



Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies

By Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly

The notion that our nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies (so-called "cyber-based systems"), is more than an abstract, theoretical concept. As shown by the 1998 failure of the *Galaxy 4* telecommunications satellite, the prolonged power crisis in California, and many other recent infrastructure disruptions, what happens to one infrastructure can directly and indirectly affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy.

In the case of the *Galaxy 4* failure, the loss of a single telecommunications satellite led to an outage of nearly 90% of

all pagers nationwide [1]. From an interdependency perspective, it also disrupted a variety of banking and financial services, such as credit card purchases and automated teller machine transactions, and threatened key segments of the vital human services network by disrupting communications with doctors and emergency workers. In California, electric power disruptions in early 2001 affected oil and natural gas production, refinery operations, pipeline transport of gasoline and jet fuel within California and to its neighboring states, and the movement of water from northern to central and southern regions of the state for crop irrigation [2]-[6]. The disruptions also idled key industries, led to billions of dollars of lost productivity, and stressed the entire Western power grid, causing far-reaching security and reliability concerns [7]-[10].

Peerenboom (jpeerenboom@anl.gov) is with Argonne National Laboratory, 9700 S. Cass Ave., Bldg. 900, Argonne, IL 60439, U.S.A. Rinaldi is with the Air Force Quadrennial Defense Review, Washington, D.C. 20330-1670, U.S.A. Kelly is with the Executive Office of the President, Washington, D.C. 20502, U.S.A.

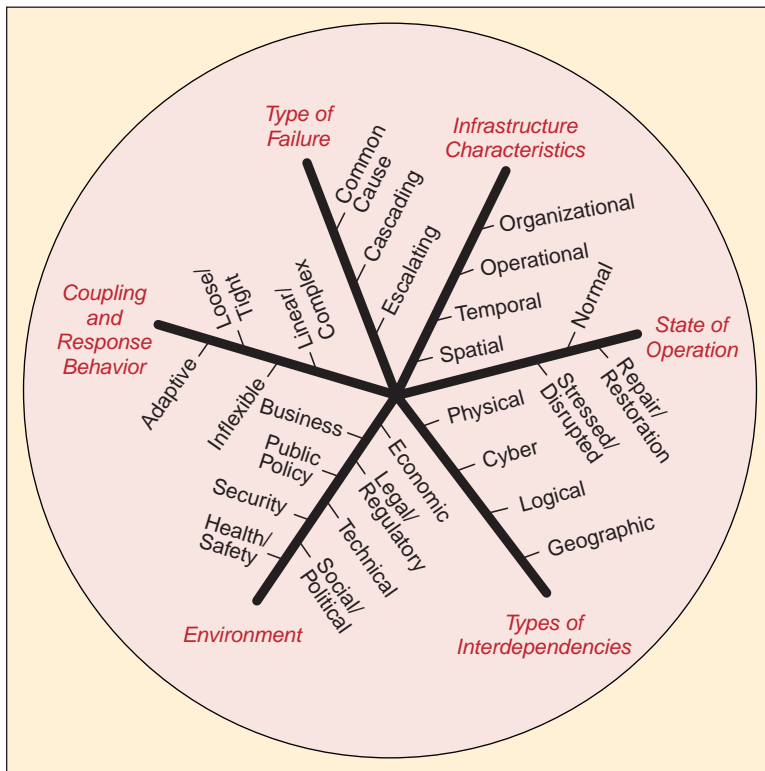


Figure 1. Dimensions for describing infrastructure interdependencies.

Identifying, understanding, and analyzing such interdependencies are significant challenges. These challenges are greatly magnified by the breadth and complexity of our critical national infrastructures. These infrastructures, which affect all areas of daily life, include electric power, natural gas and petroleum production and distribution, telecommunications (information and communications), transportation, water supply, banking and finance, emergency and government services, agriculture, and other fundamental systems and services that are critical to the security, economic prosperity, and social well-being of the nation.

Further complicating this challenge is a broad range of interrelated factors and system conditions that we represent and describe in terms of six “dimensions,” as depicted in Fig. 1. They include the technical, economic, business, social/political, legal/regulatory, public policy, health and safety, and security concerns that affect infrastructure operations. The environment comprising these concerns influences normal system operations, emergency operations during disruptions and periods of high stress, and repair and recovery operations. The degree to which the infrastructures are coupled, or linked, strongly influences their operational characteristics. Some linkages are loose and thus relatively flexible, whereas others are tight, leaving little or no flexibility for the system to respond to changing conditions or failures that can exacerbate problems or cascade from one infrastructure to another. These linkages can be physical, cyber, related to geographic location, or logical in nature. Interdependent infrastructures

also display a wide range of spatial, temporal, operational, and organizational characteristics, which can affect their ability to adapt to changing system conditions. And finally, interdependencies and the resultant infrastructure topologies can create subtle interactions and feedback mechanisms that often lead to unintended behaviors and consequences during disruptions.

A basic discussion of the concept and importance of interdependencies is presented in *Critical Foundations: Protecting America’s Infrastructures*, the report of the U.S. President’s Commission on Critical Infrastructure Protection (PCCIP) [11]. Although this report articulated the inherent dangers of uncontrolled interdependencies, it did not provide a methodology for thinking about or analyzing this phenomenon. This article presents a conceptual framework for addressing infrastructure interdependencies that could serve as the basis for further understanding and scholarship in this important area.

We use this framework, namely, the dimensions shown in Fig. 1, to explore the challenges and complexities of interdependency. We set the stage for this discussion by explicitly defining the terms *infrastructure*, *infrastructure dependencies*, and *infrastructure interdependencies* and introducing the fundamental concept of infrastructures as complex adaptive systems. We then focus on the interrelated factors and system conditions that collectively define the six dimensions. Finally, we discuss some of the research challenges involved in developing, applying, and validating modeling and simulation methodologies and tools for infrastructure interdependency analysis.

Concepts and Definitions

Infrastructure

The term *infrastructure*, which is defined as “the underlying foundation or basic framework (as of a system or organization)” [12], took on new meaning and importance as a result of the work of the PCCIP. In its October 1997 report to the U.S. President, the Commission defined an infrastructure as a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services. [11]

In its deliberations, the Commission narrowly focused on eight critical infrastructures “whose incapacity or destruction would have a debilitating impact on our defense and economic security” [11]. These eight are telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services. The Commission

noted that “[t]here is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructures” [11].

That definition was later broadened and refined by the Critical Infrastructure Assurance Office (CIAO), an interagency office created under Presidential Decision Directive 63 to assist in coordinating the federal government’s initiatives on critical infrastructure protection [13]. The CIAO defined infrastructure as

the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole. [13]

In this broader perspective, other examples of infrastructures (in addition to the Commission’s eight critical infrastructures) include food/agriculture (production, storage, and distribution), space, numerous commodities (iron and steel, aluminum, finished goods, etc.), the health care industry, and the educational system.

Infrastructures as Complex Adaptive Systems

All of the aforementioned critical infrastructures have one property in common—they are all complex collections of interacting components in which change often occurs as a result of learning processes; that is, they are complex adaptive systems (CASs) [14]. Seen from this perspective, which has important benefits for modeling and analysis, each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. All components are influenced by past experiences. For example, electric transformers slowly degrade from overuse, and natural gas pipes age over time. And many components are individually capable of learning from past experiences and adapting to future expectations, such as operating personnel who try to improve their performance and real-time computer systems that adjust electric generator outputs to meet varying power loads.

From a CAS perspective, infrastructures are more than just an aggregation of their components. Typically, as large sets of components are brought together and interact with one another, synergies emerge. Consider the emergence of reliable electric power delivery from a collection of well-placed electric generators, transformers, transmission lines, and related components. Simply aggregating the components in an ad hoc fashion will not ensure reliable electricity supplies. Only the careful creation of an intricate set of services will yield a system that reliably and continuously supplies electricity. This additional complexity exhibited by a system as a whole, beyond the simple sum of its parts, is called emergent behavior and is a hallmark of CASs [15].

