Information Modelling and Simulation in Large Dependent Critical Infrastructures – An Overview on the European Integrated Project IRRIIS

Rüdiger Klein*

Frunhofer IAIS, Schloss Birlinghoven, D-53757 Sankt Augustin, Germany
{Ruediger.Klein}@IAIS.Fraunhofer.de

Abstract. IRRIIS ("Integrated Risk Reduction of Information-based Infrastructure Systems") is a European Integrated Project started in February 2006 within the 6^{th} Framework Programme and ending in July 2009.

The aim of IRRIIS is to develop methodologies, models and tools for the analysis, simulation and improved management of dependent and interdependent Critical Infrastructures (CIs). Middleware Improved Technology (MIT) will provide new communication and information processing facilities in order to manage CI dependencies.

This paper will give an overview of the IRRIIS project to outline these methodologies, models, and tools. Scenarios of depending CIs developed in IRRIIS are used to validate our approach and to demonstrate the usefulness of our results.

Keywords: critical infrastructures, dependability, CI dependency, information models, federated simulation, simulation environment, improved CI communication and management.

1 Introduction

Critical infrastructures (CIs) are getting more and more complex. At the same time their dependencies and interdependencies 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.

The EU Project "Integrated Risk Reduction of Information-based Infrastructure Systems" (IRRIIS) is a European Project within the 6^{th} Framework [1]. It started in February 2006 with a duration of 3.5 years including 16 partners from nine European countries from industrial companies like Siemens, Telecom Italia,

* Project coordinator of the EU Project IRRIIS.

R. Setola and S. Geretshuber (Eds.): CRITIS 2008, LNCS 5508, pp. 131–143, 2009.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

Red Electrica, ACEA, and Alcatel-Lucent, research organisations like Fraunhofer, VTT, TNO, IABG, and ENEA, universities like City University London, ETH Zürich, and Telecom Paris Tech, and SMEs like AIS Malta and Grupo AIA in Barcelona.

Modelling and Simulation of Critical Infrastructures is of course not a new topic. For recent overviews on this subject see, for instance, [2,3,4]. The IRRIIS project has a clear focus on enhancing substantially the dependability of *dependent* large complex Critical Infrastructures (CIs) by introducing appropriate middleware based communication technologies between CIs. The key idea behind the IRRIIS project is the following: if CIs depend on each other, they have to be able to communicate with each other in order to manage these dependencies. The challenge is that these Critical Infrastructures are quite different in their structure, behaviour, and dependencies. Depending CIs form a network of networks. In order to provide valuable support for their management and control we have to describe this network of networks on an appropriate level of *technical detail*. The communication between depending CIs will allow us to use information from one CI to operate the depending CI. This will be facilitated by so-called Middleware Improved Technology (MIT) including a communication backbone and MIT add-on components to process information from/to depending CIs.

In order to develop and optimise this information interchange, appropriate simulation techniques are needed. They have to provide the necessary modelling granularity and diversity in order to model and simulate the *behaviour* and *control* of large, complex, dependent, heterogeneous networks of networks. This is the second research focus of the IRRIIS project. It is closely related to MIT and enables its development.

IRRIIS' main objectives can be summarized as follows:

- to determine a sound set of public and private *sector* requirements based upon scenarios and related data analysis;
- to design, develop, integrate and test communication components suitable for preventing and limiting cascading effects as well as supporting recovery and service continuity in critical situations;
- develop, integrate, and validate novel and advanced modelling and simulation tools integrated into a simulation environment for experiments and exercises; and
- to validate the functions of the middleware communication (MIT) components using the simulation environment and the results of the scenario and data analysis.

Because of their central importance and their typical dependencies electrical power infrastructures and their supporting telecommunication infrastructures are chosen as example test cases.

The IRRIIS approach is based on the analysis of vulnerabilities of large complex CIs and on the knowledge CI stakeholders have acquired about management and control of their systems [5].

Novel types of ICT systems are tested and validated by applying the IRRIIS simulation environment for comprehensive experiments.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

The IRRIIS project is a highly interdisciplinary effort. It brings researchers from quite different domains together: industrial stakeholders from power and telecommunication domains, experts in dependability analysis, and specialists in various modelling and simulation techniques. The challenge is to develop a *coherent* approach including methodological, modelling and simulation aspects. Scenarios and experiments are developed and used to validate and optimise the approach.

