Environment and Planning B: Planning and Design 2007, volume 34, pages 1103 – 1124

DOI:10.1068/b32078

Learning the critical infrastructure interdependencies through an ontology-based information system

Robert K McNally, Seok-Won Lee, Deepak Yavagal, Wei-Ning Xiang¶
Department of Geography and Earth Sciences, Department of Software and Information Systems, University of North Carolina at Charlotte, 9201 University City Boulevard, Charlotte, NC 28223, USA; e-mail: rkmcnall@uncc.edu, seoklee@uncc.edu, dsyavaga@uncc.edu, wxiang@uncc.edu
Received 4 May 2005; in revised form 6 August 2006; published online 1 October 2007

Abstract. A critical infrastructure (CI) is an array of assets and systems that, if disrupted, would threaten national security, economy, public health and safety, and way of life. Essential to the practice of critical infrastructure planning and drills are two pieces of knowledge. One concerns the interactions within a CI system (intradomain interdependencies), and the other concerns the interactions among the CI systems (cross-domain interdependencies). A thorough understanding of these two interwoven CI interdependencies is crucial to such tasks as vulnerability assessment, scenario composition, and homeland security drills. In this paper we present a new approach that facilitates the learning of the interdependencies. Employing a loosely coupled system of GIS and an ontology-based object modeling system developed in this study, it represents and visualizes the intradomain and cross-domain CI interdependencies both diagrammatically and geographically. The system and its knowledge representation methodology were tested through a case study in the Southeastern United States.

1 Introduction

An infrastructure is a set of basic facilities, services, and installations that are necessary for the functioning of a community or society, such as transportation and communications systems, water and power supplies, employment centers, medical facilities, and public institutions, including schools, post offices, and prisons. They are *critical* in that a disruption would threaten the security, economy, public health, safety, and way of life of a community or society. In recent years, unfortunately, critical infrastructure (CI) systems have become a symbolic target, as well as a mass casualty opportunity, for terrorist attacks (Bolz et al, 2002; Branscomb, 2004). Because of this dual identity of CI systems and the high level of vulnerability they bear, critical infrastructure protection (CIP) has topped the list of priorities in the practice of homeland security planning in the United States (Terner et al, 2004).

Essential to the practice of CIP planning and drills is the knowledge or understanding of the behaviors of the system of critical infrastructures—its functionalities and vulnerabilities. Before further deliberation, it is important to draw distinctions between two related but different concepts—a CI system, and a system of CIs. A CI system is an assemblage of functional objects that provides a certain essential good or service. A power supply system, for example, provides electrical service through the synergistic interactions among its components—the power plant, substations, transformers, and transmission and distribution lines.[1] At the same time, a CI system is also a part of an even larger system—a system of CIs, which offers a range of public goods and services through the collaborative operations of, or interdependencies among, its individual CI system components. The behavior of a system of CIs, as a manifestation of the usually complex interdependencies, cannot be fully described and understood by the behaviors of its CI system components (Rinaldi et al, 2001).

¶ Corresponding author.
[1] A glossary of the related terms is provided in the appendix.

The utility of traffic control in a municipality, for instance, is provided by a system of three CIs—power grid, telecommunication network, and traffic control boxes. However, the proper functioning of the three CI system components is only a necessary condition for the normal operation of the traffic control system. It alone is not sufficient. The configurations under which the three CI components are bonded together, the nature and magnitude of their bonding (positive and/or negative feedbacks, for example), and the self-regulating mechanisms (power back-ups and surge protections, for example) are all *emergent features* that are essential to the normal operation of the traffic control system but do not exist when the three CI system components are separate. [For a detailed account of emergent features and other concepts in the general systems theory, see Bowler (1981), Vemuri (1978), and von Bertalanffy (1973); for emergent system features in software engineering, see Sommerville (2004, pages 23–25)]. Upon this distinction, two types of CI interdependencies can be identified. The functional connections among CI objects within a CI system are intradomain interdependencies, and those among CI objects across different CI systems within a system of CIs are cross-domain interdependencies.

Therefore, there exist two types of knowledge within the CI domain. The first concerns the behaviors of a CI system when it is (or assumed to be) a stand-alone system, which are grounded on the intradomain interdependencies. The second concerns the behaviors of a system of CIs grounded on the cross-domain interdependencies. Both types of knowledge are contributive to a sound practice of CIP planning and drills. However, it is the second type of knowledge that provides greater insights needed for the key tasks of problem diagnosis, scenario composition, and emergency response (Rinaldi et al, 2001; Xiang et al, 2005).

In this paper we present an ontology-based information system that facilitates CIP professionals' learning of the behaviors of the system of CIs. Employing a generic object-modeling tool and a GIS, we represent and visualize the two types of knowledge both diagrammatically and geographically. The system and its knowledge representation methodology were tested through a case study in the Southeastern United States.

The remainder of the paper is organized as follows. Section 2 discusses a quadruple perspective of the interdependencies within a system of CIs. Section 3 details a proposed ontology-based information system. Section 4 presents a methodology for representing the two types of knowledge with the system. Section 5 reports the case study. In section 6 we draw conclusions.

2 A quadruple view of CI interdependencies

The CI interdependencies, both intradomain and cross-domain, within a system of CIs can be viewed from many different vantage points (Rinaldi et al, 2001). Among the most relevant and useful vantage points with respect to CIP planning and drills are those of functional dependency and spatial proximity.

2.1 Functional dependency

A functional dependency is a bond between two CI objects when one object relies on another object in order to operate properly. Functional dependencies can be unidirectional or bidirectional. Telephone offices, for example, rely on commercial power supplies, and the power company uses telemetry to monitor operational equipment. Furthermore, unidirectional functional dependencies under normal conditions can turn bidirectional during a catastrophic event. Traffic lights, for instance, rely on a power supply for their normal operations, but the power supply does not rely on traffic lights to operate. However, when power disruption occurs, the repair crews of the power company could be affected by the malfunctioning traffic lights.

The functional dependencies among CI objects, unidirectional or bidirectional, fall into two broad categories—direct and indirect. Objects A and B are said to be functionally dependent or interdependent directly when A immediately relies on B, and/or B immediately relies on A. Objects A and C are related indirectly when there are one or more mediating objects in between them—object C relies on object A through object B, for instance.

2.2 Spatial proximity

The other type of relationship that CI objects within a system of CIs possess pertains to their spatial proximity. As physical objects, they are spatially tangible. As such, they usually exhibit a certain degree of adjacency in geographic space. This spatial proximity usually reflects the technological requirements to deliver the service. For instance, networked objects are geographically distant from one another to ensure an adequate coverage of the service area. It may also manifest the functional dependencies—some CI objects simply need to be proximal to one another for mutual functional support. Objects that require commercial power may receive that power from a nearby substation (a high degree of spatial proximity), whereas the substations themselves are dispersed across the region to provide the electric service (a low degree of spatial proximity). Still, there are cases where proximity is either determined by such land-use factors as land availability, zoning, and NIMBY (not-in-my-backyard) mentality, or is defined by such physical barriers as mountains, oceans, rivers, lakes, and terrains.

2.3 A quadruple view

Additional insights emerge when the CI interdependencies are examined under a framework that combines functional dependency with spatial proximity (figure 1).

The CI objects in quadrant A functionally depend upon one another directly and demonstrate a high degree of spatial proximity. For example, a long-distance toll center and a local telephone central office are often housed in the same building not only for their direct functional interdependencies but also for the reduction in transfer costs. A mobile telephone switching office (MTSO) and a long-distance toll center, for another example, are both close to a telephone central office on a long-distance network for call completions. This quadrant has been, and will continue to be, the main focus of CIP planning and drills for the high level of vulnerability it bears.

The CI objects in quadrant B functionally depend on one another indirectly but demonstrate a high degree of spatial proximity. A main natural gas pipeline and a power transmission line, for instance, often share the same right-of-way easements as a result of cost sharing, zoning regulations, and/or NIMBY constraints. Along with this proximity comes a high level of vulnerability, because a simultaneous disruption of multiple CI systems is not only damaging itself, but can also cascade reactions among CI objects in quadrant A. However, owing largely to the indirectness in their functionalities, CI objects in this quadrant usually receive much less attention for protection than they should have in the practice of CIP planning and emergency drills.

