Chapter 16

ONTOLOGY-BASED CRITICAL INFRASTRUCTURE MODELING AND SIMULATION

Vincenzo Masucci, Francesco Adinolfi, Paolo Servillo, Giovanni Dipoppa and Alberto Tofani

Abstract This paper describes a knowledge-based system (KBS) designed to support a federated environment for simulating critical infrastructure models. A federation of simulators is essentially a "system of systems," where each simulator represents an entity that operates independently with its own behavior and purpose. The interactions among the components of the federated system of systems exhibit critical infrastructure vulnerabilities as emergent behavior; these vulnerabilities cannot be analyzed and simulated by considering the behavior of each system component individually. The KBS, which is based on ontologies and rules, provides a semantic foundation for the federated simulation environment and enables the dynamic binding of different critical infrastructure models. The KBS-based simulation environment can be used to identify latent critical infrastructure interdependencies and to test assumptions about interdependencies.

Keywords: Modeling, simulation, ontology, federated environment

1. Introduction

The DIESIS Project, which is funded by the European Community, is currently investigating the feasibility of creating a European Infrastructure Simulation and Analysis Center (EISAC). EISAC would function as a distributed e-infrastructure for conducting interoperable federated simulations of critical infrastructures in support of risk analysis and management efforts. EISAC would connect various modeling and simulation communities through the deployment of high-level services. Despite the utmost importance of critical infrastructures to citizens, the economy and society at large, the understanding of critical infrastructures and their interdependencies is still relatively immature. Com-

prehensive, systematic investigations of complex infrastructures demand joint efforts by researchers, infrastructure owners and operators, and government agencies to overcome obstacles such as the availability of models and data, interoperable simulation environments for multiple infrastructures, testbeds and benchmarks for protection solutions.

The main concepts and definitions related to critical infrastructure interdependencies are widely accepted (see, e.g., [19]). A report on European critical infrastructure disruptions [11], which classifies the cascading effects in critical infrastructures, emphasizes the importance of analyzing such events. However, the scale, complexity and coupling of critical infrastructures present numerous theoretical and practical challenges to the modeling, prediction, simulation and analysis of cause-and-effect relationships. Critical infrastructure systems are heterogeneous mixtures of dynamic, interactive, non-linear entities with unscheduled discontinuities and numerous other significant effects. Thus, the modeling and analysis of these systems requires the consideration of their large-scale, non-linear and time-dependent behavior.

The EISAC facility, which is intended to have the same functionality as the U.S. NISAC [20], will support collaborative activities in critical infrastructure protection and advance the state of the art in the field of federated simulation. One of the key requirements is a knowledge-based system (KBS) that would provide the semantic foundation for a federated simulation environment. A federation of simulators can be considered to be a "system of systems," where each simulator represents an entity that operates independently with its own behavior and purpose [12]. The interactions between simulators display emergent behavior that cannot be analyzed by simulating the individual entities in isolation.

This paper describes the design of a KBS for a federated critical infrastructure simulation environment being developed under the DIESIS Project. The KBS, which is based on ontologies and rules, provides a semantic foundation for the federated simulation environment and enables the dynamic binding of different critical infrastructure models. The KBS-based simulation framework can be used to identify latent critical infrastructure interdependencies and to test assumptions about interdependencies. In addition, it facilitates the development of strategies for operating critical infrastructures and articulating risk management policies.

2. Background

The IEEE High Level Architecture (HLA) Standard specifies a common architecture for distributed modeling and simulation, including a framework for the interconnection of interacting simulations. However, environments based on HLA and related approaches are not well-suited to simulating critical infrastructures. In particular, the coupling of simulators is based on a common data model, which must be implemented by all the involved simulators. Moreover, the data model is purely syntactic and does not provide semantic information about the modeled domains. The proposed federated simulation environment

is specifically designed to address the semantic interoperability of critical infrastructure simulators.

Several modeling and simulation approaches have been developed to analyze critical infrastructure interdependencies. Pederson, *et al.* [16] categorize them as integrated and coupled approaches. Integrated approaches engage a single monolithic framework to express multiple infrastructures and their interdependencies. In contrast, coupled approaches model individual infrastructures separately and couple the individual models to analyze the infrastructures and their cascading effects.

