THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

DECEMBER 2014

VOLUME 14 NUMBER 5

Investments and Assessments in Critical Infrastructure

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

This month's *The CIP Report* focuses on **Assessments and Investments in Critical Infrastructure**.

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

First, Scott Edelman, Director of the AECOM Water Resources, discusses the impact of climate-related events on design standards. Next, Dr. Dane Egli and Jared McKinney of Johns Hopkins University Applied Physics Laboratory write about the economics of resilience in the globalized critical infrastructure environment. An article written by Frédéric Petit, Rosalie Laramore, and David Dickinson of Argonne National Laboratory, highlights a campus-wide resilience assessment approach centered on business continuity principles. Then, Drs. Luca Galbusera, Georgios Giannopoulos, and David Ward of the European Commission's Joint Research Centre present a paper on their efforts to introduce stress testing into various European critical infrastructure sectors. In a second article authored by colleagues of Argonne National Laboratory, critical infrastructure dependencies and interdependencies assessments are discussed. Finally, David Vaughn and Jeff Plumblee, of Fluor, have written about managing risk through critical infrastructure investment.

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.

Happy Holidays!

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

Climate Implications and Design Standards

by Scott Edelman*

Introduction

In the aftermath of Superstorm Sandy, our government agencies, communities, and citizens are focusing on how to make our cities and communities more resilient. Before rebuilding flood-damaged communities, the engineering community and our public officials owe it to residents to inform them about how to rebuild safely. One of the lessons learned from Sandy is that many people do not realize the risk they face by living near the coasts, or even in inland areas that also experienced extensive flooding. We need to better inform communities and residents about their risk of flooding, so they can make decisions accordingly.

Ranges vs. Averages

Riverine and coastal hydrologic and hydraulic analyses and numerical flood modeling are fundamentally based upon statistics. These statistical results are often reported as the average storms at a certain recurrence interval.

Figure 1. The aftermath of Superstorm Sandy, at the corner of 18th and Surf Avenues in Belmar, NJ, shows extensive flooding and debris (remnants of the boardwalk). This area is outside of the FEMA floodplain, but was underwater after Sandy

For example, the United States Geological Survey's (USGS) definition of the 1-percent-annual-chance-flood, upon which the Federal Emergency Management Agency (FEMA) bases its Flood Insurance Rate Maps (FIRM), is based on averages: "[b]ecause the 1-percent [annual exceedance probability] AEP flood has a 1 in 100 chance of being equaled or exceeded in any 1 year, and it has an average recurrence interval of 100 years, it often is referred to as the '100 year flood.'"[1] However, the past 100 years proves that averages are not the norm, and "average" flooding can be exceeded many times, sometimes even within a single hurricane season.

The use of the 1-percent-annual-chance flood as the average design flood (with regard to building codes) has led to structures that are designed to withstand an average 1 percent or perhaps 0.2 percent storm. However, the reality is that 50 percent of the time, floods (and the associated damage) will be worse than the average design flood. Buildings and structures that were designed to protect against a particular event can still suffer catastrophic damage when a stronger event occurs, as we saw in countless places after Sandy (see Figure 1).

Defining flood risk based on an

(Continued on Page 3)

[1] U.S. Geological Survey, *100-Year Flood—It's All About Chance: Haven't We Already Had One This Century?* (Washington, D.C.: Department of the Interior, April 2010), available at http://pubs.usgs.gov/gip/106/pdf/100-year-flood_041210web.pdf.

(Continued from Page 2)

average storm confuses the public and policy makers (as well as many architects, engineers, and planners) about how to understand, communicate, and mitigate the actual flood risk.

Design Standards vs. Insurance Standards

The public trusts engineers to keep them safe in many ways, and when engineers provide information about our safety or risk, the public tends to rely on them. For example, if a driver sees a sign on a bridge that states the safe rating of the bridge is 20 tons, the driver expects to be able to drive a 20-ton truck over the bridge once, twice, or a thousand times without the bridge failing. As engineers, we have conditioned the public to trust without exception the safety limits we set, whether it is the number of people that should be on an elevator, or the maximum safe speed limit to exit an interstate.

However, when it comes to flooding, it is more difficult to draw a line between what is safe and what is not. Flood elevations and floodplain boundaries on a FIRM are not based on absolute values, nor do they include an associated factor of safety. Instead, these numbers are the statistical means or averages used by the insurance companies to generate rate tables for various conditions. While the insurance industry needs the statistical averages, these averages are not where we should base design criteria.

From a statistical perspective, the 1-percent flood has a 1-percent chance of occurring in any given

year. To better put this into perspective, based on probability theory, during the 30 years of a typical 30-year mortgage, any property with a 1-percent-annual chance of flooding actually has a 26 percent chance of being flooded during the term of the mortgage, by the average flood. Imagine the bank telling you, during refinancing, that you should expect major flooding at least a quarter of the time that you are paying the mortgage on a property you are purchasing. The public would not accept a bridge that had a 26 percent chance of failure at any given time for 20 ton trucks passing over it during a 30-year lifespan of the bridge, so why should we accept that risk for our homes and businesses?

For the most part, calculations of flood risk for planning and design include little to no factor of safety. Factors of safety are applied in almost every other engineering field to take into account uncertainty of the science and to protect the safety of the public. Many people believe that if they build to an elevation that is reported on the FEMA FIRM or outside a FEMA-delineated floodplain, they will be safe from flooding. This simply is not the case.

Figures 2 and 3 are graphs of flood elevations' statistical "average" along with 5 percent and 95 percent confidence limits. As shown, the uncertainty of the numbers is large. For example, for the riverine flooding in the Ramapo River near Pompton Lakes, NJ, the 1-percent annual-chance elevation could be 3.8 feet higher or 2.4 feet lower than the average shown. For the coastal flooding at the National Oceanic and Atmospheric Administration's (NOAA) Battery, NY Tidal Station, the elevation could be 1.6 feet higher or 2.3 feet lower than

(Continued on Page 4)

(Continued from Page 3)

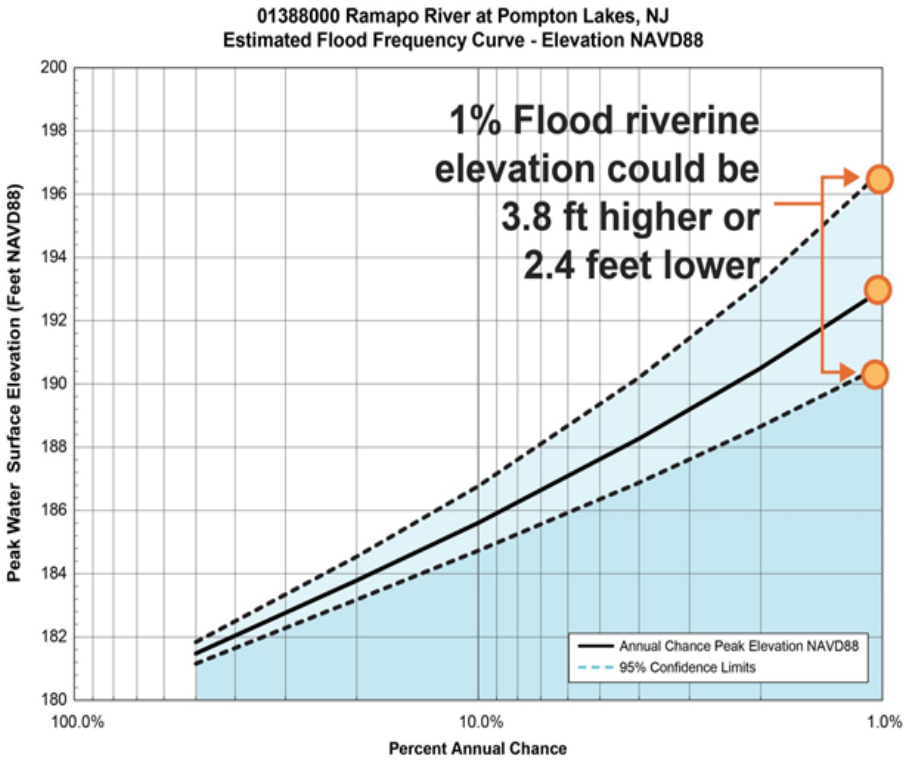

Figure 2. Range and average of flood elevations (within 95 percent confidence) for the Ramapo River at Pompton Lakes, NJ

the average, depending upon the data source.

Implications / Impacts of Decisions Made Today

The design criteria and flood elevations that are established today will impact generations to come. Professor Arthur Nelson of Virginia Tech has studied the probable life of facilities built today, and determined that a typical residential house built today will have a useful life of over 150 years. One estimate of damage from Superstorm Sandy counted over 650,000 houses that were damaged or destroyed. If we do not better inform people today about their future flood risk, and these structures are rebuilt at the 1-percent-flood elevation, we could see similar or worse damages in the future, placing a heavy financial burden on future generations.

Additional Design Considerations

The process we use to define flood risk today, as shown in insurance or statistical "average" recurrence interval elevations, includes important foundational assumptions that should be reconsidered when design elevations are recommended. Design elevations indicate where we can reasonably build a structure to be protected from failure due to flooding. Some of these assumptions include:

1) ***All flood related structures will operate properly and will never fail.*** We should consider the risk of a flood control structure such as a levee or dam failing, or the interior drainage of levees or flood walls not working as designed.

