ANL/DIS-10-9

Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program

Decision and Information Sciences Division

ANL/DIS-10-9

Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program

by
R.E. Fisher, G.W. Bassett, W.A. Buehring, M.J. Collins, D.C. Dickinson, L.K. Eaton,
R.A. Haffenden, N.E. Hussar, M.S. Klett, M.A. Lawlor, D.J. Miller, F.D. Petit, S.M. Peyton,
K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom
Decision and Information Sciences Division, Argonne National Laboratory

August 2010

CONTENTS

TABLES

FIGURES

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contributions of many people who helped bring this project to its current state of development, including the Protective Security Coordination Division management team of the U.S. Department of Homeland Security, Office of Infrastructure Protection. The authors are particularly thankful to Mike Norman, Donald Erskine, Derek Matthews, Kariann McAlister, and Sean McAraw, without whom all of this work would not have been possible. Their leadership and dedication inspired the Argonne National Laboratory team.

The authors also want to thank Glen Sachtleben, Duane Verner, Jeffrey Murray, Stan Hanzel, Michael Morral, John Busch, Robert Mooney, and Edward Buikema and their Argonne colleagues who contributed to the methodology and weighting process.

NOTATION

CIKR	critical infrastructure and key resources
DHS	U.S. Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection (program)
NIAC	National Infrastructure Advisory Council
PMI	protective measures index
PSA	protective security advisor
RI	resilience index
QA	quality assurance
VI	vulnerability index

CONSTRUCTING A RESILIENCE INDEX FOR THE ENHANCED CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

R.E. Fisher, G.W. Bassett, W.A. Buehring, M.J. Collins, D.C. Dickinson, L.K. Eaton, R.A. Haffenden, N.E. Hussar, M.S. Klett, M.A. Lawlor, D.J. Miller, F.D. Petit, S.M. Peyton, K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom

EXECUTIVE SUMMARY

In 2009, the U.S. Department of Homeland Security (DHS) and its protective security advisors began assessing high-risk critical infrastructure and key resource (CIKR) assets using a targeted questionnaire: the infrastructure survey tool. The survey tool produced individual protective measure and vulnerability values through protective measure and vulnerability indices (PMI/VI). As sites continue to be assessed using the PMI/VI, academic research, practitioner emphasis, and public policy formation have increasingly focused on resilience as a necessary component of risk management and infrastructure protection. This increased attention led to a detailed study and report by the National Infrastructure Advisory Council, which called for an increased focus on resilience for U.S. infrastructure protection programs (NIAC 2009). The report also underlined the importance of an increased understanding of resilience to an overall risk management strategy for both public and private CIKR.

Enhancing the resilience of critical infrastructures requires their owners/operators to determine the ability of the system to withstand specific threats and to return to normal operations after degradation. Thus, a resilience methodology requires comprehensive consideration of all parts of critical infrastructure systems — from threats to consequences. The methodology must generate reproducible results that can support decision making in risk management, disaster response, and business continuity.

Considering these issues, Argonne National Laboratory, in collaboration with the DHS Protective Security Coordination Division, has developed a comprehensive methodology that uses uniform and consistent data to develop a resilience index (RI) on the basis of data collected through a modified version of the DHS Enhanced Critical Infrastructure Protection (ECIP) program. The RI is derived from three categories: robustness, resourcefulness, and recovery.

The RI ranges from 0 (low resilience) to 100 (high resilience). A high RI does not mean that a specific event will not affect the facility and will not cause severe consequences. Conversely, a low RI does not mean that a disruptive event will automatically lead to a failure of the critical infrastructure and to serious consequences. The RI instead compares the level of resilience at critical infrastructures and guides prioritization of limited resources for improving resilience. The RI also provides valuable information to owners/operators about their facility's standing relative to those of similar sector assets and about ways they can increase resilience.

Applications and uses of the RI for the ECIP program continue to evolve. Concept improvements and additional enhancements and approaches are expected as the program

matures. In addition, the RI will be combined with other indices such as the vulnerability index, the protective measures index, and the forthcoming criticality index to support overall decision making about risk, protection, business continuity, and emergency management of CIKR.

1 INTRODUCTION

Following recommendations made in Homeland Security Presidential Directive 7, which established a national policy for the identification and increased protection of critical infrastructure and key resources (CIKR) by Federal departments and agencies, the U.S. Department of Homeland Security (DHS) in 2006 developed the Enhanced Critical Infrastructure Protection (ECIP) program. The ECIP program aimed to provide a closer partnership with state, regional, territorial, local, and tribal authorities in fulfilling the national objective to improve CIKR protection. The program was specifically designed to identify protective measures currently in place in CIKR and to inform facility owners/operators of the benefits of new protective measures. The ECIP program also sought to enhance existing relationships between DHS and owners/operators of CIKR and to build relationships where none existed (DHS 2008; DHS 2009).

In 2009, DHS and its protective security advisors (PSAs) began assessing CIKR assets using the ECIP program and ultimately produced individual protective measure and vulnerability values through the protective measure and vulnerability indices (PMI/VI). The PMI/VI assess the protective measures posture of individual facilities at their "weakest link," allowing for a detailed analysis of the most vulnerable aspects of the facilities (Schneier 2003), while maintaining the ability to produce an overall protective measures picture. The PMI has six main components (physical security, security management, security force, information sharing, protective measures assessments, and dependencies) and focuses on actions taken by a facility to prevent or deter the occurrence of an incident (Argonne National Laboratory 2009).

As CIKR continue to be assessed using the PMI/VI and owners/operators better understand how they can prevent or deter incidents, academic research, practitioner emphasis, and public policy formation have increasingly focused on resilience as a necessary component of the risk management framework and infrastructure protection. This shift in focus toward resilience complements the analysis of protective measures by taking into account the three other phases of risk management: mitigation, response, and recovery (Figure 1). Thus, the addition of a robust resilience index (RI) to the established PMI/VI provides vital information to owners/operators throughout the risk management process.

Combining a pre-incident focus with a better understanding of resilience, as well as potential consequences from damaged CIKR, allows owners/operators to better understand different ways to decrease risk by (1) increasing physical security measures to prevent an incident, (2) supplementing redundancy to mitigate the effects of an incident, and (3) enhancing emergency action and business continuity planning to increase the effectiveness of recovery procedures. Information provided by the RI methodology is also used by facility owners/operators to better understand how their facilities compare to similar sector/subsector sites and to help them make risk-based decisions.

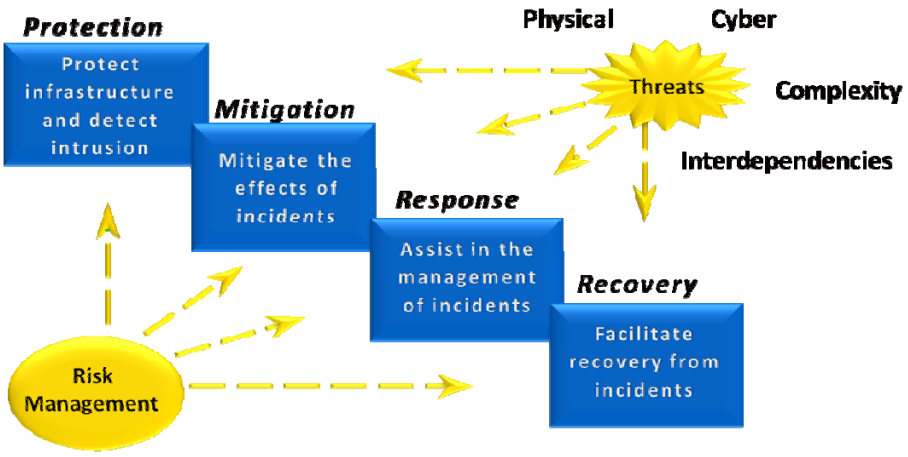

FIGURE 1 Risk Management Process (Peerenboom 2002)

This report provides an overview of the RI methodology developed to estimate resilience and provide resilience comparisons for sectors and subsectors. The information will be used to (1) assist DHS in analyzing existing response and recovery methods and programs at facilities and (2) identify potential ways to increase resilience.

The RI methodology is based on principles of Appreciative Inquiry, which is "the co-evolutionary search for the best in people, their organizations, and the relevant world around them" (Cooperrider et al. 2005). Appreciative Inquiry identifies the best of "what is" and helps to envision "what might be."

The ECIP program and the RI represent a new model (using Appreciative Inquiry principles) for information sharing between government and industry (Fisher and Petit 2010). A "dashboard" display, which provides an interactive tool – rather than a static report, presents the results of the RI in a convenient format. Additional resilience measures can be modeled to illustrate how such actions would impact the asset's RI value.

