JITTA
JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

DESIGNING MALLEABLE CYBERINFRASTRUCTURE TO BREACH THE GOLDEN BARRIER

ROBB KLASHNER, New Jersey Institute of Technology
Information Systems Department, New Jersey Institute of Technology, Newark, New Jersey
E-mail:robert.m.klashner@njit.edu

SAMEH SABET, New Jersey Institute of Technology
Information Systems Department, New Jersey Institute of Technology, Newark, New Jersey
E-mail: ssabet@tycotelecom.com

ABSTRACT

Design research perspectives may have a great deal of insights to offer emergency response researchers. We consider man-made and natural disasters as events that often require rapid change to existing institutionalized technical, social, and cultural support structure—a fundamental problem for static systems. Built infrastructure such as electric power and telecommunications or emergency response systems such as fire, police, and National Guard all have static information systems that are tailored to their specific needs. These specialized systems are typical of those developed as a result of applying traditional information systems design theory. They are designed to control domain specific variables and mitigate a specific class of constraints derived from a well-articulated environment with firm application boundaries. Therefore, typical mission-critical Information and Communication Infrastructure (ICTI) technologies empower knowledge workers with the ability to change current environmental events to ensure safety and security. Disasters create situations that are challenging for typical designs because a disaster erodes control and raises unexpected constraints during an emerging set of circumstances. The unpredictable circumstances of disasters demonstrate that current emergency response ICTI systems are ill equipped to rapidly evolve in concert to address the full scale and scope of such complex problems. A phenomenon found in the treatment of trauma victims, the Golden Trauma Time Interval, is generalized in this paper to all emergencies in order to inform designers of the next generation

Murray Turoff and Bartel Van de Walle acted as senior editors for this paper.

Klashner, R. and S. Sabet, "Designing Malleable Cyberinfrastructure to Breach the Golden Barrier," *Journal of Information Technology Theory and Application (JITTA)*, 6:3, 2004, 59-84.

ICTI. This future ICTI or "Cyberinfrastructure" can provide the essential foundation necessary to dynamically adapt conventional ICTI into a configuration suitable for use during disasters. However, Cyberinfrastructure will suffice only if it can be sufficiently evolved as an Integrated Information Infrastructure (I3) that addresses the common sociotechnical factors in these domains. This paper describes fundamental design concepts derived from interdisciplinary theoretical constructs used to inform the creation of a framework to model "complex adaptive systems" (CAS) of which emergency response infrastructural systems and I3 are instances. In previous work, CAS was synthesized with software architecture concepts to arrive at a design approach for the electric power grid's I3. We will present some of the foundational concepts of CAS that are useful for the future design and development of a Cyberinfrastructure. The ICTI may exist today in a raw form to accomplish the task, but further ICTI design research is required to pinpoint critical inhibitors to its evolution. Also, social, organizational, and institutional issues pertaining to this research will be highlighted as emergency response system design factors needing further consideration. For example, this discussion infers a resolution to the basic tradeoff between personal privacy rights and public safety.

INTRODUCTION

The inability to deliver the appropriate data and information to specific knowledge workers during or immediately following a disaster often results in the needless loss of human life. We assert this inability to respond is tightly coupled with the inappropriate methods and techniques used to design the Information and Communication Technologies Infrastructure (ICTI) that the key agents utilize. In order to develop better methodologies, design researchers could benefit from a different theoretical framework when attempting to solve the problems presented in this paper. This research juxtaposes some very general constructs such as communication and control within the context of large disasters in order to show that there is a diminishing emergency response capability to respond due to inadequate and/or inappropriate ICTI designed using conventional information system theories. Issues associated with organizational forms, institutional forces, privacy, and freedom of the citizenry further convolute this examination of emergency response capabilities. These general constructs and issues typically interact, resulting in certain common systemic behavior that we describe using trauma emergencies, electric power blackouts, and examination of a possible real-world scenario (given today's independent technological developments). We address this lack of appropriate design approaches by presenting a broad theoretical framework that has been synthesized from existing research and observed phenomena. The framework can be used for complex sociotechnical problems.

Disasters are man-made or natural events that disrupt normal operations of the existing technical, social, and cultural support structure such as built infrastructure and emergency response. These events often require that the existing information infrastructure be rapidly interfaced so that agencies not accustomed to working together can now share information. Examples of these complex tasks include the integration of information systems (IS) supporting the supply chain for the first Gulf War or the coordination and interaction between NYC utilities after 9-11. Built infrastructure such as the intermodal transportation system, electric power grid, natural gas system, Internet, or telecommunications networks all have robust underlying information infrastructure that is

separate from the other infrastructural systems. Emergency response systems such as fire, police, and National Guard usually have well established IS that are tailored to their specific needs, but are also difficult to interface together if the disaster requires such a reconfiguration. Disasters present new design challenges because conventional requirements are often not applicable due to changing domain specific constraints. The unforeseen behavior of a disaster tends to erode control and raise unexpected constraints during an emerging set of circumstances that are only partially known in advance.

Current emergency response systems that were designed using a traditional IS design notion of firm system boundaries are ill equipped to rapidly evolve in concert with other IS. These specialized ICTI systems are typical of those developed as a result of applying traditional information systems design theory as described by (Walls, Widmeyer and El Sawy 1992). Walls et al. "used the name 'IS design theories' to refer to an integrated prescription consisting of a particular class of *user requirements*, a type of *system* solution (with distinctive *features)*, and a set of effective *development practices.* Thus, there are design theories for familiar system

CONTRIBUTIONS

This interdisciplinary design research is guided by a Complex Adaptive Systems (CAS) framework. We use the framework to synthesize disparate concepts in a new approach to inform Emergency Response infrastructural systems researchers about design approaches intended to reduce complexity associated with many real-world development efforts. Design research can be an effective perspective on real-world systems associated with emergencies. These design research approaches include the analysis of Information and Communication Technology Infrastructure (ICTI) artifacts in order to explain, extend, and/or evolve their behavior. The goal of such analysis is to guide current ICTI towards a more robust sociotechnical instantiation such as an Integrated Information Infrastructure (I3) and/or a technologically advanced and interconnected version of ICTI (i.e., a futuristic Cyberinfrastructure). Design research is typically interdisciplinary due to the artifact being researched to investigate complex problems. Generally, design research begins with problem articulation. This paper's primary thrust, structure, and contribution are the articulation of a complex emergency response related problem in terms of the CAS theoretical framework not previously associated with phenomena from various mission-critical domains.

The paper informs the reader how to conceptualize an extremely large design research project; such as I3 based on sociotechnical constraints arising from powerful stakeholders and resulting in ambiguous high-level requirements. We demonstrate how to draw together various streams of research within the CAS framework in order to structure the problem arising from a particular emergency response phenomenon— the Golden Trauma Time Interval (GTTI). The GTTI phenomenon is the concept that during an emergency, a small window of opportunity exists in which a trauma victim can be saved if appropriate medical attention is provided. The obstruction preventing the utilization of needed resources to avert tragedy is referred to as the "Golden Barrier" among emergency personnel. Although coined specifically for medical emergencies, this concept may also be generalized to all emergency situations. The paper articulates the general case of the phenomenon as a problem that can be somewhat addressed through the next generation of I3 as a Cyberinfrastructure design.

This research contributes to community knowledge by walking through the steps necessary to articulate the problem, namely theory justification, suggestions for method development, and a future scenario as a mechanism to crystallize aspects of the theory and methodological analysis. An architectural approach was leveraged in order to show the full cohesive process involved in problem development and articulation. Without this deep understanding of design research, many less experienced researchers would not discover the correct or valid problem to solve.

types, like DSS [Decision Support Systems], TPS [Transaction Processing Systems], EIS [Executive Information Systems], etc." (Markus, Majchrzak and Les Gasser 2002). These types of information systems are the result of system analysis practices that generate narrowly bounded requirements and solutions. Per the resulting requirements, they were designed to control domain specific variables and mitigate a specific class of constraints derived from a well-articulated environment. An empirical study (Curtis, Krasner and Iscoe 1988) of 17 large software design projects revealed:

- *Deep* domain-specific knowledge applicable to early analysis and design phases was woefully lacking,
- Fluctuating or conflicting system requirements always cause problems, and
- Communication and coordination breakdowns often constrain project success.

In addition, their data and behavioral study indicated the actual implementation (e.g., "writing code") was not a problem, but "understanding the problem is the problem" (Curtis, Krasner and Iscoe 1988). These insights agree with software engineering perspectives and problem articulation research in decision sciences (Kleindorfer, Kunreuther and Shoemaker 1993). Therefore, more theoretically grounded research is needed to address the myriad of technical, social, psychological, and cultural issues surrounding the development and deployment of ICTI systems. Also, these ICTI systems must be designed malleable due to unexpected domain constraints. But, software is notoriously "brittle" and prone to failure when configured into large systems.

We generally believe if critical design issues can be effectively addressed that emerging ICTI will facilitate better utilization of the knowledge gained from the analysis of phenomena such as those we present later in this paper. We present the following vision as a focal point for the reader to keep in mind.

> **Vision statement:** Emergency personnel are knowledge workers who will continue to rely on real-time information, their intuitive understanding of the domain, and advanced technology in order to reduce risk for the public and mitigate loss of life. In the future, these knowledge workers will ***know*** you (or your spouse, your children, your parents, your friends) have entered a life-threatening situation the moment the threat arises—no matter where you (they) are in the world.

The technology appears to be almost prepared so that technologists can offer the world this option as the following quote supporting the development of "Cyberinfrastructure" indicates:

> The combination of wireless LANs, the third generation of cellular phones, satellites, and the increasing use of unlicensed wireless bands will cover the world with connectivity enabling both scientific research and emergency preparedness to utilize a wide variety of "sensornets". Building on advances in micro-electronic mechanical systems (MEMS) and nanotechnology, smart sensors can be deployed widely, will be capable of multiple types of detection, and can survive for long periods of time. The integration of real-time multisensor data with data mining across large distributed data archives opens further avenues for adaptive monitoring/observation, situational awareness, and emergency response. (Atkins et al. 2003)

However, it remains to be seen if the social, cultural, organizational, and institutional barriers can be overcome to leverage the technology when it is actually ready. This paper attempts to articulate some of the inhibitors as we search for an accurate problem definition(s).