(Continued on Page 5)

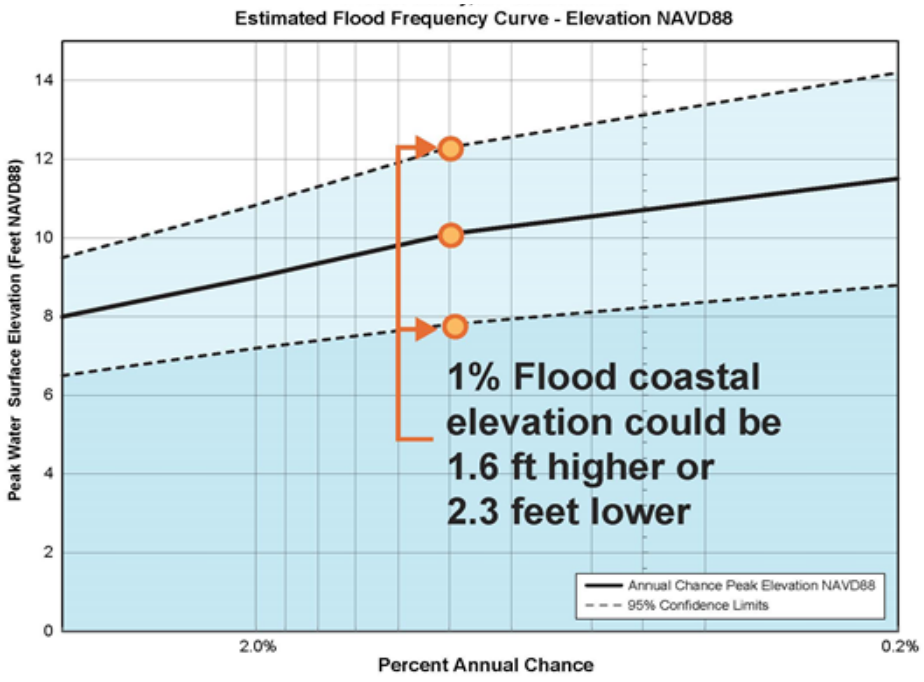

Figure 3.Range and average of flood elevations (within the 95 percent confidence) at the NOAA Battery, NY Tidal Station

(Continued from Page 4)

2) ***No debris will ever occur during a storm that will impact flood elevations.*** Houses, mobile homes, tanks, trees, and all types of debris clog culverts and bridges during storms, and create large backups in water surface elevation. We need to take into account the likelihood of debris for design elevations.

3) ***Future conditions will not impact flood elevations.*** FEMA commissioned a study on climate change that was released in June 2013, which shows that floodplains nationwide are likely to increase by 45 percent by the year 2100, and that the geography impacted by Sandy will increase by nearly 100 percent.[2] We need to account for these changes.

Establishment of Design Elevation Criteria

The elevation used for the design flood should take into account life and safety issues of the structure or facility expected during the life of the structure. The following equation can be used as a guide to develop design elevations:

The last item in the equation, a factor of safety, is critical to take into account the uncertainties of the predictive science of hydrology, hydraulics, and climate change.

$$\text{Design Elevation} = \text{Probability of flood control structure failure at a certain confidence limit} + \text{Probability that debris will impact the structure} + \text{Future Conditions (increased population impacts and climate change impacts)} + \text{An appropriate factor of safety}$$

A Move in the Right Direction

FEMA is aware of the differences between insurance elevations and design considerations. In 2013, FEMA introduced a non-regulatory product called 1-percent +, which shows the existing elevations at one standard deviation level of existing flooding. This is a step in the right direction to better inform communities of their potential for flood damage.

Summary

The way we talk about flood risk should be aligned with how we talk about other safety limits (i.e. the weight limits of bridges and elevators). If we continue to choose to communicate statistical "average" flood elevations, then we have the duty to explain the assumptions and variability around those numbers so that the every stakeholder fully understands the risk.

About the Author

Scott Edelman is the director of the AECOM Water Resources. He has 32 years of experience devoted to flood insurance studies and floodplain mapping. Mr. Edelman has been responsible for overseeing AECOM's floodplain mapping and mitigation work for the Federal Emergency Management Agency, as well as many state and local agency Cooperating Technical Partners, including agencies in Georgia, Alabama, North Carolina, South Carolina, Mississippi, Maryland, and California and local/regional CTPs in Florida, Texas, North Carolina, and Virginia. ❖

[2] AECOM, *The Impact of Climate Change and Population Growth on the National Flood Insurance Program Through 2100* (June 2013), available at http://www.aecom.com/deployedfiles/Internet/News/Sustainability/FEMA%20Climate%20Change%20Report/Climate_Change_Report_AECOM_2013-06-11.pdf.

Economics of Resilience

By Dane Egli and Jared McKinney

The degree of interdependence across critical infrastructure sectors has been amplified by globalization, advanced technologies, and supply chain pressures. Our team at Johns Hopkins University Applied Physics Laboratory is studying—through modeling, analyses, and empirical research in places such as the Port of Baltimore and Austin, Texas—the measurable impact of disruptive events, governance, and societal demands upon resilience ecosystems in bounded geographic areas.

Governments, communities, and individuals are not helpless in the face of natural disasters like Typhoon Haiyan, the category-5 super typhoon that struck the Philippines in November 2013, killing thousands and displacing hundreds of thousands. There are practical safeguards that can be designed within the multidisciplinary worlds of engineering, cyber-physical, and the social, behavioral, and economic (SBE) sciences if we systematically identify the independent variables that contribute to critical infrastructure interdependencies, conduct analyses that support a generalizable model, and test these methods under simulated and real-world conditions. Drawing from the principles of collective action theory and computational analytics our studies are seeking to quantify the cost accounting and value proposition behind resilience by integrating economic factors into the research.

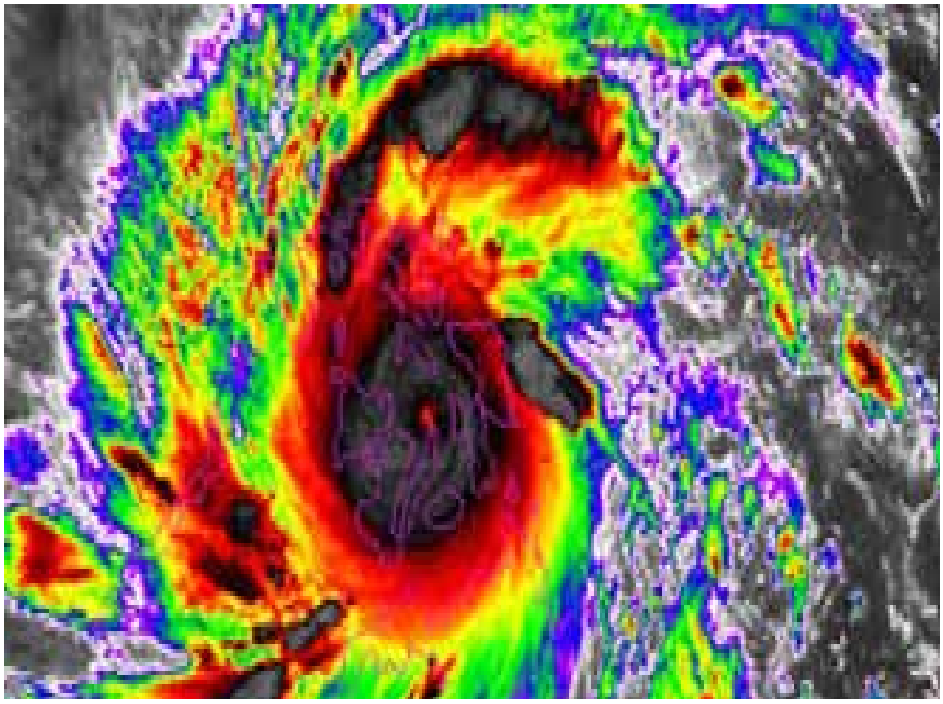

Figure 1. Typhoon Haiyan pictured in a NOAA satellite image taken November 8, 2013

By creating a more connected world, globalization and technology have increased transparency and business efficiencies while simultaneously making systems more vulnerable. Businesses have more complex supply chains than ever before, allowing for greater speed and specialization. Further, outsourcing permits businesses to benefit from the competitive advantage of diverse countries and companies. Purchasing from a single source reduces costs, and just-in-time delivery is reducing inventory and excess capacity. But these advances have also resulted in cascading impacts due to a global system with little room for error, in which a local disruption adversely impacts the entire supply chain in distant locations. This connectedness amplifies the consequences of small, local disruptive events as well as high-impact but low-probability "Black Swan" events, and the associated costs are high.

