Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies

Lawrence Paul Lewis, JD,

Program Lead for Technology Implementation, Decision and Infrastructure Sciences Division, Energy and Global Security Sciences Directorate, Argonne National Laboratory, Argonne, IL USA

Frédéric Petit, PhD,

Principal Infrastructure Analyst and Research Scientist, Decision and Infrastructure Sciences Division, Energy and Global Security Sciences Directorate, Argonne National Laboratory, Argonne, IL USA

Abstract

Critical infrastructure systems provide vital resources and services to the population, commercial ventures, industrial operations, government entities, as well as to other interdependent critical infrastructure. These infrastructure systems depend upon extensive interconnections with one another; thus, the consequences resulting from one infrastructure dysfunction can propagate across infrastructure systems, generating cascading and escalating failures that could scale up a crisis. Critical infrastructure interdependencies are therefore fundamental considerations when assessing the resilience of infrastructure assets, systems, and, ultimately, the communities they serve. Expanding our understanding of how critical infrastructure systems operate in concert is essential in order to anticipate potential disruptions, manage the impacts, and develop adaptation measures for future conditions. Managing the dynamics and complexities of critical infrastructure interdependencies requires the combination of top-down and bottom-up analysis techniques in a flexible and adaptive approach. This paper proposes a critical infrastructure interdependency analysis framework and illustrates its application in Puerto Rico following Hurricane Maria. This framework leverages system-level and asset-level infrastructure analyses to illustrate potential cascading and escalating failures, as well as to identify and prioritise potential resilience strategies. The Puerto Rico case study also elucidates the elements and required conditions to operationalise critical infrastructure interdependency analysis in all phases of risk and emergency management, and in the broader perspective of long-term adaptation planning and sustainable development.

Keywords: critical infrastructure interdependencies; complex systems; systemic risk assessment; disaster risk reduction; resilience strategies

1 Introduction

Nations and communities across the world face significant challenges in formulating and implementing effective strategies to address the risks posed by myriad natural and man-made hazards. Although protecting life before, during, and after disasters is the highest priority, the potential impacts of these events to critical infrastructure assets, systems, and operations that enable the basic functioning of community institutions, public health systems, and economic activities are also of grave concern. Enhancing the resilience of critical infrastructure is recognised as an urgent goal in the *Sendai Framework for Disaster Risk Reduction* as well as in other international development and disaster management frameworks. However, successfully operationalising this goal requires that these strategies also be informed by the inherent system interdependencies each infrastructure sector shares with other infrastructure sectors, supply chains, and governance structures.

These represent the "system-of-systems" that comprehensively characterise critical infrastructure resilience. The consequences of disasters may thus extend well beyond the individual infrastructure systems directly affected by an event, and carry the potential risks of cascading and escalating failures across other interdependent infrastructure systems and jurisdictional boundaries. A more thorough understanding of the complex interactions among critical infrastructure is therefore essential in preparing for, responding to, and recovering from disasters. Critical infrastructure interdependency analysis could support national and local stakeholders in making better informed and more holistic solutions to address the risks they may face.

The body of this paper is subdivided into four sections. Section 2 provides a general overview of the main characteristics and dimensions of critical infrastructure interdependencies, and how these elements influence disaster risk reduction and resilience strategies. Section 3 proposes a critical infrastructure interdependency analysis framework combining top-down (i.e., system-level) and bottom-up (i.e., asset-level) approaches to inform resilience strategies. Section 4 discusses the application of this analysis framework to drive recovery investments in Puerto Rico after Hurricane Maria. Finally, Section 5 summarises how the analysis framework can be used to operationalise the consideration of critical infrastructure interdependencies in enhancing local, national, regional, and global resilience.

2 Theoretical Underpinnings of Critical Infrastructure Interdependency Analysis

The term “critical infrastructure” has varying yet largely parallel definitions around the world (Public Safety Canada, 2018a; USDHS, 2018a; Australian Government, 2010; European Commission Migration and Home Affairs, 2019; UNISDR, 2017a). Although the definitions and taxonomies may differ, this term is generally used by governmental agencies to describe assets providing resources and services that support significant societal functions. The importance of societal functions, and therefore of the critical infrastructure assets supporting them, may be determined by emergency management situations or societal goals (Swedish Emergency Management Agency, 2014). Critical infrastructure encompass not only technical assets but also functional sectors and essential services (Pescaroli and Alexander, 2016). It is therefore important to prepare, invest in, and manage all categories of critical infrastructure, including lifeline networks (e.g., energy, water, communications, and transportation) and life support networks (e.g., emergency services, public health, and medical services), for the potential conditions of both normal operations and emergency situations.

Although the term “resilience” has been defined in several fields (e.g., ecology, economics, and computer science) since the 1970s, it is only recently that this concept has been incorporated into the management of critical infrastructure systems (Dahlberg, et al., 2015). The traditional risk management approach for critical infrastructure emphasises an all-hazards approach, taking into account both natural hazards and man-made threats. It has evolved from a pure vulnerability and physical security approach to a more comprehensive consideration of the missions and functioning of critical infrastructure. It is still important to “protect” critical infrastructure from risks, but infrastructure owners and operators increasingly recognise the importance of ensuring the resilience of their operations in light of the dynamic socio-technical systems they support (Dahlberg, et al., 2015). This paradigm shift in traditional risk management to include resilience is fundamentally based on the observation that it is impossible to be protected against all risks or to predict what is by definition unpredictable (Porod, et al., 2012).

The term “risk” is traditionally defined as a function of three elements: the hazards and threats to which an asset is susceptible; the vulnerabilities of the asset to the hazard or threat; and the consequences potentially generated by the degradation of the asset (USDHS, 2010). If risk is a function of hazards, threats, vulnerabilities, and consequences, the challenge is to define how resilience fits into the determination of risk. Resilience, as

defined by the U.S. Department of Homeland Security, is the “ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions” (USDHS, 2010). The U.S. Department of Homeland Security lexicon also states that “[r]esilience can be factored into vulnerability and consequence estimates when measuring risk” (USDHS, 2010). In order to manage critical infrastructure effectively from a “risk perspective,” it is necessary to form an approach that is not based exclusively on protection and prevention. Risk and emergency management must include a balance between preparedness, mitigation, response, and recovery (Petit, 2018).

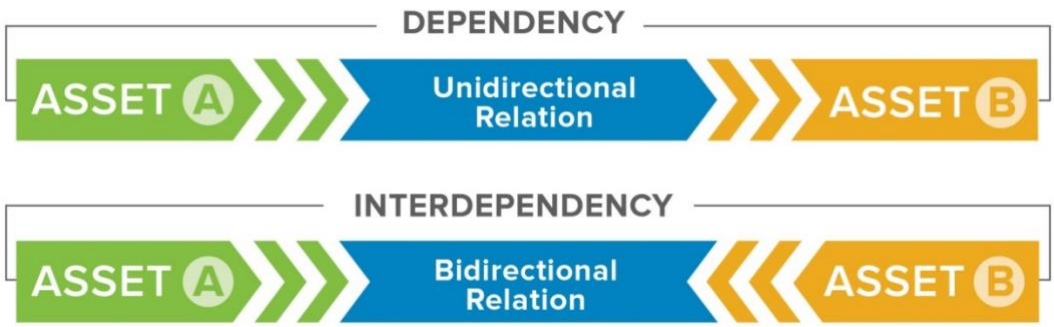
Risk management and resilience management strategies are therefore inseparable and complementary. Risk management strategies are implemented to mitigate known threats and resilience management strategies are implemented in case the protection measures are not sufficient to prevent negative consequences resulting from known or unknown threats (Petit, 2018). Furthermore, both scholarship and experience also point to the need to consider the growing complexity of large socio-technical systems and combinations of organisational and technical failures to reduce risks and enhance resilience (Pescaroli and Alexander, 2016; Curt and Tacnet, 2018).

The tendency for critical infrastructure sectors to be managed and regulated in isolation from one another hampers the understanding of challenges arising from interdependencies (Flynn, 2015). Resilience management approaches need to move beyond developing business continuity and emergency management plans that focus mainly on risks to individual facilities and assets, and toward developing plans that consider regional resilience management capabilities and integrate elements that may be outside of one organisation’s control. It is not sufficient to have generators, fuel storage, and refuelling priority to prepare for a power outage. Rather, enhancing the resilience of critical infrastructure involves the promotion of regional coordination, the definition of restoration priority, and the reallocation of resources to limit consequences and channel potential cascading failures.

