Simulating interdependent Critical Infrastructures with SimCIP

The Simulator for Critical Infrastructure Protection SimCIP is an integrated Simulation environment used for the modelling and simulation of interdependent critical infrastructures. It is under development in the framework of the EU integrated project IRRIIS.

Andrij Usov

Researcher at Fraunhofer IAIS, Sankt Augustin, Germany. Diploma in Theor. Computer Science (Univ. of Dortmund, Germany). Currently working in the EU project IRRIIS. Developer of SimCIP.
andrij.usov@iais.fraunhofer.de

Césaire Beyel

Researcher at Fraunhofer IAIS, Sankt Augustin, Germany. Diploma in Computer Science (Univ. of Bonn). Currently working in the EU project IRRIIS. Developer of SimCIP.
cesaire.beyel@iais.fraunhofer.de

Critical infrastructures are infrastructures for which failures, attacks or accidents would have a serious impact on the health, safety, security or economic well-being of citizens. Due to progresses in the Information and Communication Technologies ICT, Critical infrastructures have become increasingly complex and (inter)dependent. Therefore they are sometimes characterised as "Large, Complex Critical Infrastructures LCCI". Some examples of LCCIs among others are energy supply, telecommunication, financial sector, transportation, health and public administration. The integrated EU funded Project IRRIIS [1][2] has the objective to enhance substantially the dependability, survivability and resilience of European LCCIs.

SimCIP builds a synthetic simulation environment for studied CIs. It also serves as a test-bed for the inter-dependency analysis.

In order to achieve these goals, IRRIIS focuses on three main domains of activity:

Modelling and analysis of the inter-dependencies: enhancing the understanding of these interdependencies among LCCIs is one of the main activities. Different modelling approaches are studied that reach from models with very high level of abstraction like the Möbius Stochastic Automata Networks (SAN) approach [4] to so called high-fidelity models [3] that tend to model a system or parts of it as concretely as possible.

Middleware Improved Technology (MIT): LCCIs are confronted with various challenges like the assessment of network state, the situational awareness, decision support, etc. MIT is a set of tools and concepts aimed at dealing with these challenges. The following gives an excerpt of some MIT tools and concepts: Communication Components, Tools for Extracting Functional Status (TEFS), Incident Knowledge Analyzer (IKA) and the Risk Estimator (RE).

Simulation is a very powerful method for implementing and testing the various concepts of IRRIIS. The simulation environment SimCIP which is used in this aim is one of the core elements of IRRIIS. SimCIP not only has the goal of building a synthetic environmental representation of the studied LCCIs, it also will be used as a test-bed for the different concepts and approaches regarding MIT.

This article introduces the simulation environment SimCIP as it is implemented so far at Fraunhofer IAIS. At first we'll briefly introduce the Implementation, Services and Effects (ISE) model SimCIP is based upon. The next section then describes how this concept is implemented. Thereafter we will give a picture of the actual state of SimCIP. The last section of the article then closes by giving a look at the future works and further goals of SimCIP.

The ISE Metamodel

The challenge of the modelling of the interdependent critical infrastructures consists into managing the exchange of heterogeneous domain-specific data in the appropriate level of abstraction between the different model components. The ISE meta-model minimizes the modelling effort through a stepwise implementation [3] of the model. The basic idea is to split the model into three separated levels:

The *implementation (I) layer* encapsulates the domain specific data, logic and behaviour model of the components.

The *service (S) layer* represents the exchange of data between the model components. Data can be exchanged within a single domain or between different domains.

The evaluation and the processing of the service data occurs at the *effect (E) layer*. The results of the effects can be local (affect the own domain) or global (effects on the environment or other domains). The relationships between the layers can be described by an appropriate mapping e.g. mapping of implementation to service data.

The ISE-metamodel has been extended to the more concrete *IRRIIS Information Model* [2] which the implementation of SimCIP is based on. For the sake of a better comprehension though, we'll concentrate the description of the SimCIP structure on the more abstract ISE-metamodel.

