IRRIIS - Integrated Risk Reduction of Information-based Infrastructure Systems

Uwe Beyer, Felix Flentge
Fraunhofer Institute for Autonomous Intelligent Systems, Sankt Augustin, Germany
uwe.beyer@ais.fraunhofer.de, felix.flentge@ais.fraunhofer.de

1. Introduction

The EU Integrated Project "Integrated Risk Reduction of Information-based Infrastructure Systems" (IRRIIS) will be carried out under the motto: Enhance substantially the dependability of Large Complex Critical Infrastructures (LCCIs) by introducing appropriate Middleware Improved Technology (MIT) components within the next three years. IRRIIS will increase dependability, survivability and resilience of EU critical information infrastructures based on Information and Communication Technology (ICT) and has the objectives to:

- determine a sound set of public and private sector requirements based upon scenario and related data analysis;
- design, develop, integrate and test MIT components suitable for preventing and limiting cascading effects and supporting automated recovery and service continuity in critical situations;
- develop, integrate, and validate novel and advanced modelling and simulation tools integrated into a synthetic environment (SYNTEX) for experiments and exercises;
- validate the functions of the MIT components using the SYNTEX environment and the results of the scenario and data analysis;
- disseminate novel and innovative concepts, results, and products to other ICT-based critical sectors.

IRRIIS will address the challenges of Complex Information Infrastructure Protection (CIIP) by a "diagnosis - therapy strategy" and "therapy implementation and validation approach" starting with the electrical power infrastructure and its supporting telecommunication infrastructure. After thoroughly analysing these infrastructures and their interdependencies, the synthetic simulation environment (SYNTEX) will be build. MIT components will be developed, tested and validated inside SYNTEX to demonstrate their capabilities before dissemination to potential stakeholders. The approach is open for successively including additional critical infrastructures.

The interdisciplinary research will be performed in the coming three years by a European consortium of fifteen partners, ranging from academia to key stakeholders from the fields of energy supply and telecommunication. The project is supported by the European Union Sixth Framework Programme within the area of "Information Society Technologies" with seven million Euro funding and is co-ordinated by the Fraunhofer Institute for Autonomous Intelligent Systems (Fraunhofer AIS).

2. LCCI Analysis and Requirements

Up till now there is a lack of advanced understanding of Large Complex Critical Infrastructures (LCCIs) dependability and interdependency particularly with regard to the use of Information and Communication Technology (ICT). Although some models and tools dealing with these issues exist, LCCI complexity and criticality cannot yet be tackled properly. Basic research is necessary to understand the phenomena of interdependency, dynamic behaviour and cascading effects in order to support the development of solutions for protecting and managing existing LCCIs in case of incidents. IRRIIS will perform in-depth research regarding the topological structure of LCCIs and the interdependencies between different LCCIs. Appropriate analytical approaches will be applied such as simulation models or analytical models suitable to investigate interdependency, network dynamics and cascading effects.

Starting from a thorough analysis of LCCIs, incorporating the stakeholder's views regarding ICT tools and models, a sound set of public and private sector requirements can be determined. These requirements will build the basis for the development of the SYNTEX simulation environment and the Middleware Improved Technology (MIT) components.

In order to enhance the understanding of LCCIs and to gain a sound foundation for the development of the SYNTEX simulation environment and the MIT components IRRIIS will:

- Survey LCCI stakeholder's requirements on technology and tools needed for understanding and mitigating cascading effects
- Survey and analyse existing tools and models
- Analyse current research gaps to identify relevant research and development efforts
- Provide detailed scenario and risk analysis
- Perform in-depth topological analysis of LCCIs
- Analyse the interdependency between different LCCIs
- Analyse the upcoming Next Generation Networks (NGN), i.e. networks based on IP connectivity or wireless connections with mainly software based services

This work will not only help to ensure the adequacy of the SYNTEX environment and the MIT components to the stakeholder's needs but also contributes to the ongoing world-wide research efforts concerning LCCIs.

