THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

DECEMBER 2013
VOLUME 12 NUMBER 6

RESILIENCE

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

In both December and January, *The CIP Report* will focus on **Resilience**. Presidential Policy Directive 21 defines resilience as "the ability to to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions." This month our authors provide practical tools for designing and measuring resilient systems, organizations, cities, and personal emergency plans.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, Duane Verner and Frederic Petit of Argonne National Laboratory's Infrastructure Assurance Center provide resilience assessment tools that incorporate both top-down and bottom-up approaches to address critical infrastructure system interdependence. Next, Ann Coss of Personal Recovery Concepts and Ronald Bearse of Nauset National Security Group highlight the importance of personal resilience. Dr. Steven D. Hart of the U.S. Army Engineer Research and Development Center follows with practical steps for developing resilient civil infrastructure. Then, Tracy Hatton, Erica Seville, and John Vargo of the Resilient Organisations research program in New Zealand discuss the defining factors of organizational resilience and provide two tools for its measurement. Finally, Michael Stevns of Siemens uses New York City's electrical grid to illustrate lessons in resilient urban planning.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Resilience Assessment Tools for Critical Infrastructure Systems

by Duane Verner and Frederic Petit
Infrastructure Assurance Center, Decision and Information Sciences Division,
Argonne National Laboratory*

Introduction

The United States faces significant challenges in preparing for, responding to, and recovering from disasters. Of particular concern are the impacts that natural hazards—including hurricanes, wildfires, floods, and droughts—have on the Nation's critical infrastructure systems. Enhancing the resilience of U.S. infrastructure has emerged as an urgent goal—a goal made more challenging by the complexity of these systems and their inherent dependencies/interdependencies. A combination of top-down and bottom-up approaches must be used to assess the resilience of these hyper-connected[1] systems. This paper addresses the benefits of combining top-down and bottom-up approaches to assess and improve the resilience of critical infrastructure systems, and—by extension—the resilience of the cities and regions these systems support.

Background

Assessing infrastructure resilience requires consideration of many interconnected socioeconomic, ecological, climatic, and technical elements. These interconnections mean that disruption or failure of one element can lead to cascading failures in others. The dependencies/interdependencies among infrastructure systems lead to a level of complexity that masks many systemic risks. As a result, an impact to a single node or link—the proverbial "single point of failure" that is often hidden deep within these interconnected systems—can result in catastrophic economic and physical damage on a city-wide, regional, or even national or international scale.

For example, storm surge from Superstorm Sandy led to the flooding of the Con Edison 14th Street Substation, resulting in nearly a week-long power outage in lower Manhattan. This outage cascaded to other infrastructure assets, such as communication systems that were rendered inoperable.[2] The vulnerabilities exposed during Sandy led many senior government officials, including Energy Secretary Ernest Moniz, to stress the need to learn from and act on the lessons from Sandy.[3] In some cases, post-event analyses of Sandy have led to wholesale re-evaluation of infrastructure planning, design, and management programs and have prompted some experts to call for new regulations to improve the resilience of critical infrastructure.[4] Sandy and other recent disasters have underscored the need for focused resilience assessment programs that utilize a combination of tools to improve overall understanding of critical infrastructure systems and lay the foundation for enhanced resilience.

Resilience Assessment Tools

To help meet the challenge of improving the resilience of critical infrastructure systems, the U.S. Department of Homeland Security (DHS) developed the Regional Resiliency Assessment Program (RRAP). The RRAP facilitates the collection and analysis of resilience data within a defined region or system. Participation in an RRAP

(Continued on Page 3)

[1] The World Economic Forum has used the term hyper-connectivity to describe the increasing risks associated with the coupling of complex infrastructure, financial, climatic, and ecological systems. Source: Helbing, D., 2013, "Globally Networked Risks and How to Respond," *Nature* (497): 51–59, May 2, http://www.nature.com/nature/journal/v497/n7447/full/nature12047.html, accessed Nov. 1, 2013.
[2] Marshall, A., 2013, "After Sandy: New Money, New Rules," *Planning: The Magazine of the American Planning Association*, Aug./Sept.
[3] Juliano, N., 2013, "Moniz Urges Study of Link between Grid Reliability, Fuel Availability," Governors' Wind Energy Coalition, July 17, http://www.governorswindenergycoalition.org/?p=6143, accessed Oct. 21, 2013.
[4] Smith, G., 2012, "Hurricane Sandy Delivers 'Another Catastrophe' to Verizon's Home, Complicating Network Repairs," *Huffington Post*, Nov. 3, http://www.huffingtonpost.com/2012/11/03/verizon-sandy_n_2069033.html, accessed Oct. 20, 2013.

(Continued from Page 2)

provides a dynamic and ongoing capability for Federal, State, and local partners to enhance critical infrastructure operational and planning-related capabilities.[5] Further, RRAP findings can inform Threat and Hazard Identification and Risk Assessments (THIRAs),[6] which provide the foundation for a systematic approach to improving critical infrastructure resilience.

Resilience assessment tools used in the RRAP are focused on understanding impacts of losing external dependencies (e.g., electric power, water, and telecommunications) and recovery times for critical infrastructure systems. This combination of tools allows analysts and planners to assess the resilience of critical infrastructure using both bottom-up and top-down approaches and to identify the systemic risks[7] inherent in these systems. Table 1 lists the general attributes of bottom-up and top-down approaches. A few of the tools used in the RRAP are described below.[8]

Table 1: Attributes of Bottom-Up and Top-Down Approaches to Critical Infrastructure Resilience Assessment

Bottom-Up Approaches	Top-Down Approaches
Decentralized	Centralized
Targeted data collection, typically at facility level	Broad data collection, typically at regional level
Based on actual operations and conditions	Often based on models and large data sets
Identification of facility-level dependencies and resilience characteristics	Identification of system-level dependencies/ interdependencies and cascading failures

EPFast

EPFast, an electric power simulation and impact analysis tool, explores the tendency of power systems to spiral into uncontrolled islanding and simulates the impacts of high-consequence events on large-scale power systems.[9] It is a top-down approach that provides a system-wide, quantitative estimate of impacts and graphical representations of the extent of blackouts and the spatial location of island grids (Figure 1). EPFast

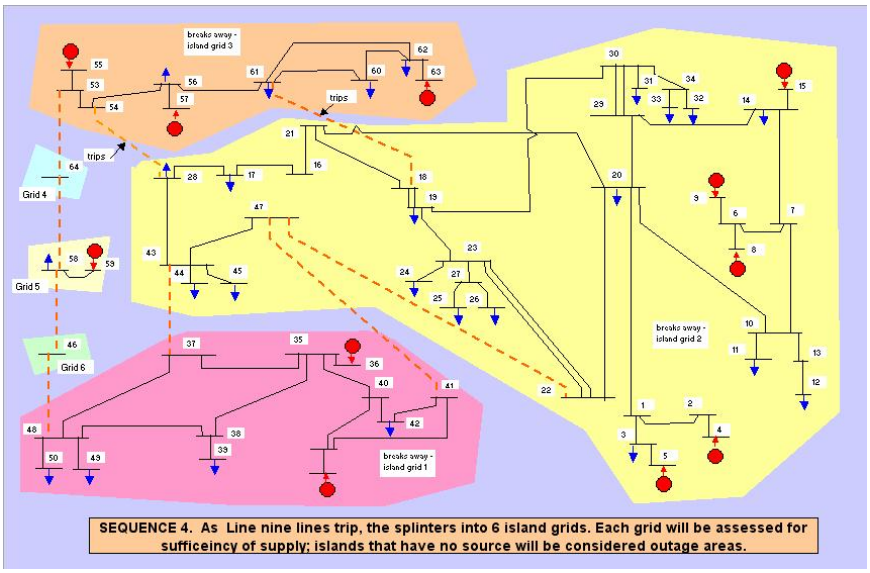


Figure 1: Sample Output from EPFast Showing Island Grids (islands that have no generation source are considered outage areas)[10]

(Continued on Page 4)

[5] DHS, undated, "Regional Resiliency Assesment Program," http://www.dhs.gov/regional-resiliency-assessment-program, accessed Oct. 20, 2013.

