Domestic Preparedness Journal, Aug. 19, 2015.

Screening Risk Analysis Tools for Resilience of Critical Infrastructure & Regions

by JERRY P. BRASHEAR & PAULA SCALINGI

Resilience, a central element in any recovery, is established before potentially disastrous events. Twenty-one federally sponsored risk methods and tools were screened for possible use as the core of a defensible, repeatable risk/resilience management process that would capture the greatest benefits for available budgets. None was fully ready for this role, but several hold promise for further improvement.

One of the most effective strategies for dealing with disaster is resilience – being able to withstand threats and hazards while continuing to function or, if discontinuity is unavoidable, restoring operations with minimal service outage. Although resilience is observed during and immediately after potentially disastrous events, it is created *before* the events based on assessing risk, planning, and performance assessment. The resilience of communities across the country depends on the resilience of the interdependent lifeline infrastructures that support them – energy, water/wastewater, transportation, communications – and other essential services, as well as local government emergency response and recovery functions. Consequently, decisions by operators, managers, and oversight boards of these infrastructures largely determine the nation's level of resilience. At the same time, the rigorous regional risk assessment process to enable these decisions is lacking. Developing such an effective process for risk and resilience remains a key goal.

The federal government has issued a number of policies, plans, methods, tools, and incentives to assist in making resilience decisions. Presidential Policy Directives 8 (National Preparedness) and 21 (Critical Infrastructure Security and Resilience) emphasize the central role of critical infrastructure systems, state and local governments, and regional public-private partnerships in advancing the national goals of critical infrastructure security and resilience, especially at the regional scale.

The Business Process Engineering Risk Management Project

The National Institute of Building Sciences undertook a project for the U.S. Department of Homeland Security Office of Infrastructure Protection to assist in operationalizing the risk and resilience analysis framework outlined in the 2013 National Infrastructure Protection Plan (NIPP 2013) into a conventional business process – critical infrastructure security and resilience risk management process that could be used at the grassroots level. The project used business process engineering to extend that framework into a workable, scalable, repeatable, defensible, and practical process that lifeline critical infrastructures, local governments, and public-private partnerships can use collaboratively to determine the allocation of constrained resources for security and resilience. The process, importantly, incorporates assessing risk related to infrastructure interdependencies. This article focuses on one key task of this larger project (the final report of which is available at NIBS.org).

Screening Approach

The key task was a screening of certain federally sponsored methods, processes, and tools for lifelines and other critical infrastructures to determine whether any provided a fully defensible method that could be used or could serve as a point of departure for an improved risk management process. A central criterion for a risk analysis process is *defensibility*. According to the methodological supplement to NIPP 2013, the process "must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as free from significant errors or omissions."

Defensibility is not simply a narrow academic consideration. Risk management has evolved to its current state by demonstrating that certain practices contribute more to maximizing benefits under constraints than any alternative. Any method that could materially distort this decision-making process is likely to result in inefficient and poor choices. This is especially important in making choices about which resilience options to include in budgets and plans – how to allocate scarce resources to yield the greatest net benefits under practical constraints.

To identify candidate tools for use or adaptation for a critical infrastructure security and resilience risk management process, the project team met with federal agencies with lifeline infrastructure responsibility. Only federally sponsored tools were considered because they potentially can be acquired and modified by the federal government, whereas privately developed tools entail additional costs, proprietary rights, and control issues. Altogether, the team identified and screened 21 tools.

Screening Results

Of the 21 tools, three estimate important elements in risk analysis – for example, economic consequences or future weather – but do not actually estimate risk or benefits. These were set aside. Such tools can materially contribute to risk analyses, but only to complement a true risk tool. Seven more tools were detailed surveys that produce index scores that benchmark an organization against others. Although these tools can identify areas of potential concern and suggest options for improving security and/or resilience, they do not measure risks, expected outages, consequences, or mitigation benefits – information necessary for cost-effective resource allocation decisions. These tools were not further assessed for the project.