A groundbreaking 2005 study by Kevin Hendricks and Vinod Singhal analyzed the effects of 827 disruption events. The study found that over the course of three years, the average disruption reduced stock returns by up to an incred-

(Continued on Page 7)

(Continued from Page 6)

ible 40 percent. The result was a negative regardless of a disaster's cause.[1] A follow-up study showed that disruptions increase share price volatility by 13.5 percent, reduce operating income by 107 percent, decrease sales growth by 7 percent, and increase costs by 11 percent.[2] Infrequent and unlikely disruptions thus can destroy value created over a long period in a moment. As the study asserted, "There is a direct relationship between efficiency and risk."[3]

Supply-chain disruptions of varying degrees of severity are common. 73 percent of the respondents of The Business Continuity Institute's 2012 Annual Supply Chain Resilience Survey experienced at least one supply-chain disruption. Of these, nearly 40 percent occurred below the immediate tier-one supplier, showing the interconnectedness and complexity of modern business practices. Interestingly, information technology and telecommunications outages were the top sources of disruption, with severe weather taking a close second. The primary consequences of these disruptions are loss of productivity, increased-cost of work, loss of revenue, and customer complaints.[4]

Therefore globalization and supply-chain efficiencies—while among the great advances of the modern era—are only part of the value equation. Just as important is supply-chain *resilience*: the ability to withstand a crisis, absorb damage, recover quickly, and adapt to disruptive events. Resilience requires long-term planning and investment in redundancy, interoperability, and agility. Disruptions often cannot be predicted or controlled, but their negative impacts are incontrovertible. As Hendricks and Singhal conclude, "Investments in increasing reliability and responsiveness of supply chains could be viewed as buying insurance against the economic loss from disruptions."[5] This is part of the adaptive learning process that resilience offers in response to the lessons of 9-11, active shooters, storms like Katrina and Sandy, as well as the current Ebola outbreak.

In addition to mitigating the risks and hazards of supply-chain disruptions, resilience helps prepare businesses for future market slumps. According to Morgan Swink of the Neeley School of Business, "A firm's ability to weather economic downturns, deal with volatility and manage costs under shrinking demands depends in large part on the resiliency of its supply chains."[6] According to research he conducted with Nancy Nix, companies with supply-chain flexibility and adaptability are better able to reduce expenses during a downturn, allowing them to outperform competitors and receive a substantially higher return on assets and equity. Our team at Johns Hopkins is working at operationalizing resilience in various geographic locations—including key maritime ports and economic mega-regions of our nation—in order to establish a better interdisciplinary understanding of interconnected critical infrastructures in terms of physical, informational, and social phenomena.

Resilience is "disaster agnostic," meaning it will favorably mitigate damage, to varying degrees, caused by earthquakes, terrorists, pandemics, and economic downturns. And though it may be difficult to

(Continued on Page 8)

---

[1] Kevin B. Hendricks and Vinod Singhal, "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm," *Production and Operations Management* 14, no. 1 (Spring 2005): 35-52, available at http://www.wilfridlaurieruniversity.ca/documents/17398/scm_glitches_and_shareholder_risk.pdf.

[2] Kevin B. Hendricks and Vinod Singhal, "The Effect of Supply Chain Disruptions on Long-term Shareholder Value, Profitability, and Share Price Volatility," *Supply Chain Magazine* (June 2005), available at http://www.supplychainmagazine.fr/TOUTE-INFO/ETUDES/singhal-scm-report.pdf. A 2013 study by Accenture found that supply-chain disruptions reduce the share price of affected companies by 7% on average (World Economic Forum, *Building Resilience in Supply Chains* [January 2013]: http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf.

[3] Hendricks and Singhal, "The Effect of Supply Chain Disruptions": 3.

[4] Business Continuity Institute, *4th Annual Survey: Supply Chain Resilience 2012* (November 2012): h*ttp://www.zurich.com/internet/main/sitecollectiondocuments/reports/supply-chain-resilience2012.pdf*.

[5] Hendricks and Singhal, "An Empirical Analysis": 51.

[6] Neeley School of Business at TCU, "Weathering the Storm: How to Achieve Strategic Resilience Through Supply Chain Excellence" (06/16/12): http://www.neeley.tcu.edu/News_and_Events/Press_Releases/Weathering_the_Storm__How_to_Achieve_Strategic_Resilience_Through_Supply_Chain_Excellence.aspx.

(Continued from Page 7)

quantify, after every disaster businesses that prepared ahead of time come out on top.[7] For example, an earthquake three years before the 2011 Japanese Fukushima tsunami helped prepare a semiconductor manufacturer to recover before its competitors because it had established a strategy to shift production to unaffected manufacturing plants.[8] Maintaining critical operations in the face of disruptive events confers a measurable competitive advantage in the marketplace.

We know, from the emerging national policies and governance, that investing in resilience is a national imperative and increasingly considered a basic business practice. In addition to mitigating disaster-related damage by introducing new flexibility, it increases productivity, revenue, reputation, and shareholder value.[9] Investing in resilience before disaster strikes is the smart choice for individuals, companies, and governments alike. What is the value proposition or return on investment? For individuals, it is an investment in adaptive safety and security. On the part of the government, it saves lives and property. For businesses, it protects the bottom line and sharpens their competitive advantage.

About the Authors

Dr. Egli is a senior advisor at Johns Hopkins University and author of, "Beyond the Storms—Strengthening Homeland Security & Disaster Management to Achieve Resilience." Mr. McKinney is a dual-degree graduate student in International Affairs at Peking University and London School of Economics. ❖

[7] Mukta Agrawal and Casey Church, "Resilience Return on Investment – An Impossible Argument?" Analytic Service, Inc. (04/24/12): http://tisp.org/index.cfm?pk=download&pid=10261&id=12606%E2%80%8E.

[8] Kelly Marchese, Siva Paramasivam, and Michael Held, "Bouncing Back: Supply Chain Risk Management Lessons from Post-tsunami Japan," Industry Week (03/09/12): http://www.industryweek.com/global-economy/bouncing-back-supply-chain-risk-management-lessons-post-tsunami-japan.

Campus-Wide Resilience Assessment

By Frédéric Petit, Rosalie Laramore, and David Dickinson*

Introduction

There are many ways to conduct vulnerability, resilience, or risk assessments. Assessing resilience or vulnerability for a single building or single facility is rather straightforward, but assessing it for a campus-like environment that has many buildings or facilities and diverse missions presents several challenges. For example, a campus environment could be a group of several facilities within a well-defined perimeter. In other cases, it could be a group of buildings or facilities belonging to a single organization that are in close proximity but within an area with only a minimal or no defined perimeter. These cases occur often when a college campus, a group of federal or state buildings, or research laboratories are being assessed. The common theme in most campus environments is the various buildings' dependence on a common utility (e.g., electric power, steam, water, wastewater removal services, natural gas, and communications) or utility provider; however, the business impact of a loss of service on each individual facility or asset within the campus is unique.

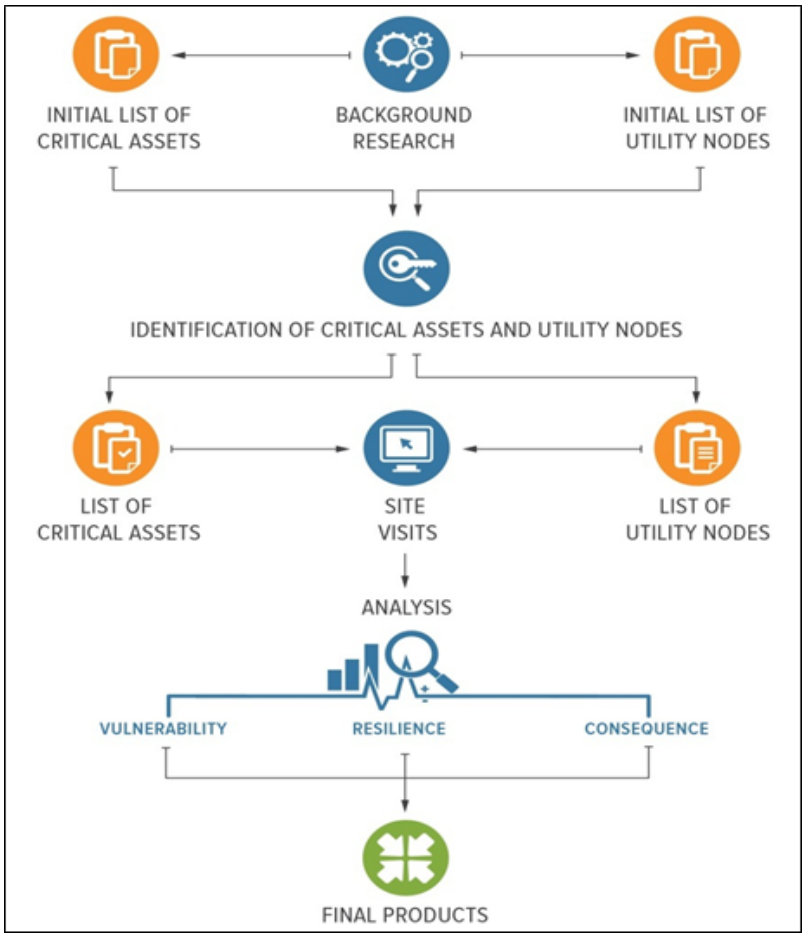

Figure 1. Overview of the Assessment Methodology

Objective of the Assessment

Recent events (e.g., the assault on a California power station[1]; the discovery of an incendiary device in a substation near Tucson, Arizona[2]; the incident at a Federal Aviation Administration air-traffic control center in Aurora, Illinois, which halted operations across Chicago Air Route-controlled airspace[3]; and the shutdown of two national-

(Continued on Page 10)

[1] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *The Wall Street Journal* (Feb. 5, 2014), http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778, accessed Nov. 8, 2014.

