2012

On Critical Infrastructure Interdependency

Polinpapilinho F. Katina
Old Dominion University

C. Ariel Pinto
Old Dominion University

Original Publication Citation

Katina, P. F., & Pinto, C. A. (2012). On critical infrastructure interdependency. *Annual International Conference of the American Society for Engineering Management 2012, ASEM 2012 - Agile Management: Embracing Change and Uncertainty in Engineering Management, 17-20 October 2012, Virginia Beach, Virginia* (pp. 29-38). American Society for Engineering Management.

Annual International C-onference of the American Society for Engineering Management 2012 (ASEM 2012)

Agile Management: Embracing Change and Uncertainty in Engineering Management

Virginia Beach, Virginia, USA
17-20 October 2012

ISBN: 978-1-62748-282-0

ON CRITICAL INFRASTRUCTURE INTERDEPENDENCY

Polinpapilinho F. Katina, Ph.D. Student., Old Dominion University
C. Ariel Pinto, Ph.D., Old Dominion University

Abstract
Developing effective protection, mitigation, and recovery measures for critical infrastructure (CI) systems is paramount in the wake of increasing natural and manmade hazards, risks, and threats. Influencing protection, rescue, and recovery measures are interplays (i.e., interdependencies) among infrastructure systems. Understanding interdependencies plays an essential role in minimizing and reducing cascading failures among complex interdependent infrastructure systems. This paper asserts that deployment of protection, mitigation, and recovery *solutions* can have little effect on infrastructure management if infrastructure operators and policymakers have partial understanding of infrastructure interdependencies. Using narrative research, authors illustrate that effective coordination and response for protection, mitigation, and recovery requires understanding complex interdependencies among infrastructures. Themes commonly associated with CI protection are examined from an interdependency perspective. Using the healthcare sector as an example, authors discuss potential complexities and interdependencies in sustaining public health. This paper concludes with a need for methodological approaches capable of holistically analyzing infrastructure systems.

Keywords: Critical infrastructure, critical healthcare infrastructure, interdependencies, healthcare, system

Introduction

In the 21st century, the well-being of the public is intrinsically intertwined with certain infrastructures and key asset provisions. The destruction of key assets can cause large-scale property damages, human injury and/ or death. Furthermore, the destruction of key assets can profoundly damage national prestige and confidence (Bush, 2003). Hence, such infrastructures are vital to national security, national economic security, and national public health or safety. Collectively known as critical infrastructures (CI), such "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Congress, 2001, 115 Stat. 401). Because the United States of America and other well-developed nations heavily depend on products, goods, and services that such infrastructure systems provide, there has been an unprecedented need to protect such CIs. What do such systems include? How did they come to be critical? In addition, what are we doing about managing them? A simple literature review reveals that there is marginal consensus on what constitutes CIs. For example, Bush (2003), Thissen and Herder (2003), and the U.S. Department of Homeland Security, DHS, (2006) view CI differently.

As the demand for provisions (products, goods, and services) has increased, so has inside and outside influence that disrupt normal operations of the infrastructure system activities and processes rendering such systems inoperable. The inoperability of CI is linked to several societal changes that have occurred in the late 20th and 21st century. For example, Thissen and Herder (2003) stipulate that technological advancement, rapid institutional changes, increasing complexity, trans-boundary dependencies, and increasing demand for quality services coupled with increasing natural threats present a grave challenge for policymakers, engineers, and scientist in sustaining societal operations. The need for understanding of infrastructure relationships is especially essential in CI because infrastructure systems do not operate in isolation. The intricate interdependencies among infrastructures have already illustrated that there is a need for a shift in the infrastructure management paradigm. For example, a single blackout in Germany on November 4, 2006 caused loss of power for millions in France, Italy, Spain, and Austria. Cascading unintended electric failure resulted in transport systems (i.e., trains, traffic signals) delays and disruptions of other interconnected operations (UCTE, 2006)

It is from this perspective that this paper espouses that understanding the relationship among elements, components, and infrastructure systems is an essential step in improving infrastructure designs, protection, and security measures. Using a narrative research approach (Patton, 2002), authors explore potential interrelationships among infrastructure systems using themes associated with CI research. To achieve this objective, this paper is divided into several sections. First, authors provide the reasoning behind the need for dependable infrastructure systems. Second, examination of themes commonly associated with CI research is established. Each established theme is essential in understanding interconnectedness among infrastructures. Third, the term interdependency is explored in the context of dependable infrastructure systems to illustrate that sustaining public well-being requires dependable interdependent systems. In section four, critical healthcare infrastructure (CHI) is used as an example to illustrate complexity and interdependencies. The paper concludes with several future research questions under consideration.

The Need for Dependable Infrastructures

While much has been written regarding CIs since 2000, the concept of dependability has not been addressed sufficiently. In infrastructure systems, dependability means an infrastructure is performing normal, especially when its services are needed. Revisiting the CI definition, this suggests that the concept of dependability and objectives of public health, economy, and security are intrinsically related. For example, whenever the destruction of a dependable infrastructure occurs, severe impact to public health/safety, economy or any combination of those matters ensues. Consider the events that shocked the world on September 11, 2001. Four planes were hijacked from a dependable aviation sector leading to over 2,500 deaths, over 6000 injured, loss of power and water, closure of the New York Stock Exchange, all of which affected the local as well as the international economy and security (Kröger & Zio, 2011). Hence, dependability of the aviation sector is linked to public health, economy, and security. Following the same logic, authors stipulate that for the inoperable infrastructure systems to cause debilitating impact on the public health, security and/or economy, the infrastructure system must have the ability to weaken people's *way-of-life*. Therefore, infrastructure systems that the public heavily depends upon have this ability. Identifying such infrastructure systems is an essential element in making society more prepared for failures in such systems. From this perspective, the term *dependable* is critical in advancing current dialog and essential in future research.

