"An Ontology-Based Approach to Blind Spot Revelation in Critical Infrastructure Protection"

William J. Tolone, Joshua Blackwell, Seok-Won Lee, Wei-Ning Xiang and Lydia Marsh. The University of North Carolina at Charlotte

Research Questions: What are blind spots in critical infrastructure protection (CIP), what are the sources and how can they be revealed?

Research Outcomes: Based on case study a formal approach for revealing blind spots in CIP is designed.

The Formal Approach to Revelation

Describe CIP Domain in Ontology and GIS

Scan Area to Investigate Blind Spots

Use Tools and Techniques to Reveal

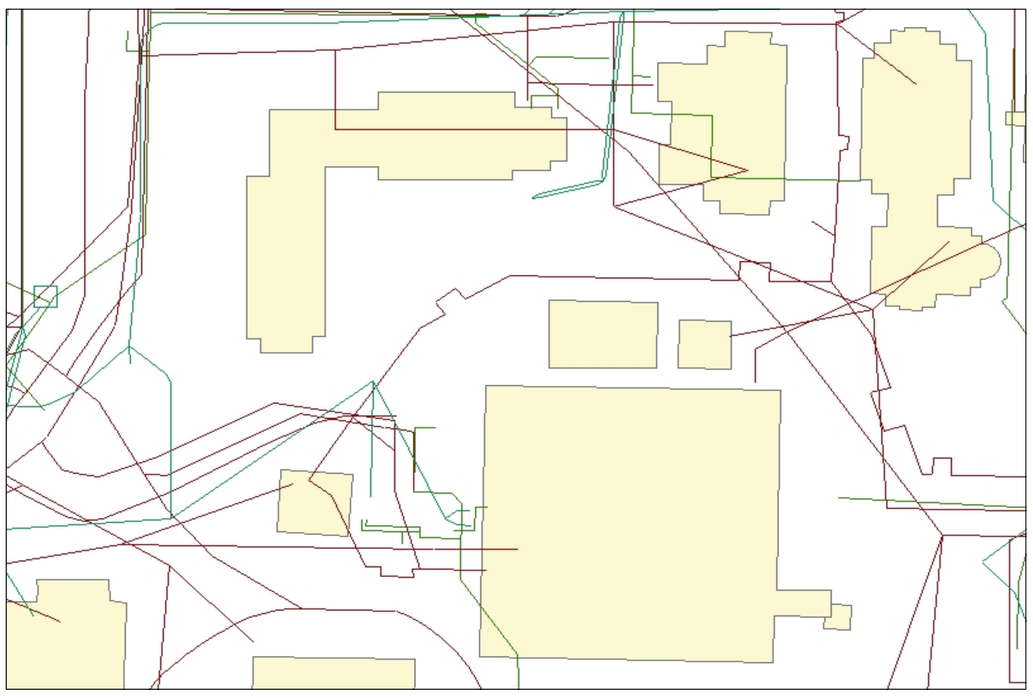
Further Diagnosis

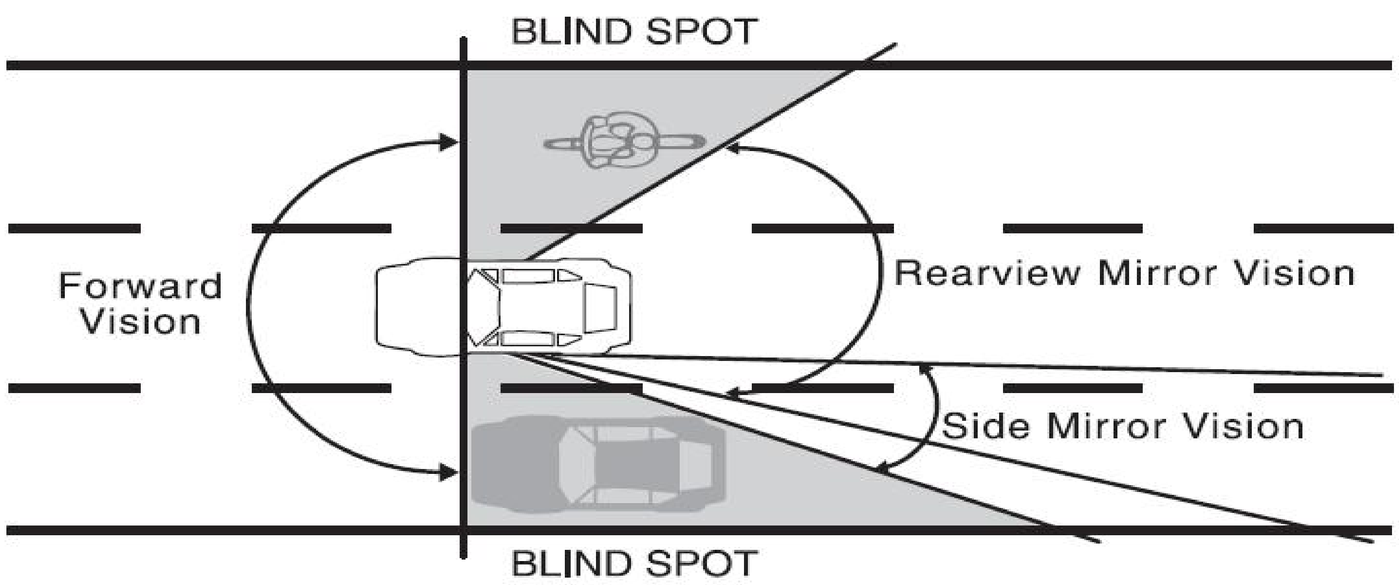
Implement Policy / Install CI Component

Tools and Techniques: Ontology-based information system. Utilized to generate scenarios. Using top-down approach of interdependency recognition and bottom up approach of data mining information is gathered represented and refined to reveal blind spots.

Verification and Validation: utilized throughout the process to insure accurate representation and assist with gathering new information.

Given Data in GIS Model





What are the sources of blind spots? In CIP surprises can result from several sources. They are documented here but this is not an exhaustive list.

The Sources of Blind Spots in CIP	
Complexity	CI Interdependencies
	Spatial Variations
	Temporal Variations
	Observation Scale Dependence
Imperfect Information	Lack of Data
	Lack of Cross-Domain Knowledge
Perception	Availability Heuristic
	Adjustment Heuristic
Imperfect Tools	Geographic Information Systems
	Ontology
	Other Tools

Case Study: Described objects in Ontology, realized needed more information, utilized Delphi questioning and data mining to get information from subject matter experts (using techniques to reveal) about interior of buildings (abstraction). Power panel found to supply power to lighting and electrical outlets in Vivarium. When power is lost the HVAC is shut down. The emergency generator comes online to provide power to the lighting circuits. A human needs to be prepared to plug in a emergency HVAC unit to the outlets (new policy) which then controls the temperature in the critical lab. The research animals are preserved. Blind Spots diagnosed were scale-dependence, lack of information and usage of tools.

Acquired Knowledge in Ontological Model