There is a need to take advantage of the opportunity provided by these emerging technologies. New design approaches should help capture value from these emerging technologies if the appropriate research can be done. This revelation is being recognized throughout scientific and engineering communities, which is evidenced by the U.S. National Science Foundation Design Science solicitation for grant proposals (NSF 2004). Having such an infrastructure that allows for immediate response to emergencies and therefore results in fewer human lives loss is

indeed a valuable safety net. However, what would you trade for that safety net? Would you trade your privacy, money, and/or freedom? Because these systems could easily be used for evil as well as good, what ethical mandate should accompany the scientific investigation of these technologies? These are complex and highly controversial questions, which this paper will only partially augment. The critical design research questions we examine in this paper at some length are more manageable. How can one design complex systems:

1. to mitigate the impacts of the phenomena associated with emergency events; i.e., the Golden Barrier?
2. to conform to a myriad of organizational, institutional, social, and technical domain-specific constraints?
3. with an enhanced, if not full, awareness of domain forces arising from crosscutting effects?
4. to mollify the complexities associated with wicked infrastructural problems?

We will point out in the next section that the trauma and electric power data indicates there is a temporal correlation between emergency response and the eventual consequences incurred. In addition, we are asserting that the solution to the Cyberinfrastructure design problem must factor in numerous dynamic constraints to be correct. Then we elaborate the problem in more depth to present the multifaceted design considerations that force an examination of a broader theory than currently available to IS designers. The theoretical considerations are enumerated in the Theory section through the presentation of a Complex Adaptive Systems (CAS) theoretical framework. The CAS framework is useful to reduce systemic complexity by facilitating the integration of various cross-disciplinary research into a cohesive whole. The related research that has been integrated for this work is then presented to further demonstrate the CAS utility and cross-functionality. Characteristics of a plausible method to match the theoretical framework are presented briefly to substantiate the theory's possible research applicability. To connect our Vision Statement, aforementioned phenomena, theory, and real problems, emergency medical services are contextualized with some historical background prior to presenting a brief design example. This futuristic emergency response scenario is used to piece together the puzzle formed by communication, control, GTTI, infrastructure, architecture, and generic emergency events through a Cyberinfrastructure analysis premised on the previously suggested method. The case also draws out salient issues confounded with morals and ethics that must be addressed when designing systems through the weighing of human life and personal freedoms or privacy. The paper will then be summarized and the final section will lay out recommendations for future research and conclusions.

ELABORATING ON THE PROBLEM

The domain drives the choice of theory in our research because of the strong influence domain constraints have on the evolution of ICTI with respect to mission-critical infrastructure. In this case, built or urban infrastructure is the primary domain constraint since it has to be evolved due to economic constraints and cannot be simply replaced. Markus further points out that the expanded meaning of infrastructure is "the structure within" (Markus 1984). Therefore, when her definition is applied to organizational systems, the term refers to "both tangible equipment, staff and applications and the intangible organization, methods and policies by which the organization maintains its ability to provide system services" (page 148) implying an inseparable relationship. The Markus definition is very consistent with field observations in energy utilities (Klashner 2002) and Reddy's observation of trauma centers (Reddy, Dourish and Pratt 2001). In order to further demonstrate these domain drivers and symbiotic organizational relationships, certain domain phenomena will be presented next that shows a level of organized complexity, which will be revisited later, in the theory section.

DOMAIN SPECIFIC PHENOMENA

The loss of system control often coincides with the erosion of system structure creating a set of phenomena associated with an emergency event. Several large mission-critical infrastructural systems and emergency

response industries share certain characteristics that are tied to the lack of accurate information delivered in a timely fashion. To further ground this discussion, we present concrete real-world cases before continuing with the theoretical research aspects of this paper.

Severe Trauma

> "*'The first 60 minutes following an accident largely dictate whether a critically injured person will live or die.'* Dr. R Adams Cowley (Cowley 1976) the pioneering Maryland trauma surgeon, is often credited with coining the term, 'The Golden Hour of Trauma'. It is important to realize that he did not mean that a discreet 60 minute time interval elapses from the time of injury until the onset of irreversible shock or death." (CWDMG 2003)

We assert the properties of the GTTI are common to all sizable emergency response situations.

A small window of opportunity exists in which a trauma victim can be saved if appropriate medical attention is provided. This concept of a Golden Trauma Time Interval is further elaborated in Figure 1 (CWDMG 2003). This temporal window—the GTTI—is of the gravest importance. However, much of the GTTI is wasted in locating the victim and initial analysis. Therefore, this barrier is "golden" because it greatly influences the severity of the event. Note how the lack of information and attention drastically changes the severe trauma scenario and the outcome of the GTTI event in Figure 1. Notification of the occurrence of an incident and attention to the appropriate resource allocation are literally the difference between life and death. Of all trauma victims, approximately 30-50% perish due to lack of timely care or appropriate technology during a given GTTI when it is required. So, to what degree does societal dependency on the control infrastructure, and the emergency response system structure contribute to higher than necessary fatalities? It is difficult to say because of scarcity of data due to its sensitive nature (i.e., medical,

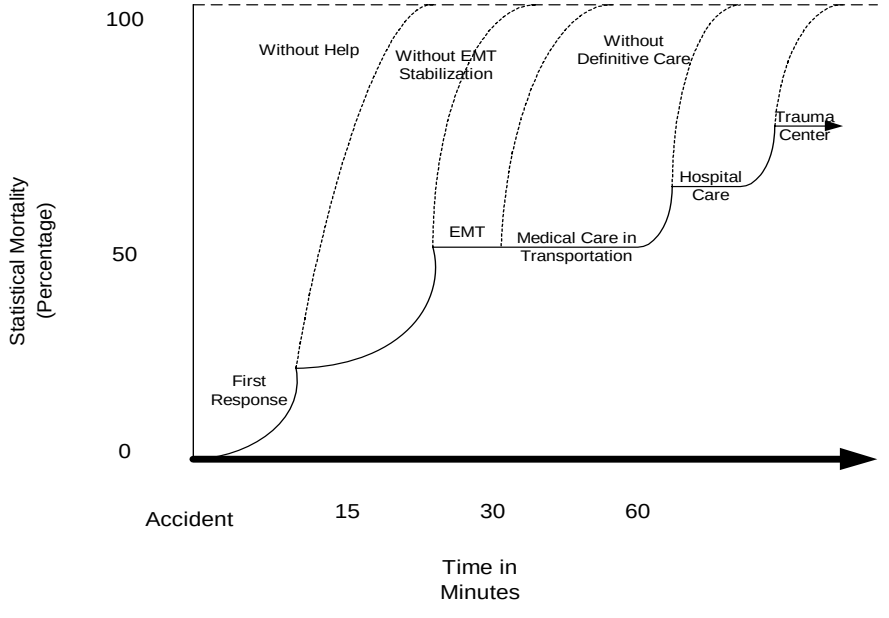

Figure 1. The Visual Representation of the Golden Trauma Time Interval (GTTI) Phenomenon

national security, etc.). However, what is even more compelling is that the GTTI phenomenon can be generalized to most man-made and natural disasters. Generally, the GTTI phenomenon can be attributed to the same control-structure dynamic observed in the electric power grid (described below). It is therefore important to examine this relationship further.

Electric Power Domain

The electric power industry evolved over the last century and its integrated information infrastructure (I^3) (Klashner 2002) is the culmination of four decades of evolution. The real time, mission-critical, and ubiquitous characteristics of this industry magnify domain complexity arising from the sheer size of the system. For example, electric power grid operators control the flow of electricity over thousands of square miles and to millions of customers. Both antiquated and cutting edge technologies coexist and interact to provide the necessary services through I^3. The development and operation of I^3 for the electric power industry establishes a distinct *domain* of interest. Interactions between domain entities and I^3 result in domain-specific system *behavior*. In other words, the electric power grid behaves in a particular manner because of the I^3 it is utilizing, which includes the social and intangible ramifications inferred in the Markus definition of infrastructure. The electric power domain is very *complex* necessitating the use of complex research tools to gain intellectual leverage over the problem's breadth and depth. The I^3 designer often uses an abstraction such as *architecture* to gain intellectual control over complex domain data. There exists a natural relationship between the concepts of infrastructure and architecture, which often have a great deal of design overlap, socially constrained juncture, or even common physical components. A great number of various architectural abstractions exist, but *software architectures* are particularly relevant for developing I^3 (Klashner 2002). The high architectural level of abstraction coincides with the view of the electric power grid system from the grid dispatch center—their command and control center. As one informant at grid dispatch phrased it, they have the "view from 30,000 feet" (Klashner 2002).

The electric power grid is typically very stable in the US; i.e., a normal state of economic dispatch. However, the electric power grid does experience state changes. A state change event in electric power would be a power line fault or generator malfunctioning, which would effectively change the grid frequency. When system faults occur, the grid state changes to a brownout (i.e. reduced voltage or supply pattern for a geographical area) or blackout (i.e. complete loss of voltage for a given area). The large blackout in the Western United States in 1995 was physically the result of harmonics building up in the grid system over a period of several weeks. A series of unforeseen circumstances and events in the mountain states rapidly escalated the situation until a fault caused by a tree touching a high-voltage wire started a cascading failure. The rolling failure lasting a few minutes created a brownout condition throughout the West Coast and complete blackout in Arizona. However, the blackout had social and political causes as well as technical causes. Grid dispatch experts often understand the nature of an emergency through intuition. But deregulation has confused their traditional domain understanding and diluted the effectiveness of their organizational memory by introducing additional high-level abstractions and ambiguity primarily associated with the politics of electric power, thereby making the problem even more intractable.

Prior to the 2003 blackout in the Northeast United States, the electric power grid began behaving irregularly indicating electric power grid operators were losing control of the system (Ellis 2003). The final report by the joint U.S. and Canadian task force investigating the blackout determined the "Loss of Eastlake 5, however, did not initiate the blackout. Rather, subsequent computer failures leading to the loss of situational awareness in FE's [FirstEnergy] control room and the loss of key FE transmission lines due to contacts with trees were the most important causes" (Ellis 2003).

This lack of "situational awareness", in both the West Coast and Northeast blackouts, is effectively the capability of command and control personnel to manage knowledge based on a plethora of continuously replenished information and data, which is delivered to

their control center via the ICTI. As a direct result of these failures, large geographical regions disconnected and/or had voltage collapse coinciding with the rapid erosion of the grid structure. The dependence on ICTI (i.e., no manual mechanisms) and the absence of appropriate sensors in conjunction with a shared knowledge base contributed to these blackouts. These factors combine to work against the command and control personnel. In addition to proactive situational awareness to prevent emergencies, similar ICTI mechanisms should be applied reactively to any emergency response situation.