Assuring critical infrastructure continuity of operations requires a consideration of the complexity of cross-sector connections and an understanding of the diversity of hazards and threats they could face. Critical infrastructure assets are part of a “system-of-systems” and cannot be considered independently of their operating environment. As described by Rinaldi, Peerenboom, and Kelly (2001): “it is clearly impossible to adequately analyse or understand the behaviour of a given infrastructure in isolation from the environment or other infrastructures.” These interconnections mean that disruption or failure of one element can lead to cascading failures in others. Interdependencies among infrastructure systems can result in important economic and physical damage on a citywide, regional, or even national or international scale.

An infrastructure interdependency is generally defined as a bidirectional relationship between two assets in which the operations of both assets affect each other. An interdependency is effectively a combination of two dependencies; therefore, understanding an interdependency requires analysis of the one-way dependencies that comprise it. Figure 1 illustrates dependency and interdependency between two critical infrastructure assets.

Figure 1: Dependency and Interdependency between Two Assets (Petit, et al., 2017)



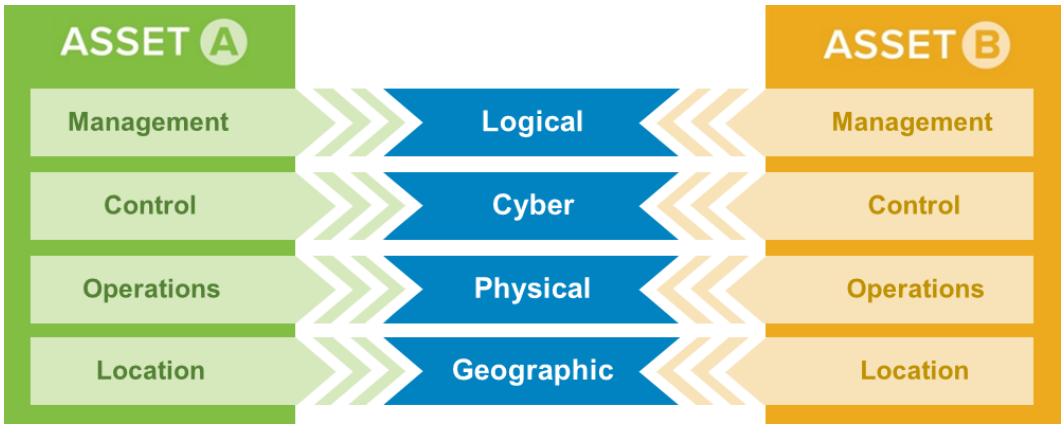
As defined by Rinaldi, Peerenboom, and Kelly (2001), it is possible to differentiate four classes of dependencies and interdependencies based on the nature of resources transiting between the systems and the level of interactions (Rinaldi, et al., 2001; Petit, et al., 2015):[1]

- Physical dependencies among infrastructure assets characterise the connections at operational levels relating to the transfer of goods or resources (e.g., electric power, water, chemical products).
- Cyber dependencies among infrastructure assets characterise the connections at control levels relating to the transfer of information or data.
- Unlike other dependency classes, geographic dependencies do not characterise usual functional connections; rather, they depict the collocation of infrastructures and the potential that the disruption of one infrastructure asset may have an impact on other infrastructure assets located nearby.
- Logical connections were originally defined as connections that do not fit under one of the three other categories (i.e., physical, cyber, or geographic). These characterise the decisional connections at strategic levels relating mostly to the management of human and financial resources.

[1]It should be noted that other taxonomies exist to categorise critical infrastructure interdependencies. Ouyang (2014) presents several examples of existing taxonomies. However, the taxonomy developed by Rinaldi, et al. (2001) remains the most widely used in Homeland Security. This taxonomy also has the advantage to be the most useful and comprehensive, as each of the elements identified in subsequent taxonomies can be found in the classes and dimensions established in this taxonomy defined in 2001.

These four classes characterise the functional organisation of critical infrastructure systems: physical interdependencies relate to connections through civil infrastructures (e.g., pipes, lines); cyber interdependencies relate to industrial control systems (ICS) and supervisory control and data acquisition (SCADA); geographic interdependencies relate to the location of infrastructure assets in close proximity; and logical interdependencies relate to the proactive and reactive decision-making of interdependent infrastructure managers. Figure 2 illustrates the four classes of interdependencies between two infrastructure assets.

Figure 2: Interdependency Classes



The required data inputs, relevant qualitative and quantitative analytical techniques, and resulting products from dependency and interdependency analyses may differ across these four classes.

A critical infrastructure is in constant interaction with its environment, using and transforming inputs (i.e., critical resources and services) from the environment in order to provide outputs to the same environment. Several dimensions of its environment may directly affect the operations of a critical infrastructure (Rinaldi, et al., 2001):

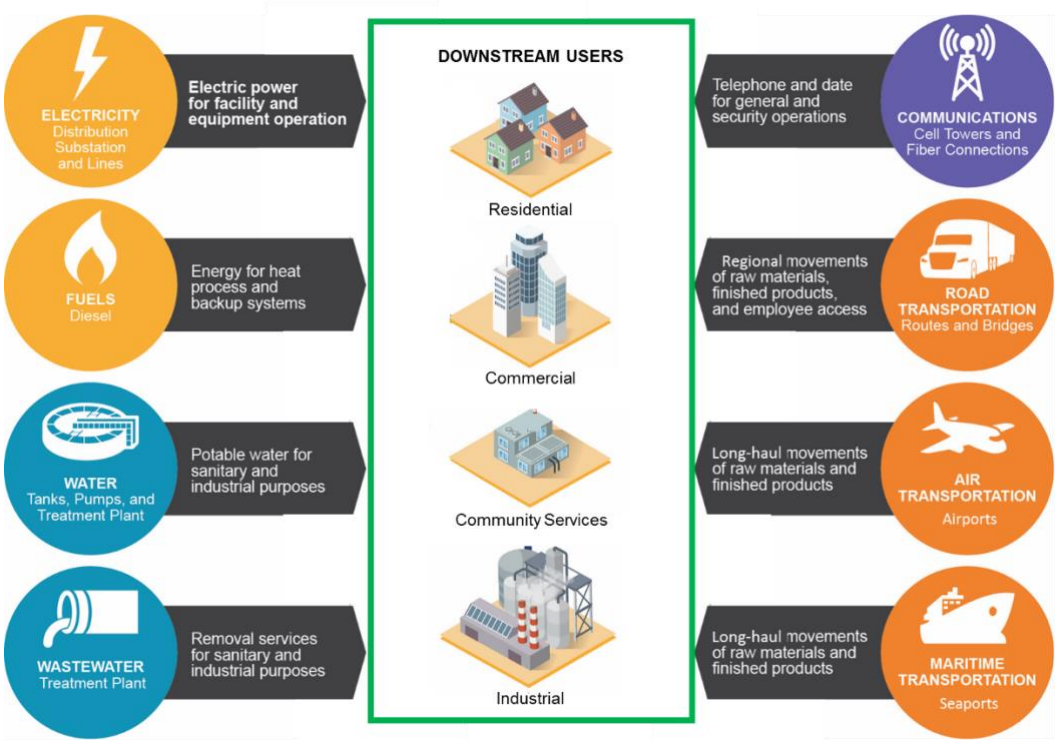
- Operating environment, including broader business, policy, legal, security, safety, and political considerations;
- Coupling and response behaviour(s) for critical infrastructure following a disruption;
- Type(s) of failure affecting critical infrastructure;
- Infrastructure characteristics that influence the effects of a disruption; and
- State of operations for critical infrastructure (e.g., normal day-to-day operations, degraded operations).

Infrastructure dependency can also be characterised by the relative position of critical infrastructure assets and their proximity to dependent users. An infrastructure asset is positioned “upstream” from entities to which it provides resources or services. The recipients of those resources or services are therefore “downstream,”

and may include traditional customer bases such as residential neighbourhoods, commercial zones, community service providers, and industrial facilities, as well as other infrastructure assets that depend on these resources and services in order to operate (Petit, et al., 2015). For example, an upstream electric utility distribution substation may provide electricity service to both downstream residential customers and downstream water utility pump stations that depend on electricity to provide water service within the same community.

The proximity of connections between infrastructure and its users may be either direct or indirect. A "first-order" dependency describes a relationship in which an infrastructure asset provides a direct service or resource to a user. This provision could be through a specific connection delivering the service or resource, and by which the operation of the upstream infrastructure asset will have an immediate impact on downstream users. Figure 3 illustrates a notional example of the first-order dependencies of downstream users on lifeline infrastructure, which includes electricity, fuels, water, wastewater, communications, and transportation sectors.