Structure of the SimCIP Environment

Developed in the framework of the IRRIIS project, SimCIP is a multi-agent-based modelling and simulation environment implemented using the LAMPS (Language for Agent Modelling and Simulation, developed at Fraunhofer IAIS [5]). The main aim of SimCIP is to model and simulate a variety of interdependent

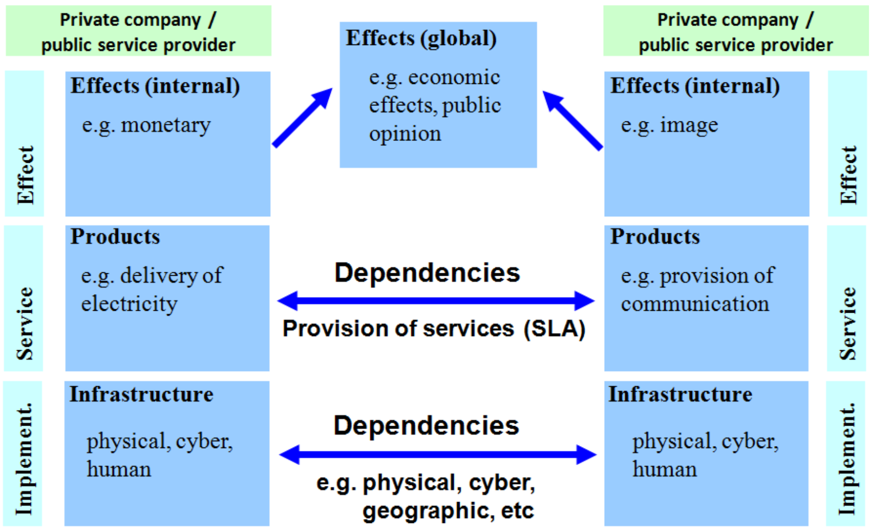

Fig. 1: The Implementation-Service-Effect CI metamodel [9].

critical infrastructure domains within an integrated environment. Different infrastructure domains have a very varying behaviour model. As a consequence, the logic for modelling the components and their behaviour also differs from one domain to the other. Therefore SimCIP is conceived as a federated simulation environment. The computation of the behaviour within one domain can be done by a dedicated external simulator. SimCIP has the task of defining the dependencies between the components, setting the initial values and collecting and evaluating the results of the simulation done by the external simulators. Predefined external events can also be scheduled to occur during a simulation.

SimCIP is an integrated environment that allows the coupling of different CI-models and simulators.

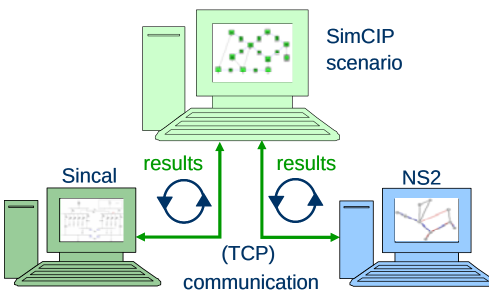

Fig. 2: Federated simulation in SimCIP

In SimCIP, network components are represented by agents. The agent state is described through network-specific state variables. These state variables, along with the domain specific logic and the internal network effects (encapsulated in external simulators) build up the implementation layer of the ISE model. For the I-S-mapping i.e. mapping the implementation to the service layer, some specific state variables are transformed into variables that are abstract enough to be exchanged on the service layer.

The internal state of the agent depends on the services consumed by the corresponding component. It can also be modified by a dedicated control instance which is responsible for the general network control. This instance gathers some specific network-wide data and evaluates the overall system state. It has the ability to compute the resulting effects and choose the appropriate next control action. The equivalent instances in the real world are the SCADA for the power network and the NOC (Network Operation Control) for the telecommunication network.