[6] Completion of a THIRA is a requirement for states and urban areas receiving FEMA preparedness grant funding. Source: FEMA, 2013, "FY 2013 HSGP Supplemental Resource: Regional Resiliency Assessment Program (RRAP)," last updated May 21, http://www.fema.gov/media-library/assets/documents/32607, accessed Nov. 1, 2013.

[7] The term "systemic risk" is described in Helbing (2013) as "the risk of having not just statistically independent failures, but interdependent, so-called 'cascading' failures in a network of *N* interconnected system components... In such cases, a localized initial failure ('perturbation') could have disastrous effects and cause, in principle, unbounded damage as *N* goes to infinity." Source: Helbing, D., 2013, "Globally Networked Risks and How to Respond," *Nature* (497): 51–59, May 2, http://www.nature.com/nature/journal/v497/n7447/full/nature12047.html, accessed Nov. 1, 2013.

[8] In addition to supporting the RRAP, the tools discussed below have been used by the U.S. Departments of Energy and Defense and the U.S. Environmental Protection Agency, among others, to help improve the resilience of the Nation's critical infrastructure.

[9] Portante, E.C., et al., 2011, *EPfast: A Model for Simulating Uncontrolled Islanding in Large Power Systems*, Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 2011 Winter Simulation Conference, AZ, Dec. 14, 2011.

[10] Ibid.

(Continued from Page 3)

is used in conjunction with facility-level dependency data to identify (1) layers of "built-in" risks within the critical infrastructure systems that support a sector or region of focus and (2) the cascading failures that can result from an impact to system operation.

Resilience Measurement Index

The Resilience Measurement Index (RMI), a bottom-up approach that captures the fundamental aspects of critical infrastructure resilience, considers all hazards and characterizes a facility in terms of its preparedness, mitigation measures, response capabilities, and recovery mechanisms. The value of the RMI ranges between 0 (low resilience) and 100 (high resilience). The RMI enhances the ability of facility owners and operators to manage investments by allowing comparisons among different options that can increase the resilience of their facility.[11] All the data and levels of information used for the calculation of the RMI are presented on an interactive, Web-based tool called the IST RMI Dashboard (Figure 2), which allows owners and operators to take the information that emerges from calculating the indices and use it for day-to-day operations, as well as investment justification and strategic planning.

Restore©

Restore is a stochastic model of the complex sets of steps required to restore a system following an incident that affects critical infrastructure. Restore© offers insights into outage restoration times at critical infrastructure facilities that can inform regional response and recovery activities. For example, loss of external dependencies can affect one or more steps required to restore a system. Considered within a regional context, Restore© can provide insights into dependencies/interdependencies among systems and identify the "most active path" through the network of tasks—which can ultimately lead to reduced recovery times.[13] Analysts rely on the first-hand experience of infrastructure operators for input to the Restore© model.[14] Thus, Restore© combines a top-down, system-level modeling approach with bottom-up inputs from infrastructure operators to develop insights into the restoration process and how to improve it. Figure 3 (p. 5) shows an example of the model output.

Conclusion

EPFast, the RMI, and Restore© are just a few examples of tools that can be used as part of a resiliency assessment program to improve our understanding of complex critical infrastructure systems. To prioritize

(Continued on Page 5)

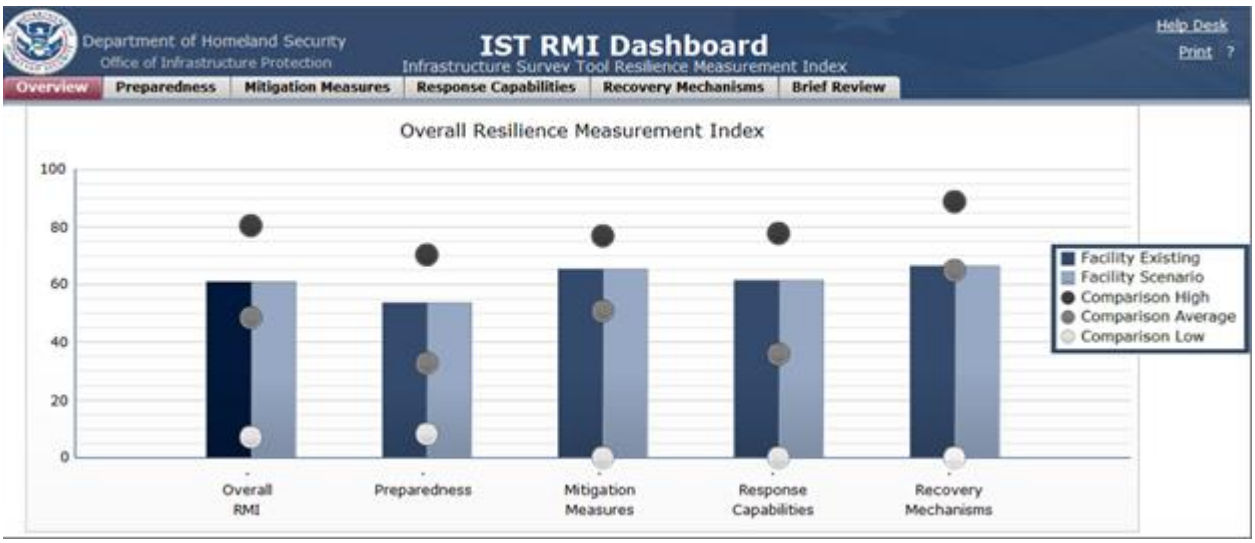


Figure 2: RMI Dashboard Overview Screen[12]

[11] Ibid.
[12] Ibid.
[13] Argonne National Laboratory, undated, *Restore: Modeling Interdependent Repair/Restoration Processes*, http://www.dis.anl.gov/pubs/67184.pdf, accessed Oct. 20, 2013.
[14] Ibid.