Figure 3: Notional Illustration of First-Order Dependencies on Lifeline Infrastructure[2]

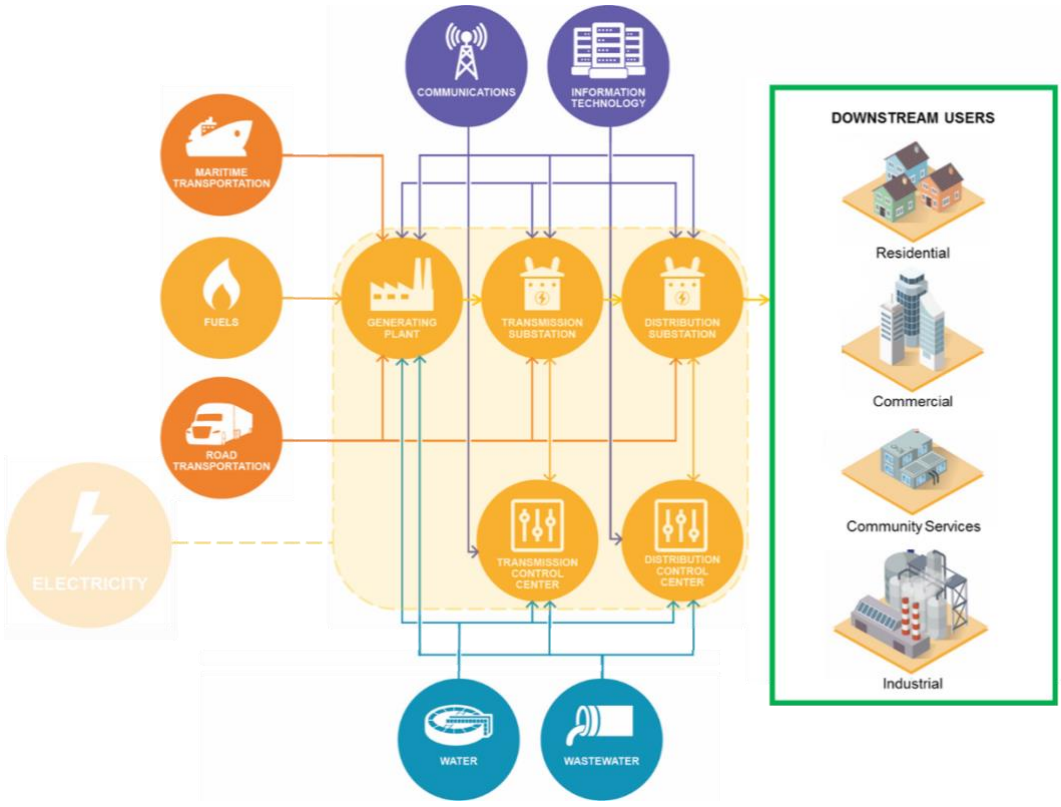


A "second-order" dependency describes a relationship in which an infrastructure asset indirectly supports a downstream entity. These include upstream interactions between interdependent infrastructure

[2]Figure adapted from USDHS. 2018. *Puerto Rico Infrastructure Interdependency Assessment*. May 2018. Prepared by Argonne National Laboratory. Available upon request.

assets that are critical for the operation of one or more assets that ultimately provide direct services or resources to a user. Figure 4 illustrates a notional example of second-order dependencies of downstream users, focusing on those that are critical to supporting electricity infrastructure operations. Each of the electricity infrastructure assets (represented within the shaded area in the figure) has first-order dependencies on services or resources from other infrastructure sectors (represented by arrows in the figure) that must be satisfied in order for those electricity infrastructure assets to operate. These connections are therefore second-order dependencies of the downstream users, without which their first-order dependency on electricity could be disrupted.

Figure 4: Notional Illustration of Second-Order Dependencies on Lifeline Infrastructure[3]



Characterising infrastructure in terms of relative position and proximity enables analysts to develop network models representing the complex interactions between assets, systems, and operations across infrastructure sectors. These network models may be used to characterise how a change in upstream infrastructure operations may propagate cascading and escalating failures both within a given infrastructure sector or across infrastructure sectors. Understanding the different orders of dependencies and

[3]Figure adapted from USDHS. 2018. *Puerto Rico Infrastructure Interdependency Assessment*. May 2018. Prepared by Argonne National Laboratory. Available upon request.

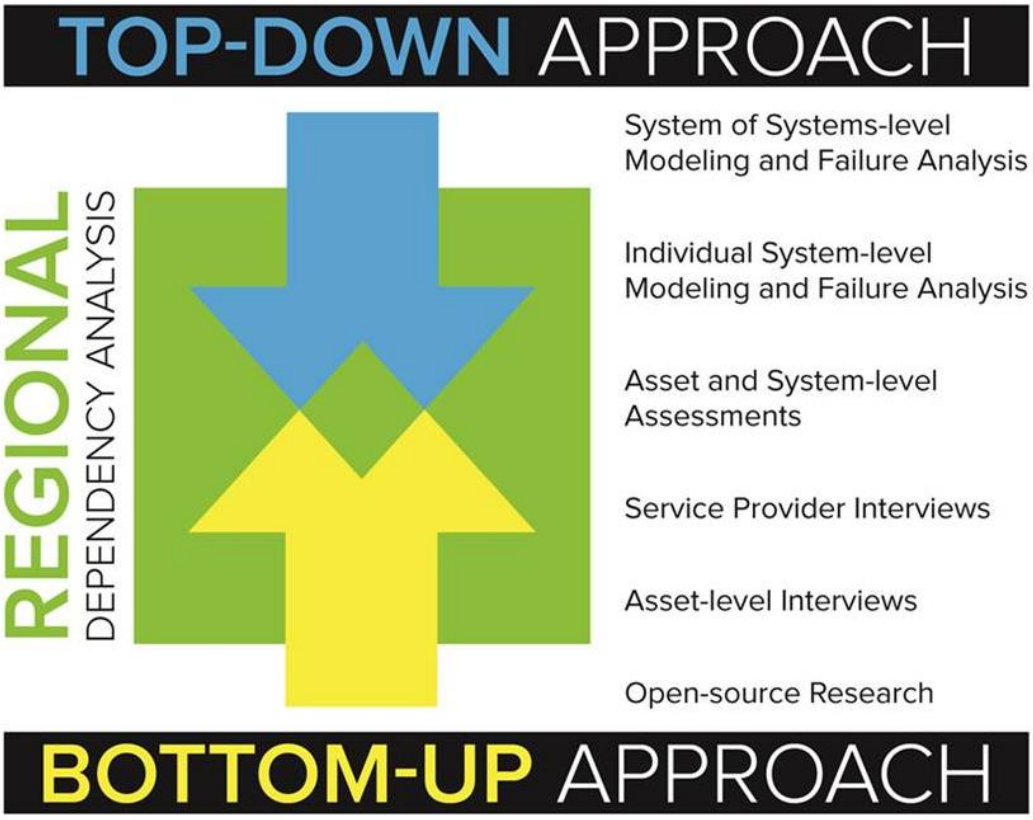
interdependencies is particularly important to identify potential investment targets that will have the greatest cumulative effect on cross-sector infrastructure resilience and, ultimately, community resilience.

Infrastructure interdependencies are complex and dynamic, and it is important to assess and visualise consequence propagation to manage cascading failures and avoid escalating failures that could potentially scale up a crisis (UNISDR, 2017b). Infrastructure interdependency analysis can be complicated, time consuming, and costly. This, in turn, can limit the ability of stakeholders to understand and use this information to make risk-informed decisions that enhance resilience. To manage these complexities, the infrastructure community is increasingly using a systems science approach 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 help determine where to conduct more detailed site assessments, focusing only on the most critical asset-level components (Carlson, et al., 2012).

A systems approach helps to establish the appropriate scope of analysis, as well as the specific assets and subsystems for which resilience-related information should be collected (Carlson, et al., 2012). Using this approach, an analysis considers the high-level context (e.g., a geographic region or an economic sector) and the associated states of these systems, ultimately represented by the most critical assets that will inform the scope and focus of a resilience assessment.

A systemic infrastructure interdependency analysis requires the combination of top-down and bottom-up data collection and assessment methods (Figure 5).

Figure 5: Top-down and Bottom-up Approaches to Regional Dependency Analysis (Petit, et al., 2017)



Integration of infrastructure interdependency analysis in risk management and regional resilience strategies leads to a better understanding of how critical infrastructure systems operate, anticipation of potential cascading and escalating failures, and identification of possible adaptation measures. Increasing critical infrastructure awareness and integrating interdependency analysis into risk management will support the development of resilience-driven strategies adapted to local needs (UNISDR, 2017b).

Even if significant efforts have been made to better understand and analyse infrastructure interdependencies, there is still a limited understanding of the critical infrastructure system operations and the possible resulting cascading failures. Emergency planners need to move beyond crafting disaster response procedures that focus only on managing immediate life safety issues and toward developing recovery plans that enable the rapid restoration of essential and normal infrastructure functions. This evolution of critical infrastructure system management requires developing new tools to characterise infrastructure interdependencies and identify the systems, assets, and functions that are truly critical for regional resilience.

