SAND2010-0572C

Overcoming Challenges in Critical Infrastructure Resilience Analysis: A New Framework for Resilience Assessments

Drake E. Warren, Eric D. Vugrin, and Mark A. Ehlen
Sandia National Laboratories, Albuquerque, NM
dewarre@sandia.gov, edvugri@sandia.gov, maehlen@sandia.gov

Abstract

Under the direction of the U. S. Department of Homeland Security's (DHS's) Science and Technology (S&T) Directorate, Sandia National Laboratories (Sandia) has developed a comprehensive resilience assessment framework for evaluating the resilience of infrastructure and economic systems. This framework includes a definition of system resilience, a quantitative methodology that measures resilience costs, and a qualitative analysis methodology for identifying system characteristics that promote resilience. This framework has two primary advantages for infrastructure and economic resilience analysis. First, the framework is general enough to be applied to all 18 of DHS's critical infrastructure/key resource (CIKR) systems [1]. Second, it explicitly considers recovery costs following infrastructure disruptions. Recovery is a fundamental aspect of resilience, and evaluation of the recovery costs is necessary to provide a comprehensive resilience assessment. To the authors' knowledge, this resilience assessment framework is the first of its kind to address both of these considerations.

1. Introduction

Historically, U.S. government policy toward critical infrastructure protection (CIP) has focused on physical protection and asset hardening (for examples, see [2], [3], [4], and [5]). Recently, the federal government has realized "protection, in isolation, is a brittle strategy" [6] and not all disruptive events, natural or manmade, can be prevented. Hence, national CIP policies must prepare the nation for unavoidable disruptive events.

With the formation of the DHS's Critical Infrastructure Task Force in 2005, this shift in policy become a national priority as the task force made critical infrastructure resilience (CIR) its top-level strategic objective. CIR is the concept concerned with how critical infrastructures absorb, adapt, and recover from the effects of a disruptive event to ensure delivery of critical infrastructure services. To take CIR from an abstract to an actionable concept, several challenges must be overcome.

First, an actionable resilience definition that leads to quantitative resilience measurement methodologies must be agreed upon. There are notable differences of opinion across professional disciplines over the fundamental definition of resilience. These differences often originate from inherent complexities in resilience concepts and how and to which disciplines they are applied; e.g., whether resilience is concerned with deviations from a steady state (engineering resilience) or with changes between completely different states (ecological resilience).

Second, this definition and resulting measurement methods must be general enough to apply to all eighteen of DHS's CIKR systems [1]. Current frameworks are often tailored to a narrow domain, such as those of seismic resilience [7] and economic resilience [8]. Definitions and measurement methods that can be applied to multiple types of infrastructure systems or domains will permit cross-sector resilience comparisons. Furthermore, cross-sector dependencies commonly affect the resilience of infrastructure systems; thus, to comprehensively address the resilience of these systems, a resilience analysis methodology must be able to be applied to multiple, possibly very different, infrastructure systems. Additionally, a general approach will permit the development of resilience standards that can be broadly applied to all critical infrastructure systems.

Third, there has been much discussion of "all-hazards resilience." To evaluate the resilience of a system to multiple hazards, resilience definitions and methods must consider multiple methods.

Fourth, resilience assessment methods should not assume that disrupted infrastructure systems return to a pre-disruption state. Owners of severely degraded infrastructure systems may choose to take advantage of insurance payments to make capital investments to improve the system beyond its original state. Or, they may choose to fundamentally change the system from its pre-disruption state due to new market conditions.

Last, the costs associated with recovery processes and resilience enhancing strategies must be considered in resilience assessments. Current resilience evaluation methods tend to focus on the loss of system productivity due to infrastructure disruptions, but they tend to ignore the cost of resources expended during recovery efforts [9]. Ignoring this factor is a shortcoming of current resilience methods because infrastructure and business owners must balance business losses with recovery costs following disruptive events.

No existing resilience evaluation approaches currently address each of these challenges. To overcome these limitations, the DHS S&T Directorate tasked Sandia to develop a resilience methodology to address these challenges. This paper outlines Sandia's new resilience assessment framework for critical infrastructure and economic systems.

2. A Definition of System Resilience

A review of many definitions of resilience is included in [9]. These previous definitions all include some aspect of withstanding change, whether by reducing the impact of the change, adapting to the change, or recovering from the change. Many of them assert that one aspect is the speed of the recovery and, for national infrastructure and economic systems, this speed is important; a recovery that takes hours is better than one that takes weeks, all else being equal. Only a few of these definitions assert that adjusting easily to the change is important. In the case of homeland security policy, if a disrupted critical infrastructure system can adjust easily and essentially on its own, fewer resources (time and money) need to be committed to the recovery process, and the overall loss of service is lessened as well.