(Continued from Page 4)

mitigation and adaptation efforts and inform response and recovery decisions necessary to avoid catastrophic failures, government officials should consider implementing a combination of bottom-up and top-down approaches to resiliency assessment as standard practice within programs dedicated to critical infrastructure planning, coordination, and management.❖

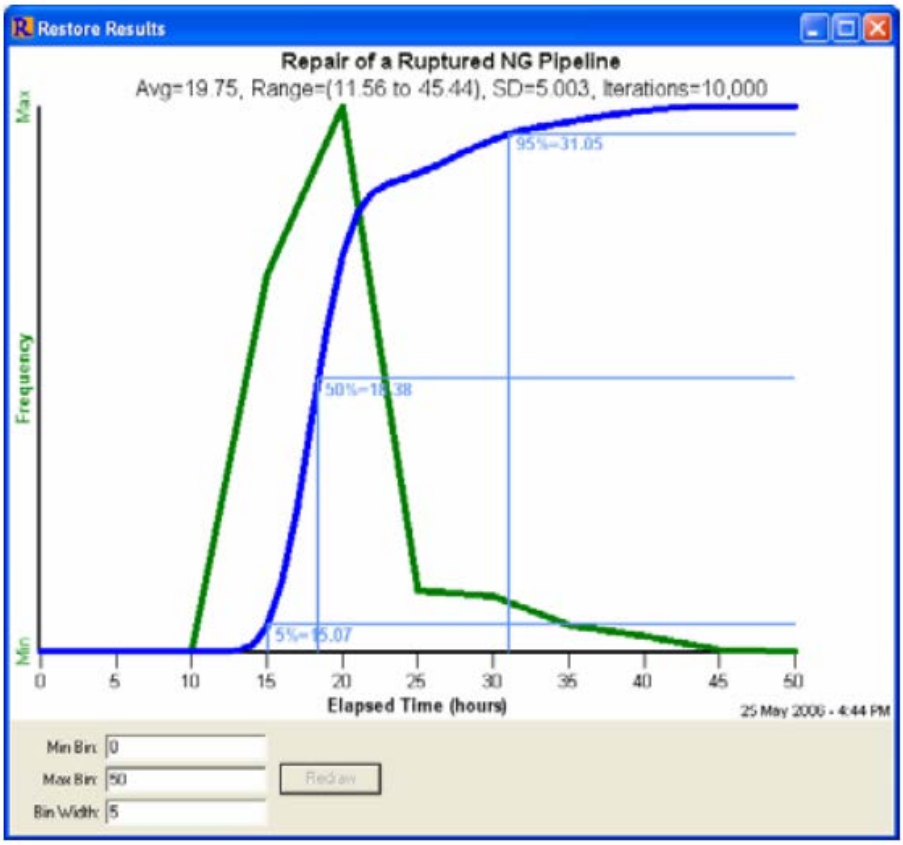


Figure 3: Sample Output from Restore© Showing a Completion Time Distribution and its Corresponding Cumulative Probability Function, Simulation Statistics, and Graph Input Areas.[15]

Acknowledgment

The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

[15] Ibid.

Strengthening Resilience of the Nation's Most Important Asset: People

by Ann Coss, Founder and CEO of Personal Recovery Concepts, LLC
and Ronald Bearse, CIP/HS Senior Fellow and President of Nauset National Security Group, LLC*

In proclaiming last month (November 2013) as "Critical Infrastructure Security and Resilience Month," President Obama stated: "This month, as we recognize that safeguarding our critical infrastructure is an economic and security imperative, let each of us do our part to build a more resilient Nation." We not only applaud the President for penning his proclamation and call to action, but actually resolved to act accordingly. So we decided to pen this article to bring attention to the importance of strengthening *personal* resilience as part of the continuing challenge to achieve and maintain a demonstrably effective national resilience posture.

The United States has spent hundreds of billions of dollars on strengthening homeland security and domestic disaster response and recovery capabilities since 9-11, yet millions of Americans are now being told to be prepared to be self-reliant for as long as a week, or even two, when disaster strikes.

Absolutely, and so they should be—personal resilience is a critical component of national resilience.

Question: Is enough being done to increase *personal resilience*—the ability and capacity of Americans to recover as quickly as possible from adverse events—to a crisis, emergency or disaster? Let's take a look.

Americans know hospitals can be overloaded in a major disaster; that the destruction of telecommunication and transportation infrastructure can prevent assistance from arriving for days; and that the restoration of disrupted electrical power, water, sewer, and natural gas pipeline infrastructure could take much longer. The aftermath of Hurricane Katrina and Super Storm Sandy are particularly instructive in this regard. Does this mean that individuals and families need to jump on the "doom boom" wagon? Certainly not, but these two events, as well as others in recent memory, do warrant prudent planning for "emergency certainty" and the need for understanding the practical, everyday benefits of having up-to-date personal and family emergency recovery plans.

Do you have a personal emergency or disaster plan? Does your family have an emergency plan? Do members of your organization's emergency response team and/or business continuity team have a personal or family emergency plan specific to their life, work, and geographic location? Has anyone told you that their personal or family preparedness plan helped reduce their stress during an unexpected life event and improve their recovery time?

These are important questions. Consider the following facts:

- Most Americans are not prepared for a disaster or an emergency.
- Less than 10% of Americans have documented or safely stored their personal, financial, emergency, household, medical, and legal information.
- Everyday workforce disruptions, absenteeism, and presenteeism are costing our nation hundreds of billions of dollars every year for a variety of reasons, including the lack of personal preparedness for events such as home fires, identity theft, eldercare, childcare, unexpected death, health problems, etc., and the stress that accompanies these events.
- A sizeable percentage of businesses with emergency preparedness and business continuity plans have not adequately accounted for human resiliency.

There is a link between personal and family preparedness and organizational readiness and resilience, and it is vital to building a national culture of resilience. Recent major catastrophic events in

(Continued on Page 7)

(Continued from Page 6)

the United States have underscored three critical weaknesses in American culture with regard to disaster preparedness:

1. A sense of complacency with our own safety;
2. A reliance by citizens on the help of authorities in life-threatening situations;
3. An unrealistic expectation that our first responders and critical business recovery teams will be available and focused to support rescue or recovery when they themselves (or their families) are victims of the same event.

A number of recent homeland security studies, policies, and executives have identified these cultural weaknesses, which have helped make investment in personal resilience a key priority in the nation's pursuit of demonstrable resilience.

The personal resilience gap of greatest concern is not in defining employer-specific roles and responsibilities an employee has in a disaster or emergency. It lies in the employees' own personal preparedness—a key factor in ensuring their self-reliance (or that of their family)—so the employees are available more quickly (with better focus) to the organization that relies on them to carry out their emergency roles and responsibilities when emergencies occur.

Creating a national culture of resilience has begun and will continue to require changing the way Americans perceive themselves in relation to a disaster, emergency, or crisis. Therefore, the extent to which you and others invest in helping individuals see themselves as capable, connected, adaptable, and self-sufficient, rather than dependent, victimized, or helpless, will affect their decisions, actions, and ability to cope in the face of disaster, emergency, or crisis. The collective return on the investment in personal resilience can be enormous for our country, particularly if everyone who can (and should) make this investment commits to doing so.

Enabling individuals and families to realize they must provide their own first line of defense against disasters and emergencies is both a moral imperative *and* a shared responsibility. This isn't a new fact—disasters and emergencies have been part of the human condition since day one. However, if the key to improving the nation's ability to absorb, recover from, and adapt to disasters, emergencies, and crises starts with the development of individual and family resilience plans, then why have so few individuals and families actually taken responsibility for developing them? Since it is a shared responsibility, why hasn't government and industry taken more responsibility to ensure that human resources resilience planning is taking place? Isn't the economic benefit alone self-evident? At the end of the day, who incurs the costs of unpreparedness?

