ANL/GSS-15/4

Analysis of Critical Infrastructure Dependencies and Interdependencies

Risk and Infrastructure Science Center
Global Security Sciences Division

About Argonne National Laboratory

Argonne is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC under contract DE-AC02-06CH11357. The Laboratory's main facility is outside Chicago, at 9700 South Cass Avenue, Argonne, Illinois 60439. For information about Argonne and its pioneering science and technology programs, see www.anl.gov.

ANL/GSS-15/4

Analysis of Critical Infrastructure Dependencies and Interdependencies

prepared by
Frédéric Petit, Duane Verner, David Brannegan, William Buehring, David Dickinson, Karen Guziel, Rebecca Haffenden, Julia Phillips, and James Peerenboom

Risk and Infrastructure Science Center, Global Security Sciences Division,
Argonne National Laboratory

June 2015

Contents

Contents (Cont.)

Figures

Tables

Tables (Cont.)

This page intentionally left blank.

Notation

ANSI	American National Standards Institute
Argonne	Argonne National Laboratory
ASIS	American Society for Industrial Security
BSI	British Standards Institute
DHS	U.S. Department of Homeland Security
FEMA	Federal Emergency Management Agency
GIS	Geographic Information System
IDT	Infrastructure Data Taxonomy
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NFPA	National Fire Protection Association
NIPP	National Infrastructure Protection Plan
PPD-21	Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience
PS-Prep™	Voluntary Private Sector Preparedness Program
RISC	Risk and Infrastructure Science Center
SCADA	Supervisory Control and Data Acquisition

This page intentionally left blank.

Summary

The United States faces significant challenges in preparing for, responding to, and recovering from disasters. Of particular concern are the impacts that natural hazards and manmade threats, including cyber threats, have on the Nation's critical infrastructure systems. Enhancing the protection and resilience of U.S. infrastructure has emerged as an urgent goal—a goal made more challenging by the complexity of these systems and their inherent dependencies and interdependencies.

Key policy documents—including Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, the 2013 National Infrastructure Protection Plan, and the Voluntary Private Sector Preparedness Program—highlight the need for owners and operators to consider dependencies and interdependencies that exist among critical infrastructure systems and how they affect business continuity, security, and resilience management. However, these resources do not define dependency or interdependency, nor do they explain how to integrate them into risk and resilience management processes.

This report seeks to address that gap by defining key terms and outlining a data-driven, adaptive, and flexible analytic framework for critical infrastructure dependencies and interdependencies. The report begins by defining dependencies and interdependencies and exploring basic concepts of dependencies in order to facilitate a common understanding and consistent analytical approaches. Key concepts covered include:

- *Characteristics of dependencies*: upstream dependencies, internal dependencies, and downstream dependencies
- *Classes of dependencies*: physical, cyber, geographic, and logical
- *Dimensions of dependencies*: operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operations

From there, the report proposes a multi-phase roadmap to support dependency and interdependency assessment activities nationwide, identifying a range of data inputs, analysis activities, and potential products for each phase, as well as key steps needed to progress from one phase to the next. The report concludes by outlining a comprehensive, iterative, and scalable framework for analyzing dependencies and interdependencies that stakeholders can integrate into existing risk and resilience assessment efforts.

Ultimately, the concepts, roadmap, and analytical framework defined in this report will position decision makers in the public and private sectors to understand relevant dependencies and interdependencies in critical infrastructure and to anticipate potential disruptions, including cascading and escalating failures.

This page intentionally left blank.

1 Introduction

The United States faces significant challenges in preparing for, responding to, and recovering from disasters. Of particular concern are the impacts that natural hazards and manmade threats, including cyber threats, have on the Nation's critical infrastructure systems. Enhancing the protection and resilience of U.S. infrastructure is an urgent goal—a goal made more challenging by the inherent dependencies and interdependencies within infrastructure systems. Dependencies and interdependencies influence all components of risk (threat/hazard, vulnerability, resilience, and consequence), can themselves be a threat or hazard, affect the resilience and protection performance of critical infrastructure, and lead to cascading and escalating failures. In addition, critical infrastructure dependencies and interdependencies are characterized by different interactions, classes, and dimensions—making their identification and analysis both challenging and complex. Based on these factors, it is essential to integrate dependencies and interdependencies into risk and resilience assessment methodologies.

This report seeks to enhance understanding of critical infrastructure dependencies and interdependencies by providing a data-driven, adaptive, and flexible analytic framework that operationalizes the analysis of dependencies and interdependencies. This framework will enable an unprecedented level of situational awareness and better enable decision makers to anticipate disruptions in key infrastructure systems. The present report:

- Provides an overview of the foundational dependency- and interdependency-related strategic policies and standards.
- Explains the relationship between dependencies and risk.
- Provides the definitions of dependencies and interdependencies and of the elements (i.e., categories, classes, and dimensions) that should be considered when analyzing them.
- Presents an overview of the characteristics to be considered for analyzing the four main classes of dependencies (i.e., physical, cyber, geographic, and logical).
- Presents a roadmap defining the four phases of development toward a comprehensive and holistic dependency and interdependency assessment.
- Presents an assessment framework for critical infrastructure dependencies and interdependencies.

This page intentionally left blank.

2 Dependency- and Interdependency-Related Policy and Standards

Consideration of critical infrastructure dependencies and interdependencies and their integration into risk management and business continuity processes are important elements of *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (PPD-21), the *2013 National Infrastructure Protection Plan* (NIPP), and the Voluntary Private Sector Preparedness Program (PS-Prep™):

- PPD-21 defined three strategic imperatives, one of which is to, "implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure." This strategic imperative calls for operational and strategic analysis to anticipate dependencies/interdependencies and cascading impacts into assessment and management procedures (The White House, 2013). The directive also highlights the importance of lifeline critical infrastructure dependencies, noting the need to consider "sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems" (The White House, 2013).

- Following the recommendations adopted in PPD-21, the 2013 NIPP affirms that "effective risk management requires an understanding of the criticality of assets, systems, and networks, as well as the associated dependencies and interdependencies of critical infrastructure" (DHS, 2013). Assessment of critical infrastructure dependencies and interdependencies is one of the seven core tenets defined in the 2013 NIPP. According to the plan, "understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience" (DHS, 2013). These strategic directives reveal the importance of analyzing infrastructure dependencies, interdependencies, and associated cascading effects from critical infrastructure disruptions to improve national security and resilience.

- Many standards require the consideration of dependencies and interdependencies between organizations and the effect on their risk management and business continuity practices. The PS-Prep™ and associated standards (e.g., British Standards Institute [BTI] 25999 Standard on Business Continuity, National Fire Protection Association [NFPA] 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, American National Standards Institute/American Society for Industrial Security [ANSI/ASIS] SPC.1-2009 Standard on Organizational Resilience, and International Organization for Standards [ISO] 22301 Societal Security – Business Continuity Management Systems – Requirements 06-15-2012) all define elements to be considered for promoting the resilience of an organization (FEMA, 2014).

  NFPA 1600 – 2013 recommends that emergency planners "identify dependencies and interdependencies across functions, processes, and applications to determine the potential for compounding impact in the event of an interruption or disruption" (NFPA, 2013). The inclusion of internal and external dependencies and interdependencies requires consideration of critical supply chains. ANSI/ASIS SPC.1-2009 reinforces this point by

> stipulating that “the risk assessment and impact analysis should consider its dependencies on others and others’ dependencies on the organization, including critical infrastructure and supply chain dependencies and obligations” (ASIS, 2009). ISO 22301 incorporates the same principles by specifying that “the business impact analysis shall identify dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties” (ISO, 2012). British Standards Institute 25999-1:2006, for its part, specifies that analysts “verify that the business continuity plan incorporates all organizational critical activities and their dependencies and priorities” (BSI, 2010).