NISAC uses several modeling approaches and simulation tools [1] ranging from detailed to abstract. NISAC also offers the Critical Infrastructure Protection Knowledge Management Portal (CIP KM Portal) that supports the rapid access of information (documents, presentations, media files and web links). The information is organized into multiple taxonomies covering programs, projects, infrastructures, models and tools. The DIESIS KBS is similar to the NISAC CIP KM Portal in terms of the model and infrastructure taxonomies. In addition, the DIESIS KBS will play a major role in federated simulations and facilitate the automatic acquisition of new knowledge about infrastructure interconnections and interdependencies.

Tolone, *et al.* [23] and others [5, 7] also focus on infrastructure interdependencies. The modeling and simulation approaches, which are based on comprehensive models of critical infrastructures, primarily support high-level analysis (also, see [3, 6, 13]). Marti, *et al.* [14] have developed an infrastructure interdependencies simulation (I2Sim) system based on integrated, supply and demand system models. I2Sim has been applied to several infrastructures (e.g., electrical power grid, water supply, telecommunications and transportation) to coordinate planning, response and recovery during large-scale disaster situations (e.g., earthquakes, hurricanes and terrorist attacks).

The Idaho National Laboratory (INL) has designed CIPR/sim simulators that allow emergency planners to visualize the real-time cascading effects of multiple infrastructure failures before an actual emergency occurs. CIPR/sim adheres to the IEEE HLA Standard and can import real-time data from numerous existing analysis modules, including the Real-Time Digital Simulator (for electrical power grid analysis), QualNet [21] (for telecommunications system analysis) and other tools for wind speed and flood surge analysis. CIPR/sim can be categorized as employing a coupled, high-fidelity modeling and simulation approach.

Several interesting approaches have been developed by European researchers as a result of national and EU initiatives. Klein, *et al.* [10] have proposed a comprehensive critical infrastructure modeling and simulation approach. Another notable contribution is the CRESCO architecture [9] developed under an Italian initiative. The CRESCO architecture provides facilities for defining and configuring simulation scenarios, analyzing critical infrastructure interdependencies, and integrating domain-specific models in order to simulate the detailed behavior of critical infrastructures. CRESCO engages two approaches

for modeling critical infrastructure interdependencies: CISIA, which is based on an entity resource model [4]; and CIAB, which exploits an agent-based model [2]. All these systems can be considered to use macroscopic approaches: a key limitation is that the coupling of critical infrastructure domain simulators often yields inadequate simulation results.

The approach of Tolone, *et al.* [23] is conceptually very similar to our work. This service-oriented framework for integrated modeling and simulation also uses meta knowledge to formalize agent behavior and inter-infrastructure relationships.

3. Ontology-Based Modeling and Simulation

This section describes the formal processes involved in representing knowledge about critical infrastructures and their interconnections, and guiding KBS development. The ontological framework used in the DIESIS KBS permits the specification of domain knowledge (definition), the application of inference rules (reasoning), and the generation of new knowledge from the knowledge base (deduction).

3.1 DIESIS Knowledge-Based System

The top-down design approach used for the DIESIS KBS is intended to promote flexibility. Domain ontologies express concepts in a highly specialized manner and are often very detailed; consequently, it is difficult to merge ontologies into a general representation. However, as described below, the DIESIS KBS can be integrated via existing standardized domain models in a bottom-up fashion. Figure 1 presents the DIESIS KBS architecture, which is inspired by [17, 18].

The DIESIS KBS design incorporates a meta knowledge infrastructure ontology (MKIONT), infrastructure ontologies (IONTs), a federation ontology (FONT) and gateway components.

3.1.1 MKIONT. The meta knowledge infrastructure ontology (referred to as MKIONT) defines a general template for expressing the basic concepts and relationships of critical infrastructures and their interconnections. The MKIONT assumes that it is possible to model every critical infrastructure as a set of interconnected system components. Infrastructure ontologies (IONTs) are defined by specializing the MKIONT definitions to specific critical infrastructure domains. The MKIONT template permits the representation of cross-domain critical infrastructure interconnections and the related semantics. In particular, the abstract concepts and relationships defined within the MKIONT are represented as classes (meta classes) and relations (properties) that are specialized as IONTs and a federated ontology (FONT) by specifying sub-classes and sub-properties. Thus, the MKIONT template essentially provides an object-oriented approach for defining the IONTs and FONT.