2 RESILIENCE AND VULNERABILITY

Figure 2 indicates where resilience fits into the overall risk management picture, from threats to consequences, and where potential actions can be taken to prevent realization of the threats or consequences. The chart aligns the spectrum of risk with the different types of measures (preparation, mitigation, response, and recovery) that can be used to manage risk and reinforce the system. This "bow-tie" representation of risk illustrates the importance of resilience, from its emphasis on robustness and mitigation through recovery and potential consequences.

The need to better understand current resilience postures, as well as options for increasing resilience among CIKR culminated in a detailed study and report by the National Infrastructure Advisory Council (NIAC), which called for an increased focus on resilience for U.S. infrastructure protection programs (NIAC 2009). The report tackled one of the most difficult challenges to gaining a broad view of CIKR resilience in the country — clearly defining the meaning of resilience — and underlined the importance of an increased understanding of resilience to an overall risk management strategy for both public and private CIKR.

NIAC defined resilience, in the context of CIKR, as *the ability to reduce the magnitude and/or duration of disruptive events*. The effectiveness of a resilient infrastructure or enterprise depends on its ability to *anticipate, absorb, adapt to, and rapidly recover from a potentially disruptive event, whether naturally occurring or human caused* (NIAC 2009). Anticipation and absorption capabilities reflect the capacity of the system to avoid a disruptive event or to decrease the detrimental impacts of that event. Adaptation and recovery reflect the capacity of the system during an event to avoid or to decrease the importance of the consequences to the environment by quickly returning to a normal state of operation (Figure 3).

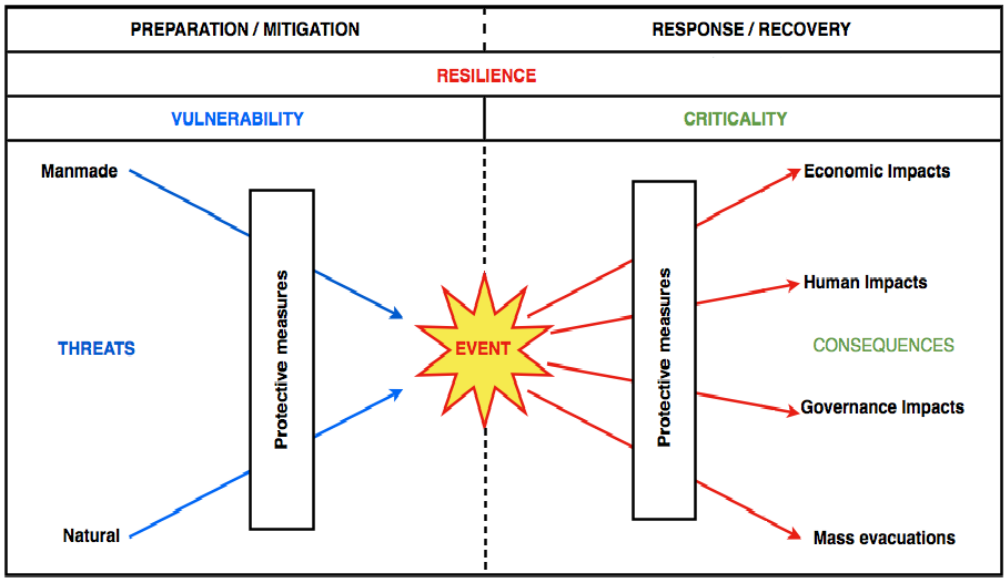

FIGURE 2 The Risk Bow-Tie (Fisher and Norman 2010)

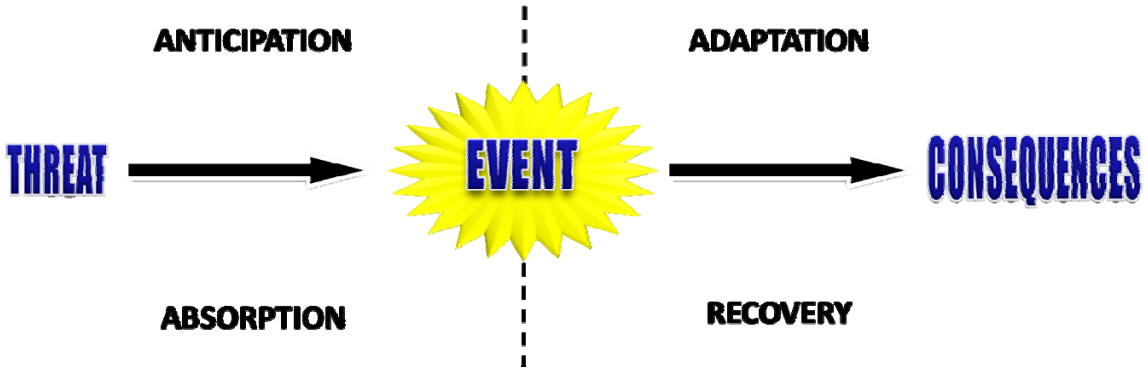

FIGURE 3 The Four Dimensions of Resilience

Although these topics accurately describe the overall concepts of organizational resilience, NIAC chose to further define them in operational terms to better relate them to the CIKR community. NIAC proposed to analyze the organization or system under study in terms of *robustness*, *resourcefulness*, and *rapid recovery* (Figure 4). Each of the terms matches a previously discussed concept, although resourcefulness is split between pre-event measures and post-event measures to cover the concepts of anticipation and adaptation.

The *robustness* component of resilience is the ability to *maintain critical operations and functions in the face of crisis* (NIAC 2009). It is directly related to the ability of the system to absorb the impacts of a hazard and to avoid or decrease the importance of the event that could be generated by this hazard. Robustness can be seen as the protection and preparation of a system facing a specific danger. The objective is to define the measures that can help the system withstand or adapt to a hazard. In contrast to protective measures, for which much of the focus is on preventing an incident, robustness emphasizes the ability of an asset to withstand the incident should protective measures fail. Robustness also integrates the capacity of the asset to function in a degraded state. The importance of robustness is not necessarily defined by how the asset continues to function in the face of an incident, but rather by how the asset is able to continue to accomplish its mission and to provide its products and services through preventative measures, mitigation, or absorption capabilities.

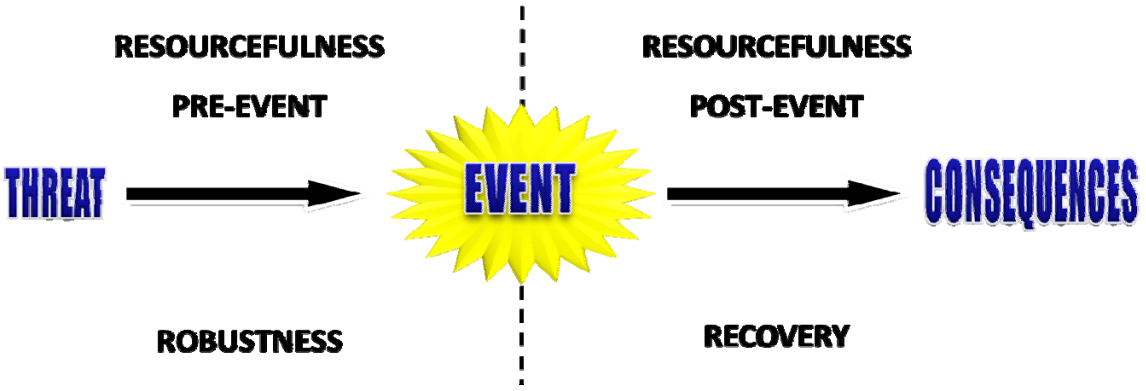

FIGURE 4 The Four Operational Dimensions of Resilience

Rapid recovery is the ability to *return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption* (NIAC 2009). The concept of rapid recovery defines the passage of an asset from a degraded state to one of acceptable operation. This concept builds off of the robustness component in that, if measures of robustness fail to fully prevent, mitigate, or allow the asset to absorb the damage event, rapid recovery constrains the impacts of a stoppage in production. Rapid recovery refers to the ability to not only return to acceptable operating levels, but also to recover fully from the effects of an incident.

Resourcefulness is the ability to *skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds* (NIAC 2009). Resourcefulness begins prior to an event and continues into the response phase. It comprises the steps taken prior to an event to prepare employees and management for possible threats and the application of the training and planning once an event occurs. Resourcefulness can be seen as a complement to robustness and allows for a smooth and expedited transition from the response phase to the recovery phase.