Complex adaptive systems do not require strong central control for emergent behaviors to arise [15]. In fact, many CASs would not function as well with such restrictive operating procedures. However, it is vital for managers responsible for systems of this type, such as the eight critical infrastructures defined by the Commission, to recognize the nature—and particularly the emergent behaviors—of their systems.

One effective way to investigate CASs is to view them as populations of interacting agents [14]. An agent is an entity with a location, capabilities, and memory. Although the term *agent* is frequently used when discussing specific modeling techniques, we use it here in the abstract to describe entities with general characteristics. The entity’s location defines where it is in a physical space, such as a geographic region, or an abstract space, such as the Internet, or both. The entity’s capabilities define what it can do from its location, such as an electric generator increasing its output or an oil pipeline reducing its pumping rate. The entity’s memory defines what it has experienced, such as overuse or aging. Memory is often expressed in the form of agent state variables. Most infrastructure components have a location and capabilities and are influenced by past experiences. Thus, most infrastructure components can be viewed as agents.

Consider an oil pipeline. The pipeline’s location can be expressed physically as a set of latitudes and longitudes and abstractly as a specific stage in the oil delivery process. The capabilities of the pipeline include not only its ability to move oil, but also the ways in which it responds to emergencies. Naturally, these responses may not always be positive. For instance, the pipeline might respond to a rupture or the loss of electricity at a pumping station by simply shutting down the flow of oil. The memory of the pipeline may include the current and past flow rates, pressures, temperatures, operating status of its pumps, and so forth.

Agents communicate with one another as they operate in a particular environment. Each agent receives inputs from other agents and sends outputs to them. These “inputs” and “outputs” need not be resources used in, or products made by, an infrastructure or process. Metrics that describe the state of an agent can also be viewed as outputs that other agents can sense (use as input) and act upon. The inputs to an oil pipeline include electricity to power the pumps and the current demand for oil, whereas its outputs include the flow of oil to external agents and price information. (We will examine inputs and outputs in detail when we discuss the “types of interdependencies” dimension in Fig. 1.)

Dependency

Consider a specific, individual connection between two infrastructures, such as the electricity used to power a telecommunications switch. In this case, the relationship is usually unidirectional; that is, infrastructure *i* depends on *j* through the link, but *j* does not depend on *i* through the same link:

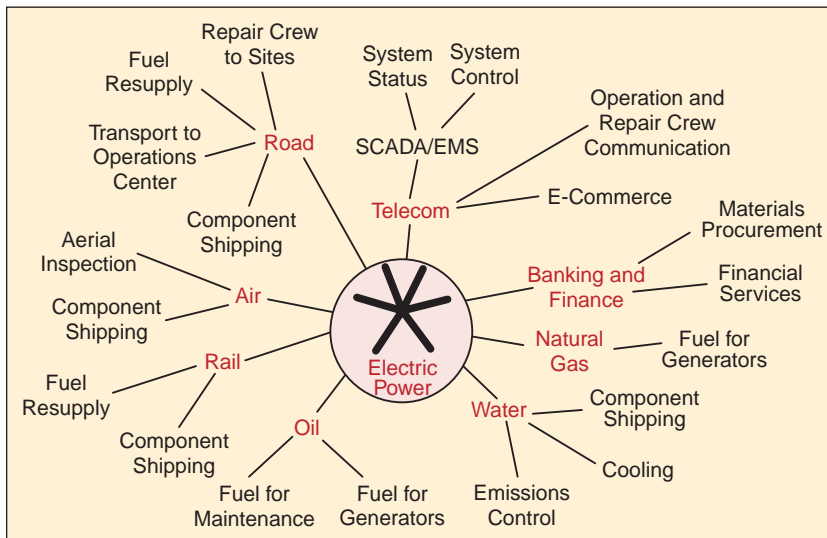


Figure 2. Examples of electric power infrastructure dependencies.

Dependency: A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.

Fig. 2 illustrates the concept. Under normal operating conditions, the electric power infrastructure requires natural gas and petroleum fuels for its generators, road and rail transportation and pipelines to supply fuels to the generators, air transportation for aerial inspection of transmission lines, water for cooling and emissions control, banking and finance for fuel purchases and other financial services, and telecommunications for e-commerce and for monitoring system status and system control (i.e., supervisory control and data acquisition (SCADA) systems and energy management systems (EMSs)). During emergencies or after component failures, the electric power infrastructure will have potentially different yet critical dependencies on the same infrastructures. For example, the utility may require petroleum fuels for its emergency vehicles and emergency generators and road transportation (and in some cases rail and air transportation) to dispatch repair crews and replace component parts.

As depicted in Fig. 2, electric power is the *supported* infrastructure, and natural gas, oil, transportation, telecommunications, water, and banking and finance are *supporting* infrastructures. Although not shown, emergency and government services are also supporting infrastructures.

Interdependency

When examining the more general case of multiple infrastructures connected as a “system of systems,” we must consider interdependencies. Infrastructures are frequently connected at multiple points through a wide variety of mechanisms, such that a bidirectional relationship exists between the states of any given pair of infrastructures; that is, infrastructure i depends on j through some links, and j likewise depends on i through other links:

Interdependency: A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.

The term *interdependencies* is conceptually simple; it means the connections among agents in different infrastructures in a general system of systems. In practice, however, interdependencies among infrastructures dramatically increase the overall complexity of the “system of systems.” Fig. 3 illustrates the interdependent relationship among several infrastructures. These complex relationships are characterized by multiple connections among infrastructures, feedback and feedforward

paths, and intricate, branching topologies. The connections create an intricate web that, depending on the characteristics of its linkages, can transmit shocks throughout broad swaths of an economy and across multiple infrastructures. It is clearly impossible to adequately analyze or understand the behavior of a given infrastructure in isolation from the environment or other infrastructures. Rather, we must consider multiple interconnected infrastructures and their interdependencies in a holistic manner. For this reason, we use the term *interdependencies* rather than *dependency* throughout the remainder of this article.

Dimensions of Infrastructure Interdependencies

Using these concepts and definitions, we now explore the six dimensions shown in Fig. 1. These dimensions and their components are descriptive and are intended to facilitate the identification, understanding, and analysis of interdependencies. They do not represent a comprehensive set of orthogonal interdependency metrics, although they provide a foundation for developing such metrics. As we will discuss later, metrics and new modeling and simulation approaches are needed that can address, in a consistent manner, all of these interrelated factors and system conditions.

Types of Interdependencies

Interdependencies vary widely, and each has its own characteristics and effects on infrastructure agents. In the sections that follow, we define and examine in detail four principal classes of interdependencies: physical, cyber, geographic, and logical. Although each has distinct characteristics, these classes of interdependencies are not mutually exclusive.

Physical Interdependency

Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other.

As its name implies, a physical interdependency arises from a physical linkage between the inputs and outputs of two agents: a commodity produced or modified by one infrastructure (an output) is required by another infrastructure for it to operate (an input). For example, a rail network and a coal-fired electrical generation plant are physically interdependent, given that each supplies commodities that the other requires to function properly. The railroad provides coal for fuel and delivers large repair and replacement parts to the electrical generator, while electricity generated by the plant powers the signals, switches, and control centers of the railroad—and in the case of electrified rail, directly powers the locomotives. The state of one infrastructure (whether the railroad is able to provide adequate coal stocks to the electrical generator) directly influences the state of the other (whether the generator can produce sufficient power to meet the railroad’s needs) and vice versa. By means of this direct connection, a state change in the railroad (halt in the delivery of coal) can drive a corresponding state change in the electrical grid (switch to alternative fuels or additional generation from non-coal-fired plants). In this manner, perturbations in one infrastructure can ripple over to other infrastructures. Consequently, the risk of failure or deviation from normal operating conditions in one infrastructure can be a function of risk in a second infrastructure if the two are interdependent.

Cyber Interdependency

An infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure.