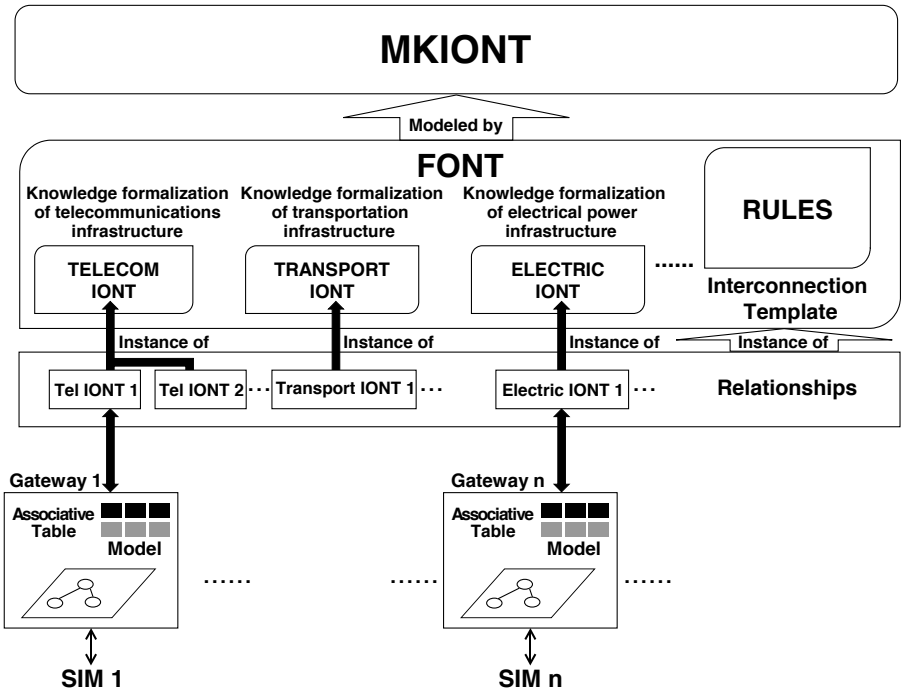

Figure 1. DIESIS KBS architecture.

In summary, the MKIONT provides: (i) a critical infrastructure template that captures basic concepts and relationships pertaining to a critical infrastructure; and (ii) an interconnection template that represents critical infrastructure interconnections and their relative semantics.

3.1.2 IONT. An infrastructure ontology (IONT) represents knowledge about a particular critical infrastructure (e.g., telecommunications, transportation or electrical power). The IONT, which is derived from the MKIONT template, defines the set of concepts and properties used to formalize the critical infrastructure domain. The definition could rely on existing standards as in the case of the electrical power domain, for which the relative IONT has been defined with respect to IEC standards [15].

The MKIONT template is used to define IONTs for the considered critical infrastructures, ensuring the semantic interoperability of the different critical infrastructure models. An IONT is "simulator independent" because it conceptually models and formalizes the knowledge of a particular domain and because it is possible to define different IONTs for a domain to accommodate different levels of granularity. However, the various IONTS for a given domain are independent of each other and cannot be used in a federated simulation environment unless the appropriate interconnection rules are specified using a FONT (described below). The IONTs are instantiated by populating them with ac-

tual critical infrastructure components and data to represent specific critical infrastructure models (e.g., electrical power transmission/distribution grid of a particular zone, city or district). These IONTs are subsequently translated to the appropriate simulator models. In general, IONTs created at different granularity levels (for a given critical infrastructure domain) run on different simulators, each corresponding to a defined level of granularity. This approach allows for the modular composition of simulators in the federation and the ability to employ different levels of detail for a given critical infrastructure.

3.1.3 FONT. A federation ontology (FONT) formalizes critical infrastructure interconnections and their semantics. In particular, a FONT expresses knowledge about the interconnections between different domains and the rules that govern the interconnections. The FONT definition includes all the objects and relationships relevant to a federated simulation (i.e., the defined IONTs). Therefore, a FONT specializes an MKIONT interconnection template that formalizes the interconnections between the elements of IONT instances.

Note that we distinguish between interconnections and interdependencies. An interconnection is an explicit identification of a relation between items of different domains (e.g., a router in a telecommunications network receives electricity from a power distribution network). On the other hand, an interdependency represents emergent behavior due to the interaction modalities of interconnected critical infrastructure networks.