Robustness, resourcefulness, and recovery should not be seen as distinct and nonoverlapping, but as a comprehensive process of prevention, mitigation, absorption, and recovery (Matthews et al. 2010).

3 RESILIENCE ANALYSIS METHODOLOGY

A resilience analysis must generate reproducible results that can support decision making in risk management, disaster response, and business continuity. In response, Argonne National Laboratory has developed a comprehensive methodology of consistent and uniform data collection and analysis through a resilience index.

3.1 DATA COLLECTION

Information must be accurate and transparent if it is to yield an effective resilience score that can be compared with other scores. Reproducibility is especially critical because an index loses value if it cannot be compared and interpreted in a consistent manner.

The ECIP program's site visits support the collection of accurate information that is used to compare CIKR in terms of vulnerabilities, resilience, consequences, and ultimately, overall risk. Based on a questionnaire containing more than 1,500 data points, the program is appropriate for a wide range of CIKR facilities, including commercial buildings, electrical substations, and dams. The ECIP questionnaire allows PSAs to collect, within a limited timeframe (typically 4 to 8 hours), pertinent information that characterizes a facility. PSAs, who are critical infrastructure and vulnerability assessment specialists assigned to local communities (DHS 2007), are specifically trained to ensure the uniformity and coherence of the data they collect. They survey the protection and resilience measures in place at a facility by gathering data at the most vulnerable point for each measure (e.g., the electric connections). The data are then verified at both DHS headquarters and Argonne National Laboratory through a quality assurance (QA) review process that comprises six steps:

1. The questions that are required for RI development are "validated" upon initial submission. A PSA cannot submit the data about a particular facility until all required questions are answered.

2. An initial QA review is conducted by DHS personnel who are trained in the methodology and have direct and immediate access to the questionnaire.

3. A second QA review is conducted by ECIP subject matter experts. This second review provides for an objective assessment of the initial QA and refinement of the process in case data were overlooked or the methodology was not appropriately followed. The subject matter experts can also approve or disapprove of any of the changes suggested during the initial QA.

4. The PSA reviews the data and the changes to the initial data collection to help clarify what data are required and help maintain consistency in the methodology.

5. After the PSA review, a final QA review is conducted by another round of ECIP subject matter experts. This final review includes grammatical edits and clarification of any data that were not clearly understood.

6. A final check is conducted during the development of the RI (scoring process) from the raw data to ensure that all the selected elements feed into the database properly.

The QA process is an integral part of the larger RI methodology because it maintains the integrity of the information collected and the products disseminated. The process also helps ensure the validity of the data and decreases the variance across data collected at different sites. Additionally, cleaning the data before they are used to produce an RI score reduces the overall time it takes to return a final product to the owner/operator.

Beyond its benefits to the end product, the QA process also has several other benefits. The PSA review serves as a constant training opportunity for the PSAs involved, reinforcing, over time, a consistent application of the methodology. The process can also highlight problems that may exist in the question set. The questions and their potential responses can be reevaluated following identification of a pattern of errors. Often, questions are revised to enhance their clarity and consistency of interpretation.

After the QA review process, the data are stored in an Oracle database, allowing for management and selection of the data that will be used to define the RI.

3.2 CALCULATION OF THE RESILIENCE INDEX

To capture resilience, the relevant data collected in the ECIP program are aggregated into levels of information.

The resilience analysis organizes the information collected into five levels in order of increasing specificity; raw data are combined into groups at level 5 and are combined further through levels 4 to 1. The RI combines three level 1 components (robustness, recovery, and resourcefulness), corresponding to the resilience components defined by NIAC; 12 level 2 components; and 47 level 3 components, defined by subject matter experts (Table 1).

Each question (raw data), and all components and subcomponents of the RI, is assigned a weight representing its importance relative to other questions/components/subcomponents in its grouping. The weights were obtained in accordance with the principles of “decision analysis,” an approach that helps manage risk in terms of uncertainty (Keeney 1992; Keeney and Raiffa 1976). The methodology is based on a numerical representation of the value pattern, obtained by comparing different elements of a facility and by using relations “better than” and “equal in value to” to define their relative importance. Another important element in this decision analysis tool is the transitivity of the ranking, which means that if an element A is more important than an element B, and an element B is more important than an element C, then logically A will be more important than C. This approach produces a relational representation of a facility’s resilience alternatives by providing a numerical value assignment for each of its components.

TABLE 1 Major Components and Subcomponents Constituting the Resilience Index

Major Components and Subcomponents of RI	
Robustness	Resourcefulness
a. Redundancy (8)	a. Training/Exercises (7)
b. Prevention /Mitigation (7)	b. Awareness (3)
c. Maintaining Key Functions (3)	c. Protective Measures (3)
	d. Stockpiles (2)
Recovery	e. Response (3)
a. Restoration (3)	f. New Resources (2)
b. Coordination (2)	g. Alternative Sites (4)

(*) Denotes number of subcomponents.

The methodology involves separating a facility into its component parts and using a mathematical formula to define possible decisions from the component parts and to propose different alternatives to increase resilience. This method helps decision makers select simple and familiar choices in the context of a seemingly complex issue.

A relative weight is assigned to each component that contributes to the RI. The weights for a set of components depend on the ranges (worst to best) that are included as options in the question set. Preferences for the specific values within the ranges of single components have been provided by subject matter experts and sector/subsector representatives via an elicitation process. Figure 5 shows an example of results of that process, done with three groups of experts, for components of Business Continuity Plan Training, subcomponents of the Training/Exercises variable, which is part of the Resourcefulness component.

In the index, Business Continuity Plan Training has five alternatives. Each group of experts must rank each of these alternatives in relation to the others, from 1 (most important element for training) to 5 (least important element for training). If the subject matter experts decide that two elements have the same importance, they can give them the same rank. The element with rank 1 is given a weight of 100%. Each group defines the weight of each other element in the category, considering its relative importance compared with the element ranked 1. Experts can assign equal weights to two elements if they have the same importance or relatively close weights if the elements are not of equal importance but are separated only by a slight increase in value. Conversely, the difference in assigned weights can be increased if one element is considered significantly less important than another.

Figure 5 shows that Groups 1 and 3 ranked the variables the same, even though the weights they assigned to each element varied. Group 3 weighted the second-, third- and fourth-ranked elements lower than Group 1 did, meaning that they believed those elements were less important than Group 1 compared with the element ranked number 1. Group 2 had both different

Resourcefulness - Training /Exercises									
			Group 1		Group 2		Group 3		
			Rank	Weight	Rank	Weight	Rank	Weight	Combined Weights
Business Continuity Plan Training	Only key personnel have access to a copy of the plan		5	35	5	35	5	25	31.67
	Only key personnel are trained on the plan but only at initial employment		4	50	4	50	4	35	45.00
	Only key personnel are trained on the plan at initial employment as well as at least once a year		3	70	2	80	3	50	66.67
	All personnel are trained on the plan but only at initial employment		2	60	3	70	2	65	70.00
	All personnel are trained on the plan at initial employment as well as at least once a year		1	100	1	100	1	100	100.00

FIGURE 5 Example of Value Assessments from Experts

weights, as well as different rankings for the elements ranked 2 and 3. For Group 2, to have "only the key personnel trained on the plan at initial employment and at least once a year" is more important than having "all personnel trained on the plan but only at initial employment."

When all experts' ranks and weights are defined for a specific subcomponents group, final weights are obtained by using an average of weights defined by the subject matter expert groups. For the Business Continuity Plan Training, the final weights vary from 100, for the most important element, to 31.67, for the relatively least important element.

Because the function of the RI is modeled after the PMI/VI (Argonne National Laboratory 2009), the individual variables are arranged so that they can be aggregated from the raw data (level 5) stage into broader variables, culminating — through an additive process — into an overall RI value.

The levels of information are rolled up through a tree organization to take into account all elements that promote resilience and to develop an RI. Figure 6 shows the flow organization of the first two levels of components.

