**An Ontology-Driven Approach to Representing and Visualizing Critical Infrastructure Interdependencies**

Robert K.McNally, Seok-Won Lee, Deepak Yavagal, Wei-Ning Xiang

Department of Geography and Earth Sciences
(704)687-4247
(704)687-3182 (fax)

rkmcnall@uncc.edu
wxiang@uncc.edu

Department of Software and Information Systems
Phone: 704-687-3862
Fax: 704-687-4893
seoklee@uncc.edu
dyavagal@uncc.edu

University of North Carolina at Charlotte
9201 University City Boulevard
Charlotte, NC 28223

**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 is about the interactions within a CI system, and the other the interdependencies between systems of CI. In this paper, we present an ontology-driven method that facilitates the learning of the interdependencies among systems of critical infrastructure. Employing an integrated system of Geographic Information Science and a generic object-modeling tool, it represents and visualizes the two pieces of knowledge both geographically and diagrammatically.

## 1. INTRODUCTION

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 and safety, and way of life in a community or society (PPD63 1998). In recent years, unfortunately, critical infrastructure systems have become a symbolic target, as well as the mass casualty opportunity, for terrorist attack. (Bolz *et al* 2002) Because of this dual identity of critical infrastructure (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, National Strategy for Physical Protection of CI and Key Assets 2003).

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 critical infrastructure system (CI system, thereafter), and a system of critical infrastructures (a system of CIs, thereafter). A CI system is an assemblage of functional objects that provides 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, transmission and distribution lines. On the other hand, a CI system is also a part of an even larger system—a system of CIs, which offers a range of public good 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). The utility of traffic control in a municipality, for instance, is provided by a system of CIs—power grid, telecommunication network, and traffic control boxes. The proper functioning of the three CI system components is a necessary condition for the normal operation of the traffic control system. This knowledge alone, however, 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 serge protections, for example) are all "emergent features" that do not exit when the three CI system components are separate (For a detailed account of emergent features and other concepts in the general systems theory, see Bertalanffy 1973).

Therefore, there exist two types of knowledge within the critical infrastructure domain. The first is about the behaviors of a CI system when it is (or assumed to be) a stand-alone system, and the second about the behavior of a system of CIs, which is grounded on the interdependencies among its component CI systems. 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 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-driven method that facilitates CIP professionals' learning of the behaviors of the system of CIs . Employing an integrated system of GIS and a generic object-modeling tool (GenOM), it represents and visualizes the two types of knowledge both geographically and diagrammatically. Furthermore, the inference engine embedded in GenOM allows CIP professionals to explore various scenarios of system failure and their spatial ramifications with "what-if" queries.

The remainder of the paper is organized as follows. Section 2 discusses the quadruple viewpoint of interdependencies within a system of CIs. Section 3 explores the need for an integrated information system for representing CI interdependencies. Section 4 presents a methodology for representing the knowledge, especially the second type of knowledge. Section 5 illustrates the outcomes of the methodology through a case study in the Southeastern United States. Finally, Section 6 draws conclusions.

## 2. A QUADRUPLE VIEW OF CI INTERDEPENDENCIES

The interdependencies among the component CI systems (CI interdependencies, hereafter) within a system of CIs can be viewed from many different vantage points (Rinaldi, *et al* 2001). Among the most relevant and helpful to CIP planning and drills are functional dependency and spatial correlation.

### 2.1. Functional Dependencies

A functional dependency is when one object relies on another object in order to operate properly in any way. There may be functional dependencies that are one-way in their relationship. For example, roads rely on traffic lights to control the flow of traffic at intersections. The traffic light does not rely on the road for its functionality. Other functional dependencies are bi-directional such as telephone offices relying on commercial power supply and the power company using telecommunications for daily operations as well as monitoring equipment via remote telemetry. Many times in a crisis, one-way functional dependencies become bi-directional. An example would be that a traffic light relies on power supply to operate normally; conversely the power supply does not normally rely on traffic lights to operate. When power disruption occurs however, the repair crews of the power company are delayed by the malfunctioned traffic lights.

Some dependencies are directly related, such as object *A* relies on Object *B*, others are indirectly related in that the have one or more mediating objects before the dependency is realized (object

*C* relies on object *A* through object *B*). Table 1 shows examples of functional dependencies between some CI objects in a system of CIs under our investigation (Xiang *et al*, 2005). This is a system of 4 CIs—power grid, natural gas supplies, transportation networks, and telecommunication networks.

Table 1: Functional dependencies between CI objects

**Functional Relationships**

**Functional Dependencies**
1=Direct; 0=Indirect; Blank=None

| | PowerPlant | Substation | HighPowerLine | Tele.XchgeCtr. | Tele.Tandem | mtso | TollCenter | ASRtower | CellTower | MobileComm | GasPipeline | Regulator | Roads | TrafficLight |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Power* | | | | | | | | | | | | | | |
| Power plants | 0 | | | | | | | | | | | | | |
| Substations | 0 | 0 | | | | | | | | | | | | |
| High power lines | 1 | 1 | 1 | | | | | | | | | | | |
| *Telecommunications* | | | | | | | | | | | | | | |
| Tele.XchgeCtr. | 0 | 1 | 0 | 1 | | | | | | | | | | |
| Tele. Tandem | 0 | 1 | 0 | 1 | 0 | | | | | | | | | |
| MTSO | 0 | 1 | 0 | 1 | 1 | 1 | | | | | | | | |
| Long Dist. Toll Ctr. | 0 | 1 | 0 | 1 | 1 | 0 | 0 | | | | | | | |
| ASR tower | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | | | | | | |
| Cell tower | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | | | | | |
| Mobile Comm Tower | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | | | | |
| *Natural Gas* | | | | | | | | | | | | | | |
| Main Gas Pipeline | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | 1 | | | |
| Nat. Gas Regulator | 0 | 1 | 0 | 1 | 0 | 0 | 0 | | | | 1 | 0 | | |
| *Transportation* | | | | | | | | | | | | | | |
| Roadways | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | |
| Traffic Control Box | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