Cyber interdependencies are relatively new and a result of the pervasive computerization and automation of infrastructures over the last several decades. To a large degree, the reliable operation of modern infrastructures depends on computerized control systems, from SCADA systems that control electric power grids to computerized systems that manage the flow of railcars and goods in the rail industry. In these cases, the infrastructures require information transmitted and delivered by the information infrastructure. Consequently, the states of these infrastructures depend on outputs of the information infrastructure. Cyber interdependencies connect infrastructures to one another via electronic, informational links; the

outputs of the information infrastructure are inputs to the other infrastructure, and the “commodity” passed between the infrastructures is information.

Geographic Interdependency

Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them.

A geographic interdependency occurs when elements of multiple infrastructures are in close spatial proximity. Given this proximity, events such as an explosion or fire could create correlated disturbances or changes in these geographically interdependent infrastructures. Such correlated changes are not due to physical or cyber connections between infrastructures; rather, they arise from the influence the event exerts on all the infrastructures simultaneously. An electrical line and a fiber-optic communications cable slung under a bridge connect (geographically) elements of the electric power, telecommunications, and transportation infrastructures. The interdependency in these cases is simply due to proximity; the state of one infrastructure does not influence the state of another. Traffic across the bridge does not influence the transmission of messages through the optical fiber or the flow of electricity. Because of the close spatial proximity, however, physical damage to the bridge could create correlated perturbations in the electric power, communications, and transportation infrastructures. Note that more than two infrastructures

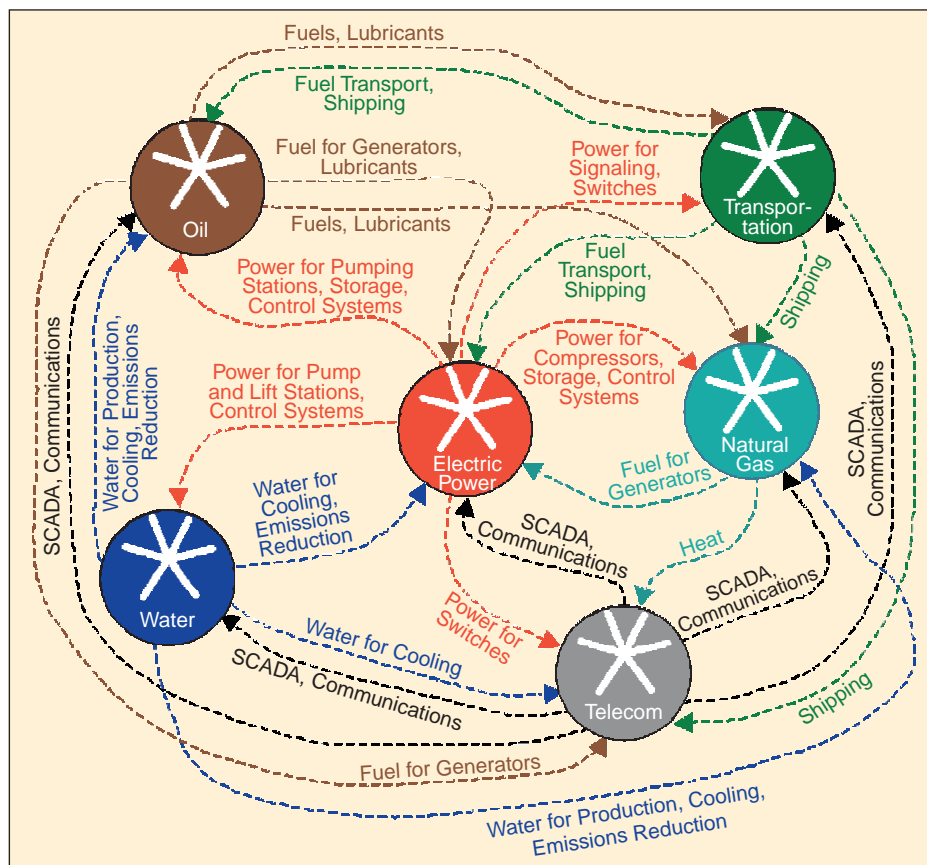


Figure 3. Examples of infrastructure interdependencies.

can be geographically interdependent based on their physical proximity.

Implicit in our discussion is the fact that some interdependencies and their effects on infrastructure operations are caused by physical phenomena, whereas others result from human intervention and decisions. For example, if an electric power utility should fail, then the backup generators at a telecommunications switch start automatically, the result of physical interactions and phenomena without human intervention.

Logical Interdependency

Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.

Logical interdependencies may be more closely likened to a control schema that links an agent in one infrastructure to an agent in another infrastructure without any direct physical, cyber, or geographic connection. Consider the power cri-

What happens to one infrastructure can directly and indirectly affect other infrastructures, impact large geographic regions, and send ripples throughout the national and global economy.

sis that emerged in California in late 2000 and the logical interdependency between the electric power and financial infrastructures. The genesis of this crisis can be traced to the deregulation legislation that was passed in 1996 to open California's electricity market to competition. Under that legislation, California's investor-owned utilities were required to sell off their power-generating assets and purchase electricity on the open market. At the same time, however, the state experienced substantial load growth, a lack of investment in new generating capacity and transmission lines, reduced generation from aging power plants, high natural gas prices, transmission and environmental constraints, a drought in the Pacific Northwest, and a volatile spot market. This confluence of factors, plus the fact that utilities were not permitted to pass soaring wholesale power prices through to consumers, led to an unprecedented financial crisis that pushed one of the state's largest utilities to bankruptcy and another to the brink of bankruptcy. In addition to enormous financial losses, the bond ratings of these utilities were downgraded to below investment grade (or into the status of junk bonds). This state variable of the financial market made it nearly impossible, without intervention by the federal and state governments, for the utilities to buy power. As a result, the utilities' abilities to provide sufficient electric power (electrical state variable) in California were decreased by their bond rat-

ings (financial state variable), and their bond ratings were affected by their inability to produce enough power. In this example, the logical interdependency is bidirectional and does not depend on any physical or cyber connection between the electric power and financial infrastructures.

Furthermore, human decisions may play the predominant role in logical interdependencies in particular. In the previous example, the decline in financial standing of the power companies was due to human decisions. Another example is that summer vacationers may flock to the highways when gasoline prices are low, resulting in increased traffic congestion. In this case, the logical interdependency between the petroleum and transportation infrastructures is due to human decisions and actions and is not the result of a physical process.

Infrastructure Environment

Infrastructures operate in an environment described not only by their individual inputs, outputs, and states, but also by the characteristics of other infrastructures and certain general concerns. The infrastructure environment is the framework in which the owners and operators establish goals and objectives, construct value systems for defining and viewing their businesses, model and analyze their operations, and make decisions that affect infrastructure architectures and operations [16]. The operating state and condition

of each infrastructure influence the environment, and the environment in turn exerts pressures on the individual infrastructures. In a very real sense, infrastructures and the environment are interdependent. Using Fig. 1 as a guide, we describe general concerns that must be considered when investigating the environment and its influence on infrastructures. There is substantial overlap and no firm boundaries among these areas of concern—yet another manifestation of interdependencies in the environment.

Note that although the discussion has addressed infrastructures as entities, we do not assume they are homogeneous or connected. The water sector, for example, consists of tens of thousands of municipal suppliers that are not physically connected, and each is a separate business. In contrast, in the telecommunications sector, anyone with a telephone can easily connect with anyone else who has one.

Economic and business opportunities and concerns are major forces that shape the environment in which infrastructures evolve and operate. Innovation and technology provide opportunities for great gain, have in many ways created our interdependencies, and tend to be synergistic. Opportunities and concerns lead to fundamental constraints on infrastructure operational characteristics and behaviors, owner-operator decisions, and, in some cases, infrastructure architectures and topologies. The relative importance of these con-

cerns can be loosely tied to the degree of government ownership and regulation. Water systems, for example, are generally owned and operated by municipal governments (although privatization is becoming a more widely accepted business strategy). The owners focus on service provision rather than on the profit concerns that motivate private-sector owners. Nevertheless, they still must address economic and business concerns, such as the cost of changes to their system architectures, maintenance, technology upgrades, and changing service demands from growing or contracting communities. Other factors, such as financing, operations, just-in-time delivery practices, and staffing costs, affect the owner communities and shape business decisions and the environment. Business concerns of some government-supported infrastructures, such as Amtrak, may be highly politicized and therefore vital to the health and survival of those infrastructures.