The remaining 11 federally sponsored risk tools for lifeline infrastructures, shown in the table, attempt to estimate risk and support risk-mitigation decisions. *Key decisions* (Column A) are the major decisions required for rationally managing resources to achieve the greatest net benefit to both the infrastructure owners and the communities they serve. These decisions require specific *Process outputs* (Column B), which, in turn require systematic, repeatable, defensible estimation of the listed *Constituent Terms* (Column C). Logical consistency of process (not necessarily identical processes) and directly comparable results are crucial for allocating resources across divisions of large, diverse corporations or governments for analyzing interdependencies among CIs and for aggregating to organizational totals at regional and higher levels for accountability and governance. In addition to the logical consistency of the analytical processes, comparability requires a standardization of the initial set of threat/hazard scenarios (Column D). The "design objectives" row (in red) characterizes the desired process.

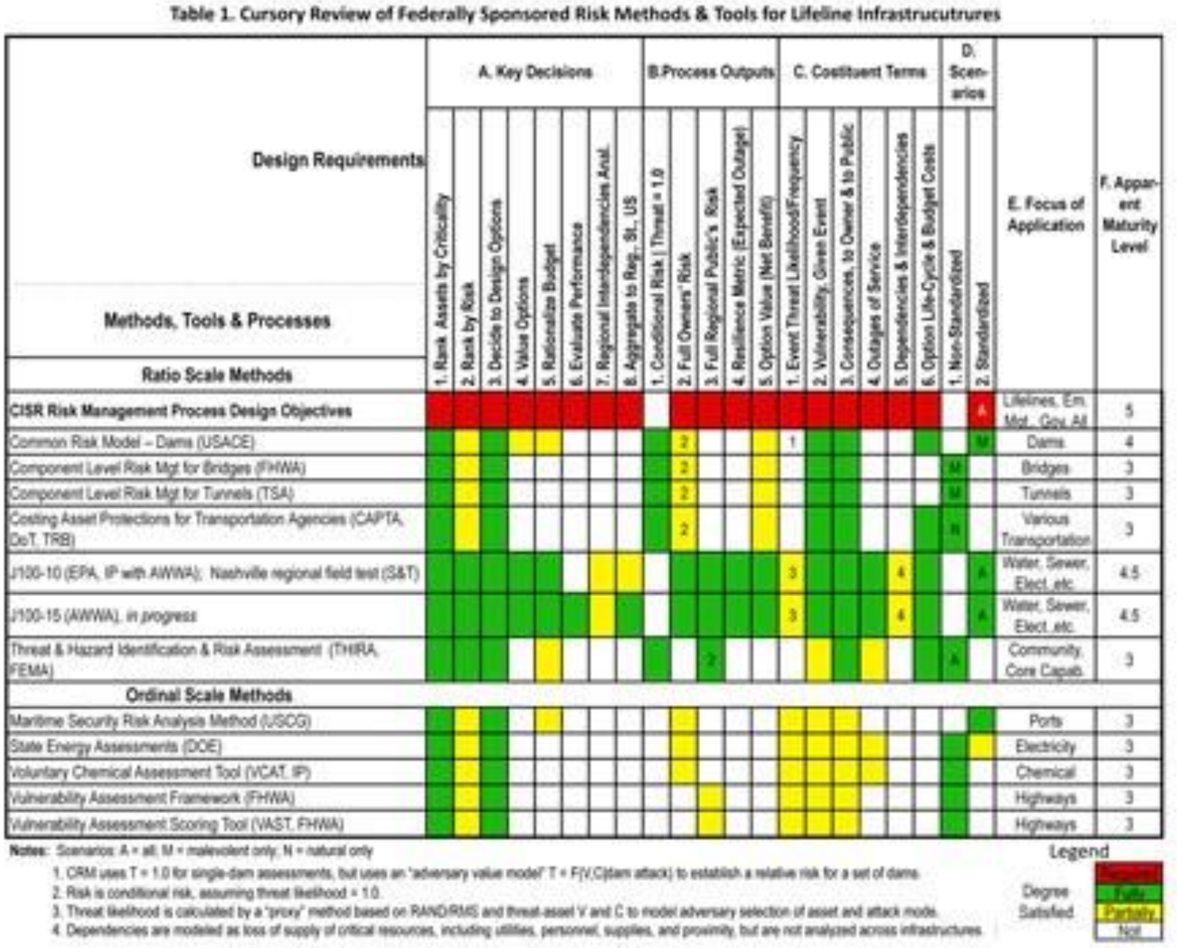

Table 1. Cursory Review of Federally Sponsored Risk Methods & Tools for Lifeline Infrastrucutrures