For the most part, the drive for dependable infrastructure systems has emerged out of shocking events. For example, Fletcher (2002) and Moteff (2010) espouse that the events of 9/11 have had a tremendous impact on infrastructure research and how current society views certain systems. For example, following 9/11, President Bush signed Executive Order No. 13228 and 13231 in 2001, the U.S. Congress passed USA Patriot Act of 2002 and established DHS in 2002 to help sustain the public well-being via protection and restoration of critical assets. Hence, DHS sets the "concept of operations...approaches, processes, coordinating structures, and incident-related actions required for the protection and restoration of CIKR [Critical Infrastructure and Key Resources] assets, systems, networks, or functions within the impacted area and outside the impacted area at the local, regional, and national levels" (DHS, 2008, 6).

However, the concept of the need for dependable infrastructure systems started well before the events of 9/11. For example, Thissen and Herder assert that "the functioning of modern society...depends on the quality of infrastructure facilities available"...and that "over time infrastructures have become increasingly *critical* to the functioning of society, as economic and social processes to a large extent rely on the services provided by such systems" (2003, 1). Bringing the leaders of government, academia, and industry together to discuss current and future issues of critical importance and how using science and technology can foster regional economic development, the International Conference on *Technology, Policy, and Innovation* used a theme of *Critical Infrastructure* during the fifth conference that was held in June 2001 at The Hague.

During this conference, as illustrated in the subsequent publications, the conference established that certain systems are critical to sustaining public well-being in well-developed nations. Effectively known as infrasystems, transportation, telecommunication and information systems, energy systems, and water systems were recognized as critical to sustain minimum operation of society and its governments (Thissen & Herder, 2003). While the conference in The Hague focused on a few infrastructures, recent events have indicated that critical infrastructures go beyond those outlined in 2001. For example, Harrington, Miller, and Wang (2005) note that healthcare systems (i.e., hospitals, ambulatory and nursing care facilities, insurance companies, pharmaceutical manufactures, etc.) heavily contribute to the well-being of the society. Hence, the list of infrastructure systems that are critical is not limited to some *official* list of infrastructure; rather any infrastructure system that has implications on public health, economy, and security is critical.

The public's increasing dependency on certain systems (e.g., agriculture and food, water systems public health and safety, emergency services, electricity, etc.) along with rapid institutional changes (i.e., shifting from public to private, deregulation, privatization, market driven economies, etc.) and increasing technological changes have changed the landscape of traditional infrastructure systems (Gheorghe, 2006). Furthermore, increased demand for quality services, coupled with tensions of profitability, globalization, and trans-boundary dependencies have had tremendous impact on operations of infrastructure systems such that infrastructure systems are now intricately interconnected resulting in complex infrastructures with intricate relationships. The *old* structure of centralized electricity offered the advantage of being simple and easy to coordinate, but Gheorghe (2006), argues that this structure has been transformed via liberalization and internationalization (i.e., a decentralized control of systems across multiple actors who are responsible for system performance). Such changes have resulted in unforeseen infrastructure dynamics that ensure that infrastructures cannot be operated in isolation. The result is what researches are refereeing to as a *system- of-systems* whose function depends on the performance of individual complex systems (Jovel & Jain, 2009; Kröger & Zio, 2011). This stems from the realization that a seemingly isolated infrastructure failure can cause cascading failures because of interdependency and could eventually cripple the whole infrastructure system-of-systems.

By characterizing infrastructure as a system, researchers are realizing that infrastructures are comprised of "a set of elements so interconnected as to aid in driving toward a defined goal" (Gibson, Scherer, & Gibson, 2007, 2). Authors maintain that public *way-of-life* is a product of well-interconnected complex systems that must work as an integrated system-of-systems to fulfill objectives of the society. Following the logic that infrastructure systems do not operate in isolation, authors stipulate that infrastructure research benefit from a careful examination of dependency, exposure, interdependency, resiliency, risk, and vulnerability all of which is necessary for the understanding of the interplay that can exacerbate consequences, hazards, risks, and threats in the management of infrastructure systems.

Major Themes in CI

Successfully producing the desirable outcomes depends on whether each system is dependable. Hence, in designing infrastructure to be dependable, it is necessary to understand relationships that can exist among infrastructure systems. Expounding on the idea of dependability, authors provide a synthesis of themes commonly associated with concepts in CI research. Such themes, authors argue, illustrate the importance of understanding relationships among infrastructures in a system-of-system setting where sustaining public well-being depends on intricate relationships among multiple integrated infrastructure systems. Furthermore, authors stipulate that understanding intricate relationships among infrastructure systems is an essential step that should take place before the development of infrastructure protection, mitigation, and recovery measures since they enable the realization of how risks and threats can permeate infrastructure systems and cause cascading failures.

