Infrastructure Resiliency: A Risk-Based Framework [1]

Why do we Need a Resiliency Framework?

We are living in a world of escalating risks. Globalization and spiraling infrastructure interdependencies have created complex and interlinked systems that generate many benefits but also significant risks. High-impact disruptions – whether caused by natural disasters, structural failures, or human-engineered terrorist events – are no longer rare and low-probability events (Kunreuther and Michel-Kerjan, 2008). Most notable among the factors contributing to these growing risks are:

- *Climate change impacts*. Manifested through rising sea-levels and water temperatures and changing precipitation, climate patterns of the past century have been changing slowly but their impacts have become more severe.
- *Accelerating growth in the scale of developments in coastal regions.* Some 80 percent of the population growth in the U.S. since 1950 has been within 100 miles of coastlines.
- *Exponential growth in the value of assets lost during catastrophic events, for both insured and uninsured assets.* Just a stretch of coastal development from the Texas Gulf Coast to New York City has an asset concentration with the value over $8 trillion.
- *Risks of global connectivity*. Our interlinked information, trade, financial, and transportation infrastructure systems are exposing us to new threats of terrorism, new vulnerabilities, and new risks that can cascade through our physical and cyber infrastructures.

The confluence of these factors – greater frequency of high-impact events spurred on by climate change and population growth coupled with the cascading effects of interconnected technology systems – has made us increasingly vulnerable to catastrophic disruptions. A resiliency approach to designing, building, and protecting our critical infrastructures and managing their risks is what is needed to address these risks at the systemic level. The concept of resiliency takes a risk-based and layered approach to addressing inter-linkages among today's complex infrastructures, and looks for solutions through a lifecycle approach to design, construction, and operation of our

[1] This summary was prepared for *Beyond Bouncing Back: A Roundtable on Critical Transportation Infrastructure Resilience* held at the Volpe Center on April 30, 2013. It is excerpted from a draft white paper on "A Risk-Based Infrastructure Resiliency Framework" currently in development by Dr. Bahar Barami, Senior Economist, RVT-51, the John A. Volpe National Transportation Systems Center, U.S. Department of Transportation, 55 Broadway, Cambridge, MA, 02142. She can be reached at 617-494-2150; bahar.barami@dot.gov.

complex infrastructure systems. Such an approach would enable us to harness these growing risks by crafting solutions that leverage today's technological complexities while minimizing their risks.

A Risk-Based Layered Defense is the Cornerstone of Resiliency

The cornerstone of a resilient critical infrastructure system is the conventional process for a systematic risk assessment coupled with the principles of a layered defense. A risk-analysis model estimates the risks of adverse events as the product of two parameters: the likelihood that the *threats/hazards* will materialize, and the severity of the *consequences.* The *threat* component is further quantified as the product of two probabilities: a) the *exposure* of the infrastructure subsystems to potential harm; and b) the embedded *vulnerabilities* of the infrastructure system, which together make it more likely for the threat to be realized (Haimes, 1998). A resiliency approach to infrastructure protection also shares the elements of the homeland security National Infrastructure Protection Plan (NIPP) and layered defense with foundations in:

- *Protective* measures supported by robust and fault-tolerant design and construction that reduce structural vulnerabilities and exposure to high-impact failures;
- *Prevention, detection, and attribution* capabilities supported by situational awareness, adaptive threat assessment, real-time decision-making capability, and safeguards of redundant assets for avoiding risks of single-point failures; and
- *Response and Recovery operations* supported by countermeasures designed to mitigate consequences of adverse events and rapidly restore normal operations.

Resiliency Framework

Resiliency is a *process* for managing complex infrastructures. Resiliency is <u>not</u> a single <u>outcome</u>. It is a cradle-to-grave process for engineering, building, and operating a fault-tolerant, safe, secure, smart, efficient, and sustainable transportation infrastructure system. Resiliency is a risk-based and lifecycle process for addressing the vulnerabilities of our critical infrastructure systems, making the system work smarter and better able to adapt to unexpected challenges. Resiliency is <u>not</u> just about a post-disaster capability for rapid recovery. Nor is resiliency only about protecting assets.