[2] Elizabeth Kreft, "Another Attack Discovered at an Electricity Substation near the Border – and One Congressman Says It's 'Only a Matter of Time' before More Attackers 'Exploit This Vulnerability,'" *The Blaze* (June 16, 2014), http://www.theblaze.com/stories/2014/06/16/another-attack-discovered-at-an-electricity-substation-near-the-border-and-one-congressman-says-its-only-a-matter-of-time-before-more-attackers-exploit-this-vulnerability/, accessed Nov. 8, 2014.

[3] Bart Jansen, "FAA Prepares to Reopen Chicago Control Center after Fire," *USA Today* (Oct. 12, 2014), http://www.usatoday.com/story/news/nation/2014/10/12/faa-chicago-fire-air-traffic-control-center/17158951/, accessed Nov. 28, 2014.

(Continued from Page 9)

laboratory supercomputers because of smoke from a nearby wildfire[4]) have reinforced the need for an all-hazards risk assessment that could identify the vulnerabilities of utility systems and also the enhancements that could improve these systems' resilience. For a campus, such an assessment would have to characterize the vulnerability and resilience of the main utilities that supply resources to the campus and also define how their disruption or loss might affect the campus's essential functions.

Methodology

The proposed assessment methodology is "threat-agnostic" in order to capture the widest possible range of vulnerabilities and resilience measures as well as to consider the potential consequences, protective and emergency measures already in place, and dependencies on utility supply. This type of method also avoids overlap or interference with any regulatory or ongoing security or threat assessments. As shown in Figure 1, the assessment includes four main phases:

- Background research,
- Identification of critical assets and utility nodes,
- Site visits, and
- A vulnerability, resilience, and consequence analysis.

Phase 1: Background Research

The first phase consists of reviewing previous assessments, existing plans, and other available information to refine the assessment's scope, identify the campus's essential functions, develop preliminary lists of critical assets and utility nodes, and support the subsequent assessment activities.

Phase 2: Identification of Critical Assets and Utility Nodes

The second phase prioritizes the assets and utility nodes that are most critical with regard to campus operations and that would, if disrupted or lost, negatively affect the campus's ability to fulfill its essential functions. This second phase specifically uses the principles of business impact analysis (BIA), presented in PS-Prep™ program and associated standards,[5] to define a final list of critical assets and utility nodes that support the essential functions of a campus that will be visited during the assessment.

Phase 3: Site Visits

The third phase consists of 1-hour to 3-hour site visits at each critical asset and utility node identified during the previous phase. During each visit, analysts meet with building managers, maintenance foremen, and facility engineers to learn about the building's operations, potential impacts from a utility loss, and existing security and emergency procedures. Each visit concludes with a tour of the buildings to observe the protective and resilience measures in place and the utility connections.

Phase 4: Vulnerability, Resilience, and Consequence Analysis

The fourth and final phase of an assessment consists of analyzing the data collected during the earlier phases in order to conduct a comprehensive risk analysis that identifies vulnerabilities, resilience, and consequences related to the operations of the utilities that supply resources or services to the campus.

Security specialists seek to conduct a rigorous *vulnerability analysis* that identifies the protective measures in place and then proposes options to increase the campus's protection and thus decrease its vulnerability. Analysts first address the elements of security (e.g., protective measures) and risk management standards and manuals.[6] Next they consider the facility's equipment and procedures in order to identify the elements that could increase the protection and decrease the vulnerability of the campus's critical assets.

(Continued on Page 11)

[4] Patrick Thibodeau, "Los Alamos Shuts Down Supercomputers as Fire Advances," *Computerworld* (June 29, 2011), http://www.computerworld.com/s/article/9218042/Los_Alamos_shuts_down_supercomputers_as_fire_advances_, accessed Nov. 8, 2014.

[5] ISO (International Standards Organization), *ISO 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements* (2012), http://www.iso.org/iso/catalogue_detail?csnumber=50038, accessed Nov. 10, 2014; BSI America, BS 25999 Business Continuity (2010), http://www.bsiamerica.com/en-us/Assessment-and-Certification-Services/Management-systems/Standards-and-Schemes/BS-25999/, accessed Nov. 10, 2014.

[6] These include FEMA (Federal Emergency Management Agency), *FEMA 426 – Risk Management Series, Reference Manual to Mitigate Potential Terrorist Attacks against Buildings* (2003); FEMA, *FEMA 452 – Risk Management Series, Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks against Buildings* (2005); ASIS International, *ASIS – Protection of Assets Manuals (2012); and Interagency Security Committee, Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard* (2010).

(Continued from Page 10)
The vulnerability analysis focuses primarily on five components: physical security; security management; security force; information sharing; and security activity, history, and background. A specific emphasis is placed on identifying the measures that have been implemented to protect the connections between utility supply systems and the campus's critical assets.

Engineering, business continuity, and emergency management specialists conduct a *resilience analysis* by considering relevant national programs and standards. Their analysis specifically addresses elements of resilience.[7] The analysts review existing continuity of operations and emergency plans and procedures. They then consider the existing equipment and procedures at the facility level. The team identifies the elements that are in place (or could be implemented) to decrease the level of consequences on facility operations and campus functions as a result of the loss of utility services. The resilience assessment focuses primarily on four components: preparedness, mitigation measures, response capabilities, and recovery mechanisms.

Finally, the *consequence analysis* seeks to assess the impacts on critical assets' operations and essential functions in the event of a disruption in or a loss of utility services. Data collection focuses on capturing the variation of consequences over time. This information can be used to generate dependency visualization tools, which characterize the amount of degradation over time resulting from a loss of utility service and the impact on the critical asset's core operations.[8] These curves summarize elements of the vulnerability and resilience analysis and allow the campus managers to anticipate the impact of the loss of utility services on campus operations and ultimately on the campus's missions.

The scope of an analysis is directly related to the requirements of the stakeholders that are in charge of campus business continuity and to the types of final products desired (e.g., report or interactive display tool).

Benefits and Challenges

Conducting a campus-wide assessment can help prioritize assets and the interconnection of the facilities and the utilities required to operate them. Presenting the findings to the users of each facility can help form a BIA for each facility. That BIA information can then be aggregated to include all campus facilities and used to help set priorities for protection and resilience and better understand how each part of the campus fits into the overall mission from a utility infrastructure perspective. This process, combined with ongoing threat and risk management functions, informs leaders regarding potential issues and guides them regarding possible funding.

As in the case for most assessments, interviewing the appropriate people who actually operate and know the systems is the key to successful results. The security manager might represent the initial path into a facility but might not be able to explain in detail how a steam boiler operates and what is required to keep the boiler functioning. These assessments can also take time. Coordinating the site visits, collecting the information, and analyzing the results might take several months and require a team with members having expertise in multiple areas (e.g., engineering, emergency management, security management, business continuity).

Conclusion

Recent events reinforce the need for resilience and risk assessments to consider dependencies on utility services. Such dependencies are usually considered in assessments at the facility level, but it is more challenging to consider them when the assessment is focusing on a campus of facilities with different missions. However, using such an approach, which is centered on business continuity principles and the consequences that occur over time due to the degradation of utility services,

(Continued on Page 12)

[7] Specialists address elements of resilience as characterized in FEMA, *PS-Prep™ Program,* and in associated standards such as these: BSI America, *25999 Standard – Business Continuity* (2014), http://www.bsiamerica.com/en-us/Assessment-and-Certification-Services/Management-systems/Standards-and-Schemes/BS-25999/, accessed Nov. 10, 2014; NFPA (National Fire Protection Association), *1600 Standard on Disaster/Emergency Management and Business Continuity Programs* (2013); ASIS International, *ANSI/ASIS SPC.1-2009 Standard on Organizational Resilience* (2009); and ISO, *22301:2012 – Societal Security – Business Continuity Management Systems – Requirements* (2012), http://www.iso.org/iso/catalogue_detail?csnumber=50038, accessed Nov. 10, 2014.

[8] Frédéric Petit, K. Wallace, and J. Phillips, "Interactive Dependencies Curves for Resilience Management," *Journal of Business Continuity & Emergency Planning* (London: Henry Stewart Publications, accepted for publication).

(Continued from Page 11)
outlines the repercussions of service degradation on a campus's operations and ultimately its missions. Combining such an evaluation of the utility infrastructure with known threats and hazards information is an excellent exercise for any organization to conduct to decrease its vulnerabilities and increase its resilience.

Acknowledgment

The work presented in this paper was partially supported by Argonne National Laboratory under US Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of 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.

About the Authors

Frédéric Petit, Rosalie Laramore, and David Dickinson are with the Risk and Infrastructure Science Center in the Global Security Sciences Division of Argonne National Laboratory. ❖

Stress Tests and Critical Infrastructure Protection Resilience

by Luca Galbusera, Georgios Giannopoulos, and David Ward

The term 'stress tests' probably brings to mind the scrutiny of financial institutions especially as regards debt exposure and suspicious dealings in finance. The connotation appears to doubt the robustness not just in terms of solidity in the event of a financial recession but also resiliency versus a potential economic meltdown. From this we evolve our thoughts towards validation and verification of banks and overall, rethink the solidity of the banking sector.