## 2.2. Spatial Correlation

The other type of relationship that CI objects within a system of CIs possess pertains to their spatial correlation. As physical objects, they are spatially tangible. The spatial correlation of these objects usually reflects the technological requirements to deliver the service and the functional dependencies that exist between CI objects. Some objects need to be proximal to another object for some functional reason, in other cases; objects are more distant since they are part of a network. Objects that require commercial power may receive that power from a nearby substation (Highly Correlated); the substations themselves are disbursed across the region to provide the service (Low Correlation). Still, there are cases where proximity is either determined by such land use factors as land availability, zoning, and NIMBY (not-in-my-back-yard) mentality, or defined by such physical barriers as rivers, lakes, and terrains. Therefore, basing spatial correlation upon proximity alone can be misleading. Table 2 shows examples of the spatial correlation of some CI objects in the same system of CIs as Table 1.

Table 2: Spatial correlation between CI objects

| Spatial Correlation<br>1=High, 0=Low, Blank=None | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PowerPlant | Substation | HighPowerLine | Tele.Xchge Ctr | Tele.Tandem | mtso | TollCenter | ASRtower | CellTower | MobileComm | GasPipeline | Regulator | Roads | TrafficLight |
| *Power* | | | | | | | | | | | | | | |
| Power plants | 1 | | | | | | | | | | | | | |
| Substations | 0 | 0 | | | | | | | | | | | | |
| High power lines | 0 | 1 | 0 | | | | | | | | | | | |
| *Telecommunications* | | | | | | | | | | | | | | |
| Tele.Xchge.Ctr. | 0 | 1 | 0 | 0 | | | | | | | | | | |
| Tele. Tandem | 0 | 1 | 0 | 0 | 0 | | | | | | | | | |
| MTSO | 0 | 1 | 0 | 1 | 1 | 0 | | | | | | | | |
| Long Dist. Toll Ctr. | 0 | 1 | 0 | 1 | 1 | 1 | 0 | | | | | | | |
| ASR tower | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | |
| Cell tower | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | | |
| Mobile comm towers | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| *Natural Gas* | | | | | | | | | | | | | | |
| Main Gas Pipeline | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | | | |
| Nat. Gas Regulator | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | | |
| *Transportation* | | | | | | | | | | | | | | |
| Roadways | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| Traffic Control Box | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

## 2.3. A Quadruple View

By combining functional dependency with spatial correlations, additional insights emerge as we examine the interdependencies among the CI objects within a system of CIs from a quadruple vantage point (Table 3). Quadrant A is a collection of objects that have a direct functional dependency with another object with a high spatial correlation to it. Many times this is a result of being the most proximal object that another object can rely on for a functional purpose. Sometimes this is a result of collocation of assets such as when a long distance toll center and a local telephone central office are within the same building due to dependant functionality. The MTSO and the long distance toll centers, for another example, are proximal to a local tandem central office that is necessary for call completions. This quadrant represents the most elemental viewpoint in CI protection planning. The direct functionality can make it more obvious to protect these assets, to compose scenarios and the proximity makes emergency response drills logistically easier to accomplish.

Quadrant B represents those objects that are proximal to each other but have an indirect functional dependency. A main pipeline and a high power line may share an easement that provides the right-of-way for these objects to functionally deliver their services. Although they are not directly related functionally, they are proximal. In these cases, the proximity is not a reflection of the functionality, but the spatial correlation is of the other causes listed previously. These interdependencies are not recognized immediately for protection or scenario composition due to their indirect functionality. Due to this oversight, emergency drills may neglect this aspect of CI interdependencies. Ultimately, their proximity makes them highly vulnerable to multiple CI system disruptions that can cascade into Quadrant A interdependencies.

Table 3: A quadruple view of CI Interdependencies

| Critical Infrastructure Interdependancy Matrix | | | |
|---|---|---|---|
| | | **Functional Dependencies** | |
| | | Direct | Indirect |
| SPATIAL CORRELATION | High | Substations and regulators | Gas pipelines and high power lines |
| | | Roads and Traffic Control Boxes | MTSO's and Toll Centers |
| | | Tandem Offices and Toll Centers | power plants and power plants |
| | | Central Offices and MTSO's | Roads and power plants |
| | | Central offices and traffic control boxes | Roads and Substations |
| | | Substations and high power lines | Roads and Central Offices |
| | | Regulators and Pipelines | Roads and Towers |
| | | Substations and Traffic control boxes | Roads and Regulators |
| | | Substations and Central offices | Roads and MTSO |
| | | Substations and Towers | Roads and Toll Centers |
| | | Substations and Toll Centers | |
| | | Substations and MTSO | |
| | | Central Office and Regulators | |
| | | MTSO to MTSO | |
| | | A | B |
| | Low | Substation to substation | Power plant and central office |
| | | Central office to Central office | Power plant and MTSO |
| | | Towers and MTSO | Power plant and toll centers |
| | | Powerlines | Power plant and towers |
| | | Pipelines | Power plant and regulators |
| | | Power plants and substations | Central offices and towers |
| | | | Central offices and towers |
| | | | Tandem-type Central Offices |
| | | | Roads and Pipelines |
| | | | Roads and High Power Lines |
| | | D | C |

Quadrant C objects reflect the lesser degree of functional and spatial relationships between objects. These interdependencies are the result of several sequences of more direct relationships within the systems of CI. The low spatial correlation in these cases are due to the lower level of functional dependency as well as the lack of other correlating spatial factors as well, therefore proximity or distance have little meaning. For example, although distribution power and gas service pipelines are highly correlated spatially to the road network, the main pipeline and the high power lines are not. They have low spatial correlation to the roads though used only for access to right-of-way entry points for inspection and repair. This is the most challenging quadrant for scenario composition because of the remote functional and spatial relationships. These extended interdependencies, along with quadrant B, demonstrate the necessity to understand CI interdependency knowledge, for what sequences of events would need to occur to have an effect on both of these objects?