Heavily regulated infrastructures are more constrained than unregulated, private-sector infrastructure firms. Owners are required to consider certain aspects of service provision over business concerns. These firms (including airlines, some energy companies, and common carriers in the telecommunications sector) have the same motivations as unregulated firms but operate under tighter constraints on permissible operations as set by regulation. Within these constraints, profitability, economics, and business concerns are paramount. The cost of financing, the availability of a skilled workforce, market competition, image, and related business issues are other important variables that help set constraints.

Information technology, deregulation, and the many business mergers during recent years are three forces that have dramatically affected the economic and business aspects of the infrastructure environment. Information technology provided business with a powerful tool to increase operational efficiency, but it subsequently led to the proliferation of cyber interdependencies (and new vulnerabilities) in most infrastructures. At the same time, the move toward deregulation of some sectors (such as energy) resulted in the shedding of excess capacity that had previously been mandated and had served as a shock absorber against system failures. Mergers further eliminated redundancy and overhead in infrastructure operations. The combination of these three forces has created an environment in which infrastructures are much more interdependent than in the past, have little or no cushion in case of failures, and have few if any alternative sources of service. These environmental changes have critical implications for interdependencies and their influences on infrastructure states and operating behaviors.

Public policy is another important environmental dimension. Legal and regulatory concerns are a distinct and important subset of public policy that we consider separately. Examples of nonregulatory public policies that affect infrastructure analyses include federal energy, security, and eco-

omic policies; policies that frame the federal response to disasters, such as the Federal Emergency Management Agency's Federal Response Plan; and policies that define regulatory jurisdiction, such as the Federal Communication Commission's (FCC's) decision to not regulate Internet service providers. These policies shape how industry and various levels of government operate, put bounds on the set of permissible operational states and characteristics, and influence the growth and structure of entire infrastructures. For example, the FCC's decision to not regulate the Internet created open-market conditions that, according to common wisdom, fueled the spectacular growth in the U.S. information technologies sector, the information infrastructure, and the number of cyber interdependencies.

Government investment decisions are another major aspect of public policy that influences the infrastructure environment. Research, development, and acquisition decisions have had a wide-ranging influence on many aspects of our lives and culture, ranging from the creation of entirely new infrastructures to small nudges of existing infrastructures. The government played a major role in the creation of infrastructures by investing in specific technologies that were highly risky, expensive, and lacked near-term return on investment—conditions that all but precluded private-sector investment. Such investments have frequently been in defense technologies, such as early research in computer networks (ARPANET) and satellite communications, upon which extensive commercial infrastructures eventually developed. More often, however, government investments have focused on clearly identified governmental needs and simply nudged new technologies onto the scene. However, the net effect of federal investments on large, firmly established infrastructures, such as in the \$3 trillion/year telecommunications industry, is typically small or negligible.

Legal and regulatory concerns form a special subset of public policy that warrants separate consideration. Categorizing all aspects of the effects of laws and regulations on the provision of services would require an exhaustive study; a few examples, however, are provided to illustrate their pervasive influence. Some legal and regulatory concerns directly affect infrastructure operations. The requirements of the Health Insurance Portability Accountability Act and the Gramm-Leach-Bliley Act, which hold corporations liable for the disclosure of private health and financial records, respectively, exemplify this trend. Others may influence infrastructure architectures and topologies, as did the Telecommunications Act of 1996. Among other things, this law established service requirements in underserved areas and mandated certain aspects of the infrastructure architecture itself.

A closely related consideration is *public health and safety*. Legal and regulatory actions that are designed to protect lives, property, and public health and safety directly affect the configuration and operation of the infrastructures and

thus their interdependencies. For example, environmental regulations in California that establish stringent power plant emissions standards to reduce air pollution and associated health-related problems directly influence decisions about system operation, new plant construction (technology selection and siting), reliance on SCADA and other electronic systems, and backup fuels. Each of these decisions affects the interdependencies among the infrastructures. Identifying, understanding, and analyzing such interdependencies are also of particular concern to the emergency services infrastructure, which is made up of fire, emergency medical, rescue, public health, law enforcement, and other services that support public health and safety at the local, state, and federal levels. Disruptions to the interdependent infrastructures (for example, if electric power system disruptions resulted in communications failures, water shortages, and extensive traffic congestion) can hinder their effective coordination and response to all disasters.

Technical and security issues underlie all aspects of interdependencies and the infrastructure environment. Technology is both an enabler of infrastructures and a primary source of interdependencies. Advances in technology, such as computerization and automation, have increased the efficiency, reliability, and service offerings of infrastructures. Infrastructure owners and operators must make business decisions about acquiring and inserting new technology to increase infrastructure functionality, add capability and capacity, or increase efficiency. Technology is largely responsible for the tightly coupled, interdependent infrastructures we enjoy today—extensive automation has dramatically increased cyber interdependencies across all infrastructures and concurrently increased their complexity. However, tighter, more complex, and more extensive interdependencies lead to increased risks and greater requirements for security.

We noted briefly that interdependencies can cause risk in one infrastructure to be a function of risk in another. If infrastructure i depends on infrastructure j , and j has a high risk of failure, then the likelihood of i being disrupted or failing is correspondingly higher than if i were independent of j . In a similar sense, security is a shared function—and responsibility—in interdependent infrastructures. Security weaknesses in one infrastructure increase the level of risk and decrease security in the other infrastructures that it supports. Consider a municipal water system powered by the local electrical grid. For this example, we assume that the electric power utility's SCADA system has security weaknesses that a hacker or terrorist could exploit [17]. If an attacker were to disrupt power generation by attacking the SCADA system, then the water system could suffer disruptions. The security of the water system is thus a function of the security of the electric power utility, as is the risk of disruption or failure.

As the PCCIP discussed in detail, physical and cyber security are paramount for infrastructure owners and operators. Physical security, although extremely important, is a

relatively mature field in which the threats and preventive measures are well understood. (The fact that they are well understood does not mean they are easy to detect or prevent—they are not.) Cyber security, however, is relatively new and represents a particular challenge to interdependent infrastructures. Given extensive cyber interdependencies, careful attention to cyber security is essential for virtually all modern infrastructures. Technological advances created the information infrastructure and its associated cyber security problems, and we frequently fall into the trap of believing that further technological advances will provide security solutions. In fact, no technical solution is effective without equal consideration of human factors, security practices and policies, and training. Information technology is also a moving target. Just as information technology advances permit dramatic improvements in infrastructure service offerings, capabilities, and efficiency, the very same advances also create new security issues and can even change the paradigm in which cyber security is considered. Trade-offs between functionality and security can dictate new methods of cyber and physical security that we cannot predict today.

Social and political concerns tie all environmental issues together. These concerns drive markets (economic/business, technical, and security) and elections (public policy, legal/regulatory, and technical). They create the perception that laws or regulations are needed (or not), a service is needed (or not), certain types of behavior are acceptable (or not), and certain protections are needed (or not). Less directly evident, yet critically important, are international social and political forces that shape the infrastructure environment. Many of today's infrastructures are inherently international. For example, the telecommunications, banking and finance, and oil and gas infrastructures are truly global in scope, and the U.S. and Canadian electric power infrastructures are inseparable. Political issues as diverse as OPEC decisions, hydroelectricity and salmon issues in the Pacific Northwest, instability in the Caucasus region, and foreign ownership of parts of the U.S. telecommunications infrastructure substantially affect the infrastructure environment. Political and social issues, at both national and international levels, are important variables that fundamentally shape the infrastructure environment and must be part of any comprehensive study of interdependencies.