Dependency. Dependency has two distinctive meanings for CI research; first, it refers to a one-way relationship that can exist between societal needs and needs fulfillment by the outcomes offered by infrastructure systems. For example, modern society heavily *depends* on services provided by a healthcare infrastructure. Second, dependency can also refer to "the relationship between two products [infrastructures, systems, or services] in which one product is required for the generation of the other product" (Luiijf, Nieuwenhuijs, & Klaver, 2008, 1). For example, proper functioning of a hospital depends upon availability of energy in its various forms (i.e., electricity, solar, and/or generators). Hence, dependency entails that proper functioning of infrastructures is contingent on the availability of products, goods, and services from other systems.

When a dependency relationship exists among infrastructures, a new dynamic relationship is created between CI. When the expected outcome is not available, then the next infrastructure's outcomes are interrupted and effectively cutting-off the line of delivery. For example, daily hospital functioning depends on the availability of electricity. On the other hand, sustaining public well-being depends on the availability of both infrastructure systems (e.g., energy and healthcare sector). This relationship creates interdependence among infrastructure systems. Hence, understanding dependency among infrastructures is essential in discovering possible ways an isolated and inane event can cause a cascading failure.

Exposure. Often associated with people's health, exposure is usually related to concepts of dose amount, pollution, toxicity, and surface area (Gheorghe, 2005). It also entails the condition of being unprotected especially from something severe (Merriam-Webster Inc., 2006). In epidemiological studies, exposure effects can be estimated based on concentration-response (Cao & Frey, 2011). Exposure suggests that interconnected system and their outcomes (systems, products, and services) are affected by system openness since infrastructures do not operate in isolation (i.e., they are in constant contact with other infrastructures). The constant contact with other infrastructure systems ensures that there is a continuous level of exposure from the interconnected infrastructures. Exposure, whether planned or unplanned, affects expected infrastructure outcomes.

Understanding the exposure relationship between CI, the environment, and other systems is essential in identifying ways of reducing negative influences on system outputs. Since CIs are interdependent, unplanned exposure can affect the whole CI system via connecting nodes (Kröger & Zio, 2011). Moreover, exposure also ensures that infrastructures produce what is needed for continued operability of infrastructure products, goods, and services. However, it can also influence the outcomes of an infrastructure in a negative manner. For example, cyber systems ensure interconnectivity between banking and government but it can be a source of cyber threat to banking and government (Dunn-Cavelty, 2007) . To understand potential implications (i.e., causes, benefits, etc.) and ways of managing exposure, the examination of the types of interdependencies, relationship nodes, and the infrastructure environment is essential.

Resiliency. A resilient system has the ability to recover after deformation (Merriam-Webster Inc., 2006). In engineering terms, it has been noted that resiliency can be defined in terms of vulnerability and capacity. According to Sauser, Mansouri, and Omer (2011, 3), system resiliency "is considered to be a function of the system's vulnerability, and adaptive capacity." In Sauser et al., (2011, 3) it is suggested that "reducing the system's susceptibility to shocks [extraneous agents] reduces its vulnerability and consequently improves its resilience" and therefore, "increasing the system's adaptive capacity makes it [infrastructure] more resilient." Since infrastructure do not operate in isolation, lack of resiliency in one infrastructure can cripple the whole system. Hence, authors espouse that resiliency is also related to infrastructure interdependency. The ability of the infrastructure to bounce back after a negative event and return to the normal operations is related to the number of interdependent systems.

Infrastructure resiliency is an important concept in CI because of two major factors: first, if CIs are unable to recover and return to normal operations, the debilitating impacts become severe by affecting other interdependent systems. For example, the California Electricity Crisis in which the state suffered large-scale blackouts, collapse of several companies, and eventual political turmoil (Sweeney, 2002) provides an exemplary model. Second, making one infrastructure resilient does not translate into resiliency of the whole infrastructure system-of-systems. Moreover, resiliency is necessary at the metasystem level because the provision of public health, economy, and security are only possible when infrastructure systems operate as a unit despite natural and manmade events (i.e., hazards, risks, threats, etc.). Therefore, authors stipulate that studying resiliency in terms of infrastructure interdependency is essential in making the whole infrastructure resilient.

Risk. There is no one widely accepted definition of risk. The term risk has been widely debated in literature for years (Holton, 2004; Knight, 1921). The INCOSE handbook notes that "every new system or modification of an existing system is based on pursuit of opportunity" and that "Risk is always present in the life cycle of systems..." due to technical factors (INCOSE, 2011, 214). From the decision making perspective, risk is associated with probabilities of unknown outcomes and uncertainty (Gibson et al., 2007). On the other hand, Blanchard (2008, 344) defines risk as "the potential that something will go wrong as a result of one or a series of events" while Garvey (2009, 33) equates risk to "a probability event." Gheorghe, Mock, and Kröger (2000) espouse that risk should be perceived differently in different levels of infrastructure systems. For example, addressing risk at a nuclear power plant level is different from risk at a regional and a societal level. The foregoing definitions point to the fact the risk is that which happens without one planning, anticipating, or intending the event.

Constantly under risk, infrastructures are exposed to different extrinsic and intrinsic hazards, risks, and threats via interconnectedness. Additionally, CIs are always under threat from natural hazard events (e.g., flooding, severe heat, pandemics, etc.) and manmade events (e.g., sabotage accidents, etc.). Interconnectedness among infrastructure almost ensures that risk from one infrastructure will cause a failure in interconnected systems. Hence, authors espouse that risk should be addressed within interdependency theme.