The next section presents a critical infrastructure interdependency analysis framework that has been developed to combine top-down and bottom-up infrastructure interdependency analysis to inform regional resilience strategies.

3 Critical Infrastructure Interdependency Analysis Framework

Analysing infrastructure interdependencies to improve regional resilience requires a scalable approach that can be tailored based on decision support needs, stakeholder requirements, and relevant critical infrastructure assets. Stakeholder goals, available data, time, budget, and analytical sophistication are all combined to influence the scope and complexity of potential interdependency analysis. Thus, the core concept of the critical infrastructure interdependency analysis framework is to establish a flexible approach that covers a broad spectrum of options, starting with relatively simple and tightly-scoped efforts, and culminating in more complex, integrated evaluations. The critical infrastructure interdependency analysis framework is comprised of four phases.

3.1 Phase 1: Identification of Stakeholder Needs

This first phase aims to identify the primary stakeholders in the community or region (i.e., governmental organisations, non-governmental organisations, private sector, and population) and define their requirements and the information they need to integrate infrastructure interdependency considerations in resilience enhancement strategies. A solid understanding of the information needs of decision-makers and the processes in which these decisions occur is essential to scoping the critical infrastructure systems for analysis and the required level of analysis, particularly since interdependency analysis of critical infrastructure can be tailored to different levels (i.e., asset, system, network, or functions). In this phase, the assessment team conducts an initial review of existing documentation (e.g., previous assessments and characterisations of infrastructure systems, existing plans, and other available information) and of operating environment factors to refine the project scope and identify a preliminary list of sites (i.e., downstream users [industry, commerce, population] and utility systems assets).

This first phase is particularly important as it defines the scope and the extent of the analysis to be conducted. It is specifically important to identify the stakeholders (and their jurisdictional responsibilities), the specific intent of the analysis (e.g., identify interdependencies, conduct a vulnerability assessment, or identify resilience enhancement options), the classes of dependencies to be considered, and what constitutes the region

of concern. All these elements are connected. The stakeholders' intents and requirements, as well as the type of critical infrastructures of interest, will help to define the geographic scope of the analysis. The study will not be the same if we consider water treatment and distribution systems that are usually operated at municipal level or electric grid transmission systems that are operated at a much larger scale. The best approach for defining the stakeholder needs is to build a collaborative environment through information-sharing mechanisms and facilitated discussions. This approach is currently used worldwide and is a foundation of the Regional Resiliency Assessment Program and the Protected Critical Infrastructure Information program in the United States (USDHS, 2018b; USDHS, 2018c), the Regional Resiliency Assessment Program in Canada (Public Safety Canada, 2018b), the European Union Agency for Network and Information Security (ENISA) in Europe (ENISA, 2018), and the Trust and Information Sharing Network in Australia (Commonwealth of Australia, 2018).

3.2 Phase 2: Identification of Major Assets

The second phase aims to identify and prioritise the most critical assets for both downstream users and utility systems which, if disrupted, would have detrimental social, environmental, or economic impacts in the region assessed. During this phase, the assessment team analyses, revises, and prioritises the preliminary lists of downstream users and utility systems based on input from private and public sectors as well as infrastructure system owners and operators. Socio-economic analysis can be used to evaluate the significance of downstream users and identify geographic clustering with similar characteristics and resource requirements. After identification of these socio-economically significant areas, the assessment team conducts facilitated discussions and specific surveys to define the list of critical sites that helps focus data collection and analysis activities.

3.3 Phase 3: Data Collection

The third phase aims to gather qualitative and quantitative data to characterise the first-order upstream and downstream dependencies for each critical utility system assets and the first-order upstream dependencies for each critical site identified during Phase 2. For this phase, the assessment team uses a hybrid approach, including:

- Review of existing open source and proprietary data sources (e.g., databases, geographic information system [GIS] data layers, reports, best practices).
- Visits to identify critical assets and utility sites to learn about the facility's operations; potential impacts from disruptions to supporting infrastructure (e.g., power, water, wastewater, communications, transportation); and existing security and emergency procedures.

- Dependency surveys to collect standardised information across facilities to assess the impacts of a disruption or loss of utility services on asset's operations and an industry's essential functions. These surveys specifically gather the information requested to generate dependency curves that characterise upstream dependencies (Petit, et al., 2014).
- Facilitated discussions with subject matter experts and main stakeholders to understand perspectives on industry and utility operations. These discussions uncover operational characteristics of relevant industries and utilities and their role in potential cascading and escalating failures.
- Structured interviews with industry and utility operators. These interviews occur face-to-face and remotely to amplify data gathered through other avenues.

Data collection and analyses are expanding from traditional evaluations of physical dependencies to include cyber and geographic dependencies, as well as visualisations of first- and second-order cascading failures. A key element of the data collection phase is the development of a data architecture and data dictionary to understand the completeness of available data; facilitate a common understanding of infrastructure dependency and interdependency characteristics; support system-level modelling and analysis; and identify opportunities for future engagement with public and private sector stakeholders.

3.4 Phase 4: Infrastructure Analysis

This fourth and final phase constitutes the core of the analysis approach. In this phase, the assessment team analyses the data collected for characterising critical assets' downstream and upstream dependencies, as well as the utility systems, to model how failures could cascade or escalate through infrastructure system-of-systems and potentially impact downstream users. The infrastructure analysis specifically focuses on resilience analysis for the assets and systems, and related interdependency analysis.

3.4.1 Resilience Analysis

Resilience analysis centres on developing an understanding of existing system-level continuity of operations and emergency plans and procedures, as well as related equipment and procedures in place at the facility level. The resilience analysis seeks to identify the existing and potential measures to reduce the consequences of a loss of utilities on facility operations. Information to support resilience analysis at the asset level is gathered during site visits, interviews, and facilitated discussions with industry and utility managers using a structured set of questions. The resilience analysis focuses primarily on preparedness, mitigation, response, and recovery measures, including plans, procedures, and backup capacity.

3.4.2 Interdependency Analysis

The interdependency analysis process combines top-down and bottom-up approaches to characterise infrastructure connectivity within and across sectors. Top-down dependencies analysis involves network-based and system dynamics-based approaches to estimate the service capabilities of utility systems (Table 1). The network-based approach hinges on identifying critical utility nodes and their functions, and then identifying potential resilience enhancements. This approach captures key characteristics (e.g., flows, operational mechanisms) of utility systems. The system dynamics-based approach complements the network-based approach by modelling the effect that the operating environment has on utility system functions. It helps to capture the effects of policy and technical factors that affect utility system evolution.

Table 1: Components of Top-down Analysis

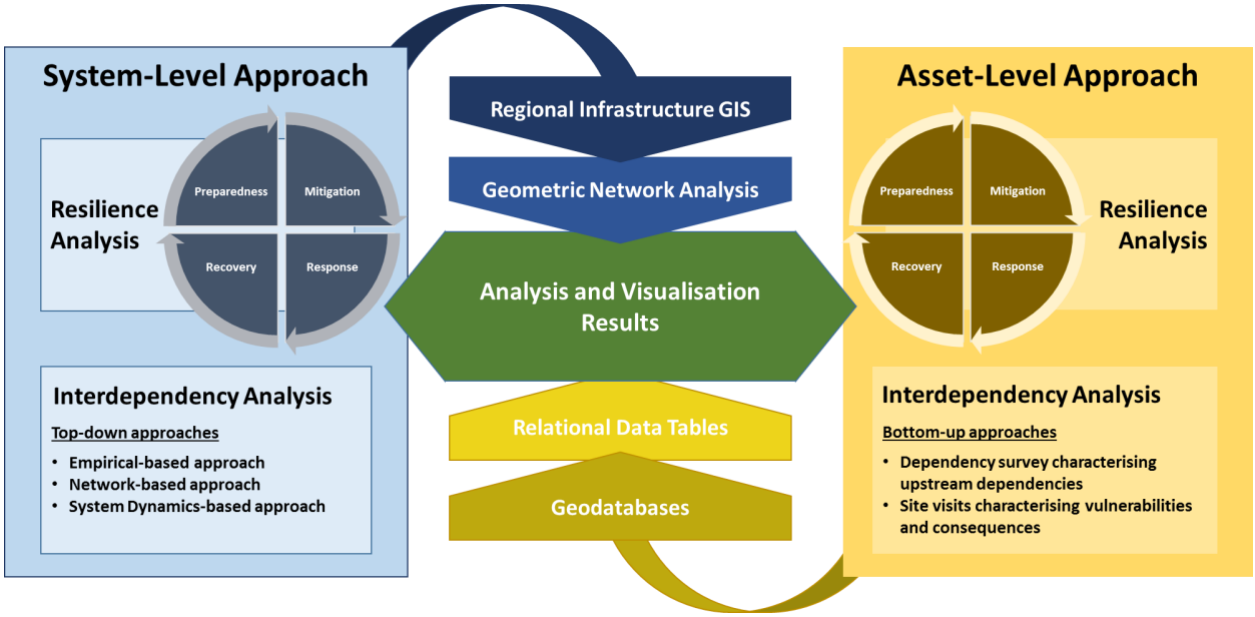
Component	Definition
Network-Based	Describe infrastructure systems as networks where infrastructure assets are represented as nodes and the physical connections are represented as arcs. The two main network-based approaches are topology-based methods and flow-based methods.
System Dynamics-Based	Analysis of the dynamic behaviour of complex systems using a top-down approach to model a system's dynamic and evolutionary behaviour by using stock and flow exchanges and causal loops.