Sandia has developed a novel framework for evaluating the resilience of infrastructure and economic systems [9]. The framework includes a new definition of resilience, a mathematical resilience cost measurement approach, and a qualitative analysis methodology that assesses system characteristics that affect resilience. This framework can be applied to studies of natural and manmade disruptions. The following sections describe the three components of the resilience assessment framework in detail.

We propose to define *system resilience* as follows:

> *Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels.*

The following discussion clarifies subtleties of the definition:

Disruptive event: This definition considers resilience of a system in the context of a specific disruption. That is, one should analyze the resilience of that system to a particular disruption because different disruptions may affect a system in different ways and, thus, necessitate different recovery processes. Hence, a system may have different levels of resilience to different disruptions.

Multiple infrastructures: The definition is general enough to apply to multiple infrastructure systems. Different systems will use different units of analysis to measure terms like "system performance" and "efficiency."

Systems focus: The definition is generally applicable to infrastructure and economic systems; that is, sets of related and often interconnected entities that form a whole. Engineered systems—such as infrastructure systems—have a precise, collective, measurable purpose.

Efficiency: The term "efficiency" refers to the value of resources and how those resources are used for recovery. Depending on the domain under consideration, these resources could be dollars, repair man-hours, infrastructure replacement assets, or time. The definition acknowledges that multiple recovery strategy options exist and the costs of those options vary. Generally, the more resilient systems will use the more cost-efficient recovery options. By defining efficiency in terms of resource utilization, the definition of resilience has the broadest domain application and the framework can be easily applied in other analytical areas, such as consequence, risk, benefit-cost, and policy analyses.

Recovery (post-disruption actions): Recovery actions take place after the initial shock to the system and are primarily intended to increase system performance. Recovery may be enhanced by preparatory actions. Recovery may occur by way of the system's internal mechanisms or by the mechanisms provided by external entities (e.g., government entities). The efficiency of the recovery considers recovery actions by both internal and external mechanisms. A system that can recover within its own means will generally be more resilient than one that requires external help.

System performance: Given the flexibility of many systems to adjust and reconfigure to a disruptive event, maintaining system structure is not as important as maintaining system performance. Hence, measurement of resilience should evaluate how a disruption affects system performance and causes productivity to decrease relative to targeted system performance levels.

Targeted system performance: Disruptions to system performance are measured in terms of the deviation of actual performance levels from targeted performance levels. The phrase "targeted performance level" refers to a system output level that is reasonable and acceptable following a disruptive event. In general, this level does not necessarily refer to the pre-disturbance level. It may vary according to the disruption type and change over time. This performance level provides a reference point for comparing actual system performance.

This definition of system resilience presents several challenges to an analyst. By overcoming these challenges during a resilience assessment, an analyst will develop a more complete understanding of a system's structure, performance, and resilience.

3. Calculation of resilience costs

To quantitatively evaluate resilience, Sandia has developed a mathematical resilience costs measurement approach that can be used to objectively determine the impacts of disruptions on a system and the resilience costs associated with disruptions. The resilience cost measurement approach requires quantification of two key components of the definition of system resilience: systemic impact (*SI*) and total recovery effort (*TRE*).

SI is the impact that a disruption has on system productivity and is measured by evaluating the difference between a targeted system performance (*TSP*) level and the actual system performance (*SP*) following the disruption. Fig. 1 graphically represents *SI* for a hypothetical system that has been disrupted. In this example, *SP* decreases immediately following the disruption shock. With the onset of recovery actions, performance levels eventually increase and ultimately attain *TSP*. At this point, recovery is considered complete. *SI* is quantified by calculating the area between the *TSP* and the actual *SP* curves in Fig. 1. This area is calculated using the formula in (1).

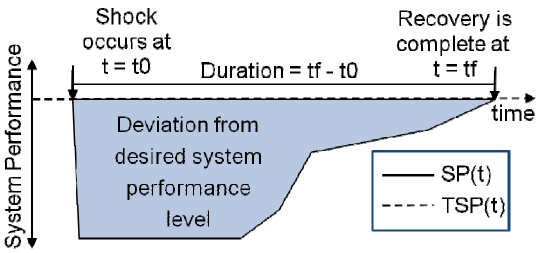

Figure 1: Systemic Impact

$$SI = \int_{t0}^{tf} [TSP(t) - SP(t)]dt \qquad (1)$$

TRE refers to the efficiency with which the system recovers from a disruption and is measured by analyzing the amount of resources expended during the recovery process. Fig. 2 illustrates the recovery response for the system shown in Fig. 1. After the disruption initiates, the recovery response begins and resources are expended in this effort. The *TRE* is the cumulative amount of resources expended during the recovery period and is represented by the area under the recovery effort (*RE*) curve in Fig. 2. This area is calculated by (2).

