such as transportation networks, water resource systems, electricity grids, and others are critical for societal functioning and therefore their vulnerability to extreme events is of great consequence to human well-being. For this reason, risk assessment—a systematic approach to evaluating potential risks—and risk management—steps taken to eliminate, reduce, or mitigate risk—in these systems and networks have been formally or informally performed for centuries. Yet in the past several decades the planning and management of critical infrastructures in the United States, including regulation and funding priorities, have become increasingly reliant on quantitative risk assessment [18,20,25]. In this method, risk is calculated as *threat* scaled by *vulnerability* scaled by *consequence*, where threats, vulnerabilities and consequences are described probabilistically or classified on scales of relative severity. The risk management that follows generally

---

[*] Corresponding author at: US Army Engineer R&D Center, 696 Virginia Rd., Concord, MA 01742, USA.
E-mail address: igor.linkov@usace.army.mil (I. Linkov).

https://doi.org/10.1016/j.ress.2018.02.025
Received 14 January 2017; Received in revised form 5 February 2018; Accepted 6 February 2018

0951-8320/

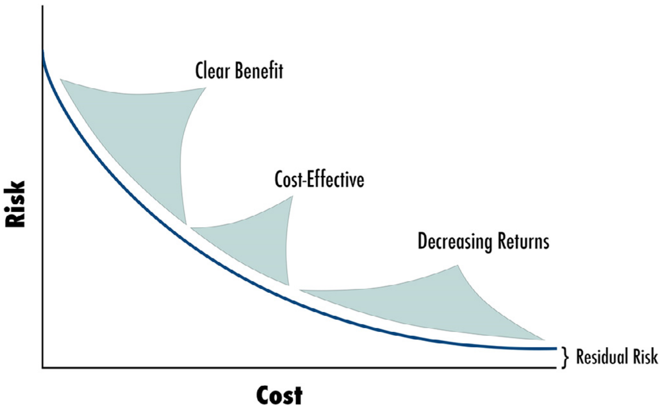

Fig. 1. Conceptual diagram of the cost of buying-down risk in major infrastructure systems. As the risk is reduced, the cost to achieve that reduction increases. At all points along the curve, some residual risk remains.

focuses on strengthening individual vulnerable system components against specific threats in order to reduce the risk score or classification.

Quantitative risk assessments are intelligible and effective for developing risk management practices when disruptions and infrastructure function are similar to those that have occurred in the past because the effects are well defined. Despite obvious successes, risk assessment and related risk management, as currently implemented, have a few major shortcomings [21]: (i) limited ability to account for emerging threat scenarios due to lack of past data on performance, (ii) focus on preventing failure of individual components through engineered solutions without consideration of the larger system due to the tendency to limit the scope to the quantifiable aspects of the system, and (iii) acceptance of a residual risk without preparation for their eventual occurrence.

Although there are several other approaches to risk analysis that focus more on the process and learning rather than obtaining a final score, traditional risk assessment is appealing for governance due to the quantitative nature and the single risk value that is output. These characteristics make risk thresholds easy to formalize in policy documents and to regulate in a consistent manner at the federal level [20]. However, quantitative risk assessment typically involves quantification of the likelihood of an event's occurrence and of the vulnerability to the event. Emerging realities and technologies including climate change, terrorism, and cyberattack, are presenting new threats with uncertain intensity and frequency and the vulnerabilities and consequences in terms of the extent of casualties, economic losses, time delays, or other damages are not yet fully understood or modeled. With greater uncertainty in the input parameters, more action has to be taken to mitigate risk before an acceptable level of risk has been reached with confidence. As risk assessment is expanded to incorporate modern processes, multiple, often hypothetical, threat scenarios could point to many vulnerabilities and catastrophic system failures that are enormously costly to mitigate or prevent. Furthermore, users, residents, and other stakeholders may have preferences for accepting some loss in performance of one part of the system over any degradation in another part [3]. One outcome can be significant funding spent in ways that do not align with stakeholder values, resulting in dissatisfaction with performance, despite the expense, or even litigation that interferes with the risk reduction efforts.