Vulnerability. Infrastructure that is vulnerable is *open to* and *capable of being* physically damaged (Merriam-Webster Inc., 2006). However, since not all infrastructures are physical in nature the qualifier of physical damage is spurious in the CI research. Aven (2011, 515) offers a slightly differing definition where "[v]ulnerability is defined as the manifestation of the inherent states of the system that can be subjected to a natural hazard or be exploited to adversely affect that system." On the other hand, The International Risk Governance Council (IRGC, 2007) stipulates that vulnerability of infrastructures is a viable area of research especially for coupled infrastructures because of mutual interdependences that exists among infrastructure systems. Pointing to electricity usage as an example, the IRGC notes that the smooth functioning of other infrastructures (i.e., rail, communications, etc.) heavily depends on availability of electricity. This could present as a major source of vulnerability of systems that depend on electricity. Based in the preceding notes, authors contend that vulnerability is an inherent characteristic of infrastructure systems and is related to infrastructure openness.

The whole infrastructure becomes vulnerable if one independent infrastructure is open to and capable of being damaged. This is especially the case for CI, since we have established that infrastructure systems do not operate in isolation. Several past examples have illustrated how vulnerability of one infrastructure can affect other facets of health, economy, and security (Gheorghe, 2006; Kröger & Zio, 2011). Authors espouse that defining vulnerability as inherent opens of infrastructures, then understanding structural interconnections and enhancing infrastructures structural integrity to prevent damage is paramount. The concept of interdependency is also essential in infrastructure vulnerability since protection, mitigation, and recovery measures depend on knowing the vulnerabilities of infrastructure systems and their parts within the whole system-of-systems interdependent infrastructures. Especially chosen to illustrate inherent complexity in maintaining and sustaining infrastructure systems, these themes indicate the need to understand intricate infrastructure relationships.

Interdependency in Dependable Infrastructures

It is well established that hazards, risks, and threats to infrastructure systems and their missions can stem from natural phenomena and/or manmade activities. For example, biological attacks such as smallpox, 9/11 attacks, oil spills, and numerous cyber threats are a results of manmade events. On the other hand, the 2004 tsunami in South Asia, Hurricane Katrina, etc. are natural events. Manmade hazards, risks, and threats can be in the form of cyber and physical whose agents often include hostile nations, bandits and criminals, and insiders. Such threats often target soft points-of-weakness in infrastructure systems with debilitating effects on national, state, and/or regional operations (Gheorghe, 2006). Hence, increasing infrastructure reliability, resiliency, and decreasing vulnerability, can significantly aid in maintaining and sustaining public well-being.

Authors espouse that using the concept of interdependency is one of the ways infrastructure operators/owners, policymakers, and researchers can ensure the design, management, and operation of dependable infrastructure systems. The Merriam-Webster Encyclopedic Dictionary (2006) notes that the term *interdependency* is a combination of two distinctive words; *inter* and *dependency*. The prefix *inter* has meaning related to *among*, *between*, *within*, and *shared*. On the other hand, dependency means being *influenced*, *determined by*, *conditioned by*, or *subject to* another for support. From the CI perspective, interdependency means operability of one infrastructure system is contingent on the operability and outcomes of another interconnected infrastructure system. Working on the assumption that the goal of maintaining and sustaining public health, economy, and security depends on the inputs and outputs of multiple well-interconnected infrastructure systems, the relationship among infrastructures is not one-to-one rather it is multidirectional. In the multidirectional relationship concepts of risk, dependency, exposure, resiliency etc. take on a new meaning beyond their traditional formulations (Garvey & Pinto, 2009).

Emerging concerns regarding infrastructure interdependencies have been echoed by leading organizations including the European Commission (EC) and DHS. For example, EC (2004) notes that dependency on common technological advances such as the internet, space-based radio-navigation, and communication systems have made infrastructures more interdependent forming a *system-of-systems*. The same report notes that interdependency among infrastructures have created new risks and vulnerabilities effecting public well-being, security, and economic prosperity. Preliminary research into infrastructure interdependencies suggests that understanding how outputs of infrastructure affect the operability of other infrastructure systems can be useful in developing prevention, mitigation and recovery measures. For example, the U.S. Technical Support Working Group based at Idaho National Laboratory stipulates that knowledge regarding enhancing infrastructure protection is limited because of a lack of understanding of the complex relationships that exist among CIs. In the analysis of infrastructure inoperability and operability, a good starting point includes initiating events and how events travel from one infrastructure to another.

Authors contend that interdependency enables the realization that the protection of infrastructure systems cannot be developed in isolation. For example, Kandiah & Rao (2008) have demonstrated that water infrastructures cannot be protected in isolation primarily because to interdependencies that exist between water systems, supervisory control and data acquisition (SCADA) systems, storage, transport, power, and regulatory agencies. Contributing to interdependency argument is the seminal work of Rinaldi, Peerenboom, and Kelly (2001) where interdependency is categorized into four types (i.e., physical, cyber, geographical, and logical). As research is directed towards interdependency, there is a realization that this discipline is lacking tools for management. There is a call for visual and interactive tools capable of observing cascading events and their consequences (Dudenhoeffer, Permann, & Manic, 2006).