Resiliency is derived from the fundamental principles of layered defense and risk mitigation outlined above. As such, a resiliency framework takes an adaptive lifecycle approach to tackling the dynamic challenges confronting today's complex infrastructure systems because embedded in it is the capability to protect its assets, anticipate and detect threats, prevent risks of known failures, withstand unanticipated disruptions, and respond and recover rapidly when the worst

does happen:

A Resilient Infrastructure is Robust and Fault-Tolerant. It has design-based components that ensure adequate functional capacity and structural fault-tolerance and hardiness. The system is built with protective measures enabling it to resist severe blows, absorb shocks, withstand extreme events with tolerable levels of loss, and degrade gracefully when it must.

A Resilient Infrastructure is Adaptable, Aware, and Resourceful. It is capable of anticipating and preventing risks, limiting hazards, and ensuring continuity of operations through access to smart decision-making capabilities and situational awareness; it has agility and flexibility for taking alternative paths and making real-time decisions for "drift correction" to avert looming threats.

A Resilient Infrastructure has Functional Flexibility and Layers of Redundant Safeguards. Its flexibility enables it to reorganize rapidly, shift inputs and resources, and sustain some acceptable level of functionality as the disruption unfolds. Its redundant system components and spare safeguards provide operational flexibility and distributed functionalities that would enable system operators and users to substitute assets and modes to avoid single-point failures.

A Resilient Infrastructure has Response and Recovery Capability for Mitigation of Event Consequences. When all preventive and protective measures have failed, the system's response and recovery capabilities are essential for mitigating the consequences of system failures. Figure 1 depicts the elements of a Resiliency Framework along with the corresponding components in infrastructure management strategies and the layered defense strategy.

Figure 1 – Infrastructure Resiliency Framework

Graphic Source: The Volpe National Transportation Systems Center

Resiliency Performance Criteria

By approaching infrastructure asset management in accordance with a systematic process of engineering system resiliency, we are more likely to have a safe, efficient, survivable, and sustainable infrastructure system. The *outcome* of instituting a resiliency process is that the infrastructure systems that are engineered in accordance with these principles are likely to meet three high-level performance criteria*: efficiency*, *sustainability,* and *survivability:*

Efficiency. This criterion requires that an infrastructure system perform its functions in order to meet its specified functional requirements (*technical efficacy*) at lowest cost (*cost-effectiveness).* Metrics for efficiency include the costs of building and maintaining a complex infrastructure system within the constraints of its technical performance, reliability, and service-continuity.

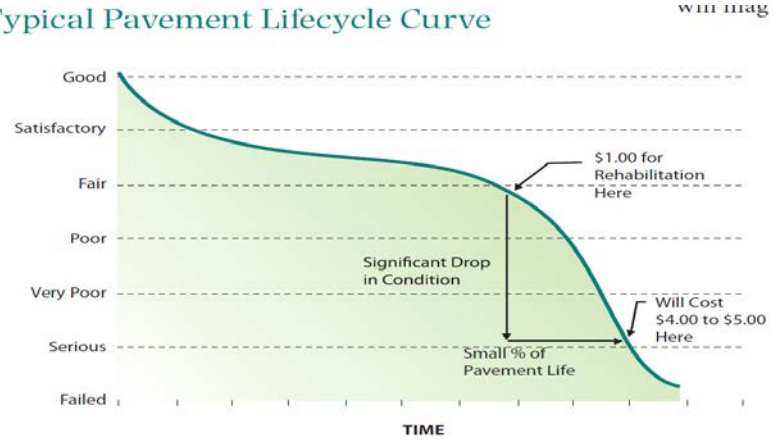
Sustainability. This performance criterion evaluates the extent to which the system uses resources – natural, human, and manufactured – in a sustainable manner. Sustainability is defined as a resource-use pattern that "meets today's needs while protecting resources for future use." To be sustainable, critical infrastructures must be designed and operated within the context of their impacts on the surrounding ecosystems, now and in the future. The metrics for assessing an infrastructure's sustainability include the extent to which transportation construction and operating inputs and resources are used in accordance with the long-term economic and environmental standards developed for the system.

Survivability. A third key performance criterion for resilient infrastructure is the ultimate test of safety, security, and survival of the people, infrastructure assets, and the ecosystem. In accordance with this criterion, an infrastructure meets the resiliency standards if it is capable of withstanding damages with minimal adverse impacts – lost lives, ecological impacts, structural damage – on the people, transportation operations, economy, and the environment.