All of these documents—the strategic imperatives as well as the operational standards—require the consideration of dependencies and interdependencies that can exist among infrastructure, how they are managed, and how they affect business continuity, security, and resilience management. Despite the emphasis on the importance of dependencies and interdependencies, none of the documents provide definitions for dependency or interdependency, nor do they suggest how they could be integrated into risk and resilience assessment. While this may be deliberate to provide flexibility on the selection of resilience and risk assessment approaches, the lack of detail makes it difficult to analyze dependencies and interdependencies in a consistent, rigorous manner. Section 3 seeks to initiate the process of fillings these gaps by providing context regarding the relationship between dependencies and risk analysis.

3 Risk and Dependencies

Risk is a function of four components: (1) threat/hazard, (2) vulnerability, (3) resilience, and (4) consequences. In the context of critical infrastructure, for a given threat/hazard type, the risk at an asset[1] is a function of the threat/hazard likelihood, the asset's vulnerability (the likelihood that the threat event will be successful), the resilience of the asset, and the magnitude of the consequences resulting (Carlson *et al.*, 2012; Petit *et al.*, 2013). These risk components are not independent (Figure 1). Considering a threat or hazard (manmade[2] or natural), the vulnerability and resilience of the asset (infrastructure) will lead to consequences.

The intrinsic complexity of risk is increased by dependencies and interdependencies that impact the components of risk. As highlighted in the 2013 NIPP, "growing [dependencies and] interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these [dependencies and] interdependencies and the ability of a diverse set of threats to exploit them" (DHS, 2013).

Figure 1: Risk Components

[1] Facility refers to any type of critical infrastructure such as an office building, an arena, or a refinery.
[2] A wide range of academic research exists on the transfer of risk when considering the intelligent adversary. See Phillips *et al.*, 2012, for a literature review on such.

Dependencies and independencies have a multiplicative effect on risk. A threat or hazard can result in the loss of a service (e.g., electric outage), potentially impacting the critical infrastructure using this resource, which further impacts other critical infrastructure dependent upon that infrastructure's services. The total consequences of an event may be amplified by these connections (i.e., dependencies and interdependencies) that exist among critical infrastructure facilities.

Infrastructure dependencies and interdependencies lead to a level of complexity that masks many systemic risks. As a result, an impact to a single node or link—the proverbial "single point of failure" that is often hidden deep within these interconnected systems—can result in significant economic and physical damage on a city-wide, regional, national, or international scale.

Section 4 provides the definitions of dependencies and interdependencies and of the elements (i.e., categories, classes, and dimensions) that should be considered when analyzing them.

4 Theory and Definitions

As mentioned, several documents (e.g., PPD-21, 2013 NIPP, and PS-Prep™ standards) highlight the need to consider the dependencies and interdependencies among critical infrastructure in risk and resilience assessment. However, these strategic documents do not provide consistent definitions or guidance required to integrate dependency and interdependency analysis in a risk and resilience assessment methodology framework. By leveraging the taxonomy developed by Rinaldi, Peerenboom, and Kelly (2001), this section aims to provide these definitions as well as considerations for such a framework. In particular, categories, classes, and dimensions of dependencies are addressed.

4.1 Dependencies and Interdependencies

In 2001, Rinaldi, Peerenboom, and Kelly defined the terms "dependencies" and "interdependencies" for complex systems; it is recommended that their definitions be used to support consistency among risk and resilience assessment methodologies. The definitions presented in their work are as follows:

> A dependency is a "linkage or connection between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other."
>
> An interdependency is a "bidirectional relationship between two infrastructures in which the state of each infrastructure influences or is reliant upon the state of the other."

A dependency is a unidirectional relationship between two assets (e.g., critical infrastructure, firm, organization, or facility) where the operations of Asset A affect the operations of Asset B. As an example, a water treatment plant depends upon communications services supporting supervisory control and data acquisition (SCADA) systems required for control of plant operations.

An interdependency is a bidirectional relationship between two assets where the operations of Asset A affect the operations of Asset B, and the operations of Asset B then affect the operations of Asset A. For example, the water treatment plant requires communications for its SCADA system, and, in turn, it provides water that is used by the communications system to cool its equipment. An interdependency can be thought of as a combination of two dependencies where the understanding of the interdependency requires an understanding, assessment, and characterization of the two, one-way dependencies.

Figure 2 is a schematic of the relationship between two assets when dependency and interdependency exist.

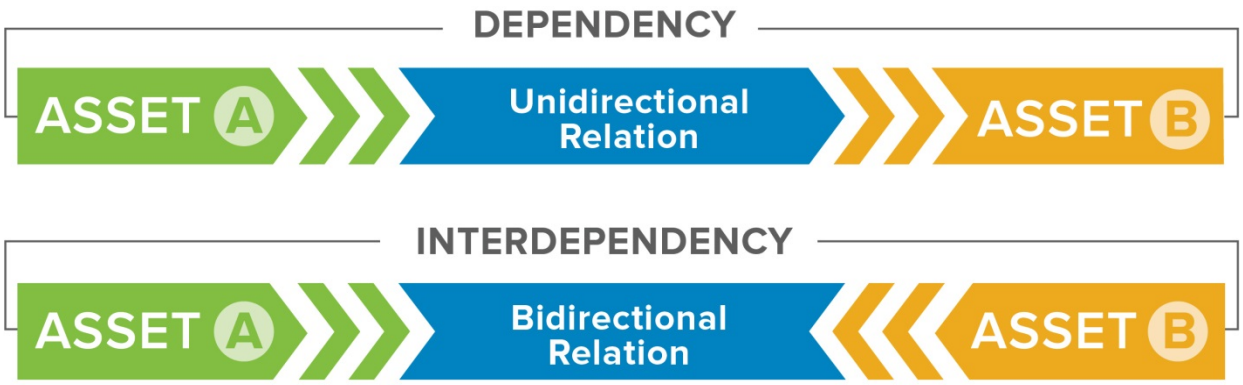

Figure 2: Dependency and Interdependency between Two Assets

Dependencies and interdependencies between critical infrastructure assets are affected by the conditions surrounding the assets and more generally by the characteristics of their social-technical-ecological environment.

4.2 Categories of Critical Infrastructure Dependencies

As Rinaldi, Peerenboom, and Kelly state, "it is clearly impossible to adequately analyze or understand the behavior of a given infrastructure [organization] in isolation from the environment or other infrastructures" (Rinaldi, Peerenboom, and Kelly, 2001). Critical infrastructure is thus in constant interaction with its environment, using and transforming inputs from the environment to provide outputs to the same environment (Figure 3).

The interactions between critical infrastructure and its environment can be characterized into three categories:

- *Upstream dependencies***.** The products or services provided to one infrastructure by another external infrastructure that are necessary to support its operations and functions.

- *Internal dependencies***.** The interactions among internal operations, functions, and missions of the infrastructure. Internal dependencies are the internal links among the assets constituting a critical infrastructure (e.g., an electric generating plant that depends on cooling water from its own onsite water well).

- *Downstream dependencies***.** The consequences to a critical infrastructure's consumers or recipients from the degradation of the resources provided by a critical infrastructure.