3. Middleware Improved Technology

Starting with the knowledge gained from the LCCI analysis and the survey of stakeholder's requirements and existing tools, Middleware Improved Technology (MIT) components will be developed. These MIT components will facilitate the communication between different LCCIs and will allow identifying and evaluating incidents and malicious attacks and responding accordingly.

Currently, one big problem for the dependability, security and resilience of LCCIs is the high interdependence between different LCCIs within the same sector and also between different sectors. The consequence is that problems within one LCCI can lead to severe problems in dependent LCCIs. The resulting cascading effects are not limited to one kind of infrastructure and do not stop at national borders. To make things worse there is often a lack of appropriate communication structures between the dependent LCCIs (see Figure 1). This results in a lack of awareness of problems occurring in other infrastructures and mitigating actions can not be performed in time.

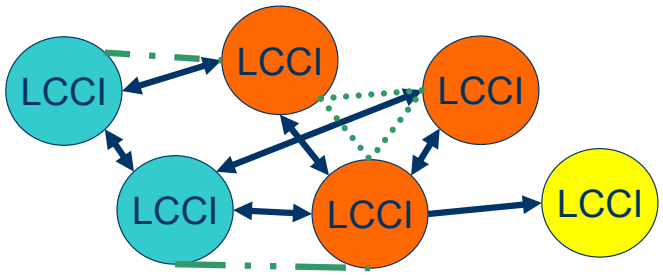

Figure 1: Interdependent LCCIs of the same and different sectors. The blue arrows indicate interdependencies and the green lines communication links using different standards.

To facilitate the communication between different infrastructures, IRRIIS will develop appropriate middleware communication components. All communication between different LCCIs should run via this middleware. The advantage is that each LCCI only needs one communication link towards the middleware and does not have to interface several other LCCIs (see Figure 2).

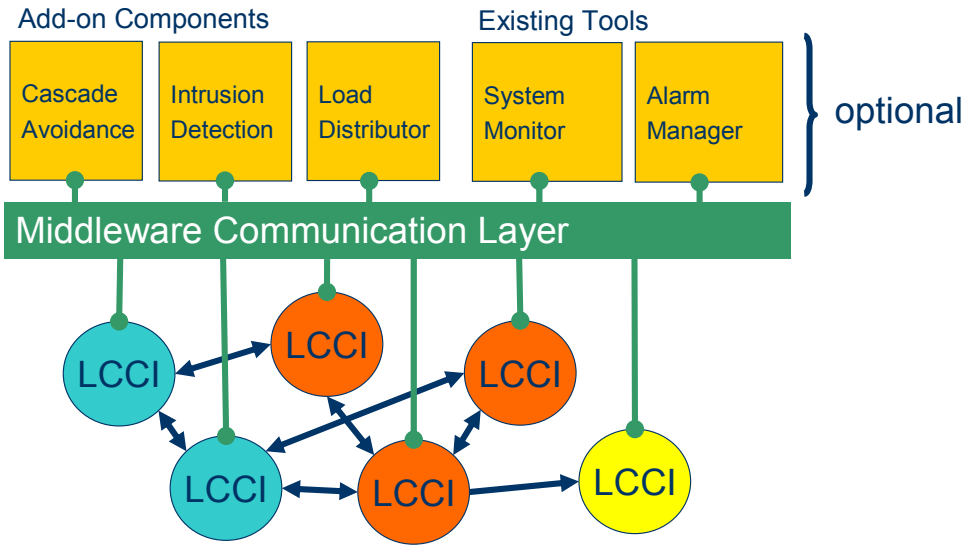

Figure 2: Interdependent LCCIs with Middleware Communication Layer and Middleware Improved Technology components,

The middleware will also be used by the optional MIT add-on components which have some kind of build-in "intelligence". These add-on components will monitor data flowing within and between the infrastructures and raise alarm in case of intrusions or emergencies and take measures to avoid cascading effects. They will be able to detect anomalies, filter alarms according to their relevance and support recovery actions and will thus contribute to the security and dependability of LCCIs. MIT components will interface existing systems and will not require major replacement of existing hardware or software. The flexibility of the middleware allows the easy integration of new LCCIs or new kind of information to be exchanged.

