Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS

Rüdiger Klein, Erich Rome, Césaire Beyel,
Ralf Linnemann, Wolf Reinhardt, and Andrij Usov

Fraunhofer IAIS, Schloss Birlinghoven,Augustin, Germany,
{FirstName.LastName}@iais.fraunhofer.de

Abstract. Critical Infrastructures (CIs) and their protection play a very important role in modern societies. Today's CIs are managed by sophisticated information systems. These information systems have special views on their respective CIs – but can frequently not manage dependencies with other systems adequately.
For dependency analysis and management we need information taking the dependency aspects explicitly into account – in well defined relations to all other relevant kinds of information. This is the aim of the IRRIIS Information Model. It is a *semantic model* or *ontology* of CI dependencies.
This Information Model allows us to *integrate* information from different CIs – from real ones as in SCADA systems, or from simulations – in order to manage their interdependencies.
This paper gives an overview of the IRRIIS Information Model and the way it is used in the IRRIIS simulator SimCIP for the analysis of interdependent infrastructures. An example will be given to illustrate our approach.

Keywords

CI dependability, CI dependencies, information modelling, federated simulation, simulation environment

1 Introduction

Critical infrastructure systems are getting more and more complex. At the same time their (inter-)dependencies grow. Interactions through direct connectivity, through policies and procedures, or simply as the result of geographical neighbourhood often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries. In the years to come the number, diversity, and importance of critical infrastructures as well as their dependencies will still increase: advanced traffic management and control systems, mobile information services of any kind, ubiquitous computing, ambient intelligence – just to mention a few key words. Even classical domains like electric power networks will change their shape: more distributed generation facilities, intelligent consumers, smaller but interdependent distribution networks are examples of developments to be expected. The good news is that more or less all of these critical infrastructures provide and use many kinds of information during operation. This allows us to use this information also for interdependency analysis and management.

The modelling and analysis of dependencies between critical infrastructure elements is a relatively new and very important field of study [2]. Much effort is currently being spent to develop models that accurately simulate the behaviours of critical infrastructure [12, 14, 15].

Today, there exists already comprehensive knowledge about managing large and complex systems. There are sophisticated approaches dealing with optimal operation, management of interoperation, safety and risk management issues, etc. Different modelling and problem solving approaches are considered [2] including agent based modelling, game theory, mathematical models, Petri nets, statistical analysis, etc.

One of the main challenges for managing CIs and their dependencies comes from the *quite different kinds of behaviour* of critical infrastructures. Electrical power networks, traffic systems, water and oil pipelines, logistics, or telecommunication systems have their information and communication systems needed for their control – but at the same time they exist in the physical world, they behave according to the laws of physics, and they interact with their physical environment. The management of many critical infrastructures has to take both dimensions and their mutual interactions into account: the physical and the information and communication aspect.

For this purpose we need

- information models which are sufficiently expressive for CI dependency modelling and analysis – for the physical as well as the information and control aspects and their relationships;
- simulation techniques which allow us to describe the physical behaviour of the different systems, their control, and the resulting dependencies; and
- methods and tools supporting communication between CIs in order to manage their dependencies.

These are the main goals of the IRRIIS project. The modelling and simulation approach taken in this project to deal with CI dependencies will be outlined in this paper.

The paper is organized as follows: In Chapter 2 we motivate and describe our modelling approach to CI dependencies. How to use the IRRIIS models for the simulation of critical infrastructures will be explained in more detail in Chapter 3. In Chapter 4 we summarize our results and give an outlook to future research.

2 The IRRIIS Information Model

Today, the management and control of critical infrastructures depends to a large extend on information and communication technologies (ICT). They provide the "nerve systems" of these large infrastructures. There are highly sophisticated software systems allowing the stakeholders to manage, control, and analyse their systems under more or less every condition. What is frequently missing today is information related to dependencies to other systems: geographic neighbourhood information, physical or information and control dependencies, etc.

The information systems used to model the critical infrastructures tend to be very different. There is no common modelling approach. They are quite different for different domains, but even within the same domain different information modelling and processing approaches are used. This is quite natural considering the many different kinds of information and the various approaches and algorithms taken for these purposes.