Design Requirements	A. Key Decisions								B.Process Outputs					C. Costituent Terms						D. Scen-arios		E. Focus of Application	F. Appar-ent Maturity Level
Methods, Tools & Processes	1. Rank Assets by Criticality	2. Rank by Risk	3. Decide to Design Options	4. Value Options	5. Rationalize Budget	6. Evaluate Performance	7. Regional Interdependencies Anal.	8. Aggregate to Reg., St., US	1. Conditional Risk | Threat = 1.0	2. Full Owners' Risk	3. Full Regional Public's Risk	4. Resilience Metric (Expected Outage)	5. Option Value (Net Benefit)	1. Event Threat Likelihood/Frequency	2. Vulnerability, Given Event	3. Consequences, to Owner & to Public	4. Outages of Service	5. Dependencies & Interdependencies	6. Option Life-Cycle & Budget Costs	1. Non-Standardized	2. Standardized		
Ratio Scale Methods																							
CISR Risk Management Process Design Objectives	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥		🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥		🟥 A	Lifelines, Em. Mgt., Gov. All	5
Common Risk Model – Dams (USACE)	🟩	🟨	🟩	🟨	🟨				🟩	🟨 2			🟨	1	🟩	🟩			🟩		🟩 M	Dams	4
Component Level Risk Mgt for Bridges (FHWA)	🟩	🟨	🟩						🟩	🟨 2			🟨		🟩	🟩				🟩 M		Bridges	3
Component Level Risk Mgt for Tunnels (TSA)	🟩	🟨	🟩						🟩	🟨 2			🟨		🟩	🟩				🟩 M		Tunnels	3
Costing Asset Protections for Transportation Agencies (CAPTA, DoT, TRB)	🟩	🟨	🟩						🟩	🟨 2			🟨		🟩	🟩			🟩	🟩 N		Various Transportation	3
J100-10 (EPA, IP with AWWA); Nashville regional field test (S&T)	🟩	🟩	🟩	🟩	🟩		🟨	🟨		🟩	🟩	🟩	🟩	🟨 3	🟩	🟩	🟩	🟨 4	🟩		🟩 A	Water, Sewer, Elect. etc.	4.5
J100-15 (AWWA), *in progress*	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩		🟩	🟩	🟩	🟩	🟨 3	🟩	🟩	🟩	🟨 4	🟩		🟩 A	Water, Sewer, Elect. etc.	4.5
Threat & Hazard Identification & Risk Assessment (THIRA, FEMA)	🟩	🟩	🟩		🟨				🟩		🟩 2				🟨	🟩	🟨		🟩	🟩 A		Community, Core Capab.	3
Ordinal Scale Methods																							
Maritime Security Risk Analysis Method (USCG)	🟩	🟨	🟩		🟨					🟨				🟨	🟨	🟨					🟩	Ports	3
State Energy Assessments (DOE)	🟩	🟨	🟩							🟨				🟨	🟨	🟨	🟨			🟩	🟨	Electricity	3
Voluntary Chemical Assessment Tool (VCAT, IP)	🟩	🟨	🟩							🟨				🟨	🟨	🟨	🟨			🟩		Chemical	3
Vulnerability Assessment Framework (FHWA)	🟩	🟨	🟩								🟨			🟨	🟨	🟨				🟩		Highways	3
Vulnerability Assessment Scoring Tool (VAST, FHWA)	🟩	🟨	🟩								🟨			🟨	🟨	🟨				🟩		Highways	3

Notes: Scenarios: A = all; M = malevolent only; N = natural only

1. CRM uses T = 1.0 for single-dam assessments, but uses an "adversary value model" T = F(V,C|dam attack) to establish a relative risk for a set of dams.
2. Risk is conditional risk, assuming threat likelihood = 1.0.
3. Threat likelihood is calculated by a "proxy" method based on RAND/RMS and threat-asset V and C to model adversary selection of asset and attack mode.
4. Dependencies are modeled as loss of supply of critical resources, including utilities, personnel, supplies, and proximity, but are not analyzed across infrastructures.