Thus, the specification of all possible critical infrastructure interconnections is insufficient to generate interdependency phenomena in a federated simulation environment. To this end, the FONT enriches the definition of interconnections with semantic rules. In particular, a rule specifies how two critical infrastructure elements are interconnected (i.e., how one element depends on the other, enabling effects to propagate in different domains). For example, the FONT could define an interconnection named *isaLoad* between a router element (in the telecommunications domain) and a load element (in the electrical power domain). The semantics of this interconnection can be defined as follows: if a certain router in the telecommunications domain relates to a particular load in the electrical power domain via the *isaLoad* interconnection and the load is not fed, then the router is off." This rule is applicable to every router instance connected to a load instance (by a FONT relationship). Thus, the propagation of events between the two domains is enabled.

Figure 2 shows how rules, IONT instances and relationships (instances of the interconnections) permit the identification of critical infrastructure interdependencies. Domain experts develop a set of basic rules that express knowledge about cross-domain interconnections. These rules are used in an inference process with IONT instances and their relationships to simulate and analyze inter-domain interdependencies.

3.1.4 Gateways. Gateway components provide bridges between the KBS and simulators of specific domains. Well-defined gateways make it

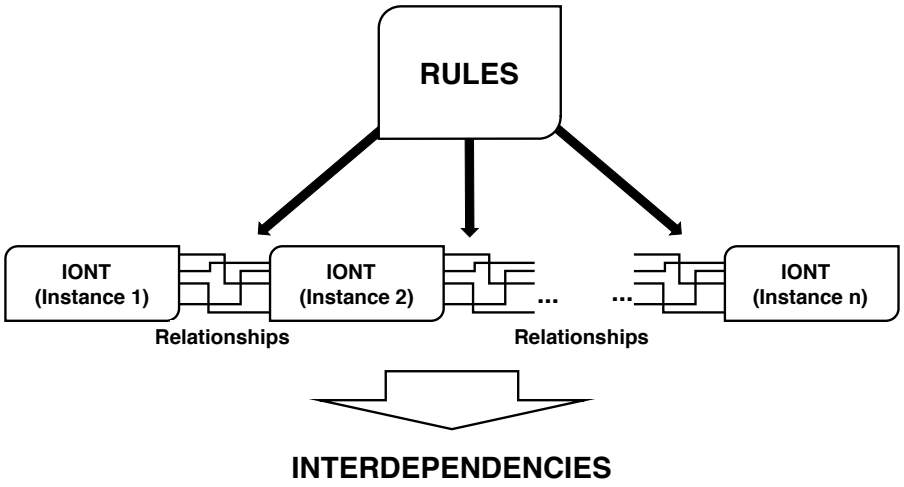

Figure 2. FONT rules.

possible to exploit the functionalities of the standalone simulators. Gateways also manage the input/output models of simulators in a federated environment.

A gateway has two components: a simulator model and an associative table. A simulator model is the simulator equivalent of an IONT instance. The domain IONT is an abstraction over a set of different simulator models, while an IONT instance has only one corresponding domain simulator model. For this reason a simulator model must be realized for each IONT instance in the KBS and for each simulator available for the domain.

An associative table exists for each IONT instance and its related simulator model. The table maps the objects defined in an IONT instance to specific simulator model objects.

3.2 KBS Development Process

The KBS development process has five steps: (i) MKIONT definition; (ii) domain IONT definition; (iii) IONT instantiation; (iv) FONT definition; and (v) FONT instantiation. The KBS development process starts with the MKIONT definition, which represents the highest abstraction level used in the KBS. As mentioned above, critical infrastructure IONTs are created using the MKIONT. To this end, the MKIONT critical infrastructure template can be used in two ways:

- **Derivative Template:** The first step in the IONT definition process is to import the MKIONT concepts and relationships. The IONT then specializes the MKIONT concepts and relationships (properties) to represent domain knowledge about the critical infrastructure.
- **Container Template:** The specific domain IONT is developed starting with existing standards and/or ontology definitions. Then, the defined