This paper will give an overview of the results reached so far within this project. We start with an overview on methodological issues relevant for dependency modelling and management of Critical Infrastructures (section 2). The models used in IRRIIS are summarized in secion 3. The SimCIP simulation tool developed in the IRRIIS project for the simulation of Critical Infrastructure dependencies is outlined in section 4. Section 5 contains a brief introduction to the MIT methods and tools created in our project. Section 6 is devoted to the scenarios used in IRRIIS, followed by a summary and outlook in Section 7.

2 The IRRIIS Methodology

Methodological work and empirical studies done in IRRIIS resulted in an increased understanding of dependencies and interdependencies between CIs [6]. Dependency is typically *not* an on/off relationship as most models up till now assume, but a relationship of qualities (e.g. pressure, biological contamination level) which have specific decay and restore behavior[1]. These empirical studies underline the growing importance of CI dependencies. This improved understanding of CI dependencies provides the ground for our methodology, our modelling approaches, the tools developed, and the prepared scenarios and experiments.

Fig. 1 shows a typical case for the methodology developed in IRRIIS which is also used as one of our test cases: the so-called Rome scenario (see also Section 6). Power and telecommunication systems are depending in this scenario on each other in different ways. Power networks have their own telecommunication networks connecting power components with SCADA control centres. In parallel, they use additional external telecommunication networks to avoid building expensive proprietary information infrastructures or simply as back-up systems to their own networks. The other way round is also of a very high relevance: telecommunication networks need electrical power typically coming from standard power networks. Hence, these power systems have to provide the needed energy to maintain their own back-up power systems which allow them to survive a certain amount of time till the standard energy sources work again.

[1] Dependencies and Interdependencies: Analysis of empirical data on CI dependencies all over the world show that the mutual dependencies or interdependencies are seldom reported in the news and in CI disruption incident reports. Only three cases worldwide with interdependencies in over 1050 CI outage incidents with dependencies have been found [6].

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

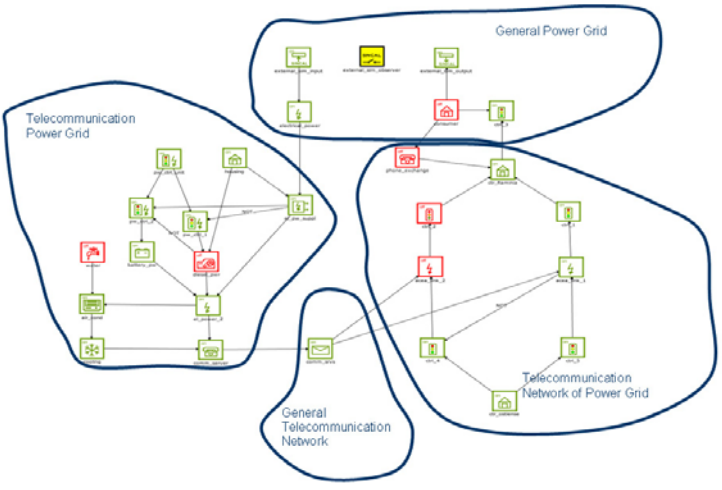

Fig. 1. The example Rome scenario: it shows four power and telecommunication networks in Rome with some of their components and their dependencies

This is a typical case for CI dependencies. Networks provide and need services from each other. This can happen within the same domain (power-power, telecommunication-telecommunication), or between different domains (for instance power-telecommunication). Correspondingly, we address different types of dependencies: physical, cyber, logical, and geographic [7].

Today, the management and control of critical infrastructures depend 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 stakeholders to manage, control, and analyse their own systems under more or less every condition. What is frequently missing today is information about other systems the respective network depends on in one or the other way. But these dependencies are of growing importance: not just for dependability but also for economic efficiency.

There are a number of reasons for the problems related to dependencies between CI. Every network is different. This is true for networks of the same domain (power, telecommunication, etc.), and of course also for CIs from different domains. Consequently, each network has its own approach to information management and control.