Critical infrastructures are physical systems or based on such systems. Electrical power networks, traffic systems, or telecommunication systems exist in the physical world, they behave according to the laws of physics, and they interact with their physical environment. They process information about their state, and they may also exchange information with other systems in order to manage their dependencies. The dependency analysis of critical infrastructures has to take both dimensions and their mutual interactions into account: the physical and the information and communication aspect.

Consequently, a key issue is to establish information models and simulation techniques which take exactly these issues into consideration: the components and systems, their behaviours, events, actions of control, risks, etc. This will help to manage critical infrastructures more effectively and efficiently, and it will improve information interchange between those information systems dealing with control of different critical infrastructures.

The main point is to bring all *dependency* related information together with all other kinds of information necessary to manage and control the various kinds of critical infrastructures. We need an information model which is

- as general as necessary in order to represent the commonalities of critical infrastructures for dependency analysis independent from their concrete type,
- sufficiently *expressive* in order to represent the many different kinds of related information, and
- which is well defined with *clear semantics* in order to be manageable by the different kinds of information systems working with them.

Following established *semantic* modelling techniques [4] we build the IRRIIS Information Model as an *ontology* [11] of Critical Infrastructures. In order to be as general as necessary and at the same time as adaptive as needed for the different kinds of CI the IRRIIS Information Model is built on three levels of generalization:

1. the *Generic* Information Model (GIM): it is the top level ontology of Critical Infrastructures. It is based on the assumption that there is a common core information model for critical infrastructures and their dependencies. Whatever the CI to be modelled and its dependencies are: for the purpose of CI dependency analysis and management it will be described in terms of this

IRRIIS Generic Information Model and its domain specific extensions (see below). This common model provides the basis for communication between different CIs. It provides a common semantically well-defined vocabulary as pre-condition for this communication. It captures the basic physical structure of the CI with its components and systems and their connections, their behaviours on an appropriate level of abstraction, the services they provide, and events, actions and associated risks. In this way it is sufficiently expressive to capture all dependency related information.
2. The *domain specific* information models: they adapt, specialize and extend the Generic Information Model according to the special needs of the various domains (like electrical power networks, traffic systems, or telecommunication nets). They contain the specific types of components and their behaviours as specializations of the more general concepts introduced in the GIM.
3. The instance level models: this third layer describes the *concrete* critical infrastructures in terms of the respective domain specific information model as instantiations of the concepts and relations defined in this model.

2.1 The IRRIIS Generic Information Model

These three models are, of course, tightly related to each other – to be shown in more detail now.

The Static Information Model The Static Model is the basic ontology describing the main concepts, their relations and attributes (see fig. 2) needed for CI modelling [1].

Components and systems:
describe the structure and topology of a CI. Components and systems can be described by a set of relevant attributes (not shown here). In the domain model more specific sub-classes of systems, components and attributes can be introduced.

Part Structures:
Systems have parts – described by the hasPart relation. Its terminal elements are components.

Connections:
Systems and components are connected to other systems and components. (Because connections form a central element in typical CI models they are described by classes with attributes etc. – not just as relations). There can be *different types* of connections like physical and control connections in the domain models (see below).

[1] The UML diagrams are just used as illustrations of the model. UML does not provide the necessary semantic precision.

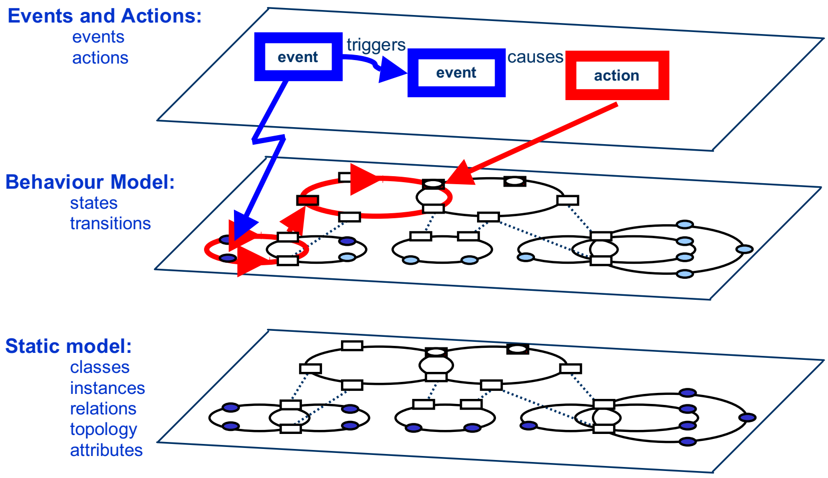

Fig. 1. An overview of the three layers of the IRRIIS Generic Information Model: the static model, the behaviour model, and the event and action layer.