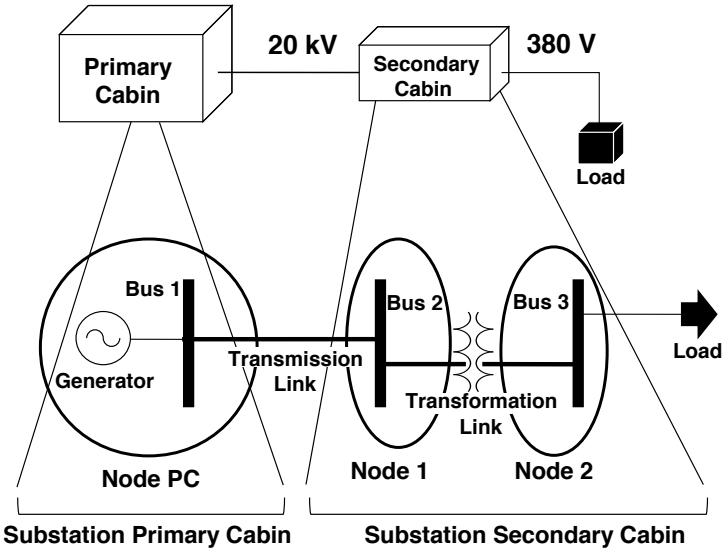

Figure 3. IONT instantiation.

IONT is made MKIONT compliant. In particular, the MKIONT template is used as a container for the IONT knowledge definition. Note that the inclusion of the IONT in the MKIONT template ensures the applicability of the interconnection template to permit the definition of semantic interconnection bridges with other critical infrastructure components in a federated simulation environment.

The development of a domain IONT requires deep knowledge of the corresponding critical infrastructure. For this reason, the DIESIS KBS development team should include both knowledge engineers and domain experts. We developed a railway infrastructure IONT in collaboration with RFI (Italian Railway Infrastructure) experts; and telecommunications and electrical power IONTs in cooperation with the appropriate domain experts and managers. A domain IONT is subsequently instantiated to effectively model a real critical infrastructure network (e.g., electrical power grid of a city district). The topology and requirements of a real critical infrastructure are translated into IONT objects by populating the IONT ontological schema.

Figure 3 shows an IONT instantiation corresponding to an electrical power distribution infrastructure. The infrastructure topology and specifics are represented using the ontology formalism harnessed by the IONT schema.

The FONT must include all the domain IONTs in a federated simulation environment. It supports the semantic interoperability of IONTs in the federation by defining cross-domain interconnections enriched with semantic rules. In this way, an interconnection template is realized as a set of relationships between concepts of different IONTs. Next, rules are defined to govern the interactions between interconnected objects. Thus, developing the FONT involves

three steps: (i) importing the domain IONTs; (ii) creating the interconnection template; and (iii) defining rules.

Finally, a FONT instance is created to serve as the core for a federated simulation session. Since DIESIS employs the Ontology Web Language (OWL) and Semantic Web Rule Language (SWRL), the acquired knowledge must be represented in terms of OWL classes, sub-classes, properties, sub-properties, restrictions on properties and SWRL rules. First, the concepts, relationships and constraints are expressed in natural language. Next, classes are created to represent the relevant concepts and sub-classes to express hyponym relationships. Then, properties are used to represent relationships between classes (object properties) and relationships between classes and datatypes (datatype properties). Eventually, restrictions on properties with respect to specific classes are defined. The ontology is then enriched with rules to enable a rule engine to infer new knowledge (assertions and facts).

4. Test Case

This section describes a test case related to the DIESIS Project that illustrates the flexibility and effectiveness of the proposed approach.

The proposed approach was used to define IONTs for the electrical power, telecommunications and railway transportation infrastructures. The IONTs were defined based on domain-specific standards. A FONT schema and rules were also defined to facilitate interoperability between the three domains from a semantic point of view. In particular, the FONT instance integrated the electrical power IONT with the telecommunications and railway IONTs to demonstrate how the proposed approach could be used to represent cross-domain interconnections.

This section presents a detailed description of the electrical power domain IONT, which was defined according to the IEC Common Information Model (CIM) Standard [8]. The CIM Standard, which is maintained as a UML model, enables applications software developed for electrical power transmission and distribution systems to exchange information about the configuration and status of electrical networks. The CIM Standard also defines a common vocabulary and ontology for the electrical power industry. The IEC 61970-301 Standard defines the core packages of the CIM with a focus on the needs of electricity transmission, where related applications include energy management, SCADA, planning and optimization systems. The IEC 61970-501 and 61970-452 Standards provide an XML specification of network model exchanges using RDF. The IEC 61968 Standard extends the CIM to meet the needs of electrical power distribution, where related applications include distribution management, outage management, planning, metering, work management, geographic information, asset management, customer information and enterprise resource planning systems.

