

# Information Sharing and Decision Support for C(I)IP

Stephen D. Wolthusen

Computer Science Department  
Gjøvik University College  
N-2802 Gjøvik, Norway  
swolthusen@ieee.org

## 1 Introduction

Interdependencies among the elements of national and transnational critical infrastructures necessitate coordination and cooperation among infrastructure operators as well as with government [TH03]. The scope of information sharing is typically limited by confidentiality requirements since infrastructure operators may both be in competition with one another and have concerns over commercial intelligence and excessive disclosure of internal procedures and processes to the general public. This, however, can change rapidly when transitioning from regular operations to crises or large-scale disruptions.

Such transitions from regular operations to damage or crisis control may occur very rapidly and frequently must be dealt with quickly to avoid further cascading effects and damage. Controls on information exchange that are effective and prudent during normal operations may no longer be appropriate in such environments, and normal communication channels may either become unavailable or prove to have bandwidth and latency that is too low for the amount of data that needs to be exchanged (e.g. in case of communication that is normally handled by voice or facsimile during regular operation). While exercises (e.g. LÜKEX exercises at the national level in Germany) can assist in establishing and exercising communication channels for use in crisis environments, the ad-hoc nature of these communication paths clearly limit their overall utility.

Information sharing mechanisms for critical infrastructure environments should therefore provide benefits to the efficiency and efficacy of normal operations of critical infrastructures to provide an incentive to use the information and information sharing platform regularly and extensively and permit its efficient use during crises and major events. Improving familiarity of operators with the platform as well as with the internetworking capabilities can then provide valuable increments in the speed and efficacy of handling critical situations while improving the cost-effectiveness of regular operations through increased transparency of infrastructure assets, procedures, and operations.

Moreover, the precautionary integration of data sets and streams that are potentially of interest to a decision maker during a crisis event could be justified only with difficulty if no tangible benefit can be derived for the infrastructure operator during regular operations.

Even if the overall cost of a large-scale cascading infrastructure failure and probability of such an event would indicate that such a course of action would be beneficial on a global scale, it should be noted that such considerations are not compelling for individual infrastructure operators as the total (or even fractional) cost of such a disruption is not borne fully by the infrastructure operator. It is therefore of vital interest to provide an additional incentive to infrastructure operators in the form of efficiency gains during regular operation for the adoption of information sharing and decision support systems.

Information sharing and decision support systems integrating heterogeneous data sources are of interest not only for use among multiple infrastructure operators but also within individual infrastructure operator organizations since data repositories and sensor data are both heterogeneous and subject to frequent change over time and may therefore require integration measures even within a single unified organization. This is in part owed to the considerable costs associated with recording e.g. geospatially referenced data that must be retained for long periods of time during which measurement and record-keeping procedures may change significantly.

## **2 A Standards-Based Information Sharing Framework**

Information sharing for C(I)IP can be performed efficiently if two core requirements are met. One is that the data formats used to represent the various types of streams and data items must be capable of reflection, i.e. of incorporating the requisite ontological information to ensure long-term stability as well as the ability to exchange data sets among (sub-)organizations with disjoint operational semantics. This ensures that the semantics of data streams can be retained even if changes or translations need to occur. The second, closely related requirement is the use of a common underlying syntactical format for the representation and classification of varying media types that are constituting the total operational situation. Moreover, individual data items need to be verifiable in their integrity and authenticity both at the time of use and at a later date, e.g. during the course of an audit or other review process.

Given that infrastructure operators will frequently already have command and control systems in place, it is also highly desirable to create an information sharing and decision support infrastructure that is modular and can be integrated into such existing systems with a loose coupling.

These requirements (as well as additional requirements described in [Wol04]) can be met by using techniques developed within the W3C Semantic Web project. Web services with well-defined interfaces for data sources that can be self-describing provide fine-grained input data streams that can be modified and extended individually as well as being subject to precise security controls. Moreover, the syntax and semantics of the individual data streams and sources can be described within the W3C resource definition framework (RDF) [BR05, Wol04], providing the ability to dynamically transform and translate metrics and error probabilities between sensors and data sources. Provided that a command and control system is equipped with the necessary transformation and filtering ru-

described within the RDF framework, it can integrate new sources into the information system without requiring extensive adjustments to the overall system architecture.