The CI objects in quadrant C functionally depend on one another indirectly and demonstrate a low degree of spatial proximity. These objects usually belong to different CI systems. For example, local telephone central offices receive electricity from a power generation plant through a series of objects on an electrical power grid—transmission substations, transmission lines, and distribution substations, and there is usually no proximal requirement between a power plant and phone central offices. Despite their functional indirectness and spatial remoteness, however, there are many cases in which major catastrophic events at national and/or international scales are

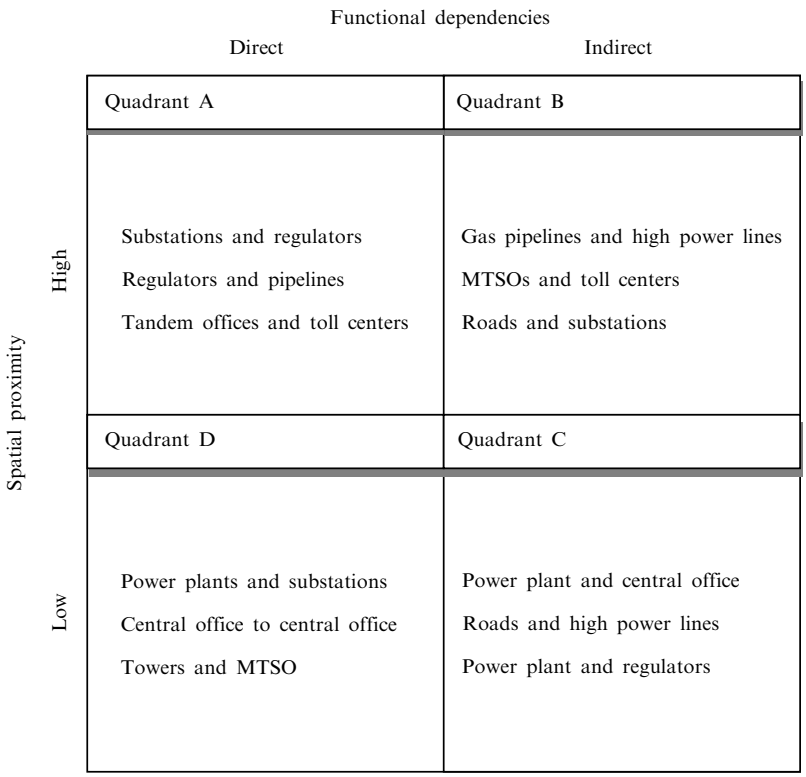

Figure 1. A quadruple view of critical infrastructure interdependencies. MTSO denotes mobile telephone switching office.

triggered by a seemingly trivial incidence in these CI objects.[2] Nevertheless, the CI objects in this quadrant are usually overlooked in the practice of CIP planning and emergency drills.

The CI objects in quadrant D are essentially the networked objects within each component CI system. As each CI system provider has a vested interest in sustaining the continued operations of the network, such measures as contingency plans and crisis response protocols are already established. However, the segmented nature of the CI service deliveries often constitutes a 'corporate firewall' that prevents CI system providers from incorporating into their contingency planning those vulnerabilities of their systems caused by the CI interdependencies in other quadrants.

It is evident that the above quadruple view of the two inextricable aspects of CI interdependencies is more advantageous than the individual vantage points. Not only does it offer greater insights about the interdependencies among CI objects within a system of CIs, but it also provides a more comprehensive, relevant, and thus useful framework for the practice of CIP planning and drills. What is needed then is an information system that allows CIP professionals to learn the behaviors of a system of CIs and to plan and design drills from this elevated vantage point. Such a system should be capable of representing and visualizing both aspects of CI interdependencies—

[2] For instance, the power blackout in the Northeastern United States and Southeastern Canada in August 2003 was originated by an incident in Parma, Ohio, a suburb of Cleveland, where untrimmed overgrown trees severed one section of high-voltage power transmission line (US–Canada Power System Outage Task Force, 2004). The cascading effect that resulted in other CI systems—the telecommunication services, aviation, and transit—affected millions of people in both countries.

functional dependencies and spatial proximity—seamlessly and effectively. In this way the knowledge of CI interdependencies becomes readily available to CIP professionals when they undertake such tasks as vulnerability assessment, scenario composition, and emergency response.

In the next section (section 3) we present an ontology-based information system that is capable of supporting the representation and visualization of CI interdependencies from the quadruple vantage point. In section 4 we discuss a methodology for knowledge representation with the system. We then demonstrate, through a case study in section 5, how the information system and its knowledge representation methodology operate in support of the quadruple viewpoint of CI interdependencies.

3 An ontology-based information system

3.1 Ontology-based information systems and their approach to knowledge representation

In the fields of information systems and software development, ontology is a systematic way to organize information in general, and knowledge in particular (Fonseca et al, 2002; Guarino, 1998; Nunes, 1991). For a given real-world system an ontological model provides a holistic view of the system which gives an equal amount of attention both to the system's component objects and to the relationships among them. More specifically, in an ontology-based model system, each domain of knowledge is represented as an ontology of hierarchical structure; different domains of knowledge at one level of specification are intertwined through a network of ontologies to form an ontology of higher order, which under the same organizational principle is a component of a networked ontological hierarchy of an even higher order.

The use of an ontology-based system in knowledge representation and visualization has been reported in many areas of research, such as bioinformatics (Stevens et al, 2000), legal arguments (Zeleznikow and Stranieri, 2001), and software requirements engineering (Evermann and Wand, 2005; Lee and Yavagal, 2004; Lee et al, 2004), but has only been discussed implicitly in CIP research papers (for example, Wolthusen, 2004, pages 33 – 34). Nevertheless, the systematic approach to knowledge representation undoubtedly entitles an ontology-based information system to be an ideal tool for CI interdependency representation and visualization. First of all, an ontology-based object model built on this approach is capable of articulating an array of knowledge or expertise from different domains under one overarching framework with a common language. Upon this harmonic system of knowledge, communications among various domain experts can be readily achieved. This is especially beneficial to the understanding of CI interdependencies, as a system of CIs typically assembles a wide range of CI systems that operate on diverse conditions and under various sets of standards. GenOM [Generic Object Model, the system used in this study (see Lee and Yavagal, 2004)], for instance, represents and organizes the knowledge about CI interdependencies through a three-leveled hierarchy of object classes. Those at the top level of the hierarchy are conceptual or abstract objects that generally subsume the objects at the intermediate level. Those objects at the intermediate level are in turn composed of the actual instances at the bottom level of the hierarchy. Objects across levels of the hierarchy are bound by *inheritance*—an object can 'inherit' characteristics or properties of a higher-level object (Turban and Aronson, 2001)—and *multiple inheritance*—an object inherits characteristics or properties of multiple higher-level objects (Egenhofer and Frank, 1992; Frank, 1997). This way of knowledge abstraction and structuring is not only effective, especially with regard to objects with pertinent operations (Egenhofer and Frank, 1992), but is also natural cognitively. Secondly, a system of networked ontologies can express dynamic relationships such as temporal events (Egenhofer and Frank, 1992). This knowledge can then be represented visually in a semantic network model.

Thirdly, an inference engine, a standard feature of an ontology-based object model system, allows the execution of production rules in order to reason about the causal relationships of state variations of the objects.

Among the drawbacks of an ontology-based object model system is the lack of spatial data handling, rendering, and analysis features that are necessary to represent and visualize effectively the spatial aspects of ontologies (that is, CI interdependencies, in our case). Since these are exactly the major strengths of GIS, in this study a loosely coupled system of a GIS and an ontology-based object model system is proposed that combines the strengths of the two individual systems.

3.2 An ontology-based information system for CI interdependency representation and visualization

The ontology-based information system developed in our study is composed of five subsystems (shown in figure 2). These are users, including CIP planners and decision makers; a user interface; a database management system (DBMS); a model base management system (MBMS); and a knowledge base management system (KBMS). DBMS and MBMS reside in a GIS, and KBMS resides in GenOM, a knowledge representation and management system (Lee and Yavagal, 2004). Since both GIS and GenOM have their own user interfaces, a consolidated user interface is proposed that combines their strengths under one overarching framework. This task of consolidation is accomplished through a system integration environment (Lee et al, 2004). The spatial DBMS component contains CI data both in cartographic and in attributive formats, and can exchange attributive information with GenOM. It also offers an environment for visualizing spatial information. The spatial MBMS is a repository of analytical tools for spatial statistics and cartographic modeling. The KBMS is the 'brain' of the loosely coupled system that provides capabilities of knowledge representation, knowledge visualization, and reasoning.