Exhibit 1. Types of Critical Infrastructure Interdependencies

Type of Interdependency	*Definition*

Physical interdependency	Exists between infrastructure systems if the state of infrastructure depends on the outputs (i.e., product, goods, and services) of another infrastructure. In Rinaldi, et al., (2001, 15), it is demonstrated that the physical interdependency in infrastructures "arises from the physical linkage between the inputs and outputs of two agents [where the] commodity produced or modified by one infrastructure (an output) is required by another infrastructure for it to operate (an input)."
Cyber interdependency	Exists among infrastructure systems if the functioning of an infrastructure and its components depends on the output that is transmitted via information and telecommunication systems. Rinaldi (2004, 2) notes that "computerization and automation of modern infrastructures and widespread use of SCADA systems have led to pervasive cyber interdependencies."
Geographical interdependency	Exists among infrastructure systems if infrastructure systems share same environment (DiSera & Brooks, 2009). Sometimes a common environment is needed in the coupling of infrastructure and components; however this poses a threat to all interdependent infrastructure systems in case of failure stemming from explosion.
Logical interdependency	According to Rinaldi (2004, 2) logical interdependency exists in infrastructures "if the state of each [infrastructure] depends upon the state of the other [infrastructure] via some mechanism that is not a physical, cyber, or geographic connection." A good example is regulatory stipulations that linked the California power crisis and financial infrastructure (Sweeney, 2002).

With increasing technological, institutional changes, increasing complexity, and increasing trans-boundary relationships, current society cannot analyse infrastructure systems in isolation (Thissen & Herder, 2003). Despite being operational and managerially independent systems which are geographically distributed, CI must be governed as a whole primarily because of the interdependencies that exist among them. In fact, several researchers are currently calling for a system-of-systems approach to deal with problems in this domain (Haimes, 2008). The expectation is that maintaining, sustaining, and improving the well-being of the public does not belong to one system. Hence, the design, redesign, deployment, operation, and transformation of CI requires holistic view of infrastructure systems.

Critical Healthcare Sector

The aim of this section is to describe interdependencies in the healthcare sector. By healthcare, authors refer to the sector charged with providing direct care (e.g., chiropractic, dentistry, medicine nursing, pharmacy, insurance coverage providers, etc.) and indirect care (e.g., institutional research, regulation, transportation, etc.) and involved in physical and mental impairments, diagnosis, treatment, prevention of disease, illness, and injury in humans (White & Griffith, 2010). In terms of infrastructure systems, the healthcare sector and its constituent systems are charged with alleviating natural hazards, risks, and threats that affect public well-being (e.g., hurricanes, extreme heat, earthquakes) and manmade incidents (e.g., bioterrorism) (Harrington et al., 2005).

Authors contend that the healthcare sector does not operate in isolation. It is interconnected to water, energy, transportation, baking and finance, and agriculture. Hence, a seemingly remote interdependent infrastructure can have a significant effect on healthcare operations. The analysis of CHI, authors espouse, should consider interdependencies because they can offer insights into possible sources of risks, potential dependencies, exposure levels, resiliency, vulnerability etc. at the metasystem level. In this section, authors examine intricate complexities and interdependencies of managing healthcare infrastructure systems from the CI perspective.

Complexity and Interdependency. The availability of any given healthcare system depends upon a variety of system components and other interdependent infrastructure systems that must work as an integrated whole. According to Davidson (2010), healthcare system components include the workforce, environment, and facilities and their interactions. For example, the workforce (i.e., physicians, etc.) interacts with the environment for provisions (e.g., transportation of pharmaceuticals). In addition, tools and equipment are essential during diagnosis, treatment, observation, and prevention of disease and other health related issues. Furthermore, physicians use facilities (e.g., hospitals) during treatment and diagnosis procedures. Hence, meeting patient care requires coordination of workforce, the environment, and facilities.

Additionally, monitoring and improving public health requires understanding intricate relationships among infrastructure systems beyond immediate healthcare systems. For example, Sypek, Clugston, and Phillips (2008) demonstrate that providing healthcare requires understanding global relationships of culture and people. Furthermore, healthcare operations are heavily interrelated to other CI systems. For example, Macaulay (2008) demonstrates that within just eight hours of an incident, one is able to detect the effects of food, safety, and government sectors via a cascade of events. Authors offer the following definition of CHI: *a system-of-systems comprised of multiple physical and/or virtual systems vital to maintaining, sustaining, and improving public* *health whose failure can cause severe impact to public well-being.*

Healthcare can also be considered a *system-of-systems* since it produces emergent system behaviors. Emergent system behavior is a result of the interactions of multiple complex interdependent systems that must work as an integrated unit whole. Emergent behavior are also a result of lack of communications among infrastructure owners who include private competing entities that do not share information (Chertoff, 2009). Additionally, emergent behavior develop because of interactions between numerous systems, unstable environmental conditions, cultural issues, technological advances, policy, and politics (Keating, Padilla, & Adams, 2008). In the CI context, emergent behavior asserts the need to know input and output flows and the potential relationships they create.