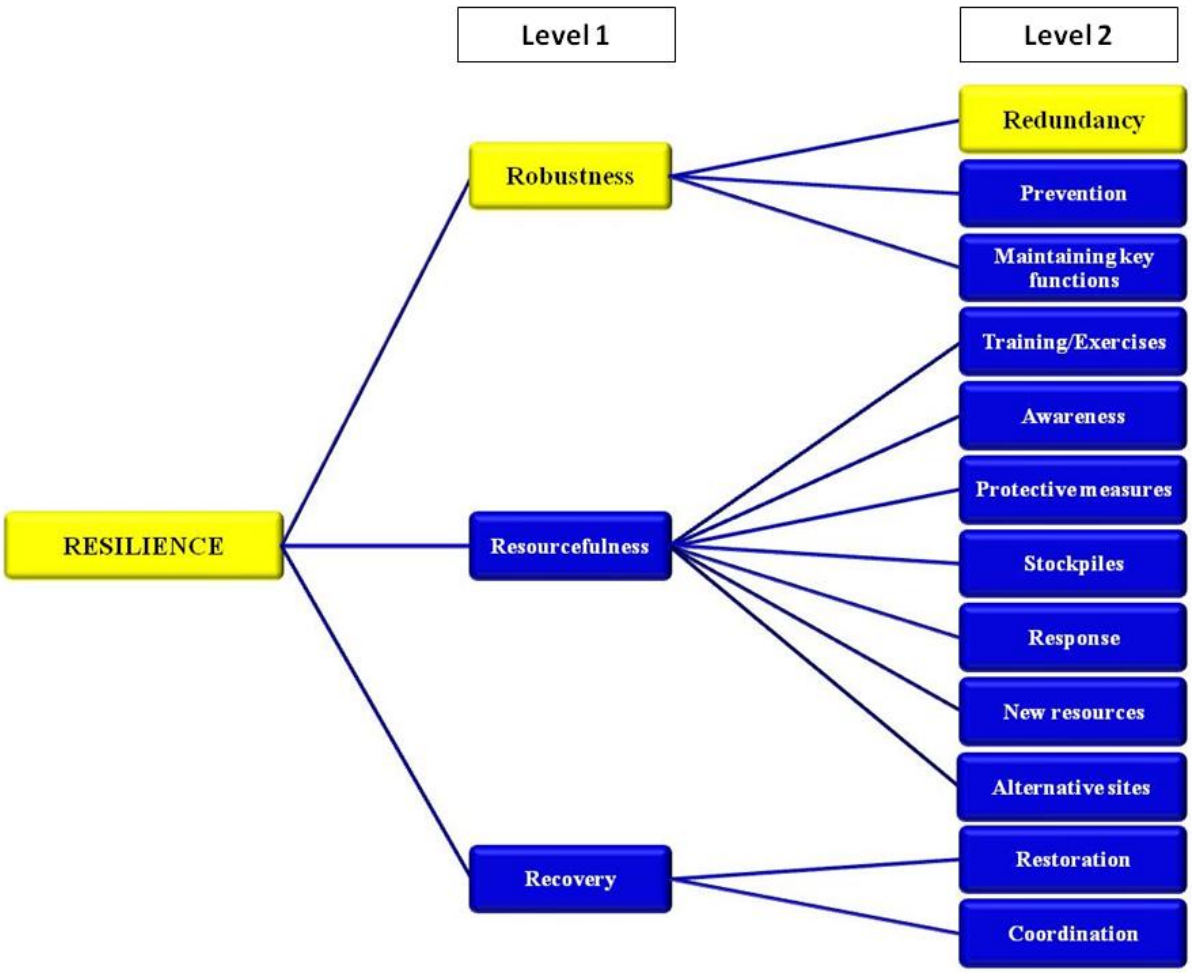

FIGURE 6 Levels 1 and 2 of the Resilience Index

Each of the 12 level 2 components is subdivided into another level of information, as shown in Appendices 1 through 3. For example, redundancy (level 2) is a component of robustness (level 1) and has eight subcategories, as shown in Figure 7 (electric power, natural gas, telecommunications, information technology, water, wastewater, transportation, and critical products). Figure 7 also shows that level 3 categories (e.g., electric power) are subdivided into additional variables. In this case, the electric power category is made up of four subcategories (on-site backup generation, uninterrupted power system, internal generation, and connections).

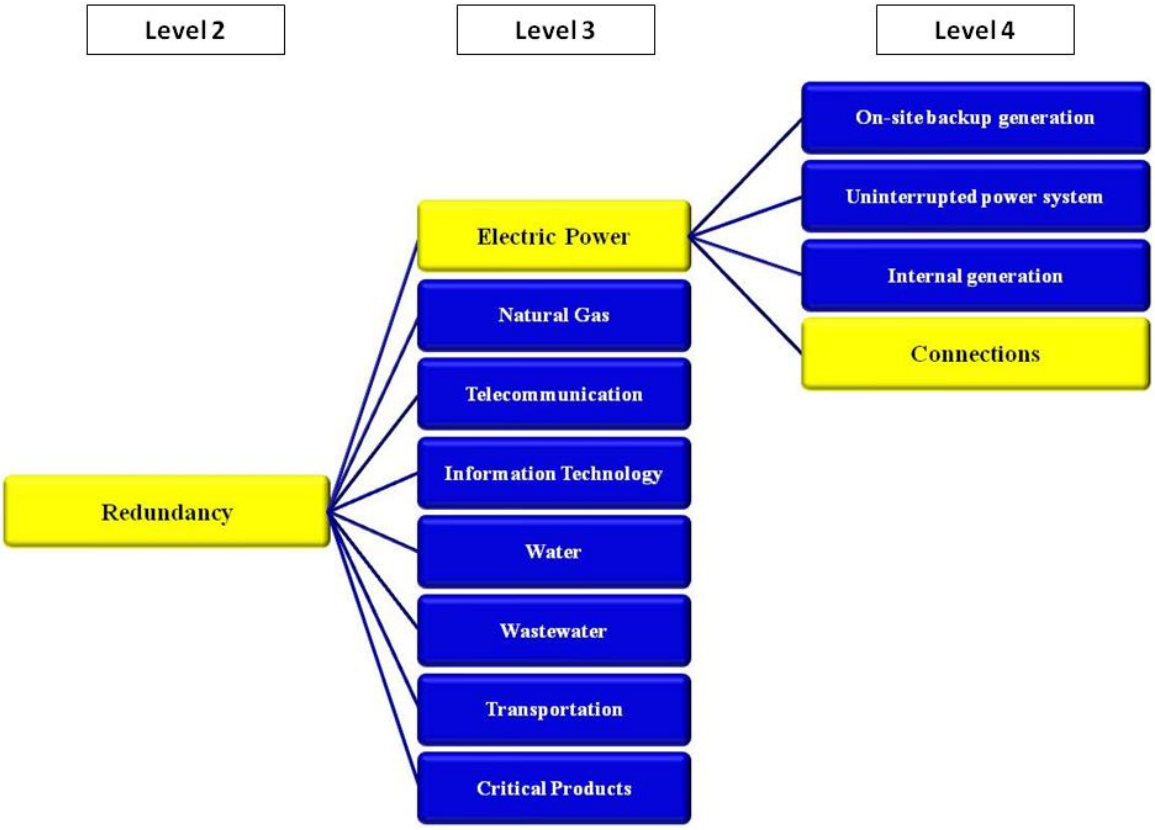

FIGURE 7 Levels 2, 3, and 4 of the Redundancy Component

To measure level 4 components, such as the one defining electrical power connections, raw data (level 5) (in the form of facility answers to individual questions) are collected. Table 2 lists the alternatives used to characterize electric connections; the answers are rolled into an overall value for electric connections.

The level 5 weights listed in Table 2 imply that elements P.1 and P.4 are more important than P.2 and P.3 — that it is more important to have more than one service connection, each of which can handle the entire facility load, than to have more than one service connection, not all of which can handle the entire facility load. While these two choices are mutually exclusive, the index also implies that it is more important — in terms of robustness — to have more than one service connection where each can handle the entire facility load than having power lines from substations follow independent pathways — although the weighted importance is close. These two possibilities are not mutually exclusive.

TABLE 2 Level 4 Electric Connections Index (Illustrative Asset)

	Electric Connections Component (Level 5)	Level 5 Weight	Answer	Weighted Index
P.1	More than one service connection, each can handle entire facility load.	0.335	No[a]	0
P.2	More than one service connection, not all of them can handle entire facility load.	0.220	Yes[b]	22.0
P.3	Power lines from the substation(s) follow independent pathways (e.g., geographically different paths) to the area of the asset/facility.	0.330	Yes[b]	33.0
P.4	Multiple service lines are in different geographic locations.	0.335	Yes[b]	33.5
Level 4 Electric Connections Index			**Value:**	**88.5**

[a] No corresponds to a numerical value of 0.
[b] Yes corresponds to a numerical value of 100.

Collected data are aggregated to define an electric connection, a level 4 component of resilience, by using Equation 1:

$$EC = \sum_{i=1}^{4} a_i \times Z_i \quad (1)$$

where:

EC = electric connections index, level 4 (ranging from 0 to 100);
a_i = scaling constant (weight) indicating the relative importance of possibility i (i = 1,2,3,4) for electric connections; and
Z_i = value of component i of electric connections (0, if not present, or 100, if present).

