ELECTRIC PERSPECTIVES

January/February 2002

STUDYING THE CHAIN REACTION

By James P. Peerenboom, Ronald E. Fisher, Steven M. Rinaldi, and Terrance K. Kelly

Jim Peerenboom is director of and Ron Fisher is a researcher with the Infrastructure Assurance Center at Argonne National Laboratory in Argonne, IL. Steve Rinaldi is the chief of the Modernizations and Technology Issues Branch, Air Force Quadrennial Defense Review Office. Terry Kelly is the senior national security officer in the White House Office of Science and Technology Policy.

Interdependency studies show how the dominoes can fall and what infrastructure operators must do to keep them standing.

The nation's energy infrastructure—the electric power, oil and natural gas production, transmission, storage, and distribution systems that fuel and power the economy—is inextricably interconnected with other critical infrastructures. Our nation and economy depend on energy, telecommunications, water supply systems, transportation (road, rail, air, and water), banking and finance, emergency and government services, agriculture, and other systems and processes that produce and distribute essential goods and services. Collectively, these systems underpin almost every aspect of our lives.

In the new economy, these interconnected infrastructures have become increasingly fragile and subject to disruptions that can have broad regional, national, and global consequences. The September 11 terrorist attacks on the World Trade Center in New York City, for example, set off a complex chain of local, regional, national, and global infrastructure and interdependency-related impacts. At the local level, the attacks disrupted electric power, telecommunications, transportation, financial services, and other infrastructures. For example, two ConEd substations that served a large area of lower Manhattan were destroyed when the World Trade Center buildings collapsed. Local landline telephone outages occurred due to damaged facilities, and cellular service quickly became overloaded. Financial markets were closed, and three subway stations were heavily damaged. Regional rail transportation to and from

the city was also briefly halted. Electricity outages exacerbated many infrastructure repair and restoration efforts.

Nationally, all air transportation was halted. Commercial flights did not resume until several days after the attacks. Road transportation was disrupted at border crossings, thereby affecting just-in-time delivery of manufacturing parts. Auto manufacturers were hard hit by long backups at major ports of entry. Refiners, reacting to reductions in air travel, reconfigured their production slates to make less jet fuel. Trading on the U.S. stock market was suspended for four days, affecting global financial markets. Liquefied natural gas tankers, which supply nearly 20 percent of the natural gas distributed throughout New England, were banned from Boston Harbor in response to security concerns. And world oil prices rose immediately after the attacks, later falling as the negative impacts on the US and global economy became evident. Heightened security measures are now being taken to protect power plants and grids, telecommunications networks, water supply facilities, bridges, ports and rail lines, financial institutions, and other critical infrastructures. (See the sidebar, "CIP Challenges and Solutions.")

Different Disasters

But there is a wide range of infrastructure disruption and effects. In California, electricity outages in early 2001 affected oil and natural gas production, refinery operations, pipeline transport of gasoline and jet fuel within California and to its bordering states, and the movement of crop irrigation water. The disruptions also idled key industries, led to billions of dollars of lost productivity, and burdened the entire Western power grid, causing security and reliability concerns.

In July 2001, a train carrying chemicals and paper products derailed in a downtown Baltimore tunnel, caught fire and, in the ensuing five days, caused a series of infrastructure failures and public safety problems. The train leaked several thousand gallons of hydrochloric acid into the tunnel, and the fire caused a water main to burst. More than 70 million gallons of water spread over the downtown area, flooding buildings and streets and leaving downtown businesses without water. The fire also burned through fiber-optic cables, causing widespread telecommunication problems, while the fire and burst water main damaged power cables and left 1,200 Baltimore buildings without electricity.

In June 1999, a supervisory control and data acquisition (SCADA) system failure is suspected of contributing to a pipeline incident in which approximately 277,000 gallons of gasoline leaked from the

Olympic Pipeline in the state of Washington. The leaking gasoline caught fire, destroyed one and half miles of shoreline, and killed three people. The pipeline was shut down for nearly 18 months. During this time, tanker trucks and barges were used to transport petroleum products, leading to higher retail prices.

So, disruption in one system causes disruptions in others. Interdependency studies are aimed at identifying and understanding the range of potential vulnerabilities. Such studies involve analyzing infrastructure-to-infrastructure linkages (dependencies) to identify the key infrastructure components that, if lost or degraded, could adversely affect the performance of other infrastructures. An infrastructure service provider must answer a number of questions. Does another infrastructure affect yours directly or indirectly? Do dependencies on other infrastructures hinder your response and recovery efforts? What backup systems or other mitigation mechanisms are in place to reduce the impacts? This information provides a foundation for making defensible, cost-effective infrastructure operation and management decisions to ensure the security and reliability of interdependent systems.