Services:
Systems and components provide services to other systems/components, and systems and components need services in order to work correctly. This is a useful and attractive abstraction providing a lot of flexibility for modelling – especially for the action of systems and critical infrastructures. In parts of the model or in the whole model we may use services as the basic level of description – omitting the component layer.

Effects:
Services may have effects. An effect is described as resulting in certain values for attributes of involved components or services (heating, cooling, ...). A connection may be used to mediate some services – that's a way how actions of systems and components can be described in IRRIIS.

Dependencies:
A connection causes a dependency. Due to the different types of connections there may be different types of dependency. Dependencies may be characterized in more detail by various attributes.

Geospatial attributes:
Components, systems and events (see below) may be described by their geospatial locations. Locations and areas are related to each other through geospatial contained-in, neighbourhood, or distance relations.

Systems and services Every service is provided by a system/component. In the same way a system/component needs services in order to work correctly. The failure of any of these input services results in a failure of the component or systems – with the consequence that the services normally provided by it will also fail.

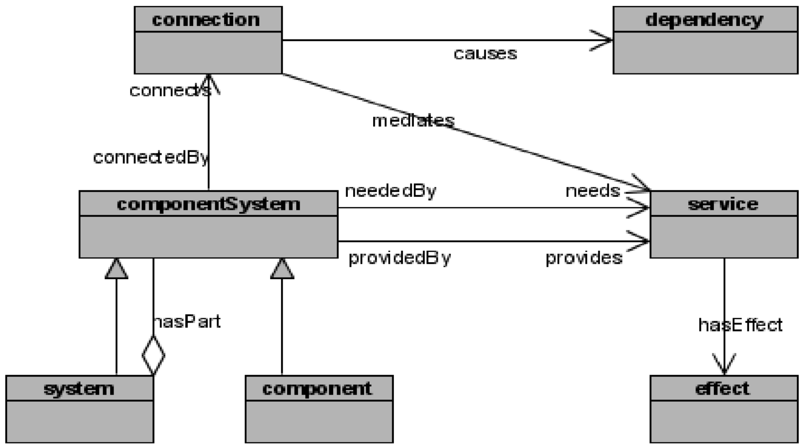

Fig. 2. The core of the IRRIIS Static Model: components, systems, services and connections.

A service oriented modelling is an adequate abstraction in those cases where a system or CI provides this service in different ways to other systems/CIs [3].

The IRRIIS Behaviour Model The key elements in the IRRIIS behaviour model are states and transitions (Fig. 3).

States:
Components/systems, services, and connections can have states. An entity is in a certain state either if explicitly given (like 'broken' or 'switched-off') or if the criteria defining this state are fulfilled by this entity (see below). The states are defined according to the respective entity type, i.e., components of a certain type can have different states then other component types or services. Which states are defined depends on the application – the IRRIIS model does deliberately not provide any restrictions here. All we need is a finite set of states.

States and Services:
The state of a service is determined by the state of the component or system which provides this service. The state of a component or system depends on the state of the services it needs.

Transitions:
States (as discrete entities) are related to each other via transitions. States and transitions together form finite state machines for the entities they apply to. The transitions do not have to be deterministic – i.e., we may have probabilistic state machines. We may also assign temporal aspects to such transitions (duration, delay, etc.).

Propagation of state transitions:
The state of a system/component depends on the states of the services it

needs or on the states of other components/systems it depends on. If one of those states is changed this transition will be propagated to the depending systems/components.

Temporal aspects:
state transitions are not necessarily instantaneous. They can occur with a certain delay. An overloaded power transmission line will withstand this overlaod for a while (depending on the amount of overload). Only then it will break.