The facility in the example has more than one electric service connection in different geographic locations. The power lines from the substation follow different geographic pathways, but each of them alone cannot handle the entire facility load. In Equation 1, the weighted values of the questions answered affirmatively are combined to give the facility an overall electric connections index of 88.5 (Table 2).

Level 4 components are aggregated into level 3 components, which represent the main characteristics of the facility studied, such as its individual dependencies and its emergency and continuity plans. For example, the electric connections variable, level 4, is one component of the level 3 electric power variable (Table 3).

TABLE 3 Level 3 Electric Power Index (Illustrative Asset)

Electric Power Component (Level 4)	Level 4 Weight	Level 4 Index	Weighted Index
On-site backup generation	0.300	93.40	28.02
Uninterrupted power system / battery backup on-site	0.195	92.20	17.98
Internal generation	0.295	0	0
Electric connections	0.210	**88.50**	**18.59**
Level 3 Electric Power Index		**Value:**	**64.59**

On the basis of the level 4 weights, it is most important for electric power to have on-site backup generation (weight of 0.300); nearly as important is internal generation (weight of 0.295). The facility in the example does not have internal generation, but it does have an on-site backup for its core operations.

Level 4 components are combined to create a level 3 index. These level 4 components can be derived from either yes or no values (internal generation) or rolled up from level 5 questions, as is the case with electric connections.

The electric power index (level 3) is obtained by using Equation 2:

$$EP = \sum_{i=1}^{4} b_i \times Y_i \qquad (2)$$

where:

EP = electric power index, level 3 (ranging from 0 to 100);
b_i = scaling constant (weight) indicating the relative importance of component i (i = 1, 2, 3, 4) of electric power; and
Y_i = index value of component i of electric power (e.g., electric connections).

The relative importance (weight) of electric connections for electric power is 0.210. By multiplying the value of electric connections (88.5) by its weight, we obtain a weighted electric connections value of 18.59. This value is added to the other weighted components that constitute electric power (level 3) to obtain an overall electric power index of 64.59 (Table 3).

Level 3 components are aggregated to define level 2 components. This level represents the main functions that promote resilience of the facility and the key contributors to robustness, resourcefulness, or recovery. Categories such as redundancy, prevention, maintenance of key functions, and training and exercises are level 2 components. Electric power is one of eight level 3 components that are aggregated to form the redundancy subcomponent of robustness (Table 4).

TABLE 4 Level 2 Redundancy Index (Illustrative Asset)

Redundancy Component (Level 3)	Level 3 Weight	Level 3 Index	Weighted Index
Electric power	0.125	**64.59**	**8.07**
Natural gas	0.125	100	12.50
Telecommunication	0.125	62.80	7.85
Information technology	0.125	58.4	7.30
Water	0.125	0	0
Wastewater	0.125	21.50	2.69
Transportation	0.125	100	12.50
Critical products	0.125	100	12.50
Level 2 Redundancy Index		**Value:**	**63.41**

In the case of redundancy, all the subcomponents that constitute the redundancy component have the same relative importance and therefore the same relative weight (0.125). An index value of 100 for these level 3 components indicates that the asset is not dependent on a specific element (gas and critical products) or that it is dependent but has measures in place to fully mitigate the potential implications of this dependency (transportation). A value of 0 indicates a dependency with no protective or redundant measures in place. Values between 0 and 100 indicate a dependency with partially redundant or protective measures. In the example above, the facility has a backup for the telephone with one terminal in the facility (index = 62.8). There is only one connection to the water network without any backup (index = 0), and the asset has its own wastewater treatment plant but does not have enough capacity to handle a fully operational facility (index = 21.5).

Level 2 components are estimated as the weighted sum of level 3 components. The level 2 index for redundancy is obtained by using Equation 3:

$$R = \sum_{i=1}^{8} C_i \times X_i \tag{3}$$

where:

R = redundancy index, level 2 (ranging from 0 to 100);
c_i = scaling constant (weight) indicating the relative importance of component i (i = 1,…, 8) of redundancy; and
X_i = index value of component i of redundancy (e.g., electric power).

The relative importance (weight) of electric power for redundancy is 0.125. By multiplying the value of the electric power index (64.59) by its weight, we obtain a weighted electric power index of 8.07. This new value is added to the other weighted index values that constitute the redundancy components (level 2) to obtain a level 2 redundancy index of 63.41 (Table 4).

Level 2 components are aggregated to define the level 1 components, which represent the three main concepts of resilience:

- *Robustness,* which characterizes the capability of a system to resist a specific event. This level 1 component groups its level 2 subcomponents that characterize redundancy, prevention, and maintenance of key functions (Appendix 1).

- *Resourcefulness,* which characterizes both the current resources developed to enhance a facility's robustness and new resources to support the response to an event and recovery of the system. This level 1 component groups its level 2 subcomponents that characterize the pre- and post-event facility capabilities, such as training/exercises, awareness, new resources, and response capabilities, as well as the ability to operate from an alternate site (Appendix 2).

- *Recovery,* which characterizes the capability of a system to rapidly recuperate after a crisis. This level 1 component groups its level 2 subcomponents that characterize facility capabilities to restore its functions and coordinate its actions (Appendix 3).

Per the RI, redundancy is the most important subcomponent of robustness, with a weight of 0.400 (Table 5). Prevention is the least important subcomponent for the determination of robustness, with a weight of 0.267. The facility analyzed in our example has an index of 59.39 for prevention, which corresponds to a facility with no specific protective measures in terms of building codes, and one that is located in an area with possible wildfires, severe winter storms, and high-wind events (thunderstorms or tornados). The facility was constructed considering these potential hazards. The facility is dependent on several elements, such as water, wastewater, electricity, information technology, and telecom, but has protective measures, to some degree, in place for all of these dependencies. The index of the facility for the maintenance of key functions is 51.71, which corresponds to different elements of planning and procedures; for example, the facility may have specific procedures for emergency communication, human resources, and the identification of key personnel. Some potential procedures are still missing, such as work arrangement or relocation.

TABLE 5 Level 1 Robustness Index (Illustrative Asset)

Robustness Component (Level 2)	Level 2 Weight	Level 2 Index	Weighted Index
Redundancy	0.400	**63.41**	25.36
Prevention	0.267	59.39	15.86
Maintaining key functions	0.333	51.71	17.22
Level 1 Robustness Index		**Value:**	**58.44**

The overall robustness index is calculated as the weighted sum of its three subcomponents using Equation 4:

$$\mathrm{Ro} = \sum_{i=1}^{3} d_i \times W_i \tag{4}$$

where:

Ro = robustness index, level 1 component of resilience (ranging from 0 to 100);
d_i = scaling constant (weight) indicating the relative importance of component i (i = 1, 2, 3) of robustness; and
W_i = index value of component i of robustness (e.g., redundancy).

The relative importance (weight) of redundancy for robustness is 0.400. By multiplying the value of the redundancy index (63.41) by its weight, we obtain a weighted index of 25.36. This value is added to the other weighted subcomponents of robustness (level 1) to obtain a robustness index of 58.44 (Table 5).

Finally, the three Level 1 components are aggregated to define an overall RI (Table 6).

TABLE 6 Resilience Index (Illustrative Asset)

Resilience Component (Level 1)	Level 1 Weight	Level 1 Index	Weighted Index
Robustness	0.380	**58.44**	22.21
Resourcefulness	0.316	60.77	19.20
Recovery	0.304	48.63	14.78
Overall Resilience Index		**Value:**	**56.19**

According to the overall weights, robustness is the most important component of facility resilience with a weight of 0.380, while resourcefulness and recovery are nearly equal in importance. The facility analyzed in our example has an index for resourcefulness of 60.77, which corresponds to a facility that has already conducted a vulnerability assessment and developed training plans for emergency, security, and business continuity. However, the facility needs further coordination with first responders and the addition of an alternative site (hot or cold). Furthermore, the training it utilizes might be for key personnel only, and the facility has only conducted a tabletop exercise, rather than a full-scale exercise, over the past year. The facility index for recovery is 48.63, which corresponds to a lack of internal coordination and specific agreements with external authorities and responders.

The overall RI consists of a weighted sum of three level 1 components (robustness, resourcefulness, and recovery), as shown in Equation 5:

$$RI = \sum_{i=1}^{3} e_i \times V_i \quad (5)$$

where:

RI = relative resilience index (ranging from 0 to 100);
e_i = scaling constant (weight; a number between 0 and 1) indicating the relative importance of component i (i = 1, 2, 3) of resilience; and
V_i = index value of component i of resilience (i.e., robustness, resourcefulness, and recovery).