While healthcare infrastructure worldviews may vary from nation to nation or region to region, in this paper authors have attempted to explore the commonalities that unite different healthcare worldviews. These commonalities include being able to provide access (Penchansky & Thomas, 1981) and diagnose and treat patients (Jonas, Goldsteen, & Goldsteen, 2007). Additionally, Davidson (2010) stipulates that first care contact, longitudinality, comprehensiveness, and coordination/integration are essential in healthcare services. However, meeting such objectives requires integration of numerous well-interconnected complex systems that must work toward the defined goal of public well-being. To illustrate, authors use an example of the U.S. healthcare system (USHS) to illustrate complexities and interdependencies. The USHS is used as a case study because many industrialized nations use a similar healthcare structure (Jonas et al., 2007).

In describing USHS, Jonas et al., (2007) notes that the healthcare system is comprised of five major components including facilities, workforce, suppliers, knowledge systems, and a finance component. Major stakeholders include principal governmental health authorities, other government agencies, private health care sector, non-healthcare commercial enterprises, and voluntary healthcare agencies. In addition, healthcare oversight is required if different systems must work together towards a common goal. For example, Frankel, Gandhi, and Bates (2003) note that improving health (specifically, patient safety) requires system-wide changes with implications on cultural changes, process changes, and measurement of health services. The management component (i.e., administration, planning, regulations, and evaluation) provides the oversight along the lines of quality of healthcare provision, equity achieved, efficiency, first care contact services, longitudinality, comprehensiveness, and coordination (Davidson, 2010; Jonas et al., 2007).

Working under the assumption that the "focus of health care is to restore or prevent exacerbation of health problems" (Jonas et al., 2007, 6) then, one has to take into account all systems that enable the realization of restoring or preventing the exacerbation of health-related problems. As discussed earlier, technological changes, institutional changes, increasing complexity, growing trans-boundary dependencies, and the demand for higher quality products, goods, and services have changed the structure of infrastructures creating structural complexity (Gheorghe, Masera, & Voeller, 2010; Goertzel, 1992). Additionally, increased concerns regarding extraneous agents (i.e., hostile nations, criminals, bandits, insiders, etc.) who seek to disrupt public well-being by attacking *soft-targets* in healthcare make the design and management of such infrastructure systems paramount. Exhibit 2 exemplifies some of CI themes in healthcare. As previously illustrated, these themes are better understood from the interdependency perspective.

Exhibit 2. CI themes in healthcare

CI Theme	*Healthcare Implications*
Dependency	Daily hospital activities *depend* on the availability of energy (i.e., electricity) and other infrastructure system outputs
Exposure	Healthcare infrastructures *exposed* to natural and cyber threats via ubiquitous computing and telecommunications
Resiliency	Healthcare systems must be able quickly bounce back from effects of natural events (e.g., power outage due to storms) and manmade events
Risk	Healthcare systems operate under multitudes of risks including data breach, fraud and theft, compliance and meeting regulations. They also have to contend with increasing societal changes
Vulnerability	Healthcare systems operate in the *open* and are therefore capable of being damaged by physical harm (e.g., explosions) and cyber attacks

Authors contend that understanding types of infrastructure interdependencies can heavily contribute to designing safer, reliable, and dependable infrastructure systems. For example, *healthcare geographical interdependency* offers infrastructure owners and policymakers an opportunity to design for better health access, diagnosis, treatment, and patient safety by being able to identify optimal healthcare facility locations to minimize potential failure from cascading events. Similarly, identifying physical, cyber, logical, policy, and societal infrastructure interdependencies are essential since healthcare systems do not operate in isolation. Hence, authors contend that it is to the advantage of healthcare infrastructure operators/owners, policymakers, and researchers to know interdependencies among infrastructure systems. The identified themes do not occur in isolation.

Additionally, knowledge regarding intricate relationships among elements is necessary. Knowledge regarding health facilities, workforce, suppliers, knowledge systems, and finance systems and their relationship contributes understanding structure complexity. For example, by understanding the intricate relationships among the 4 million professionals who operate over 6,600 hospitals with over 492,000 ambulatory healthcare, healthcare infrastructure system operators/owner and policymakers are able to identify *soft targets*, identify critical services, and effectively respond to emergencies, disasters, risks, and threats (Harrington et al., 2005).

Clearly, seemingly isolated events can influence the operations of a critical infrastructure. Of greater concern is the fact that seemingly isolated events cascade and cause massive failures. Rather than reacting to crises that can arise due to complexities and interdependencies, Calida and Katina (2012) suggest early participation from infrastructure operators/owners, policymakers, and academia to detect slow and evolving hazards, risks, and threats. Such efforts contribute to the:

- Identification of dependencies and interdependencies among infrastructure systems
- Understanding of exposure rates and their influence on interconnected infrastructures
- Determination of likelihood of infrastructure failure due to internal and external factors
- Understanding of the infrastructure's ability to withstand extraneous agents' influences
- Identification of infrastructure reliability, resilience, and vulnerability and possible means of their improvement; and the
- Identification of potential risks, how such risks can affect public health/safety (consequences), and ways to mitigate risks

Conclusion and Future Research

Authors has espoused that an exanimation of infrastructure interdependencies is an essential step in developing protection, failure detection, threat mitigation, and recovery measures. To make CI more secure, dependable, and resilient, there is a need to understand intricate relationships among the infrastructure systems that work together as an integrated whole for the well-being of society. Only then, can the attempts to reduce the levels of exposure, fragility, susceptibility, and vulnerability yield better results. While placing more emphasis on interdependencies, authors provide a compelling argument that major CI themes are better studied holistically because infrastructure systems do not operate in isolation. Hence, the underlying message of this paper is a call for: 1) increased understanding of structural complexity stemming from numerous interactions among infrastructure systems and 2) development of methods and tools capable of holistically analyzing infrastructure systems. To this end, authors propose the following questions to aid in this dialog:

1. What are the methods, tools, and techniques holistically analyzing infrastructure structural complexity?
2. How can systems engineers holistically quantify infrastructure susceptibility, reliability, resiliency, risk, etc. in system-of-systems setting?
3. How does the intricate interaction among infrastructure systems influence protection, mitigation, and recovery measures?
4. What are the implications of having multiple infrastructure interdependencies on resources allocation?