Legend	
Degree Satisfied	🟥 Required
	🟩 Fully
	🟨 Partially
	Not

The five tools shown in the lower portion of the table estimate elements of the risk equation but rely on *ordinal scales* of measurement (e.g., low-medium-high-very high; green-yellow-red; 1-to-5 or 1-to-10 scales or even finer gradations), so they run a serious risk of distorting resource allocation decision-making. Ordinal scales have neither equal intervals nor a true zero (absence of the quantity) and necessarily have open ended "greater than" categories for consequences and "less than" for threat likelihoods, both of which may vary over hundreds, thousands, even millions of times. These limitations make estimating risk levels and benefits of options mathematically impossible, so these tools cannot support rational resource allocation – although many advocates have tried. Such scales, however, provide evidence of risk-oriented thinking among their users. Such tools might be able to be evolved into effective risk methods by changing the scales used.

The remaining six tools, shown at the top of the table, estimate the terms of the risk equation using *ratio scales* (equal distances between numbers and a true zero – things that can be counted). However, five of the six use conditional risk (assuming the likelihood of unwanted events to be 1.0, or certainty). This unavoidably distorts key decisions, because the likelihood of a terrorist attack on a specific asset or subsystem in a given location is several orders of magnitude smaller than the likelihood of other hazards – for example, weather events. Any of these six tools could readily be upgraded to demonstrate full risk by providing the missing terrorism threat likelihood.

The exception to using conditional risk is provided by the standard *ANSI/AWWA J100-10: Risk and Resilience Management of Water and Wastewater Systems*, which the American Water Works Association first released in 2010 and is currently updating it to be released as ANSI/AWWA J100-15. Although the earlier version permitted use of ordinal scales (in the form of pre-set ranges) and conditional risk, neither will remain in the updated version because of the shortcomings just described. Both versions provide a "proxy" method for approximating terrorist threat based on the notion of the terrorist selecting a target and attack mode. It is referred to as the "proxy" method because it stands *in lieu* of a true likelihood estimate. The proxy method is a placeholder until an authoritative threat likelihood measure is available. The method adapts a study of actual terrorist attacks conducted by the RAND Corporation and Risk Management Solutions Inc., and local conditions to estimate likelihood. The six ratio-scale tools use roughly comparable concepts and definitions of conditional risk, vulnerability, and consequences. All six tools measure risk from the perspective of critical infrastructure owners, as opposed to the public (J100-10 does both). Three of the tools apply only to terrorist or malevolent threats, one deals only with natural hazards associated with climate change, and the remaining two – THIRA and J100 (both editions) – use an all-hazards approach. The similarities are sufficient to conclude that THIRA and J100 could either be converted to a common approach (perhaps with tailored versions to apply to specific sectors) or made comparable enough to analyze regional risk and resilience of interdependent lifelines and other critical infrastructures and to support aggregation to organizational, jurisdictional, regional, state, and national levels. The last column of the table summarizes each tool's maturity level based on the model used by the U.S. Department of Defense and other agencies, including elements of the Department of Homeland Security. The scale ranges from 1 (*ad hoc*, beginning, undocumented); through 2 (repeatable); 3 (defined enough to be a standard business process); 4 (managed through quantitative metrics); to 5 (optimizing choices and self- improvement). None of the tools relying on conditional risk can reach level 5 because conditional risk cannot be used to calculate benefits. By defining and using a crude approximation of terrorist threat likelihood, J100-10, can support constrained optimization, but lacks full, cross-infrastructure collaborative treatment of interdependencies, so it was assigned a 4.5. THIRA is the primary tool for the National Preparedness Program under Presidential Policy Directive 8. All states and the 28 highest risk metropolitan regions currently participating in the Urban Areas Security Initiative program use THIRA, as required to qualify for FEMA grants. To date, though, its application has been limited to 13 response and selected recovery core capabilities out of the total of 31 defined core capabilities. The 2013 National Infrastructure Protection Plan calls for THIRA to be "employed" for critical infrastructures but, as this analysis suggests, it could distort decisions because it uses conditional risk and broadly specified methods. THIRA would need to be refined in the direction of J100-15 if it is to be effective for resource allocation decisions for critical infrastructure risk management.