Figure 4 presents the IONT created for the electrical power domain using the UML definitions of IEC COM objects [8].

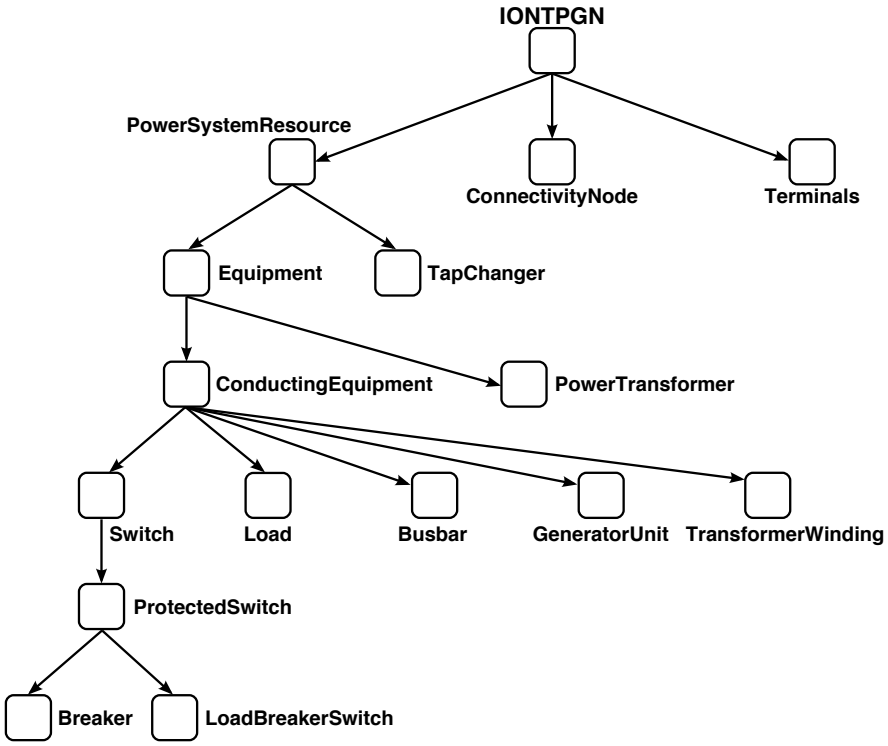

Figure 4. Example IONT domain.

Figure 5 shows the mappings of electrical power domain components and CIM objects. Interested readers are referred to [15] for the remaining OWL IONT classes and additional details. Note that the IONT defined for the electric power domain may be used to create models of real electrical power grids.

A FONT instance was used to integrate the electric domain IONT with IONT instances for the telecommunications and railway domains. Figure 6 shows an example where simple cross-domain interconnections are defined for these domains. Note that some components of the telecommunications and railway networks are fed through electrical network components. These components are represented as loads in the electrical network, and the interconnections are expressed using *isaLoad* OWL properties in the FONT instance. Other interconnections involve electrical network components that are telecontrolled using telecommunications network components. The scenario in Figure 6 was represented ontologically and formalized using OWL and SWRL. A rule engine such as Jess may be used to verify that the model addresses semantic interoperability (at least from the conceptual point of view). Our future work will focus on implementing gateways for each simulator to enable the federated simulation environment to manifest interdependency phenomena.