References

Aven, Terje., "On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience," *Risk Analysis,* Vol. 31, No. 4 (2011), pp. 515-22.

Blanchard, Benjamin S., *System Engineering Management.*, Edited by Andrew P. Sage. 4 ed, Systems Engineering and Management. Hoboken, NJ: John Wiley and Sons, Inc (2008).

Bush, George W., "National Strategy for the Physical Protection of Critical Infrastructures and Key Assests," The White House (2003), Washington, DC.

Calida, Behnido Y., and Polinpapilinho F. Katina., "Regional Industries as Critical Infrastructures: A Tale of Two Modern Cities," *International Journal of Critical Infrastructures,* Vol. 8, No. 1 (2012), pp. 74-90.

Cao, Ye, and H. Christopher Frey., "Assessment of Interindividual and Geographic Variability in Human Exposure to Fine Particulate Matter in Environmental Tobacco Smoke," *Risk Analysis,* Vol. 31, N. 4 (2011), pp. 578-91.

Chertoff, Michael "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency," DHS (2009), Washington, DC.

Congress, U.S., "Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism (USA Patriot Act) Act of 2001," 107th Congress (2001), Washington, DC.

Davidson, Stephen M., *Still Broken: Understanding the Us Health Care System,* Stanford, CA: Stanford Business Books (2010).

DHS. "Critical Infrastructure and Key Resources Support Annex," http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf, (cited December 2008)

DHS. *National Infrastructure Protection Plan*. U.S. Dept. of Homeland Security (2006), Washington, DC.

DiSera, David, and Talbot Brooks., "The Geospatial Dimensions of Critical Infrastructure and Emergency Response," *Pipeline and Gas Journal,* Vol. 236, No. 9 (2009), pp. 1-4.

Dudenhoeffer, Donald D., May R. Permann, and Milos Manic., "CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis," Paper presented at the Proceedings of the 38th conference on Winter simulation (Decemeber 2006), Monterey, CA.

Dunn-Cavelty, Myriam., *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age*, New York, NY: Routledge (2007).

E.C. "Communication from the Commission to the Council and the European Parliament: Critical Infrastrcture Protection in the Fight against Terrorism," Commission of the European Communities (2004), Brussels, Belgium.

Fletcher, David R., "Spatial Information Technologies in Critical Infrastructure Protection: A Research Agenda in CIP," In *National Consortium on Remote Sensing in Transportation Infrastructure*, University of California (2002), Santa Barbara, CA.

Frankel, Allan, Tejal K. Gandhi, and David W. Bates., "Improving Patient Safety across a Large Integrated Health Care Delivery System," *International Journal for Quality in Health Care,* Vol.15, No. S1 (2003), pp. i31-i40.

Garvey, Paul R., *Analytical Methods for Risk Management: A Systems Engineering Perspective*, Boca Raton, FL: Chapman & Hall/CRC (2009).

Garvey, Paul R., and Cesar A. Pinto., "Introduction to Functional Dependency Network Analysis," Paper presented at the The Second International Symposium on Engineering Systems, Massachusetts Institute of Technology (June 2009), Cambridge, MA.

Gheorghe, Adrian V., *Critical Infrastructures at Risk: Securing the European Electric Power System*, Topics in Safety, Risk, Reliability and Quality, Dordrecht, The Netherlands: Springer (2006).

Gheorghe, Adrian V., *Integrated Risk and Vulnerability Management Assisted by Decision Support Systems: Relevance and Impact on Governance*, Vol. 8, Topics in Safety, Risk, Reliability, and Quality, Dordrecht, The Netherlands: Springer (2005).

Gheorghe, Adrian V., Marcelo Masera, and John G. Voeller., "Critical Infrastructures at Risk: A European Perspective," In *Wiley Handbook of Science and Technology for Homeland Security.*, Edited by John G. Voeller, Hoboken, NJ: John Wiley & Sons, Inc. (2010), pp. 1-21.

Gheorghe, Adrian V., Ralf Mock, and Wolfgang Kröger., "Risk Assessment of Regional Systems," *Reliability Engineering & System Safety,* Vol. 70, No. 2 (2000), pp. 141-156

Gibson, John E., William T. Scherer, and William F. Gibson. *How to Do Systems Analysis*, Wiley Series in Systems Engineering and Management, Hoboken, NJ: Wiley-Interscience (2007).

Goertzel, Ben., "Measuring Static Complexity," *International Journal of Mathematics and Mathematical Sciences* Vol. 15, No. 1 (1992), pp. 161-174.

Haimes, Yacov Y., "Models for Risk Management of Systems of Systems," *International Journal of System of Systems Engineering,* Vol. 1, No. 1 (2008), pp. 222-236.