Unfortunately there are many reasons why Americans do not have personal and family preparedness plans. The biggest drivers of the personal or human resources resiliency gap include: (1) shortage of personal time; (2) lack of opportunity; (3) lack of understanding, and (4) complete reliance on government authority and volunteers.

For example: Americans are over-scheduled. Dual income households and market dynamics drive companies to operate lean. This often results in added hours and responsibility to an already burdened workforce and causes most individuals to place emergency preparedness on the proverbial "to do list" for tomorrow, next week, or next year. Determining what an individual or family needs to do to be prepared for a disaster or emergency situation can be an overwhelming task for a person or household. Sitting down and preparing a plan from scratch requires an individual to compile information from over a dozen national agencies that relates to the individual's specific geographic location. For companies or government organizations to do this across their employee workforce, in a way that is specific at an individual level, requires resources and costs that make a solution untenable. This does not have to be the case. We and others have developed software that can help people and families prepare recovery plans for any unforeseen event. Other programs and tools are also available for free online and in the marketplace to help people and families prepare emergency plans. Yet the fact remains: far too many Americans have not prepared a personal or family emergency plan,

(Continued on Page 8)

(Continued from Page 7)

and this is our message.

What is truly unfortunate is that most Americans simply do not know what they will need to recover from an adverse event until after the event has actually occurred. They are unfamiliar with the wide array of agencies they can draw upon and they are not at all clear on what information is most needed to aid in their recovery from a disruption. Most government resources, such as Ready.gov, provide guidelines and checklists that focus primarily on survival after a disaster and what to do when disaster strikes. Yet higher frequency/lower impact events, such as home fires, and other more localized threats such as severe storms, cause significantly more deaths and destruction of property in any given year. Further, agencies offer one-size-fits-all guidelines even though preparing for these types of events and establishing a plan for recovery will vary by individual and geographic location. Moreover, an individual's attitude of reliance on public entities (be they local, state, or federal) or their place of employment to account for their personal well-being also leaves them unprepared.

This does not imply that the information available to individuals and families through government or other websites is not useful or valuable, for it clearly is. However, the reality is that seriously addressing the personal or human resources resiliency gap requires:

1. Providing understanding for why individual and family preparedness is needed and how to do it;
2. Providing the opportunity to do it;
3. Acknowledging self-reliance and its benefits;
4. Making it simple and attainable for the individual and organization they support;
5. Shortening the time it takes to achieve demonstrable resilience to disasters and emergencies; and
6. Providing for the security of an individual's personal data, yet ensuring the individual's access to it when needed.

As we stated at the outset, our nation has made heavy investments to strengthen homeland security and disaster response and recovery capabilities. While some people focus these investments exclusively on building capability and desired end states at the community, regional, and/or national level, we cannot afford, both literally and figuratively, to neglect the fact that personal resilience is the critical and basic foundation of national resilience. Therefore, citizens, businesses, and government organizations alike must increase their investment in personal and human resources resilience to bolster the efforts underway on many fronts to build resilient communities and regions.

The efforts that have been in progress since the attacks of September 11, 2001 to safeguard our nation against a wide variety of current and emerging threats are truly impressive, particularly those which have increased the security of critical infrastructure. We know that you are aware of the personal and societal consequences of the lack of preparedness, and encourage you to think about your own plans, as well as the emergency and continuity plans of the organizations you work for. Our nation urgently needs people like you to sound the trumpet and be a champion for personal resilience at home, at work, and in the communities we reside and serve.❖

* *Ann Coss is the Founder and CEO of Personal Recovery Concepts, LLC and a world-renowned leader in personal resilience planning for individuals, families, and public, private, and non-profit organizations.*

Ronald Bearse is a Senior Fellow at the George Mason University Center for Infrastructure Protection & Homeland Security and the President of Nauset National Security Group, LLC in Hyannis, MA (www.nnsgllc.com) and served in a variety of analytical, managerial, and leadership positions within the national security emergency preparedness community during his 20+ year career with the Departments of Defense, Homeland Security, and the Treasury.

Organisational Resilience

by Tracy Hatton, Erica Seville, and John Vargo
Resilient Organisations, New Zealand*

Since 2004, the Resilient Organisations research program in New Zealand has been researching what makes organisations able to survive a crisis and thrive in a world of uncertainty. In an increasingly volatile and uncertain world, one of the greatest assets an organisation can have is the agility to survive unexpected crises and to find opportunity to thrive in the face of potentially terminal events.

More resilient organisations lead to more resilient communities and provide the honed human capital to address some of our most intractable societal challenges. Organisational Resilience consists of three interdependent attributes; Leadership and Culture, Change Readiness, and Networks. These attributes build Business as Usual (BAU) effectiveness as well as robust and agile response and recovery from crises and disasters.

Organisational Resilience Indicators

Through extensive research, Resilient Organisations has identified thirteen indicators that can be used to assess an organisations' resilience:

- **Leadership:** Strong crisis leadership to provide good management and decision making during times of crisis, as well as continuous evaluation of strategies and work programs against organisational goals.
- **Staff Engagement:** The engagement and involvement of staff who understand the link between their own work, the organisation's resilience, and its long term success. Staff are empowered and use their skills to solve problems.
- **Situation Awareness:** Staff are encouraged to be vigilant about the organisation, its performance and potential problems. Staff are rewarded for sharing good and bad news about the organisation, including early warning signals, and these are quickly reported to organisational leaders.
- **Decision Making:** Staff have the appropriate authority to make decisions related to their work, and authority is clearly delegated to enable a crisis response. Highly skilled staff are involved or are able to make decisions where their specific knowledge adds significant value, or where their involvement

(Continued on Page 10)