Interdependencies in Quadrant D are essentially the network of objects within each CI system. The good news is that each CI system provider has a vested interest in providing for the continued operations of the network. Hence, contingency planning, crisis response, and monitoring devices are in place to ensure that functionality. The bad news is that a narrow focus due to the segmented nature of CI system service delivery can ignore the interdependencies of other quadrants. In these cases, the nodes are directly functional objects that are disbursed across an area. A method to assess the criticality of the nodes is needed to determine which one warrants increased security measures based upon their interdependencies to other CI system objects.  This is important because over protection of objects may result in the under protection of a more critical object due to the fact of finite security resources.

It is evident that the above quadruple view of CI interdependencies is more advantageous than the two 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. In other words, these are inextricable aspects of the same phenomena. Although present and effective in varying degrees, any examination of CI interdependencies must include all four vantage points.  For example, a telephone office does not operate in a vacuum.  It has functional relationships within its own system as well as with objects of other CI systems.  Its location may be influenced by its functionality and its dependencies to other objects or other spatial factors involved in the environment to which it exists.

What is needed then is an information system that allows CIP professionals to not only learn the behaviors of a system of CIs but also plan and design drills from this elevated vantage point. More specifically, such a system should be capable of representing both aspects of CI interdependencies—functional dependencies and spatial correlation seamlessly and effectively so that the knowledge of CI interdependencies becomes readily available when undertaking such tasks as vulnerability assessment, scenario composition, and emergency response.

## 3. THE NEED FOR AN INTEGRATED SYSTEM

Unfortunately no single system currently available is suitable for fulfilling this request. In the following subsections, through an examination of the complementary capabilities of two promising information systems–Geographic Information System (GIS) and an ontology-based object model system, we call for an integrated system that combines the strengths of the individual systems while mitigating the other's weaknesses.

### 3.1. GIS

As a spatial data handling system, the strengths of GIS lie in its ability to handle large quantity of geographic information, and in the ability to visually represent and analyze objects spatially (The Geographic Information Center of the National Academies, 2005). Underlying a GIS is a layer-based and topology-driven approach. A GIS organizes geographic objects according to the topological principles, and stores them in different data layers. These transparent visual layers can be overlaid atop others to represent a geographic space. In addition, GIS is equipped with a set of tools for analyzing and modeling spatial data. Through its buffering function, for example, a GIS can delineate the geographic scope of impact caused by the failure of a CI object. The proximity analysis tools in GIS, for another example, measure the distance between objects to identify spatially correlated CI objects, such as those in quadrant A and B in Table 3; its network utility tool can represent each CI system networks separately (quadrant C in Table 3).

Although this layer-based and topology-driven approach makes GIS a powerful system that supports a wide range of spatial analysis, modeling, and visualization, it has been proven ineffective when dealing with applications of data with a complex structure because it does not match the natural concepts one has about spatial data. People are then forced to transform their mental models into a restrictive set of non-spatial concepts (Edgenhofer and Frank 1992). More specifically, the limitation of GIS in explicitly representing functional dependencies lies in the division of objects into layers. By separating the information into representative layers, the functional interdependencies have been severed and need to be reconstructed in the database layers (Figure 5), which cannot be done without significant manipulation or even re-engineering of the databases. This can lead to over specification and inconsistencies (Frank 1997). Furthermore, the relational databases in GIS connect geographic objects on one layer with their attributes in tables. Although these tables can be referenced across different layers, the resulting representations usually explicitly convey spatial connectivity on the one hand, but only imply functionality, on the other. In order to effectively present CI interdependencies, these barriers must be overcome while maintaining the spatial representation and analysis capability that a GIS possesses.

### 3.3. Ontology-Based Object Model Systems

Ontology is typically defined as the explicit formal specification of the terms in a domain and the relations among them (Gruber, 1993). The term "ontology" in philosophy relates to the study of being, but it has been applied to data management as a method to organize data and/or knowledge. The difference between ontology and a database is that ontology represents a view of the world, while a database schema represents only the information within it.

Underlying an ontology-based object model system, such as Protégé (2000) and GenOM (Lee and Yavagal, 2004), is the principle of networked ontological hierarchies (Lee and Yavagal, 2004). More specifically, 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 even higher order. Because it fundamentally conforms to the general systems theory (Bertalanffy 1973), this approach to knowledge representation is more advantageous than its layer-based counterpart in GIS. First of all, an ontology-based model system 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. For instance, GenOM (Generic Object Model, the system used in our project, see Lee and Yavagal, 2004) organizes information using object-oriented technologies and it organizes knowledge, both declarative and procedural, into a hierarchical structure of object classes. These classes of objects use the concept of *inheritance*; an object can "inherit" characteristics or properties of another higher-level object (Turban and Aronson 2001). This way of knowledge abstraction and structuring is more natural cognitively. Therefore, it is more effective to examine the complex relationships among objects, such as CI interdependencies, than the layer-based relational DBMS equipped in GIS. This is especially effective with regard to objects with pertinent operations (Egdenhofer and Frank, 1992). Secondly, a system of networked hierarchically organized ontologies can express dynamic relationships such as temporal events, whereas a DBMS can only utilize a property or attribute to modify an object. This knowledge can then be represented visually in a semantic network graphic. Thirdly, an inference engine, a standard feature of an ontology-based model system, allows the formulation of production rules on the hierarchically organized set of ontologies that will then illustrate the causal relationships of state variations of the objects. This reasoning capability based on procedural knowledge is peculiar and not available to the layer-based and topology-driven GIS.

Among the drawbacks of an ontology-based model system is the lack of spatial data handling, rendering, and analysis features that are necessary to effectively represent and visualize the spatial aspects of ontologies (that is, CI interdependencies in our case). Since these are exactly the major strengths of GIS, in our research, an effort is made to utilize both information systems to create a decision support system in, at least initially, a loosely integrated fashion to represent and visualize CI interdependencies.