MULTIFACETED DESIGN CONSIDERATIONS

There is a great deal of overlap between the concepts of a Cyberinfrastructure (Atkins *et al*. 2003) and the earlier I^3 conceptualization, but Cyberinfrastructure as presented by Atkins et al neglects some of the concerns voiced by Klashner such as the inclusion of the Markus intangibles. Therefore, we have chosen to expand the definition of Cyberinfrastructure here to include aspects of I^3 to demonstrate the utility of having more degrees of freedom with respect to sociocultural aspects of information infrastructure design. Thus, our Cyberinfrastructure design recommendations will be augmented with some of the foundational concepts used in I^3 design. The general research we are proposing to address the aforementioned questions should focus design on both Cyberinfrastructure and I^3 conceptual issues because a critical intersection between the concepts revolves around the nontechnical aspects of requirements for these systems. In both instances, a variety of domain constraints translate into somewhat intractable, but important “high-level requirements” that directly effect design considerations. To make this point more salient, we introduce the research by King (King *et al*. 1994; Forster and King 1995; Pickering and King 1995; King, Grinter and Pickering 1997) into "high-level requirements analysis.”

King et al focus on issues of organizational and institutional usability that have created difficulties for software designers and software developers. The problem inherent in the design of complicated sociotechnical information infrastructures is that they must function effectively in complex organizational and institutional settings. Their research of high-level requirements is set in highly institutionalized production sectors that are affected in dramatic ways by the regulatory and influential efforts of social institutions, both formal (e.g., Federal policy-makers), and informal (e.g., professional associations). Infrastructural systems investigated by King et al include: control of electric power generation, transmission, and distribution resources in deregulated markets; communication IS for intermodal logistics and transport; signaling and addressing systems in global common-carrier wireless networks; case management systems in criminal courts; patient record systems in health care; systems for curricular education in "distance learning" in higher education. Baldwin states the problem of business strategies and government policies designs for innovation and technology in the following manner:

> Compounding this problem is the fact that many social scientists, business leaders and policy makers misunderstand the nature of designs and design processes in fundamental ways. For example, many believe that the process of creating a large, complex design is rational, orderly, and deterministic. Designers and others close to the actual processes know that such processes are creative, messy, and have highly uncertain outcomes. It is a fact that uncertain and open-ended processes require radically different institutions, organizations and incentives from deterministic processes: the factory approach will not work for designs. (Baldwin 2003)

The compounding of domain constraints and high-level requirements, as noted above, interact in a complex manner resulting in a “wicked problem”(Rittel and Webber 1973). Wicked problems do not have solutions, only best possible resolutions. This complexity is especially apparent in the area of command and control center design (Klashner 2002) where emergencies must be resolved based on large quantities of data interpreted by experts.

These concepts can be summarized as follows: External domain and internal

structural constraints interact through organizational and institutional associations resulting in high-level requirements that often lead to system development failure. The situation is further confounded in mission-critical infrastructural domains required for emergency response wherein the design of information systems infrastructure necessary to operate is obfuscated by social factors not easily explicated by traditional IS or software engineering design approaches that focus on an application domain. The interplay across these concepts throughout the infrastructure also create crosscutting effects that surface as domain considerations and must be resolved during architectural and/or design decision-making depending on the scope or level of system abstraction. Drawing arbitrary application domain boundaries or creating abstract models in order to exclude these crosscutting effects results in the creation of more complex problems that must be addressed later in the evolution of the system. This dynamic was observed in the deregulation of the US electric power industry (Klashner 2002; Klashner 2004). This is especially true in California where over $20 billion was lost due to inappropriate deregulatory efforts founded on a particularly flawed IS design exploited by Enron (Swartz 2003). Therefore, this sort of "wicked" problem (Rittel and Webber 1973) can be attacked in a broad Cyberinfrastructure/I^3 design context. In answering the research questions presented earlier, this paper further articulates all of the prior aspects as a "wicked" design problem in order to enumerate some of the more tangible constraints and tradeoffs. We elaborate on an initial Cyberinfrastructure design theoretical framework in the next section that we envision as necessary to provide emergency response capabilities to society.

THEORETICAL FRAMEWORK

The general problem in the prior section noted how organizational, institutional, social, and technical crosscutting effects complicate already difficult mission-critical infrastructure design problems. These infrastructures are necessary for emergency preparedness and response. These difficulties necessitate the use of theory to provide guidance throughout complex design tasks inherent within the wicked problem of designing ICTI to address such phenomena as the Golden Barrier. Typical information systems are already a critical component of all mission-critical infrastructures. The integration of IS infrastructure to form the ubiquitous nature of Cyberinfrastructure (Atkins *et al*. 2003) create design difficulties for IS researchers. In the past, application definitions and boundaries were imposed in order to gain intellectual mastery over the complexity in the problem domain (Walls, Widmeyer and El Sawy 1992). That is, 'IS design theories' as defined by Walls et al adhere to a particular class of user requirements, and a type of system solution (e.g., DSS, TPS, EIS) in order to assure success, defining away the problem complexity through specific conceptualizations. However, even if these conceptualizations helped designers, the true high-level requirements are obscure (as noted above), and since the problems are "wicked" there is no absolute solution. So, traditional IS design theories do not provide representational sufficiency or intellectual mastery over the problems and are not generally applicable to Cyberinfrastructure designs.

There exists a strong correlation between the *complexity* of built infrastructure design, the domain, and the apparent wickedness of the problem. In other words, the role of the environment should be considered when assessing the impacts of complexity on the design. Definitions of complexity (e.g., Santa Fe Institute versions) often include convoluted mathematical descriptions of little practical benefit to IS designers. Other definitions utilize controversial or abstruse notions such as postmodernism (Cilliers 1998). Complexity experts feel that a precise definition of complexity is unlikely in the near future (Axelrod and Cohen 2000). Some descriptions of domain complexity are primarily concerned with sociocultural domains; e.g., Jackson's "informal" domain (Jackson 1995). Also, apparent complex entity behavior over time does not necessarily have a direct causal association with internal entity complexity (Simon 1995). To make this point about environment, Simon describes the semi-random path an ant would follow on the beach resulting from domain interdependencies (pages 63-66). We believe his illustration is somewhat analogous to sociocultural domain constraints guiding the design of infrastructure

through policy-making. The resulting convoluted design is not an engineering derivative, but a product of the sociotechnical political process.

The scale and scope of these design difficulties necessitates the utilization of theory that has an intellectual foundation capable of managing all aspects of sociocultural complexity, wicked problem definition, and behavioral diversity. Leveson argues that science and engineering were making good progress toward a science of design up until the late 1970s and early 1980s, but have “started all going down one narrow path…without much regard for complexity, intellectual manageability, or many of the principles derived in the 70’s” (Leveson 2003). She further asserts that a science of design “must” include “understanding the many aspects of complexity; go beyond simple hierarchical decomposition and create design principles and concepts based on ***systems theory*** [emphasis added], including the principle of emergence; and explore such topics as the relationship between human cognitive limits (intellectual manageability)…” To address these same difficulties found in the electric power industry, Klashner utilized a theoretical framework for sociocultural systems (Buckley 1967; Buckley 1998), which was strongly influenced by *general systems theory*. The framework was developed to model “complex adaptive systems” (CAS) and had been derived from several disciplines. Klashner synthesized CAS and software architecture concepts to arrive at a design approach for the electric power grid’s integrated information infrastructure (Klashner 2002). We will present some of the foundational concepts of CAS below for later use in the presentation of Cyberinfrastructure design method recommendations.

The “modern systems theorists” from the 1950s and 1960s had tightly coupled the concepts of organization, information, control, and communication (all of which will be enumerated in the following case). The environment can be viewed as a "set” or “ensemble" of elements, states, or events that are to some degree distinguishable based on spatial relations, temporal relations, or properties (Buckley 1967). These distinguishable differences are generally regarded as "variety". Buckley extended those peculiar organizational concepts to assert that CAS elements were almost entirely linked by the intercommunication of information rather than through some other mechanism, such as energy or inherent structure, as with many other popular sociological approaches of his time. The term "organized complexity" (Buckley 1967) (pp 38); which he extracted from (Rapoport and Horvath 1959), to define a "collection of entities interconnected by a complex net of relations". Within the framework, every entity has some degree of organization—albeit relative—that lie between two organizational extremes represented by the ideal constructs presented next.

The first construct is called “organized simplicity”. Organized simplicity "is a complex of relatively unchanging components linked by a strict sequential order or linear additivity, without closed loops in the causal chain." Buckley’s second extreme organizational construct is “chaotic complexity”. Chaotic complexity refers to "a vast number of components that do not have to be specifically identified and whose interactions can be described in terms of continuously distributed quantities or gradients, as in statistical mechanics." In other words, Buckley constructs a continuum wherein all conceptual definitions of organization may fall.

The continuum formed between organized simplicity and organized complexity as endpoints was synthesized by Buckley with the help of Norbert Wiener’s (Wiener 1956) “notion” of “contingency” (pp 82). This combination of an organizational continuum and contingency introduces dynamism by integrating complex adaptive organization into preexisting theory. In other words, if all things are necessary and nothing is contingent, no significant concept of organization can be arrived at, but with contingency comes degrees of organization lying between organized simplicity and chaotic complexity. Based on (Ashby 1962), Buckley also asserted relatively stable spatial, causal, and/or temporal relations between elements or events are considered to be "constraints". Chaotic complexity is complete lack of constraint and organized simplicity is the presence of maximum constraint. Typically, stable causal relationships exhibit a high degree of constraint.

The third key concept, in addition to "contingency" and "constraint" used by Buckley to explicate complex organization, is "degrees of freedom in the interrelation of parts" (pp. 83). When no freedom of choice exists, the system is in a state of maximal organization. Inversely, when complete or absolute freedom of choice exists a state of systemic chaos exists. So, constraint and degrees of freedom are dynamic constructs that describe a complex adaptive systems' relation to a changing set of contingencies. This dynamic results in the organizational state of the system that informs the designers of information systems during the integration activities, which are representative of CAS evolution. Designers seek to maximize their control of this process by maximizing their understanding of the current set of available contingencies, constraints, and degrees of freedom at their disposal in order to reduce risk. IS designers are thus seeking as much relevant information as possible, which is important for another aspect of CAS.