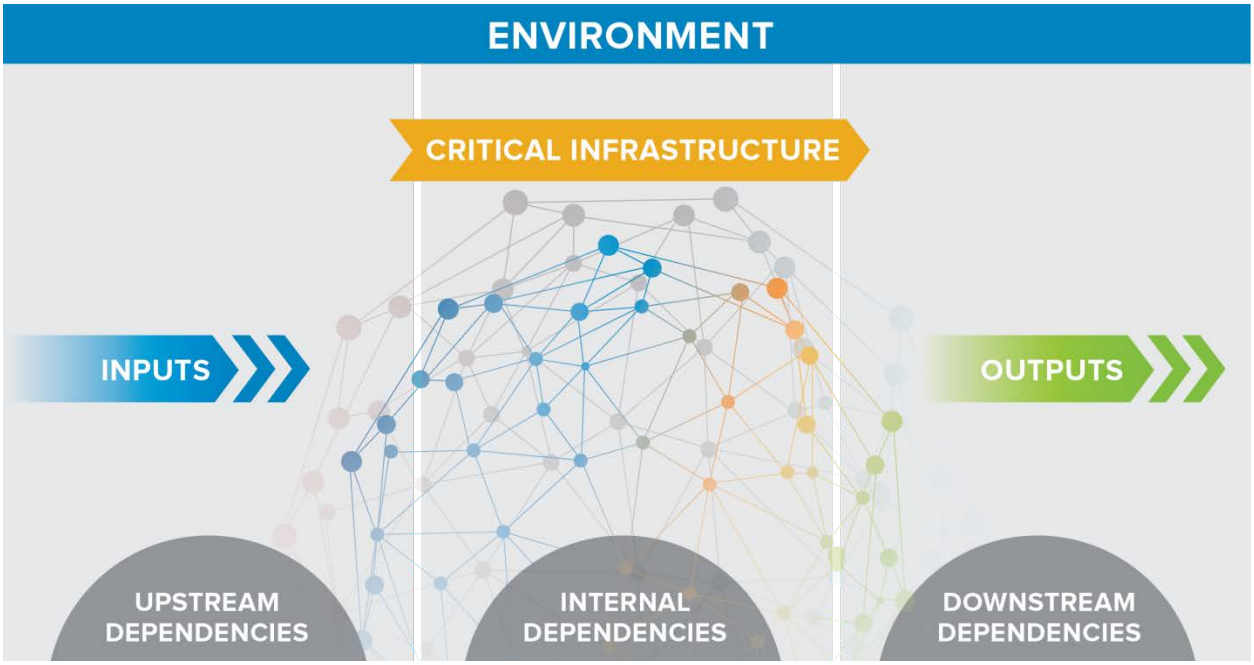

Figure 3: Interaction between Critical Infrastructure and Its Environment

4.3 Classes of Dependencies

Each category of dependency interactions can include one or more of four classes of dependencies (Rinaldi, Peerenboom, and Kelly, 2001):

- *Physical.* An infrastructure is physically dependent if the state of its operations is dependent on the material output(s) of another infrastructure through a functional and structural linkage between the inputs and outputs of two assets: a commodity (i.e., good or service) produced or modified by one infrastructure (an output) is required by another infrastructure for its operation (an input).

- *Cyber*. An infrastructure has a cyber dependency if its state of operation depends on information and data transmitted through the information infrastructure via electronic or informational links. Outputs of the information infrastructure are inputs to the other infrastructure, and the commodity passed among the infrastructure assets is information.

- *Geographic.* Infrastructure assets are geographically dependent if a local environmental event can create changes in the state of operations in all of them. A geographic dependency occurs when elements of infrastructure assets are in close spatial proximity (e.g., a joint utility right-of-way).

- *Logical.* An infrastructure is logically dependent if its state of operations depends on the state of another infrastructure via a mechanism that is not a physical, cyber, or geographic connection. Logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes.

4.4 Dimensions of Dependencies

In addition to the four classes of dependencies, the connections among critical infrastructure assets are multidimensional, adding to their complexity. Rinaldi, Peerenboom, and Kelly (2001) propose five dimensions to characterize dependencies (and interdependencies) among critical infrastructure (Figure 4).

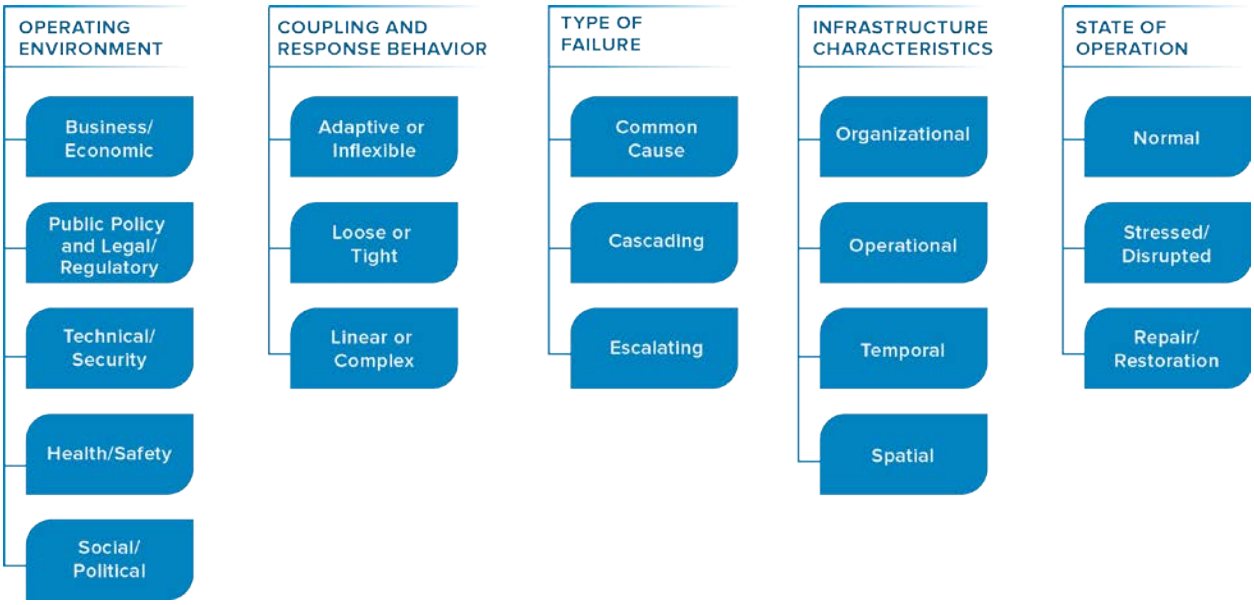

Figure 4: Dimensions of Dependencies (Adapted from Rinaldi, Peerenboom, and Kelly, 2001)

Several elements of the *operating environment* may affect critical infrastructure dependencies:

- Business/Economic – Economic and business concerns shape production scheduling and business agreements.
- Public Policy and Legal/Regulatory – Laws, regulations, or policies influence the growth and structure of organizations or bound the operating environment.
- Technical/Security – Security and technical requirements influence modes of operation.
- Health/Safety – Health and safety requirements and regulations affect the operation of associated systems.
- Social/Political – Social or political factors may influence the operational decisions of owners and operators.

Coupling and response behavior captures how a critical infrastructure would respond to a disruption to one or more of its dependencies:

- Adaptive versus inflexible response – An adaptive infrastructure is more likely to respond well to disturbances and continue to fulfill its missions. An inflexible infrastructure is incapable of learning from past experiences and unable to respond well to disturbances.

- Loose versus tight connection – In a loose connection, the state of one infrastructure is only weakly correlated to, or independent of, the state of the other. A tight connection is characterized by time-dependent processes that have little margin of error.

- Linear versus complex processes – In linear processes, infrastructures have expected and familiar production or maintenance sequences. In complex processes, infrastructures have unfamiliar sequences or unplanned and unexpected sequences.

The third dimension characterizes the *type of failures* affecting a dependency:

- Common cause – Disruption of two or more infrastructure at the same time.

- Cascading – Disruption of one infrastructure subsequently causes a disruption in the second infrastructure. This type of failure is also called the domino effect.

- Escalating – Disruption of one infrastructure exacerbates an independent disruption of a second infrastructure. This type of failure is also called the snowball effect.