Making a System Fault-Tolerant Improves its Performance by Making it Cost-Effective and Survivable

Structural fault-tolerance is enhanced through design components and preventive maintenance. This makes the lifecycle system operations more cost-effective. Research has shown that it is cheaper to perform routine maintenance on a critical infrastructure system than to repair damages. A study on the maintenance costs of the nation's aging highways showed that for every dollar asset-owners spent on routine maintenance of a decaying highway or bridge infrastructure, they saved $4 to $5 on comparable repair costs when deteriorated structures had actually failed (Figure 2; Brookings Institution, 2011).

Figure 2 – Lifecycle Cost Differences: Maintenance vs Repairs



Source: Brookings Institution, 2011.

In another study, researchers estimated that every $1 spent on pre-disaster preparedness is worth $15 in terms of future damages it mitigates. Yet, the researchers noted that because of "voter myopia" expenditures are more readily approved for post-disaster repairs, but not enough programs are funded for preventive damage-reduction improvements (Healy and Malhorta, 2009).

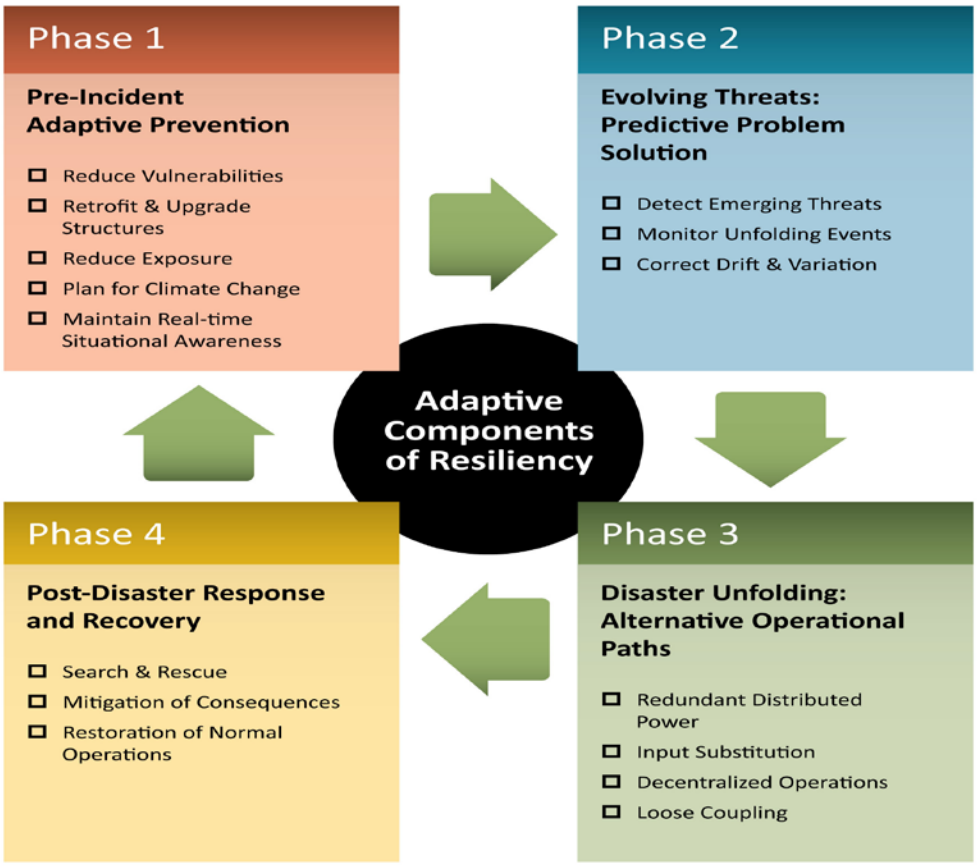
A cost-effective method for ensuring infrastructure integrity is deployment of adaptive structural monitoring devices as a mechanism for detecting, interdicting, neutralizing, avoiding, and redirecting the infrastructure system threats before the hazards reach a critical stage. For instance, METRANS Transportation Center of the California State University is conducting research on applications of fiber-optic "smart structures" for monitoring transport infrastructure components. One of the applications is the Structural Health Monitoring (SHM) system developed as a distributed deployment of passive fiber-optic devices that do not require a centralized power control capability (METRANS, 2010).