GenOM is a knowledge representation and management tool that aids the design and development of software applications by using object-oriented technologies (Lee and Yavagal, 2004). Built on the theoretical foundations of frame representation in artificial intelligence and domain modeling from software engineering, it provides three sets

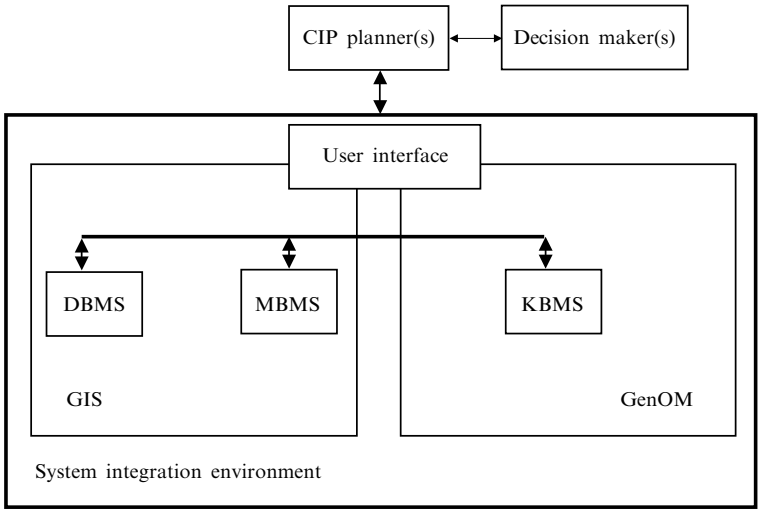

Figure 2. The ontology-based information system for critical infrastructure interdependency representation and visualization. CIP—critical infrastructure protection; DBMS—database management system; MBMS—model base management system; KBMS—knowledge base management system.

of functions. These are: object modeling in its representation—domain understanding through the conceptualization of the domain model; the usage of objects in its application model—application-oriented problem solving; and the aggregation of evidence that supports the analysis of objects' behaviors—semantic analysis of units of measure. The harmonization of these functionalities often determines the intelligence level of the developed applications. Furthermore, when a software computing paradigm converges toward domain-independent interdisciplinary research, the objects (or models) used in each application model are interoperable/sharable and reusable. GenOM is fully compatible with the Open Knowledge Base Connectivity specifications [that is, OKBC specifications (Chaudhri et al, 1998)] as well as the Web Ontology Language [that is, OWL (McGuinness and van Harmelen, 2004)] representation format.

As shown in figure 3, a domain-specific application is built on top of the GenOM foundation layer, while GenOM itself serves as an integrated environment to create, edit, browse, search, and maintain various types of objects in the application domain model. An application domain model is represented by class, property, feature, and instance objects in the GenOM knowledge base (that is, rule base). Hierarchical representations of such objects are synthesized and compiled as a knowledge structure of the given problem context. The inference model provides a rule engine that can infer relationships in the object model hierarchy. The viewpoints model provides a way to identify and incorporate different views or perspectives of the domain model. The visualization model provides a mechanism to visualize the object model hierarchy. The collaboration model supports various mechanisms that facilitate collaborative domain model construction through semantic integration of knowledge from multiple domain experts. In addition, GenOM provides mechanisms for mediating, mapping, merging, and integrating different levels of knowledge representation of domain-specific objects.

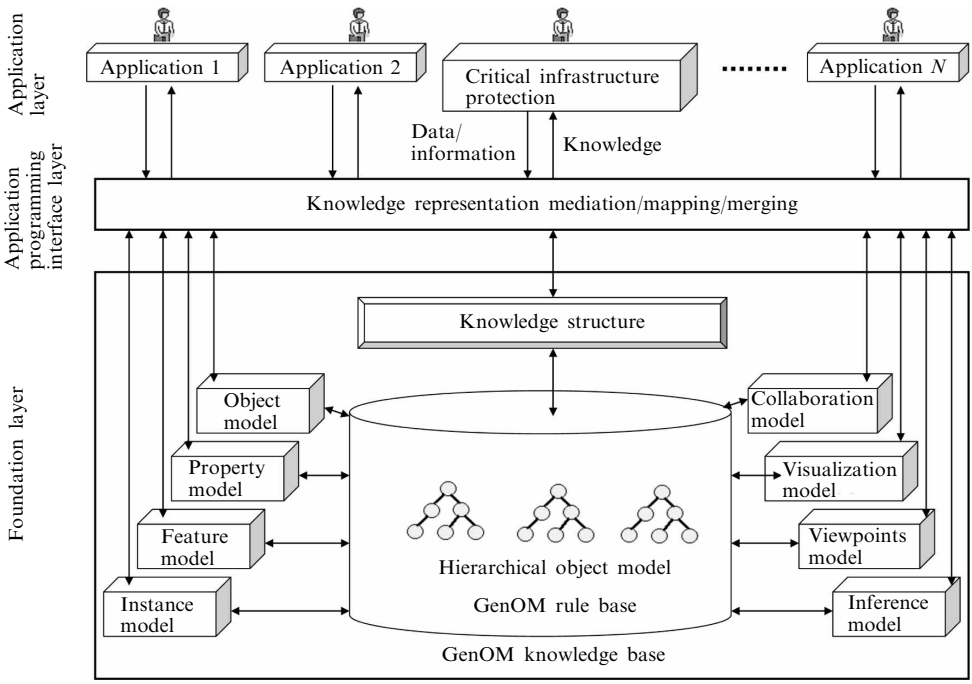

Figure 3. The conceptual architecture of GenOM.

In a GenOM rule base each CI system is represented as a *domain* within which all the component CI objects are rendered as *objects* along with their attributes. The knowledge about interdependencies among CI objects within each domain—that is, the intradomain interdependencies, is semantically represented, as is the knowledge about cross-domain interdependencies. All of these can be visualized diagrammatically in GenOM and geographically in GIS.

It should be noted that there are tools of similar ontological representation capabilities. The Unified Modeling Language (UML), for example, supports the construction of ontological models that are powerful and flexible in representing study cases, and is highly usable and transparent to the users (Berenbach, 2004; Kogut et al, 2002). Our choice of GenOM is based upon the realizations that a hierarchical representation of the CI objects and their interdependencies, both intradomain and cross-domain, can be readily materialized with the existing capabilities in GenOM; and that the diagrams of the study cases constructed with UML are focused more on the system–actor boundary than on the relationships in and across the domains (Jackson and Zave, 1993; Offen, 2002) and their characteristics in the environment (Jackson, 1997).

4 A methodology for CI interdependency representation

In this section we present a methodology for representing CI interdependencies with the ontology-based information system described above. The methodology is developed upon the following premise. Each expert of a CI system is well versed in the knowledge of the intradomain functional dependencies and the geographic locations among their CI objects. What is not well understood by system experts, government officials, and emergency planners, however, is the knowledge of the interdependencies, both functionally and spatially, within each individual domain and across the domains in a system of CIs. Therefore, the methodology proposed seeks not only to replicate system experts' knowledge of CI systems but also to represent both the intradomain and cross-domain CI interdependencies within a system of CIs. The methodology is a waterfall model with feedback loops (figure 4).

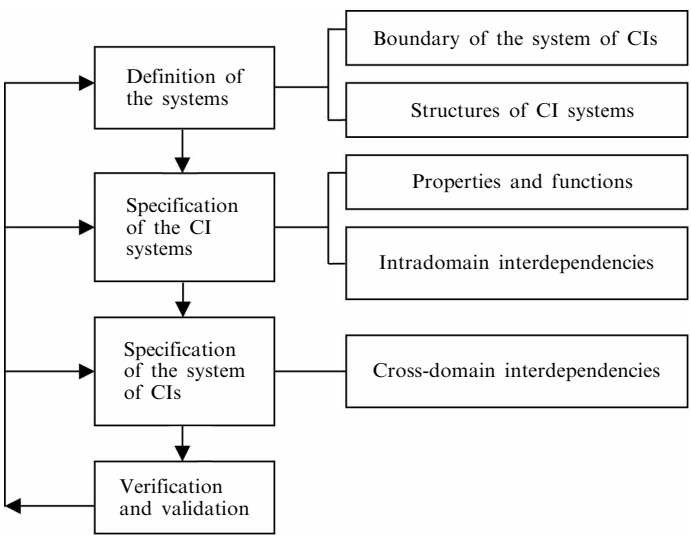

Figure 4. A methodology for representing critical infrastructure (CI) interdependencies with the ontology-based information system.