- For a long time, Critical Infrastructures have been relatively stable and homogeneous. There was one national telecommunication network built over decades, and there was one national power transmission system with stable structures. Today, we encounter a growing diversity within these domains from a technical perspective and from an organisational/commercial one.
- Information and communication techniques are key issues in this context today as enablers and as new risk factors. The World Wide Web, mobile and

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

IP based communication services, and the upcoming Web of Things build a ubiquitous ICT infrastructure which enables completely new approaches to manage Critical Infrastructures. It also generates new risk factors. A loss of communication within a CI may disable its function partially or completely. The ICT systems are highly interconnected Critical Infrastructures on their own with vulnerability against failures and attacks.

The information systems currently used in critical infrastructures tend to be very different. There is no common modelling approach. The ICT systems used for the management and control of CI are highly sophisticated and highly adapted to the special needs of the respective network. The challenge for the IRRIIS project is to provide new approaches to information modelling, information processing and simulation as well as to communication between CIs which enables them to manage their dependencies.

3 Models in IRRIIS

In order to achieve the main goals of CI dependency analysis and management we need models which allow us to capture the essential aspects of Critical Infrastructure behaviours and their dependencies. This can be done on different levels of abstraction.

In IRRIIS, we use two kinds of models:

- Four different network analysis approaches (see Subsection 3.1) which *abstract away* many technical details of Critical Infrastructures and allow us to run complex simulations [8]:
  - the NAT approach;
  - the Preliminary Interdependency Analysis (PIA) with the Möbius tool;
  - the Leontief approach; and
  - the bio inspired dynamic network analysis.
- A more detailed technical modelling and simulation which allows us to describe depending Critical Infrastructures as a network of networks including the services they provide to each other, their logical dependencies, and the temporal aspects of their behaviours. This modelling approach, called the IRRIIS Information Model is described in more detail in Subsection 3.2 and in [9]. The simulation of IRRIIS Information models with the SimCIP simulation tool is outlined in Section 4.

3.1 Network Models in IRRIIS

To analyse the impact of dependencies on Critical Infrastructure operability a number of models within IRRIIS, at various levels of granularity, have been developed. These range from *high-fidelity, scenario-specific* models, used within the SimCIP simulation environment (see next subsection 3.2), to models based on services or the physical topology of networks. Within these boundaries there are a number of models, with various objectives, that have been applied. These

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

medium and *low fidelity* models, as a consequence of their level of abstraction, have some advantages; they allow us to study very large systems and the models take into account uncertainty inherent in analysing large scale Critical Infrastructure operation. Uncertainty in these systems may arise either from a lack of available system data or the complexity of these systems. In [9] we have classified these models, distinguishing between models that give *generic* and *specific* results. Within this section we shall briefly discuss these two types of models.

Generic models give results that are applicable to a wide class of situations while *specific* models give results based on the functional and topological peculiarities of particular networks. Typically, the generic models are used to test hypotheses that depend on general properties of the modelled network while specific models help to either anticipate the behaviour, or assess the properties, of concrete systems. Generic models include *Leontief-based* model [10], *Generic cascading* model [10], *common-mode failure* model [11], and *stationary/dynamic cascading* models [11]. Specific models are either based on functional relationships between/within infrastructures or physical network-topologies. Functional models are employed in *Preliminary Interdependency Analysis* (PIA) [10]. Also, the *Implementation-Service-Effect* (ISE) [12] model is an example of a functional-based model used within IRRIIS. Alternatively, a study of the evolution of the French power grid [11] uses models of specific physical network topologies. This is also the case for a stochastic analysis of interacting networks carried out within IRRIIS [10].

The results of these models are complimentary; service-based modelling provides information about dependencies that are different from modelling based on network topology. These, in turn, are complimentary to the detailed SimCIP-based models, which focus on simulating network operation under specific scenarios. Furthermore, some of these models may be used as part of an effort to validate MIT-related hypotheses (e.g., assumptions, made by the designers of an MIT component, about the long-run consequences of MIT in operation).

3.2 The IRRIIS Information Model

Many different kinds of information are relevant for CI dependency analysis, modelling, and simulation. Because dependencies exist between quite different systems, information exchange between them about critical situations, risks, vulnerabilities needs a system independent approach. Proprietary information approaches are not sufficient for this purpose. We need a generic information model as a reference model or *lingua franca* for communication between CIs [9, 13]. This reference model allows us to exchange information between different systems in a way that the *meaning* of this information is "understood" by all stakeholders and their ICT systems independent from the concrete kind of CI.