Critical *infrastructure characteristics* themselves can influence the impact of a disruption of a dependency:

- Organization – Organizational and decisional structure and size of the organization (e.g., local, national, or international) affect how a disruption is managed.

- Operational – Emergency and business continuity measures affect the importance of impacts potentially generated by a failure.

- Temporal – The duration of outages and of recovery has substantial implications for the importance of impacts potentially generated by a failure.

- Spatial – The geographical extent of the critical infrastructure also affects the potential consequences generated by a failure. They will be different for a single asset or an asset that is a node of a system or supply chain.

Finally, the current *state of operations* may impact the types of good and services the critical infrastructure may depend upon as well as the extent of the impact upon the loss of a key good or service:

- Normal – Operations are optimal or near optimal levels. Major assets and supporting systems are fully operational and meet customer demands.

- Stressed or disrupted – Operations are at a reduced capacity due either to increased demand or damage/degradation of critical assets or supporting systems.

- Repair or restoration – Operations have been voluntarily or forcibly halted and repairs or new equipment are needed to resume operations.

Each dependency can therefore be defined by its category, class, and a combination of dimensions.

4.5 Approaches To Characterizing Dependencies

Each dependency has its own characteristics, therefore analyzing dependencies requires different approaches to successfully consider their category, class, and dimension(s). These approaches can generally be described as either top-down or bottom-up. Top-down approaches consist of analyzing a system in its entirety and then focusing on its component parts. Bottom-up approaches consist of analyzing the component parts of a system and building on this analysis to describe the system as a whole.

Figure 5 represents the concept of bottom-up and top-down approaches applied to critical infrastructure. Dependencies and interdependencies exist at individual levels (e.g., assets are interconnected with other assets) and between levels (e.g., assets are interconnected with facilities, facilities with sub-segments, and so on).[3]

Table 1 presents attributes of bottom-up and top-down approaches to critical infrastructure dependencies and interdependencies assessments.

A comprehensive analytic approach must address dependencies within and between all levels and combine both top-down and bottom-up approaches. Section 5 presents the elements that should be considered when analyzing the four classes of dependencies (i.e., physical, cyber, logical, and geographic) by categories (i.e., upstream, internal, and downstream). The other dimensions, presented in Figure 4, must also be considered. However, these dimensions (operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operations) are not specific to a given interaction-class dependency combination. They apply to all interactions and classes.

[3] The U.S. Department of Homeland Security (DHS) created the Infrastructure Data Taxonomy (IDT) to facilitate a common understanding of infrastructure terminology within the critical infrastructure protection community. The IDT organizes critical infrastructure in different levels (i.e., sector, sub-sector, segment, sub-segment, and asset) where each component within a level is defined by a distinct description. For example, a wastewater lift/pump station X (facility X) is categorized in the Water Sector, Wastewater Facility Sub-Sector, Wastewater Collection System Segment, and Lift/Pump Station Sub-Segment. Furthermore, facility X requires that operational and technical elements (assets) be functional.

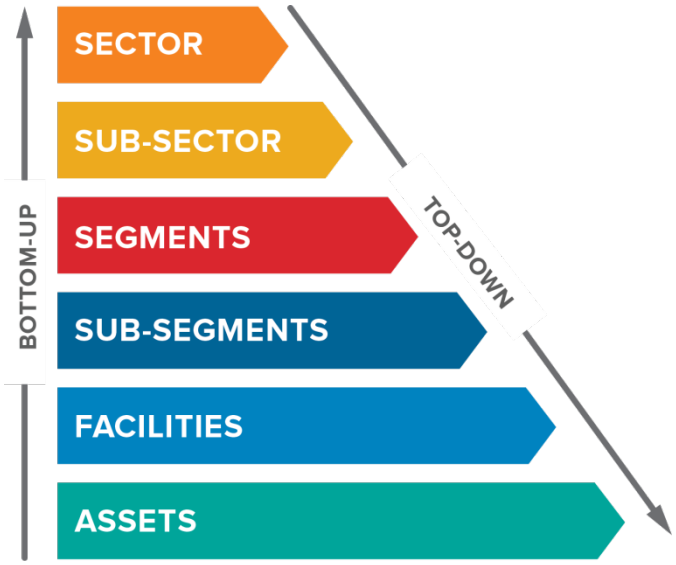

Figure 5: Bottom-up and Top-down Approaches

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

Bottom-Up Approach	Top-Down Approach
• Decentralized	• Centralized
• Target data collection at asset level	• Target data collection at sector level
• Based on actual operations and conditions	• Often based on models and large data sets
• Identify facility-level dependencies and interdependencies characteristics	• Identify system-level dependencies and interdependencies
• Goes from the specific to the global	• Goes from the global to the specific

This page intentionally left blank.

5 Analyzing Critical Infrastructure Dependencies and Interdependencies

Consideration of both dependencies and interdependencies is the basis of cascading and escalating failure analysis. Analyzing dependencies and interdependencies also requires the consideration of several elements such as interactions (between a critical infrastructure and its environment or within critical infrastructure), classes, and dimensions.

The following sections expand upon the fundamental considerations for analyzing dependencies. Similar considerations apply for the assessment of interdependencies.

5.1 Physical Dependencies

5.1.1 Definition

An infrastructure is physically dependent if there is a functional and structural linkage between the input(s) and output(s) of two assets: a commodity produced or modified by one infrastructure (an output) is required by another infrastructure for its operation (an input) (Figure 6).

Figure 6: Physical Dependencies

5.1.2 Elements To Consider

Several elements characterizing an asset's operations may be considered when addressing upstream, internal, and downstream physical dependencies (Table 2).

Table 2: Elements To Consider When Analyzing Categories of Physical Dependencies

Upstream	Internal	Downstream
• Information on resources and services required by an asset (e.g., an asset may require water at a certain volume, pressure, or quality, such as a chemical plant requiring water for its processes).	• Understanding of internal physical connections (e.g., the different processes using water in the chemical plant and their impacts on the plant's operations and missions).	• Impact on dependent assets upon the degradation of a physical resource provided (e.g., possible delays in the production of chemicals and how they would impact other assets).

5.2 Cyber Dependencies

5.2.1 Definition

An asset has a cyber dependency if its operation depends on information transmitted via electronic or informational links (Figure 7).

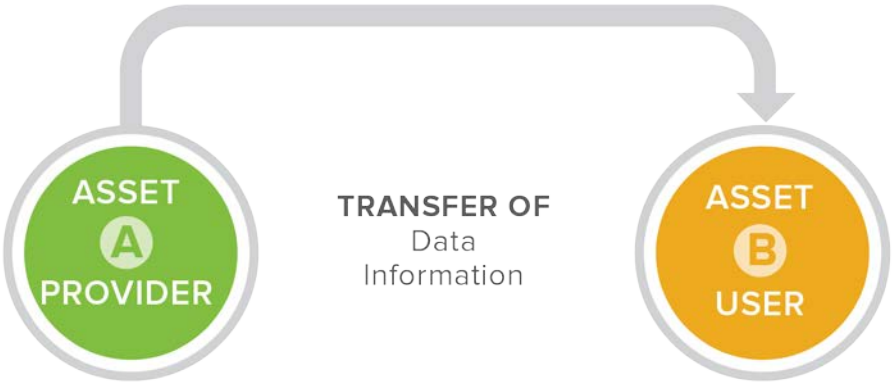

Figure 7: Cyber Dependencies

Transfer and processing of cyber resources (e.g., data, information) are principally done by two critical infrastructure sectors: Communications (transmission of data and information) and Information Technology (use and process data).

5.2.2 Elements To Consider

Similar to physical dependencies, several elements may be considered when addressing upstream, internal, and downstream cyber dependencies (Table 3).