4.1 Definition of the systems

System definition involves two tasks—definition of the system of CIs, and definition of the components of CI systems. The task of defining the system of CIs addresses the foremost issue as to which CI systems should be included in the whole—the system of CIs. The ten critical infrastructures identified by the United States Department of Homeland Security (2003) serve as a benchmark for useful reference. But the decision on the component CI systems should be made in accordance with the purpose of CIP planning and drills.

Once the system of CIs is bounded, the second task is to define the hierarchical structure of each CI system. For each CI system there are at least three levels of object abstraction that need to be defined. Figure 5 illustrates this concept with two CI systems, but the same concept can be extended to any number of CI systems within a system of CIs. At the top level are overarching objects that bear the domain names of the CI systems. For example, water supplies, telecommunicatios, and sewer systems are top-level objects, each subsuming its unique set of component parts. At the intermediate level are the objects that are subclasses of the top-level object. The domain of water supplies, for instance, has component objects at the intermediate level, such as reservoirs, treatment facilities, pump stations, valves, and distribution pipelines. At the bottom level are the specific cases or instances of the intermediate level objects. These are the actual objects in existence that are usually, but not necessarily always, multiple in number. The category of pump stations, for example, may comprise many water pumping stations that are located at different geographic regions with specific names, addresses, and attributes.

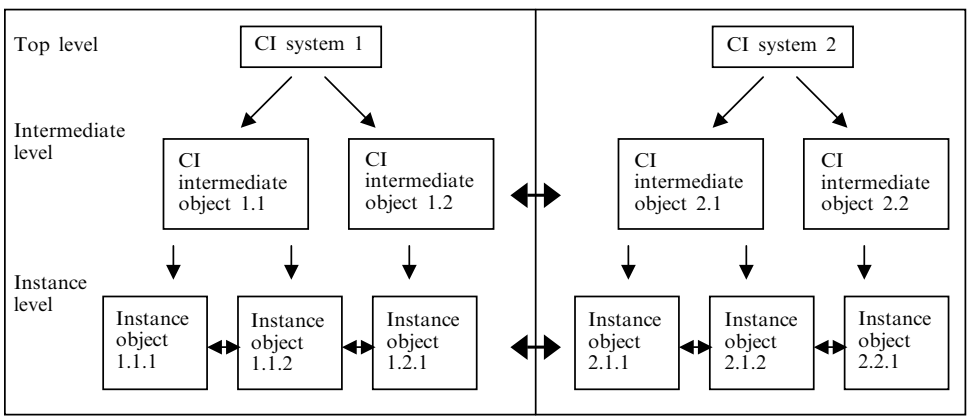

Figure 5. The abstraction levels of a system of two critical infrastructures (CIs).

4.2 Specification of the CI systems

The process of specifying each CI system involves two tasks. The first task is to detail characteristic properties and functions for the component objects. The second task is to represent intradomain dependencies that need to be explicitly expressed among objects with respect to their functional dependencies and geographic proximities.

4.2.1 *Properties and functions*

The first task is to assign the characteristic properties to the various objects at the top and/or intermediate levels. Properties are the attributes of a particular object, and each object can have multiple properties of different types. These properties can be classified as strings (text), real numbers or integers, Boolean, or even a nexus of objects as values. A telephone office, for instance, has properties of 'number of switches' and 'building

square footage'. Just as multiple properties can be assigned to an object, several values can be assigned to each property. For example, the property station type can take a value of booster station or transformer reducer. An object at the intermediate level inherits all the properties from its particular parent at the top level, so the properties can be as common or as limited as is warranted. Similarly, the instances inherit all the properties of their parent objects at the intermediate level, differing only in property values if other than the default values. For example, an instance of the telephone office may have 35 switches and 1080 ft^2, versus another instance of a telephone office with 18 switches and 765 ft^2.

The second task involves specifying functions for objects at the intermediate level. A function refers to the purpose, behavior, or action of an object. For example, the string produces electricity can be the assigned function of the object power plant. Similarly, transforms electricity can be the function of a transformer substation. Functionalities can also be assigned characteristic properties. A case in point is that power lines which connect substations carry different amounts of power; these amounts can be entered as several property values in the property amount of power at the intermediate level. Once again, the instance level objects inherit the functionalities identified with their intermediate level parent objects, but differ in the amount of power they receive in real scenario instantiations.

4.2.2 *Intradomain interdependencies*

The intradomain functional relationships of each CI system are first specified at the intermediate level, mainly because the top-level objects of CI systems are usually too broad, and thus abstract, to begin with. For example, telephone offices are functionally interconnected with other telephone offices; this intradomain relationship is represented ontologically under the domain of land-based telephones using the functional features established for each intermediate level object.

Next, the process of representing intradomain interdependencies proceeds down to the instance level. Again, instance level CI objects inherit the functional features of their parent objects at the intermediate level. These inherited functional features are then utilized to represent functional relationships among the instance-level objects. For example, the function of produces electricity can be assigned at the intermediate level from the power station object to the substation objects. Inheriting the functional traits of its parent object power station, the instance of the function produces electricity, Meadow Nuclear Plant produces electricity, is assigned to an instance of the substation object, substation 35.

4.3 Specification of the system of CIs

The cross-domain interdependencies are the focus of this stage. These relationships are first represented through the functional features of intermediate level objects across individual CI systems. For example, the substation, an intermediate level object in power grid, functionally provides electricity to its counterpart objects at the intermediate levels in other CI systems, such as telephone offices, traffic lights, and natural gas regulator stations.

Next specified are the functional relationships of instance level objects across different CI systems. Based upon the inherited functionalities and service area analysis, these relationships can be identified and then explicitly represented in GenOM. For example, the instance level object of substation 35, functionally provides electricity to other cross-domain instance level objects in its service area, such as Elm St. telephone office and the traffic light at Main and 4th Streets.

4.4 Verification and validation

Verification refers to the process of assessing whether a model has been constructed as intended (Benbasat and Dhaliwal, 1989; Hodges and Dewar, 1992; Kleijnen, 1995; Williams and Sikora, 1991). In our case this relates to the issue of how faithful the ontologies in the knowledge base are in representing the knowledge about CI interdependencies. It is incorporated in the system definition and specification phases, and is executed through a combination of structured and unstructured interviews with domain experts, the GIS database, and open source documents.

Validation is the process of determining the degree to which a model and its associated data provide an accurate representation of the real world from the perspective of the intended users of the model (Defense Modeling and Simulation Office, 2004; Hodges and Dewar, 1992). In our study this is the issue as to how accurate the knowledge elicited from subject matter experts (SMEs) about CI interdependencies is in representing real-world CI interdependencies. The method adapted for the study is representational validation (Benbasat and Dhaliwal, 1989) or face validation (Hodges and Dewar, 1992; Williams and Sikora, 1991) that relies both on source SMEs—the human experts from whom the knowledge is originally elicited, and on nonsource SMEs—those who are not involved in the initial knowledge acquisition.

It should be noted that knowledge acquisition precedes and continues through the execution process of the methodology. In order to examine CI interdependencies, both declarative and procedural knowledge need to be solicited. The former includes, but is not limited to, hierarchical diagrams, the roles of components, and their functional relationships; the latter includes locations of specific objects, safety protocols, redundancies, and emergency procedures. The procedural knowledge is not usually disseminated publicly for security, proprietary, and business concerns of the mostly private corporations that operate the CI systems in the United States. In this study a methodology by Xiang et al (2005) is used, which acquires both declarative and procedural knowledge through a combination of interviews of SMEs, open source documents, and geographic data. This knowledge acquisition process permeates every step in the aforementioned methodology.

5 A case study

Both the ontology-based information system (as a loosely coupled system of GIS and GenOM) and the methodology were applied to a study in a municipality in the Southeastern United States. In the following descriptions, certain aspects of the figures have been omitted to preserve the security of the CI systems.