The Meaning of Interdependency

The importance of infrastructure interdependencies was highlighted in 1998, in "Critical Foundations: Protecting America's Infrastructures," the report of the President's Commission on Critical Infrastructure Protection. (See the sidebar,"Protecting Power.") The commission recognized that the security, economic prosperity, and social well-being of the nation depend on the reliable functioning of our increasingly complex and interdependent infrastructures. The commission noted that the "disruption of any infrastructure is always inconvenient and can be costly and even life threatening. Major disruptions could lead to major losses and affect national security, the economy, and the public good. Mutual dependence and interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways they never have been before." The report went on to state that "this creates an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. It also creates new assurance challenges that can only be met by a partnership between owners and operators and government at all levels."

"Interdependence" implies that two or more infrastructures depend on each other. Such linkages vary in scale and complexity and can be described in four general categories:

- physical, where the material output of one infrastructure is used by another;
- cyber, where an infrastructure depends on information transmitted through the information and communications infrastructure;
- geographic, where two or more infrastructures are co-located, such as in a common utility corridor, and can be affected by a local event; and n logical, where the state or condition of an infrastructure depends on the state of another infrastructure in a way that is not physical, cyber, or geographic (for

example, linkages through financial markets).

We have generally considered interdependencies to be physical and geographic. For example, electric power generators depend on natural gas for their operation while, at the same time, the gas industry depends on electric power for control systems, storage operations, and other critical functions. Virtually all infrastructures are negatively affected by extended power disruptions; similarly, the electric sector may be negatively affected when natural gas, telecommunications, and water supply systems are disrupted. In addition, infrastructure components—such as transmission lines, buried gas pipelines, and telecommunications cables—often share common corridors, multiplying the systems and vulnerabilities to local physical hazards and sabotage.

But the proliferation of information technology (IT), the increased use of automated monitoring and control systems (such as the SCADA systems used by the energy and other infrastructures), and the reliance on the open marketplace for purchasing and selling infrastructure commodities and services have increased the prevalence and importance of cyber and logical interdependencies. Information and communications systems have linked infrastructures in new and complex ways. They also have created a host of new vulnerabilities. The dependence of the new energy marketplace on the internet and other e-commerce systems, and the complicated links to financial markets, highlight the breadth of cyber and logical interdependencies.

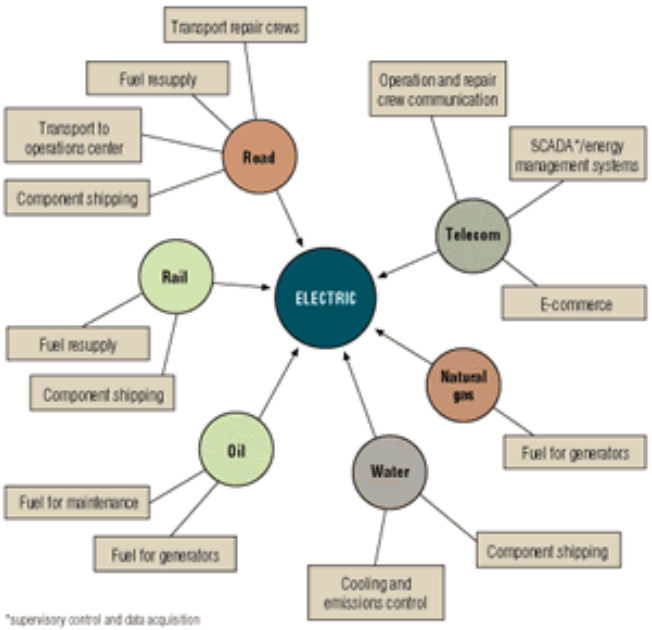
By definition, infrastructure interdependencies transcend individual sectors and generally transcend individual companies. Further, they vary in scale and complexity, ranging from local linkages (e.g., municipal water supply systems and local emergency services), to regional ones (e.g., electric power coordinating councils), to national ones (e.g., interstate natural gas and transportation systems), to international ones (e.g., telecommunications, banking, and financial systems). These scale and complexity differences create a variety of spatial, temporal, and system representation complexities that are not well understood or readily analyzed.

Such gaps in understanding and analytic capability are apparent in the context of analyzing multiple contingency events involving interdependent infrastructures. Each linkage in the electric power

infrastructure (for instance) has important, and potentially different, spatial, temporal, and system characteristics. (See Figure 1.)

FIGURE 1

ELECTRIC INFRASTRUCTURE DEPENDENCIES



Extending this dependency notion to multiple infrastructures, Figure 2 depicts a "system of systems" perspective. The complexity of multiple linkages and the implications of multiple contingency events that may affect infrastructures are apparent even in this simplified representation.

Fitting the Pieces Together

Three types of failures can affect interdependent infrastructures.