A key risk management strategy is to identify critical components of a system that are vulnerable to failure and subsequently, to fortify them. This approach can be appropriate for many isolated infrastructure systems, but when the nature of the threat is unknown, as discussed above, it is difficult to identify all of the critical components and it becomes increasing expensive to act conservatively to strengthen or protect all parts of the system against all types of threats [2]. Fig. 1 shows a risk reduction cost curve similar to those used by US federal agencies to communicate how cost-effective solutions should be targeted and that residual risk will nonetheless remain. For most infrastructure systems, the actions that provide a clear benefit and those that are cost-effective have already been implemented. Yet, aging infrastructure is shifting the curve to the right and emerging threats and are shifting the curve upward. From a risk management perspective, more action is needed to reduce risk to an acceptable level, yet further reducing risk through traditional risk management strategies will have minimal returns.

The result has been stagnation in investment. As risk mitigation plans become more expensive and are delayed while funding is sought, infrastructure and societal systems are left largely unprepared for emerging and uncertain threats [17]. Furthermore, there are fewer and fewer isolated systems in our world and the degree of interdependency and interconnectedness can be difficult to characterize and quantify. A risk management approach that focuses on individual system functions and components may fail to identify when damage to sub-critical components could initiate a cascade of impacts throughout the connected system. This is especially true of socio-economic systems. While federal agencies do collaborate for risk reduction and disaster recovery, funding decisions are almost exclusively determined within each separate agency with regard to their own mission and authority [8,23].

2. Resilience science

The National Academy of Science (NAS) 2012 definition of disaster resilience—"the ability to plan and prepare for, absorb, recover from, and more successfully adapt to disruptive events" [19] —is general but a useful guiding definition for a framework that can be applied across fields. It also points to a critical distinction between risk and resilience. Whereas the focus in the risk field is on the likelihood of experiencing loss (and therefore in managed through to prevent (prepare)_or mitigate (absorb) the loss), resilience adds equivalent focus on maintaining performance even as losses in some systems occur (and so is managed through enhancing recovery and adaptation) The US Army Corps of Engineers has recently adopted these four stages in resilient performance in the 2018 Implementation of Resilience Principles in the Engineering & Construction Community of Practice [24].

A combination of these stages (prepare, absorb, recover, adapt) and the essential parameters that are observed in the fields where the resilience of systems under stress is studied, are proposed as a way forward [6]. Together they provide the scaffolding for a useful heuristic for understanding how the functionality of a system changes as it experiences a disruptive event (Fig. 2). The essential parameters of resilience correspond to management decisions (critical function and threshold) and the contours of the system functionality curve (time and memory of the system) and can be understood in the context of the four stages. Identifying the *critical function* of a system helps answer the question "resilience of what, to what?" Specifying performance *thresholds* helps define the ability of a system to absorb a disruption and the tipping points at which cascading effect begin. *Time* defines a critical aspect of recovery and *memory* of past performance (both good and bad) through data collection or institutional knowledge is important for successful adaptation to future events.

Planning and preparing for adverse events takes place, presumably, during a time of normal system functioning. When an adverse event occurs, the performance of some components of the system are degraded, and beyond some threshold, system functionality declines precipitously. The ability to absorb describes the system's capacity to delay decline toward critical thresholds or immediately reconfigure so that when one part of the system fails, it does not cause a series of cascading failures in other system components. The shape of the recovery curve can take many forms, and vary in both steepness and smoothness. While many approaches to measuring resilience do so in terms of the area of this "recovery basin", the key metrics from many stakeholders' perspectives is the amount of time it takes for the full functionality of the system to return. Memory is particularly important for both infrequent events and slow recovery events. In the former, memory of past performance