Similarly, and especially since the Fukushima incident, nuclear plants and the nuclear sector in general have been forced to rethink their risk assessment and failure mode analysis approach by introducing stress testing. Here stress testing focuses more on the infrastructure and its criticality if things get out of control.

In both the financial and nuclear sectors the onset was caused by unexpected and extraordinary scenarios that had a very low probability as such but also an extreme impact on both the citizen and society should they occur, which they did. The response of the authorities was the introduction of new regulations, tighter controls, and stress testing. In the nuclear sector the main aims of stress testing are to:

1. assess the safety and robustness of the nuclear power plants (NPPs) in case of extreme natural events (as in Fukushima) shutting down the normal safety functions of the plant, and
2. assess the ability of the NPPs to deal with severe accidents.

In the financial sector, stress testing dates back to the early '90s, albeit in small numbers and through wide lenses. This shows that the sector was already aware of the risks that, if verified, could cripple not just a bank and a banking system but fundamentally also the credibility of a country and region. In banking, stress testing refers to a range of techniques used to assess the vulnerability of a financial system to "exceptional but plausible" macroeconomic shocks. Just as with nuclear plants, banks can also be stress-tested to reveal vulnerabilities and subsequently make contingency plans. The end goal is to introduce measures to mitigate against severe circumstances and ultimately protect both the infrastructures and those who benefit from the services they provide.

To this end Joint Research Centre (Ispra, Italy) is exploring the opportunity to introduce stress tests to other sectors with the intent to improve CIP at a European level, if not beyond.

The current line of thought is to measure, mitigate and monitor in the context of prevention and preparedness. The purpose is to associate the severity of a hazard or a disruptive event with the potential impact on a system or on society as a whole.

Stress Tests and the European Context of CIP

The European Program for CIP (EPCIP) established in 2006[1], was recently revised. The result was a staff working document[2] which may be summarized in four points:

1. Draw and drive more attention towards the issue of interdependencies between critical infrastructures (CIs) especially in terms of functionality;
2. Take into account the spatial dimension of CIP. So in addition to the functional dimension push for a better understanding of cross-border, cross-sectorial interdependencies as well as intra-sector equivalents;
3. Protect infrastructures against all-hazards, not just specific threats, and more specifically realize this risk management approach;
4. Take into account resilience. While risk assessment discusses probability and severity with the aim to set risk barriers, resilience sets out to identify the landscape

(Continued from Page 14)

[1] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[2] COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD(2013) 318 final, Brussels, 28.8.2013

(Continued from Page 13)

of the relevant measures that need to assure the continuity of services implicitly accepting that not everything can be prevented. In other words resilience is seen also as a means of assessing low probability but high impact events such as natural catastrophes for which a traditional risk assessment process fails.

This last point is where stress tests can come into play because they support the work of operators, stakeholders, and policy makers by providing insight into the impact of such events. Moreover, such tests also help to provide understanding of the limitations of existing measures, assess the resilience margins of systems and lastly, improve the awareness for the consequences of such events. Highlighting the application of stress tests for critical infrastructures and realizing the expectancies for future work in this field is also captured in STREST, a Seventh Framework Programme (FP7) program funded research project in which JRC is a participant. The aim of this project is to define a framework for stress tests in the domain of critical infrastructures by taking a holistic view on this topic (http://www.strest-eu.org/opencms/opencms/).

Stress Tests vs Exercises in the Context of Critical Infrastructures

A common misconception is to consider stress tests to be a synonym for exercises. In reality they cover two different temporal spaces (see Figure 1) with possibly some overlap in between.

Exercises mainly focus on the assessment of the response mechanisms in the aftermath of a critical event and the communication between the various actors to resolve the crisis. The event provoking an emergency/crisis is part of the scenario.

Figure 1. Exercises and stress tests in the EPCIP framework.

Stress tests on the other hand serve the purpose of associating the severity of a hazard or a disruptive event with the potential impact on a system or on the society as a whole. To achieve this implies identifying the operative limits as well as the vulnerabilities of CIs. Henceforth the importance of stress tests to achieve these targets is paramount.

Another differentiating factor between exercises and stress tests is the type of involvement of different actors. Exercises typically focus on the public authorities (e.g. fire brigade, civil protection) being requested to respond to crisis situations and to interface with the sectorial operators. Then again stress tests often involve CI operators and/or the sectorial associations according to a hierarchical perspective. This choice is in compliance with the idea that the identification of the operative limits and vulnerabilities mentioned above can be best performed by directly resorting to first-hand information and to technical competencies most strictly related to the CIs themselves. That said, both exercises and stress tests represent the core part of the prevention and preparedness work by assessing the limits of infrastructures and systems in such crises.

Stress Tests: Considerations for CIP in Europe

Modern CIs are often characterized by a high degree of interconnectedness and display complex performance capability. This complexity derives from several features including:

- the extent of the infrastructure;
- interaction with other infrastructures belonging to the same or different classes;
- different ownership and competitive aspects; and
- in many cases with a high degree of specialization, in the service delivered.

These features suggest that the interpretation of the task of CI stress testing should be a collaborative effort involving public (national and international) authorities, sectorial associations, and firms. Experience from current stress tests reveals that individual firms often have some capability to deliver a detailed analysis of the risk factors specific to the infrastructure they manage, as well as its fragility. In high-specialization sectors, the exploitation of specific competencies and knowledge is both a need and advantage for the different parties (security, insurance companies, certifiers, etc.) involved.

Furthermore, in the EU the assessment of critical sectors and their interdependencies has two dimen-

(Continued on Page 15)

(Continued from Page 14)

sions. First, and in a jurisdictional/national sense, we have to take into account how the different critical sectors of a country interact with the corresponding partners of other countries (cross-national interdependencies). Second, and generally speaking, interdependencies involve different sectors (cross-sectorial interdependencies).

Together these dimensions take CI stress testing initiatives into the domain of System-of-Systems testing. Within this framework the exchange of data and the interfacing among different infrastructure operators becomes awkward. Further it considerably complicates the analysis because during critical events a trigger starting in one sector will affect others causing occasional cascading effects that equally represent a criticality. This eventuality is even more pressing because of today's market liberalization initiatives that involve an increasing number of European CIs and introduce further competitive dynamics. All these features (network structure, interdependence, competitive framework) emphasize some similarities with stress testing in the financial sector.

The cornerstone of stress tests development is the mobilization and involvement of the right actors. This is based both on real case studies in the nuclear and banking sectors and the need to involve both private and public representatives (national and international) in a multi-layered approach. Previous stress testing initiatives have involved different approaches. Most notably, we can distinguish between top-down approaches (i.e. the analysis is performed entirely by the governing institution, relying on its own internal models and simulations based on data received from the involved stakeholders) and bottom-up approaches (i.e. where the authority provides a set of scenarios to the individual stakeholders, which perform their analyses based on internal models, and the authority finally aggregates the results).

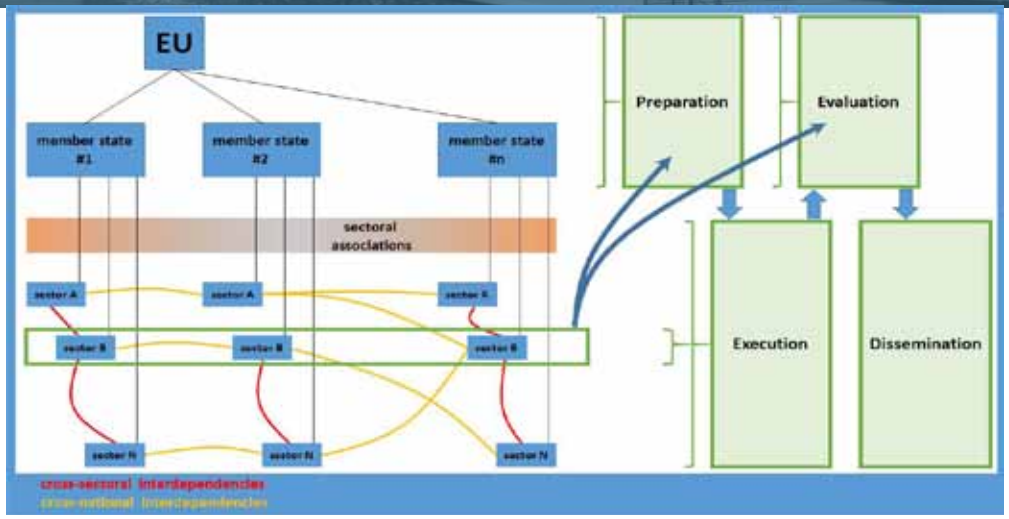

Figure 2. Top-down and bottom-up approaches promote inclusiveness for CIP (from authorities to operators).

Both these approaches may coexist in development of stress tests for CIs, for instance in the EU. Four distinct phases can be envisioned: preparation, execution, review, and dissemination of the test results (see Figure 2).

The preparation phase is the definition of the stress test scenario(s) and implies defining the relevant technical detail in close agreement among the actors. This is to match the high-level objectives of the authorities with the feasibility assessment done by the owner of the infrastructure, so that the owner is in a position to evaluate the relevant CI limitations and can provide feedback on the requests from the authorities or the regulator. A bottom-up type of high-level analysis could support this preparation stage.