The relative importance (weight) of robustness for resilience is 0.380. By multiplying the value of the robustness index (58.44) by its weight, we obtain a weighted robustness index of 22.21. This value is added to the other weighted index values of components of resilience to obtain an overall RI of 56.19 (Table 6).

The RI is defined by the aggregation of five levels of information. Each type of data collected and each element comprising Levels 5 through 1 have been weighted by a group of experts to represent the relative importance of variables, subcomponents, and components compared with other data in the same groupings, but also considering their contribution to the overall resilience of the critical infrastructure analyzed. The weights for a set of variables depend on the ranges (worst to best) of each component compared with others in the same group. The weights represent a general sector (or subsector) and a general threat. Additional weights could be elicited to develop indices specific to sectors (or subsectors) and threats.

This process results in an overall RI that ranges from 0 (low resilience) to 100 (high resilience) for the critical infrastructure analyzed, as well as an index value for each level 1 through 5 component. This method of characterizing the resilience of a critical infrastructure allows DHS to consider the specificity of all subsectors but also to compare the efficiency of different measures to enhance resilience in the studied system.

It is important to note that the RI is a relative measure. A high RI does not mean that a specific event will not affect the facility and will not cause severe consequences. A low RI does not mean that a disruptive event will automatically lead to the failure of the critical infrastructure and to other serious consequences. Simply stated, the RI is a way to compare the levels of resilience of critical infrastructures and to help prioritize investment of resources to enhance resilience.

4 COMPARISON OF FACILITIES USING THE RESILIENCE INDEX

The RI for a single facility has significant value, and using that value to compare similar facilities with respect to resilience allows for vital additional benefits to owners/operators, as well as DHS. The comparison of a facility's RI value to that of other, similar facilities allows for an appropriate analysis of RI values and their role in facility risk management. Furthermore, the ECIP program does not collect all information about a facility, just information on the weakest elements — other characteristics of a facility could easily override these resilience elements. Thus, combining the RI with other indices or information will help identify areas for needed in-depth analysis or potential improvements.

While important in terms of the data it represents, an individual RI can be difficult to fully interpret. Without a frame of reference, the value generated by the index does not convey its full meaning. For instance, without an understanding of the other scores, does an overall RI score of 42 lead one to believe the facility is quite resilient? Or possibly lacking key resilience measures? Indeed, this value is strongly related to a specific type of sector and to the context of a facility's operating environment. Thus, a comparative framework is necessary.

An individual score becomes more meaningful when compared with the scores of a set of similar facilities. Providing the owner/operator of a facility with a detailed analysis of its RI and a comparison across other similar facilities is useful because it provides perspective about where the subject facility stands relative to its peer group. The comparison can be made at the highest level (overall RI), at the next-highest level (e.g., robustness, level 1), or at numerous lower levels (e.g., electric power, level 3, or telecommunication, also level 3). The lower-level comparisons provide good starting points for the owner/operator when considering which new resilience measures may be worthwhile. The higher-level comparisons provide a good indication of how the overall resilience posture at the facility compares to those of other, similar facilities. The most useful ways in which the information can be displayed to the owner/operator are being improved as ECIP program experience increases.

Figure 8 shows a display option that includes an overall RI and the three level 1 components. The sector maximum, average, and minimum values are shown as dots.

In Figure 8, the overall RI and the different values for the first-level components are above or near the average for this facility. The robustness index is one of the highest levels found for that type of site and sector, with a value just below the sector maximum. Compared with its sector, this facility seems to be better prepared in terms of resilience; however, its resilience is not necessarily sufficient, nor does its high RI guarantee that an event or disruption will not occur. Figure 9 shows the same chart as Figure 8 for another facility.

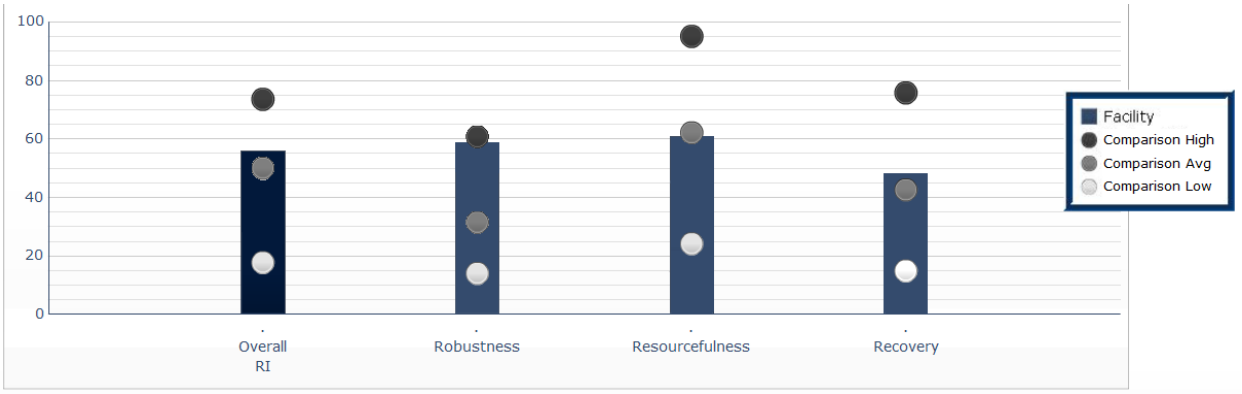

FIGURE 8 Display Option Showing Values of RI Components for a Facility Compared with Sector Averages

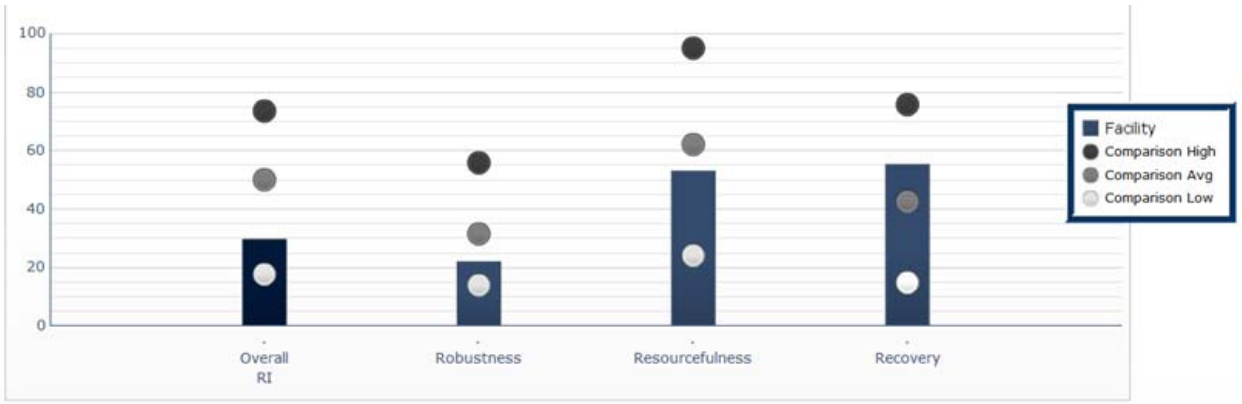

FIGURE 9 Display Option Showing Values of RI Components for another Facility Compared with Sector Averages

The overall RI, robustness index, and resourcefulness index of this second facility are below average. The recovery index value is above average. These values give beneficial information to the CIKR owner/operators and may help in prioritizing future investments. An owner/operator may decide that he/she needs to improve the robustness of the facility. In order to understand the significance of increasing robustness, he/she should consider the resilience information and protective measures at the facility. Indeed, if the facility is well protected, the owner/operator may not need to increase its robustness or, therefore, its resilience.

Beyond the first-level RI comparisons, additional charts, such as the one shown in Figure 10, can be produced for all levels of information available from the ECIP program data and levels included in the RI calculations. For example, comparisons can be made of electric connections, electric power, redundancy, robustness, and the overall RI. These additional levels are vital to understanding why a facility is higher or lower than the average in a given component. The reasoning may not be a general increase or decrease across all subcomponents, but the deviation from the average may simply be based on a single low or high value of a subcomponent.

Figures 10 and 11 show examples of level 2 comparisons for resourcefulness and robustness levels for a facility.