Buckley connects the aforementioned organizational concepts to a type of information theory that provides a "generalized logical framework for the discussion of symbolic intercommunication" (pp. 84); i.e., it is not of the signal coding and transmission type. Generally, an information theory starts with a set of continuous signals, symbols, or messages generated by a source in various patterns. When maximal organization exists, no variety is present, which is the same as negative entropy per Buckley's analysis of information theory. If environmental "variety" exists, it must be converted into information in order to have meaning for the receiving entity (e.g., the IS designer). The conversion process includes recognizing and selecting a subset of the variety, then "mapping" the environmental variety and constraints into its own organized structure and/or information. For example, living creatures acquire, organize, and incorporate information that facilitates their survival in particular environments through genetic alteration during evolution. Therefore, part of the receiving entity and the environment become isomorphic with respect to the subset of variety that is freely chosen during evolution. This process is basically communication of the original variety and its associated constraints in a manner that remains somewhat invariant between transmitting and receiving elements (Buckley 1998).

THEORETICAL FRAMEWORK SUMMARY AND APPLICABILITY TO EMERGENCIES

CAS has been briefly described using a behavioral sociocultural framework developed by Buckley in order to facilitate its applicability to emergency situations. Since Buckley's work was a synthesis of a large body of interdisciplinary research that mapped into the General Systems umbrella, only the essence of the CAS framework has been presented. The essence of this design framework applies to complex systems wherein a set or ensemble of elements, states, or events are distinguished based on variety associated with spatial and temporal relations through concepts of information, control, and communication within an organizational continuum bounded by organized simplicity and chaotic complexity. Ensemble or set members also have properties of varying types that contribute to their ability to be contingent or to constrain other systemic elements, states, or events within given interrelated degrees of freedom, thereby factoring into organizational state. The CAS framework can guide the utilization of other broadly or narrowly defined theories and methods because it is an "integrationist" framework (Burrell and Morgan 1979) developed to research emergent phenomenon. For example, to draw out diverging aspects of co-located mission-critical infrastructure one may choose to utilize discourse as a methodological tool (Ulrich 2001) to tease out integration issues and further specify meanings associated with terms such as information since Ulrich relies on rigorous semiotic approaches.

Emergent circumstances are reflected in the GTTI phenomenon described earlier wherein control-structure relationships are critical. Large systems such as infrastructure or networks of emergency response resources have extensive stand-alone IS that can be separately evolved under normal situations using conventional IS design theory (Walls, Widmeyer and El Sawy 1992). Although we agree with a great deal of what Gasson asserted (e.g., much of design science is currently misplacing the emphasis on arbitrary

objectives) (Gasson 2003), we disagree that "sociocultural work and technology-interaction are incommensurable" because CAS is fundamentally a sociocultural theoretical perspective we have found to resonate with many technical design perspectives such as the software architecture process metaphors (Klashner 2002). Thus, the CAS theoretical perspective permits reuse of specialized theories such as DSS, EIS, etc. within the conceptual framework for normal design and evolution. Institutional or social stimuli (e.g., deregulation of the electric power industry or a large-scale terrorist act) creates the need to rapidly integrate these systems into a cohesive whole to adapt the general system for the emergency situation(s) at hand. The typical IS theory is not equipped for that sort of dynamic integration because it is not the status quo. Using CAS as the theoretical design framework, one would reinterpret the status quo as existing systemic constraints arising from institutionalized entities and process maintaining maximal organization by exerting legitimate power to control the degree of freedom of choice with respect to the set of possible contingency states.

We propose designing emergency response systems within the CAS theoretical framework in a manner that they will not be abandoned during an emergency, but instead evolve dynamically based on the emergent phenomenon represented by the variety received via the dispersed infrastructural or emergency network nodes. We concur with Turoff that for IS to be beneficial and utilized during an emergency it must be a version of the systems used on a daily basis (Turoff, Chumer, Van de Walle, and Yao 2004), but must also be able to dynamically evolve into an integrated form with other IS in order to effectively manage event variety. The next section describes some basic building blocks that were derived by Klashner from the CAS framework (Klashner 2002) we will utilize to present possible methods.

RELATED RESEARCH

The related work presented in this section adds concepts, background, and information from several disciplines for use within the CAS framework. Since the problem is "wicked" (Rittel and Webber 1973) and the domain complex, triangulation of related research is intended to facilitate an understanding of the general systems theoretical underpinning from which CAS was derived. This related work would also be needed to fully understand the scenario presented later. In addition, several of the more technical research concepts were synthesized into CAS (Klashner 2002) in order to map the CAS principles into a software tool for use by stakeholders such as IS designers, software architects, and nontechnical agents in the electric power industry.

Mission-critical built infrastructure such as electric power, telecommunications, and air traffic control rely heavily upon software and information systems to operate (Arango 1989; Wets 1991; Denning 1992; Oreizy, Medvidovic and Taylor 1998; Boehm and Sullivan 2000; Salasin 2001; Klashner 2002; Markus, Majchrzak and Gasser 2002). The Internet provides a great deal of capability such as exemplified when it facilitated the deregulation of the electric power industry (FERC 1996), but the Internet is not the complete solution for all problems (Oreizy, Medvidovic and Tayler 1998; Boehm and Sullivan 2000). Integration of technology is important, such as for Air Traffic Control (Wets 1991). Satellites orbiting the earth form an important infrastructure for security and Global Positioning Systems. However, the growing dependence on software and information systems raises concerns about security vulnerabilities (Boehm and Sullivan 2000). The result is countermeasures such as the use of cryptography by the US National Security Agency (Denning 1992). The military utilizes a wide variety of software infrastructure for their "Knowledge-centric Operations" (Salasin 2001). Built infrastructure can be supported with the appropriate reusable software infrastructure design (Arango 1989), but enhancing and propagating these relationships will be the focus of much research in the future (Atkins *et al*. 2003). To evolve the infrastructure through software component reuse, "a reusable infrastructure" also needs to be designed (Oreizy, Medvidovic and Taylor 1998).

The software and information systems comprising the supporting computational infrastructure can be architecturally conceptualized as an Integrated Information

Infrastructure (I^3) (Klashner 2002) or Cyberinfrastructure (Atkins *et al*. 2003). "The newer term *cyberinfrastructure* refers to infrastructure based upon distributed computer, information and communication technology" (Atkins *et al*. 2003). The Cyberinfrastructure can be conceptually abstracted as software architectures (Tracz 1988; Perry and Wolf 1992) or information system architectures (Zachman 1987). Depending on the discipline and level of engagement, architectural representations can capture business scope/objectives, business model, elements, forms, constraints, user functional and nonfunctional requirements, and abstract design rationale. The interface with the user is a significant architectural issue as well (Taylor and Coutaz 1994; Taylor, Medvidovic, Anderson, Whitehead and Robbins 1996).

A common means of leveraging the architectural metaphor is through software architectural styles that focus on component-connector abstractions rather than lines of program code (Tracz 1988; Perry and Wolf 1992). Nontechnical stakeholders can more easily interpret stylistic views that are generated based on the captured data. The Representational State Transfer (REST) architectural style was used to design the Internet that "has succeeded in large part because its software architecture has been designed to meet the needs…" (Fielding and Taylor 2002). The C2 architectural style supports the graphical user interface design requirements of applications (Taylor, Medvidovic, Anderson, Whitehead and Robbins 1996).

Domain Specific Software Architecture (DSSA) (Tracz, Coglianese and Young 1993; Taylor, Tracz and Coglianese 1995) grew out of the recognition that within specific domains (e.g. fighter aircraft) certain architectural design considerations are consistent. A DSSA is typically augmented with reference architecture and standardized requirements that are consistently reusable within the specific domain. The DSSA should be flexible and extensible to augment future technology. The DSSA encapsulates and expresses relationships that facilitate the implemented system's tolerance to change. The flow of control and data are more tightly defined in a DSSA because of the domain constraints being multilateral. Temporal events and component interconnections are described in a DSSA within a context of legacy systems and dominant standards for the domain, which form a constraint set easily mapped within CAS. A fundamental CAS concept necessitates the analysis of domain specific resources. Therefore, some of the resources relevant for a Cyberinfrastructure to support dynamic EMS are enumerated next.

Resources that are conceptualized as multifunctional equipment are a logical extension for the scenario presented here, given the increasingly popular approaches by firms to make devices multitasking (e.g. Sony's PlayStation that plays games and DVDs). These devices often function in a control, communication, organizational, or informational capacity, which is relevant to an analysis of emergency response systems using CAS. Domain-specific examples include: a low-level unconventional CPU design transfers the decision of what application algorithm to run from the CPU (Ziavras 2003), or smart electric power meters communicate across the existing building power infrastructure to collect, store, and transmit detailed electrical consumption and system monitoring information using data encryption (Echelon 2001). Also, Java™ language technologies were originally designed for the "convergence of digitally controlled consumer devices and computers" (http://java.sun.com/features/1998/05/birthday.html), but not the wide-scale utilization on the Internet. However, Java™ technologies are now showing dramatic growth (Chen 2004) and fostering ubiquitous computing for the software "infrastructure products" (e.g. PDA), thereby becoming a fundamental enterprise communication medium (McMillan 2001) demonstrating the emergent phenomena one would expect within a CAS (Buckley 1967; Buckley 1998).

Other examples of "smart appliances" may include the vehicles we use every day. The OnStar™ (www.onstar.com) system is becoming more popular with many car manufacturers integrating the service in new vehicles. The system employs a GPS receiver in the vehicle and a wireless modem and voice connection. Using the modem, the OnStar call center can download the exact location of the vehicle as well as remotely control aspects of the vehicle (such as unlocking the doors). Self-

aware information and communication technology and ubiquitous data collection implies many larger resource constraint issues that overlap social concerns. Inferences about unethical and immoral abuses of resources to gain or maintain illegitimate power are easily imaginable. All of these issues must be considered when creating an architectural design.

METHODOLOGICAL EXPECTATIONS

The methods described here are a derivative from CAS and the synthesized intellectual concepts from the applicable research just described, since the CAS framework integrates these diverse perspectives. Domain variety should be captured using appropriate quantitative or qualitative data collection methods. The data is then classified into constraint types since constraint is essential to CAS analysis. Note, the capture and articulation of domain variety as constraint categories are not the most difficult aspect of design. Historically, difficulties typically arise for practitioners when they attempt to formalize the more ambiguous constraints found in the socially oriented categories. We argue the established intellectual constructs for articulating the more ambiguous variety can be used to cull out crosscutting effects spanning constraint categories, which should be theoretically applicable to all mission-critical infrastructure and emergency response networks.