Bottom-up analysis of infrastructure interdependencies focuses on understanding the needs of critical assets (for both utility systems and downstream users) and for specific resources (i.e., power, fuels, water, wastewater, communications, critical supplies). The focus is on impacts of a disruption to these resources and services at a specific asset. Data collection addresses the variations in facility performance over time in light of these disruptions, including timelines, extent, and duration of the loss of services; measures in place (i.e., procedures, backup) to mitigate loss; and the extent of overall degradation on facility's operations.

Top-down and bottom-up interdependency analyses are then combined to define a high-level abstraction of infrastructure interdependencies that allows the assessment team to anticipate potential cascading and escalating failures within and across sectors. Each utility and industry system is visualised as a

layer based on top-down interdependency analysis. The specific connections between layers are characterised through bottom-up interdependency analysis (Figure 6).

Figure 6: System-of-Systems Interdependency Abstraction Visual[4]



For example, top-down analyses of the electric grid shows how the disruption of a given asset (e.g., generator, line, or substation) or a combination of assets (e.g., n-2 contingency studies) would propagate across the electric grid and cause outage areas. Bottom-up analysis is used to characterise how operations at facilities within the power outage areas would be impacted. This use of "system-of-systems" interdependency analysis sheds light on downstream cascading and escalating failures. However, the approach also informs upstream analysis about how utility systems supply critical resources and services to a specific area of interest.

The proposed infrastructure interdependency methodology and framework have been designed to be flexible. The most important element was to propose an adaptive process that can be tailored to answer stakeholder's needs and requirements. On the basis of the desired level of analysis, the data available, and the capabilities of people conducting this analysis, four levels of assessments are possible:

- Initial level assessment consists of building the collaborative environment supporting information sharing about critical infrastructure operations. At this level, assessment consists primarily of

[4]Figure adapted from USDHS. 2018. *Puerto Rico Infrastructure Interdependency Assessment*. May 2018. Prepared by Argonne National Laboratory. Available upon request.

researching open source information and provides a limited analysis of physical and geographic interdependencies.

- Moderate level assessment involves access to proprietary datasets, and uses specific critical infrastructure models to anticipate and visualise first-order dependency cascading failures. At this level, assessment provides a better analysis of physical, geographic, and cyber dependencies.
- Advanced level assessment addresses all classes of dependencies. This level of assessment requires coordination of existing datasets and development of new data collection mechanisms. At this level of assessment, the focus switches from the first-order dependencies of particular critical infrastructure assets to promote a more holistic assessment of second- through *n*-order of dependencies.
- Comprehensive level assessment integrates all classes of dependencies as well as all interdependency dimensions to anticipate and characterise in real time how interdependencies influence the resilience and security of critical infrastructure systems and ultimately the region of concern.

Table 2 presents a general overview of the elements characterising the different level of assessments

Table 2: Overview different assessment levels

Initial Level Assessment	
Data	• Open source (e.g., potential impacts, potential dependencies, and general service)
Analysis	• General understanding of sector dependencies and of assets within a sector • Limited knowledge of cascading impacts • No knowledge of escalating failures
Products	• Static service maps and general sector informational reports • Evaluation of failures from common causes and their direct consequences
Level of effort	At this level, most of the work can be done through discussions between critical infrastructure owners and operators, and emergency management officials. The objective is to have a general understanding of critical assets located in the region of concern.
Moderate Level Assessment	
Data	• Open source • Surveys • Proprietary databases

	• Facilitated discussions with stakeholders
Analysis	• 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
Products	• Refined visualisation 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 characterising upstream physical dependencies
Level of effort	At this level, the objective is to refine the understanding of first-order dependencies to characterise how a specific asset would be affected. If a collaborative environment is in place, few weeks are needed to collect the information characterising existing backups and redundancy, and specific degradation of asset performance resulting from a lack of resource supply. At this level of assessment, only bottom-up approaches are used.
Advanced Level Assessment	
Data	• Implement new data collection mechanisms • Capture new characteristics of dependencies (e.g., added detail on physical and cyber dependencies; integration and analysis of geographic dependency)
Analysis	• Integrate system-level models • Integrate cyber and physical models • Address conditions during normal operations and degraded-state operations
Products	• Refine cascading and escalating visualisation, including second- and third-order cascading failures • Improved temporal and spatial visualisation
Level of effort	This level of assessment is more time and data consuming. It requires access to system modelling techniques to characterise the behaviour of critical infrastructure systems. Several models have been developed by academia and research centres that can be combined by

	using data-centric modelling/simulation platforms (Portante, et al., 2017). GIS platforms also have utility components that can be used to illustrate system behaviour. The major challenge for this level of assessment is to get access to the data needed to run the different models. The level of effort can go from months to years for small research teams.
Comprehensive Level Assessment	
Data	• Collect information for all dependency dimensions • Develop a process to capture all needed information (e.g., beyond critical infrastructure)
Analysis	• 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
Products	• Real time visualisation 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
Level of effort	This level of assessment requires developing an ad-hoc approach and often the use of high performance computing capabilities. This level of assessment is the one difficult to achieve if you don't have access to important research capabilities.

These four levels of assessment build on each other. They require a collaborative environment that promotes information sharing and multidisciplinary analyses and must go beyond a consideration of only the critical infrastructure (e.g., 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 characterise critical infrastructure interdependencies.

The next section illustrates how this critical infrastructure interdependency analysis framework has been applied in Puerto Rico.

4 Application of the Framework in Puerto Rico's Recovery

Hurricane Maria caused catastrophic damage throughout Puerto Rico when it made landfall on 20 September 2017. Escalating failures across all critical infrastructure sectors impacted every community and economic function on the island. As Governor Ricardo Rosselló observed in his request for federal assistance on behalf of the Commonwealth, "[w]ithin a matter of hours, 100% of Puerto Rico's population, economy, critical infrastructure, social service network, healthcare system, and even the government became casualties of the storm" (Rosselló, 2017).

Beginning in October 2017, the framework described above was operationalised to support the U.S. Department of Homeland Security's Infrastructure Security Division and the Federal Emergency Management Agency in analysing disruptions to interdependent infrastructure and contributing the results to whole-of-government long-term recovery planning efforts. The goal of the project has been to conduct an infrastructure interdependency analysis that could inform the targeting, prioritisation, and packaging of infrastructure recovery investments (USDHS, 2018d).

The study of infrastructure interdependencies in Puerto Rico aimed to identify infrastructure recovery needs of a selection of economically-significant regions, as identified by stakeholders, and the critical infrastructure assets upon which these regions depend (Phase 1 of the framework). The study focused on the potential downstream effects of a series of upstream recovery activities for disrupted lifeline infrastructure assets, systems, and operations, including electricity, fuels, water, wastewater, communications, information technology, and transportation (Phase 2). In-field data collection activities conducted over the course of five months captured the characteristics and performance of community institutions and economic actors (i.e., "users") as well as critical infrastructure assets (Phase 3). To facilitate the analysis, a dynamic GIS software environment was developed to assess and visualise the dependencies on and interdependencies between critical infrastructure systems supporting these communities (Phase 4).

The Puerto Rico Infrastructure Interdependency Assessment (PRIIA) toolset, developed by Argonne National Laboratory, consists of several components that analysts incorporated into an interactive Esri® ArcGIS web application, and was used to build a system-of-systems analysis to support local and national government collaboration and decision-making on infrastructure recovery.

4.1 Geodatabases

To conduct the bottom-up analysis in this project, geodatabases were first developed to house standardised data collected through structured interviews with community officials, private industry representatives, infrastructure operators, and local government partners conducted between November 2017 and March 2018. These geodatabases include searchable characterisations of the operations and dependencies for users and infrastructure assets within the study regions. Data points of interest consist of the following:

- Community profiles, including demographic statistics and land-use zoning areas;
- Economic activity, including commercial or industrial perspective, description of the services or products, position on the supply chain, and market share of the user in relation to regional and global markets;
- Internal processes, including the raw materials required, equipment used for operations or manufacturing, and timing of services or production lines;
- Impacts resulting from Hurricane Maria, including the disruptions to operations, mitigation policies in place, and economic impact on infrastructure operations; and
- Infrastructure dependencies, including the specific upstream first-order connections, alternative or redundant sources that could be utilised, and the criticality of services and resources.