## 4. AN INTEGRATED SYSTEMS APPROACH TO CI INTERDEPENDENCY REPRESENTATION AND VISUALIZATION (R&V)

The integrated system proposed in this paper combines the strengths of GIS and GenOM while mitigating the each other's weaknesses (Figure 1). It is a powerful tool that supports the understanding of CI interdependencies, the composition of scenarios, developing protection strategies, and helping to respond more effectively during a crisis. In the remainder of this section, we will present a methodology of ontology building with the integrated system.

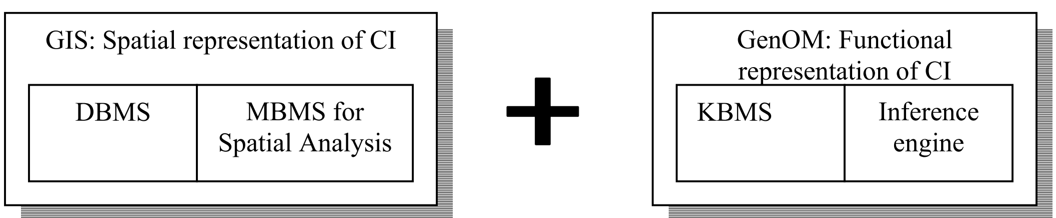
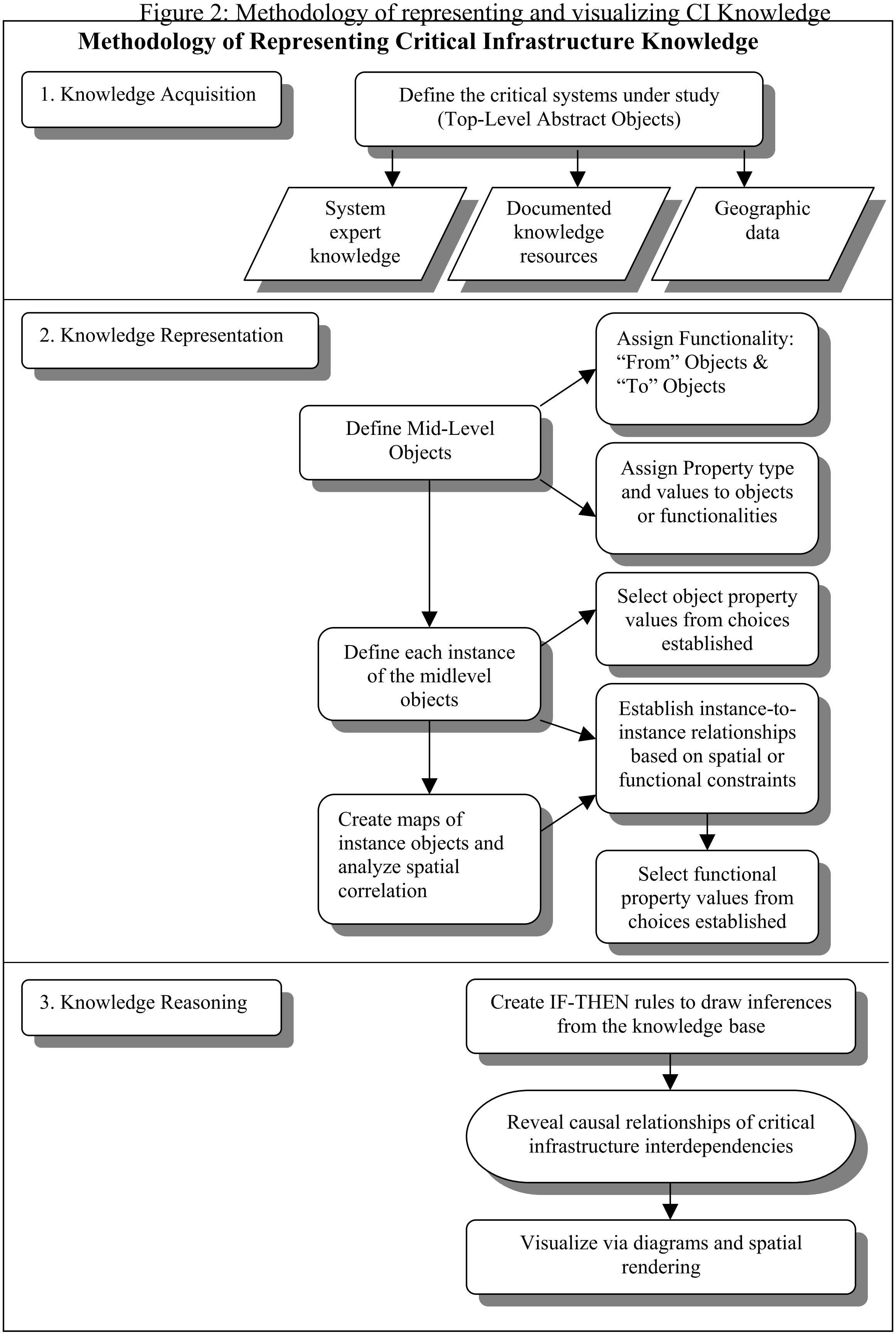



Figure 1: An integrated system of GIS and GenOM for CI knowledge representation

There are three parts in the proposed methodology—knowledge acquisition, knowledge representation and reasoning (Figure 2)

Figure 2: Methodology of representing and visualizing CI Knowledge



4.1. Knowledge Acquisition

Once a determination of which critical systems to study is made (Top-Level Objects), knowledge about these systems needs to be acquired. In order to develop CI interdependency knowledge, internal knowledge of each system should be understood at the outset. This includes knowledge about the mid-level objects; their properties, functions, and their locations. Although a wealth of declarative information about critical systems exist in multiple formats, much of the procedural knowledge is possessed by system experts, and as stated previously, difficult to obtain. A methodology of acquiring CI knowledge utilizing system expert interviews, open source documents and geographic data was developed by Xiang, *et al* (2005) to be able to extract the declarative and procedural knowledge necessary to construct a CI knowledge base.