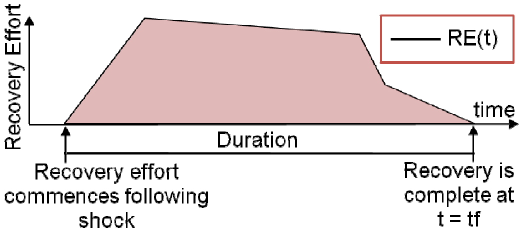

Figure 2: Total Recovery Effort

$$TRE = \int_{t0}^{tf} [RE(t)]dt \qquad (2)$$

The measurement of system resilience costs requires the quantification of both *SI* and *TRE* because *SP* is determined by the *RE*. That is, different *RE*s lead to different *SP*s. For example, if no *RE* is made following the disruption, the loss of *SP* may be great. In contrast, if recovery resources are deployed shortly after the system shock, *SP* may not be significantly affected, and *SI* may be small. The recognition that *SI* is implicitly determined by the selected recovery strategy leads to the development of two types of resilience cost measurements: optimal resilience (*OR*) costs and recovery-dependent resilience (*RDR*) costs. *OR* costs are the resilience costs for a system when the optimal recovery strategy, minimizing the combined *SI* and *TRE* costs, is employed. *RDR* costs are the resilience costs of a system under a particular recovery strategy and are calculated with (3). *OR* costs are simply the minimal *RDR* costs over all possible recovery strategies.

$$RDR(RE) = \frac{SI + \alpha \times TRE}{\int_{t0}^{tf} \left| TSP(t) \right| dt} \qquad (3)$$

RDR costs are linear combinations of *SI* and *TRE*. The denominators in (3) are normalization factors that permit the comparison of the resilience of systems of different magnitudes. Because resilience represents a balancing of *SI* and *TRE* costs, the calculation of *RDR* costs includes the parameter α, which is a weighting factor that allows an analyst to assign the relative importance of the *SI* and *TRE* terms. Assigning a small positive value to α weighs the *SI* more heavily; a large positive value for α weighs the cost of recovery more heavily. To equally weigh *SI* and *TRE*, α is set to 1.

Sandia's resilience cost measurement approach is similar to previous resilience measurement approaches in that it accounts for decreased system productivity; that is, *SI*. Sandia's approach has some fundamental differences from previous methods reviewed in [9]. Most notably, it is the only approach discussed that explicitly considers the costs associated with the expenditure of resources during recovery processes; that is, *TRE*.

4. Qualitative resilience analysis

Joseph Fiksel [10] suggests that "it is important to assess not only performance outcomes but also the intrinsic characteristics that contribute to system resilience." Consequently, Sandia's resilience assessment framework features a qualitative analysis component that can be used to explain the results of quantitative measurements, suggest ways of improving resilience to future disruptions, or take the place of quantitative results when no data are available. This analysis is done through consideration of system structures, characteristics, and features.

This portion of the framework uses three fundamental system capacities (*absorptive capacity, adaptive capacity, and restorative capacity*) to formulate how properties of a system can determine system resilience, specifically by reducing *SI* and *TRE*. (These capacities are similar to the abilities to "absorb, recover from, or successfully adapt to adversity or a change in conditions" in the official DHS definition of resilience [11], but do not include that definition's ability to resist a threat.)

These capacities are affected by resilience enhancement features; that is, the features of the system that are in place before a disruption and that affect one or more of the system's capacities. Identifying resilience enhancement features enables a better understanding of fundamental characteristics that contribute to resilience. Most importantly, pre-disruption preparatory actions can target these resilience enhancement features to increase the resilience of the system.

Absorptive capacity is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort. For example, storage can enhance the absorptive capacity; if a manufacturing plant is disabled, but a large amount of storage of its product is undamaged, customers can continue to be supplied by the stored quantities, with little cost to the producer or customer, while the plant is repaired. Other examples of resilience enhancement features that increase this capacity include system robustness and redundancy.

Adaptive capacity is the degree to which the system is capable of self-organization for recovery of system performance levels. It is a set of properties that reflect actions that result from ingenuity or extra effort over time, often in response to a crisis situation. It reflects the ability of the system to change endogenously during the recovery period. Substitutability, the ability to replace one system component or input with another, is a resilience enhancement feature that can increase adaptive capacity. Other resilience enhancement features that increase adaptive capacity tend to be more difficult to identify because they often rely upon the ingenuity of people faced with adversity.