4.2 Relational Data Tables

Relational data tables were then structured to align the infrastructure dependency elements from the geodatabases into a network of connections between upstream infrastructure operations and downstream users and infrastructure assets. These were produced for both users (e.g., critical manufacturing facilities) and infrastructure assets that serve those users (e.g., local electricity distribution substations). These tabulate the first-order dependencies of each user and infrastructure asset within the study regions. Table 3 provides an example of the relational data table developed for a single user of interest (i.e., the hypothetical “U001”).

Table 3: Example of Relational Data Table Elements for a Single User of Interest

	First-Order Dependencies						
UID	**AID**	**Asset Type**	**Asset Name**	**Coordinates (x/y)**		**Shape**	**Criticality**
U001	A001	Electricity	Distribution Substation A	−12.345	67.890	Point	Medium
U001	A002	Electricity	Distribution Line A.1	−12.345	67.890	Line	Medium

U001	A004	Water	Water Pump Station B	−12.345	67.890	Point	Medium
U001	A005	Water	Water Pipe B.1	−12.345	67.890	Line	Medium
U001	A008	Wastewater	Treatment Plant C	−12.345	67.890	Point	High
U001	A009	Wastewater	Sewer Line C.1	−12.345	67.890	Line	High
U001	A013	Communications	Cell Tower D	−12.345	67.890	Point	High
U001	A018	Info. Tech.	DSL Junction E	−12.345	67.890	Point	High
U001	A019	Info. Tech.	DSL Fibre Optic Line E.1	−12.345	67.890	Line	High
U001	A025	Air Trans.	Airport F	−12.345	67.890	Point	Medium
U001	A032	Maritime Trans.	Seaport G	−12.345	67.890	Point	High
U001	A040	Road Trans.	Highway Route H	−12.345	67.890	Line	Low
U001	A041	Road Trans.	Highway Route I	−12.345	67.890	Line	High

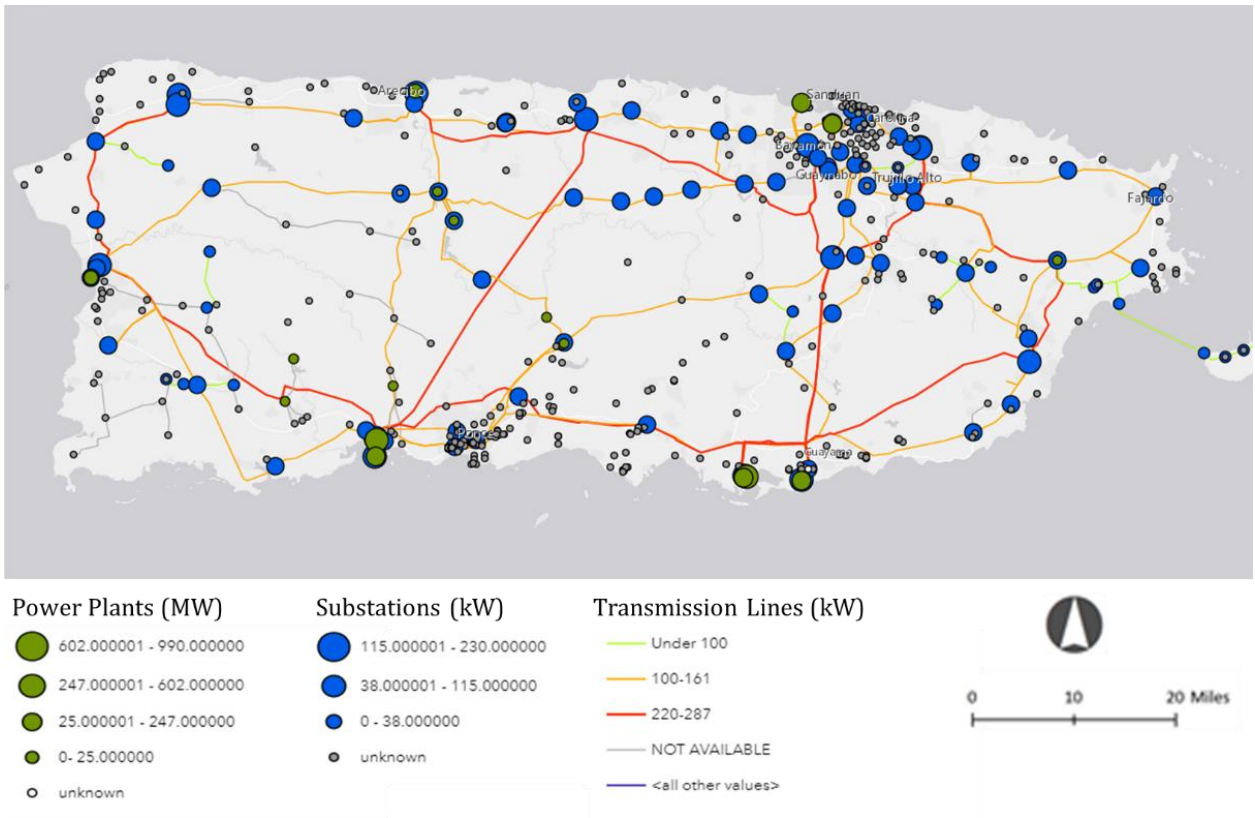
An identification number was assigned to each user (“UID”) and infrastructure asset (“AID”) within the geodatabase, which is used to align connections between users and infrastructure assets as well as among assets in the tables. The tables also associate a description of the upstream infrastructure “asset type” by sector, the “asset name”, its “coordinates” for geotagging, the type of “shape” feature that would be illustrated by the geotagging (e.g., a point or line), and a simple “criticality” ranking (e.g., high, medium, or low) for that service or resource as described by stakeholders.

With these geodatabases and relational data tables, the bottom-up analysis identifies and aligns first- and second-order dependencies that are critical to users and infrastructure assets within the study regions.

4.3 Regional Infrastructure GIS

To inform the top-down analysis in this project, partnerships between the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency and other national and local government agencies supporting recovery operations were essential in collecting the necessary regional (i.e., system-level) GIS data on each critical infrastructure sector. The availability of open source data was especially important in order to maximise the distribution of the analytical results. Figure 7 provides an example of the electric grid GIS data collected to support the analysis.

Figure 7: Illustration of System-level GIS Data in Puerto Rico (Esri, 2018; USDHS, 2017) [5]



4.4 Geometric Network Analysis

The characterisations contained in the geodatabases and connections aligned within the relational data tables were combined with regional infrastructure GIS data to geotag the dependencies and interdependencies. Geometric network analysis is currently being used to establish system-level schematics of interactions between the users and infrastructure assets, as well as between the assets themselves, in the study regions. This enabled analysts to combine the flow and cardinality of system-level dynamics with asset-level characterisations and connections developed through in-field data collection.