In order to achieve the necessary granularity and precision of our models for detailed technical simulations and for the analysis of dependencies based on this simulation we need an *expressive* information model [9, 19, 20]. This information has to be processed in different kinds of ICT systems so we need models with clear *semantics*. For this purpose we build the IRRIIS Information Model on

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

semantic modelling techniques [14]. The IRRIIS Information Model can be seen as an *ontology* [15] of Critical Infrastructures and their dependencies [20]. It is described in detail within these proceedings [1a].

4 The SimCIP Simulation Tool

SimCIP (*Sim*ulator for *C*ritical *I*nfrastructure *P*rotection applications) is an agent-based simulation system based on the LAMPS (*L*anguage for *A*gent-based *S*imulation of *P*rocesses and *S*cenarios) language and the LAMPSYS agent simulation framework both developed at Fraunhofer IAIS [16, 17, 18]. It provides the main modelling and simulation platform for Critical Infrastructures and their dependencies. It allows us to simulate different scenarios on different CI models. The integrated MIT tools provide the communication capabilities between different Critical Infrastructures as one of the main goals of the IRRIIS project.

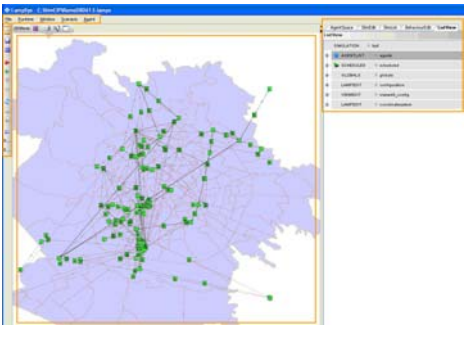

Fig. 2. SimCIP GUI

The IRRIIS Information Model (see Subsection 3.2) is implemented as a SimCIP model. This SimCIP modelling environment is completely agent based. CIs differ to a large extend in their structure, the types of components they have, their behaviours, etc. The agent based modelling and simulation capabilities of SimCIP enable us to model these quite different CIs in a coherent and transparent way.

SimCIP comes with an sophisticated GUI (see fig. 3) and enables the user to create, edit, modify, copy, rename and delete agents as well as to functionally connect them to each other. These agents represent the components of critical infrastructures, their attributes and their behaviour. Agents belong to different types with different attributes and behaviours. Their connections can also be of different types allowing us to describe different kinds of dependencies. In this way SimCIP allows us to build complex network of network models of depending Critical Infrastructures within one SimCIP simulation model.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

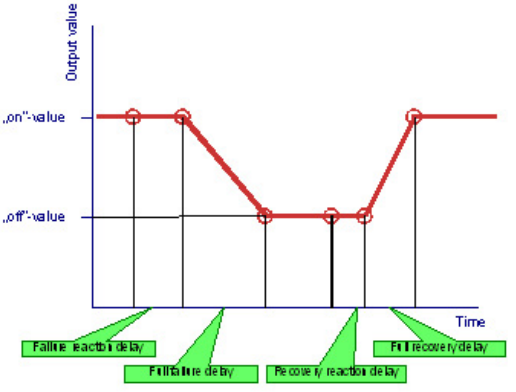

Fig. 3. Behaviour of an agent

Events allow us to trigger state changes of components (agents) from outside. These changes are propagated in the agent network and allow us to simulate the network behaviour. Events can be collected in complete scenarios where different events happen at defined points in time affecting various components in our network model.

The behaviour of agents can be characterised by various temporal aspects: delays, declines, etc. (see fig. 3). The state of an agent can depend on states of related agents. A change of an agent's state will be propagated according to these relationships within the network. This allows us to model complex Critical Infrastructures of quite different types including their dependencies. The simulation of network behaviour can include quite special algorithms (for instance, routing in telecommunication networks, or load distribution in power networks). It is not feasible to re-implement such special behaviours within SimCIP. By this reason SimCIP supports federated simulation: external special-purpose simulators can be integrated with SimCIP. In this way their simulation capabilities can be used within the overall simulations of SimCIP. The expressive IRRIIS Information Model providing the basis for SimCIP allows us to use a very flexible semantic approach to federated simulation.