Restorative capacity is the ability of a system to be repaired easily. These repairs usually restore the system to near its original pre-event state, but can also restore the system to a completely new state or regime that anticipates future system requirements. Therefore, the repairs are a form of investment. Following massive catastrophic events, systems may not be able to repair themselves or they may not be able to do so rapidly enough to prevent unacceptably large consequences. In these circumstances, repairs may be performed or enabled by entities external to the system such as the government. Government agencies may not directly perform the repairs, but may serve as lead restoration planners or restoration planning coordinators. Restorative capacity directly affects the *TRE*, although repairs to the system enabled by the system's restorative capacity also increase system performance and may reduce recovery duration, thereby reducing *SI*. For example, the electric power grid has monitoring systems that can automatically detect when and where a break in the grid emerges. Such technologies enhance the restorative capacity of the power grid because repair crews can quickly be sent to the location of the break.

5. Summary

The resilience assessment framework presented herein addresses many of the challenges that must be overcome before institutionalizing CIR in CIP policies. The framework contains a new definition that is broad enough to be applied to all CIKR systems and infrastructure hazards. It explicitly considers the costs associated with recovery processes and does not assume that disrupted systems necessarily return to pre-disruption states. Most importantly, the definition provides for quantitative and qualitative means for evaluating resilience and resilience costs.

However, even under this framework, challenges remain that must be overcome. First, because the framework is fairly general and broadly applicable, application of the framework requires that the scope of the system and resilience must be clearly defined at the beginning of the analysis. Questions that need to be addressed before starting resilience analyses include: what are the boundaries of the system being considered, what dependencies are being considered, what are appropriate system performance and recovery metrics, how should targeted system performance levels be selected, and when is recovery considered "complete." By answering these questions, a resilience analyst gains a greater understanding of the system.

Furthermore, this framework considers resilience in a contextual manner. That is, the framework can be used to draw conclusions such as "System X is more resilient than System Y to disruption Z." It does not allow one to conclude "System X is resilient."

Finally, the inclusion of recovery costs and the concept of efficiency require a more sophisticated mathematical approach for measuring resilience costs. The field of optimal control provides some promise for developing more rigorous mathematical approaches [9], but additional research must be employed to understand how theoretical constraints (e.g., linearity of systems) limit the application of optimal control techniques for resilience analyses.

6. Acknowledgements

The authors would like to thank Adam Rose and Tony Barrett from the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) for the thoughtful insights that they provided.

The authors performed this work with funding from the DHS Science and Technology Directorate.

Sandia is a multiprogram laboratory operated by Sandia Corporation for the Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

7. References

[1] U.S Department of Homeland Security, "Infrastructure Protection Plan: Partnering to enhance protection and resiliency," 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf; and "Sector-Specific Plans," http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm

[2] Reagan, Ronald, "Executive Order 13282, National Security Telecommunications Advisory Committee," 1982

[3] Clinton, William, "Presidential Directive PDD-63, Protecting America's Critical Infrastructures," 1998

[4] Bush, George W., "Homeland Security Presidential Directive 3 (HSPD-3)," 2002

[5] Bush, George W., "Homeland Security Presidential Directive 7 (HSPD-7)," 2003

[6] "Infrastructure Resilience Requires All Hazards Plan, Panel Advises DHS," *Emergency Preparedness News*, March 21, 2006

[7] Bruneau, Michel, Stephanie E. Chang, Ronald T. Eguchi, George C. Lee, Thomas D. O'Rourke, Andrei M. Reinhorn, Masanobu Shinozuka, Kathleen Tierney, William A. Wallace, and Detlof von Winterfeldt, 2003. "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra* 19(4), pp. 737-38

[8] Rose, Adam, 2007. "Economic Resilience to Natural and Man-Made Disasters; Multidisciplinary Origins and Contextual Dimensions," *Environmental Hazards* 7(4), pp. 383-398

[9] Vugrin, Eric D., Drake E. Warren, Mark A. Ehlen, and R. Chris Camphouse, "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," in *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, Kasthurirangan Gopalakrishnan and Srinivas Peeta, eds., Springer-Verlag, Inc., forthcoming, May 2010

[10] Fiksel, Joseph, "Designing Resilient, Sustainable Systems," *Environmental Science and Technology*, 37(23), pp. 5330-5339, 2010

[11] U.S. Department of Homeland Security Risk Steering Committee, *DHS Risk Lexicon*, 2008