While this ability to dynamically configure multiple source information sharing is an important improvement over existing information systems for C(I)IP in its own right for both internal use within a single infrastructure operator and, more importantly, also among multiple infrastructure operators even on an ad-hoc basis when e.g. necessitated by a major crisis requiring large-scale cooperation among infrastructure operators, another property of an RDF-based model for information structuring and exchange is that it is possible to use the embedded semantics and formalized ontology as the basis for automated reasoning over the data contained within the individual sources and data streams.

Provided that all data sources are rigorously annotated with the necessary ontological data, the semi-rigorous model-theoretic definition of the formal semantics of RDF e.g. allows for the formulation of queries regarding semantically related information sources (e.g. of sensors related to a specific component of a power plant or within a specific geolocation) and the identification of extraordinary and correlated events. This ontological representation [Sow00] is also implementable using W3C Web Ontology Language (OWL), which can be considered a syntactical and semantic extension of RDF and defines descriptions, classes, properties and their instances and, more importantly, semantic entailments which can be used for reasoning within the ontological model. To ensure that entailments can be computed and computed efficiently, the OWL language must be constrained in its expressiveness; for the purposes of the modeling described in this paper a well-defined subset of OWL called OWL description logic provides such a constraint. Description logics are somewhat limited in their expressiveness [BCM<sup>+</sup>03] but do permit the use of a deterministic computational model.

Moreover, the RDF/OWL framework, in conjunction with a graph-based dependency model, can also form the foundation of a provably secure and fine-grained model of security controls that is equally applicable to individual and internetworked infrastructure operators [Wol04]. This provides the necessary assurance and flexibility to dynamically interlink information sources.

### **3 Geospatial Data-Based Decision Support for C(I)IP**

Information sharing, particularly when large numbers of data sources must be integrated and correlated, is faced with two key challenges. First, any information sharing and decision support system must take into account the cognitive limitations of decision makers in the number of events that can be recognized and integrated in the decision maker's situational picture and awareness. It must therefore provide the ability to aggregate and prioritize information (as described in the preceding system, this can at least be partially automated) before presentation to the decision maker. Moreover, given the same source information, an information and decision support system must provide individualized representations to reflect differing cognitive capacities, mental models, and different priorities and objectives among multiple (also distributed) decision makers.

The second challenge is to provide a shared cognitive platform for the representation of the various information sources. A multimodal visual presentation mechanism using both topological and topographical information can provide situational awareness by presenting objects, dependencies, and interrelations within a common situational view that also incorporates background information from various sources. The presentation of the collected data on infrastructure elements and environmental conditions as well as the integration into relevant information that is immediately required by decision makers can occur in a number of different views depending on the task at hand.

Since a significant number of infrastructure elements have network characteristics (i.e. depend on edges connecting individual vertices, as in the case of telecommunication or power transmission lines), a topological view provides key insights in an abstract format which permits dependencies to be identified and analyzed. However, a purely topological view may omit highly significant data points that can be critically important to know for decision makers. Particularly when multiple infrastructure elements or external threats such as weather events are to be considered, a topological view does not provide the appropriate context to judge such influences. Moreover, while some mutual and transitive dependencies can be identified automatically, these dependencies and interactions may not be known in advance and can only be derived intuitively given an appropriate presentation of the data.

Geographical information systems [LGMR99] can provide this contextualization as well as a foundation for integrating the varied types of information that must be aggregated and selectively displayed for decision makers. A particular challenge for the presentation mechanism is tightly coupled with the usage patterns likely to be found in all application areas from planning to emergency management, namely that the information presented is likely to be shared visually (e.g. in the same situation room or in the field) with individuals for which the security controls have no information.

## 4 Related Work

The modeling and simulation of critical infrastructures has gained significant attention in recent years [Ami00, DPS02, Rin04], but has been mainly constrained to the assumption that sensors and information sources were defined a priori and homogeneous in nature. The types of analysis imposed by the analytical models ranged in their level of detail from simple dependency analyses to elaborate models containing continuous physical submodels (e.g. for oil and gas pipelines or electrical grid systems) [NNC<sup>+</sup>05] as well as behavioral models. Among the earliest and most widespread is the application of a control systems approach [SKDG99] including hybrid mechanisms [JM04]. Particularly for behavioral modeling, agent-based systems have also been investigated in detail [Nor00, TNMP03].

The use of computer-supported cooperative working environments (CSCW) and group support systems (GSS) has been investigated extensively, primarily from a human-computer interface perspective [Ram99, SJY01, AvD05].