Table 3: Elements To Consider When Analyzing Categories of Cyber Dependencies

Upstream	Internal	Downstream
• Information and data used by an asset—including the characteristics of the dependency, such as quality of service (QoS), which characterizes the degree of satisfaction of a user of the service (ITU, 2014).	• Internal cyber links (e.g., internal cyber response and recovery activities, availability of third-party assistance, reporting and forensic requirements).	• Impact on dependent assets upon the degradation of information or data provided (e.g., loss or degradation of service to customers, cybersecurity breaches resulting in loss, theft or destruction of data, economic and brand impacts).[a]

[a] Network performance, which is the ability of a network to provide the functions related to communications among users, includes confidentiality (i.e., protection of transmitted data from passive attacks), authentication, integrity (i.e., ensuring no message duplication, insertion, modification, reordering, and replay), non-repudiation (i.e., prevention of denying a transmitted message), access control, and availability (i.e., characterization of denial of service) (ITU, 2014).

5.3 Geographic Dependencies

5.3.1 Definition

Assets are geographically dependent if an event in the local environment can create changes in those assets' state of operations. A geographic dependency occurs when elements of infrastructure assets are in close spatial proximity (Figure 8).

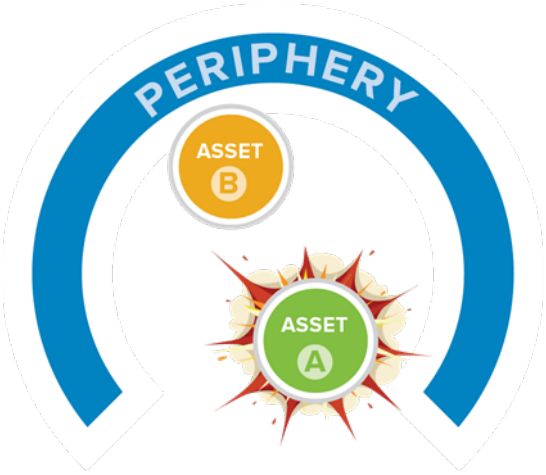

Figure 8: Geographic Dependencies

Geographic dependencies are unique in that they do not relate to the asset's operational requirements but rather to its location (e.g., a water pipe break may cause flooding that could impact the assets in the vicinity of the pipe). An event (e.g., the disruption of Asset A) can create changes in the operational state of Asset B located in the proximity (periphery) of Asset A.

5.3.2 Elements To Consider

The approach used to characterize physical or cyber dependencies cannot be used to address geographic dependencies which relate more to the locality of the asset considered than to the study of the resources required for its operations. Several elements may be considered when addressing geographic dependencies (Table 4).

Table 4: Elements To Consider When Analyzing Categories of Geographic Dependencies

Upstream	Internal	Downstream
• Identification and characterization of other critical infrastructure assets in the vicinity and how their failure may impact the asset's operations. • Consideration of natural elements (e.g., geology and geography) and urban spatial structure that may promote the propagation of consequences and ultimately affect the asset's operations.	• Consideration of internal dependencies combines similar elements to those used for characterizing both upstream and downstream dependencies.	• Identification and characterization of other critical infrastructure assets in the vicinity and how the degradation of an asset's operations would impact them.

5.4 Logical Dependencies

5.4.1 Definition

An infrastructure is logically dependent if its state of operations depends on the state of another infrastructure via a mechanism that is not a physical, cyber, or geographic connection. Logical dependency is attributable to human decisions and actions (Figure 9).

Logical dependencies occur at both operational and strategic decision levels. They relate more to business and strategic decisions that affect an asset's operations For example, Asset B is influenced by elements enacted by Asset A (e.g., geopolitical developments increase Asset A's operational risks, which in turn influences Asset B in the form of higher prices).

Figure 9: Logical Dependencies

5.4.2 Elements To Consider

The approach to address logical dependencies is similar to physical or cyber dependencies. Several elements may be considered when addressing upstream, internal, and downstream logical dependencies (Table 5).

Table 5: Elements To Consider When Analyzing Categories of Logical Dependencies

Upstream	Internal	Downstream
• How external factors may affect the asset's operations (e.g., financial market; human resources, which require certain skills, training, and expertise).	• Consideration of human reliability, human error, and cognitive systems.[a]	• Identification of policies, regulations, and other logical elements enacted by an asset that may impact other assets.

[a] Human reliability is the probability that an individual, a team, or a human organization will accomplish a mission, under given conditions, within acceptable limits, for a certain period. Human error is the behavior that exceeds acceptable limits. Resilience engineering and cognitive analysis may be used to address the consideration of human factors in sociotechnical interactions (Reason, 1990).

As demonstrated in the previous sections, identification and characterization of dependencies and interdependencies require the consideration of several characteristics (i.e., interactions, classes, and dimensions). Integration of these characteristics in a comprehensive approach is complex. Section 6 presents a roadmap for the development of dependencies and interdependencies analysis.

This page intentionally left blank.

6 Roadmap for Assessing Critical Infrastructure Dependencies and Interdependencies

The Risk and Infrastructure Science Center (RISC) at Argonne National Laboratory (Argonne) has defined four phases of development for dependency and interdependency assessment. Each phase of development varies in the level of data required, the type of analysis conducted, and the type of resulting products (Figure 10). This roadmap supports the development of a comprehensive assessment of critical infrastructure dependencies and interdependencies.

6.1 Phase 1 – Initial Estimate

Data collection in the Initial Estimate Phase consists primarily of researching open source information and provides a limited analysis. Such an analysis offers a general understanding of the functions of a critical infrastructure asset; however, it does not support an understanding of all dimensions of dependencies nor the real-time visualization of cascading and escalating failures. Table 6 is an overview of the elements characterizing the Initial Estimate Phase.

Table 6: Initial Estimate Phase: Level of Analysis

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

6.2 Phase 2 – Present

In the Present Phase, several research teams are developing data collection tools[4] and models, which allows for a more detailed analysis of critical infrastructure dependencies and interdependencies. Data collection and analyses start to address physical, cyber, and geographic dependencies and initiate the anticipation and visualization of first-order cascading failures. However, most of the existing tools and models operate in silos and have little interaction with complementary tools and models. Understanding logical dependencies and escalating failures is

[4] For example, Argonne has provided key technical support to a DHS program by developing a methodology for assessing critical infrastructure risk and resilience to a variety of natural and manmade hazards. Argonne also developed statistical and data-mining procedures to analyze and display data, including critical infrastructure dependencies, collected in easy-to-use "dashboards" (Argonne, 2014).