4. SYNTEX Simulation Environment

The purpose of the SYNTEX simulation environment is twofold: On the one hand side simulation can be used to improve the understanding of interdependent LCCIs. On the other hand the MIT components will be tested and validated in experiments using SYNTEX. Furthermore, their applicability and usefulness will be demonstrated to stakeholders within the SYNTEX environment before deployment to "real world" systems (see Figure 3).

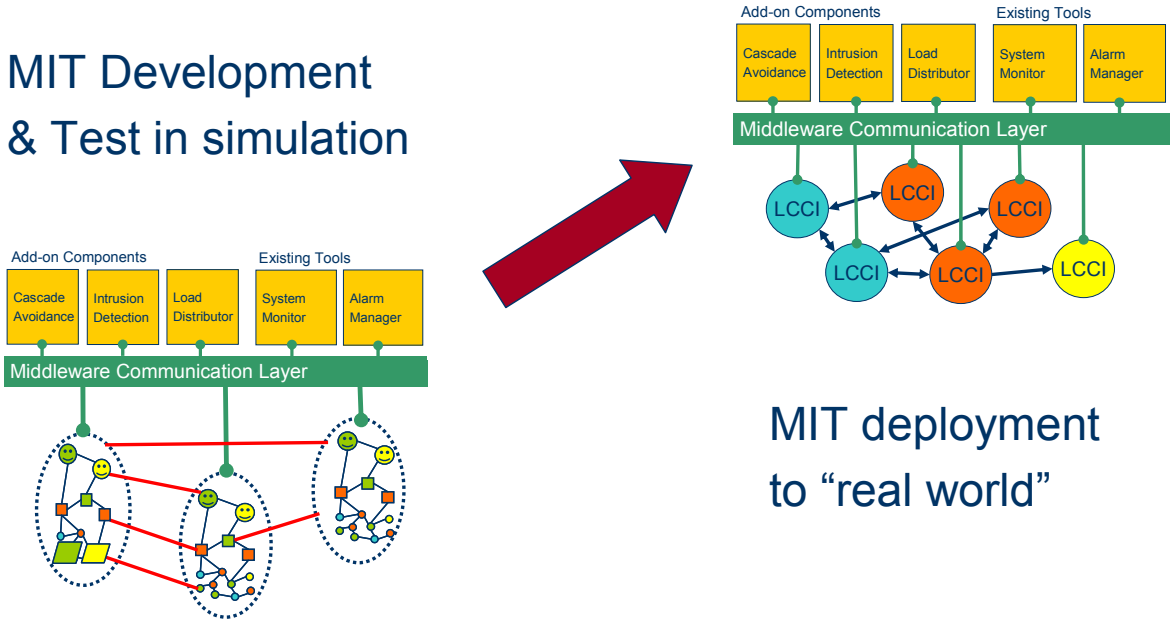

Figure 3: The role of the SYNTEX simulation environment in the development of the MIT components.

Building the SYNTEX environment is a big challenge because the simulation will not only have to include physical simulations but also has to simulate the cyber layer and the management layer of a LCCI as well (see Figure 4). For this purpose SYNTEX will use the principles of agent-based simulation. Each object will be modelled as an agent with clear interfaces to its environment and other agents.

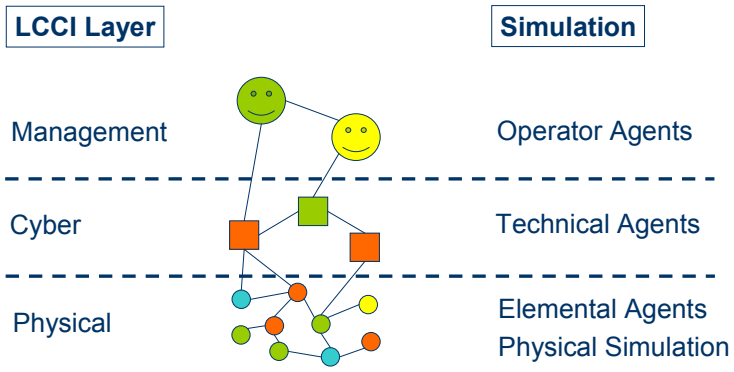

Figure 4: The different layers of a single LCCI and the according SYNTEX simulation objects.