Safety and survivability are another outcome measure for fault-tolerant infrastructures. The fatalities in the aftermath of the August 1, 2007 collapse of the 8-lane I-35W bridge over the Mississippi River that led to the loss of 13 lives could have been avoided if the bridge had been built better and maintained adequately. The 40-year old steel truss bridge had been identified as a "fracture critical" structure, i.e., it was known that a failure at a single point would have resulted in the failure of the entire bridge. In 2005, inspectors had found cracks and fatigue in the structure that indicated the bridge was in "need of a major overhaul or replacement." Retrofitting the bridge with new plates had been postponed until 2020 since it was deemed too costly, though the retrofit costs would have been far less than the $250 million price tag for rebuilding it after it collapsed; not to mention the 13 lives lost (ASCE, 2009).

Adaptive Capability Improves a System's Performance by Making it more Efficient, Survivable, and Sustainable

Adaptation is a proactive component of the resiliency framework. Adaptive measures can prevent disasters by detecting threat signals, maintaining situational awareness, and improving infrastructure conditions. Adaptation is not just about "coping" behavior after a disaster. The concept applies to seeking smart solutions to the risks that confront any complex infrastructure system. At the core of the lifecycle process of adaptive defensives are capabilities for detecting looming threats, reducing vulnerabilities, maintaining real-time domain awareness, and interrupting negative feedback loops by reducing component tight-coupling. Figure 3 depicts lifecycle adaptive strategies for addressing pre-incident as well as post-incident threats, vulnerabilities, and consequences.

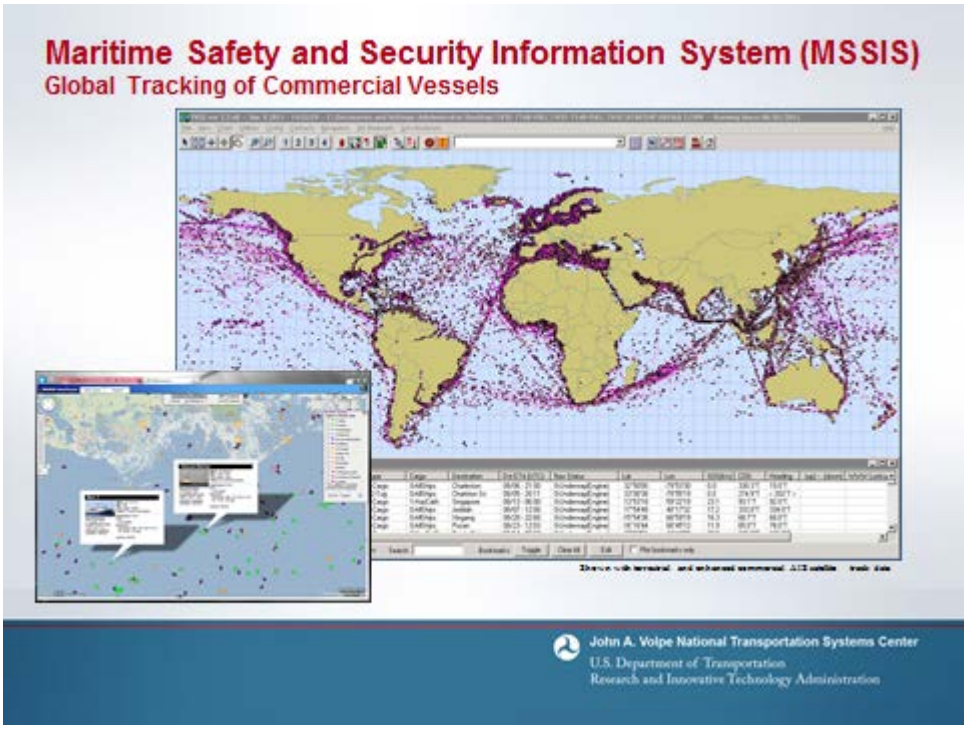
Figure 3 – Lifecycle Adaptive Components of a Resiliency Framework



Graphic Source: The Volpe National Transportation Systems Center

Maritime information display and communication systems for situational awareness are among industry best practices in deployment of adaptive technologies for real-time and automated monitoring and control of vessel movements in domestic and international waters. Vessel Traffic Service (VTS), Automatic Information System (AIS), and the use of AIS transceivers in the international Maritime Safety and Security Information System (MSSIS) are among legacy marine safety and security systems with proven performance records. Figure 4 shows the scope of the more than 70 maritime nations around the globe participating in the international MSSIS data sharing and vessel tracking program.