4.2. Knowledge Representation through Ontology Building

The use of ontology to conceptualize the domain model has been utilized in many applications, but the application of knowledge engineering within the realm of critical infrastructure is new. When most people think about systems or organizations, a conventional hierarchical structure paradigm comes to mind. These hierarchies are structured by levels of responsibility or flows of service from origin to end-user. Unlike a conventional hierarchy, object hierarchies are classified into several levels of abstraction. This paradigm of representation of objects is the key to understanding the basis for the methodology. The levels of abstraction are classified according to their specificity. For example in figure 3, the top-level objects are usually conceptual or abstract objects that generally subsume subclass levels of objects. At the mid-level are common domain concepts of the top-level object that can compose of multiple locations across a geographic region. These locations are the actual instances of the mid-level object type and are deemed instance-level objects.

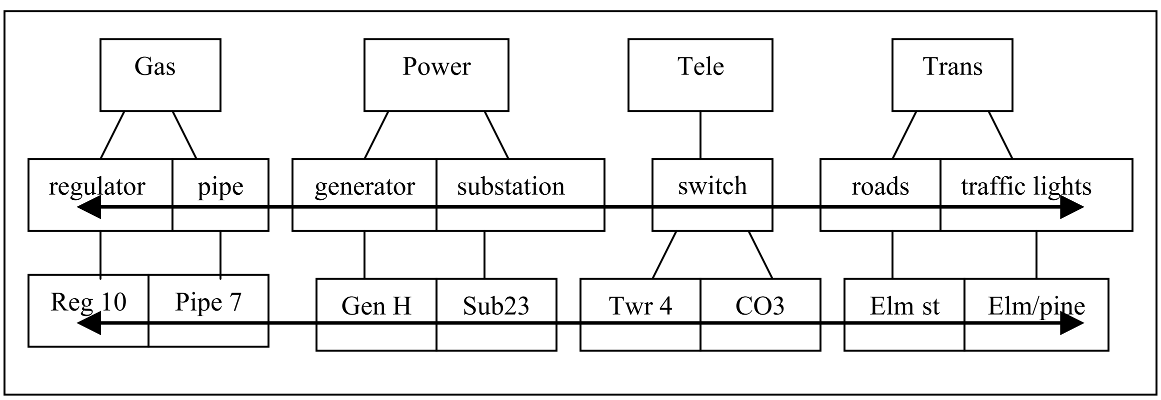



Figure 3: An example of the abstraction levels of Critical Infrastructure Systems

Each system expert is well versed in the knowledge of the internal relations of their system and the locations of each instance-level object. What is not well understood is the knowledge of the interdependencies between critical systems; therefore the methodology proposed is focused on representing this aspect of critical infrastructure knowledge. In other words, the system experts have the knowledge of the vertical relationships within their domain; we are interested in representing the horizontal interdependencies between the domains of critical systems (Figure 3). The top-level objects of critical systems are too broad-spectrum to begin to investigate interdependencies; this is why the application of representing CI interdependencies begins with the mid-level objects. Explicitly representing how the mid-level objects of one system interrelate to the mid-level objects of another system, decision-makers will have a better understanding of critical infrastructure interdependencies. By applying this knowledge to specific instances of mid-level objects, production rules can be composed that will infer the causal relationships during a disruption as well as determine of the level of criticality and vulnerability of an instance-level object.

4.2.1. Define mid-level objects

From the knowledge acquisition process, define the type of objects that compose each critical system. For example, the water supply has component mid-level objects of a reservoir, a treatment facility, pump stations, valves and distribution pipelines, among others. These objects are the types of components that compose the critical system.
Each mid-level object has a function that is the reason for its existence. A function is the objects purpose, behavior, or action. For example, a power plants function can be said to produce electricity. "Produces electricity" could be the assigned function of the object "power plant". The question becomes: to what or to whom is the power plant producing electricity for? A table can be created listing the functions and the objects that are assigned to them as well as the recipient objects of the functions. Such as: The function "produces electricity" is from the object "power plant" to the object "substation".

The next step involves identifying and assigning the characteristic properties of the various objects created. These properties can be classified as strings (text), real numbers, an integer, Boolean, or even another object if necessary. Such as a telephone office has properties of number of switches, building square footage, among others. Just as multiple properties can be assigned to an object, several values can be assigned for each property. For example, a substation may be a booster station or a transformer reducer; this property (Station type) is assigned to the object "substation". Functionalities can be also be assigned characteristic properties that need to be identified and assigned appropriately. A case in point is power lines that connect substations carry different amounts of power; these amounts would be entered as several property values in the property "amount of power".

4.2.2. Define instance of the mid-level objects

Each of the mid-level objects can have multiple specific instances in an area. For example, each telephone switch office location is a specific instance of the object "Telephone Switch Office". Through the knowledge acquisition process, the office locations should be determined and classified under the appropriate mid-level object it is an instance of. The instance-level objects inherit the properties assigned to the mid-level objects except here a specific property value from the values established can be selected. The instance-level objects should be spatially rendered and analyzed for spatial correlation relationships. The knowledge base of critical infrastructure interdependencies can be built by using the results of the spatial analysis as well as functional knowledge from the acquisition process. The specific instances can be related to each other based upon the functional assignment of their mid-level object. For example, from the instance "Meadow Nuclear Plant" of the object "power station", "produces electricity" to the instance

“Eastside Substation” of the object “substation”.   Any property values that have been assigned to a functionality that is relating these objects can be selected at this time (24 kilovolts).