The Cyberinfrastructure designer can use concrete resource concepts when categorizing constraints and reasoning about the interaction of constraints across categories, which are two conditions for sufficient domain representation. Concrete resources constraints arise from stakeholder empowerment within an objective perspective and vary in density from physical laws (e.g. $E=mc^2$) to governmental policy (e.g., FERC NOPR to deregulate the electric power industry (1996)). Other "stylistic" constraints are subjective and tightly coupled with epistemological constructs used to determine what is "knowledge" because "Design, in all of its realizations (e.g., architecture, landscaping, art, music), has style" (Hevner, March, Park and Ram 2004). Stylistic views map easily into typical software and information systems architectural abstractions to enable software tool support.

Generally speaking, any variety or type of act perpetrated by actors can explain a large portion of the world. This perspective facilitates the examination of representational sufficiency by establishing a consistent framework across all constraint types. The "wicked" problem of Cyberinfrastructure design depends on accurately capturing the symbiotic relationship already present in the domain, which is enormous when one considers built infrastructure such as electric power. Nevertheless, to design a malleable Cyberinfrastructure some approach must be adopted. As noted earlier, we think a Domain Specific Software Architecture (DSSA) style (Tracz, Coglianese and Young 1993; Taylor, Tracz and Coglianese 1995; Klashner 2002) would facilitate discovering the best "fit" when considering a solution to the GTTI problem. The concept of "domain" has been applied to many different levels of architectural abstraction (Klashner 2002) such as operating systems or electric power. This flexibility can be applied to emergency response, urban infrastructure, or interacting ICTI. Reuse was a primary motivation for establishing DSSA concepts that are intended to result in a representational sufficient architectural baseline. Thus, a DSSA style can be developed to span all constraint categories to satisfy the theoretical framework. Also, the DSSA style can be used because infrastructure is often logically treated in a holistic fashion, with reusable concepts, that is consistent with systems theory upon which CAS rests.

The requirements to solve the GTTI problem are tightly coupled with the breadth of the problem domain (i.e., anywhere people inhabit or travel) and the need to have complex sensornets for a Cyberinfrastructure. To address this constraint with its crosscutting effects, we choose to leverage the worldwide electric power infrastructure because it is ubiquitous in the sense that electrical voltage is never too far away from any populated location. Since electric power mediums can and will carry data (Echelon 2001), the electric power grids will effectively become a primary sensory medium. Therefore, electricity is a consistent resource to consider for the design solution. However, the designed Cyberinfrastructure would integrate a number

of existing infrastructures (e.g. telecommunications). The actual final system design would include most if not all of the other built infrastructures, but they have less scope with respect to proximity to population.

Initial concept drawings of built architectural structures in architectural processes are rough and rarely closely resemble the finished product. These drawings serve several purposes within the traditional architectural process that has been conceptually leveraged by IS architects (Zachman 1987) and software architects (Perry and Wolf 1992; Perry 1997). The strength of such a process is the enumeration and negotiation of domain constraints that must be factored into an effective design. These approaches are synergistic and complimentary with IS design research (Hevner, March, Park and Ram 2004).

The method should allow designers to capture the essence of the domain in a manner that is relevant to all stakeholders associated with a wide variety of resource allocation issues. The approach is used to produce an accurate constraint-based design representation of the application domain. It should be able to sufficiently represent known domain "states" because of existing relationship categories that have reflective validity in past and ongoing domain events. Stylistic constraints serve to sufficiently represent crosscutting effects in order to reduce complexity. Resources, constraints, and views work in concert to facilitate the dynamic construction of a new Cyberinfrastructure to extend or otherwise manipulate the GTTI. We suggest the following utilization of resources and constraints to illustrate design functionality:

1. Resources in the form of concrete constraints associated with technologies (referenced in the related work section):
    a. The existing and emerging technologies all create and function within a path dependent (Liebowitz and Margolis 1995) paradigm because of the scale and scope of the electric power industry.
    b. The Cyberinfrastructure designer must be cognizant of current and possible dependencies when considering the concrete domain resources in his\her design. Dependency considerations are important for:
        i. Evolutionary or maintenance requirements
        ii. Associations between constraints that are fundamental to the architecture
2. Stylistic constraints:
    a. Are context dependent
    b. Are subjective
    c. Will be elaborated upon later in the analysis section
    d. Can be viewed as:
        i. Domain variety captured as data that is transformed into information
        ii. Communication carried out through primary connections (i.e. fully functional) in contrast to communication that is ignored, inferred, or mitigated in some manner

We describe a small scenario next to demonstrate how requirements can be elicited to augment our Vision Statement. The more tangible and understandable scenario should also facilitate the development of methodologies based on the theoretical framework.

AN EMERGENCY RESPONSE SCENARIO

This hypothetical scenario is presented in order to bring together the many individual concepts presented up to now. The motivation for this scenario is to demonstrate how a Cyberinfrastructure would facilitate the accomplishment of the initial research questions. This scenario was chosen as much for its technical variety as for its sociocultural constraints, which must be considered in Cyberinfrastructure design using an adaptive method within the CAS framework. The scenario described here effectively juxtaposes current and emerging future technologies with the temporal constraints arising from the GTTI

and societal issues such as privacy and freedom.

As demonstrated in the development of CAS (Buckley 1967; Buckley 1998), one cannot arbitrarily restrict the boundaries of a system for convenience sake because the systemic behavior arises from the degree of organizational complexity internally generated by the system; i.e., not externally imposed by the designer. We are contending that control must be maintained in a holistic manner under the rubric of information interpreted using the appropriate theoretical constructs. Otherwise, per CAS, mission-critical systems can quickly fail as they transform into a state approaching chaotic organization as noted within the electric power grid blackout and GTTI phenomena. The following scenario presents this balance that must be attained in the design of Cyberinfrastructure in order to avoid degradation toward chaos as massive amounts of domain variety overwhelm conventionally designed IS.

The scenario must be contextualized, which is done next with a discussion of the CAS concepts as they apply to an emergency. Then, a brief history of a particular emergency preparedness network is introduced to help further ground the method presentation and present domain-specific motivational arguments. A technological component (Smart Buildings with there associated sub-technologies) is then introduced into the emergency scenario to demonstrate the pivotal role a new (architectural) resource can make in the design of mission-critical infrastructure. Following this scenario presentation is the discussion section, which uses the stylistic method to analyze the emergency response scenario described below.

CONTEXTUALIZATION OF EMERGENCIES USING CAS CONCEPTS

When infrastructures or emergency preparedness networks are operating in a normal state and maintaining full control of emerging situations they exhibit a well-organized behavior. Since they are not being presented with any new event variety, we can infer that little new information is gained during this situation. However, if a severe emergency event occurs, the source of the emergency event generates more variety in the domain than had been experienced before. Each entity, such as an electric power grid dispatch center or a hospital, receives event messages and interprets the variety based on their contingency plans, expertise, and IS support infrastructure (e.g., DSS) in order to map it into their view of the domain. If the level of variety increases beyond their ability to process it, the infrastructure or emergency preparedness network begins to approach the chaotic complexity organizational state, which means they have too much information or information overload. The normal set of constraints no longer correctly apply in these chaotic situations and information systems designed using traditional methods are often abandoned in favor of manual methods such as with electric power grid dispatch centers during a grid system disturbance leading to a major electricity blackout (Klashner 2002; Klashner 2004). Historically, there have been incidences where analysis of situations (such as battles during wars or tragedies) indicates the necessary data and/or information was available to arrive at an accurate appraisal of their situation, but the individuals involved did not receive and/or configure their information resources. The result was tragic loss of life because the variety existing in the domain had not been appropriately identified, processed, and delivered to the correct legitimate control entity. Analysis of the data in these cases shows that there was sufficient statistical verification of an imminent event, but individuals utilizing separate systems processed the crucial knowledge from the domain variety. Therefore, these individuals exercised their degree of freedom to choose appropriate contingency alternatives based on existing systemic constraints. The incorrect mapping of the variety resulted in the loss of human life. Similar examples exist today in mission-critical infrastructure emergency events that threaten human life and cost billions of dollars.

HISTORY AND MOTIVATION FOR A DOMAIN-SPECIFIC CYBERINFRASTRUCTURE

Emergency Medical Services (EMS) prior to the 1970s was often provided in an ad hoc manner or through facilities that served other purposes. For example, funeral homes

provided the ambulance service in Texas. There were several significant changes in the US beginning in the late 1960s that established a modern, coordinated EMS effort (BEMTDH 2001):

1. Advanced trauma (i.e. injury) research, resulting from the Vietnam War, demonstrated how well-trained non-physicians could save lives
2. Congress passed the EMS Act of 1973
3. American College of Surgeons developed a comprehensive emergency prehospital training program for ambulance attendants

In the last thirty years since modern EMS began, two critical elements are still missing from most disaster preparedness efforts. First, hospitals need to "establish communications linkages among themselves and to share information about what resources are available." Second, EMS should "deliver victims to hospitals with resources to meet their needs" (CWDMG 2003); i.e., evenly spread the load on the EMS infrastructure. Mass patient incidents (MPI) and mass casualty incidents (MCI) stretch the abilities of EMS in many communities. A MPI (e.g. a building fire) is distinct from a MCI (e.g. a hurricane) in scale and scope, but either can be caused by a wide variety of disasters (CWDMG 2003). For example, disaster types include:

- Natural such as tornadoes
- Technological as in a building collapse
- CBNRE which stands for Chemical, Biological, Nuclear, Radiological, or Explosive
- A National Security incident involving some combination of the above disasters

The largest number of trauma incidents arises from daily disasters (DD) such as auto accidents involving small groups. These DD cause tens of thousands of fatalities and millions of injuries per year. MPI are much less common and constitute far fewer deaths than the DD. MCI are very rare and cause far fewer total annual trauma deaths than the other two types. However, MCI have significant psychological and economic repercussions that cannot easily be quantified or predicted.