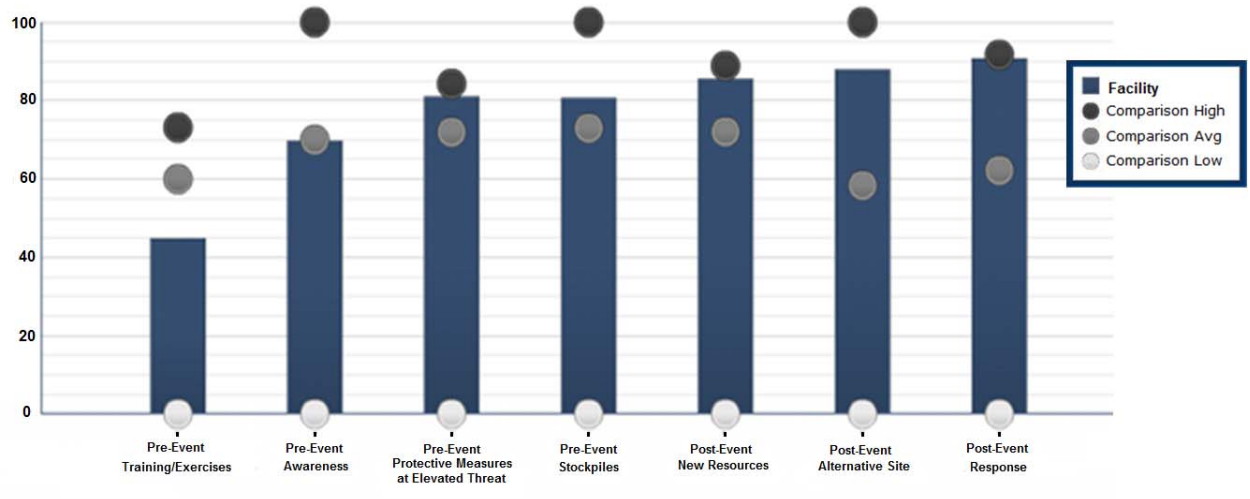

FIGURE 10 Display Option Showing Values of Resourcefulness Components for a Facility Compared with Sector Averages

As Figure 10 indicates, the different components of resourcefulness are near or above average for the facility. Only pre-event training/exercises falls below the sector average. For robustness, shown in Figure 11, the redundancy and prevention indices are zero, but this seems to be a characteristic of the sector because the averages for these categories are near zero. In these cases, the sector maximum seems to be an exception to the norm. Maintenance of key functions, on the other hand, is the only component significantly below the sector average.

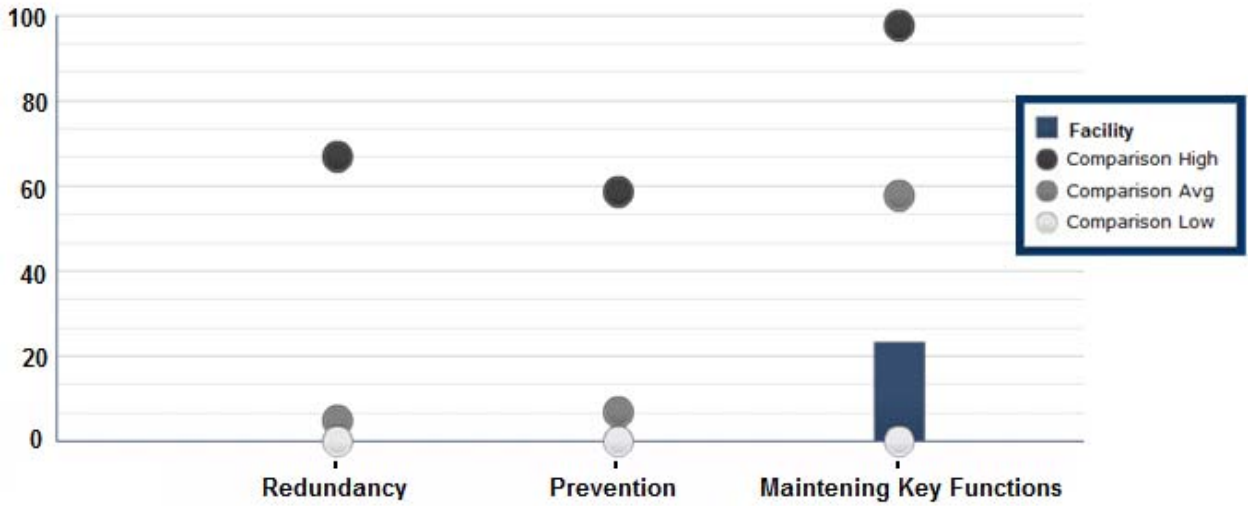

FIGURE 11 Display Option Showing Values of Robustness Components for the Same Facility Shown in Figure 10, Compared with Sector Averages

With the type of information such as that shown in Figures 8 through 11, owners/operators can decide to implement new procedures to improve training and exercises of facility personnel to increase the resourcefulness value, and/or to invest in maintenance of key functions that would increase robustness.

An advantage of the comparisons shown in Figures 8 through 11 is that they draw attention immediately to components that are below the sector average, as well as those that are significantly higher or lower than values obtained for facilities in the same sector. Collecting the ECIP program data and comparing the sector RI values (minimum, average, maximum) can provide DHS with useful insights, as well. Although the infrastructure survey tool is a data collection tool, and PSAs do not specifically identify gaps or provide options for consideration within the ECIP framework, the data do incorporate judgments that allow owners/operators to use the information provided after an ECIP site visit to identify their own gaps (e.g., a business continuity plan that is far below the average for similar facilities within the sector). They can also use this information to help identify measures that will improve their overall RI.

The average comparison should not be seen as the level of resilience that should be reached by the facility. It is simply an indication and appropriate level for comparison. Even when the facility is near the sector maximum for a component of resilience, there may be areas in which it can and should still improve.

To facilitate comparisons among different possible actions, and consideration of possible resilience measures, Argonne National Laboratory has developed a Web-based tool, the ECIP Dashboard. The tool allows managers, simply by selecting possible options for consideration, to change characteristics at each level and immediately see the changes to the overall values of the calculated indices.

Instead of analyzing only one scenario, the Dashboard allows managers to consider as many scenarios as needed, reducing the uncertainty inherent in risk management by providing additional information to managers trying to determine the best courses of action to take to ensure a better-functioning and more resilient facility.

The Dashboard provides different interactive windows that are particularly relevant to supporting decisions for proactive risk management. One of these windows is an RI scenario screen that helps identify what resilience measures can be implemented (Figure 12).

FIGURE 12 PMI Dashboard Screen

At the top of the Dashboard screen, different tabs allow users to select one of the three level 1 RI parameters; Resourcefulness is subdivided into Resourcefulness Pre-Event and Post-Event. When one of these components is selected, the related level 2 and level 3 components appear in the middle of the screen, which enables the user to choose the different characteristics that apply to her/his facility. At the bottom of the screen, the user can see — in real time — the repercussions of modifying these components in the different RI values that result (bottom of the screen). Three representations are used to support this functionality (moving clockwise from the bottom left of the screen):

- A gauge shows the value of the RI for the selected level 1 component (i.e., resourcefulness);
- A counter shows the value of the overall RI;
- Bar charts show the values of indices for the level 2 components and compare them to the subsector averages.

The ability to change the parameters, the speed with which users can see the results, and the possibility for assessing different scenarios all serve to make the Dashboard a very powerful tool and particularly relevant for helping to manage risk-related decisions about critical infrastructures.

Facility-specific RIs demonstrate the potential effectiveness of measures for a particular facility. The list of common options identified through comparison with other, similar facilities is intended to assist managers in making decisions regarding a site-specific resilience strategy. No two facilities are alike — each facility's safety staff and management team must determine the appropriate combination of measures on the basis of its own assessment of risks, taking into consideration threat, specific assets to be protected, consequences, overall vulnerability, facility characteristics, business impacts, return on investment, and overall resilience. The information from the ECIP program methodology provides consistent insights into elements of resilience, vulnerability, and consequence that can aid in an overall analysis (Fisher and Petit 2010).

By applying techniques of Appreciative Inquiry, the Dashboard provides a new paradigm for government information sharing. The product can help reduce the risk to CIKR through additional proactive, resilient actions taken by organizations through the "spirit of inquiry." Instead of dictating to an organization what they must do, the ECIP Dashboard allows an organization to conduct "what if" scenarios to help them implement the four dimensions (discovery, dream, design, and destiny) of an organization's Appreciative Inquiry cycle. The product helps with discovery — providing insights into the inquiry "the best of what is" by allowing organizations to see what other, similar organizations are doing with regard to resilience. It also allows organizations to examine, within their own risk frameworks, the dream phase, or "what might be," and the design phase, called "what should be the ideal." The Dashboard is provided as a tool to assist organizations in conducting positive inquiries into resilience decisions, as opposed to the traditionally negative approach of historic information sharing that identified gaps and vulnerabilities, accompanied by the threat of regulation.