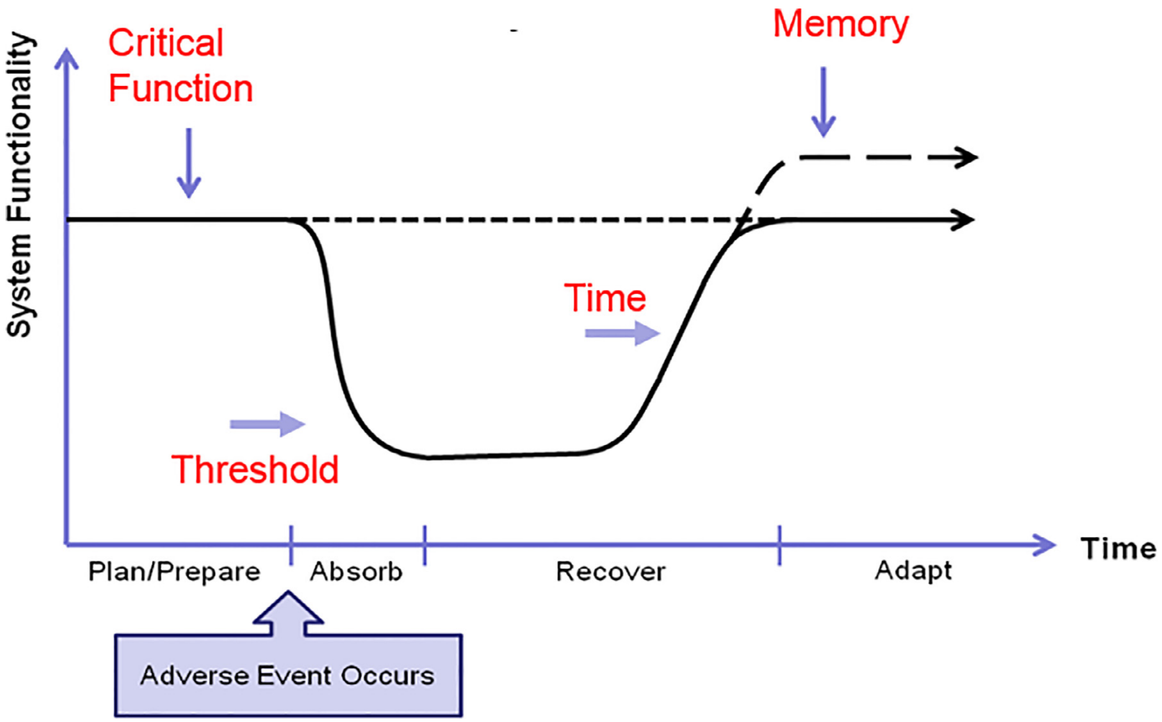

Fig. 2. The resilience curve, which conceptually describes the changes in functionality of a system, such as electrical service in communities affected by Hurricanes Irma and Maria.

is crucial to identifying appropriate adaptive methods, especially those that can be implemented at lower cost through operational and behavioral changes rather than infrastructure investment. In the latter, very long recovery processes lead to issue fatigue and resource depletion so that when the system is finally functional and stable again, there is little willpower to invest in additional adaptive measures. Nonetheless, discussion of adaptation and evolution of system priorities are important in order to jump-start the plan and prepare stage of the next cycle.

3. Resilience-based policymaking

Resilience-based policymaking addresses shifts in societal values, uncertainties, and time horizons. Instead of basing policies only on the risk of a hazard occurring, policies should consider the resilience of infrastructure and other systems to uncertain future disruptions, including both physical and social-behavioral events. Resilience specifically considers the flexibility of a system and its ability to adapt to or rebound from a disruption [16]. This adjustment to resilience-based policies is challenging for a generation that has internalized threshold-based risk management.

Adopting a resilience-based approach to system management requires acknowledgement that not all threats can be fully prevented or withstood and requires decision makers to consider what level and form of loss will have to be accepted and how the system should be changed– ideas that will be anathema to most stakeholders. On the other hand, community stakeholders may accept some loss, particularly if they cannot afford to pay for the risk-based solutions, but decision makers may not. Implementation of these policies will require some reallocation of funds from immediate concerns and needs to preparation for recovery from uncertain futures; again, actions that are difficult for officials working within budget cycles. Risk and resilience discussions are increasingly tied to discussions of data, privacy and security as resilience analysis, or even improved risk analysis, requires understanding the performance and vulnerabilities of privatized entities if a true system-level evaluation is to be achieved. As a result, few resilience assessment and improvement approaches have been demonstrated in practice, beyond hypothetical or simple case studies.