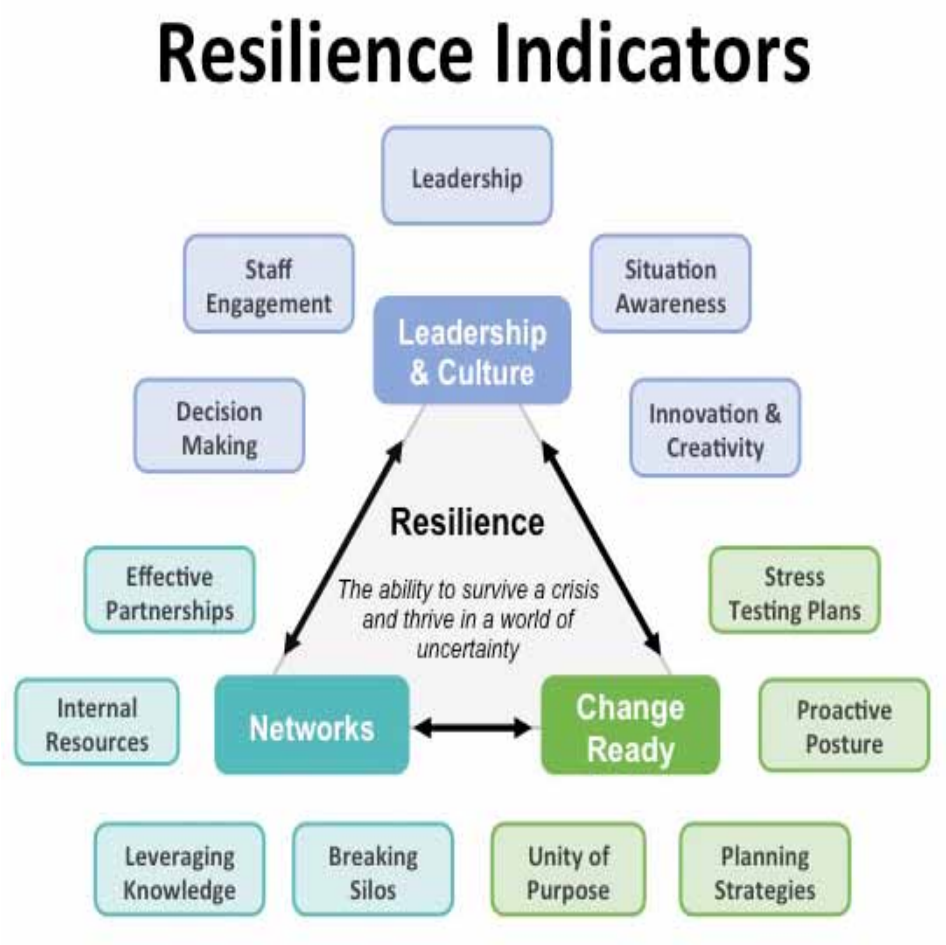


Figure 1: Model of Organisational Resilience Indicators

(Continued from Page 9)
will aid implementation.

- **Innovation and Creativity:** Staff are encouraged and rewarded for using their knowledge in novel ways to solve new and existing problems, and for utilising innovative and creative approaches to developing solutions.

- **Effective Partnerships:** An understanding of the relationships and resources the organisation might need to access from other organisations during a crisis, and planning and management to ensure this access.

- **Leveraging Knowledge:** Critical information is stored in a number of formats and locations and staff have access to expert opinions when needed. Roles are shared and staff are trained so that someone will always be able to fill key roles.

- **Breaking Silos:** Minimization of divisive social, cultural, and behavioural barriers, which are most often manifested as communication barriers creating disjointed, disconnected, and detrimental ways of working.

- **Internal Resources:** The management and mobilisation of the organisation's resources to ensure its ability to operate during BAU, as well as being able to provide the extra capacity required during a crisis.

- **Unity of Purpose:** An organisation-wide awareness of what the organisation's priorities would be following a crisis, clearly defined at the organisation level, as well as an understanding of the organisation's minimum operating requirements.

- **Proactive Posture:** A strategic and behavioural readiness to respond to early warning signals of change in the organisation's internal and external environment before they escalate into crisis.

- **Planning Strategies:** The development and evaluation of plans and strategies to manage vulnerabilities in relation to the business environment and its stakeholders.

- **Stress Testing Plans:** The participation of staff in simulations or scenarios designed to practice response arrangements and validate plans.

What Gets Measured—Gets Done

Resilient Organisations has developed two measurement tools which allow organisations to measure their current levels of resilience. These tools enable organisations to estimate how their organisation compares to others in terms of resilience, what the organisation's strengths as well as their weakest aspects of resilience are, and provide a suggested action plan for improving resilience.

Resilience Benchmark Tool

The Resilience Benchmark Tool is a self-report survey that can be administered online, over the phone, or as a paper-based survey. It can be used to support internal resilience development, as well as cross-sector or supply-chain resilience initiatives. It is intended to measure an organisation's resilience, allowing it to benchmark against other organisations in the same or related industries. Such benchmarking can support sector and supply-chain resilience initiatives as well as provide the organisation with a self-analysis of resilience strengths and weaknesses to support the Business Case for internal resilience initiatives. The survey is intended to be taken by as many individuals within an organisation as possible to provide a comprehensive view of the organisation by employee category and department comparison.

The survey is in two forms, one for all employees and a second form for completion by the CEO or other senior executive, which includes additional demographic and business performance measures on the organisation.

Outputs from the process can be tailored to each organisation's requirements and can include analysis by departments, by regions, or across organisations. Figure 2 (p. 11) illustrates one of the outputs from a recent report benchmarking the resilience of five Australian water companies identifying both their strengths and opportunities to improve their ability to adapt to future extreme climatic events.

Resilience Thumbprint

The second measurement tool is a greatly abbreviated version aimed at smaller businesses. This consists of an online or paper-based survey which takes only five minutes to complete and provides a simple evaluation of a resilience profile, suitable for smaller organisations in the early stages of exploring the

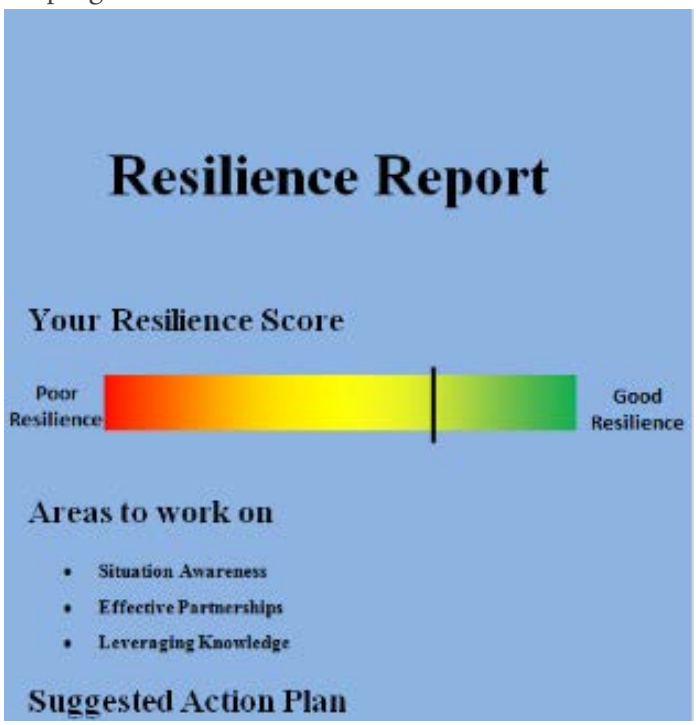
(Continued on Page 11)

Figure 2: Comparison of 3 resilience attributes for the 5 water utilities

(Continued from Page 10)
concept. Similarly to the benchmark tool, this measure can be tested repeatedly to gauge progress or in conjunction with the benchmark tool to provide a time series for larger organisations.

Both of these tools have been tested for reliability and validity and provide a much needed way to ensure that organisational resilience can be measured, actions taken, and measurable progress made.