## 5 Conclusions

In this paper we have argued the need for the establishment of a common technical and organizational framework for the representation and controlled exchange of georeferenced data among critical infrastructure operators and other interested parties, including national and regional governments and governmental agencies.

Using a standards-based platform for information sharing and fine-grained and provably secure access controls provides the ability to cross-link infrastructure operators and geographically dispersed organizational units within individual infrastructure operator organizations as needed using a common cognitive model that can support both topographic and topological visualization mechanisms.

## References

- [Ami00] M. Amin. Toward Self-Healing Infrastructure Systems. *IEEE Computer*, 33(8):44–48, August 2000.
- [AvD05] J. H. Appelman and J. van Driel. Crisis-Response in the Port of Rotterdam: Can We Do Without a Facilitator in Distributed Settings? In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*, Big Island, HI, USA, January 2005. IEEE Computer Society Press.
- [BCM<sup>+</sup>03] F. Baader, D. Calvanese, D. McGuinness, D. Nardi, and P. Patel-Schneider, editors. *The Description Logic Handbook*. Cambridge University Press, Cambridge, UK, 2003.
- [BR05] Travis D. Breaux and Joel W. Reed. Using Ontology in Hierarchical Information Clustering. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*, Big Island, HI, USA, January 2005. IEEE Computer Society Press.
- [DPS02] Donald D. Dudenhoeffer, May R. Permann, and Elliot M. Sussman. A Parallel Simulation Framework for Infrastructure Modeling and Analysis. In *Proceedings of the 33rd Winter Simulation Conference*, San Diego, CA, USA, December 2002. IEEE Computer Society Press.
- [JM04] J. James and F. Mabry. Building Trustworthy Systems: Guided State Estimation a Feasible Approach for Interpretation, Decision and Action Based on Sensor Data. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, Big Island, HI, USA, January 2004. IEEE Computer Society Press.
- [LGMR99] Paul A. Longley, Michael F. Goodchild, David J. Maguire, and David W. Rhind, editors. *Geographical Information Systems*. John Wiley & Sons, New York, NY, USA, 2nd edition, 1999. Two volumes.
- [NNC<sup>+</sup>05] D. E. Newman, Bertrand Nkei, B. A. Carreras, I. Dobson, V. E. Lynch, and Paul Grady. Risk Assessment in Complex Interacting Infrastructure Systems. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)*, Big Island, HI, USA, January 2005. IEEE Computer Society Press.

- [Nor00] M. J. North. Agent-Based Modeling of Complex Infrastructures. In *Proceedings of Simulation of Social Agents: Architectures and Institutions Workshop*, pages 239–244. Chicago, IL, USA, October 2000.
- [Ram99] M. Ramage. *The Learning Way: Evaluating Cooperative Systems*. PhD thesis, Department of Computer Science, University of Lancaster, Lancaster, UK, 1999.
- [Rin04] S. M. Rinaldi. Modeling and Simulating Critical Infrastructures and Their Interdependencies. In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, Big Island, HI, USA, January 2004. IEEE Computer Society Press.
- [SJY01] D. Shands, J. Jacobs, and R. Yee. Secure Virtual Enclaves: Supporting Coalition Use of Distributed Application Technologies. *ACM Transactions on Information and System Security*, 4(2):103–133, May 2001.
- [SKDG99] K. Sullivan, J. C. Knight, X. Du, and S. Geist. Information Survivability Control Systems. In *Proceedings of the 21st International Conference on Software Engineering*, pages 184–192, Los Angeles, CA, USA, May 1999. IEEE Computer Society Press.
- [Sow00] J. F. Sowa. *Knowledge Representation: Logical, Philosophical, and Computational Foundations*. Brooks Cole Publishing, Pacific Grove, CA, USA, 2000.
- [TH03] Wil A. H. Thissen and Paulien M. Herder, editors. *Critical Infrastructures: State of the Art in Research and Application*. Springer-Verlag, Berlin, Germany, 2003.
- [TNMP03] W. H. Thomas, M. J. North, C. M. Macal, and J. P. Peerenboom. From Physics to Finances: Complex Adaptive Systems Representation of Infrastructure Interdependencies. Technical report, Naval Surface Warfare Center Technical Digest, Dahlgren, VA, USA, 2003.
- [Wol04] Stephen Wolthusen. Modeling Critical Infrastructure Requirements. In *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, United States Military Academy*, pages 258–265, West Point, NY, USA, June 2004. IEEE Press.