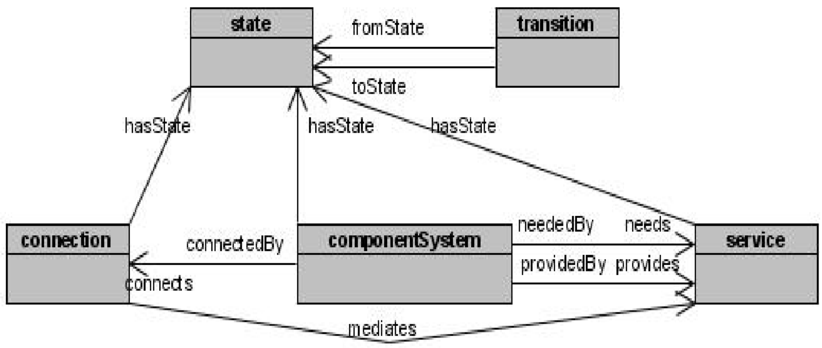

Fig. 3. The IRRIIS Behaviour Model with states and transitions.

States and Attributes The states of a component, system, or service can be related to its physical attributes: in order to be in normal operational state a system for instance has to fulfil some constraints on its attributes. In this way states can be *classified* according to attribute values using classification constraints. These constraints are part of the domain model and are applied to each instance.

States may be changed directly by events or actions – without explicit reference to physical attributes. For instance, a system's state may change when the state of one of its components changes. Or we simply say that a component is broken without saying why and in which way.

The definition of states is a key issue in an IRRIIS model. It may be adequate for an IRRIIS application just to discriminate between two states like "working" and "out of work". In other cases we may need much more fine-grained states (and transitions between them). For instance, a system may still provide the services it is responsible for but with the restriction that some of its sub-systems do not work at the moment and that the built-in redundancy or emergency systems already took over responsibility for these services (resulting in a higher risk of failure).

2.2 The IRRIIS Events and Actions Model

The IRRIS Generic Information Models contains the concepts needed to describe scenarios, events, actions, etc. – and how these concepts are related to the other main information categories.

Events:
Events trigger state transitions. They are either external or internal events. An external event is something happening outside of the respective system or component changing its state. An internal event is a state transition within one of the parts of a system.

Actions:
are like events but performed deliberately by a certain agent in order to achieve a certain state change in a certain system/component.

Scenarios:
A scenario is a sequence of events and actions. They are ordered by time, and the events and actions in a scenario may be related to each other by causal relations. They can also be independent from each other (just happening by accident) – thus allowing us to model a large variety of different types of scenarios and of analyzing in which way they affect the dependent critical infrastructures. Scenarios may contain events coming from outside, and events resulting from the evolution of the system. Actions (see below) are similar to events – with the exception that they are executed deliberately as reaction to a certain state, pursuing a certain goal (a state to be reached) and following a certain strategy or policy.

Temporal aspects:
Events and actions can be described in their temporal aspects: when they occur, if they are instantaneous or if they have a duration, etc.

2.3 The IRRIIS Domain Models and Instance Models

The IRRIIS Generic Information Model as top level CI ontology contains the main concepts and relations for modelling large Critical Infrastructures and their dependencies. It provides the basis for the concrete domain models which contain those concepts and relations needed to model domains like electrical power grids or telecommunication networks. These concrete domain concepts and their relations are *specializations* of the generic concepts defined in the GIM. For instance, in the electrical power grid domain we may have concepts like power station, transformer, and consumer as special categories under the general concept "component/system", or we may have special relations like 'controls' as specialization of the general connection concept in the GIM.

The IRRIIS domain models will then be instantiated in order to model concrete systems like the ACEA electrical power network in Rome or the Telecom Italia communication network in central Italy.

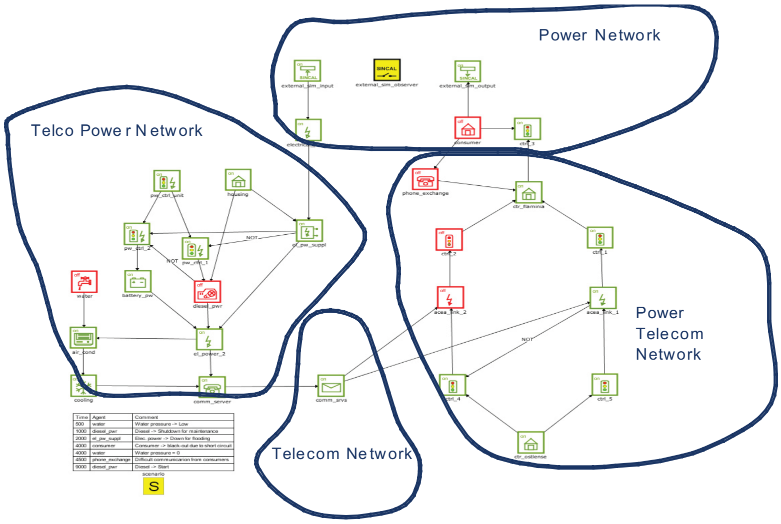

Fig. 4. Parts of the instance level models of the simulated networks and their dependencies.