Figure 4 – Maritime Safety and Security Information System



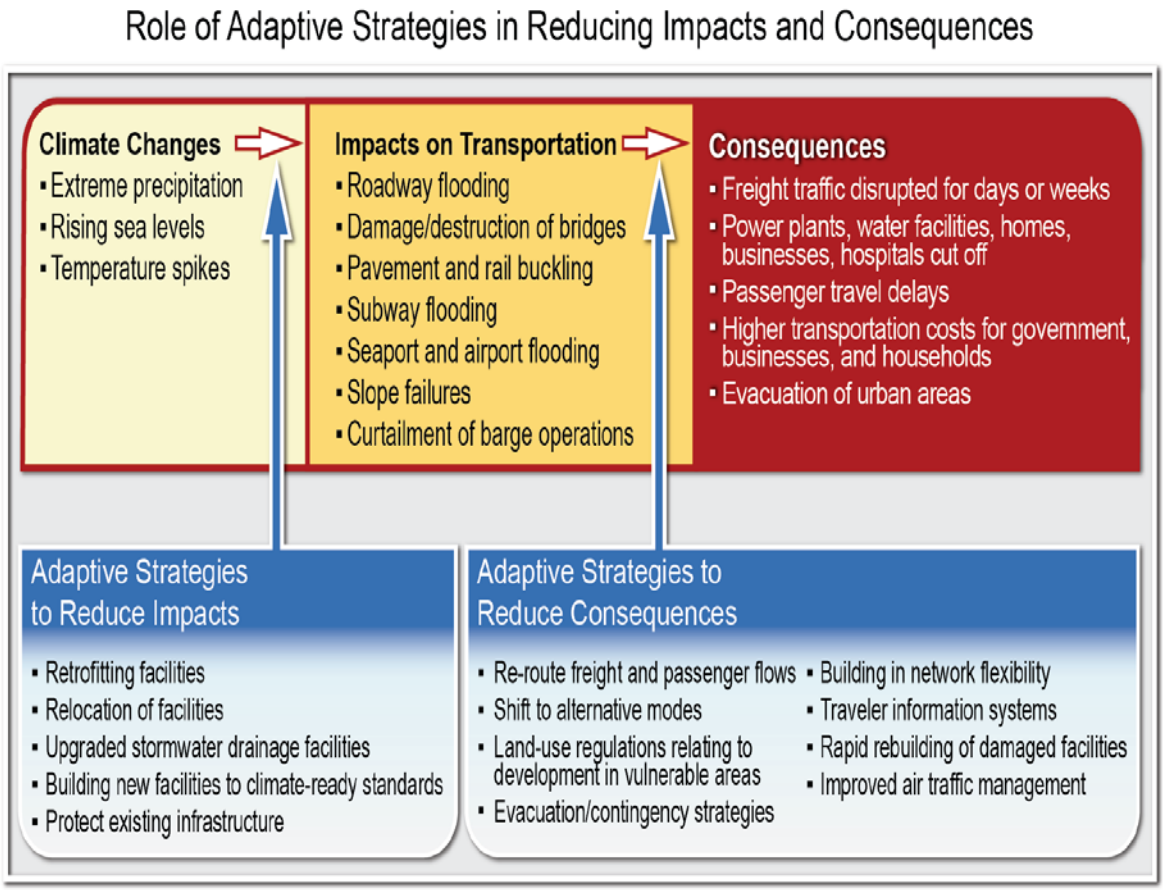
Source: The Volpe National Transportation Systems Center, 2013.

Other adaptive systems commonly deployed today are the United States Coast Guard's response and recovery system, *Search and Rescue Optimal Planning System (SAROPS*), and the National Oceanic and Atmospheric Administration's (NOAA) Search and Rescue Satellite Aided Tracking (SARSAT) system. SAROPS serves as an automated adaptive decision-support system that calculates precise location of mariners or vessels in distress, computes the probability of success for alternative approaches, and determines the most effective way to conduct search and rescue operations. NOAA's SARSAT is a search-and-rescue system supported by low-earth and geostationary-orbiting satellites that detect and locate aviators, mariners, and land-based users in distress. Another NOAA maritime information tool, the Physical Oceanographic Real-Time System (PORTS©), is a planning and decision-support tool that improves the safety and efficiency

of maritime commerce and coastal resource-management through the integration of real-time observed data and forecasts. PORTS© measures the observed and predicted water levels, currents, winds, atmospheric pressure, and visibility and disseminates them to mariners for navigation safety and voyage planning. Today, PORTS© data are readily available to nearly all marine vessels. In the aftermath of the 1989 grounding of the tanker Exxon Valdez in Prince William Sound, Alaska, the National Transportation Safety Board (NTSB) concluded that digitization of navigation charts was the single most effective initiative for improving navigation safety and risks of environmental disasters (NTSB, 1989). NOAA's PORTS© and many other navigation databases available in the past two decades have successfully met this strategic goal.