### 4.3. Reasoning to Create Knowledge

By examining the knowledge base that consists of the instance level object relationships, the failure in one or more objects can demonstrate causal relationships during a disruption.  This is accomplished through the use of production rules based on IF-THEN logic. An example would be IF “eastside substation” failed, THEN the objects that have a functional relationship to it would be affected.  The result may be the Main Street telephone switch office, the traffic lights along Route 10, and the water pump on High Ave. are without power.  The results can be visualized via diagrams and spatial renderings. Once complete, the knowledge base is ready for vulnerability assessments, scenario composition assistance, and emergency response drill maneuvers.

## 5. A CASE STUDY

Both the integrated system and the methodology, was applied to a study that involved a system of 4 CI components in a municipality in the Southeastern United States. These 4 CI systems are telecommunication networks, natural gas, transportation networks, and electric power grid. Owing to the page limitations, this section omits the description of the process in which the methodology was implemented. Only are the outcomes of this process presented.
Functional representation can occur at different levels of the methodology and be used for different purposes.  GenOM is able to represent the functional relationship between the mid-level objects of CI in such a way that it provides the basis of understanding the interwoven nature of objects. Using GenOM, figure 4 illustrates the interdependencies that a substation mid-level object has with other CI mid-level objects based upon the functional relationships.   Some properties of the objects can be seen as well although not necessary for understanding of CI interdependencies.  Although this diagram is from the perspective of substations, the viewpoint can be from any mid-level object.  This is significant to aid in the understanding of CI mid-level object interdependencies to begin protection-planning strategies.  At this point, this model can be utilized as a template to apply to other regions besides our study area to be populated with its specific object instances.

Once the methodology is populated with specific object instances, the functional representations offered within GenOM can be utilized to visualize, along with the spatial rendering, a specific instance object’s interdependencies.  For example, a CIP professional may ask, what is the functional relationship of the substation represented in a spatial rendering of Figure 5?  Figure 6 diagrams the substation’s interdependent direct functionalities. By visualizing the wider-reaching effect of an object failure, this information can be utilized by public or corporate emergency managers to plan response strategies in the event of a disruption.