We live in an increasingly complex world dealing with a broad spectrum of crises arising from both natural and man-made causes. Resilient organisations are those that are able to survive and thrive in this world of uncertainty. Resilience can bring about greater optimism, adaptability, and independence. It can lead to more innovative problem solving and faster recovery times, offering greater prospects for maintaining continuity of service in the face of extreme events.❖



** Resilient Organisations is a multi-disciplinary collaboration between top New Zealand universities and is funded by the Natural Hazards platform. Activities and outputs of the group include informing and focusing debate in areas such as Civil Defence Emergency Management, post-disaster recovery, and the resilience of critical infrastructure sectors, in addition to core activities in relation to organisation resilience capability-building and benchmarking. If you would like any further information about organisational resilience or are interested in using the measurement tools, please contact Erica Seville, Erica.seville@rsrc.co.nz, or John Vargo, john.vargo@canterbury.ac.nz.*

A Practical Guide to Designing Resilient Civil Infrastructure

by Steven D. Hart, Ph.D., P.E., U.S. Army Engineer Research and Development Center, Department of Civil and Mechanical Engineering, West Point

Imagine a conversation between the mayor and city manager in a moderately sized city with city-owned electric, water, and wastewater systems....

Mayor: "George, I've read a bunch of the reports on Hurricane Sandy and I really don't want those kinds of outcomes to happen here in our city. Everyone keeps talking about this resilience stuff. Can you tell me what resilience is?"

City Manager: "Well, Sally, the definition I like is from The Infrastructure Security Partnership (TISP) which is 'the capacity to absorb or mitigate the impact of hazard events while maintaining and restoring essential services.[1]' This is what our residents both care about and need—the services we deliver."

Mayor: "OK George, makes sense. Can you tell me how to make our city services resilient? Now remember, I have to take this answer to the city council, the Rotary Club, the press, the voters, and possibly the governor. I need a simple, correct, and effective answer in a language they can understand."

City Manager: "Sally, I'm glad I did my homework because I just read a paper on this in GMU's *The CIP Report* called "A Practical Guide to Designing Resilient Civil Infrastructures." It said . . ."

1. Define the all-hazards environment. The TISP definition of resilience refers to the "impact of hazard events," which means that the first step is to define the all-hazards environment. A wide range of stakeholders may be involved with this process. Design loads for snow, wind, and seismic events are typically specified by building codes but may be augmented by specific needs of a longer-than-normal service life or extremely high importance. Since terrorist threats are not currently addressed in building codes, alternate sources like the *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*[2] must be used. Deterioration, accidents, and life cycle performance are likewise not code-based and are determined through a stakeholder analysis. This step ends with a set of threats and hazards arrayed against the civil infrastructure being designed.

2. Network Modeling of the Infrastructure. Networks are models of actual systems that are used to understand system behavior. The network analysis helps to classify system elements into one of three classes: hubs, links, and customers. Hubs are nodes that are critical to the operation of the infrastructure like power plants, water treatment plants, and large transformer stations. They tend to be discreet locations, few in number, and expensive to build or replace. Links are the means of connection between hubs, less critical nodes, and customers that include items like electrical transmission and distribution lines, water mains, and rail lines. They tend to be long, numerous, and exposed. Customers are nodes in network terminology and are typically on the end of a distribution link. Thus a civil infrastructure system can be described as seen in Figure 1 (p. 13). This step ends with a network model of the infrastructure that is used to identify the type of network, characteristics of network behavior, and critical hubs.

(Continued on Page 13)

[1] The Infrastructure Security Partnership, "White Paper for the White House Office of Critical Infrastructure Protection and Resilience Policy and Strategy" (March 9, 2010).

[2] Federal Emergency Management Agency, *Reference Manual to Mitigate Potential Terrorist Attack Against Buildings* (FEMA 426) (Washington, D.C.: U.S. Department of Homeland Security 2003), http://www.fema.gov/media-library/assets/documents/2150.

(Continued from Page 12)

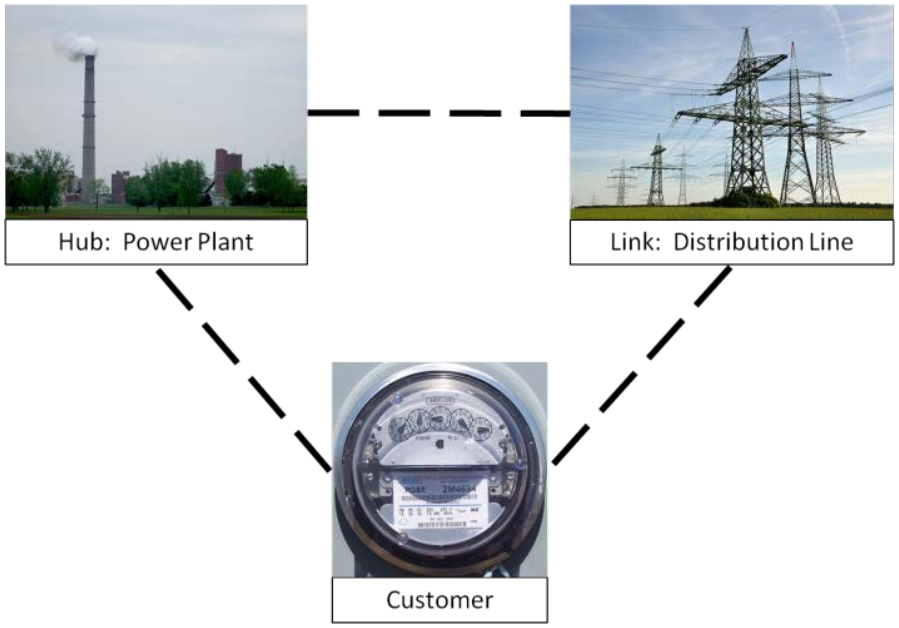


Figure 1: The Elements of a Civil Infrastructure Network[3]

3. Conceptual Design. A resilient system design must address each of these three items appropriately. First, defend the hubs. By their nature, hubs are essential to the overall functioning of the civil infrastructure system. They are typically expensive, major installations that cannot be quickly replaced. Their loss or damage causes the infrastructure network to fragment, cascade, or cease to function completely. The measures necessary to defend the hubs depend upon the threats and hazards defined in step 1 above. Based on the elements of the all-hazards environment, infrastructure owners decide the level of performance necessary in the event of each hazard and design accordingly.

Second, repair the links. Links are long, distributed elements whose size is measured in miles or thousands of miles. Because of this scale, they cannot effectively be defended against all threats and hazards. The solution is to put in place manpower, equipment, material, and procedures to repair the links as quickly as possible.

The purpose of defending the nodes and repairing the links is to restore service to the customer as soon as possible. However, the customer is an element in the infrastructure and has a major role in resilience—to survive the disruption. Customers must possess sufficient individual resources—generators, flashlights, food, water, friends, family—to allow them to survive for the time it takes to repair the links.