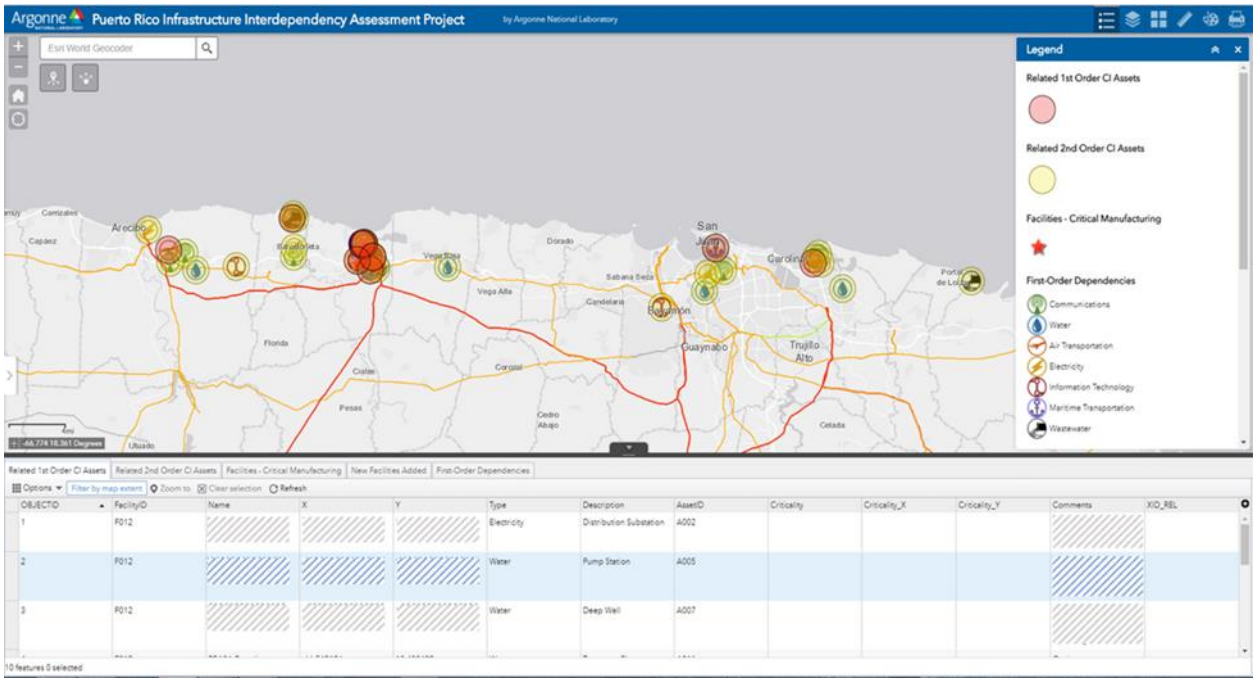
4.5 Analysis and Visualisation Results

The PRIIA software toolset displays and leverages the data and connections from the four components described above to perform the analysis on and derive visualisations of dependencies and interdependencies. These visualisations highlight the relational data assembled on the regions of interest (i.e., bottom-up) in light of

[5]The U.S. Department of Homeland Security's Homeland Infrastructure Foundation-Level Data (HIFLD) includes "geospatial data within the open public domain that can be useful to support community preparedness, resiliency, research, and more." See https://hifld-geoplatform.opendata.arcgis.com/.

the flow and cardinality of system-level GIS data established through geometric network analysis (i.e., top-down). The results of each run of the toolset are displayed in an interactive GIS environment. Figure 8 provides a notional example of a mapping and assessment of first- and second-order dependencies for a single user of interest.

Figure 8: Notional Example of Results Generated by the PRIIA Toolset (USDHS, 2018d).



By selecting a user or infrastructure asset on the map, PRIIA can return a visual tagging of upstream infrastructure assets that are critical to its operations. The red-shaded infrastructure assets in Figure 8 highlight those that were identified as a first-order dependency of the selected downstream user or infrastructure asset, and the yellow-shaded infrastructure assets highlight those that were identified as its second-order dependencies (and, therefore, first-order dependencies of the red-shaded assets).

In some instances, the toolset returned results with certain infrastructure assets highlighted in orange (combining the red and yellow shadings), denoting that those assets were both a first- and second-order dependency of the selected downstream user or infrastructure asset. For example, a selected user may have first-order dependencies on both an electricity distribution substation for electricity service and on a cellular tower for communications service. The cellular tower may also have a first-order dependency on the same electricity distribution substation to power its operation. The electricity distribution substation would therefore be highlighted with orange by the toolset as both a first- and second-order dependency of the user because its operations may have direct and indirect impacts on the user's operations. This denotes the possibility to create escalating failures if these systems were degraded.

Iterative runs of the toolset also enabled analysts to derive tallies of the cumulative demands being placed on each infrastructure asset. This exercise produced a ranking of relative criticality of infrastructure assets and, potentially, the relative stress under which these operate. In light of the desired goal to inform the targeting, prioritisation, and packaging of infrastructure recovery investments, these tallied results can be used to drive efforts by national and local government partners to build back better and more resilient communities, industries, and supporting infrastructure for the Commonwealth of Puerto Rico (USDHS, 2018). The PRIIA toolset continues to be used to support long-term recovery planning for critical infrastructure systems across Puerto Rico.[6] The critical infrastructure interdependency analysis framework described above and the processes developed for this toolset are being incorporated by Argonne National Laboratory and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency in their on-going support for the Federal Emergency Management Agency's recovery mission.

5 Operationalising Resilience Strategies for the Global Arena

The *Sendai Framework for Disaster Risk Reduction* incorporates the resilience of infrastructure as a central component of disaster preparedness, recognising the need "to ensure that they remain safe, effective and operational during and after disasters in order to provide live-saving and essential services" (UNISDR, 2015). As the example of Puerto Rico's recovery continues to illustrate, ensuring critical infrastructure operations involves cross-sector assessments of infrastructure interdependencies. In order to be effective, risk reduction efforts should target the broader enhancement of community resilience, which requires the consideration of interdependencies at the asset, community, system, national, regional, and global levels.

Modern societies face increasingly complex challenges in reducing the risks posed by climate change, extreme weather events, man-made events, and aging infrastructure. As the risks posed by these hazards continue to increase in both frequency and intensity, the efforts of infrastructure owners, operators, and governance structures to enhance the resilience of the assets and systems they manage are more crucial than ever. Interdependency relationships among critical infrastructure should be analysed using a framework and

[6]The examples and explanation of PRIIA in this paper were notional in nature due to the sensitivity of real-world data and the results produced during this assessment.

toolset like the one presented in this paper to anticipate how a change affecting these connections could cascade or escalate across other critical infrastructure operations and dependent downstream users.

This priority is echoed in the *2030 Agenda for Sustainable Development*, and specifically in the first target of Goal 9, which advocates the development of "quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being" (UN, 2015). The challenge is to go beyond traditional risk management approaches and to design critical infrastructure systems that will be adapted to their future socio-ecological environment, and that will respond to current and future population needs. Such an all-encompassing overview would support the mutual reinforcement and concerted efforts between global risk reduction, resilience, and sustainable development targets.

To be truly effective, the implementation of comprehensive disaster risk reduction and resilience management strategies also requires collaborative and multidisciplinary approaches that combine social, economic, and technical points of view. This means that the critical infrastructure interdependency analysis framework must combine not only social and system engineering methodologies, but also regional capabilities to inform multi-organisational decision-making and prioritise activities to reduce consequence duration and severity. This will fully elucidate the range of influences acting upon critical infrastructure assets and systems, and therefore promote practices supporting acceptable levels of critical infrastructure performance.

Regional coordination will help stakeholders to define what constitutes an acceptable level of consequence for identifying resilience enhancement strategies. Conceptually (and before an event), it is relatively easy to decide to prioritise response and recovery activities, and to decide to channel the consequences resulting from cascading and escalating failures. The reality may be different when the adverse event occurs. The main challenge is to define the risk ownership and to decide who will deal with the consequences, and also to establish through a scientific method that the actions taken will be beneficial for most (if not all) stakeholders.

After prioritising their operations, critical infrastructure should organise collaborative and secure exchanges with their suppliers and regional emergency managers to coordinate decision making and achieve the greatest benefit for the most critical needs. Communication is an important, and too often neglected, phase of risk management. A process for improving the resilience of critical infrastructure cannot be effective without considering all of the stakeholders involved in critical infrastructure management and regional emergency management, including the public. In risk management, it is always difficult to define what information must be communicated, to whom, and how.

The development of processes that maintain a balance between protecting sensitive information (from a business and/or national security perspective) and providing emergency managers necessary information continues to be a challenge. Understanding regional security and safety capabilities is beneficial for harmonising resilience strategies. However, communicating about resilience and security strategy can generate additional vulnerabilities that could be exploited by malevolent actors. Identifying and admitting that your system can fail, generate a loss of public confidence, and affect critical infrastructure business activities.

The difficulty in defining what consequences are acceptable and what information should be shared can be addressed by building a trusted environment to promote a sustainable development culture based on education and training. The development of trust must be supported by mechanisms to operationalise standards and policies promoting collaborative approaches and partnerships between critical infrastructure owner, operator, and government representatives. Furthermore, the objective of resilience management strategies is to complement risk management strategies, which primarily address hazards and vulnerabilities, by promoting flexible and adaptive approaches to better react to unanticipated hazards and reduce undesired consequences.

6. Conclusion

The characterisation of critical infrastructure interdependencies is essential for risk and resilience management. The integration of these relationships into risk analysis and regional resilience strategies enables decision makers to better understand how critical infrastructure systems operate, to anticipate potential cascading and escalating failures, and to identify possible adaptation measures. Infrastructure interdependencies are complex and dynamic relationships to analyse. Managing these complexities requires the combination of top-down and bottom-up analysis techniques in a proactive risk management approach that integrates current and future socio-ecological conditions. The analysis framework presented in this paper proposes a flexible and adaptive approach to anticipate how a change affecting infrastructure operations could cascade or escalate across other critical infrastructure operations and dependent downstream users. This approach can be used in all phases of risk and emergency management to support economic development and human well-being. To be effective, this approach requires a trust environment built on collaboration and information sharing to consider all stakeholders' requirements and to inform comprehensive disaster risk reduction and resilience management strategies.