Coupling and Response Behavior

We now examine the characteristics of the couplings among infrastructures and their effects on infrastructure responses to perturbations. The primary coupling characteristics are the degree of coupling (tightness or looseness), the coupling order, and the linearity or complexity of the interactions. The coupling characteristics and nature of the interacting agents in turn directly influence whether the infrastructures are adaptive or inflexible when perturbed or stressed.

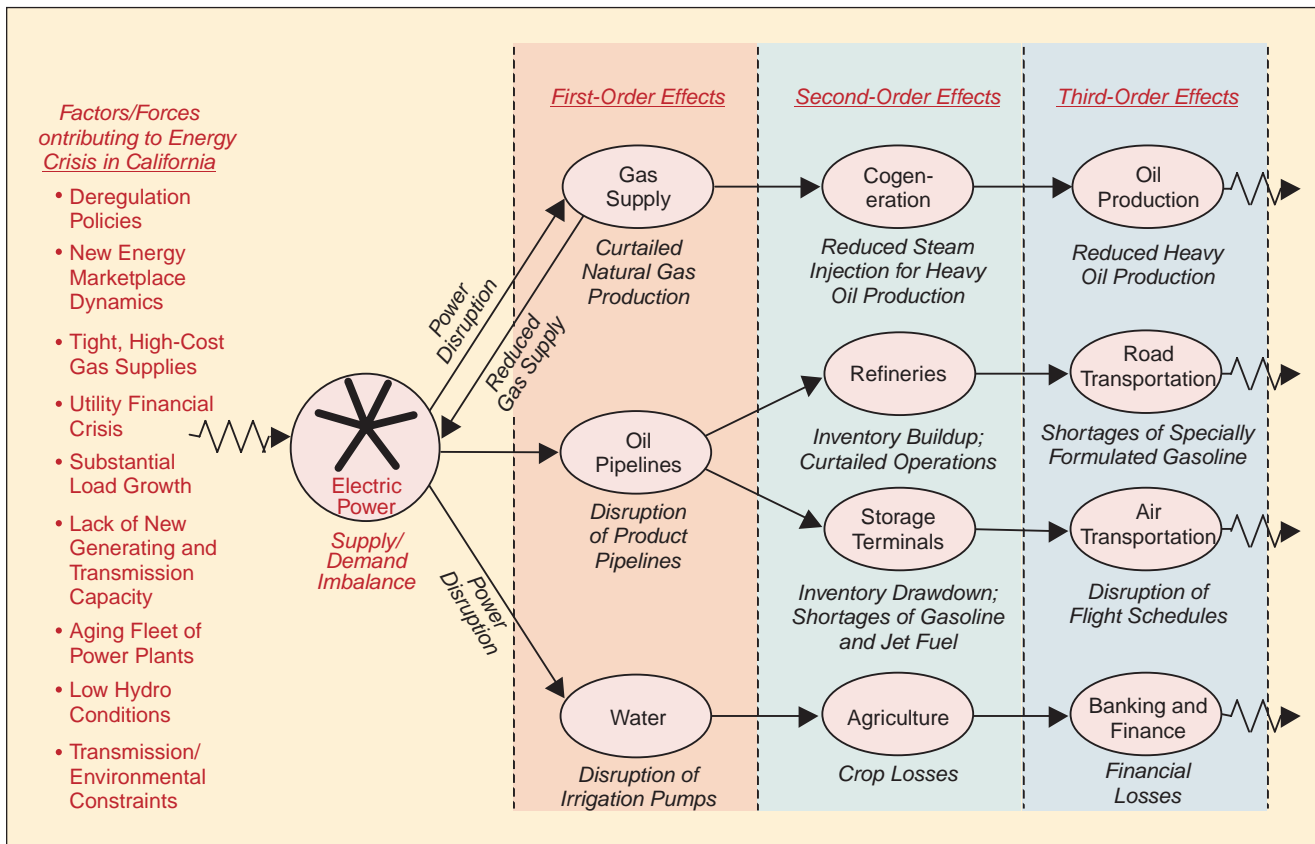


Figure 4. Examples of n th-order interdependencies and effects.

Borrowing from Perrow, we first classify linkages as either *tight* or *loose* depending on the relative degree of coupling [18]. Tight coupling refers to agents or infrastructures that are highly dependent on one another. Disturbances in one agent can be closely correlated to those in another agent to which it is tightly coupled. Disturbances tend to propagate rapidly through and across tightly coupled infrastructures. Tight coupling is characterized by time-dependent processes that have little “give” or slack. A natural-gas-fired electrical generator and the gas supply pipeline form a tightly coupled pair. In particular, if the gas-fired generator has no local gas storage and cannot switch to an alternative fuel, the generator is very tightly coupled to the gas pipeline. Disturbances in the gas supply will have almost immediate effects on electrical generation. Loose coupling, on the other hand, implies that the infrastructures or agents are relatively independent of each other, and the state of one is only weakly correlated to or independent of the state of the other. Slack exists in the system, and the processes are not nearly as time dependent as in a tightly coupled system. For example, a coal-fired electrical generator and the diesel-powered railroad network that supplies its coal are weakly coupled. Coal-fired generators often have two or three months’ supply of coal stored locally (although financial pressures are significantly reducing traditional levels of storage). Short-term disturbances in the rail supply system rarely affect power generation, so the state of the electrical

grid is thus weakly correlated to the state of the railroad through this specific interdependency. In sum, tight and loose coupling refer to the relative degree of dependencies among the infrastructures.

The *coupling order* indicates whether two infrastructures are directly connected to one another or indirectly coupled through one or more intervening infrastructures. Consider infrastructures i , j , and k , where i is linked to j , which in turn is connected to k , but k is not directly linked to i . Depending on the nature of the infrastructures and their interdependencies, changes in $State_i$ may drive changes in $State_j$, which in turn affect $State_k$. These indirect linkages and state changes are commonly referred to as n th-order interdependencies and n th-order effects, respectively, where n is the number of linkages. Of particular note is that feedback loops can also exist through n th-order interdependencies. If, for example, infrastructure i is coupled to j , j is coupled to k , and k is coupled through another route to i , then a feedback loop exists through the chain $i - j - k - \dots - i$.

The electric power problems in California provide numerous examples of such higher order interdependencies and effects. As depicted in Fig. 4, electric power disruptions at various times curtailed in-state natural gas production, the operation of petroleum product pipelines transporting gasoline and jet fuel within California and to Nevada and Arizona, and the operation of massive pumps used to move water for crop irrigation (first-order effects). In some cases,

gas production curtailed by power losses directly impacted gas supplies for generating units, further exacerbating power problems (feedback loop). Tight natural gas supplies also had the potential to shut down gas-fired industrial cogeneration units producing steam for injection into California's heavy oil fields (second-order effect), thus potentially reducing heavy oil recovery (third-order effect). Similarly, the disruption of product pipelines caused inventories to build up at refineries and draw down at the product terminals (second-order effects), including several major California airports. Declining jet fuel stocks at airports caused several major airline operators to consider contingency plans in the event of fuel shortages (third-order effects). In this

One effective way to investigate complex adaptive systems is to view them as populations of interacting agents.

case, the transportation infrastructure (specifically airlines) was affected by problems in the electrical grid through the intermediary petroleum distribution and storage network. Disruption of refinery operations also could have immediate repercussions on the transportation infrastructure because of the specially formulated gasoline used in California. In these real-world examples, disturbances rippled through and across the interconnected infrastructures and created n th-order effects.

The interactions among infrastructures can be further classified as either linear or complex. Perrow makes this distinction as follows:

Linear interactions are those in expected and familiar production or maintenance sequence, and those that are quite visible even if unplanned. ... Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible. [18]

Perrow likens linear interactions to an assembly line in which production is carried out in a series of steps or sequences. Linear interactions are generally those intended by design, with few unintended or unfamiliar feedback loops. Complex interactions are likely to exist when agents can interact with other agents outside the normal production or operational sequence, whether by design or inadvertently. Such interactions can occur in systems with branching paths, feedback loops, and jumps from one linear sequence of operations to another (possibly due to geographic interdependencies). Complex interactions are generally those not intended by design, and they can be subtle and difficult to detect.