Information from the ECIP program methodology can be interpreted and analyzed in different ways to define multiple indices such as a vulnerability index, resilience index, and criticality index. These indices can be combined and analyzed to give an owner/operator additional information to manage the security and safety of his/her facility.

5 CONCLUSION

In a complex and interconnected world, it is important to reinforce the protection and increase the resilience of CIKR. Indeed, infrastructure networks support the well-being of society. So, it is essential to support the owners/operators of critical infrastructure with tools that allow them to analyze risk in a comprehensive way and that present them with different alternatives to manage that risk.

The development of the RI is intended to assist DHS in analyzing the resilience of the Nation's CIKR and identifying ways to improve it. This index complements the previously developed PMI to enhance the current ECIP program. In addition, the index can provide valuable information to facility owners/operators about their standing relative to similar sector assets and about various ways to increase resilience. Applications and uses of the RI for the ECIP program continue to evolve, and concept improvements and additional enhancements and approaches are expected. Combining the RI with other indices will provide additional benefits, including allowing for an overall view of risk. The objective is to develop better decision-making tools that enable comparison of critical infrastructure and promote a proactive approach to improving robustness, resourcefulness, and recovery capabilities.

6 REFERENCES

Argonne National Laboratory, 2009, *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program,* ANL/DIS-09-4, Argonne National Laboratory, Decision and Information Sciences Division, Argonne, Ill.

Cooperrider, D.L., P.F. Sorensen, T.F. Yaeger, and D. Whitney, 2005, *Appreciative Inquiry — Foundations in Positive Organization Development,* Stipes Publishing, LLC, IL.

Department of Homeland Security, 2007, *Protective Security Advisors — Securing the Nation's Critical Infrastructure One Community at a Time,* Office of Infrastructure Protection, Protective Security Coordination Division, Washington, D.C., available at http://safetyservices.ucdavis.edu/emergency-management/dru-1/iaem-ucc-documents/PSA%20brochure.pdf.

Department of Homeland Security, 2008, *Protective Security Advisor (PSA) Program: ECIP Initiative Engagement,* Office of Infrastructure Protection, Protective Security Coordination Division, Washington, D.C., available at http://www.fhwa.dot.gov/security/emergencymgmt/profcapacitybldg/ecipmemo.pdf.

Department of Homeland Security, 2009, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency,* Washington, D.C., available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Fisher, R.E., and M.A. Norman, 2010, "Constructing a Protective Measures Index across the Security Spectrum," *Journal of Business Continuity & Emergency Planning*, in press.

Fisher, R.E., and F.P. Petit, 2010, *Applying Appreciative Inquiry to Facility Security Decision Making*, 3rd International Conference and Doctoral Consortium on Organization Development and Change, Institut de Socio-Economie des Entreprises et des Organisations (ISEOR), Jean Moulin University, Lyon, France, June 14–16, 2010.

Keeney, R.L., 1992, *Value-Focused Thinking: A Path to Creative Decisionmaking*, Harvard University Press, Cambridge, Mass.

Keeney, R.L., and H. Raiffa, 1976, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, John Wiley and Sons, New York.

Matthews, D., M.A. Norman, S. McAraw, and R.E. Fisher, 2010, *Constructing a Protective Measures Index across the Security Spectrum,* Contingency Planning & Management West Conference, Las Vegas, Nev., May 11–13, 2010.

National Infrastructure Advisory Council, 2009, *Critical Infrastructure Resilience, Final Report and Recommendations,* U.S. Department of Homeland Security, Washington, D.C., available at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

Peerenboom, J., 2002, *Energy Infrastructure Vulnerability Surveys and Assessment,* Argonne National Laboratory, Office of Energy Assurance, U.S. Department of Energy, API Security Directors' Conference, July 18, 2002.

Schneier, B., 2003, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Copernicus Books, New York.

APPENDIX 1: ROBUSTNESS COMPONENTS

Redundancy

- Electric Power
  - On-Site Backup Generation
  - Uninterrupted Power
  - Internal Generation
  - Connections
- Natural Gas
  - On Site Backup Generation
  - Connections
- Telecommunication
  - Mode of Telecommunication
  - Connections
- Information Technology
  - Internal IT Backup
  - Internet Backup
  - Internet System Connections
- Water
  - On Site Resource
  - Connections
- Wastewater
  - On Site Resource
  - Connections
- Transportation
  - Rail
  - Air
  - Road
  - Maritime
  - Pipeline
- Critical Products
  - Chemicals
  - Packaging
  - Medical Supplies
  - Livestock Feed
  - Byproduct/Waste
  - Raw Materials
  - Fuel

Prevention/Mitigation

- Number of Dependencies
- Window Characterization
  - Protective Measures
- HVAC
  - System Access
  - System Protection
- Mitigating Construction
  - Hurricane
  - Flood
  - Earthquake
  - Tornado
  - Wildfire
  - Severe Winter Storm
  - High Wind Event
- Egress/Ingress
  - Navigable Waterway
  - Access Road
- Dependencies Protection
  - Electric
  - Natural Gas
  - Telecommunications
  - Information Technology
  - Water
  - Wastewater
- Business Continuity Planning
  - Close Down Procedures
  - Security Protection

Maintaining Key Functions

- Number of Dependencies
- Mitigating Construction
  - Access Road
  - HVAC
  - Illumination
- Planning
  - Emergency Communications
  - Procedures
  - Arrangement/Agreements
  - Contingency/Continuity Plans

APPENDIX 2: RESOURCEFULNESS COMPONENTS

Training Exercises

- Business Continuity Plan Training
  - Access for Personnel
  - Personnel Training
- Emergency Action Plan Training
  - Access for Personnel
  - Personnel Training
- Security Plan
  - Access for Personnel
  - Personnel Training
- Business Continuity Plan Exercises
  - Type of Exercises
- Emergency Action Plan Exercises
  - Type of Exercises
- Security Plan Exercises
  - Type of Exercises
- System Testing
  - Backup Generator
  - IDS
  - CCTV

Stockpiles

- Electric Power
  - On-Site Backup Generation
  - Contracts or Procedures
  - Duration of Backup
- Critical Products
  - Chemicals
  - Fuel
  - Packaging
  - Medical Supplies
  - Livestock Feed
  - Byproduct/Waste
  - Raw Materials
  - Water

Protective Measures

- Communications and Notifications
  - Coordinate Security
  - Real Time Communications
- Initial Planning and Preparedness
  - Assignment of Personnel
  - Contingency Procedures
- Elevated Threat Enhancement
  - Cyber Security
  - Infrastructures/Redundancy
  - Incident Response
  - Communication
  - Planning

Alternative Sites

- Site Type
  - Cold Site
  - Hot Site
- Equipment
  - Capability to Perform Essential Functions
  - Support
    - Logistics
    - Communications
    - Transportation
  - Consideration of Health
- Localization
- Alternative Modes of Obtaining Supplies

Awareness

- Vulnerability Assessments
- Information Sharing
  - IT Consultation
  - Security Working Group
  - Threat Information
- Business Continuity Planning

New Resources

- Security Force
  - Coverage
  - Weapons
  - Communications
  - Training
  - Patrols
- MOU/MOA
  - Contracts
    - Fuel
    - IT System
  - Business Continuity
    - Alternative Sources
    - Notification of Suppliers
    - Mutual Aid Agreements

Response

- First Responders
  - Communication Mode
  - Minimum Response Time
  - On-Site Capacity
- Planning
  - Emergency Action Plan
  - Business Continuity Plan
- Information Sharing
  - Threat Information Origin

APPENDIX 3: RECOVERY COMPONENTS

Coordination

Internal Coordination
- EOC
  - On-Site
  - Backup
- Business Continuity Plan Components
  - Human Resources Procedures
  - Communications
  - Alternative Source for Customers
- Business Continuity Plan Point of Contact
  - Key Personnel
  - Essential Infrastructures
  - Mutual Aid Agreements
  - MOU/MOA

External Coordination
- Dependency
  - Priority Plan
  - MOU/MOA
- Access to Specialized Materials
- Civil Government Impact

Restoration

Number of Dependencies

Loss Due to Natural Disaster
- Last Occurrence
- Duration of Business Interruption
- Time to Restart Full Operations

Restoration Characteristics
- Special Material Needs
- Emergency Communications
- Priority Restoration
- Business Continuity Plan

Decision and Information Sciences Division
Argonne National Laboratory
9700 South Cass Avenue, Bldg. 221
Argonne, IL 60439-4844

www.anl.gov