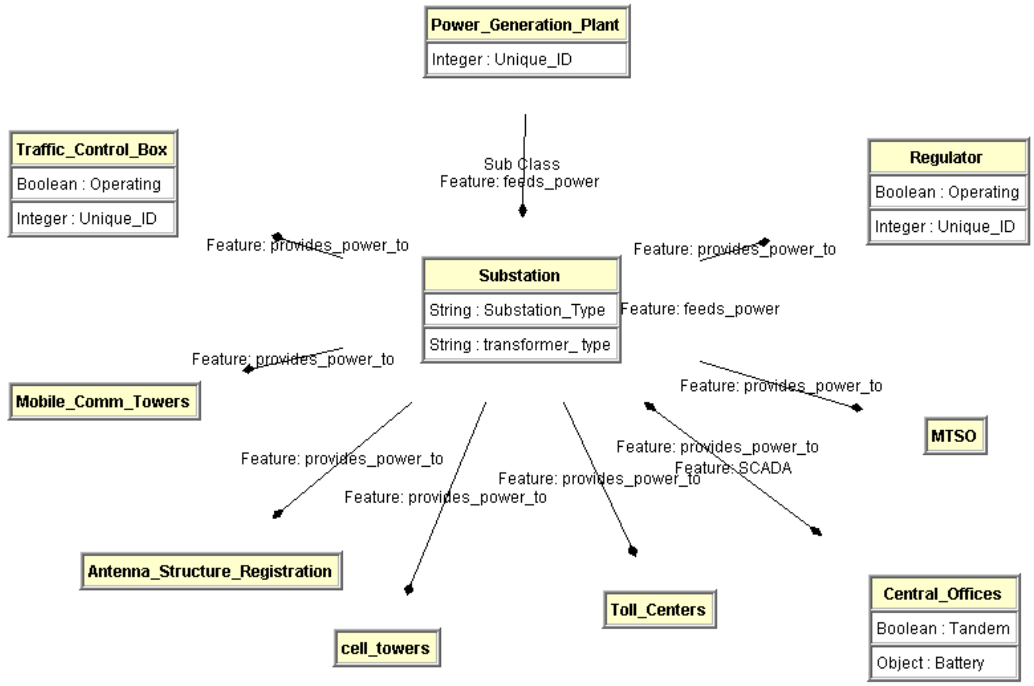



Figure 4: Mid-level object interdependencies from the viewpoint of a substation

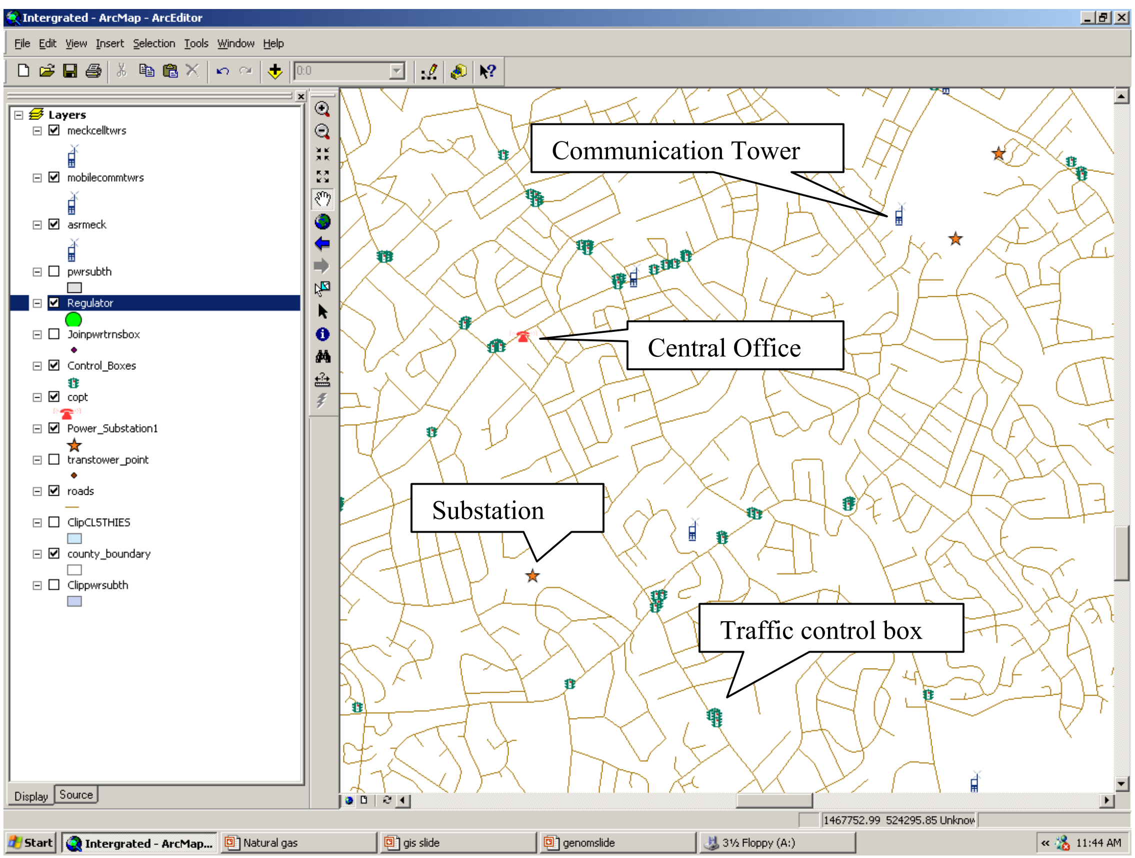



Figure 5: GIS screenshot of multiple layers of CI objects

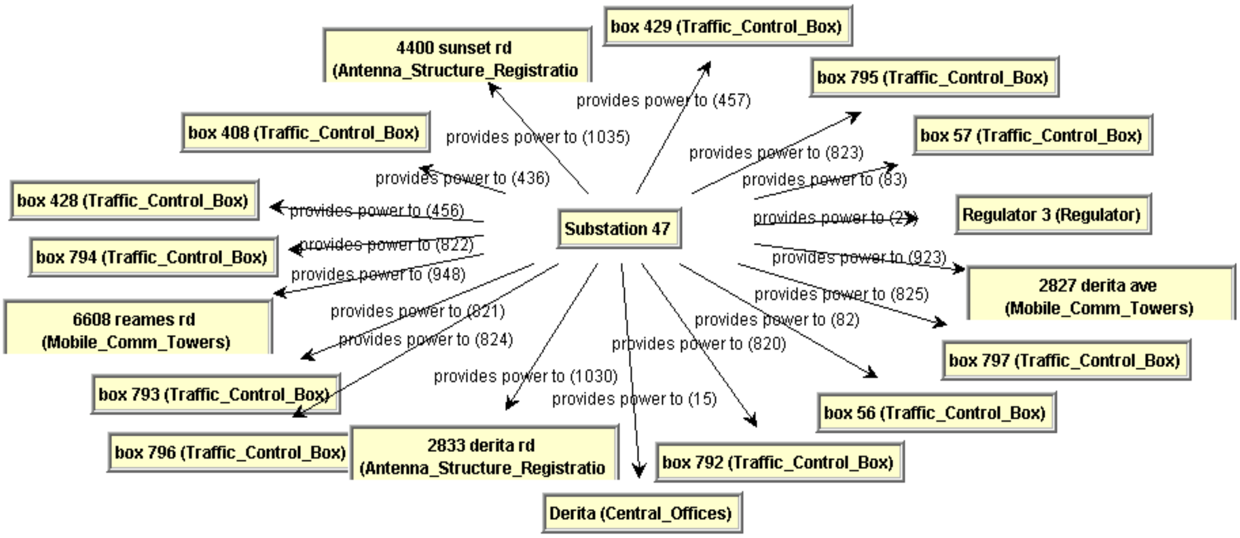



Figure 6: Instance-level direct functional interdependencies

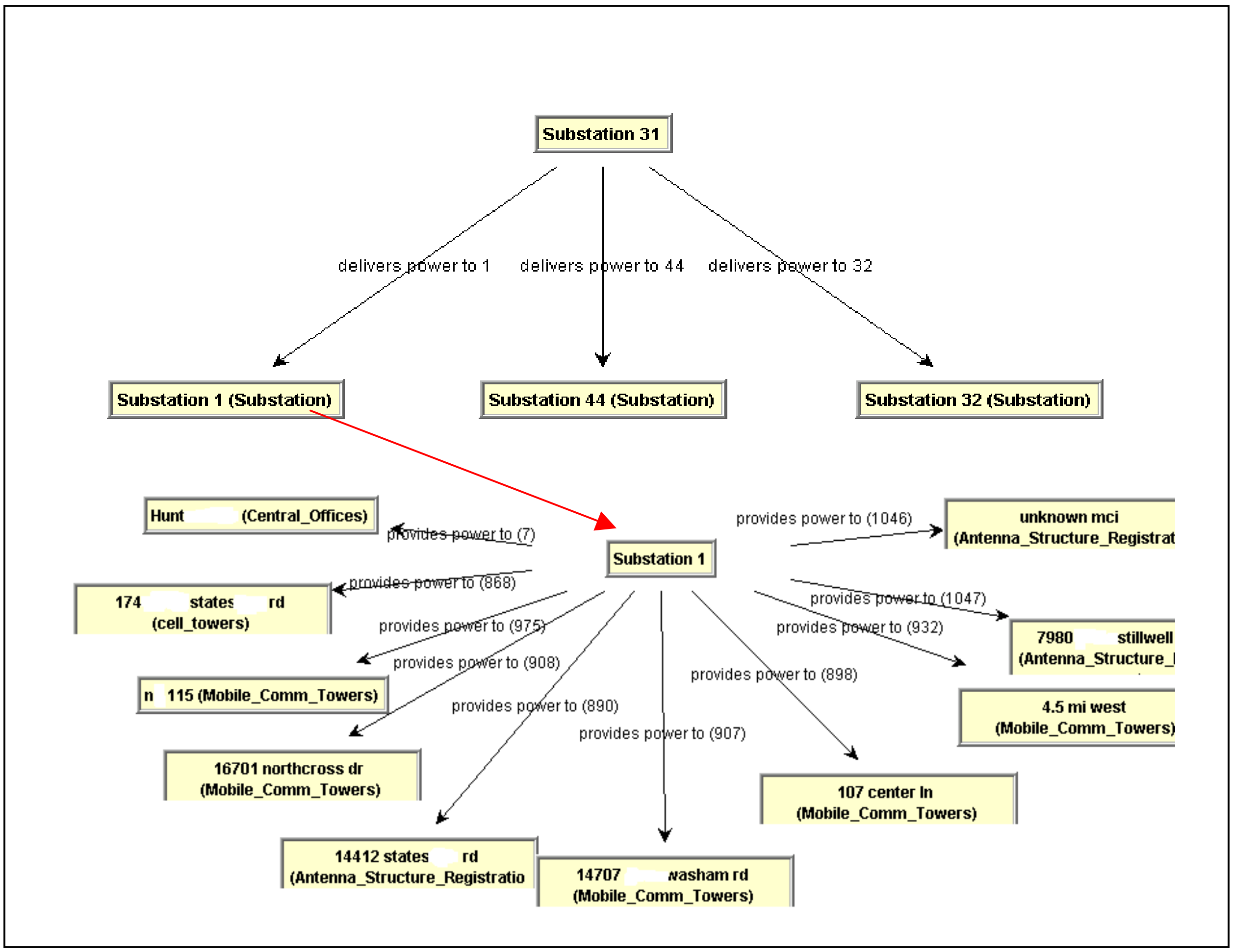



Figure 7: Instance-level direct and indirect functional interdependencies of substations

As the CI Interdependency Matrix (Table 3) illustrates, there exists indirect functional relationships between objects, one of which can be the origin of a cascade of events that ultimately affect other objects. It is the indirect relationships that are often the key to deciphering the sequences of events that can cause or have caused the wide-ranging effect of a disruption by a single critical system object. Figure 7 illustrates how GenOM can represent the indirect interdependencies within objects and the cumulative effects a disruption may have beyond its direct relationships.

## 6. CONCLUSIONS

The interwoven nature of CI interdependencies has long been an obstacle to the development of effective protection strategies. Given the importance of the services that systems of CI provide, a means to unraveling the complexity of these interactions has been developed. This has been achieved by utilizing a methodology of representing CI system knowledge based on the use of ontologies. We were able to employ a loose coupling of an object-oriented technology, GenOM, and a GIS to visualize geographically and diagrammatically, the CI system component interactions, the interdependencies within systems of CI, and the spatial locations of these objects. By doing so, this base of CI knowledge can now be analyzed to come to a common understanding of the behaviors of CI interdependencies through a common language. This facilitates the understanding of this subject to different systems experts, emergency management officials, and homeland security authorities. The ability of GenOM to visualize the direct and indirect functional relationship between instance level objects can be especially useful in the composition of scenarios to assess for criticality and vulnerability. The consistency and completeness that the knowledge base provides allows for the formation of rules of inference. These rules can be written to accompany the scenario plotline in order to assist in the understanding of effects upon other objects during a disruption.