5 Middleware Improved Technology

Middleware Improved Technology (MIT) is one of the key concepts behind IRRIIS. Today, Critical Infrastructures need highly sophisticated information and communication technologies for their management and control. But though we encounter a growing importance of dependencies from and to other Critical Infrastructures there is nothing comparable on the control level. MIT shall close this gap: by providing a sophisticated communication platform for exchange of information between Critical Infrastructures, and by providing appropriate MIT add-on components to manage this information.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

The main MIT components developed in IRRIIS are

- the MIT Communication Tool allowing different CI to exchange information (see Subsection 5.1);
- the Risk Estimator (RE) which enables the operators of a Critical Infrastructure to process information from depending CI and to send critical information from its own network to depending CI (Subsection 5.2); and
- the CRIPS decision support tool ("CRIsis management and Planning System", see Subsection 5.3).
- TEFS (Tools for Extraction of functional status) a simple data interface to SCADA and control systems, and
- IKA (the Incident Knowledge Analyser[2]).

All MIT components are integrated into the SimCIP simulation platform in order to enable experiments on scenarios. In this way we will validate how well they fit the needs of improved communication between depending Critical Infrastructures.

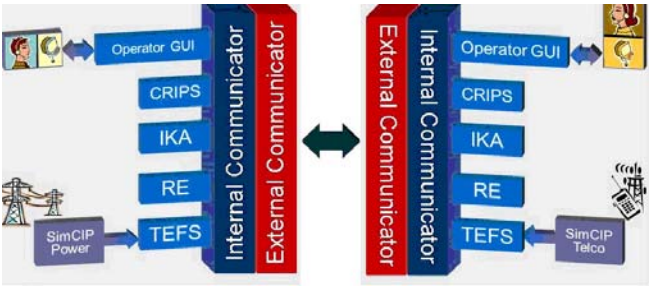

Fig. 4. Overview of the MIT Architecture: each Critical Infrastructure uses MIT add-on components like Risk Estimator (RE), the decision support tool CRIPS, TEFS (Tools for Extraction of functional status), and IKA (Incident Knowledge Analyser)

5.1 The MIT Communication Tool

Communication between depending Critical Infrastructures is an essential element for improved dependency management and increased dependability. The MIT communication backbone was designed and implemented for this purpose. Each CI has its own interface to the backbone and is enabled to send and receive messages from/to depending CI (see fig. 6). The CI control centres can receive information through the mIT backbone from depending CI and process this information for their own purposes with the MIT add-on components like Risk Estimator, decision support tool CRIPS, etc.

The information exchanged via the MIT communicator is based on the IRRIIS Information Model (see Subsection 3.2). It is represented in Risk Modelling Language (RML), an XML-shaped version of the IRRIIS Information Model supporting information exchange through Web services used in the MIT communication backbone [12].

[2] IKA will be described in a forthcoming publication.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

5.2 The Risk Estimator

A key assumption for defining the risk estimator is that specific conditions within one CI may not be critical by themselves, but that they become critical in combination with other situations. Therefore, this MIT add-on component combines and analyses more information than only the information from its home CI (fig. 7). This MIT add-on component allows us to give approximated risk estimates by using a relatively simple rule-based approach. Estimations take into account: real-time information (internal assessment), status information from other depending CI, wide-area planning information, scheduled maintenance, weather forecast, strikes, major public events, software/hardware vulnerability and other public information resources.

5.3 The CRIPS Decision Support Tool

CRIPS ("CRIsis management and Planning System") is an MIT add-on component aimed at supporting the assessment of the state of a CI and as a conclusion of this assessment at supporting the decision making in order to decrease a possible emergency situation.

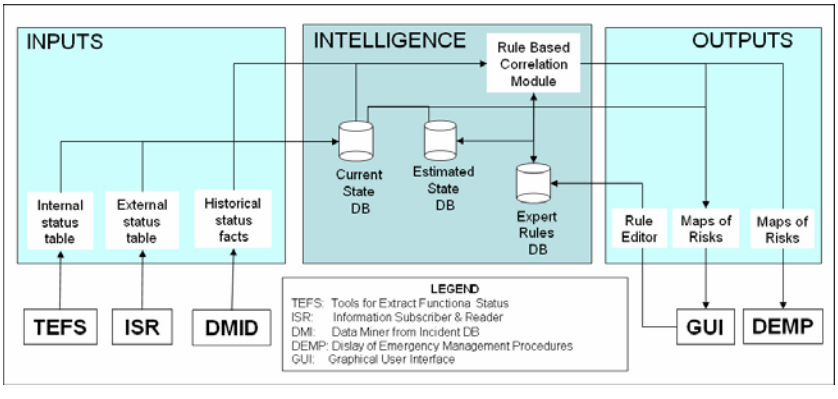

Fig. 5. The Risk Estimator

The assessment of the current situation in a network e.g. in a power network - should be more precisely characterized as "strategic assessment" of the current situation: not a normal day-to-day problem is to be identified, but the aim is to identify a situation which can cause a wide-area failure of power supply.