Scenario Technologies: Smart Buildings

Future architecture will include intelligence in the design aspect of built structures. This trend is not new (e.g., see "e/home" product convention), but will take on new meaning over the next few years. A smart building will be controlled by ICTI that enables the stakeholders (e.g. owner, tenant, utility) to control a variety of environmental factors. The familiar thermostat concept can be extended to include all digital activity; e.g., appliances reacting to changing inhabitant behavior such as with schedules. The platform independent computing allows manufacturers to open all devices for use in a networked configuration within the confines of the home combining domestic engineering and computer supported cooperative work. Sensors, preset preferences, motion detectors, and a host of other devices will be configured to take full advantage of the structure's design and occupants' habits to achieve stakeholder objectives.

A common assumption is that the typical home will have a wide variety of connectivity with the outside world (e.g. cellular phones, satellite dishes, DSL, cable with Internet modems, etc.), but due to brevity of this paper, the socioeconomic problems with this assumption will be ignored. Just as with most infrastructures, the intelligence in the appliances and structure itself may well become invisible to the occupants. The occupant may not know that the utility company can not only read the smart meter remotely, but also break down the occupants' electricity consumption by device. Instead of merely consuming power, each home will act as an intelligent node on a national network of electric power lines (Echelon 2001).

Metropolitan areas with intelligent structures/nodes scattered throughout the region will provide a ubiquitous sensor network that can be integrated into a Cyberinfrastructure. Faults in the electric power distribution (i.e. low voltage) infrastructure are often reported first by private citizens. However, in the enhanced network of the future, faults would be reported directly using the ICTI embedded throughout the distribution grid and in the homes. This data can be converted into EMS information. For example, after seismic sensors detect an

earthquake, the information could be triangulated with intelligent home and fault data utilizing the GPS infrastructure to immediately indicate the areas suffering the most damage and in greatest need of EMS. Another example, in case of a fire, wireless thermostats and burglar systems could be designed to cooperatively transmit their current ambient air temperature, number of occupants, and occupant location data that could be rapidly simulated to inform fire fighters of the fire activity and possible trauma victims within the building(s).

Intelligent electricity meters and smart devices using emerging technologies are already moving the U.S. toward this paradigm. The associated Cyberinfrastructure design issues of importance to the EMS community are intimately tied to social issues as well as technological aspects. Everyone experienced with large software system development understands the difficulty associated with integration of subsystems or components. A multilateral Cyberinfrastructure approach to support EMS will necessitate integration of extremely large existing Cyberinfrastructure (e.g. electric power, telecommunications) with emerging intelligent structure technologies.

The overall "system" state indicates the current complexion of the domain. A domain state change event is a key concept from IS and software design that can be effectively utilized for Cyberinfrastructure development. A great deal of meaning can be associated with state change events if the appropriate event source data is captured, probabilities can be assigned to an event, and events can be triangulated. Utilizing an event notification infrastructure, existing IS infrastructure such as DSS or other stand alone tools, once it is integrated will be more useful to EMS decision-makers. Each grid state has a specific set of constraints. In order to react to the emergency event, the state must be captured before an emergency or dynamically adapted to after the event. Interpreting event change data during an electric power disturbance can be very precise and proactive because the utilities have a wealth of domain-specific data and knowledge workers capable of intuitively reading the grid. Humans, unfortunately, tend to examine choices in isolation, maintain too much rigidity in problem solving, and self-impose unnecessary constraints (Kleindorfer, Kunreuther and Shoemaker 1993). An appropriately augmented and integrated DSS can utilize various models, fast statistical computation, and the entire domain state change event data to counteract these typical human restrictions. EMS personnel in the field or at other nodes on the emergency response network could have support from centralized DSS that provide additional decision options within a Cyberinfrastructure context for architectural adjustments.

Specific MPI Scenario Event

Most DD, MPI, or MCI will occur where homes or commercial buildings (but not necessarily occupants) are present. As these structures evolve, the computational resources at each node will grow exponentially. These resources can be utilized if the appropriate Cyberinfrastructure is in place. For example, given the scenario that during a storm a school bus skids off the road and collides with a power pole in a suburban or semi-rural area:

1. The bus's onboard technologies (e.g. gyroscope indicating the bus had tipped) create a state change event. Having discussed the GTTI phenomenon earlier on, it is apparent that the appropriate rescue authorities must be notified and that the appropriate help must be dispatched immediately.
    a. The bus company that has relevant occupant information, such as
        i. Emergency release forms with contact information
        ii. Average number of occupants
    b. The integrated OnStar™ system (described earlier) automatically calls directly to police and fire departments for assistance.
2. The accident may be captured on motion sensitive surveillance equipment for transmittal to the security company with live video to monitor for emerging events such as fire or additional vehicular involvement
3. The electric power utility may be able to use the smart building information (as well as video feed) to determine the

probability of a power line being down in the vicinity to determine level of danger

   a. The utility has experts with knowledge of electrocution

   b. These utility experts and/or their DSS can approximate the severity of burns based on the voltage present, weather conditions, type of soil, etc.

   c. Hospital ward specializing in burns could then be put on alert

4. Weather data gathered from smart buildings throughout the vicinity must be factored into the logistical computation to determine where to transport the MPI trauma victims based on specific injury types.

   a. The possibility of helicopter support can be factored into the calculation to determine how many trauma facilities should be considered accessible

   b. Closed roads and bridges due to flooding is automatically considered when dispatching the ambulances

Authorities can automatically access all of this data in case of an emergency without the permission of the private companies such as the bus company or school, so that it can be triangulated with school medical records. Parents could theoretically be contacted via cell phone prior to children arriving at the facilities to clarify any ambiguities such as allergies to medication or insurance discrepancies, which has delayed trauma treatment in the past. This approach is expedient, but a major privacy consideration with societal repercussions. Not only are personal records accessible, but also utilizing such technologies as OnStar™, authorities (or worse, unauthorized or malicious users) can access your exact whereabouts at any time, tracking your every movement and even controlling certain aspects of your vehicle without your knowledge. For example, home burglars could know when you were arriving or car thieves may now be able to easily unlock your car by simply hacking into your OnStar™ controller. The OnStar privacy policy states that they may share your information with legally authorized persons, which may result in your privacy being invaded.

The smart buildings demonstrate some of the technological capabilities we currently have at our disposal. The short MPI scenario event with some of the possible considerations was presented to contextualize the analysis regarding how to apply a method. Although this scenario has many resources from several different domains of concern, we will focus on the electric power to narrow the hypothetical analysis. A full analysis of this Cyberinfrastructure would not be narrowed, but encompass all applicable resources. A full domain analysis facilitates discovery through stylistic abstraction that would typically be overlooked in tradition software, information systems, or systems design efforts.

Concrete Constraints

A constraint analysis factors in expected constraints from all constraint types. Basically, the designers must methodically examine all current and near term resources to determine the broad constraints that will become applicable to the design. Each set of constraints adds both limitations and freedoms.

Plant and equipment (e.g. power lines, breakers) is a concrete resource that is currently limited in mechanistic functionality. The future extensibility of these devices for their utilization as communication network nodes will effectively remove any and all telecommunication bandwidth constraints that may still exist inhibiting an EMS Cyberinfrastructure. Hardware and low-level software that can be dynamically reconfigured in response to a state change event creates new opportunities, but also raises reliability concerns due to the increased device complexity. These developments will coincide with computer hardware and software resource developments facilitating smart buildings becoming nodes on the new network. Smart buildings can now be configured to operate in this next generation grid as software resources. If a device or building is software enabled with a proprietary technology it will not easily interface with other devices not utilizing that same technology creating an additional constraint. But the device will also more easily recognize the same proprietary application, which may provide more degrees of freedom if

the technology is somewhat ubiquitous. Intelligent devices are not as easily integrated (a constraint) into the domain as their deterministic predecessors because of their possibility to produce cascading failure. However, market constraints resulting from organizational strategy (policy resource) of competitors will likely change in order to raise barriers for adoption of proprietary offerings and slow market penetration. Also, existing domain-specific electric power market leaders with proprietary claims will not easily change standards such as those created through open source processes (a societal constraint). Cyberinfrastructure designers will have to factor in these types of path dependency considerations based on their own understanding as professionals (social resource) or even governmental policies (e.g., the Justice Departments monopoly case against Microsoft).

Security Constraint

Increasing the number of smart devices, connection or access points, sensornets, bandwidth, and so forth increases a primary architectural constraint: security. There is a direct tradeoff between the ability to observe, access, sense, and extract data to achieve security with the level of privacy of those observed. Measures can be taken to help facilitate security given data about domain state changes, but these approaches will require much research and cooperation from industry. Even though resources such as a smart building, a bus, a database, or a hospital may have the aforementioned technological features that facilitate integration during an emergency, it is a stylistic choice as to how they will be configured.

Software is very vulnerable. The ability to track activities using software creates opportunities for hackers to use the same infrastructure for unlawful pursuits (e.g., monitoring police movements). Laws typically arise from the abuse of freedoms and the violation of other people's rights. Of course, when design constraints are legislated it forcibly changes the architectural configuration of the system. The result is a shift toward centralized authority. Ultimately, "Big Brother" could legally gather whatever information it wanted using the EMS enabled systems and justify the actions under the pretense of National Security (Denning 1992). There are always numerous examples in pop culture of possible scenarios for abuse of technology (e.g., film "Enemy of the State", 1998). Certain stylistic constraints on this abuse of power would hypothetically work. For example, smart buildings could only open access to their data and facilities if a secure, encrypted signal were detected that was associated with a domain state change event directly resulting from a MPI or MCI; i.e., validation there was an actual emergency. However, it is likely with the new security awareness within funding agencies, there will be support of a new breed of more secure programming languages that would still support platform independence (a key constraint).

The final decision about what is secure enough rests with the high-level architects who depend on security engineers to plug the holes in the technology. However, a more difficult problem is how to apply the security architecture to a Cyberinfrastructure. Within the CAS framework, the stylistic constraints for security would likely be applied after a careful sociopolitical analysis wherein the results were presented to the architectural committee for further integration with other sociotechnical concerns (e.g., human computer interaction with the devices). Obviously, the context of these decisions are changing on a daily basis with emerging terrorist activity, and must be balanced with the full weight of the legal system with the appropriate human rights considerations—by no means a simplistic constraint.

Three resource views discussed below have a strong influence upon design: epistemological distinction between data and information; formalized and enumerated resource ownership, and; formalized Cyberinfrastructure behavior.