J100-10 and J100-15 demonstrably support resource allocation for one of the lifeline infrastructures, having been applied to more than 100 water and wastewater systems, including some of the nation's largest: Chicago, Illinois; the National Capital Region (three systems); Richmond, Virginia; Long Beach, California; and Minneapolis, Minnesota. It also has been used effectively in electricity and highway systems, emergency communications and dispatch, fire suppression, emergency medical services, and police emergency operations. J100 is the only tool that uses a ratio-scale measure of resilience.

Federally sponsored tools reflect federal concerns and focus on lifeline sectors predominantly operated by local public agencies – specifically water/wastewater, dams, and highways. In sectors that are predominantly operated in the private sector, such as energy and telecommunications, the project team found no comparable, widely used tools. Companies in these sectors use a wide variety of self-generated and proprietary tools applied by in-house teams or expert consultants, so it will be necessary to explore possible comparability or sharing of tools and/or information region by region. This will require a regional, collaborative approach tailored to the threats and hazards facing the communities in that region and the supporting lifelines and critical infrastructures.

Path Forward on Assessing Infrastructure & Regional Risk

None of the federally sponsored tools examined meet all the design objectives. However, several are similar and defensible enough to be adapted for rational program choices, accounting for interdependencies, at infrastructure, regional, and higher levels. The project, in which this tool screening was part, goes further to describe in detail an integrated infrastructure-region-state-nation risk management process based on a broad synthesis of these tools, first principles of the risk disciplines, and the preferences and constraints of actual decision-makers.

The federal government will need to provide an authoritative means of estimating malevolent threat likelihood for any of the methods to be fully effective. Interdependencies analysis will require protocols for cross-organization information sharing/protection enabled by regional public-private collaboration. Innovative, "bottom-up" implementation of fully defensible methods may allow more complete integration with other, ongoing business processes – for example, asset management, continuity planning, development planning, and budgeting – to encourage risk/resilience management to become as routine as budgeting. Finally, any new or synthesized approach should be launched with the commitment to continue long enough for the process to mature through field experience, systematically reviewed and iteratively enhanced. The project of which this analysis is part advances such a path forward.

Jerry P. Brashear, Ph.D., *is the managing director of The Brashear Group LLC. He is a researcher and consultant on infrastructure risk/resilience policy, analysis, and management processes. He has led risk consulting and R&D programs at ICF Consulting, The University of Texas at Austin, George Mason University, the American Society of Mechanical Engineers, and The Brashear Group LLC to advance the practice of infrastructure and regional risk/resilience analytic methods and processes. He consults to senior management in infrastructure and homeland security agencies and on infrastructure services at all levels in the United States and internationally. He holds degrees from Princeton, the Harvard Business School, and the University of Michigan.*

Paula Scalingi, Ph.D. *is president of The Scalingi Group, LLC; executive director, Bay Area Center for Regional Disaster Resilience; adjunct associate professor, Georgetown University; and 1st vice chair, The Infrastructure Security Partnership (TISP). A well-known expert on infrastructure interdependencies and principal author of the TISP Regional Disaster Resilience Guide, she works nationwide to further regional and community resilience. Her 37 years' experience includes: director, Center for Regional Disaster Resilience for the Pacific Northwest Economic Region; director, U.S. Department of Energy Office of Critical Infrastructure Protection; director for both the Decision and Information Sciences Division and Infrastructure Assurance Center at Argonne National Laboratory; staff member, U.S. House of Representatives Permanent Select Committee on Intelligence; and analyst, Central Intelligence Agency.*

Additional contributions for this article were made by:

Ryan M. Colker *is Director of the Consultative Council and Presidential Advisor at the National Institute of Building Sciences where he is responsible for leading the development of findings and recommendations on behalf of the entire building community and transmitting those recommendations to Congress and the Administration. Prior to joining the Institute, he served as Manager of Government Affairs for the American Society of Heating, Refrigerating and Air-conditioning Engineers (ASH AE) where he contributed to the development of a robust government affairs program.*