Not only is existing data hard to access, but some critical information is currently simply unknown. Large businesses generally have a business continuity plan prescribed for a set of events and electric utilities have an estimate of their downtime under given scenarios, but otherwise there has been little effort to assess and quantify recovery and adaptation processes. Yet it is during the long recovery phase when important decisions are made that establish the new risk behaviors of the future. It is also during this period when damage to communities, human health, and economies propagates from local and or short-term impacts to become regional and persistent impacts. Taking a resilience management strategy requires trade-offs to balance current spending on risk mitigation with needed spending on recovery and adaptive capacity. In exchange for accepting the current levels of risk rather than demanding greater preventative and protective measures, funding can be re-allocated towards resilience enhancement efforts. For systems that have already completed cost-effective risk reduction measures, Fig. 3 shows the funding that can be re-allocated toward resilience by accepting risk level (a) over risk level (b). In The academic community is called on to build risk-cost curves for real systems and to develop decision models that identify the optimal investment in risk reduction versus resilience and recovery improvement.

4. Direction for resilience science and practice

The science of resilience is evolving. Just as with risk analysis in the early 1970s and 1980s [1], even though significant academic investigation exists, the work to develop analytic methods for resilience that are appropriate for widespread governance is still needed as well as efforts to collect the data required to implement them. The International Risk Governance Council's, Resource Guide on Resilience (IRGC [13]) demonstrates that there is not a yet a comprehensive approach to resilience quantification. As such, actions by government agencies will likely lag until steps are taken to formalize resilience methods, similar to the process taken with risk analysis in the 1980s [20]. The

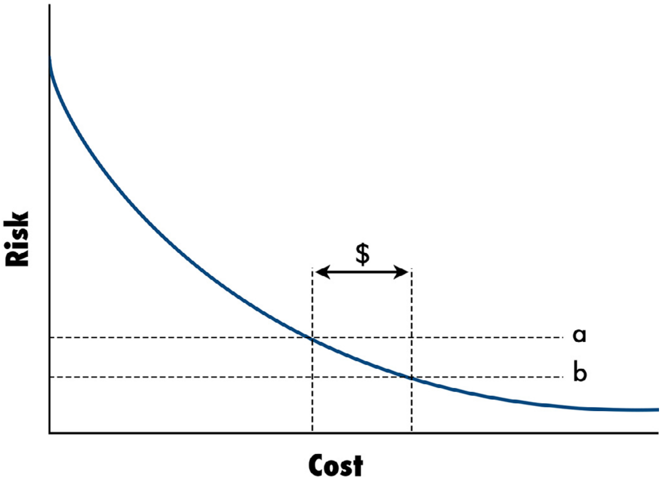

Fig. 3. Financial Resources can be realized and re-allocated to resilience management by accepting risk level (a) instead of risk level (b).

science of resilience must evolve towards embracing systems-level methods and tools for dealing with “unknown unknowns” in cost efficient ways that provide justification for investment in recovery- and adaptation-enhancing measures, not just prevention and mitigation measures. The field of risk analysis has already taken several important steps in this direction; however, the strong adherence of governance in the United States with probabilistic risk assessment requires a more definitive move beyond this method and into the realm of resilience.

Risk assessment in large-scale complex systems and associated infrastructure projects is methodologically focused on several specific functions of the system assessed by engineers and changing conditions often lead only to minor adjustments in the existing risk reduction plan. However, in large—and again, interconnected—systems, it becomes more likely that unavoidable disruptions will come to pass and that investment in recovery and rebuilding will be still be necessary. Resilience assessment builds upon the more qualitative methods of risk assessment to include consideration of the interaction between physical, information, and social systems, and more importantly, the form and speed of system recovery and adaptation after the initial emergency response but continuing until return to business as usual. Resilience assessment should offer an approach that acknowledges the uncertainty around emerging threats and guides mitigation of the consequences by enhancing the ability of a system to recover from any interruption, whether predictable or not. The best resilience assessment methods should engage stakeholders in determining acceptable tradeoffs in performance, prioritizing recovery efforts, and tracking any changing values of the community over the lifespan of the infrastructure and use in order to develop plans for adaptation away from the original design.