Viewing information is distinctly different than viewing data. There is a data glut in the world today, but knowledge workers are still unable to accomplish their tasks because they lack information that knowledge warehouses can provide if constructed (Nemati, Steiger, Iyer and Herschel 2002). The electric power industry and other mission-critical infrastructures are wrestling with a vast amount of domain data

that will theoretically facilitate the advancement of an EMS Cyberinfrastructure. Depending on the technology available (e.g., data or knowledge warehouse) during analysis, various conclusions can be arrived at because powerful stakeholders will negotiate based on what information is presented.

The political aspects of resource ownership are tightly coupled with the actual requirements chosen during analysis and design (Markus 1983; Bergman, King and Lyytinen 2000). How resource ownership is formalized, quantified, and presented to stakeholders as a stylistic view will greatly impact the ultimate design. For example, if the smart buildings are shown in a very abstract format as part of a metropolitan network with generic data extractions by utilities public opinion may be in favor of the EMS Cyberinfrastructure. However, if a lower level view with very specific data acquisition is released without an accompanying effective resource ownership constraint mapping, individuals may become very hostile to the design. A strong resource ownership and service commitment provision should be utilized to help anchor constraints to stakeholders, which is part of the problem definition. Negotiation can proceed regarding formalized resources with clear commitment agreements.

Capturing the requirements and negotiating the resource commitments both factor into the third stylistic view, which is Cyberinfrastructure behavior. Every entity, not just the lower level mechanistic or hardware devices, in the Cyberinfrastructure has an associated behavior that can be formalized in the associated domain of interest (e.g., engineering). Legislators (as government policy resources) would indirectly and directly constraint software development efforts with laws and policies. Therefore, views of the Cyberinfrastructure must be presented in a manner that transcends constraint type boundaries in order to eradicate ambiguities associated with misconceptions and negotiations between resource owners. For example, there may be very concise organizational models of how the hospitals and schools will behave, in this mini-case an architect must use a more flexible behavioral model if an effective Cyberinfrastructure design is to be presented to all the stakeholders for viewing. Of course, the specific behavioral models of any resource must be consistent with these interdisciplinary behavioral views, which is a major factor in the CAS integration framework.

In summary, the high-level system designers will aggregate the lower level concrete constraint analyses, stylistic constraint analyses, and resource views into a holistic Cyberinfrastructure designs. The more detailed analyses and views developed by specialists will benefit the big picture architectural team working on the EMS Cyberinfrastructure at a high level. Juxtaposing these detailed and high-level perspectives enables the reduction in wicked problem complexity through architectural processes proven over centuries in other professions. The primary aspect of most design approaches that is ineffective is the inability to address wicked problems in a complex domain. The crosscutting effects create an interwoven web of constraints. Crosscutting effects from concrete constraints to stylistic constraints to resource views are inherently expected to confound design efforts. A design method developed to work with the CAS framework will provide guidelines for software or IS designers to manage the complexity inherently associated with mission-critical infrastructure and life threatening situations.

SUMMARY

Current emergency response systems are built upon customized independent infrastructures that were developed based upon traditional IS design theory. However, this infrastructure has proven insufficient when large-scale MPI or MCI disasters occur that require information to be collaboratively shared among various agencies (e.g., fire, law enforcement, medical, etc.) and/or mission-critical infrastructure (e.g., electric power, telecommunications). To highlight this problem, phenomena including the GTTI were presented. The GTTI phenomenon demonstrates how the lack of ICTI augmented treatment will deterministically and exponentially increase the probability that the trauma injury will be fatal. We have generalized the GTTI phenomenon to all emergency phenomena in order to examine

infrastructural evolution using conventional IS design theories. The general emergency phenomena exemplified through constraints such as the inability of professionals to interface systems when necessary or of the individual systems being incapable of coping with unpredictable changes in the environment. We observed that these types of phenomena could cause the critical response window of opportunity (e.g., GTTI) to be largely wasted. As such we investigate the question; can technology be used to reduce or destroy the Golden Barrier associated with the GTTI?

A "Cyberinfrastructure" could be conceivably assembled in the near future given the certain technological advancements and the current level of interest at funding agencies such as the NSF. However, a technological deterministic vision of the future is unwarranted given a myriad of sociotechnical, sociopolitical, and sociocultural constraints upon the current emergency response capabilities. Nevertheless, assuming these inhibitors can be worked out enough to create an operational Cyberinfrastructure, a vision statement was presented wherein we asserted that emergency response capabilities could be extended to a nearly omnipresent state of awareness of the individual citizen. This level of ubiquitous observation then raises even more ambiguous and disconcerting issues that cannot be addressed offhandedly; e.g., the privacy and freedom of the population being exchanged for security.

Examining the aforementioned GTTI and other general phenomena, however, facilitates the discovery of important constraints that effect IS success and begins the discussion of some aspects of the solution to these problems. Social, technological, and domain constraints associated with unknown or uncommon emergency events lead to complex high-level requirements that combine to create a "wicked" design problem. We postulated that the design of a new Cyberinfrastructure is required to address these sort of "wicked" problems. In order to tease apart these constraints, we presented some initial questions tied to emergency response and the utilization of Cyberinfrastructure based on the vision statement. Namely, it will be for researchers to determine if Cyberinfrastructure can be designed to mitigate Golden Barrier phenomena, to overcome the myriad interacting constraints enumerated throughout this paper, to have innate awareness of crosscutting effects arising from domain forces, and to address the infrastructural complexities during design.

This paper has suggested that emergency response systems be designed within a CAS theoretical framework because of the need to dynamically evolve IS and integrate ICTI to conform to the Cyberinfrastructure objectives. The CAS framework facilitates the interdisciplinary research of these "wicked" problems because it was developed from the integrationist perspective as a bridge-building theoretical construct. Therefore, it is ideal as a guiding construct wherein multiple diverging, but complimentary methodologies can be developed to investigate the interaction between Cyberinfrastructure and the Golden Barrier in light of broader social concerns. A simple approach has not and will not provide the solution to our questions. The CAS framework has the appropriate constructs to achieve success, if it is possible. In order to ground the reader, we presented some emergency response background information and a scenario wherein some methodological speculations could be explored.

We showed how the next generation Cyberinfrastructure has certain innate characteristics that can be leveraged with the architectural metaphor. These relationships can be used in future research as a means to reason about Cyberinfrastructure and could be used to address socially complicated "wicked" problems. The design process is illustrated by teasing apart a "smart" building scenario to demonstrate the outlined approach's representational sufficiency for the emergency response system designs necessary that will likely be necessary in the future. In doing the analysis, a number of ethical, moral and social issues were brought to light.

RECOMMENDATIONS AND CONCLUSION

We conclude that a Cyberinfrastructure may soon emerge given existing technologies. Emergency Management System designers can benefit from it if appropriate theory-based methodologies can be brought to bear upon the

"wicked" sociotechnical, sociopolitical or sociocultural problems common in these domains. However, as we have shown here, difficult decisions must be made regarding the security, privacy, and degree of pervasiveness we are all willing to tolerate. We outlined some fundamental questions at the beginning of the paper. Without extending the current methodological insights presented here to conduct specific research, we cannot unequivocally answer our questions. However, from a theoretical and analytical perspective, it is possible to mitigate emergency response phenomena such as the Golden Barrier in order to save human lives during the GTTI. This relationship should hold true in mission-critical infrastructure that suffer from similar phenomena.

Utilizing the appropriate theoretical perspectives within the CAS framework will facilitate the resource/constraint viewpoint to be explored as we have alluded to in the scenario. It is important to take a real "life" cycle stance regarding evolutionary issues because infrastructure lasts for a very long time (i.e. continues to live on with us) as evidenced in the data from the electric power industry. Other proactive decisions about logical analysis and design processes must also be made in order not to be swayed with technological opportunities or by the immediate socially construed issues.

Crosscutting domain effects within CAS can be theoretically described and/or empirically discovered given the appropriate perspective and access to data. For example, through broad empirically grounded and theoretically substantiated systemic design approaches such as those referenced in this paper, society can hope to grapple with the complexities of Cyberinfrastructure design. We believe attacking these complexities squarely with appropriate theoretical perspectives will guide researchers to effective methodological approaches that can be used to mitigate emergency response phenomena such as those arising during the GTTI. Therefore, we do have a possibility of mollifying complexities that are growing at an exponential rate, which correlates with society's increasing dependence on ICTI. However, incorrectly designing, evolving, and depending on future technologies such as Cyberinfrastructure to address emergencies will likely push issues of complexity even further out of our reach—we must take care to insure that the "cure does not kill the patient".

REFERENCES

FERC, *Open Access Same-Time Information System and Standards of Conduct*. Federal Energy Regulatory Commission OASIS NOPR 889, 1996, pp. 145.

Arango, G., "Domain Analysis: From Art Form to Engineering Discipline," Proceedings of the 5th International Workshop on Software Specifications & Design, Pittsburgh, Pennsylvania, ACM Press, 1989.

Ashby, W.R., "Principles of the Self-Organizing System," In *Principles of Self-Organization*, H. van Foerster and G. W. Zopf (eds.), Pergamon Press, New York, NY, 1962, pp. 255-278.

Atkins, D. E., K. K. Droegemeier, S.I Feldman, H. Garcia-Molina, M.L. Klein, D.G. Messerschmitt, P. Messina, J.P. Ostriker, and M.H. Wright, "Revolutionizing Science and Engineering Through Cyberinfrastructure," 2003. Available at http://www.cise.nsf.gov/sci/reports/atkins.pdf , last accessed 10 January 2005.

Axelrod, R. M., and M. D. Cohen, *Harnessing complexity: organizational implications of a scientific frontier*, New York: The Free Press, 2000.

Baldwin, C.Y., "What can the social sciences gain from the science of design?," NSF Workshop on the Science of Design: Software and Software-Intensive Systems, Airlie Center, VA, NSF, 2003.

BEMTDH, "A Brief History of Emergency Medical Services and Trauma Systems in Texas," 2001. Available at: http://www.tdh.state.tx.us/hcqs/ems/StratPrepHistory.PDF, last accessed February 2004.

Bergman, M., J. King, and K. Lyytinen, "Large-Scale Requirements Analysis as Heterogeneous Engineering," In *Social Thinking - Software Practice*, Floyd, C. and R. Klischewski (eds.), Cambridge, MA: MIT Press, 2000, pp. 357-386.

Boehm, B., and K. Sullivan, “Software economics status and prospects,” *Information and Software Technology*, 2000, 41:14, pp. 937-946.