- A cascading failure is a disruption in which one infrastructure causes a disruption in a second.
- An escalating failure is a disruption in one infrastructure that exacerbates an independent disruption of a second infrastructure (e.g., the time for restoration of an infrastructure increases because another infrastructure is not available).
- A common cause failure is a disruption of two or more infrastructures at the same time as the result of a common cause (e.g., natural disaster).

In Figure 3, for example, a cascading failure is initiated by a disruption of the microwave communications network used for the SCADA system. The lack of monitoring and control capabilities causes a large generating unit to be taken offline; that, in turn, causes a loss of power at a distribution substation, which leads to blackouts in the area. The outages affect traffic signals, and this problem causes an escalating failure as it increases travel times and causes delays in repair and restoration activities.

The state of operation of an infrastructure (which can range from normal operation to various levels of stress, disruption, or repair and restoration) must also be considered. For example, hourly, daily, weekly, and seasonal variations in load, outages, maintenance schedules, reserve capacity, weather, and other operational factors may change the character and importance of system interdependencies. Further, an understanding is necessary both of backup systems or other mitigation mechanisms that reduce interdependence problems, and of the change in interdependencies as a function of outage duration and frequency. This adds complexity to the entire calculus.

The degree to which infrastructures are linked strongly influences their operational characteristics. Some linkages are loose and thus relatively flexible, such as the linkage between a coal-fired generator that maintains a large, local coal stockpile and the rail system that delivers the coal. Short-term disruptions of the rail delivery system may not affect power generation. Other linkages are tight, leaving little or no flexibility for the system to respond to changing conditions. For example, a gas-fired generator likely would be immediately affected by a disruption in the gas supply. Generally, highly utilized and optimized systems tend to be brittle, and seemingly modest changes in stress on the system can rapidly cause problems.

Interdependent infrastructures also can display unique characteristics that affect their ability to adapt to changing system conditions. For example, electric power systems, which are the ultimate in just-in-time delivery, operate on time scales of seconds and milliseconds. Other infrastructures operate on much longer time scales—natural gas systems, for example, can have significant local storage to mitigate short-term problems.

Infrastructure Environment

Other dimensions must also be considered. (See Table 1.) For example, the operating state of each infrastructure influences the environment, and the environment in turn exerts pressures on individual infrastructures. In a real sense, infrastructures and the environment are interdependent, making interdependency studies even more complex.

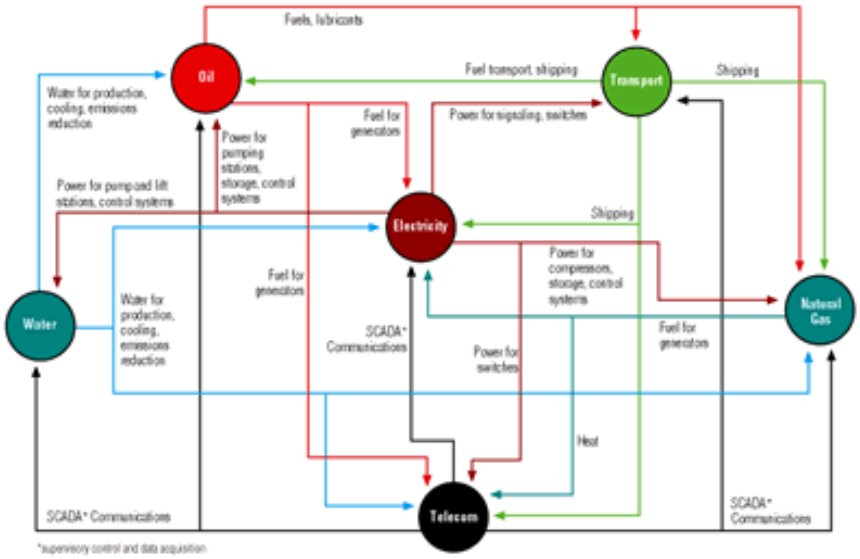
Economic and business concerns, for example, shape the environment in which infrastructures evolve and operate. Innovation and technology provide opportunities for great economic gain—they also foster interdependencies. The particular directions that business takes in organizing an infrastructure lead to basic constraints on its operational characteristics and behaviors, owner-operator decisions, and, in some cases, infrastructure architectures.

The relative importance of these concerns can be tied loosely to the degree of government ownership and regulation. Heavily regulated infrastructures are more constrained than unregulated ones—owners must consider certain aspects of service provision over business concerns. Within these constraints, profitability, economics, and business concerns are paramount. Whatever the degree of regulation, 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.