A given infrastructure can contain numerous linear and complex interactions. When examining a given interaction, however, context becomes important. Consider a natural gas pipeline. When examined in isolation from other infrastructures and the environment, the flow of gas in the pipeline may appear to be a linear process with predominantly linear interactions: gas flows from some source, traverses a gas conditioning plant, passes through many compressor stations and gateways, and finally arrives at the consumer's location. However, in a broader context that includes couplings to other infrastructures and the environment, this apparently linear process can be complex. If, for instance, the electrical grid uses natural gas supplied by the pipeline as fuel and in turn produces electricity that powers the gas conditioning plants and compressor stations, then the coupled pipeline-electrical grid system behaves more as a complex set of interactions than as two isolated, linear infrastructures. The more intricate and diverse the interconnections among agents in the infrastructures, the more complex the interactions become.

Many analyses of individual infrastructures proceed in a linear fashion, however. Analyses often make the crucial assumption that *supporting* infrastructures will continue to provide an uninterrupted supply of their goods and services, regardless of any disturbance in the *supported* infrastructure. This assumption effectively decouples the supported infrastructure from its supporting infrastructures and focuses on the dependencies rather than on the interdependencies of the infrastructure in question. This simplistic approach may be valid for some analyses, but it overlooks the true complex nature of interconnected infrastructures. As such, it may lead to incorrect and potentially disastrous results. A clear understanding of context is thus vital in analyzing the couplings among infrastructures.

Finally, the characteristics of the agents comprising the infrastructures and their interdependencies influence whether a given infrastructure is adaptive or inflexible when stressed or perturbed. We previously noted that the hallmark of a CAS is its ability to learn from past experiences and adapt to future expectations. Numerous factors contribute to adaptability, including the availability and number of substitutes for critical processes or products, workarounds and contingency plans, backup systems, training and educational programs for operational personnel, and even human ingenuity in the face of disasters. Other factors may render infrastructures inflexible, such as restrictive legal and regulatory regimes, health and safety standards, social concerns, organizational policies, fixed network topologies, and the high cost of providing extensive backups and workarounds. A collection of flexible agents is more likely to respond well to disturbances and

continue to provide essential goods and services than is an inflexible, rigid system that is incapable of learning from past experiences.

Infrastructure Characteristics

Infrastructures have key characteristics that figure in interdependency analyses. The following paragraphs articulate several of the principal characteristics, including spatial (geographic) scales, temporal scales, operational factors, and organizational characteristics. The discussion below is not an exhaustive enumeration of key characteristics, yet it frames several important aspects that warrant consideration in models, simulations, and analyses.

Spatial scales can vary widely in infrastructure analyses. Considering infrastructure composition first, pertinent spatial scales range from individual parts to the metastructure composed of interdependent infrastructures and the environment. Extending Perrow's taxonomy [18], we can define a hierarchy of elements:

- *Part*: smallest component of a system that can be identified in an analysis.
- *Unit*: a functionally related collection of parts (e.g., a steam generator).
- *Subsystem*: an array of units (e.g., a secondary cooling system).
- *System*: a grouping of subsystems (e.g., a nuclear power plant).
- *Infrastructure*: a complete collection of like systems (e.g., the electric power infrastructure).
- *Interdependent Infrastructures*: the interconnected web of infrastructures and environment.

Closely related is the notion of geographic scales, given that infrastructures span physical spaces ranging in scale from cities, regions, and nations to international levels. The particular scale of interest is largely a function of the objectives of the analysis. Deliberations on national energy policies may require analyses at the infrastructure, interdependent infrastructure, national, and international levels, whereas an analysis of the failure of a single natural gas compressor might require studies at the system level and below. These granularity considerations lead to trade-offs in model fidelity and database/computational requirements: a high level of detail implies more data on the infrastructures, their components, and interdependencies, as well as more intensive computational requirements. Spatial scale has clear implications for the way in which interdependencies are included in analyses. At the part and unit levels, interdependencies may play only a minor role, if any at all. On the other hand, if it is to be accurate, an interdependent infrastructure analysis must include interconnections among the relevant infrastructures.

Infrastructure dynamics span a vast *temporal range*. Relevant time scales of interest vary from milliseconds (e.g., power system operation) to hours (e.g., gas, water, and transportation system operations) to years (e.g., infrastructure

upgrades and new capacity). Time scales have substantial implications for models and simulations, given that certain time-related infrastructure characteristics and interdependencies might not be relevant for a specific analysis. The tightness or looseness of a specific interdependency is somewhat related to its temporal dynamics and may determine whether that interdependency is pertinent to an analysis. For example, in an examination of the propagation of sudden failure in an electrical power grid, fast processes, such as some cyber interdependencies (with millisecond to hour dynamics), might be crucial to the analysis, particularly if SCADA and EMS systems figure prominently. Slower dynamics, however, such as rail delivery of coal to generators (on the order of weeks), the enactment of new energy regulations (years), or the construction of a new power plant (years to a decade or more), would not be issues if the analysis only examined a period of several days.

Operational factors influence how infrastructures react when stressed or perturbed. These factors are closely related to security and risk and include operating procedures; operator education and training; backups and redundant systems; emergency workarounds; contingency plans, including periodic reviews and updates; and security policies, including implementation and enforcement. Even human ingenuity and determination during emergencies play crucial roles in crisis management and mitigation. All of these factors are difficult to model, yet each could substantially alter the outcome of the analysis. For example, a security and risk analysis of a major telecommunications switch should include its physical interdependency with the electric power infrastructure and with its backup diesel generators. However, if the same analysis overlooked the resupply of diesel fuel to the emergency generators—interdependencies with the petroleum and transportation infrastructures—and water for cooling, then the analysis might lead to the wrong conclusions about the overall security and reliability of the switch. Likewise, the presence of inadequately trained computer network administrators at an electric power utility would lead to a decrease in the overall cyber security of the SCADA and EMS systems and consequently raise the level of risk in other infrastructures dependent on the utility's electric power.

Finally, *organizational considerations* are important determinants of infrastructure behavior. We previously discussed the effects of globalization, international ownership, regulation, government versus private ownership, corporate policies and motivations, and the regulatory environment. These organizational aspects can be key factors in determining the operational characteristics of infrastructures, with important security and risk implications. As a result, a comprehensive study of infrastructures and interdependencies should first evaluate the importance of these factors and determine whether they merit inclusion in a more detailed analysis.

Types of Failures

Interdependencies increase the risk of failures or disruptions in multiple infrastructures, as the power crisis in California has demonstrated. The subtle feedback loops and complex topologies created by interdependencies can initiate and propagate disturbances in a variety of ways that are unusual and difficult to foresee. We classify interdependence-related disruptions or outages as cascading, escalating, or common cause. These modes differ fundamentally from disruptions confined to a single infrastructure, given

Infrastructures are connected at multiple points such that a bidirectional relationship exists between the states of any given pair.

that interdependencies are necessary for the generation or propagation of these types of failures.

A *cascading failure* occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure. For example, the disruption of a distribution network within the natural gas infrastructure—the result of an accident, a natural event (earthquake, hurricane, flood, etc.), or an intentional act—can result in a failure (disruption) of an electric utility's generating unit located in the service territory of the gas system. This event in turn can lead to a shortage of generation in the area, which can cause power disruptions (a cascading failure from the natural gas infrastructure to the electric power infrastructure). By extension, the electric power failure could lead to disruptions in other infrastructures. Cascading failures such as the infrastructure disruptions due to California's power crisis, shown in Fig. 4, are also manifestations of *n*th-order effects.