Climate change, with its gradual yet high-impact consequences, is among escalating risk factors that threaten our critical infrastructure systems. Adaptive strategies for reducing the impacts of climate change – e.g., retrofitting or relocating facilities, building new infrastructure systems to climate-ready standards, or shifting to alternative fuels to reduce the consequences of climate change – are proposed in a National Climate Assessment and Development Advisory Committee report (NCADAC, 2013), with some of the adaptive strategies depicted in Figure 5.

Figure 5 – Adaptive Climate Change Strategies



Source: National Climate Change Assessment, NCADA, January, 2013.

Redundant Capabilities Enhance the Performance of an Infrastructure by Making it Survivable and Cost-Effective in the Long Run

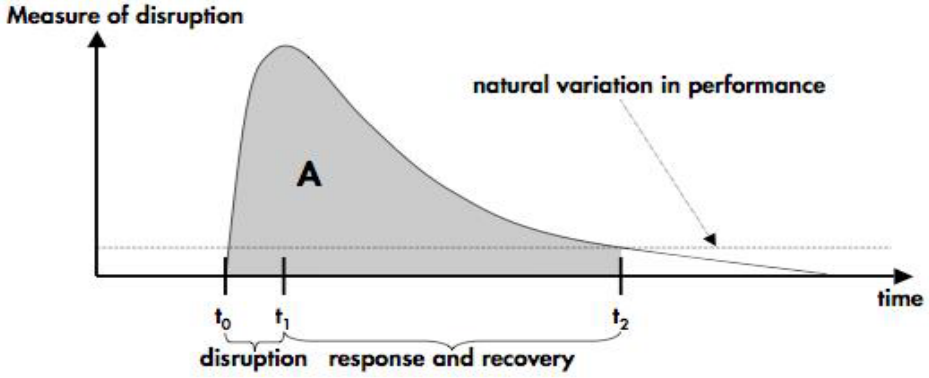
Reducing concentration of assets in large-scale centralized infrastructure systems – whether a power grid, oil refinery, or transportation network – is likely to make the system more resilient in the event of a disruption if it is coupled with availability of localized, distributed systems that serve as redundant facilities. This is because complex and centralized infrastructure systems have increasingly become tightly-coupled: a malfunction in one component is likely to cascade across the entire system. When redundant and loosely-coupled capabilities complement the operations of a larger infrastructure system, it is easier to control the propagation of the initial malfunction. The 2003 power-grid failure that led to the blackout that stretched throughout northeastern U.S and in Canada was caused by malfunction in a single Ohio utility. The failure to prevent the cascading effect was caused by lack of localized and distributed spare capacity with loose-coupling among subcomponents. Reducing centralization and tight-coupling among critical components of a complex infrastructure system is a key element of its resiliency (Perrow, 1999).

The mushrooming of impromptu marine and air terminals and transit services during recent hurricanes, when access to many centralized coastal transportation hubs was cut off, testifies to the need for, and potential benefits of, a flexible and distributed transportation infrastructure capacity. During major hurricanes, port operators have developed emergency harbor master control centers and modular ports that are deployed impromptu in inland locations to bypass the disrupted coastal port operations. When rail service was disrupted in the aftermath of Superstorm Sandy, impromptu ferry and bus services sprang up to fill the service gap and offer localized redundancy. One of the recommendations of the NYS 2100 Commission, convened on November 15, 2012, was to expand New York City's regional transit system by designing and constructing a Bus Rapid Transit (BRT) network along viable routes as a potentially cost-effective redundant system. Currently in operation in many major urban corridors, BRT has served as a high-performance transit system that combines the speed and reliability of rail-based transit with the flexibility and cost-effectiveness of buses capable of providing decentralized transit service. The flexibility of BRT as a transportation mode, described as a "train on rubber wheels," has made the system an effective and low-cost redundant transportation alternative for ensuring mobility during disruptions.