CRIPS is characterized as "knowledge based tool" and it is designed as an expert system:

– Dependency structures with respect to a support of decision making can be formulated by "if-then-else-rules", and the realization of an expert system to support a similar decision making problem in the political-military crisis management has proved the applicability of an such a representation and as consequence of an expert system for this task: It is the canonical method.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

– The representation of knowledge is simple-structured and this is a characteristic quality of an expert system separated from the processing (inference). This guarantees especially the required easy maintenance of the knowledge base.

6 Scenarios and Experiments

In order to be as close as necessary to the behaviour of real Critical Infrastructures the models we can build and simulate in SimCIP can be quite complex. The temporal aspects of component behaviours, the logical and other dependencies between components, redundancies between services, etc. can be described with high precision. The result is that the emergent behaviour of such complex models can not easily be predicted. By this reason we can run experiments with our models where different scenarios can be applied to a model of depending CI. This allows us to analyse in a systematic way how models of depending CI behave under certain circumstances and how MIT components support the reduction of cascading failures.

The first scenario created in the project is the (already mentioned) Rome scenario (see also fig. 1). It consists of four depending Critical Infrastructures: two from the power domain and two related ones from the telecommunication sector. This scenario forms a good playground for our experiments. It has been modelled using the IRRIIS Information Model and implemented within the SimCIP simulation environment. Siemens? Sincal power network simulator has been integrated with SimCIP in order to provide those aspects of power network simulation which are not directly facilitated by SimCIP[3].

SimCIP enables the specification of scenarios as sequences of events and actions happening as part of the network simulation. An event triggers a state transition in one of the network components. If this component belongs to one of the power networks its state transition is propagated to the Sincal power network simulator. The states of all related power network components is calculated there and propagated back to SimCIP. SimCIP interprets all resulting states and classifies them according to some general classification rules. These classifications may trigger new events as transitions of states.

Loss of power in a telecommunication component means activation of their back-up power systems. If this does not work either, or if after some time the back-up systems also fail the telecommunication component can not provide its service anymore. This lost service can have consequences for depending networks etc.

The federated simulation of SimCIP with its fine-grained model of heterogeneous networks and its integrated external simulator(s) enables the creation of quite complex and realistic scenarios for the investigation of dependencies of Critical Infrastructures and for the assessment of the benefits of MIT components.

[3] In a next step a telecommunication network simulator will also be integrated into SimCIP in order to enhance this aspect of dependency simulation.

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

7 Summary and Outlook

IRRIIS is an interdisciplinary project dedicated to the analysis, modelling, simulation, and improved operation of depending Critical Infrastructures. We analysed a couple of network analysis approaches for their contributions to the understanding of dependencies. In parallel we created the IRRIIS Information Model as lingua franca for communication between depending CI and as platform for CI simulation and analysis.

The concept of Middleware Improved Technology (MIT) was created in IRRIIS in order to improve information sharing between depending CI. MIT components like the MIT communication backbone, the Risk Estimator, and the CRIPS decision support tool were implemented.

The SimCIP simulation tool was developed as platform for CI simulations and for experiments with our MIT tools. It enables us to use IRRIIS Information Models for complex depending CI on the necessary level of technical precision. SimCIP supports federated simulation through the integration of external special purpose simulators.

Scenarios allow us to investigate depending Critical Infrastructures and their emergent behaviour. We can validate through experiments with different scenarios how well our models and concepts fit the needs of improved CI management.