An *escalating failure* occurs when an existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the severity or the time for recovery or restoration of the second failure. For example, a disruption in a telecommunications network, such as a failure in an end office, may escalate because of a simultaneous or subsequent disruption in a road transportation network, which in turn could delay the arrival of repair crews and replacement equipment.

A *common cause failure* occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause. Components from multiple infrastructure networks could be affected simultaneously, either because the components occupy the same physical space (a geographic interdependency) or because the root problem is widespread

(e.g., a natural disaster, such as an earthquake or flood, or a man-made disaster, such as a terrorist act). For example, telecommunications cables (both wire and fiber) and electric power lines often follow railroad rights-of-way, creating a geographic interdependency among the transportation, telecommunications, and electric power infrastructures. Consequently, a train derailment that damages the tracks could also disrupt communications cables and power lines that are located within the same corridor.

State of Operation

The state of operation of an infrastructure can be thought of as a continuum that exhibits different behaviors during normal operating conditions (which can vary from peak to off-peak conditions), during times of severe stress or disruption, or during times when repair and restoration activities

are under way. At any point in the continuum, the state of operation is a function of the interrelated factors and system conditions depicted in Fig. 1. In addition, the state of operation of a unit, subsystem, or system at the time of a failure will affect the extent and duration of any disruption or degradation in the services of an infrastructure. For example, events that occur at times of peak electric power, natural gas, or water demand, when telephone usage is heavy, or during periods of traffic congestion, will have different effects than similar events during nonpeak times.

Conceptually, the state of operation of an infrastructure can range from optimal design operation to complete failure with a total loss of service to all users (including all dependent infrastructures). Under certain conditions, an infrastructure can operate at well below the optimal design state (e.g., because one or more units, subsystems, or systems have failed) and still provide what the user perceives as full service. For example, generating units in the electric power infrastructure can be out of service for maintenance or repair with no limitation in service to users (electricity) as long as the condition does not occur during the peak usage period when reserve margins are critically low. Similarly, the inability of a natural gas network to reclaim gas from a storage system may have no effect on the users except during the peak heating season. Clearly, the timing and sequence of events that cause component failures and infrastructure disruptions are important in terms of the effect as perceived by the user.

To fully understand and analyze infrastructure interdependencies, it is necessary to determine, for each infrastructure, which other infrastructures it depends on continuously or nearly continuously for normal operations, which other infrastructures it depends on during times of high stress or disruption, and which it depends on to restore service following the failure of a component or components that disrupt the infrastructure. The normal operation of an infrastructure and the repair of a disrupted infrastructure

generally involve multiple functions (activities, processes, or operations). Some of the functions occur sequentially in time, whereas others occur in parallel. In some cases, such as for repair and restoration operations, there may be large uncertainties about the amount of time needed to successfully complete each step in the repair process. Such operational complexities, and the associated uncertainties, must be identified and incorporated into analysis frameworks to develop realistic and meaningful insights into normal operations and response and recovery strategies.

Modeling and Simulation Challenges

It should be apparent from our survey of the six dimensions that a comprehensive analysis of interdependencies is a daunting challenge. Today's modeling and simulation tools are only beginning to address many of the issues outlined above: the "science" of infrastructure interdependencies is relatively immature. Despite the long recognition that interdependencies are critical to the proper functioning of an economy and, more broadly, society in general, a deeper appreciation of their importance to economic and national security has developed only in the past decade. (Some military writings in the early 1900s described the importance of interdependencies in society to military operations. In the 1930s, the Air Corps Tactical School undertook a systematic study of interdependencies and codified its thoughts in a body of doctrine known as the "industrial web" theory [19]. However, it has only been during the past few years that this issue has taken on renewed interest. The PCCIP and CIAO emphasized and heightened the awareness of the security aspects of interdependencies. The challenges of the Y2K bug highlighted the importance of cyber interdependencies.) Fuller development of our understanding of interdependencies will require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology. We have already discussed many critical modeling and simulation factors. In the following paragraphs, we briefly outline some of the more important remaining R&D challenges and some of the promising analytic approaches designed to meet these challenges. (Much of the following material comes from discussions held during the joint White House Office of Science and Technology Policy (OSTP)–Department of Energy Workshop on Infrastructure Interdependencies (June 2000) and the deliberations of the OSTP-led interagency Interdependencies Working Group.)

Developing a comprehensive architecture or framework for interdependency modeling and simulation is a major challenge. Many models and computer simulations exist for aspects of individual infrastructures (e.g., load flow and stability programs for electric power networks, connectivity and hydraulic analyses for pipeline systems, traffic management models for transportation networks), but simulation frameworks that allow the coupling of multiple interdependent infrastructures to address infrastructure protection,

mitigation, response, and recovery issues are only beginning to emerge. This problem is exacerbated by the variety of classes of models in use: physics-based models, nodal analysis models, agent-based models, stocks-and-flows models, and more. A comprehensive architecture must:

- Leverage new or "legacy" (existing) software applications, including screening, network analysis, policy, consequence management, and impacts tools;
- Access a wide variety of data, possibly distributed over multiple sites, including threat data, dependency relationships, and repair and restoration sequences;
- Capture the dynamic interplay and coupling among models;
- Accommodate a broad range of analysis contexts, with widely varying spatial and temporal resolution and fidelity.

Recently, some progress has been made in integrating disparate model types and analyzing multiple infrastructures [20]–[27]. The results are encouraging and point out potential paths for development of an overall interdependencies framework. However, simply "hooking" several existing infrastructure models together generally does not work: every model has its own unique assumptions, data, and numerical requirements (such as time-step sizes, scaling limitations, or computational algorithms) that may not be compatible with other models. Further, such approaches generally do not capture emergent behavior, a key element of interdependency analysis.

Agent-based CAS approaches, which are being used to represent both the physics and finances of highly fluid, interdependent markets, have captured the interplay among economic and societal factors and the operation of multiple infrastructures [20]–[24]. Extensible actor-based software frameworks for the modeling, simulation, and analysis of interdependent infrastructures are also being developed [25]. Other approaches, such as those based on the Leontief economic model, compute flows of commodities and shared risks among sectors [26]. Hierarchical holographic modeling (HHM) has also been used successfully for modeling linkages among infrastructures and their external environments [27].

In addition to architecture, the nature of the available data is a fundamental concern of any modeling and simulation effort. A principal challenge is the sheer volume of data required to model multiple interdependent infrastructures to a reasonable degree of fidelity, particularly if the model contains several of the dimensions discussed above. The following are other data-related concerns:

- Real-time intake of data. Infrastructure topologies can change rapidly, one notable example being the information infrastructure. Catastrophes, such as major earthquakes or hurricanes, can rapidly destroy large sections of infrastructures.
- Database maintenance. Assembling a sufficiently detailed database (or databases) of infrastructure com-

ponents and topologies represents a major challenge. Maintaining the database(s) presents its own unique problems.

- Security and proprietary data issues. A highly detailed, comprehensive database of national infrastructures would be a valuable target for hackers, terrorists, and foreign intelligence services—particularly if it were coupled to advanced modeling and simulation tools. (Moonlight Maze, the name given to the operation traced back to Moscow (though not the Russian government) in which unclassified Department of Defense technology-related computer systems were compromised and sensitive data copied, illustrates the danger of collecting data into one unclassified comprehensive database. Coupled with comprehensive models, the information and ability to understand the dynamics of U.S. infrastructures would be very valuable to those who consider the United States an economic competitor or ideological enemy.) Maintaining a balance between the need for security and the need to provide such data to researchers will require substantial thought and effort. In addition, private infrastructure firms may be reluctant to share their proprietary data for such a database, even if granted full access to the information contained in the database for their own uses.
- Data may be distributed over multiple sites and maintained by multiple owners.