This concept is represented visually in Figure 2. In addition to Defending the Hubs, Repairing the Links, and supporting and encouraging customers to Survive the Disruption, infrastructure designers must ensure there is sufficient redundancy in the system so that it can absorb the loss of some components without failure. Single points of failure must be avoided. One element not

(Continued on Page 14)

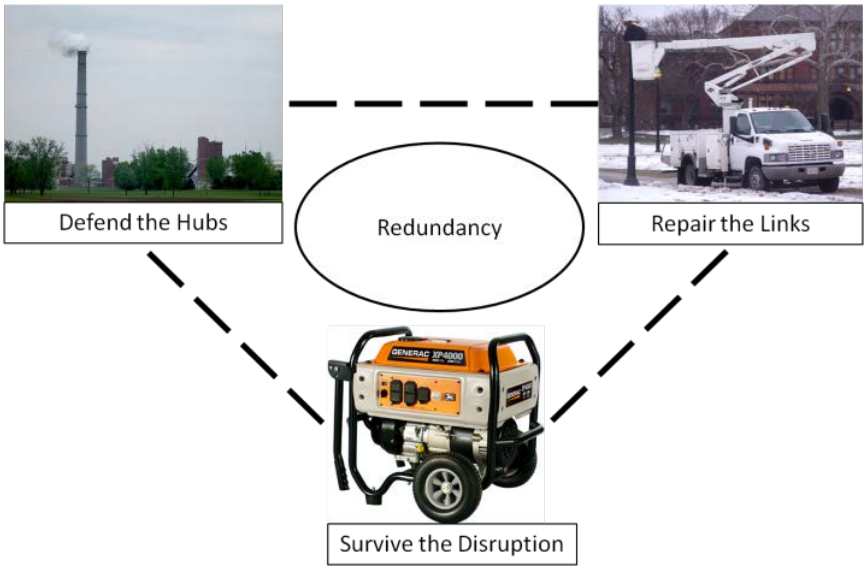


Figure 2: Conceptual Design of a Resilient Civil Infrastructure[4]

[3] Power plant by Matthew D. Wilson, Digital Image, available from Wikicommons, http://commons.wikimedia.org/wiki/Main_Page; Power line by Simon Koopmann, Digital Image, available from Wikicommons, http://commons.wikimedia.org/wiki/Main_Page; Watt hour meter by Kevin, Digital Image, available from Flickr Commons, http://www.flickr.com/photos.

[4] Power plant by Matthew D. Wilson, bucket truck in the public domain, and generator by katekrejci. All Digital Images, available from Wikicommons, http://commons.wikimedia.org/wiki/Main_Page.

(Continued from Page 13)

addressed in this construct is those nodes which are neither hubs nor customers. This could be a less critical electrical sub-station, one of six water towers, or a redundant pumping station. These nodes receive the same treatment as links—plans and procedures for rapid repair. This is an appropriate approach because the loss of these nodes has a limited effect on the entire system and they are often too numerous to be economically defended.

Infrastructure designers must also remember that a particular asset is often both hub and customer. For example, a drinking water treatment plant that is a hub in a water system is also a customer in the electrical system. As such, the plant must be defended against effects from natural disasters, terrorism, vandalism, deterioration, and accidents, as well as supplied with backup generation and fuel to survive disruptions in the electrical grid.

Conceptual design of a resilient civil infrastructure ends with accurate descriptions of how each element of the infrastructure will perform in the all-hazards environment. For example, a power plant may be required to maintain operations with less than 6 hours of down time in the face of a major earthquake, a 500 year flood, and a 100 pound car bomb. The same power company may put in place procedures and contingency contracts to restore electrical transmission and distribution lines within six days of the end of a major winter ice storm. Customers are then informed that they can expect to be without power for no more than six days and should develop individual response plans accordingly. In this way, the TISP definition of resiliency can be achieved.

4. Modeling, Simulation, and Evaluation. Step 3 may very well result in two or more different conceptual designs for achieving a desired level of civil infrastructure system resilience. For instance, a municipal water system, in replacing a 60 year old drinking water plant, may wonder if greater resiliency is provided by having two drinking water treatment plants, each capable of providing 75% of the city's water demand but designed to a minimal standard of robustness, or one drinking water plant that can meet all of the city's demand that is substantially more robust. Conceptual designs can be prepared for each and then modeling and simulation used to determine the responses of the two different concepts to the same set potential all-hazards disruptions determined in Step 1. These responses can then be compared using a decision matrix with one or more sets of the resiliency principles used as the evaluation criteria. This step ends with the selection of the most resilient conceptual design and owners and stakeholders understanding the likely performance of the infrastructure system under the stresses of the all-hazards environment.

5. Detailed System Design. In this step, individual components of an infrastructure system are designed and the system is assembled in accordance with the conceptual design. Many of the design procedures for this step are already well-established. Given the specified snow, wind, seismic, and flood loads from Step 1 and required performance from Step 3, engineers can apply well-known procedures and standards to ensure facilities perform as desired. Although not as widely known, the design procedures for blast resistant construction are also readily available. System redundancy is achieved by laying out system components in accordance with the conceptual design as validated through modeling, simulation, and evaluation. Procedures are established, contingency contracts signed, and material stockpiled for the rapid restoration of damaged links. Finally, customers are educated and informed on the expected system disruptions and encouraged, even incentivized, to take the measures necessary to survive the disruptions.

Mayor: "George, you make that sound so simple. I could explain that to anyone, but can we actually do it?"

City Manager: "Madame Mayor, that is your issue not mine. This is not a question of engineering—we can do the design and do the construction—it is a question of politics. Do we have the political will to forge a shared vision of a resilient future and to generate the revenue to fund it? If you can do that, then to quote Bob the Builder, 'Can we build it? Yes we can.'" ❖

Toolkit for a Resilient City: Infrastructure, Technology, and Urban Planning

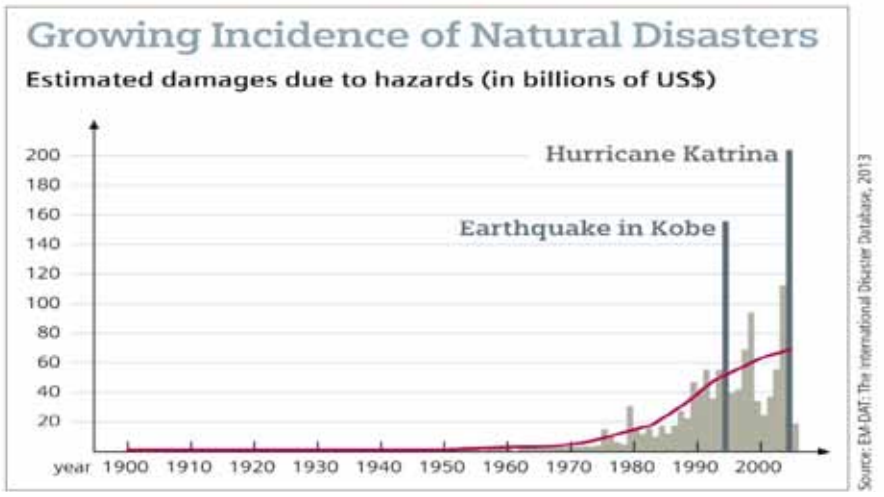
by Michael Stevns, Siemens Government Technologies, Inc.*

In a matter of hours, Superstorm Sandy turned New York City from a center of commerce connected to trade and industry throughout the world into a city struggling to meet its most basic needs: power, water, shelter, and transportation, to name a few.

Superstorm Sandy is estimated to have caused more than $19 billion[1] in overall damage to the greater New York area, but that is only one piece of the picture. The United Nations estimates that natural disasters between 2000 and 2012 have caused $1.7 trillion globally in damages[2] and the amount of disasters is growing.

