Critical Infrastructure Interdependencies Assessment

Throughout the world there is strong recognition that critical infrastructure security and resilience needs to be improved. In the United States, the National Infrastructure Protection Plan (NIPP) provides the strategic vision to guide the national effort to manage risk to the Nation's critical infrastructure." The achievement of this vision is challenged by the complexity of critical infrastructure systems and their inherent interdependencies.

The update to the NIPP presents an opportunity to advance the nation's efforts to further understand and analyze interdependencies. Such an important undertaking requires the involvement of public and private sector stakeholders and the reinforcement of existing partnerships and collaborations within the U.S. Department of Homeland Security (DHS) and other Federal agencies, including national laboratories; State, local, tribal, and territorial governments; and nongovernmental organizations.

Characterizing Critical Infrastructure Interdependencies

Critical infrastructure interdependencies constitute a risk multiplier: they can themselves be a threat or hazard, affect the resilience and protection performance of critical infrastructure, and lead to cascading and escalating failures. Interdependencies influence all components of risk (Figure 1).

Assessing critical infrastructure interdependencies requires the consideration of complex and

Figure 1 Effect of Critical Infrastructure Interdependencies on Risk Components

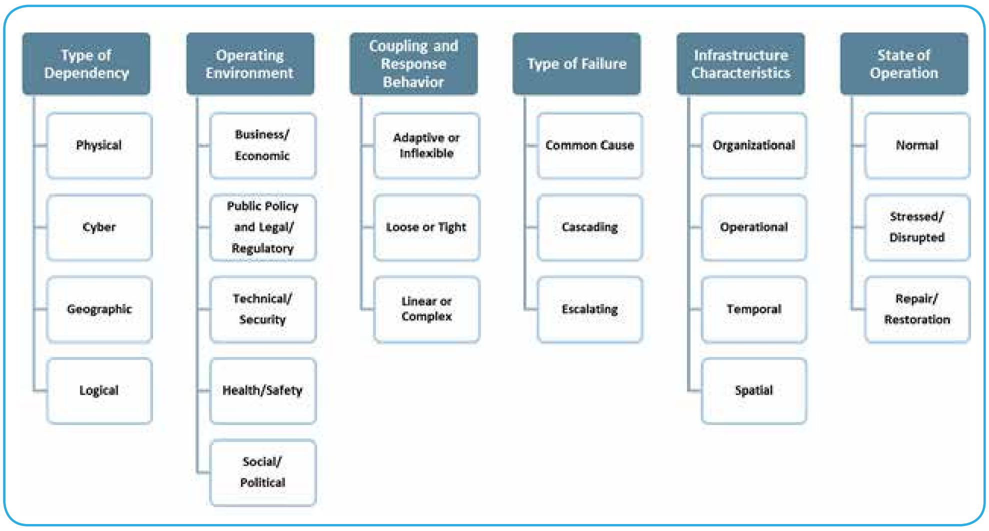

Figure 2 Dimensions of Interdependencies

multidimensional elements (Figure 2).

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

A Systems Approach to Interdependency Analysis

Infrastructure interdependency analysis can be analytically complicated, time consuming, and costly, which in turn can limit the ability of stakeholders to understand and use this information to make risk-informed decisions that enhance resilience. In order to manage these complexities, the infrastructure community should use a process that helps partners prioritize resilience assessment efforts through a "systems approach" to regional interdependency analysis.

This approach is based on the assumption that a critical asset or facility can be considered as part of a broader system of infrastructure. Higher-level constructs (e.g., a community or a region) include multiple systems. As such, a community or a region operates as a "system of systems." Viewed within this framework, high-level systems analysis—using proven and scientifically sound tools—can help identify the most critical lower-level systems. This information can in turn help determine where to conduct more detailed site assessments on only the most critical asset-level components.

A "system of systems" approach can help establish the appropriate scope of an interdependency analysis, as well as the specific assets and/or subsystems for which resilience-related information should be collected. Using this approach, analysis would consider the high-level context (e.g., a geographic region or an industry sector) and the associated states of these systems, ultimately represented by the most critical assets to inform the scope and focus of a resilience assessment, including the most critical assets from which to collect interdependency data.

Executing this "system of systems" approach requires combining top-down and bottom-up data collection and analysis methods to fully consider regional infrastructure interdependencies (Figure 3).