Capability to Mitigate the Consequences of a Disaster Improves System Survivability as well as Efficiency

Rapid response and recovery operations save lives, minimize the spread of hazards and their cascading effects, and reduce loss of valuable assets. These measures, along with the more commonly used metric, i.e., the speed with which normal operations are resumed, can be used to determine the post-disaster performance of a system. Measuring resiliency by comparing a system's performance baseline – traffic speed, network capacity, power availability, etc., – with a measure of its status after the disaster is done by estimating how wide the margin of variation around normal operations spreads after a disruption. When a disruption occurs, it pushes the system away from its performance baseline. Departure from natural variation in the event of a disturbance is depicted in Figure 6 as area A under the disruption curve, measured by the loss of system functionality during the time between t_0 and t_1 representing the duration of disruption. The size of the area A under the curve, i.e., the time it takes for the resumption of functions after the disruption has occurred, is a key measure of the performance of a resilient system. Area A shows how the disturbance raises the acceptable variation above the normal level marked by the dotted line labeled "natural variation in performance." A resilient infrastructure minimizes the area A by restoring normal network capacity and travel speed, limiting the magnitude of the effects of disruption – lives lost, property damaged, etc., – and shortening the period of recovery, making it meet the *survivability* criterion of resiliency as its key performance criterion.

Figure 6 – Resumption of Normal System Performance after a Disturbance



Source: Rand, 2009.

To sum up, in this paper we have developed a framework to identify the elements of infrastructure resiliency. We have defined resiliency as a cradle-to-grave process for designing, building, and operating critical infrastructure systems that are: a) robust and fault-tolerant; b)

smart, aware, resourceful and adaptive; capable of assessing risks, monitoring and detecting emerging threats, and making real-time decisions to correct for drift or reverse the course of unfolding events; c) have distributed capabilities and redundant resources that enable the system to adapt to loss of localized functionality and avoid single-point failures; and d) can respond and recover after a catastrophe to mitigate the consequences.

The transportation research and technology development community is well positioned to test and evaluate the extent to which the elements of such a process can foster a safer and more efficient and secure transportation system in accordance with the three proposed performance criteria – *efficiency*, *sustainability*, and *survivability.* Such a system would have the capability to harness the escalating risks of today's complex infrastructure systems through an adaptive process of learning, improving the system's performance, and reducing vulnerabilities and the consequences of disruptions.

References

American Society of Civil Engineers (ASCE), *Guiding Principles for the Nation's Critical Infrastructure*, 2009.

Brookings Institution, *Fix it First, Expand it Second, Reward it Third: A New Strategy for America's Highways*, Mathew E. Kahn and David M. Levinson, The Hamilton Project, February 2011.

Haimes, Yacov Y. *Risk Modeling, Assessment, and Management,* John Wiley, 1998.

Healy, Andrew and Neil Malhorta, "Myopic Voters and Natural Disaster Policy," *American Political Science Review*, Vol. 103, No. 3, August, 2009.

Kunreuther, Howard C. and Erwann O. Michel-Kerjan, *A Framework for Reducing Vulnerability to Natural Disasters: Ex Ante and Ex Post Considerations*, Wharton Risk Management and Decision Processes Center, Commissioned by the Joint World Band-UN Project on the Economics of Disaster Risk Reduction, Revised, November 16, 2008.

METRANS Transportation Center, *Fiber-Optic Smart Structures for Monitoring and Managing the Health of Transportation Infrastructures*, Final Report, METRANS Project 09-13, California State University, Department of Electrical Engineering, April 2010.

National Climate Assessment and Development Advisory Committee (NCADAC), *National Climate Change Assessment*, Draft Report, v. 11 January 2013.

National Transportation Safety Board (NTSB), "Proposed Findings of Fact, Conclusions and Recommendations Regarding Grounding of the Exxon Valdez," July 17, 1989.

Perrow, Charles, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, 1999.

Rand Corporation, *Adding Resilience to the Freight System in Statewide and Metropolitan Transportation Plans: Developing a Conceptual Approach*, David S. Ortiz, Liisa Ecola, and Henry H. Willis, Prepared for the American Association of State and Highway Transportation Officials (AASHTO), June 2009.