References

Australian Government. 2010. *Critical Infrastructure Resilience Strategy*. Available via https://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf. Accessed September 21, 2018.

Carlson, L., G. Basset, 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, IL. Available via https://publications.anl.gov/anlpubs/2012/02/72218.pdf. Accessed September 21, 2018.

Commonwealth of Australia. 2018. *Trusted Information Sharing Network For Critical Infrastructure Resilience*. Available via https://www.tisn.gov.au/Pages/default.aspx. Accessed September 21, 2018.

Curt, C., and J.M. Tacnet. 2018. Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. *Risk Analysis*, Vol. 38, No. 11, pp. 2441-2458.

Dahlberg, R., C.T. Johannessen-Henry, E. Raju, and S. Tulsiani. 2015. Resilience in Disaster Research: Three Versions. Civil Engineering and Environmental Systems, Vol. 32, Nos. 1-2, pp. 44-54.

Esri. 2018. ArcGIS Web Application. Version 10.4.1. Environmental Systems Research Institute.

European Commission Migration and Home Affairs. 2019. *Critical Infrastructure*. Available via https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en. Accessed September 21, 2018.

European Union Agency for Network and Information Security. 2018. *Critical Infrastructures and Services.* Available via https://www.enisa.europa.eu/. Accessed September 21, 2018.

Fackler, M., 2011. Powerful quake and tsunami devastate northern Japan. *The New York Times*, March 11, 2011. Available via http://www.nytimes.com/2011/03/12/world/asia/12japan.html?_r=1&pagewanted=all. Accessed September 21, 2018.

Flynn, S. E. 2015. *Bolstering critical infrastructure resilience after superstorm Sandy: lessons for New York and the nation*. Georges J. Kostas Research Institute for Homeland Security, Center for Resilience Studies, Northeastern University. Available via https://repository.library.northeastern.edu/files/neu:m0419677k. Accessed September 21, 2018.

Karklis, L., and S. Granados. 2017. After Hurricane Maria, Puerto Rico was in the dark for 181 days, 6 hours and 45 minutes. *The Washington Post*, October 11, 2017. Available via https://www.washingtonpost.com/graphics/2017/national/puerto-rico-hurricane-recovery/?utm_term=.b54520207218. Accessed September 21, 2018.

New York Times. 2010. Iceland volcano eruption of 2010 (Eyjafjallajokull volcano). *The New York Times*, Times topics, Tuesday, April 20, 2010. Available via http://topics.nytimes.com/top/news/international/countriesandterritories/iceland/eyjafjallajokull/index.html. Accessed September 21, 2018.

Ouyang, M. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Elsevier reliability engineering and system safety* (121):43–60.

Pescaroli, G., and D. Alexander. 2016. Critical Infrastructure Panarchies and the Vulnerability Paths of Cascading Disasters. *Natural Hazards*, 82:175-192.

Petit, F. 2018. Resilience Assessment in Homeland Security. *Resource Guide on Resilience Volume 2*, International Risk Governance Center. Available via https://irgc.epfl.ch/risk-governance/projects-resilience/. Accessed September 21, 2018.

Petit, F., D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, R. Haffenden, J. Phillips, and J. Peerenboom. 2015. *Analysis of Critical Infrastructure Dependencies and Interdependencies*. Argonne National Laboratory, Global Security Sciences Division, ANL/GSS-15/4, Argonne, Ill, USA. Available via https://publications.anl.gov/anlpubs/2015/06/111906.pdf. Accessed September 21, 2018.

Petit, F., D. Verner, and L.A. Levy. 2017. *Regional Resiliency Assessment Program Dependency Analysis Framework*. Argonne National Laboratory, Global Security Sciences Division, ANL/GSS-17/05, Argonne, IL. USA.

Petit, F., K. Wallace, and J. Phillips. 2014. "Interactive Dependencies Curves for resilience management. Henry Stewart Publications, *Journal of Business Continuity & Emergency Planning*, London, United Kingdom, Vol. 8, No 2. pp. 141-155.

Pianigiani, G., E. Povoledo, and R. Pérez-Peña. 2018. Italy Bridge Collapse Leaves 37 Dead. *The New York Times*, August 14, 2018. Available via https://www.nytimes.com/2018/08/14/world/europe/italy-genoa-bridge-collapse.html. Accessed September 21, 2018.

Porod, C., F. Petit, J. Peerenboom, R. Fisher, and J. Raess. 2012. Evolution of Critical Infrastructure Protection, In: A. Yates, M. Clarke, and G. Griffin.: *Next Generation Disaster Management*, Australian Security Research Centre (ASRC) Resilience & Security Imprint, Australia, pp. 133-146.

Portante, E. C., J. A. Kavicky, B. A. Craig, L. E. Talaber, and S. M. Folga. 2017. Modeling Electric Power and Natural Gas System Interdependencies. *ASCE J. Infrastruct. Syst.*, 23(4). Available via https://ascelibrary.org/doi/10.1061/%28ASCE%29IS.1943-555X.0000395. Accessed September 21, 2018.

Public Safety Canada. 2018a. *Critical Infrastructure*. Available via https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx. Accessed September 21, 2018.

Public Safety Canada. 2018b. *The Regional Resilience Assessment Program*. Available via https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx. Accessed September 21, 2018.

Rinaldi, S.M., J P. Peerenboom, and T.K. Kelly. 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, December 2001. Available via http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf. Accessed September 21, 2018.

Rosselló, R. 2017. *Build Back Better Puerto Rico: Request for Federal Assistance for Disaster Recovery*. Government of Puerto Rico, November 2017. Available via https://media.noticel.com/o2com-noti-media-us-east-1/document_dev/2017/11/13/Build%20back%20better%20Puerto%20Rico_1510595877623_9313474_ver1.0.pdf. Accessed September 21, 2018.

Swedish Emergency Management Agency. 2014. *Action Plan for the Protection of Vital Societal Functions and Critical Infrastructure*. Available via https://www.msb.se/RibData/Filer/pdf/27412.pdf. Accessed September 21, 2018.

UN (United Nations). 2015. *Transforming our World: The 2030 Agenda for Sustainable Development*. A/RES/70.1. Resolution adopted by the General Assembly on 25 September 2015, United Nations General Assembly. Available via http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E. Accessed September 21, 2018.

UNISDR (United Nations International Strategy for Disaster Risk Reduction). 2015. *Sendai Framework for Disaster Risk Reduction, 2015–2030*. Para. 33(c). Available via https://www.unisdr.org/we/inform/publications/43291. Accessed September 21, 2018.

UNISDR. 2017a. UNISDR terminology on disaster risk reduction. Available via https://www.unisdr.org/we/inform/terminology. Accessed September 21, 2018.

UNISDR. 2017b. *Words into Action Guidelines: National Disaster Risk Assessment*. C. Cross-Sectoral and Multi-Risk Approach to Cascading Disasters, UNISDR, Preventionweb. Available via https://www.preventionweb.net/files/52828_ccrosssectoralmultirisk[1].pdf. Accessed September 21, 2018.

USDHS (U.S. Department of Homeland Security). 2010. *DHS Risk Lexicon – 2010 edition*. Available via http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. Accessed September 21, 2018.

USDHS. 2017. Homeland Infrastructure Foundation-Level Data (HIFLD). Available via https://hifld-geoplatform.opendata.arcgis.com/. Accessed September 21, 2018.

USDHS. 2018a. *Critical Infrastructure*. Available via http://www.dhs.gov/files/programs/gc_1189168948944.shtm. Accessed September 21, 2018.

USDHS. 2018b. *Regional Resiliency Assessment Program*. Available via https://www.dhs.gov/sites/default/files/publications/rrap-fact-sheet-08-24-16-508.pdf. Accessed September 21, 2018.

USDHS. 2018c. *Protected Critical Infrastructure Information (PCII) Program*. Available via https://www.dhs.gov/pcii-program. Accessed September 21, 2018.

USDHS. 2018d. *Puerto Rico Infrastructure Interdependency Assessment*. May 2018. Available upon request.

Acknowledgment

The authors gratefully acknowledge the contributions of many people who helped bring this project to its current state of development, including the U.S. Department of Homeland Security's Infrastructure Security Division and the Federal Emergency Management Agency. More specifically, the authors want to thank Daniel Genua and William McNamara, without whom this work would not have been possible. Their leadership and dedication inspired the Argonne National Laboratory team.

The authors also want to thank their Argonne colleagues, Carmella Burdi, Scott Schlueter, Amanda Wagner, Matthew Berry, Joshua Bergerson, Kim Erskine, Duane Verner, and L-A Levy, who helped to develop the Critical Infrastructure Interdependency Assessment Framework and conduct its application in Puerto Rico.