Top-down and bottom-up approaches are used in several engineering fields, including reliability, safety, system, and resilience engineering. , Top-down approaches involve analyzing a system (or multiple systems) in

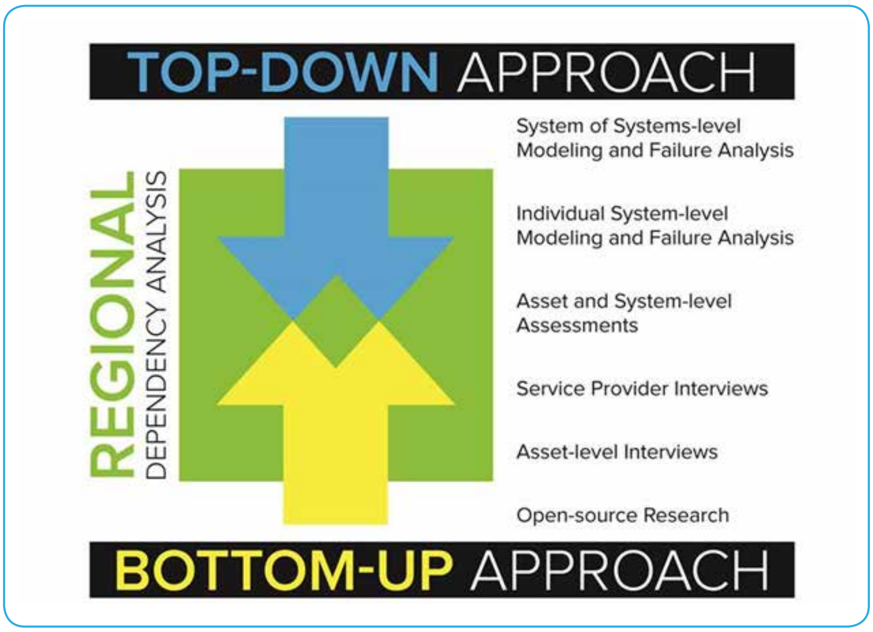

Figure 3 Top-down and Bottom-up Approaches to Regional Dependency Analysis

its entirety and then focusing on its component parts. Bottom-up approaches consist of analyzing the component parts of a system individually and then building on this analysis to describe the system as a whole. Taking a closer look at two of these engineering fields, reliability engineering generally uses a bottom-up approach to evaluate the effect of component failures on system function, while safety engineering generally requires a top-down approach that evaluates how hazardous states can occur at the system level, leading to failures of individual components. These failure and hazard analysis techniques are applicable to analysis of all types of systems, subsystems, or an integrated set of systems and can be used for a number of purposes, including:

- Aiding in system design to withstand failure,
- Assisting in operational planning, and
- Providing inputs to risk management.

Given the nature of dynamic and uncertain threats, there is a critical need for an integrated approach to optimize resilience and protection of critical infrastructure. A top-down approach provides simultaneous analysis of an entire system, enabling decision makers to define resilience measures for implementation at the system level. A bottom-up approach is more appropriate to determine resilience procedures at the facility level. Combining top-down and bottom-up approaches is a comprehensive method that can be used to support decision making based on accepted engineering principles.

Bottom-Up Approach	Top-Down Approach
Decentralized	Centralized
Targets data collection at asset level	Targets data collection at system level
Based on actual operations and conditions	Often based on models and large datasets
Identifies facility-level interdependencies	Identifies system-level interdependencies
Goes from the specific to the global	Goes from the global to the specific

Table 1 Comparison of Bottom-up and Top-down Approaches

Interdependencies exist at individual levels (e.g., assets are interconnected with other assets) and between levels (e.g., assets are interconnected with systems, systems with other systems, and so on). Table 1 presents attributes of bottom-up and top-down approaches to critical infrastructure interdependencies assessments.

Analyzing interdependencies among critical infrastructure first requires examining the unidirectional links (dependencies) and then considering the bidirectional links (interdependencies). These two types of links are the basis for conducting risk assessments considering the effects of critical infrastructure interdependencies on critical infrastructure vulnerabilities, resilience, and consequences.

Conclusion

Critical infrastructure dependencies and interdependencies are complex elements to consider. They are characterized by different dimensions (e.g., types, operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operation). They influence all components of risk; can constitute a threat or hazard, affect the resilience and performance of critical infrastructure, and lead to the propagation of cascading and escalating failures. It is therefore essential to integrate the characterization of dependencies and interdependencies into risk and resilience methodologies. To achieve this ultimate goal, the development of a comprehensive and interactive assessment of critical infrastructure dependencies and interdependencies requires integrating multiple areas of expertise (e.g., engineering, social sciences, business continuity, and emergency management) in a combination of top-down and bottom-up approaches.

Acknowledgment

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

Frédéric Petit, Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory and Duane Verner, Computation Institute, University of Chicago