Despite the accomplishments that this paper demonstrates, there is much need for future research in CI interdependencies. By extending the methodology to a different case study area, a further confirmation of its effectiveness can be achieved. The application of similar principles in an area with differing land use patterns, terrain, and population patterns would provide an adequate challenge to validate its use more universally. Although use of a loose coupling of two computer technologies, GIS and GenOM to implement the methodology was effective, a tightly coupled system that makes full use of the relational database capacity as well as the ability to use ontology, would create an interoperable environment that would be more efficient to use in the application of scenarios. The creation of rules within the inference engine explicitly defines the causal relationships so that a study of scenarios and their use within systems of CI can take place that would be beneficial to protection strategy formation and crisis intervention policies.

## ACKNOWLEDGEMENTS

The authors are grateful to the following individuals at the University of North Carolina at Charlotte for their contributions to the project: Bei-Tseng Chu, Mirsad Hadzikadic, Vikram Sharma, Robin Gandhi, Katie Templeton, Gustavo Borel, Stuart Phelps, Jocelyn Young, Paul Smith, Quinhong Tang, Ken McWilliams, and Huili Hao.

## References


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

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

Edgenhofer, M., and Frank, A. 1992. Object-Oriented Modeling for GIS. *URISA Journal*, 4(2): 3-19.

Frank, A., 1997. "Spatial Ontology." In *Spatial and Temporal Reasoning*. Stock, O. (Ed) Dordrecht, Netherlands: Kluwer Academic Publishers.

Gruber T. R., 1993. A Translation Approach to Portable Ontologies. *Knowledge Acquisition*, 5(2): 199-220.

Lee, S. and 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. (Copies available by contacting the first author).

Protégé. 2000. *The Protégé Project*. Stanford Medical Informatics at Stanford University School of Medicine. Available online: http://protege.stanford.edu

Rinadi, S., Peerenboom, J., and Kelly, T. 2001. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine*, December 2001, pp. 11-25.

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

*The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, The White House, Washington D.C., May 22, 1998.

The Geographic Information Center of the National Academies. 2005. *GI Basics*. Available online: http://gi.nationalacademies.org/background.shtml.

*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, The White House, Washington D.C., February 2003

Turban, E. and Aronson, J.E. 2001. *Decision Support Systems and Intelligent Systems*. Upper Saddle River, NJ: Prentice Hall.

Xiang, W-N, Tolone, WJ, 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”. Paper presented at 2005Auto-Carto conference, Las Vegas, NV, March 2005.