3 The Simulation of Dependent Critical Infrastructures

3.1 The IRRIIS Simulation Environment SimCIP

In the previous chapter we outlined the IRRIIS Information Model. Now we will explain in which way these models will be *used*.

There are mainly two ways to deal with CI dependency: the management of *real* critical infrastructures or the *simulation* of such CIs and their dependencies.

The simulation approach will need a simulation environment which allows us to simulate the behaviour of the systems to the necessary granularity and precision. In IRRIIS, the simulation environment SimCIP has been developed for this purpose. It is built on our agent based simulation system LampSys which provides important features for CI simulation like encapsulation, modularity, states and transitions, quite different temporal behaviours, and rule based propagation of state transitions along dependency networks. SimCIP can be connected through a generic simulation interface to other external simulators for federated simulation (see the next chapter).

3.2 Federated Simulation

Obviously, critical infrastructures can be quite different and behave in quite different ways. There is a whole bunch of highly sophisticated techniques used to simulate such diverse systems – depending on the type of the systems, their behaviours, and the purposes of the simulation. Typically these simulations do not consider dependencies between systems. That's exactly the place where the

IRRIIS Information Model and its usage come into play. The IRRIIS approach can be characterized as a federated simulation approach: SimCIP takes the simulations of each critical infrastructure and integrates them – taking in this way the dependencies between them into account.

The IRRIIS Information Model provides the information "glue" for the federated simulation. SimCIP allows us to relate the results from simulation of one CI in a *standardized* way to the simulation results of another depending CI by mapping all native simulation results to the unifying IRRIIS Information Model.

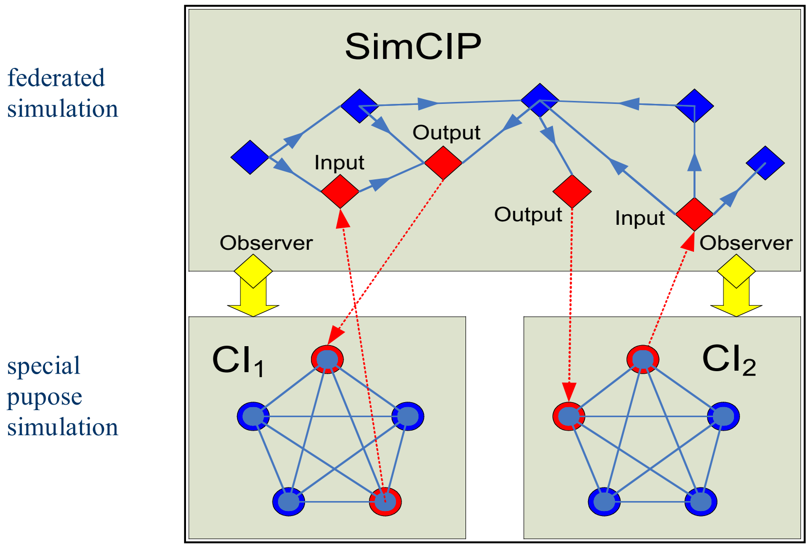

Fig. 5. Federated simulation in IRRIIS: the simulation tool SimCIP using the IRRIIS Information Model for information integration and native simulation tools for Critical Infrastructures.

Though the critical infrastructures are different they communicate through the exchange of information about state transitions and events with each other. This information is formulated in the IRRIIS Information Model allowing all CIs to get the meaning of this information from other CIs. The simulation of the system behaviour of the involved critical infrastructures is combined (or federated) to an overall simulation of dependent critical infrastructures by using the native simulations of each CI and the state transition and event chain mechanism of the IRRIIS simulation.

Two points should be highlighted here:

- The expressive information model of IRRIIS allows us to represent all relevant information (systems, components, their part structure and dependencies, their behaviours, etc.) in an *expressive*, *adequate* and *transparent* way.

– The classification of behaviour results from each CI simulation in terms of states, state transitions, and events is the main “interface” between native CI simulations and IRRIIS’ dependency simulation.