Buckley, W. F., *Sociology and modern systems theory*, Englewood Cliffs, NJ: Prentice-Hall, 1967.

Buckley, W. F., *Society - A Complex Adaptive System: Essays in Social Theory*, Australia: Gordon and Breach, 1998.

Burrell, G., and G. Morgan, *Sociological paradigms and organisational analysis: Elements of the sociology of corporate life*, London: Heinemann, 1979.

Chen, Y., *Programming Language Trends: an empirical study*, PhD thesis, New Jersey Institute of Technology, Newark, New Jersey, 2004. Available at http://www.library.njit.edu/etd/njit-etd2003-106/njit-etd2003-106.html , last accessed 10 January 2005.

Cilliers, P., *Complexity and postmodernism: understanding complex systems*, London; New York: Routledge, 1998.

Cowley, R.A., “The resuscitation and stabilization of major multiple trauma patients in a trauma center environment,” *Clinical Medicine*, 1976, 83, pp. 14-22.

Curtis, B., H. Krasner, and N. Iscoe, “A field study of the software design process for large systems,” *Communications of the ACM*, 1988, 31:11, pp. 1268-1287.

CWDMG, "An Overview of the CWDMG Plan," 2003. Central Wisconsin Disaster Management Group, Available at: http://www.ncrtac-wi.org/ppt/OVERVIEW_NO_NARRATION_update.ppt, last accessed February 2004.

Denning, P.J., “Halting the Unstoppable,” *Communications of the ACM*, 1992, 35:7, pp. 11-12.

Echelon, *Power Line-Based Meters Provide Energy Management Solutions*. L. Balistreri, Scotts Valley, Calif., Echelon Corporation, 2001.

Ellis, J., "Debunking Some Myths About the Great Northeast Blackout," 2003. Alexander's Gas & Oil Connection, Available at: http://www.gasandoil.com/goc/company/cnn34274.htm, last accessed November 2003.

Fielding, R.T., and R.N. Taylor, “Principled design of the modern web architecture,” *ACM Transactions on Internet Technology*, 2002, 2:2, pp. 115-150.

Forster, P., and J.L. King, "Information Infrastructure Standards in Heterogeneous Sectors: Lessons from the Worldwide Air Cargo Community," In *Standards for Information Infrastructure*, B. Kahin and J. Abbate (eds.), MIT Press, Cambridge, MA, 1995, pp. xiv 653.

Gasson, S., “Human-Centered Vs. User-Centered Approaches to Information System Design,” *Journal of Information Technology Theory & Application*, 2003, 5:2, pp. 29-46.

Hevner, A., S. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Quarterly*, 2004, 28:1, pp. 75-105.

Jackson, M., *Software requirements & specifications: a lexicon of practice, principles and prejudices*, New York, NY: ACM Press/Addison-Wesley, 1995.

King, J.L., R.E. Grinter, and J.M. Pickering, "The Rise and Fall of Netville: The Saga of a Cyberspace Construction Boomtown in the Great Divide," In *Culture of the Internet*, S. Kiesler (ed.), Lawrence Erlbaum Associates Publishers, Mahwah, NJ, 1997, pp. 3-34.

King, J.L., V. Gurbaxani, K.L. Kraemer, F.W. McFarlan, K.S. Raman, and C.S. Yap, “Institutional factors in information technology innovation,” *Information Systems Research*, 1994, 5:2, pp. 139-169.

Klashner, R., *Using Architecture Style to Design and Evolve Complex Integrated Information Infrastructure*. Information and Computer Science, Irvine, CA, University of California, 2002.

Klashner, R., “ICT and the Deregulation of the Electric Power Industry: A Story of an Architect's New Tool,” *Journal of Digital Information*, 2004 (to appear in a Special issue on Social Aspects of Digital Information in Perspective).

Kleindorfer, P.R., H. G. Kunreuther, and P.J.H. Schoemaker, *Decision Sciences: An Integrative Perspective*, New York, NY : Cambridge University Press, 1993.

Leveson, N.G., "Toward a Science of Software Design". NSF Workshop on the Science of Design: Software and Software-Intensive Systems, Airlie Center, VA, NSF, 2003.

Liebowitz, S., and S.E. Margolis, “Policy and path dependence: From QWERTY to Windows 95,” *Regulation*, 1995, 18:3, pp. 33-41.

Markus, M.L., “Power, Politics, and MIS Implementation,” *Communications of the ACM*, 1983, 26:6, pp. 430-444.

Markus, M.L., *Systems in Organizations*, Marshfield, MA: Pitman Publishing Inc., 1984.

Markus, M.L., A. Majchrzak, and L. Gasser, “A Design Theory for Systems that Support Emergent Knowledge Processes,” *MIS Quarterly*, 2002, 26:3, pp. 179-212.

McMillan, M., "Technology Leaders Join to Provide Key Collaboration Infrastructure that Promotes Secure Mobile Computing and Communication Between PDAs," 2001. Available at: http://www.insignia.com/content/about/releases/011003.shtml, last accessed February 2004.

Nemati, H.R., D.M. Steiger, L.S. Iyer, and R.T. Herschel, “Knowledge warehouse: an architectural integration of knowledge management, decision support, artificial intelligence and data warehousing,” *Decision Support Systems*, 2002, 33:2, pp. 143-161.

NSF, "Science of Design - Program Solicitation," 2004, Available at: <http://www.nsf.gov/pubs/2004/nsf04552/nsf04552.htm>, last accessed November 2004.

Oreizy, P., N. Medvidovic, and R.N. Taylor, "Architecture-based runtime software evolution". The Proceedings of the International Conference on Software Engineering ICSE'98 (Kyoto, Japan), 1998.

Perry, D.E., "Directions in Process Technology -- An Architectural Perspective". Workshop on Research Directions in Process Technology, Nancy, France, 1997.

Perry, D.E., and A.L. Wolf, “Foundations for the Study of Software Architecture,” *ACM SIGSOFT Software Engineering Notes*, 1992, 17:4, pp. 40-52.

Pickering, J.M., and J.L. King, “Hardwiring weak ties: Interorganizational computer-mediated communication, occupational communities, and organizational change,” *Organization Science*, 1995, 6:4, pp. 479-486.

Rapoport, A., and W. Horvath, “Organizational Theory,” *General Systems*, 1959, 4, pp. 87-91.

Reddy, M., P. Dourish, and W. Pratt, "Coordinating Heterogeneous Work: Information and Representation in Medical Care". Proceedings of European Conference on Computer Supported Cooperative Work (ECSCW'01) (Bonn, Germany), 2001.

Rittel, H.W.J., and M.M. Webber, “Dilemmas in a general theory of planning,” *Policy Sciences*, 1973, 4, pp. 155-169.

Salasin, J., "Habitats Infrastructure for Knowledge-centric Operations (KO)," Proceedings of the 8th International Conference on the Engineering of Computer-Based Systems (Washington, DC.), IEEE, 2001.

Simon, H.A., “Artificial Intelligence: An Empirical Science,” *Artificial Intelligence*, 1995, 77:1, pp. 95-127.

Swartz, M., *Power Failure: The Rise and Fall of Enron*, Aurum Press, 2003.

Taylor, R.N., and J. Coutaz, "Software engineering and human-computer interaction," Proceedings of the ICSE '94 Workshop on SE-HCI: Joint Research Issues (Sorrento, Italy), Springer, 1994.

Taylor, R.N., N. Medvidovic, K.M. Anderson, E.J. Whitehead Jr., J.E. Robbins, “A Component- and Message-Based Architectural Style for GUI Software,” *IEEE Transactions on Software Engineering*, 1996, 22:6, pp. 390-406.

Taylor, R.N., W. Tracz, and L. Coglianese, “Software Development Using Domain-Specific Software Architectures: CDRL A011A curriculum Module in the SEI Style,” *SIGSOFT Software Engineering Notes*, 1995, 20:5, pp. 27-37.

Tracz, W., *Tutorial, software reuse: emerging technology*, Washington, D.C.: IEEE Computer Society Press, 1988, pp. xi 378.

Tracz, W., L. Coglianese, and P. Young, “A Domain-Specific Software Architecture Engineering Process Outline,” *ACM Software Engineering Notes*, 1993, pp. 40-49.

Turoff, M., M. Chumer, B.A. Van de Walle, and X. Yao., “The Design of a Dynamic Emergency Response Management Information System (DERMIS),” *Journal of Information Technology Theory & Application*, 2003, 5:4, pp. 1-36.

Ulrich, W., “A Philosophical Staircase for Information Systems Definition, Design, and Development: A Discursive Approach to Reflective Practice in ISD (Part 1),” *Journal of Information Technology Theory & Application*, 2001, 3:3, pp. 55-84.

Walls, J.G., G.R. Widmeyer, and O. El Sawy, “Building an Information System Design Theory for Vigilant EIS,” *Information Systems Research*, 1992, 3:1, pp. 36-60.

Wets, J.F., "Thomson-CSF and Ada for ATC: An experience of eight years," Proceedings of the conference on TRI-Ada '91 Annual International Conference on Ada (San Jose, California, US), ACM Press, 1991.

Wiener, N., *I am a Mathematician*, New York, NY: Doubleday & Company Inc., 1956.

Zachman, J.A., “A Framework for Information System Architecture,” *IBM Systems Journal*, 1987, 26:3, pp. 454-470.

Ziavras, S.G., “Processor Design Based on Dataflow Concurrency,” *Microprocessors and Microsystems*, 2003, 27:4, pp. 199-220.

AUTHORS

Robb Klashner is an Assistant Professor in the Information Systems Department, College of Computing Sciences at the New Jersey Institute of Technology (http://web.njit.edu/~klashner). He has a Ph.D. in Information and Computer Science from the University of California Irvine. His current research interests include: decision support systems, design of emergency response systems, theoretically grounded analysis and design, mission-critical infrastructure, integrated information infrastructure, software architecture design tool environments, software engineering, and requirements acquisition using qualitative methods.

Sameh Sabet is a Distinguished Member of Technical Staff at Tyco Telecommunications Laboratories. He is also an adjunct professor at NJIT where he teaches requirements engineering. He is a Ph.D. candidate in Information Systems at NJIT. Previously, he was Director of Network Systems Development for TyCom Labs. He has over 10 years of experience in IT as well as software design, development and real-time embedded systems design for Network Management Systems in the telecommunications industry. His current research interests span augmenting alarm correlation with emerging decision support systems and knowledge management research.