At any time SimCIP writes a snapshot

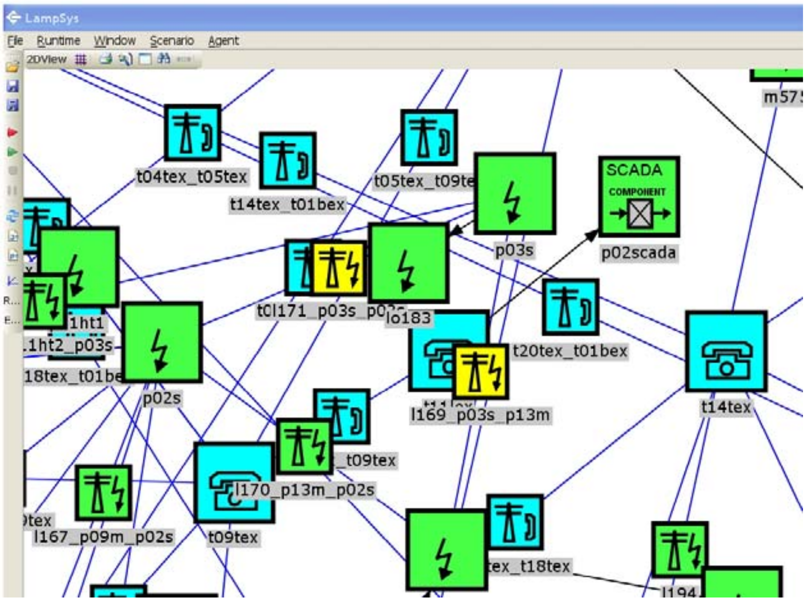

Fig. 3: SimCIP modelling environment.

of the current system state to the MIT interface. These values can be used for risk estimation and decision support. The simulation logs can be used for the evaluation of systematic experiments.

SimCIP: state of the art

SimCIP offers the possibility to model and simulate different types of critical infrastructures on a single integrated platform. The current implementation of SimCIP concentrates on the domains of electrical power and telecommunication networks. The computation of the state of these two CI-networks is done by external simulators in a distributed fashion. As the external simulator for the electrical power infrastructure, PSS Sincal [6] is used, whereas telecommunication networks are simulated using a combination of routing algorithms and the network simulator ns2 [7].

The scenario building and evaluation in SimCIP is currently based on data from some real existing European networks. Due to the huge amount of effort needed for manually modelling large CI-models, SimCIP additionally allows the import of network topologies from a predefined scenario database.

SimCIP allows to produce alarms in case of danger (e.g. overheating of power lines) and to implement some automatic network reaction (e.g. emergency disconnection of power lines).

Next steps

The implementation of the power network control unit (SCADA) is currently in progress. Our next steps will focus on following issues:

The implementation of the NOC instance for the telecommunication network could help to create more interesting and realistic scenarios.

The ability to run systematic experiment series is necessary for the evaluation of the current risk level and consequences of the scheduled actions.

The SimCIP environment can be extended to include the modelling and simulation of other critical infrastructure systems as for example water supply or public transport (see also [8]).

References

[1] The IRRIIS European Integrated Project: www.irriis.org

[2] R. Klein: Information Modelling and Simulation in Large Dependent Critical Infrastructures – an Overview of the European Integrated Project IRRIIS, in: Conference Pre-Proceedings 3rd International Workshop on Critical Information Infrastructures Security, Oct 2008

[3] U. Beyer, F. Flentge: The ISE Metamodel of Critical Infrastructures, In: Critical Infrastructure Protection: Issues and Solutions, Springer, 2007

[4] Clark G., Courtney T., Daly D., Deavours D., Derisavi S., Doyle J. M., Sanders W. H., and Webster P. (2001) The Möbius Modeling Tool. Proceedings of the 9th International Workshop on Petri Nets and Performance Models, Aachen, Germany, pp. 241-250. See www.mobius.uiuc.edu

[5] P. Huegelmeyer, T. Steffens, and T. Zoeller: Agent-based modeling of processes and scenarios with high-level Petri nets. Technical report, Fraunhofer IAIS, July 2006

[6] R. Buschmann, H. Dellwing, S. Geretshuber, C. Leick, C. Schwaegerl, O. Seifert: Increase of power system survivability with the Decision Support Tool CRIPS based on Network Planning, in: Conference Pre-Proceedings 3rd International Workshop on Critical Information Infrastructures Security, Oct 2008

[7] NS2 Network Simulator: www.isi.edu/nsnam/ns

[8] The DIESIS Project: Design of an Interoperable European federated Simulation network for critical InfraStructures, project web page: www.diesis-eu.org

[9] F. Flentge, C. Beyel, and E. Rome: Towards a Standardised Cross-Sector Information Exchange on Present Risk Factors, in: Conference Proceedings 2nd International Workshop on Critical Information Infrastructures Security, Oct 2007