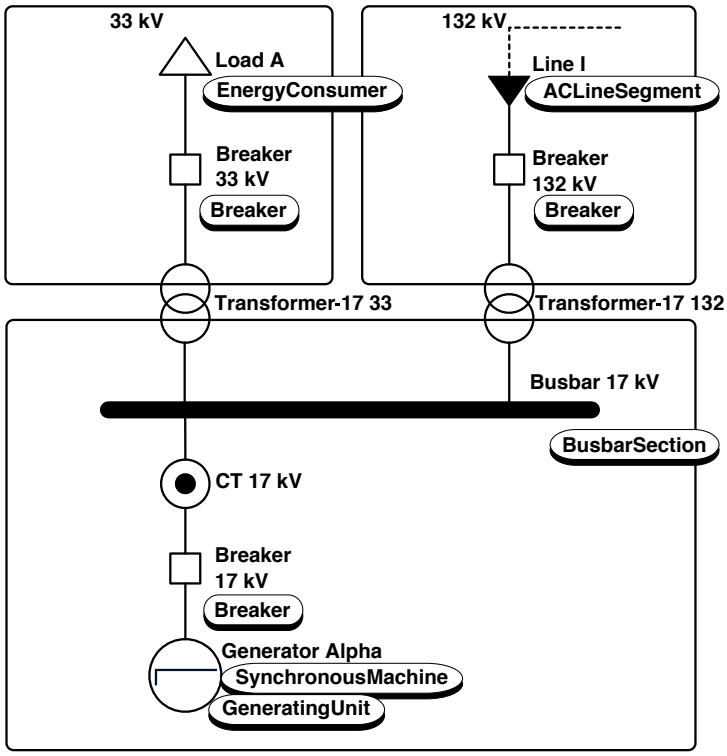

Figure 5. Mappings of electrical power domain and CIM objects [15].

5. Conclusions

The DIESIS Project is developing techniques and tools for characterizing critical infrastructures and their interdependencies. The DIESIS KBS is designed to create abstractions of critical infrastructure domains and to represent and formalize their parameters and dependencies. The KBS is intended to be used in a federated simulation environment to study the behavior of infrastructures and their components under different conditions and constraints.

The KBS defines the meta knowledge infrastructure ontology (MKIONT), which serves as a template for modeling the considered critical infrastructure domains via infrastructure ontologies (IONTs). The MKIONT template provides the semantic layer for the definition of the federation ontology (FONT), which provides semantic consistency for interconnections among IONTs and contains rules that govern the interactions among interconnected objects. To initialize a federated simulation, it is necessary to define a simulator model for each IONT instance. A gateway provides the bridge between an IONT instance and a simulator model using an associative table. The KBS can exploit a reasoning engine to manage ontologies and rules (defined using OWL and SWRL) to enable the semantic interoperability of the infrastructure domains involved

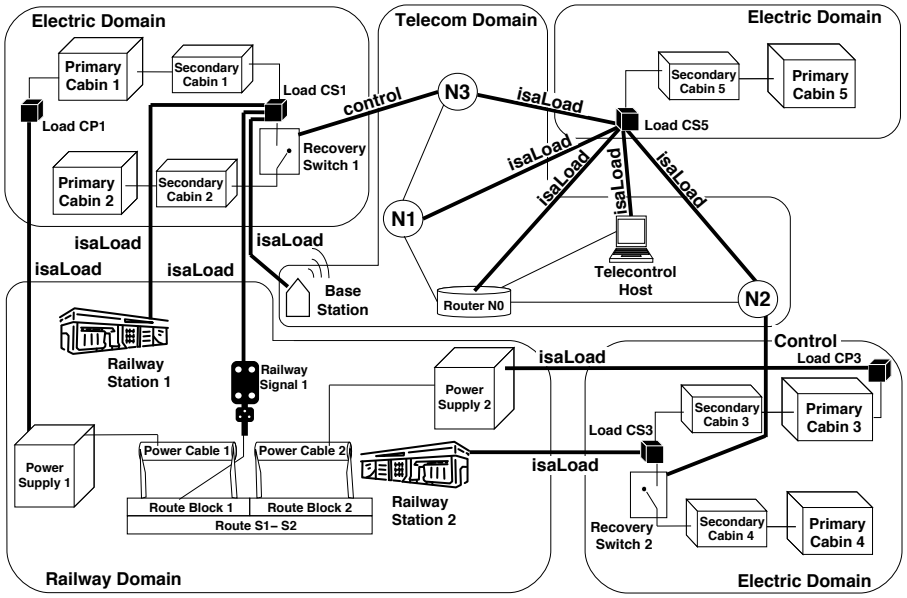

Figure 6. Example FONT instance.

in a simulation. The resulting federated environment will support complex simulation scenarios involving multiple infrastructures with different semantics and granularities.

Acknowledgements

This research was partially supported by the European Community Seventh Framework Programme FP7/2007-2013 under Grant 212830. The authors also wish to acknowledge the contributions of the DIESIS Project members, especially Erich Rome (IAIS), Erol Gelenbe (Imperial College), Eric Luiijf (TNO) and Sandro Bologna (ENEA).