Tools for resilience do not necessarily need to be complex; some initial assessment needs can be met with simple scorecard or metric approaches, while others will need more advanced system configuration modeling and scenario analysis. Despite differing levels of mathematical complexity, the scientific challenges are in addressing system-level processes and tailoring methodologies to specific needs. A number of efforts have been focused on developing metrics that are applicable to a variety of systems, including social, ecological and technical [7]. Using these metrics, agencies will be able to offer a quantification of various resilience-enhancing investments to demonstrate improvements that are otherwise neglected in traditional cost-benefit accounting. In recent work [12], risked-based criteria have been used within multi-criteria decision analysis (MCDA), and, with the development of adequate resilience metrics, a similar method can be used to incorporate considerations of resilience. The current lack of universally applicable resilience metrics as well as inability to formalize value systems relevant to the problems at hand have been barriers to wide implementation of resilience-based methodologies. Advances in decision analysis and social and economic valuation of benefits offer ways to address these challenges, with methods to assess the impact of trading off resilience attributes (e.g., flexibility, redundancy) with values currently considered in the decision-making process (e.g., cost, environmental impact, risk reduction) for diverse investment alternatives. Further research on this topic can greatly benefit both management and investment decisions for system resilience.

While quantitative risk assessment has been used as mathematical framing of risk analysis, network science is emerging as an important tool to allow quantitative framing for the future of resilience as a scientific discipline. In network science, the system is represented as an interconnected network of links and nodes that exhibit behavior in space and time. These methods have been demonstrated; though only for limited case studies where network recovery was explicitly modeled [9,4,10]. The challenge is to frame resilience as arising of several major network properties that would provide a universal foundation to the field with cross-domain applications, similar to the threat-vulnerability-consequence framework used in the field of risk analysis. The four parameters of resilience (critical function, thresholds, time, and memory) will be the basis of identifying and describing the relevant network properties. This shift in thinking and assessment tools is needed to encourage adaptability and flexibility in addition to adequately assessing the tradeoffs between redundancy and efficiency that characterize a useful resilience assessment.

Resilience-based approaches, in common with risk-based approaches, require consideration of uncertain futures and shifting values of communities [14,15,22]. Scenario-based preferences analysis explores the impact of multiple possible paths of system evolution and decisions over the lifecycle of the investments. This method can be used to identify investments that enhance resilience to a variety of potential natural disasters, as well as explore how management decisions are affected by the evolution of preferences during the lifecycle of such investments [5]. Resilience policies and investments can be developed through scenario-based preferences analysis, helping decision-makers understand tradeoffs and priorities under a variety of uncertain futures.

5. Conclusions

Resilience-based policymaking offers a number of advantages over policy informed only by risk assessment. First, resilience acknowledges the evolution of circumstances in the recovery period. Second, resilience requires a holistic understanding of the system and supports identification of resilience management strategies across the whole system. For example, resilience assessment evaluates interdependencies among systems and human/societal values and the potential for cascading effects. The use of scenarios enables resilience analysis to address a variety of futures, appreciating the uncertainty and dynamics of physical and human/social factors and knowledge and understanding over several time horizons.

Management policies and decisions can benefit from resilience and risk analysis that accounts for physical and human/social factors over the system lifecycle, changing stakeholder preferences, and evolving political, economic, and technological conditions and states-of-knowledge. The simple mathematical framing used in currently available tools does not diminish its utility. Application requires integration of multiple domains (physical, information, and social) under different spatial and social scales, varying futures, and multiple stakeholders with competing priorities through the use of stakeholder values under uncertain future scenarios.

From the devastating Hurricane Season 2017, there is opportunity for science and policy transformation. It is critical that risk-based policies are considered in conjunction with the philosophy and science of resilience. The innovations of large-scale complex systems and infrastructure will attend future evolutions of community and societal preferences.

Acknowledgments

This effort was supported by the US Army Corps of Engineers Civil Programs. Additional support was provided by National Science Foundation grant 1541165 “CRISP Type 2: Collaborative Research: Resilience Analytics: A Data-Driven Approach for Enhanced Interdependent Network Resilience”.

References

[1] Aven T. Risk assessment and risk management: Review of recent advances on their foundation. Eur J Oper Res 2016;253(1):1–13.

[2] Alderson DL, Brown GG, Carlyle WM. Operational models of infrastructure resilience. Risk Anal 2015;35(4):562–86.