In our example federated simulation by SimCIP works as follows:

1. An event in the power network changes the state of the component “power supply” from ‘on’ to ‘broken’.
2. This state transition is propagated by SimCIP to the native power network simulator.
3. This simulator calculates the new power distribution of the power network.
4. The results are taken by SimCIP and used for state classification on the power network.
5. Every state change of a component/subsystem in the power network which has a dependency relation to a component in one of the other networks is propagated by SimCIP to this depending component.
6. The state transition of this component is now propagated by SimCIP to the native simulator of this network.

This propagation can stop after a while in a new stable state (for instance, if sufficient redundancy of a network prevents it from an outage), it can result in a cascade and outage, or appropriate measures may be taken stopping this propagation.

The main point here is that SimCIP integrates the native simulations of the respective critical infrastructures through the common IRRIIS Information Model.

4 Summary and Outlook

The IRRIIS Information Model introduced here provides the basis for information modelling and simulation for CI dependency analysis and management. It is formulated as an ontology providing an expressive framework with clear semantics for the different kinds of information required. As a lingua franca of dependencies it provides the communication platform for exchanging dependency related information between different critical infrastructures even from different sectors and domains.

The model introduced here is a first approach which will be further elaborated. Especially, we plan to gather more experiences regarding the expressiveness of the IRRIIS Information Model and the granularity of the domain models (which states, which dependencies, how to model risks, etc.) required.

At the moment, event and action chains are specified manually by domain experts. A logical next step is to generate such event action chains automatically in a systematic way. This allows us to analyse dependencies more comprehensively and systematically.

Acknowledgement

The research described in this paper was partly funded by the EU commission within the 6th IST Framework in the IRRIIS Integrated Project under contract No 027568. The authors thank all project partners for many interesting discussions which greatly helped to formulate the approach described here.

References

[1] The IRRIIS European Integrated Project: www.irriis.org
[2] P. Pederson et al.: Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Technical Report, Idaho National Lab, August 2006.
[3] U. Beyer, F. Flentge: Towards a Holistic Metamodel for Systems of Critical Infrastructures, in: ECN CIIP NEWSLETTER OCT/NOV 2006.
[4] Steffen Staab, Rudi Studer (Eds.): Handbook on Ontologies. International Handbooks on Information Systems Springer 2004.
[5] Simona Bernardi and Jose Merseguer: A UML Profile for Dependability Analysis of RealTime Embedded Systems, in Proc. WOSP'07, Feb. 2007, Buenos Aires, Argentina
[6] Alessandro Annoni: Orchestra: Developing a Unified Open Architecture for Risk Management Applications, in: Peter van Oosterom et al. (eds.): Geo-information for Disaster Management, Springer, 2005.
[7] Walter Schmitz et al.: Interdependency Taxonomy and Interdependency Approaches, The IRRIIS Consortium, Deliverable D.2.2.1., June 2007.
[8] Vladimir Alexiev et al: Information Integration with Ontologies, Wiley, Sussex, 2005.
[9] Tarun Rathnam: Using Ontologies To Support Interoperability In Federated Simulation, M.Sc. thesis, Georgia Institute of Technology, Atlanta, GA, USA, August 2004.
[10] Borst, W., Construction of Engineering Ontologies. 1997, Centre of Telematica and Information Technology, University of Tweenty: Enschede, The Netherlands.
[11] T. Gruber: Toward Principles for the Design of Ontologies Used for Knowledge Sharing, in: Proceedings of the International Workshop on Formal Ontology, Padova, Italy, 1993.
[12] D. Cerotti, D. Codetta-Raiteri, S. Donatelli, G. Dondossola, F. Garrone: Representing the CRUTIAL project domain by means of UML diagrams, in: Proc. CRITIS 2007, Malaga, Spain, Oct. 2007.
[13] W. Kröger, Reliability Engineering and System Safety, Reliability Engineering and System Safety 93 (2008) 1781– 1787, Elsevier.
[14] H. J. Min, W. Beyeler, T. Brown, Y. J. Son, and A. T. Jones: Toward modeling and simulation of national CI interdependencies, IIE Transactions (2007) 39, 57–71.
[15] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, D. Coury: EPOCHS: A Platform for Agent-Based Electric Power and Communication Simulation Built from Commercial Off-The-Shelf Components, IEEE Transactions on Power Systems, Vol. 21, No. 2, p. 548–559, May 2006.