References

[1] T. Brown, Multiple modeling approaches and insights for critical infrastructure protection, in *Computational Models of Risks to Infrastructure*, D. Skanata and D. Byrd (Eds.), IOS Press, Amsterdam, The Netherlands, pp. 23–33, 2006.

[2] E. Casalicchio, E. Galli and S. Tucci, Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures, *Proceedings of the Eleventh IEEE International Symposium on Distributed Simulation and Real-Time Applications*, pp. 182–189, 2007.

[3] A. Chaturvedi, A society of simulation approach to dynamic integration of simulations, *Proceedings of the Thirty-Eighth Winter Simulation Conference*, pp. 2125–2131, 2006.

[4] S. De Porcellinis, R. Setola, S. Panzieri and G. Ulivi, Simulation of heterogeneous and interdependent critical infrastructures, *International Journal of Critical Infrastructures*, vol. 4(1/2), pp. 110–128, 2008.

[5] D. Dudenhoeffer, M. Permann and M. Manic, CIMS: A framework for infrastructure interdependency modeling and analysis, *Proceedings of the Thirty-Eighth Winter Simulation Conference*, pp. 478–485, 2006.

[6] F. Flentge and U. Beyer, The ISE metamodel for critical infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 323–336, 2007.

[7] O. Gursesli and A. Desrochers, Modeling infrastructure interdependencies using Petri nets, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, pp. 1506–1512, 2003.

[8] International Electrotechnical Commission, IEC 61970 Energy Management System Application Program Interface (EMS-API) – Part 301: Common Information Model (CIM) Base, Edition 1.0, Geneva, Switzerland, 2003.

[9] Italian National Agency for New Technologies, Energy and the Environment (ENEA), The CRESCO Project, Rome, Italy (www.cresco.enea.it).

[10] R. Klein, E. Rome, C. Beyel, R. Linnemann, W. Reinhardt and A. Usov, Information modeling and simulation in large interdependent critical infrastructures, presented at the *Third International Workshop on Critical Information Infrastructure Security*, 2008.

[11] E. Luiijf, A. Nieuwenhuijs, M. Klaver, M. van Eeten and E. Cruz, Empirical findings on critical infrastructure dependencies in Europe, presented at the *Third International Workshop on Critical Information Infrastructure Security*, 2008.

[12] M. Maier, Architecting principles for systems-of-systems (www.infoed.com /Open/PAPERS/systems.htm), 2008.

[13] J. Marti, J. Hollman, C. Ventura and J. Jatskevich, Design for survival real-time infrastructures coordination, presented at the *International Workshop on Complex Network and Infrastructure Protection*, 2006.

[14] J. Marti, J. Hollman, C. Ventura and J. Jatskevich, Design recovery of critical infrastructures: Real-time temporal coordination, *International Journal of Critical Infrastructures*, vol. 4(1/2), pp. 17–31, 2008.

[15] A. McMorran, An Introduction to IEC 61970-301 61968-11: The Common Information Model, Technical Report, Institute for Energy and Environment, Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, United Kingdom, 2007.

[16] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Report No. INL/EXT-06-11464, Critical Infrastructure Protection Division, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[17] T. Rathnam, Using Ontologies to Support Interoperability in Federated Simulation, M.S. Thesis, School of Mechanical Engineering, Georgia Institute of Technology, Atlanta, Georgia, 2004.

[18] T. Rathnam and C. Paredis, Developing federation object models using ontologies, *Proceedings of the Thirty-Sixth Winter Simulation Conference*, pp. 1054–1062, 2004.

[19] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[20] Sandia National Laboratories, National Infrastructure Simulation and Analysis Center (NISAC), Albuquerque, New Mexico (www.sandia.gov /mission/homeland/programs/critical/nisac.html).

[21] Scalable Network Technologies, QualNet, Los Angeles, California (www .scalable-networks.com/products/developer.php).

[22] R. Setola, S. Bologna, E. Casalicchio and V. Masucci, An integrated approach for simulating interdependencies, in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 229–239, 2008.

[23] W. Tolone, E. Johnson, S. Lee, W. Xiang, L. Marsh, C. Yeager and J. Blackwell, Enabling system of systems analysis of critical infrastructure behaviors, presented at the *Third International Workshop on Critical Information Infrastructure Security*, 2008.