IT, deregulation, and multiple business mergers during recent years are three forces that have

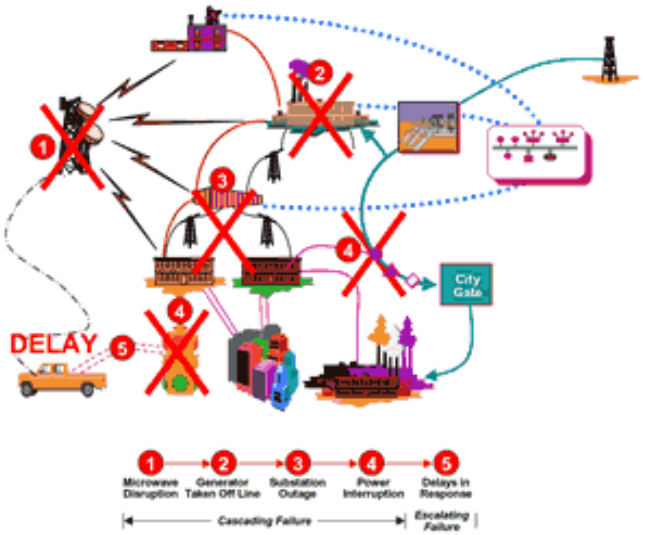
FIGURE 2

SYSTEM OF SYSTEMS



dramatically affected the economic and business aspects of the infrastructure environment. IT 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 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. Examples of nonregulatory public policies that affect interdependency studies include federal energy, security, and economic policies; policies that frame the federal response to disasters; and policies that define regulatory jurisdiction. 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 Federal Communication Commission's decision not to regulate the Internet created open-market conditions that fueled the amazing growth in the US IT sector, the information infrastructure, and the number of cyber interdependencies.



Government investment 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 ones. The government played a significant 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 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.

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—they have an effect on how those infrastructures work. Others may influence infrastructure architectures, 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.

TABLE 1

FIVE DIMENSIONS OF INTERDEPENDENT INFRASTRUCTURES

Types of failure

- Common cause
- Cascading
- Escalating

Infrastructure characteristics

- Organizational
- Operational
- Temporal
- Spatial

States of Operation
- Repair/restoration
- Normal
- Stressed/disrupted

Types of interdependencies
- Geographic
- Logical
- Cyber
- Physical

Environmental effects
- Health/safety
- Social/political
- Security
- Technical
- Public policy
- Legal/regulatory
- Business
- Economic

Coupling and response behavior
- Adaptive
- Loose/tight
- Inflexible
- Linear/complex

A closely related consideration is public health and safety. Legal and regulatory actions designed to protect lives, property, and public health and safety directly affect the configuration and operation of infrastructures. For example, environmental regulations in California that establish stringent powerplant emissions standards to reduce air pollution and associated health-related problems directly influence decisions about system operation, the construction of new plants (technology selection and siting), reliance on SCADA and other electronic systems, and backup fuels. Each of these decisions also affects the interdependencies among the infrastructures.

Identifying, understanding, and analyzing such interdependencies are also of particular concern to the emergency services infrastructure—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 result in communications failures, water shortages, and extensive traffic congestion—can hinder their effective coordination and response to disasters.

Tighter Dependencies, Increased Risks

Technical and security issues underlie all aspects of interdependencies. 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 new technology to add capability and capacity or increase efficacy. Technology is largely responsible for the tightly coupled, interdependent infrastructures we enjoy today—but extensive automation has dramatically increased cyber interdependencies across all infrastructures and concurrently increased their complexity. Tighter, more complex, and more extensive interdependencies lead to increased risks and greater requirements for security.

As noted earlier, physical security, although extremely important, is a relatively mature field in which the threats and preventive measures are well understood. Cyber security, however, is relatively new and represents a particular challenge. 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.

IT is also a moving target. Just as it 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 the 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, services, and certain protections are needed (or not), and that certain types of behavior are acceptable (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 US and Canadian electric power infrastructures are inseparable. Political issues as diverse as Organization of Petroleum Exporting Countries decisions, hydroelectricity and salmon issues in the Pacific Northwest, foreign ownership of parts of the US telecommunications infrastructure, and war in central Asia, 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.

Learning More

Today's modeling and simulation tools are only beginning to address many of those issues: 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. Fuller development of our understanding of interdependencies requires a comprehensive interdisciplinary research and development agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology.

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.

According to the North American Electric Reliability Council, in the highly interconnected economy of the future, hostile—and non-hostile—disruptions will have more potential to reverberate through our critical infrastructures. Public- and private-sector infrastructure owners and operators and others involved in critical infrastructure protection need to develop a greater awareness of interdependencies and a more complete understanding of what they mean. The appropriate role of local, state, and federal governments in support of the private-sector response to disruptions also needs to be defined. Failure to understand how disruptions to one infrastructure could cascade to others, exacerbate response and recovery efforts, or result in common cause failures leaves planners, operators, and emergency response personnel unprepared to deal effectively with the impacts of such disruptions.