5.1 Definition of the systems

The four CI systems in this case study included the telecommunications network, natural gas network, road transportation network, and the electric power grid. These CI systems were represented as top-level object classes in GenOM. Each top-level object class was defined further by its subclass intermediate level objects. Some of these intermediate objects were decomposed further into other objects within them. For example, the top-level object telecommunications has intermediate land-based and wireless system objects, which are defined further into other intermediate objects, such as telephone poles, streetlights, and telephone digital loop carriers. Connecting apparatus such as telephone lines, pipe lines, and power lines were represented in both the GIS database and GenOM's knowledge base.

The locations of instance-level objects are identified with the database and DBMS capabilities in GIS. Based on information about these objects from documented sources and expert interviews, a geographic analysis of public datasets, including parcel data,

planimetric datasets, and digital orthophotos, helped us to locate instance-level objects. These include 16 central offices, 4 toll centers, 7 MTSOs, 53 substations, 5 power generation plants, 838 traffic control boxes, 10 regulators, 23 cell towers, 109 antennae structure registration towers, and 90 mobile communication towers. They were individually specified as instances of the intermediate-level objects in the study area.

5.2 Specification of CI systems

At this stage the properties and functions associated with CI system objects were first represented in the ontology-based information system on the basis of domain experts' knowledge. The intradomain interdependencies were next specified on the basis of the functional assignments and spatial proximities.

5.2.1 *Properties and functions*

Characteristic properties and functionalities of top and intermediate level objects were represented in GenOM through its Features capability. In order for users from differing domains of expertise to have a common understanding, a natural language, instead of technical languages in different domains, is used as much as possible to describe properties and functions. Table 1 provides an example of the intermediate-level objects and their properties and features. Note that, in table 1, a Boolean property of operating (that is, true/false) was assigned to all objects. This property is used to determine the consequences of an object's failure. In addition, an integer property unique ID (not listed in table 1) was attached to each object as a key identifier that relays to the same object in the GIS database. This common identification number serves as a bridge that permits

Table 1. Properties of critical infrastructure system objects and features. MTSO denotes mobile telephone switching office and ASR denotes antennae structure registration.

Property	Type of property	Values	Of object	Of feature
Battery backup	Boolean	true/false	central office toll center MTSO towers	
Duration in hours	integer	2, 8		provides back-up power
Generator available	Boolean	true/false	central office toll center MTSO ASR towers cell towers mobile towers	
Substation type	string	transmission distribution both transmitted and distributed hanger bus	substation	
Tandem	Boolean	true/false	central office	
Amount of power in line (kV)	integer	500/230/100		feeds power
Transformer type	string	step up step down auto	substation	

a retrieval of the objects and their pertinent information from both GenOM and GIS—a key to visualization and information exchange.

5.2.2 *Intradomain interdependencies*
In order to replicate the expert's knowledge of intradomain relationships, intermediate-level objects were designated as the benefactor (From object) or as a beneficiary (To object) when connected by functionality. For example, the function produces electricity is From a power station intermediate-level object To a substation intermediate-level object.

Once the instances of the intermediate-level objects were located in the GIS and represented in GenOM, the building of the knowledge base about the instance-level interdependencies began. The functionalities that connect intradomain instance-level objects were derived from the knowledge acquisition process and spatial proximity analysis. For example, the functional relationships of power plants to substations and those between substations in GenOM were derived from the spatial rendering of the power line easements and the substation objects in the GIS database.

5.3 Specification of the system of CIs
Cross-domain functional relationships were specified for the intermediate-level objects based upon the system experts' knowledge and the open source information about CI system structure. The same type of benefactor of (From) and beneficiary (To) relationship utilized in the intradomain specification was established between cross-domain intermediate level objects. One such example is the supervisory control and data acquisition system (SCADA). According to the system expert, a SCADA system remotely monitors and controls objects, such as substations and natural gas regulators, during normal operation. During a crisis or disruption, a SCADA system functions as an alarm connection to the utility control center, and relies on communication technologies to transmit the information (Branscomb, 2004; Williams, 2003). The function SCADA was therefore used to define the functional relationship between a substation or a natural gas regulator and a telephone switch office. A compilation of the functional relationships is provided in table 2.

Inheriting all the cross-domain functional interdependencies from the parent objects at the intermediate level, interdependencies across the component CI systems in a system of CIs were further identified through a service-area analysis. Each instance-level object has a service area in which it is functionally connected to objects in other CI systems. As the information about service-area footprints was unavailable, we, upon recommendations of system experts, utilized Thiessen polygons to represent *in proxy* the instance-level service areas. Thiessen polygons do not permit gaps among CI object service areas, nor do they allow overlaps. This makes them advantageous over the use of circular buffers. The urban area that we represented did not have any physical barriers such as a river, mountain, or ocean that would create difficulties in the spatial proximity analysis.

5.4 Verification and validation
The verification of the ontological representations of CI interdependencies in the ontology-based information system aimed to check whether they were faithful renderings of the elicited knowledge. This was accomplished through a series of consultations with source SMEs—the human experts from whom the knowledge was originally elicited. The validation—that is, the check on whether the ontological renderings of CI interdependencies are accurate representations of the reality—was conducted through a panel of CI System SMEs and the emergency management experts, including emergency response managers and business continuity planners. The panel was presented with several CI disruption scenarios, and was asked to assess the plausibility of

Table 2. Functions and their assignments to objects in GenOM. MTSO denotes mobile telephone switching office; SCADA denotes the supervisory control and data acquisition system; and ASR denotes antennae structure registration.

Feature	'From' objects	Feature relationship	'to' objects
Provide gas	regulators	provides gas	central offices generator
Has a generator	generator	provides emergency power	central offices MTSO ASR towers toll centers
Processes call through	central offices	processes calls	central offices wireless towers
Provides landline access	central offices	provides landline access	MTSO
Feeds power	substation power generation plants	delivers power to	substation
SCADA	central offices	alarm connection	regulators substation
Provides access to long distance network	central offices	access to long distance	toll centers
Provides backup power	battery	provides backup power	central offices MTSO toll centers cell towers mobile communication towers ASR towers
Provides power to	substation	provides power to	central offices MTSO toll centers cell towers mobile communication towers ASR towers regulators traffic control boxes

these scenarios. Because these scenarios were composed upon the CI interdependencies in the system of CIs, as represented in the ontological renderings, a high plausibility rating on the scenarios serves as a good indicator of the accuracy of the ontological representations. For instance, one scenario titled 'substation failures' was composed by the inference engine in GenOM, based on the functional dependencies between a substation and the CI objects it supports with the premise that "IF Eastside substation failed, THEN the objects that have a functional relationship to it would lose power." The consequences of the substation failure shown in the scenario were that Main Street telephone switch office, the traffic lights along Route 10, and the water pump on High Avenue were all without power. A high plausibility rating of this scenario from the panel indicated the validity of the causal relationships, represented by the ontological renderings in the ontology-based information system, among these CI objects.

5.5 Visualization of the CI interdependencies from quadruple vantage points

At the beginning of the paper we stated that the goal of our research is to develop an ontology-based information system that facilitates CIP professionals' learning of the behaviors of the system of CIs through a quadruple perspective. In this subsection we demonstrate that with its visualization capabilities operating on the ontological representation of CI interdependencies, the ontology-based information system offers the users an opportunity to gain insights into the interwoven nature of CI objects from all of the four vantage points in the quadruple perspective matrix (figure 1, section 2). More specifically, the diagrams in GenOM can show both intradomain and cross-domain interdependencies across all the three levels of object abstraction. The maps in GIS illustrate the spatial proximities among instance level objects. The consolidated user interface allows users to query and visualize the CI interdependencies that fall into any one of the quadrants in figure 1.