[3] Bostick TP, Holzer TH, Sarkani S. Enabling stakeholder involvement in coastal disaster resilience planning. Risk Anal 2017;37:1181–200. doi:10.1111/risa.12737.

[4] Cohen R, Erez K, Ben-Avraham D, Havlin S. Resilience of the internet to random breakdowns. Phys Rev Lett 2000;85(21):4626.

[5] Kott A, Linkov I, editors. Cyber Resilience of Systems and Networks. Amsterdam: Springer; 2018.

[6] Connelly EB, Allen CR, Hatfield K, Palma-Oliveira JM, Woods DD, Linkov I. Features of resilience. Environ Syst Decis 2017;37(1):46–50.

[7] Eisenberg DA, Park J, Bates ME, Fox-Lent C, Seager TP, Linkov I. Resilience metrics: lessons from military doctrines. Solutions 2014;5(5):76–87.

[8] Flynn SE. The South Carolina deluge: lessons from a watershed disaster: a center for resilience studies assessment. Northeastern University; 2016.

[9] Ganin AA, Massaro E, Gutfraind A, Steen N, Keisler JM, Kott A, Mangoubi R, Linkov I. Operational resilience: concepts, design and analysis. Nature Sci Rep 2016.

[10] Gao J, Barzel B, Barabási A-L. Universal resilience patterns in complex networks. Nature 2016;530(7590):307–12.

[11] Exec. Order No.13653. Preparing the United States for the impacts of climate change. 3 C.F.R. (1 November 2013).

[12] Hamilton MC, Lambert JH, Connelly EB, Barker K. Resilience analytics with disruption of preferences and lifecycle cost analysis for energy microgrids. Reliab Eng Syst Saf 2016;150(June):11–21.

[13] International Risk Governance Council (IRGC). Resource guide on resilience Available at https://www.irgc.org/irgc-resource-guide-on-resilience/.

[14] Linkov I, Bridges T, Creutzig F, Decker J, Fox-Lent C, Kröger W, Nyer R. Changing the resilience paradigm. Nature Climate Change 2014;4(6):407–9.

[15] Linkov I, Palma-Oliveira JM. An introduction to resilience for critical infrastructures. In: Resilience and risk. Dordrecht: Springer; 2017. p. 3–17.

[16] McDaniels T, Chang S, Cole D, Mikawoz J, Longstaff H. Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. Global Environ Change May 2008;18(2):310–18.

[17] Meyer, R.J. (2011) Why we under-prepare for hazards. In: On risk and disaster: lessons from hurricane katrina, R.J. Daniels, D. F. Kettl, & H. Kunreuther (Eds). Ronald J. Daniels, Donald F. Kettl, Howard Kunreuther. p 153.

[18] Moser D, Bridges T, Cone S, Haimes Y, Harper B, Shabman L, Yoe C. Transforming the corps into a risk managing organization http://corpsriskanalysisgateway.us/data/docs/White_Paper_Transforming_the_Corps_into_a_Risk_Managing_Organization_Moser_et_al_Nov2007.pdf.

[19] National Research Council. Disaster resilience: a national imperative. Washington, D.C.: The National Academies Press; 2012.

[20] National Research Council. Risk assessment in the federal government: managing the process. Washington, DC: The National Academies Press; 1983 https://doi.org/10.17226/366.

[21] Sikula NR, Mancillas JW, Linkov I, McDonagh J. Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments. Environ Syst Decis 2015;35:219. https://doi.org/10.1007/s10669-015-9552-7.

[22] Thorisson H, Lambert JH, Cardenas JJ, Linkov I. Resilience analytics for power grid capacity expansion in a developing region. Wiley J Risk Anal 2017;37(7):1268–86.

[23] Trump BD, Keisler JM, Lambert JH, Linkov I. Campaign to governance: science, engineering, and policy innovation for America’s top infrastructure projects. Environ Syst Decis 2017;37:42–5.

[24] US Army Corps of Engineers (USACE) Implementation of resilience principles in the engineering & construction community of practice. Eng Construct Bull 25 January 2018-2 2018.

[25] U.S. Department of Energy (DOE). Risk management guide https://www.directives.doe.gov/directives-documents/400-series/0413.3-EGuide-07a/@@download/file.