Harrington, Michael B., Carol S. Miller, and Ming-Pin Wang., "Protecting One of the Nation's Critical Infrastructures: Healthcare," *The Edge,* Vol. 9, No. 1 (2005), pp. 12-13.

Holton, Glyn A., "Defining Risk," *Financial Analysts Journal,* Vol. 60, No. 6 (2004), pp. 19-25.

INCOSE., *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities [Incose-Tp-2003-002-03.2.2].*, Edited by Haskins, Cecilia. INCOSE (2011), San Diego, CA.

IRGC. "Policy Brief: Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures," International Risk Governance Council (2007), Geneva, Switzerland.

Jonas, Steven, Raymond L. Goldsteen, and Karen Goldsteen., *An Introduction to the Us Health Care System*, 6 ed. New York, NY: Springer Publishing Company (2007).

Jovel, Jessica, and Rashmi Jain., "Impact of Identified Causal Factors to "System of Systems" Integration Complexity from a Defense Industry Perspective," *Global Journal of Flexible Systems Management, Vol.* 10, No. 4 (2009), pp. 45-54.

Kandiah, Venu, and Prasada Rao., "Identifying and Understanding the Infrastructure Interdependencies in Water Systems," *West Indian Journal of Engineering,* Vol. 30, No. 2 (2008), pp. 36-49.

Keating, Charles B, Jose J. Padilla, and Kevin M. Adams., "System of Systems Engineering Requirements: Challenges and Guidelines," *Engineering Management Journal,* Vol. 20, No. 4 (2008), pp. 24-31.

Knight, Frank H., *Risk, Uncertainty and Profit*, New York, NY: Houghton Mifflin (1921).

Kröger, Wolfgang, and Enrico Zio., *Vulnerable Systems*. London, UK: Springer-Verlag (2011).

Luiijf, Eric H., Albert H. Nieuwenhuijs, and Marieke Klaver., "Critical Infrastructure Dependencies 1-0-1," Paper presented at the 2008 First International Conference on Infrastructure Systems and Services (November 2008), Rotterdam, The Netherlands.

Macaulay, Tyson., *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*, New York, NY: CRC Press (2008).

Merriam-Webster Inc., "Webster's New Explorer Encyclopedic Dictionary," Springfield, MA: Federal Street Press, (2006).

Moteff, John D., "Critical Infrastructures: Background, Policy, and Implementation," Congressional Research Service (2010), Washington, DC.

Patton, Michael Q., *Qualitative Research and Evaluation Methods*, 3 ed. Thousand Oaks, CA: Sage Publications, (2002).

Penchansky, Roy, and J. William Thomas., "The Concept of Access: Definition and Relationship to Consumer Satisfaction," *Medical care, Vol.* XIX, No. 2 (1981), pp. 127-40.

Rinaldi, Steven M., "Modeling and Simulating Critical Infrastructures and Their Interdependencies," Paper presented at the Proceedings of the 37th Hawaii International Conference on System Sciences (January 2004), Big Island, HI.

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly., "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems,* Vol. 21, No. 6 (2001), pp. 11-25.

Sauser, Brian, Mo Mansouri, and Mayada Omer., "Using Systemigrams in Problem Definition: A Case Study in Maritime Resilience for Homeland Security," *Journal of Homeland Security and Emergency Management,* Vol. 8, No. 1 (2011), pp. 1-16.

Sweeney, James L., *The California Electricity Crisis*, Stanford, CA: Hoover Institution Press (2002).

Sypek, Scott, Gregory Clugston, and Christine Phillips., "Critical Health Infrastructure for Refugee Resettlement in Rural Australia: Case Study of Four Rural Towns," *Australian Journal of Rural Health, Vol.* 16, No. 6 (2008), pp. 349-354.

Thissen, Wil A., and Paulien M. Herder., *Critical Infrastructures: State of the Art in Research and Application*, International Series in Operations Research & Management Science. Boston: Kluwer Academic Publishers (2003).

UCTE. "Final Report: System Disturbance on 4 November 2006," European Network of Transmission System Operators for Electricity (2006), Brussels, Belgium.

White, Kenneth. R., and John R. Griffith., *The Well-Managed Healthcare Organization.*, 7 ed. Chicago, IL: Health Administration Press (2010).

About the Authors

Polinpapilinho F. Katina is a doctoral student in the Department of Engineering Management and Systems Engineering at Old Dominion University (ODU). He received a M.Eng. in Systems Engineering and a B.S. in Engineering Technology, both from ODU, in 2011 and 2009, respectively. He currently serves as a Graduate Research Assistant affiliated with the National Centers for System of Systems Engineering (NCSoSE) at ODU. His research interests include infrastructure systems, decision-making under uncertainty, and system-of-systems engineering.

C. Ariel Pinto., Ph.D. is an associate professor in the Department of Engineering Management and Systems Engineering at ODU. Previously, he was a research fellow at the Software Industry Center at Carnegie Mellon University, and at the Center for Risk Management of Engineering Systems at the University of Virginia. He earned his doctorate degree in Systems Engineering from the University of Virginia and master and bachelor degrees in Industrial Engineering from the University of the Philippines. His research interests are in the areas of risk management in engineered systems, including project risk management, risk valuation, risk communication, analysis of extreme-and-rare events, and decision-making under uncertainty.