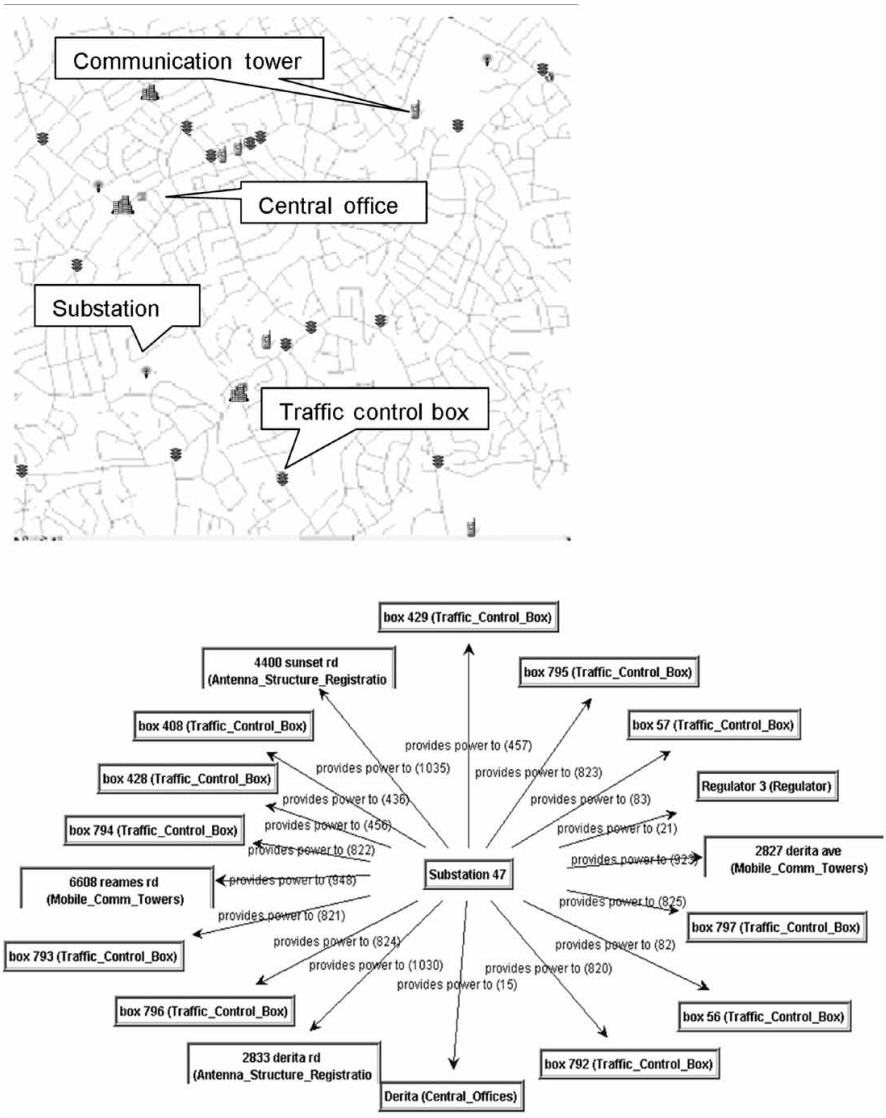

Figure 6. An example of the quadrant A critical infrastructure interdependencies.

5.5.1 *Visualization of the quadrant A CI interdependencies*
A CIP professional may inquire the CI objects that functionally depend upon one another directly and demonstrate a high degree of spatial proximity by asking "what are the CI objects within a substation's service area that have direct functional relationship with the substation?" In responding to this inquiry, GenOM in the ontology-based information system can promptly search through its ontologies and come up with a diagram that shows the instance-level objects that have either intradomain or cross-domain functional dependencies with the substation (figure 6). Through the integer property unique ID that connects the same objects in both GenOM and the GIS database, the GIS can readily identify the geographic locations of these objects and produce a map (figure 6 shows only a portion of the service area owing to page limit). On the map the telephone symbol represents a landline telecommunication switch office (that is, a central office), the wireless phone symbols indicate the locations of wireless communication towers, the symbol of a traffic light denotes the locations of a traffic control box for the intersection lights, and the lines are streets.

5.5.2 *Visualization of the quadrant B CI interdependencies*
Similarly, the system can readily respond to inquiries about CI objects that functionally depend on one another indirectly but demonstrate a high degree of spatial proximity. For example, in figure 7, a disrupted power substation that directly affects a nearby traffic control box, indirectly causes a dangerous situation on the roads at the intersection.

5.5.3 *Visualization of the quadrant C CI interdependencies*
Illustrated in figure 8 is an example of the system's response to an inquiry about the CI objects in quadrant C—objects that functionally depend on one another indirectly and demonstrate a low degree of spatial proximity. A remote telephone central office is located outside a power station's service area, and is thus indirectly connected to the power station. The low level of proximity and the functional indirectness between the two cross-domain CI objects are visualized in a GIS map and GenOM diagram, respectively. It should be noted that the retrieval of the telephone central office was made possible through the cross-domain functional dependency with the power station which the central office object inherited from its parent object telephone central office at the intermediate level.

5.5.4 *Visualization of the quadrant D CI interdependencies*
Inquiries about quadrant D interdependencies can also be well supported by the system. As the CI objects in quadrant D are essentially the networked objects within each component CI system, the retrieval of these objects with intradomain interdependencies can take place in two ways. The first way starts with a GIS data layer of the networked objects in a CI system (for example, all the substations, transmission lines, transformers, and the power generation station in a power grid), and involves the retrieval of all the counterpart objects in GenOM along with their functional dependencies. The second way of retrieval is to use GenOM's inference engine to include only the same instance-level objects with direct functional connections, and then to find their counterpart objects in the GIS database along with their geographic locations. Whichever way a CIP planners takes, he or she should get the same result. An example is provided in figure 9, where a telephone switch network (triangle symbols) is presented geographically in GIS with the network connectivity lines (darker lines), as well as diagrammatically in GenOM.

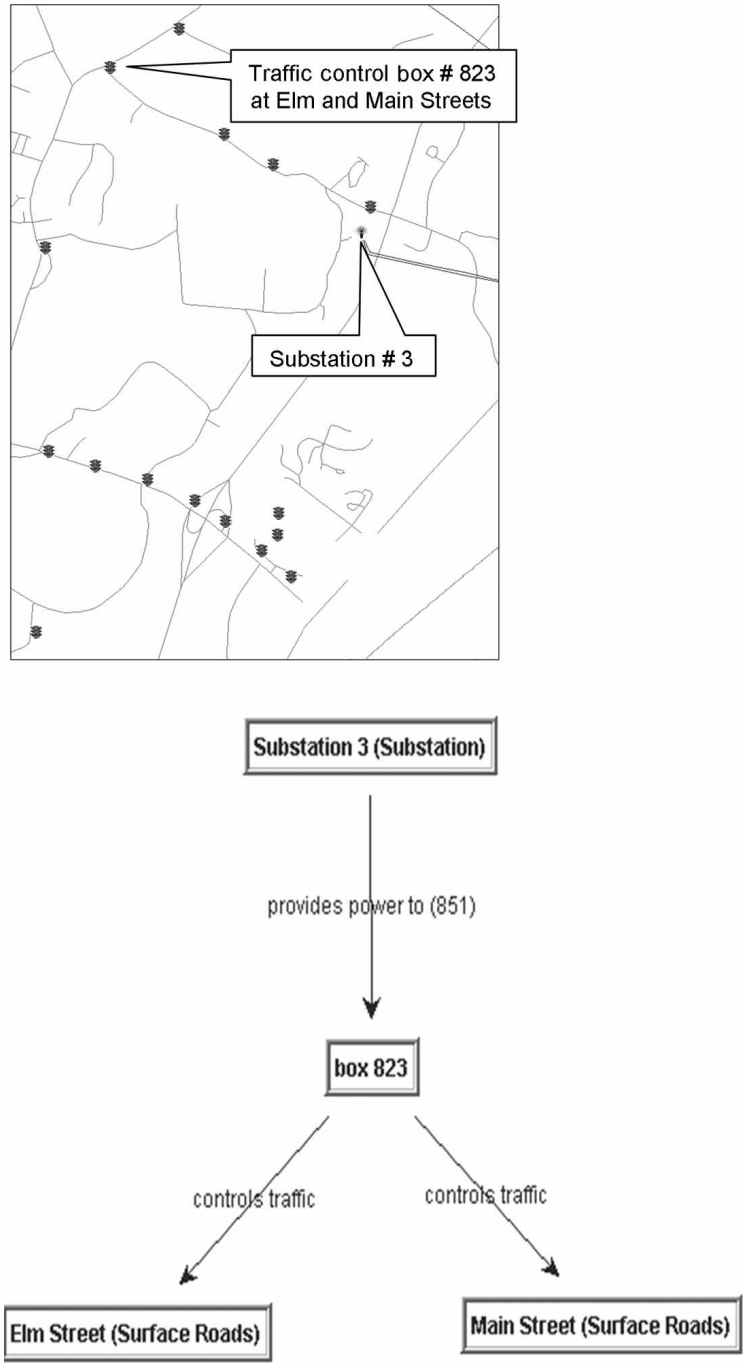

Figure 7. An example of the quadrant B critical infrastructure interdependencies.