The execution phase is entrusted to the owner/operator of the infrastructure, as is applied in the nuclear and banking sectors. The owners/operators of CIs are the only actors that are actually in a position (in terms of means, procedures, and know-how) to execute the scenario of stress tests. This option also responds to a need for trust and confidentiality. In fact, on one side it favors the active involvement of stakeholders and helps enhancing communication and transparency among public authorities, companies and sectors towards critical events. On the other side, it could serve to circumvent the reluctance of market-competitive firms to disclose private information. The next step in the process is the evaluation of the results by the regulator or national authority responsible for the particular sector. This reflects the sectorial knowledge of the critical infrastructure owner/operator who is not in a position to assess interdependencies due to a lack of

(Continued from Page 16)

(Continued from Page 15)

knowledge of the modus operandi of the other sectors. The role of the regulator/authority is to detail interdependencies in terms of key features and then exploit them in a second round of analysis. In this way it would reveal the level of interdependencies among sectors and pave the way for a detailed report. Reflecting on the best practices from the nuclear and banking sectors, the last step is to submit such reports to an international body or authority in order to identify the cross-border interdependencies and render the whole process homogeneous and comparable among the various Member States.

The final phase is the dissemination of results to the general public. As witnessed in nuclear stress tests, this would enhance the confidence in the resilience of relevant CIs.

Concluding Remarks

As briefly mentioned the revised EPCIP document suggests that stress tests can be included in the discussion for improving the protection of critical infrastructures. Our analysis pointed out some fundamental considerations for performing stress tests on CIs:

- hierarchical involvement of the authorities and sectorial associations;
- necessity for interdependency identification and description;
- choice of most appropriate scenarios and CIs;
- results of first and higher-order bottom-up stress tests;
- comparison of these results with top-down stress tests;
- review of results and findings;
- disclosure of the stress test results.

We consider that the peer review and dissemination of results of stress tests witnessed in the nuclear and banking sectors could also be followed for other CIs, albeit with suitable traffic-light protocols for sensitive information sharing. This helps build trust and confidence in the security, safety, and resilience of CIs among the general public. This praxis is considered crucial in properly completing the process of CI stress testing and understanding vulnerabilities, resilience, and interdependencies.

The revised EPCIP puts stress tests firmly in the discussion for improving prevention and preparedness of CIs. The relevant learnings from the nuclear and banking sectors show that stress tests can play an important role in assessing their safety, security and resilience. This is in spite of the fact that the approaches implemented in each sector vary significantly and yet, are complimentary. The extension to other sectors certainly seems conceptually conceivable. Indeed, top-down and bottom-up hierarchical approaches can become an inclusive reality also for CIP.

Accordingly the extension of stress tests to CIP and more specifically CIR (Critical Infrastructure Resilience) or a combination (CIPR) seems equally plausible without excluding the assessment of safety and security of an infrastructure. In terms of future work the expectation is to build stress tests tailored to the needs of the corresponding sector, stakeholders, and actors all the way down to single infrastructure level.

About the Authors

Luca Galbusera, Ph.D. holds BSc and MSc degrees in Systems and Control Engineering and a PhD in Information Engineering from Politecnico di Milano. He is currently scientific officer at the European Commission's Joint Research Centre. His research interests include optimal and robust control, multi-agent and networked systems, resilient control of critical infrastructures.

Georgios Giannopoulos, Ph.D. holds a degree in Mechanical and Aeronautical Engineering, a PhD in Engineering Sciences from Vrije Universiteit Brussel and a management degree from Solvay Brussels School in Economics and Management. He joined the European Commission's Joint Research Centre in 2007 where he is working in the domain of risk and resilience analysis of critical infrastructures with focus on systems of systems perspective, interdependencies modelling and economic impact of critical infrastructure disruption.

David Ward, Ph.D. is currently a freelance technical and managerial consultant working both in industry and for the European Commission and Regione Lombardia (Italy). He has published over 60 papers in both international and national journals on a wide range of scientific and managerial topics including critical infrastructure protection. His most recent publication in critical infrastructure security and resilience includes 2 book chapters and recent articles covering the ERNCIP project in the IJCIP and Center for Infrastructure Protection and Homeland Security's The CIP Report.❖

Critical Infrastructure Dependencies and Interdependencies Assessment

by Frédéric Petit, David Dickinson, Timothy Klett, Karen Guziel, Duane Verner, and Julia Phillips

The United States faces significant challenges to prevent, protect against, mitigate, respond to, and recover from threats and hazards. The National Infrastructure Protection Plan (NIPP) provides the strategic vision to guide the national effort to manage risk to the Nation's critical infrastructure. The achievement of this vision through understanding and enhancement of security and resilience of critical infrastructure is challenged by the complexity of critical infrastructure systems and their inherent dependencies and interdependencies. The 2013 NIPP presents an opportunity for advancing Federal efforts on further understanding and analyzing dependencies and interdependencies. Such an important undertaking requires the involvement of public and private sector stakeholders and the reinforcement of existing partnerships and collaborations within the U.S. Department of Homeland Security (DHS) and other Federal agencies, including national laboratories; state, local, tribal, and territorial governments; and nongovernmental organizations. Assessing critical infrastructure dependencies and interdependencies requires the consideration of complex and multidimensional elements (Figure 1).[2]

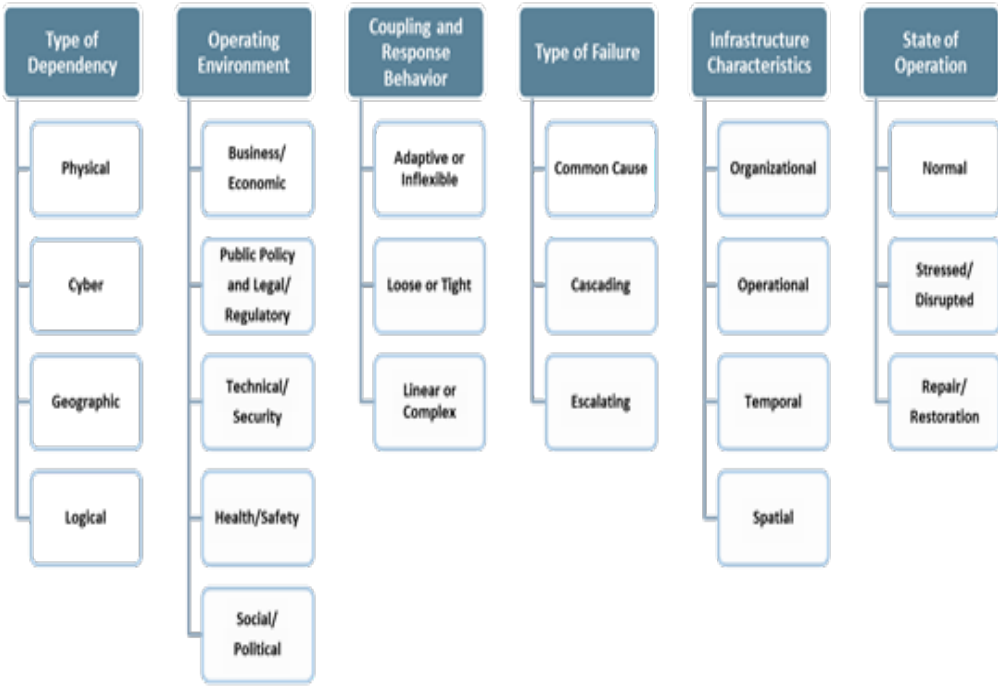

Figure 1 Dimensions of Dependencies[3]

The term, "Type of Dependency," captures the existing interactions between infrastructures. "Operating Environment" characterizes elements that could affect the different types of dependencies. "Coupling and Response Behavior" illustrates how a critical infrastructure could respond to a disruption related to a dependency. "Type of Failure" addresses the degradation that could result from existing interactions between infrastructures. Finally, a risk assessment that integrates dependency and interdependency considerations must account for the specific "Infrastructure Characteristics" of each infrastructure and for each one's "State of Operation" when an incident occurs (e.g., degradation of infrastructure interconnections). Perfect understanding of dependencies would incorporate multiple aspects of this

(Continued on Page 18)

[1] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure and Resilience* (Washington, DC: U.S. Department of Homeland Security, 2013), http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience, accessed November 10, 2014.

[2] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine 21*, no. 6 (Dec. 2001): 11–25, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=969131&tag=1.

[3] Ibid.

(Continued from Page 17)

multi-dimensional space.