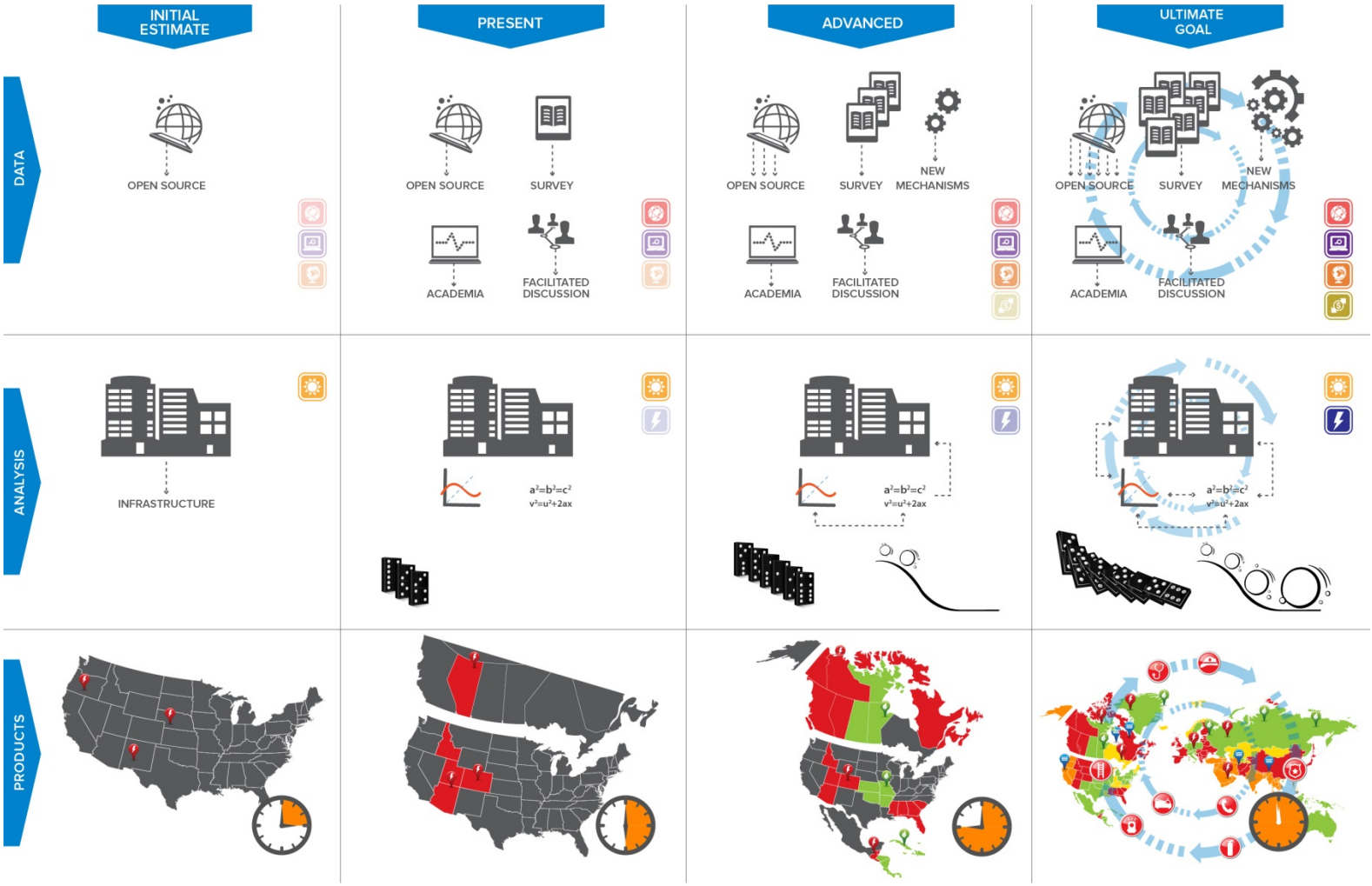

Figure 10: **Complexity of Analyses of Critical Infrastructure Dependencies and Interdependencies**

(In the top row, the pictograms in the lower right of each cell show the different types of dependency considered in each phase of development; from top to bottom, they are physical, cyber, geographic, and logical. In the middle row, the pictograms in the top right of each cell represent the states of operation considered: normal (sun) and degraded (lightning). The domino and snowballs represent the analysis of cascading and escalating failures. In the bottom row, the red pictograms in the cell at the far right (ultimate goal products) represent the different critical infrastructure sectors. Blue circle arrows in the last column represent the interactivity and iteration of the approach.)

still a challenge. Currently, few approaches consider how disruptions to facility dependencies could affect operations that are already degraded due to previous disturbances. Table 7 presents an overview of the elements characterizing the Present Phase of development.

Table 7: Present Phase: Level of Analysis

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

6.3 Phase 3 – Advanced

The Advanced Phase of development should consider all dimensions of critical infrastructure dependencies and interdependencies, as shown in Figure 4. This phase of development requires new data collection mechanisms and an integration of existing independent assessment tools and approaches. It transitions analysis centered on facilities to focusing on critical infrastructures systems. Table 8 presents an overview of the elements characterizing the Advanced Phase.

Table 8: Advanced Phase: Level of Analysis

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

6.4 Phase 4 – Ultimate Goal

The Ultimate Goal Phase contains a comprehensive understanding of all dependency and interdependency dimensions. It allows decision makers to anticipate and characterize, in real time, how all dependency and interdependency dimensions influence the resilience and protection of a critical infrastructure system, of a region, and, ultimately, of the Nation. Table 9 presents an overview of the elements characterizing the Ultimate Goal Phase of development.

Table 9: Ultimate Goal Phase: Level of Analysis

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

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

6.5 From the Present Phase to the Advanced Phase of Dependency Assessment

Moving from the Present Phase toward the Advanced Phase of development requires improving many existing capabilities to include the way data is collected and analysis capabilities, and will

lead to the development of new products to provide a more holistic understanding of dependencies and interdependencies.

6.5.1 Improvement in Data Collection

Data collection must be expanded to address all interactions and classes of dependencies. Current capabilities to gather information for physical, cyber, and geographic dependencies can be expanded upon and improved, while new data collection is required to start to understand logical dependencies. Improvement in data collection capabilities will build on existing tools and techniques but will also require the development of new collection mechanisms.

6.5.2 Improvements of Existing and Development of New Analysis Capabilities

Analysis capabilities should evolve toward an integration of methodologies and tools. This includes better integration and comprehension of cyber and physical dependencies, coupling and response behaviors, types of failures, as well as the operational characteristics and state of critical infrastructure assets as defined in Figure 4. It will be necessary to develop new approaches to integrate and combine existing mathematical and engineering models, and to identify uncertainty algorithms to extend and predict impacts of disruptions in dependencies. The improvement of analysis capabilities will be guided by the data collected, by the types of products required by stakeholders, and by the research and development conducted to better understand critical infrastructure dependencies and interdependencies.

6.5.3 Development of New Products

Moving toward an advancement of end products will require the enhancement and interactivity of existing visualization capabilities (e.g., dependency curves, geographic information system [GIS]), and the development of new products to meet the needs and requirements of stakeholders.

6.5.3.1 Dependency Curves

Dependency curves are created at the asset level and depict the impact of upstream physical dependencies and the asset's existing mitigation capabilities.[5] These curves allow visualization of the effects over time of the loss of a resource on an organization's functions (Figure 11).

[5] The RISC at Argonne has developed an interactive dependency dashboard using the elements presented in Figure 11; this dashboard allows for interactive changes to be reflected.

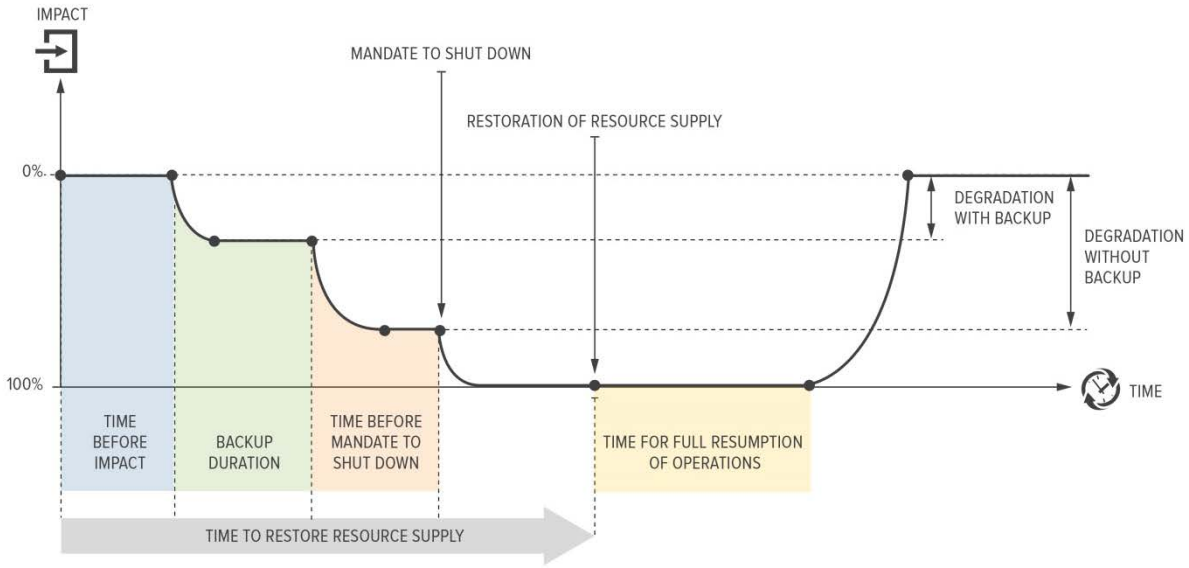

Figure 11: Dependency Curves Component (Petit, Wallace, and Phillips, 2014a)