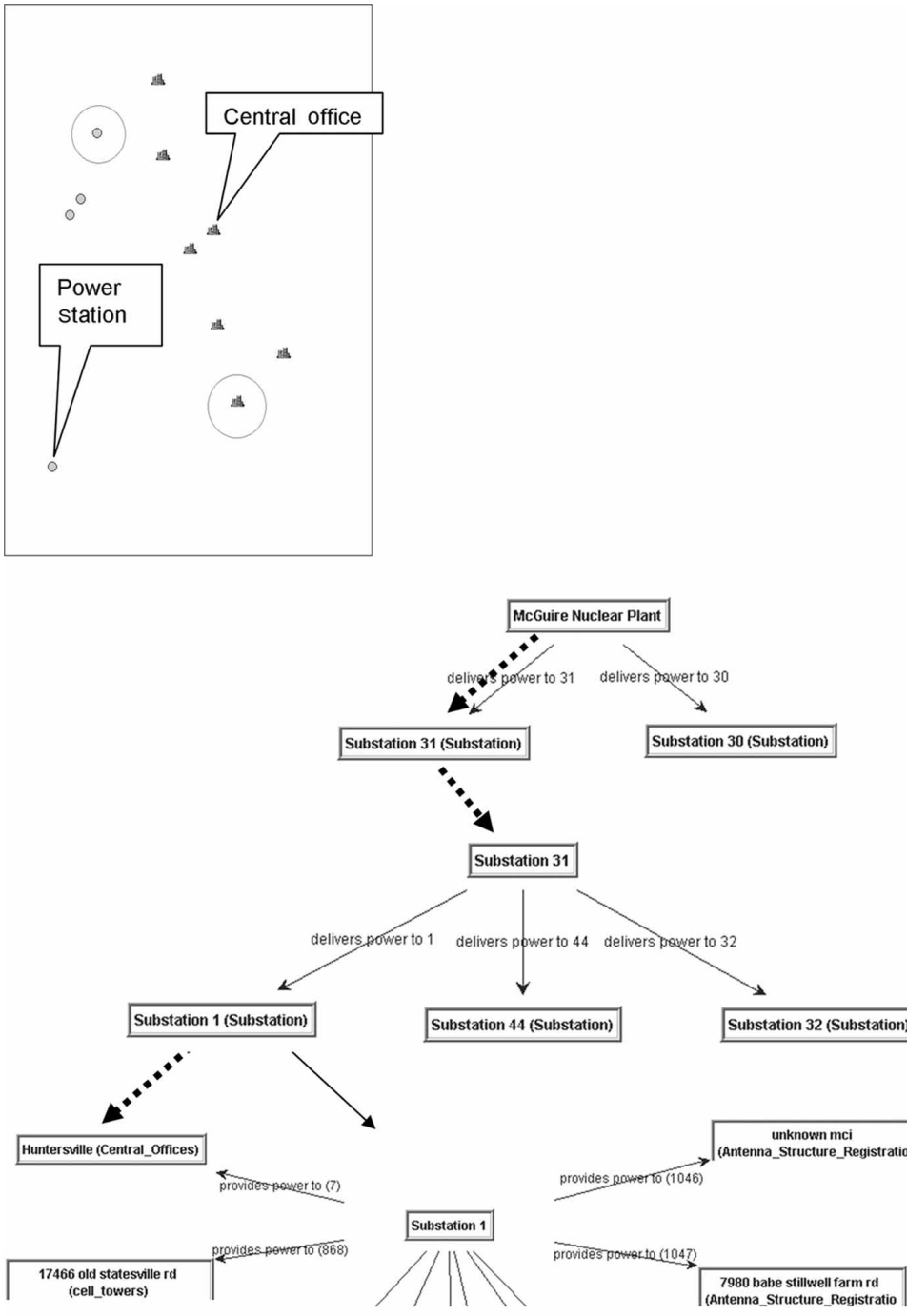

Figure 8. An example of the quadrant C critical infrastructure interdependencies.

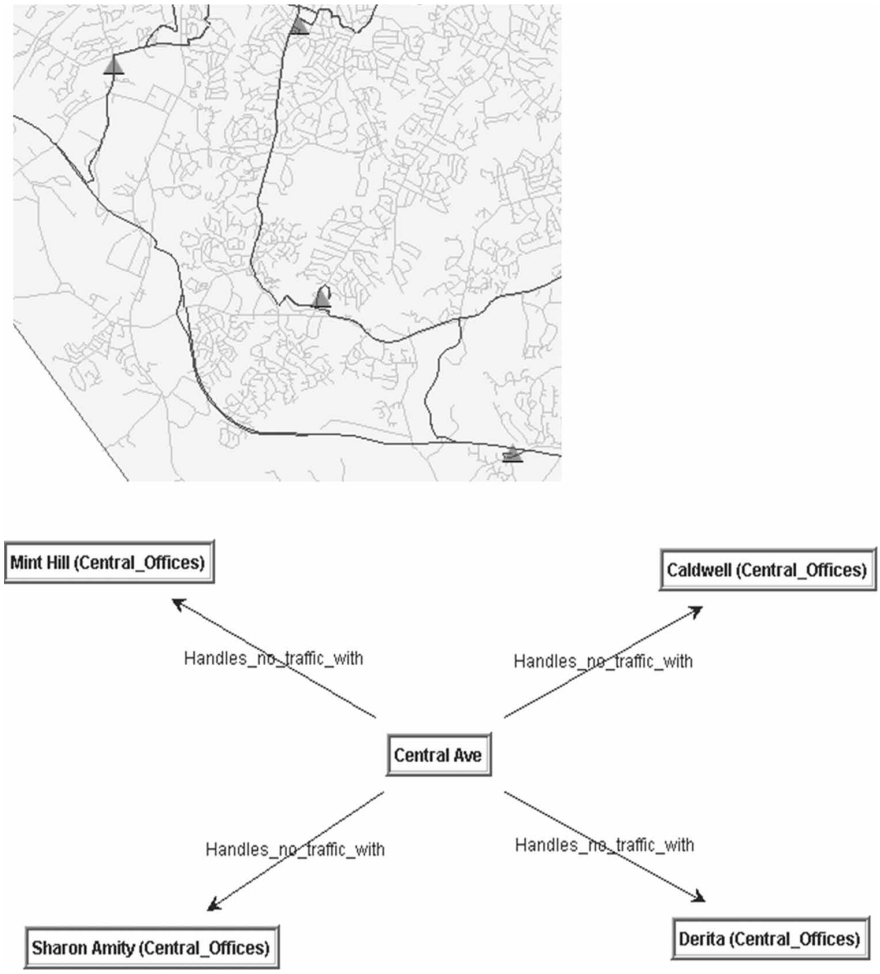

Figure 9. An example of the quadrant D critical infrastructure interdependencies.

6 Conclusions

In this paper we presented an ontology-based information system that facilitates CIP professionals' learning of the behaviors of the system of CIs. Through a coupling of GenOM and GIS, not only does it replicate intradomain SMEs' knowledge, but it also provides a way to understand the behaviors of cross-domain CI interdependencies.

Future research can be conducted along two directions. Firstly, the ontology-based information system and its knowledge representation methodology should be further tested in areas with different characteristics. Not only will this stream of research expand the applicability of the system and the knowledge representation methodology, but it will also cultivate the evolution of a formal approach to interdependency identification and representation. Secondly, a tightly coupled system of GenOM and GIS will be investigated that can create an interoperable environment that would be more effective than the loosely coupled system in knowledge representation, visualization, and scenario composition.

Acknowledgements. The authors are grateful to the following individuals at the University of North Carolina at Charlotte for their contributions to the project: Bill Tolone, Robin Gandhi, Katie Templeton, Gustavo Borel Menezes, Stuart Phelps, Qinhong Tang, Ken McWilliams, Jocelyn Young, Paul Smith, Amy Weeks, Huili Hao, and Andrew Schumpert. Our gratitude also extends to the SMEs.