IRRIIS will end in July 2009. The remaining month will be used to

- improve and extend our modelling and simulation capabilities in order to enable users of our tools to build and simulate critical infrastructures and their dependencies;
- to enhance the functionality of risk estimation and decision support including a tight integration into our simulation environment SimCIP;
- to build new scenarios directed especially towards next generation Critical Infrastructures;
- to run systematic experiments with the existing and the new scenarios in order to get a more comprehensive understanding of the emerging behaviour and of the benefits of MIT components; and
- to disseminate our results to a broad audience in the academic community and especially to industry in order to guarantee a widespread usage of our results.

Acknowledgement

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

References

1. The IRRIIS European Integrated Project, `http://www.irriis.org`; Klein, R., et al.: The IRRIIS Information Model. In: Setola, R., Geretshuber, S. (eds.) CRITIS 2008. LNCS, vol. 5508. Springer, Heidelberg (2009)

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7

2. Pederson, P., et al.: Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Technical Report, Idaho National Lab (August 2006)
3. Hämmerli, B.M. (ed.): CRITIS 2007. LNCS, vol. 5141. Springer, Heidelberg (2007)
4. Kröger, W.: Reliability Engineering and System Safety. Reliability Engineering and System Safety 93, 1781–1787 (2008)
5. Beyer, U., Flentge, F.: Towards a Holistic Metamodel for Systems of Critical Infrastructures. In: ECN CIIP Newsletter (October/November 2006)
6. Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver, M.H.A.: Modeling Critical Infrastructure Dependencies. In: Shenoi, S. (ed.) IFIP International Federation for Information Processing, Critical Infrastructure Protection, Boston. Springer, Heidelberg (2008) (to appear)
7. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 11–25 (December 2001)
8. Bloomfield, R., Popov, P., Salako, K., Wright, D., Buzna, L., Ciancamerla, E., Di Blasi, S., Minichino, M., Rosato, V.: Analysis of Critical Infrastructure dependence – An IRRIIS perspective. In: Klein, R. (ed.) Proc. IRRIIS Workshop at CRITIS 2008, Frascati, Italy (October 2008)
9. Klein, R., et al.: The IRRIIS Information Model. In: Proc. CRITIS 2008, Frascati, Italy. LNCS. Springer, Heidelberg (2008)
10. Minichino, M., et al.: Tools and techniques for interdependency analysis, Deliverable D2.2.2, The IRRIIS Consortium (July 2007), `http://www.irriis.org`
11. IRRIIS deliverable D2.1.2, Final report on analysis and modelling of LCCI topology, vulnerability and decentralised recovery strategies, The IRRIIS Consortium, `http://www.irriis.org/2007`
12. Flentge, F., Beyel, C., Rome, E.: Towards a standardised cross-sector information exchange on present risk factors. In: Hämmerli, B.M. (ed.) CRITIS 2007. LNCS, vol. 5141, pp. 369–380. Springer, Heidelberg (2008)
13. Rathnam, T.: Using Ontologies To Support Interoperabilit In Federated Simulation, M.Sc. thesis, Georgia Institute of Technology, Atlanta, GA, USA (August 2004)
14. Staab, S., Studer, R. (eds.): Handbook on Ontologies. International Handbooks on Information Systems. Springer, Heidelberg (2004)
15. Gruber, T.: Toward Principles for the Design of Ontologies Used for Knowledge Sharing. In: Proceedings of the International Workshop on Formal Ontology, Padova, Italy (March 1993)
16. Beyel, C., et al.: SimCIP Functional specification, Deliverable D.2.3.1., The IRRIIS Consortium (March 2007), `http://www.irriis.org`
17. Beyel, C., et al.: SimCIP Architecture, Deliverable D.2.3.2., The IRRIIS Consortium (March 2007), `http://www.irriis.org`
18. Beyel, C., et al.: SimCIP Simulation environment, Deliverable D.2.3.7. The IRRIIS Consortium (August 2008), `http://www.irriis.org`
19. Annoni, A.: Orchestra: Developing a Unified Open Architecture for Risk Management Applications. In: van Oosterom, P., et al. (eds.) Geo-information for Disaster Management. Springer, Heidelberg (2005)
20. Min, H.J., Beyeler, W., Brown, T., Son, Y.J., Jones, A.T.: Toward modeling and simulation of critical national infrastructure interdependencies. IIE Transactions 39, 57–71 (2007)

Lecture Notes in Computer Science, Verlag Springer Berlin / Heidelberg
Volume Volume 5508/2009 (CRITIS 2008), Publ. 2009, ISBN 978-3-642-03551-7