The SYNTEX environment will include and interface existing tools to keep the simulation meaningful with respect to existing technologies and to allow the use of the results gained in current systems. This also means that the SYNTEX environment does not have to start from scratch but can rely on already existing and proven technology. To decide which tools and models should be included in SYNTEX, an in-depth survey of existing tools and models will be performed.

However, the main strength of SYNTEX will be the simulation of interdependencies between different LCCIs. To that end it will be necessary to have the possibility to model some objects of the individual LCCIs on more abstract levels. This will ensure a high scalability and flexibility of the SYNTEX environment. SYNTEX should be as generic as possible to allow its application to various kinds of LCCIs and its adaptation to the specific needs of individual stakeholders..

5. Summary

The major parts and the main outcomes of the IRRIIS project are summarised in Figure 5. Knowledge Elicitation and Research will lead to a "diagnosis" of the current and the future status of interdependent LCCIs. The "therapy" will be implemented through the MIT components which can be tested and validated in the SYNTEX environment. The main contributions of IRRIIS are an enhanced understanding of LCCIs, the SYNTEX simulation environment and the MIT components. To disseminate the results broadly to stakeholder, technology and service providers and the research community, these interest groups will be addressed within the IRRIIS project right from the start. IRRIIS also relies on international cooperation and is open for joint efforts of all kinds to achieve its goals. To foster international cooperation IRRIIS will establish an international conference and will define scenarios and benchmarks to allow the comparison of different approaches.

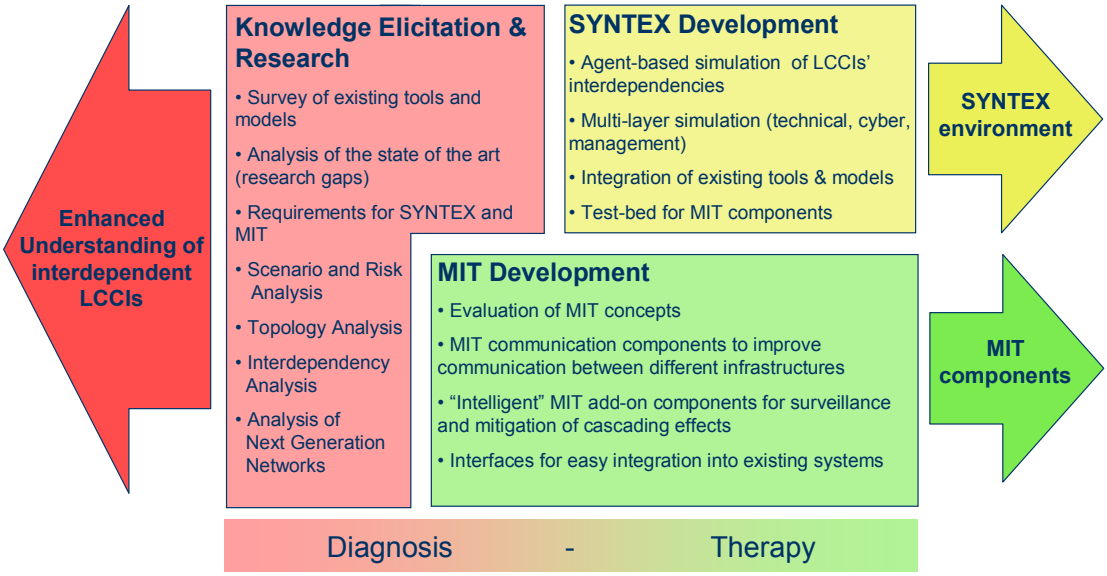

Figure 5: The major parts of the IRRIIS project and their outcomes.

Acknowledgment: IRRIIS is partly funded within the European Community's Sixth Framework Programme. However, all views expressed above are purely those of the authors and the Community is not liable for any use that may be made of the information contained therein