References

Benbasat I, Dhaliwal S, 1989, "A framework for the validation of knowledge acquisition" *Knowledge Acquisition* **1** 215 – 233

Berenbach B, 2004, "The evaluation of large, complex UML analysis and design models", in *Proceedings of the 26th International Conference on Software Engineering* ICSE-2004, 23 – 28 May (IEEE Press, Hoboken, NJ) pp 232 – 241

Bolz F, Dudonis K, Schulz D, 2002 *The Counterterrorism Handbook: Tactics, Procedures, and Techniques* 2nd edition (CRC Press, Boca Raton, FL)

Bowler T D, 1981 *General Systems Thinking: Its Scope and Applicability* (North Holland Press, New York)

Branscomb L, 2004, "Protecting Civil Society from Terrorism: The Search for a Sustainable Strategy" *Technology in Society* **26** 271 – 285

Chaudhri V K, Farquhar A, Fikes R, Karp P D, Rice J P, 1998, "OKBC: a programmatic foundation for knowledge base interoperability", in *Proceedings of the 15th National Conference on Artificial Intelligence* 26 – 30 July, Madison WI (AAAI Press, Menlo Park, CA) pp 600 – 607

Defense Modeling and Simulation Office, 2004, "Key concepts of VV&A", US Department of Defense, Washington, DC, http://vva.dmso.mil

Egenhofer M, Frank A, 1992, "Object-oriented modeling for GIS" *URISA Journal* **4** 3 – 19

Evermann J, Wand Y, 2005, "Ontology based object-oriented domain modeling: fundamental concepts" *Requirements Engineering Journal* (Springer, Berlin)

Fonseca F, Egenhofer M, Agouris P, Câmara C, 2002, "Using ontologies for integrated geographic information systems" *Transactions in GIS* **6** 231 – 257

Frank A, 1997, "Spatial ontology", in *Spatial and Temporal Reasoning* Ed. O Stock (Kluwer Academic, Dordrecht)

Guarino N, 1998, "Formal ontology and information systems", in *Formal Ontology in Information Systems* Ed. N Guarino (IOS Press, Amsterdam) pp 3 – 15

Hodges J, Dewar J, 1992, "Is it you or your model talking: a framework for model validation", Rand report R-4114-AF/A/OSD, Rand Corporation, PO Box 2138, Santa Monica, CA 90407

Jackson M, 1997, "The meaning of requirements" *Annals of Software Engineering* **3** 5 – 21

Jackson M, Zave P, 1993, "Domain descriptions", in *Proceedings of the 1st International Conference on Requirements Engineering* (IEEE Press, Hoboken, NJ) pp 56 – 64

Kleijnen J, 1995, "Verification and validation of simulation models" *European Journal of Operational Research* **82** 145 – 162

Kogut P, Cranefield S, Hart L, Dutra M, Baclawski K, Kokar M, Smith J, 2002, "UML for ontology development" *The Knowledge Engineering Review* **17** 61 – 64

Lee S-W, Yavagal D, 2004 *GenOM: Generic Object Model User Guide* Knowledge Intensive Software Engineering Research Group (NISE), Department of Software and Information Technology, University of North Carolina at Charlotte; available from corresponding author of this paper

Lee S-W, Ahn G-J, Gandhi R A, Yavagal D, 2004, "An information assurance engineering methodology for critical infrastructure protection: the DITSCAP automation study", technical report, Software and Information Systems Department, UNC Charlotte

McGuinness D, van Harmelen F (Eds), 2004, "OWL web ontology language overview: W3C recommendation, 10th February 2004", http://www.w3.org/TR/owl-features/

Nunes J, 1991 *Geographic Space as a Set of Geographic Entities* in *Cognitive and Linguistic Aspects of Geographic Space* Eds D Mark, A Frank (Kluwer, Boston, MA) 9 – 33

Offen R, 2002, "Domain understanding is the key to successful system development" *Requirements Engineering* **7** 172 – 175

Rinaldi S, Peerenboom J, Kelly T, 2001, "Identifying, understanding, and analyzing critical infrastructure interdependencies" *IEEE Control Systems Magazine* December, pp 11 – 25

Sommerville I, 2004 *Software Engineering* 7th edition (Addison-Wesley, Cambridge, MA)

Stevens R, Goble C A, Bechhofer S, 2000, "Ontology-based knowledge representation for bioinformatics" *Briefings in Bioinformatics* **1** 398 – 414

Terner M, Sutton R, Hebert B, Bailey J, Gilbert H, Jacqz C, 2004, "Protecting critical infrastructure" *GeoIntelligence* 1 March, http://www.geointelmag.com/geointelligence/article/articleDetail.jsp?id=90043

Turban E, Aronson J E, 2001 *Decision Support Systems and Intelligent Systems* (Prentice-Hall, Englewood Cliffs, NJ)

US – Canada Power System Outage Task Force, 2004, "Final report on the August 2003 blackout: causes and recommendations", https://reports.energy.gov/B-F-Web-Part1.pdf

US Department of Homeland Security, 2003 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* Department of Homeland Security, The White House, Washington, DC

Vemuri V, 1978 *Modeling of Complex Systems* (Academic Press, New York)

von Bertalanffy L, 1973 *General System Theory: Foundations, Development, and Applications* (Braziller, New York)

Williams M K, Sikora J, 1991, "SIMVAL minisymposium—a report" *Phalanx, The Bulletin of Military Operations Research* **24** 1 – 6

Williams R, 2003, "SCADA security: turning control and automation systems into hard targets" *Utility Automation* **8** http://uaelp.pennet.com/Articles/Article_Display.cfm?Article_ID=167183&pc=gls

Wolthusen S D, 2004, "Modeling critical infrastructure requirements", in *Proceedings of the 5th Annual IEEE SMC Information Assurance Workshop* (IEEE Press, Hoboken, NJ) pp 101 – 108

Xiang W-N, Tolone W J, Raja A, Wilson D, Tang Q, McWilliams K, McNally R, 2005, "Mining critical infrastructure information from municipality data sets: a knowledge-driven approach and its applications", a paper presented at 2005 Auto-Carto Conference, Las Vegas, NV, March; copy available from author

Zeleznikow J, Stranieri A, 2001, "An ontology for the construction of a legal decision support system", paper presented at the Second International Workshop on Legal Ontologies, 13 December; available from J Zeleznikow, Centre for Forensic Statistics and Legal Reasoning, Faculty of Law, University of Edinburgh

Appendix

A glossary

Antennae structure registration and **mobile communication towers**. Since only twenty-three cell towers were listed in the Federal Communications Commission database, other databases were searched for cellular sites. In our study area of over 500 square miles, including an urban center with an excess of one million people during a workday, twenty-three towers seemed extremely low. System expert knowledge revealed that much cellular equipment is located on other types of towers such as radio and television towers, public communication towers, as well as alternative structures with sufficient height, such as church steeples, buildings, and water towers. These databases contained towers with a variety of ownership; many were telecommunications companies.

Battery—an emergency power source in case of normal power disruption.

Cell towers are the means by which wireless communications can be transmitted.

Central offices are the local public service telephone network (PSTN) central switching offices. They process calls for an exchange(s) (the first three digits of a local number), and route the call to its various potential destinations.

Generator—an alternative power source in case of a normal power disruption. Although a generator can be powered by various means, system expert knowledge indicated that a vast majority of large generators for institutions are fueled by natural gas where available. It would also be acceptable to place this object instead as a subclass to the top-level object **power**.

Mobile communication towers—see **antennae structure registration**.

MTSO is an abbreviation for mobile telephone switching office. This is the equivalent of a PSTN central office, processing wireless calls from towers and routing them to various potential destinations.

Regulators are valves that regulate the pressure from the main natural gas pipeline to the local distribution system pipelines.

Power generation plant—produces electricity via fossil fuels, hydrologic, geothermal, or nuclear technologies.

Substations increase or decrease electrical power from its inputted sources to distribution means. It is a subclass of the power generation plants, as it does not produce power, it modifies it.

Toll centers are the long-distance network call-switching centers that process calls from local central offices to other toll centers outside of the local calling area to be routed to their local central offices.

Traffic control boxes are the devices that operate intersection traffic lights.