Approaches to Characterizing Dependencies

Each type of dependency has its own characteristics, which require different bottom-up and top-down approaches.[4] Figure 2 represents the concept of bottom-up and top-down approaches applied to critical

(Continued on Page 19)

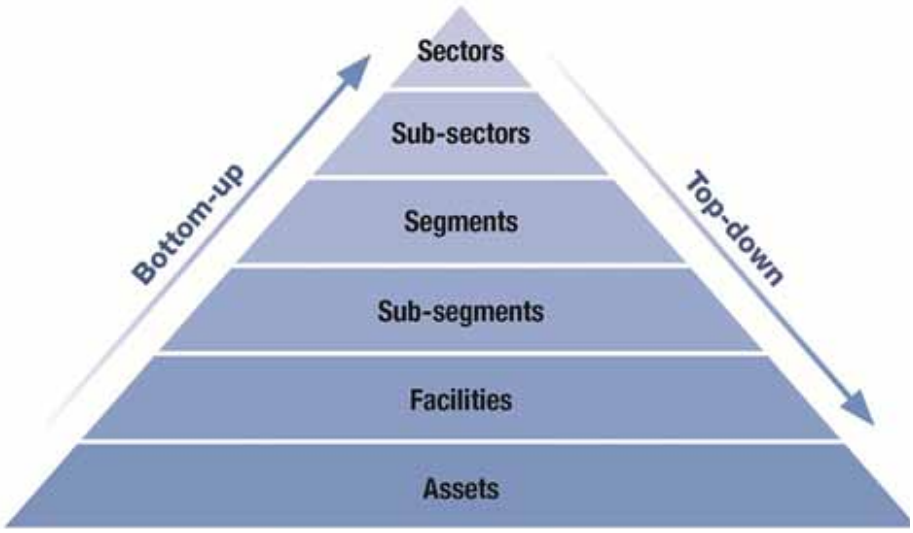

Figure 2. Bottom-up and Top-down Approaches

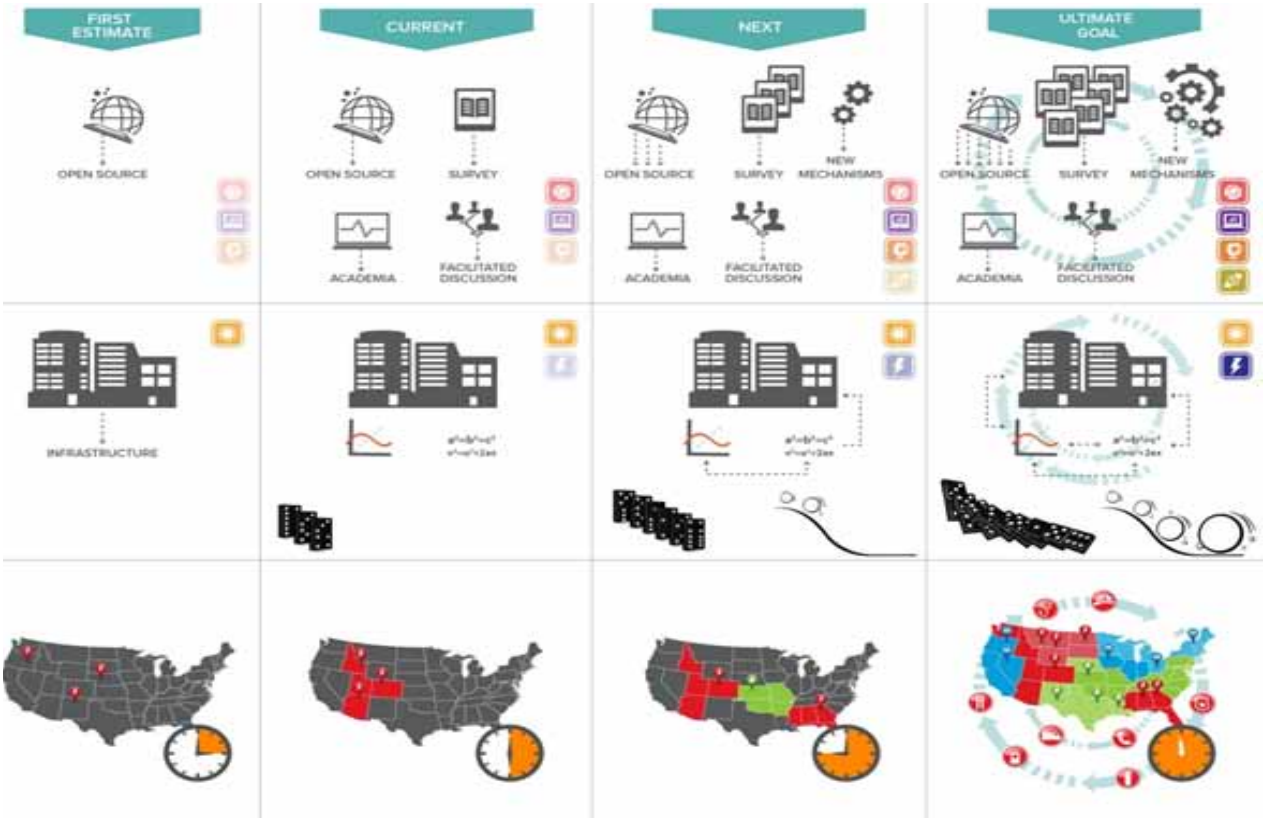

Figure 3. Complexity of Analyses of Critical Infrastructure Dependencies and Interdependencies

In the top row, the pictograms in the lower right of each cell show the different types of dependency considered in each phase of development; from top to bottom, they are physical, cyber, geographic, and logical. In the middle row, the pictograms in the top right of each cell represent the states of operation considered: normal and degraded. In the bottom row, the red pictograms in the cell at the far right (ultimate goal products) represent the different critical infrastructure sectors.

---

[4] Duane Verner, and Frédéric Petit, "Resilience Assessment Tools for Critical Infrastructure Systems," *The CIP Report 12, no. 6* (Dec. 2013): 2-5, http://cip.gmu.edu/wp-content/uploads/2014/01/December-2013_Resilience.pdf.

[5] DHS created the Infrastructure Data Taxonomy (IDT) to facilitate a common understanding of infrastructure terminology within the critical infrastructure protection community. The IDT organizes infrastructure by level (i.e., sector, sub-sector, segment, sub-segment, and asset). For example, a wastewater lift/pump station X (Facility X) would be categorized in the Water Sector, Wastewater Facility Sub-Sector, Wastewater Collection System Segment, and Lift/Pump Station Sub-Segment. Facility X requires other operational and technical elements to be functional to maintain its operation.

(Continued from Page 18)

Table 1 First Estimate Phase: Level of Analysis

Data	Analysis	Products
• Open source (potential impacts, potential dependencies, and general service areas)	• General understanding of sector dependencies and of assets within a sector • Limited knowledge of cascading impacts • No knowledge of escalating failures	• Static: general service maps and general sector informational reports • Evaluation of failures from common causes and their direct consequences

infrastructure.

Dependencies and interdependencies exist at each level of the pyramid (e.g., assets are interconnected with other assets) and between the levels (e.g., assets are interconnected with facilities, facilities are interconnected with sub-segments, and so on).[5]

Analyzing dependencies and interdependencies among critical infrastructure first requires examining the unidirectional links (dependencies) and then considering the bidirectional links (interdependencies). These two types of links are the basis for conducting cascading and escalating failure analysis. Argonne has defined four phases of development for dependency and interdependency assessment. Each phase of development varies in the level of data required, the type of analysis conducted, and the type of resulting products (Figure 3).

Phase 1 - First Estimate

The First Estimate Phase relies on open source information and provides a limited analysis. Such an analysis offers a general understanding of the functioning of a critical infrastructure but does not permit the real-time visualization of cascading and escalating failures. Table 1 is an overview of the elements characterizing the First Estimate Phase.

Phase 2 - Current Phase

In the Current Phase, several research teams are developing data collection tools and models allowing for a more detailed analysis of critical infrastructure dependencies and interdependencies. These data collection and modeling efforts start to address physical, cyber, and geographic dependencies and initiate the anticipation and visualization of first-order cascading failures. However, most of the existing tools and models operate in silos and have little interaction with similar tools and models. The consideration of logical dependencies and escalating failures is still a challenge. Currently, few approaches consider how disruptions to facility dependencies could affect operations that are already degraded due to previous disturbances. Table 2 presents an overview of the elements characterizing the Current Phase of development.

Phase 3 - Next Phase

The Next Phase of development considers all of the dimensions characterizing critical infrastructure dependencies and interdependencies, as shown in Figure 1. This phase of development requires new data collection mechanisms and a better integration of existing independent assessment tools and approaches. It transitions analysis centered on facilities to assessment focus on critical infrastructures systems. Table 3 presents an overview

Table 2 Current Phase: Level of Analysis

Data	Analysis	Products
• Open source • Surveys • Proprietary databases • Facilitated discussions with stakeholders	• Refined information specific to assets within the sector • Better understanding of specific dependencies at the asset level • Differentiation between physical and cyber dependencies during normal operations • Disconnected mathematical system models (not automated) • Normal operations	• Refined visualization of degradation propagation • Better understanding of 1st order cascading failures (some notion of temporal aspects) • Dependency/degradation curves for assets • Some interactive operational tools

(Continued on Page 20)

(Continued from Page 19)

Table 3 Next Phase: Level of Analysis

Data	Analysis	Products
• Implement new data collection mechanisms • Capture more characteristics of dependencies (added detail on physical and cyber dependencies; start integration/analysis of geographic dependency)	• Integrate system-level models • Integrate cyber and physical models • Address conditions during normal operations and degraded-state operations	• Refine cascading and escalating visualization, including second-order and third-order cascading failures • Improve temporal and spatial visualization

of the elements characterizing this next phase of development.