While initially conceived and developed for an individual asset, the dependency curve concept can be expanded for systems. The bottom-up dependency curves can be combined with a top-down approach that captures global interactions among several subsystems (e.g., critical infrastructure, population, economy, and government) to better understand the resilience of a region (Petit, Wallace, and Phillips, 2014b). Improvements to dependency curves to facilitate this combination include:

1. *Enhance the interactivity of the dependency curves.* Current assumptions made for generating the curves can be modified and updated, such as reviewing the method used to gather information, improving the user interface, and combining the curves with other analysis tools.

2. *Include effects based on an organization's environment.* Currently, the curves only address the interface between the inputs and the asset. To be fully effective, the dependency curves should be integrated into a holistic methodology, including how an asset affects its environment.

3. *Incorporate other types of dependencies and interdependencies.* The dependency curves are generated for operational (physical and cyber) dependencies that have a direct impact on an organization's daily operations. Future developments should include geographic and logical dependencies to improve understanding of the interconnections among assets and organizations and to anticipate potential cascading and escalating failures.

4. *Integrate the dependency curves in an emergency operations capability.* The ultimate goal of generating dependency curves is to better understand and anticipate the

consequences of an incident and to support incident management activities. Therefore, generating dependency curves can be the first step in enhancing emergency operations capability (Petit, Wallace, and Phillips, 2014a).

6.5.3.2 GIS Visualization Capabilities

Development of GIS visualization capabilities is vital for the analysis of critical infrastructure dependencies and interdependencies, especially in visualizing cascading and escalating failures at the regional level. This GIS visualization capability should integrate the results from the analysis methodologies for generating cascading, escalating, and common-cause failure curves to address second- and third-order dependencies (Verner and Petit, 2013). Similar concepts have been incorporated into the DOMINO modeling and mapping tool developed by the *Centre Risque & Performance* (CRP) of the Montreal Polytechnic School and should be considered (Robert, Morabito, and Cloutier, 2012).

Section 7 presents an assessment framework to address critical infrastructure dependencies and interdependencies.

This page intentionally left blank.

7 Dependency and Interdependency Assessment Framework

To manage all interactions, classes, and dimensions of dependencies and interdependencies, as well as addressing the entire resilience management spectrum, a scalable approach is needed. Such an approach can be tailored toward and applied on an asset, system, network, or functional basis, depending on the decisions it is intended to support, stakeholder needs and requirements, and the nature of the related infrastructure. Currently, no such scalable approach or standardized capability (or combination of capabilities) exists. In response to this void, the RISC proposes a general framework for assessing critical infrastructure dependencies and interdependencies (Figure 12).

The general concept behind a critical infrastructure dependency and interdependency assessment framework is to build a flexible approach that can evolve over time and allow the implementation of innovative capabilities that will reflect the evolution of technical capabilities and of critical infrastructure protection and resilience policies. This assessment approach built around the RISC's expertise and capabilities is the result of a proactive and collaborative approach promoting the development of better risk management and resilience assessment solutions. Four main elements are combined for supporting the analysis.

- *Expertise*—multidisciplinary and includes knowledge of soft (e.g., management and socioeconomic sciences) and hard (e.g., engineering and operations research) aspects influencing critical infrastructure dependencies and interdependencies, and ultimately resilience and protection.

- *Partnerships*—includes collaborations with public and private sector partners as well as research organizations. These partnerships incorporate capabilities (e.g., expertise and tools) that do not exist within the RISC.

- *Data*—includes existing databases (i.e., commercial and owned by stakeholders) and capabilities to conduct open source research and develop collection surveys specific to the analysis required.[6]

- Tools—combines mathematical and engineering models and metrics for identifying and characterizing dependencies and interdependencies, and GIS capabilities for visualizing them.

The analysis module constitutes the core of the integrated approach, as highlighted in Figure 12. The approaches used in the analysis module will be driven by the type of end products needed for resilience assessment and risk management decision support. Stakeholder goals and objectives are as vital as the four main elements mentioned above to support the analysis. These components, when combined, are designed to provide the stakeholder with a thorough picture to address the decision situation. The resulting products can include asset-specific options for

[6] Depending on the type of analysis, critical infrastructure information would require specific protection, such as that provided by the Protected Critical Infrastructure Information Program (DHS, 2014).