Since 2012, Siemens, Arup, and the Regional Plan Association, an urban research and advocacy organization, have been exploring ways to enhance and ensure the resilience of critical urban infrastructure systems. Our goal is to prepare cities more effectively for major weather-related events, thus minimizing disruption of basic services and the cost of clean-up.

The result is a report, Toolkit for Resilient Cities, which is a resource for city stakeholders. There are active steps that can be taken to influence a city's resilience, whether through sector-based investments in infrastructure and technology, or cross-sector policy making and coordination. But cities must be careful and deliberate in their decision-making if they are to maximize the impact.



An assessment of how vulnerable the city is against the projected hazards should be the foundation for any resilience and adaptation action plans. The creation of resilient infrastructure systems may require large-scale changes to the way infrastructure is planned, designed, managed, and maintained. The technologies supporting resilient energy, transportation, water, and building systems share common attributes and are largely underpinned by advanced IT and communication services. The three main actionable areas are:

1. Increasing the robustness of new and existing infrastructure

Infrastructure networks, like energy, water, and transportation must incorporate components that will continue to function in an ever-changing environment. At the network level, utility managers may consider optimizing the location of new or redeveloped infrastructure to reduce exposure to hazards, including undergrounding or elevation of essential equipment.

(Continued on Page 16)

[1] "Mayor Bloomberg Outlines Ambitious Proposal to Protect City Against the Effects of Climate Change to Build a Stronger, More Resilient New York," Official Website of the City of New York, June 11, 2013, http://www1.nyc.gov/office-of-the-mayor/news/201-13/mayor-bloomberg-outlines-ambitious-proposal-protect-city-against-effects-climate-change.

[2] "Economic Losses from Disasters Set New Record in 2012," United Nations Office for Disaster Risk Reduction, accessed December 4, 2013, http://www.unisdr.org/archive/31685.

(Continued from Page 15)

2. Stimulating decentralized resource supplies and distribution networks

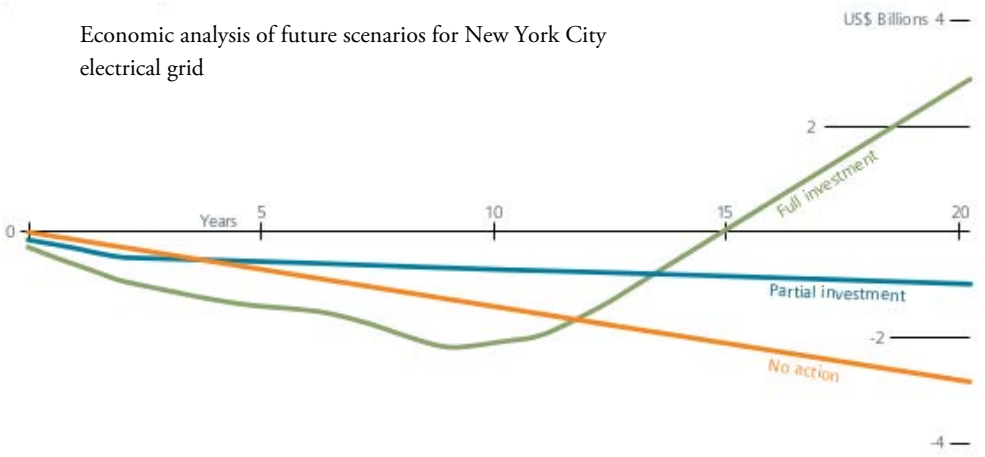
Energy, transportation, and water infrastructure can be designed to operate both as part of a large system and to serve a more localized community independently of the wider network.

3. Enhanced monitoring and controls

This includes system monitoring and control underpinned by increased application of IT networks and IT-enabled equipment (such as field devices and sensors), either embedded in new infrastructure or retrofitted into existing assets. Improved monitoring and control capabilities for infrastructure can enhance resilience by providing detailed and rapid information to utility managers and city leaders regarding operating conditions and performance.

Assessment Case Study: New York City's Electrical Grid

We identified some common technical characteristics in the architecture and components of resilient infrastructure systems across sectors which can provide a framework for assessing the resilience of infrastructure systems. In order to test our findings we undertook a high level review of the vulnerabilities of New York City's electrical grid. We investigated the impacts of four projected natural disasters on the generation, transmission, and distribution of electricity. We used this data to quantify the potential damages and economic losses from each climate-related event, as well as the actions and technologies that could ensure continuous electricity supply. Three scenarios emerged for the development of New York City's power grid over a 20 year period.



Economic analysis of future scenarios for New York City electrical grid

In the first scenario, the City pays to respond and repair the damage done by projected weather events over a 20-year period, with total costs amounting up to $3 billion. This is how repairs and upgrades are managed in the City today.

In the second scenario, flood and wind protection measures for critical assets are implemented within 3 years (on an accelerated schedule) with costs up to $400 million in order to increase the robustness of the system immediately. These measures reduce the cost of repair and response, and would reduce total costs to $2 billion compared to the first scenario. However, even after factoring money saved from infrastructure upgrades, the City still experiences a net loss of up to $1 billion.

The last scenario is a long term strategy that combines the protection measures to increase system robustness with a 12-year roadmap for introducing smart technologies to improve the management of the power grid. In the following years, city agencies and utilities spend approximately $3 billion implementing solutions that will not only reduce the impact of future events, but provide long term added benefits to the city, its residents, and its businesses. According to our projections, the financial value of these benefits— such as energy efficiency, capacity gains, and improved environments—could reach as high as $4 billion, leaving the City with a net gain.

In Closing

The idea behind our work was to provide policy makers with examples of how action plans can identify the most cost-effective measures for cities. Cities need solutions that provide a positive outcome in terms of avoiding damage as well as maximizing economic investment.

(Continued on Page 17)

(Continued from Page 16)

As with urban resilience metrics in general, a standardized methodology for this type of evaluation has not yet been established. While the scenarios will be unique for every city, we hope the Toolkit for Resilient Cities provides a place from which to begin.

Our next steps will be to have a closer look at how the cost and the benefits from the New York City business case accrue to the different parties, i.e. utilities, tax payers, electricity users, etc. Our hope is that this will enable us to be more specific on how to make the necessary investments happen.❖

** For further reading please visit www.siemens.com/urban-resilience.*

Critical Infrastructure Protection: Practical Solutions

Join us for a collaboration session with members from DHS, industry, and academia to solve three problems facing our nation's critical infrastructure. Using the Innovative Solutions Consortium's VIVID Framework (Virtually-Innovate-Vet-Incubate-Deliver), we will be exploring practical solutions for:

- **Continuously monitoring security and the resiliency of critical infrastructure elements**
- **Anticipating threats connected to actions and responses**
- **Sharing threat information in real-time with trusted organizations**

George Mason University, Arlington Campus
Tuesday, January 21, 2014
1:30 p.m. - 2:00 p.m. Registration
2:00 p.m. - 5:30 p.m. Program
5:30 p.m. - 7:00 p.m. Networking Reception

Cost: ISC Members - $20, Non-members - $45

Space is Limited - Register Today!

INNOVATIVE SOLUTIONS CONSORTIUM

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click here:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1