Phase 4 - Ultimate Goal Phase

The Ultimate Goal Phase contains a comprehensive understanding of all dependency and interdependency dimensions. It allows decision makers to anticipate and characterize, in real time, how all dependency and interdependency dimensions influence the resilience and protection of a critical infrastructure, of a region, and, ultimately, of the nation. Table 4 presents an overview of the elements characterizing the ultimate goal of development.

These four phases support the development of a comprehensive assessment of critical infrastructure dependencies and interdependencies. The characterization of the ultimate goal will guide the direction of the work needed to understand, assess, and manage critical infrastructure dependencies and interdependencies. This effort requires a collaborative environment that promotes information sharing and multidisciplinary analyses and must go beyond a consideration of only the critical infrastructure (e.g., it should consider environmental, social, and economic characteristics that affect the resilience of a region). The end goal is a comprehensive, flexible, proactive, and dynamic assessment of all dimensions that characterize critical infrastructure dependencies and interdependencies.

Conclusion

Critical infrastructure dependencies and interdependencies are complex elements to consider. They are characterized by different dimensions (e.g., types, operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operation). They influence all components of risk; they can constitute a threat or hazard, affect the resilience and performance of critical infrastructure, and lead to the propagation of cascading and escalating failures. It is therefore essential to integrate the characterization of dependencies and interdependencies into risk and resilience methodologies. A data-driven capability that operationalizes the analysis of dependencies

Table 4 Ultimate Goal Phase: Level of Analysis

Data	Analysis	Products
• Collect information for all dependency dimensions • Develop a process to capture all needed information (e.g., beyond critical infrastructure only)	• Complete risk and resilience analysis, integrating both dependencies and interdependencies • Integrate system models that are mostly automated • Conduct in-depth analysis of all dimensions of dependencies and interdependencies	• Comprehensive analysis of dependencies and interdependencies for risk and resilience assessment • Real-time visualization tool for cascading and escalating failures • Early warning system that identifies potential cascading and escalating consequences • Integrate business continuity, emergency management, and communication processes

(Continued from Page 21

(Continued from Page 20)

and interdependencies would not only provide an unprecedented level of situational awareness, it would also enable decision makers to anticipate disruptions, which would have a significant impact on regional resilience. To achieve this ultimate goal, the development of a comprehensive and interactive assessment of critical infrastructure dependencies and interdependencies requires the combination of multiple areas of expertise (e.g., engineering, social sciences, business continuity, and emergency management) in an adaptive and flexible assessment framework.

Acknowledgment

The work presented in this paper was partially supported by Argonne National Laboratory under US Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of 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.

About the Authors

Frédéric Petit, David Dickinson, Timothy Klett, Karen Guziel, Duane Verner, and Julia Phillips are with the Risk and Infrastructure-Science Center in the Global Security Sciences Division of Argonne National Laboratory. ❖

Building an Economy and Managing Risk Through Infrastructure Investment

by David Vaughan and Jeff Plumblee

Infrastructure as a Foundation for Basic Needs

Infrastructure is the foundation from which an economy should be built. The American Industrial Revolution and the expanse of the Roman Empire were made possible by solid infrastructure. As economies grow, they become more dependent upon transportation and communication networks, but before they can flourish, the groundwork must be laid to meet basic needs of the people.

This groundwork, outlined by the bottom two levels of Maslow's hierarchy of needs, includes clean water, food, shelter, and other biological, physiological, and safety needs. Basic transportation infrastructure allows goods such as food and clothing to be transported to and from communities, facilitating essential commerce. Water and sanitation infrastructure provides a variety of services, but the underlying goals are to provide potable water and disposal of sanitary and solid waste. These services reduce the prevalence of disease and illness and increase overall quality of life. Medical infrastructure is also crucial to promoting a healthy population.

In developing countries, aid organizations often apply triage medical infrastructure to make a rapid impact, but these medical efforts are designed to treat symptoms of other infrastructure deficiencies. Huge investments in medical missions are sometimes made without a systemic review of the problem. As a result, the underlying problems remain, the status quo is maintained, and the need for aid does not diminish. All areas of infrastructure, including medical, should be pushed forward in lockstep to create lasting, sustainable solutions.

Maslow's Hierarchy of Needs Pyramid

Infrastructure as a Step Towards Economic Prosperity

Once these foundational needs are met and the population can look beyond its immediate needs, focus will tend to shift towards the future. Having secured basic needs, individuals will develop higher-risk, higher-reward entrepreneurial attitudes, creating new and larger economic opportunities. Resources, both human and natural, can only be tapped if the infrastructure is in place to support such efforts.

As development efforts continue to progress, communities begin to create an economic base to support, maintain, and expand upon their infrastructure. Along with these newfound community assets, communities often begin to formalize governance. Communities realize and capitalize upon the capabilities and capacity of their location. Entrepreneurs fill niches based upon community needs and personal and

(Continued on Page 23)

(Continued from Page 22)

circumstantial strengths. They begin to rely less and less on external aid and take ownership of their future. They can also begin to prepare for and mitigate natural disasters, disease outbreaks, droughts, and other potential vulnerabilities.

Infrastructure should be dynamic. As an area grows, its needs change, and its threats and vulnerabilities likewise evolve. It is typically a government's responsibility to ensure that the infrastructure continues to meet the needs of its people, but a reactive approach is not ideal. By proactively planning and implementing infrastructure upgrades, governments can influence economic and societal growth, both in developed and developing regions.

For instance, in the state of Oregon, government officials recognized the need to upgrade Oregon's highway system to "increase safety, improve mobility and facilitate the free movement of goods on which the state's economy depends."[1] The Oregon Transportation Investment Act (OTIA) III State Bridge Delivery Program replaced or repaired 365 bridges at a total cost of over $2.1 billion, and the short-term economic impact of the program is estimated to be over $5.6 billion due to re-spending of funds in the local economy. But more importantly, the infrastructure upgrades avoided projected losses of $123 billion in productivity and 88,000 jobs over the next 25 years. By planning and strategically spending, the government has effectively performed infrastructure upgrades that will pay for themselves through projected tax revenue from future increased economic activity. Unfortunately, it is more common that infrastructure improvements are only funded once on the verge of failure. Significant upgrades are needed throughout the United States in nearly every area of infrastructure, and financial mechanisms are not in place to support the levels of funding needed.[2]

Substandard Infrastructure Creates More Vulnerability Than No Infrastructure

Infrastructure is a key driver in economic and societal development, but codes and standards are critical. In developing regions, codes must be both adopted and enforced. In developed regions, current codes should regularly be reviewed for adequacy against current threat conditions, and infrastructure components should be assessed for current code compliance to identify underlying vulnerabilities. Without proper standards in place (and proper enforcement), substandard infrastructure can give a false sense of security. As infrastructure improves and becomes more reliable, society becomes more dependent on infrastructure. For example, as U.S. highway systems have grown and improved, trucks have become larger and heavier, pushing the capacity constraints of transportation networks. But if these networks fail, the country is worse off than if it had never depended upon them. In the case of the developing world, an unreliable water treatment system can cause even worse problems. If a community believes that a water treatment system has rendered their water safe to drink, they no longer take the safeguards that they once took (boiling water, point of use chlorination, etc.). If the system fails to function properly and the water is contaminated, community members are at risk from waterborne illnesses.

Infrastructure developments, both in developed and developing regions, should be designed to withstand foreseeable events, including both natural and man-made hazards. These resilient design considerations increase reliability and decrease economic and social vulnerability. The costs associated with implementing and adhering to sufficient standards are small when compared to the potential losses and vulnerabilities from substandard infrastructure. As demonstrated by the 2010 earthquake in Haiti, without adequate standards and codes in place, poor construction techniques are prevalent and the population suffers consequently.

Infrastructure is a Double Edged Sword

Whether in the developing world or the developed world, infrastructure is one of society's greatest enablers, but it is also one of its greatest vulnerabilities. Investments in infrastructure often pay for themselves

(Continued on Page 24)

[1] Oregon.gov, *Oregon Transportation Investment Act (*OTIA) III State Bridge Delivery Program, available at http://www.oregon.gov/odot/hwy/otia/pages/bridge_delivery.aspx.

[2] American Society of Civil Engineers, *2013 Report Card for America's Infrastructure*, available at http://www.infrastructurereportcard.org/.

(Continued from Page 236765t

over a relatively short time horizon, but the infrastructure investments must be carefully planned, as these are often long-lived assets. Progressive financial mechanisms, such as public-private partnerships, can help fund infrastructure construction and maintenance. Additionally, one must realize that society can quickly become dependent upon infrastructure, creating new vulnerabilities. With this in mind, resilient codes and standards should be in place to ensure that infrastructure investments end up as assets instead of liabilities.

About the Authors

David Vaughn is the Director of Resilience Solutions, and Jeff Plumblee is a Resilience Solutions Specialist at Fluor. Resilience Solutions works with industrial, government, and non governmental clients to prepare for, mitigate, and respond to disasters. For commercial clients, Resilience Solutions offers a full spectrum of pre-event and post-event risk management solutions and comprehensive recovery services. Working with government and NGO clients, Resilience Solutions uses its ENDURE process to offer a systems-based regional or national development strategy through resilient engineering including a framework for process focused, outcome driven accountability. ❖

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 on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1