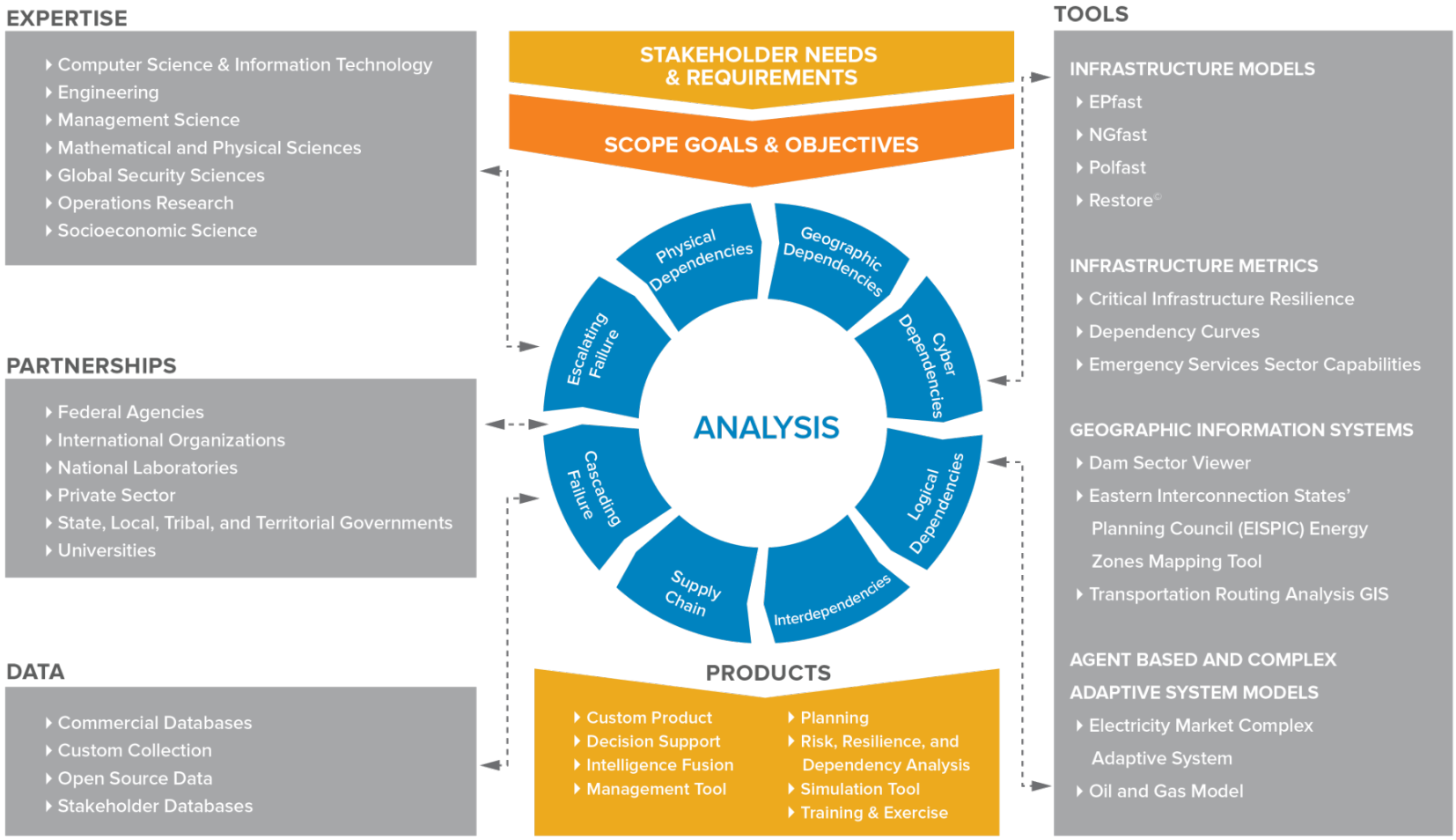

Figure 12: Critical Infrastructure Dependencies and Interdependencies Assessment Framework

consideration provided to owners and operators to improve asset or system resilience and protection, as well as higher-level resilience enhancement options that call for the establishment of cross-sector, cross-jurisdictional collaborative working groups to develop and implement mitigation strategies across a region. The holistic knowledge of critical infrastructure dependencies and interdependencies can be used in a variety of ways, such as pre-event planning, or during emergency operations as an event is unfolding. This information could be operationalized to support (1) information sharing among stakeholders, and (2) State and local prioritization of critical-infrastructure-related response and recovery activities. Anticipation of cascading, escalating, and common-cause failures and potential impact areas can support the development of coherent emergency measures. It can also assist in defining the time available before an asset or system is affected by an event and the time needed to implement specific mitigation measures.

To manage dependencies and interdependencies in the context of critical infrastructure resilience and risk management, the iterative and scalable dependencies and interdependencies framework can be integrated into existing risk and resilience assessment frameworks to answer specific stakeholders' requirements.

This page intentionally left blank.

8 Conclusion

Critical infrastructure dependencies and interdependencies are complex elements to identify and analyze. They are characterized by different interactions (i.e., upstream, internal, and downstream), classes (i.e., physical, cyber, logical, and geographic), and dimensions (i.e. operating environment, coupling and response behavior, type of failure, infrastructure characteristics, and state of operation). They influence all components of risk (threat/hazard, vulnerability, resilience, and consequence), can themselves be a threat or hazard, affect the resilience and protection performance of critical infrastructure, and lead to the propagation of cascading and escalating failures. It is essential to integrate dependencies and interdependencies into risk and resilience methodologies. A data-driven capability that operationalizes the analysis of dependencies and interdependencies would not only provide an unprecedented level of situational awareness, it would also enable decision makers to anticipate disruptions. To achieve this ultimate goal, the development of a comprehensive and interactive assessment of critical infrastructure dependencies and interdependencies, requires the combination of multiple areas of expertise (e.g., engineering, social sciences, business continuity, and emergency management) in an adaptive and flexible assessment framework.

This page intentionally left blank.

9 References

Argonne (Argonne National Laboratory), 2014, *Better Infrastructure Risk and Resilience*, http://www.dis.anl.gov/projects/ri.html, accessed December 9, 2014.

ASIS (American Society for Industrial Security), 2009, *The Organizational Resilience Standard (ASIS SPC.1-2009)*, http://organizational-resilience.com/OrganizationalResilienceStandard.htm, accessed December 9, 2014.

BSI (British Standards Institute), 2010, *BS 25999 Business Continuity*, BSI America, http://www.bsiamerica.com/en-us/Assessment-and-Certification-Services/Management-systems/Standards-and-Schemes/BS-25999/, accessed December 9, 2014.

Carlson, L., G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield, 2012, *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, Ill., USA, http://www.dis.anl.gov/pubs/72218.pdf, accessed December 9, 2014.

DHS (U.S. Department of Homeland Security), 2013, *NIPP 2013 – Partnering for Critical Infrastructure Security and Resilience*, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf, accessed December 9, 2014.

DHS, 2014, *Protected Critical Infrastructure Information (PCII) Program*, http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program, accessed December 9, 2014.

FEMA (Federal Emergency Management Agency), 2014, *The Voluntary Private Sector Preparedness Program – PS-Prep™ & Small Business Preparedness*, http://www.fema.gov/voluntary-private-sector-preparedness-program-ps-preptm-small-business-preparedness, accessed December 9, 2014.

ITU (International Telecommunication Union), 2014, *Quality of Service and Network Performance Handbook*, Telecommunication Standardization Sector of ITU (ITU-T), 109 pp.

ISO (International Organization for Standardization), 2012, *ISO 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements*, http://www.iso.org/iso/catalogue_detail?csnumber=50038, accessed December 9, 2014.

NFPA (National Fire Protection Agency), 2013, *NFPA® 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs 2013 Edition*, NFPA, Quincy, Mass., USA.

Petit, F.D., G.W. Bassett, W.A. Buehring, M.J. Collins, D.C. Dickinson, R.A. Haffenden, A.A Huttenga, M.S. Klett, J.A. Phillips, S.N. Veselka, K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom, 2013, *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-13-04, Argonne, Ill., USA, http://www.ipd.anl.gov/anlpubs/2013/11/77931.pdf, accessed December 9, 2014.

Petit, F., K. Wallace, and J. Phillips, 2014a, "Interactive Dependency Curves for Resilience Management," *Journal of Business Continuity & Emergency Planning*, Henry Stewart Publications, Vol. 8, No. 2, pp. 141–155.

Petit, F., K. Wallace, and J. Phillips, 2014b, "An Approach to Critical Infrastructure Resilience," *The CIP Report*, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, January, Vol. 12, No. 7, pp. 17–20, Washington, D.C., USA, http://cip.gmu.edu/wp-content/uploads/2013/06/January-2014_Resilience.pdf, accessed December 9, 2014.

Phillips, J.A., G.W. Bassett, W.A. Buehring, J.L. Carlson, R.G. Whitfield, and J.P. Peerenboom, 2012, *A Framework for Assessing Infrastructure Risk*, M4-I Resilience Evaluation Approaches for the Analysis of Complex Systems, Risk Analysis: Advancing Analysis, Society for Risk Analysis, 2012 Annual Meeting, December 9–12, San Francisco, Calif.

Reason, J., 1990, *Human Error*, Cambridge University Press, 305 pp.

Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, 2001, "Complex Networks, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001, pp. 11–25, http://user.it.uu.se/~bc/Art.pdf, accessed December 9, 2014.

Robert B., L. Morabito, and I. Cloutier, 2012, "Modeling and Coordinating Interdependent Critical Infrastructures in Montre," *The CIP Report*, Center for Infrastructure Protection and Homeland Security, Vol. 10, No. 11, May, Washington, D.C., USA, http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_May2012_InternationalCriticalInfrastructure.pdf, accessed December 9, 2014.

The White House, 2013, *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21, Office of the Press Secretary, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed December 9, 2014.

Verner, D., and F. Petit, 2013, "Resilience Assessment Tools for Critical Infrastructure Systems," *The CIP Report*, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, December, Vol. 12, No. 6, pp. 2–5, Washington, D.C., USA, http://cip.gmu.edu/wp-content/uploads/2014/01/December-2013_Resilience.pdf, accessed December 9, 2014.

Global Security Sciences Division
Argonne National Laboratory
9700 South Cass Avenue, Bldg. 221
Argonne, IL 60439-4854

www.anl.gov