Metrics that describe the operating states of interdependent infrastructures and scale of interdependency-related disruptions are sorely lacking. These metrics should include a range of economic, social, and national security considerations. Such quantitative measures could be used to validate models and simulations through comparisons to real-world data; to develop a baseline and analyze historical data; and to prioritize interdependency-related vulnerabilities, threats, and risks. The metrics would need to be:

- Relevant to the effects they seek to measure;
- Suitable for use in developing data sets;
- Suitable for use in running and validating models;
- Helpful in prioritizing threats and risks;
- Suitable for comparing and measuring alternative responses to interdependencies.

Currently, there is no satisfactory set of metrics or models that articulates the risk of failures, either naturally caused or human induced, for highly interdependent infrastructures. This raises questions of risk management, liability, and insurability—a particularly important set of concerns given recent laws that outline corporate responsibility for certain aspects of information-intensive business. The risk management community—insurers, auditors, market analysts, and academics—is engaged in this issue, but no satisfactory metrics and practices are in place.

Given the importance of laws, regulations, policies, and other sociopolitical concerns to the infrastructure environ-

ment, it is essential to study their impacts on interdependent infrastructures in more detail. Some preliminary work has been undertaken in these areas, but our lack of knowledge far outweighs the results to date. Simulations and other tools that could assist policymakers and lawmakers with decisions affecting key infrastructures would be invaluable.

Conclusions

Identifying, understanding, and analyzing the interdependencies among infrastructures have taken on increasing importance during the past decade. Key technological, economic, and regulatory changes have dramatically altered the relationships among infrastructures, and the information technology revolution has led to substantially more interconnected and complex infrastructures with generally greater centralization of control. Indeed, the trend toward greater infrastructure interdependency has accelerated and shows little sign of abating. The PCCIP highlighted the role interdependencies play in the continuous, reliable operation of infrastructures—as well as the increased security concerns and risks that they bring.

The operational, R&D, and policy communities are beginning to accept the importance of infrastructure interdependencies and the need to more fully understand their influence on infrastructure operations and behaviors. Interdependencies, however, are a complex and difficult problem to analyze. We have taken an initial step in this direction by proposing a taxonomy to facilitate interdependencies research. The six “dimensions” of the taxonomy frame major aspects of interdependencies: types of interdependencies, infrastructure environment, coupling and response behavior, infrastructure characteristics, types of failures, and state of operations. The dimensions point to many new research questions, yet to date relatively little effort and few resources have been devoted to understanding this important field. However, given the magnitude of their impact on infrastructure operations, and, by extension, national and economic security, these questions must not go unanswered.

Acknowledgments

The authors would like to acknowledge the important contributions of Michael North (Argonne National Laboratory) and the White House Office of Science and Technology Policy Interdependencies Working Group.

References

- [1] S. Rosenbush, “Satellite’s death puts millions out of touch,” *USA Today*, May 21, 1998.
- [2] A. de Rouffignac, “Refineries could be subject to rolling blackouts,” *Oil Gas J.*, Jan. 23, 2001.
- [3] S. Fletcher, “Electric power interruptions curtail California oil and gas production,” *Oil Gas J.*, Feb. 13, 2001.
- [4] H. Anderson, “Increased threat of outages in California,” *UPI*, Feb. 14, 2001.
- [5] P. Behr and W. Booth, “Hot, dark summer ahead for California: Drought worsens power crunch, senators told,” *The Washington Post*, p. E01, Feb. 1, 2001.

- [6] M. Thompson, "Much of Northern California in the dark: Water pumps stopped," Jan. 17, 2001. [Online]. Available: <http://www.cnn.com/2001/US/01/17/power.woes.03/index.html>
- [7] P. Arrillaga, "Nation: Energy crisis not limited to California," Feb. 4, 2001. [Online]. Available: <http://www.nandotimes.com>
- [8] P. Connoles, "Calif. power crisis may become national mess," *Reuters*, Feb. 15, 2001.
- [9] M. Klare, "California's power crisis: A warning to all," *Pacific News Service*, Feb. 7, 2001.
- [10] M. Boslet and S. Harris, "California's dark days lie ahead," *The Standard*, Feb. 13, 2001. [Online]. Available: <http://www.thestandard.com/article/display/0,1151,22098,00.html>
- [11] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (1997). [Online]. Available: <http://www.ciao.gov>
- [12] *Merriam Webster's Collegiate Dictionary* (10th ed.), Springfield, MA, 1993.
- [13] Presidential Decision Directive 63. [Online]. Available: <http://www.ciao.gov>
- [14] A. Axelrod and M.D. Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York: Free Press, 1999, pp. 32-61.
- [15] E. Bonabeau, M. Dorigo, and G. Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems*. Oxford, U.K.: Oxford Univ. Press, 1999.
- [16] A.P. Sage, *Systems Engineering*. New York: Wiley, 1992.
- [17] A. Verton, "Experts debate U.S. power grid's vulnerabilities to hackers," *Computerworld*, Mar. 2, 2001 [Online]. Available: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58300,00.html
- [18] C. Perrow, *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, 1984, pp. 89-100.
- [19] R. Finney, *History of the Air Corps Tactical School, 1920-1940*. Washington, D.C.: Center for Air Force History, 1992.
- [20] C.M. Macal and D. Sallach, Eds., *Proc. Workshop on Agent Simulation: Applications, Models, and Tools*. Washington, D.C.: Argonne National Lab., Sept. 2000.
- [21] D. Sallach and T. Wolsko, Eds., *Proc. Workshop on Simulation of Social Agents: Architectures and Institutions*, Washington, D.C.: Argonne National Lab., June 2001.
- [22] M. North, "Agent-based modeling of complex infrastructures," in *Proc. Workshop Simulation of Social Agents: Architectures and Institutions*, Chicago, IL, 2000, pp. 239-251.
- [23] M. North, "SMART II: The spot market agent research tool, version 2.0," presented at SwarmFest 2000, Logan, UT, Mar. 2000.
- [24] M. Amin, "Toward self-healing infrastructure systems," *IEEE Computer Applicat. Power*, pp. 20-28, Jan. 2001.
- [25] C. Unal, K. Werley, and P. Giguere, "Energy interdependence modeling and simulation," Tech. Rep. LAUR-01-1879, Los Alamos National Laboratory, Apr. 2001.
- [26] Y. Haimes and P. Jiang, "Leontief-based model of risk in complex interconnected infrastructures," *J. Infrastructure Syst.*, Mar. 2001.
- [27] Y. Haimes, *Risk Modeling, Assessment, and Management*. New York: Wiley, 1998.

Steven M. Rinaldi is the Chief, Modernization and Technology Issues Branch, Air Force Quadrennial Defense Review Office. His research and staff positions in the Air Force include performing research on high-energy lasers and optics and managing international cooperative military R&D. He was a military exchange scientist at École Polytechnique, France, where his research activities included nonlinear optics and light scattering. He has served as the Senior National Security Officer in the White House Office of Science and Technology Policy. He received a Ph.D. in physics and an M.S. in electro-optics from the Air Force Institute of Technology.

James P. Peerenboom is the Director of the Infrastructure Assurance Center at Argonne National Laboratory, where he has provided technical support to the President's Commission on Critical Infrastructure Protection, assisted the White House Office of Science and Technology Policy in developing a critical infrastructure assurance R&D road map, and led infrastructure interdependencies and vulnerability assessment programs for various government agencies. He received a Ph.D. in energy and environmental systems and an M.S. and a B.S. in nuclear engineering from the University of Wisconsin-Madison.

Terrence K. Kelly is the Senior National Security Officer in the White House Office of Science and Technology Policy and an Active Duty Army officer. Prior to joining the White House Staff, he served in many field and staff positions, including the 82nd Airborne Division, with which he deployed on Operation Urgent Fury to Grenada; the Army Staff; the Secretary of the Army's Legislative Affairs Staff; and as the Chief of Staff of the national Critical Infrastructure Assurance Office. He has been a visiting faculty member at Rensselaer Polytechnic Institute's Mathematical Sciences department, a faculty member at West Point's Systems Engineering department, and a White House Fellow. He is a 1982 West Point graduate and holds a Ph.D. in mathematics and an M.S. in computer and systems engineering, both from RPI.