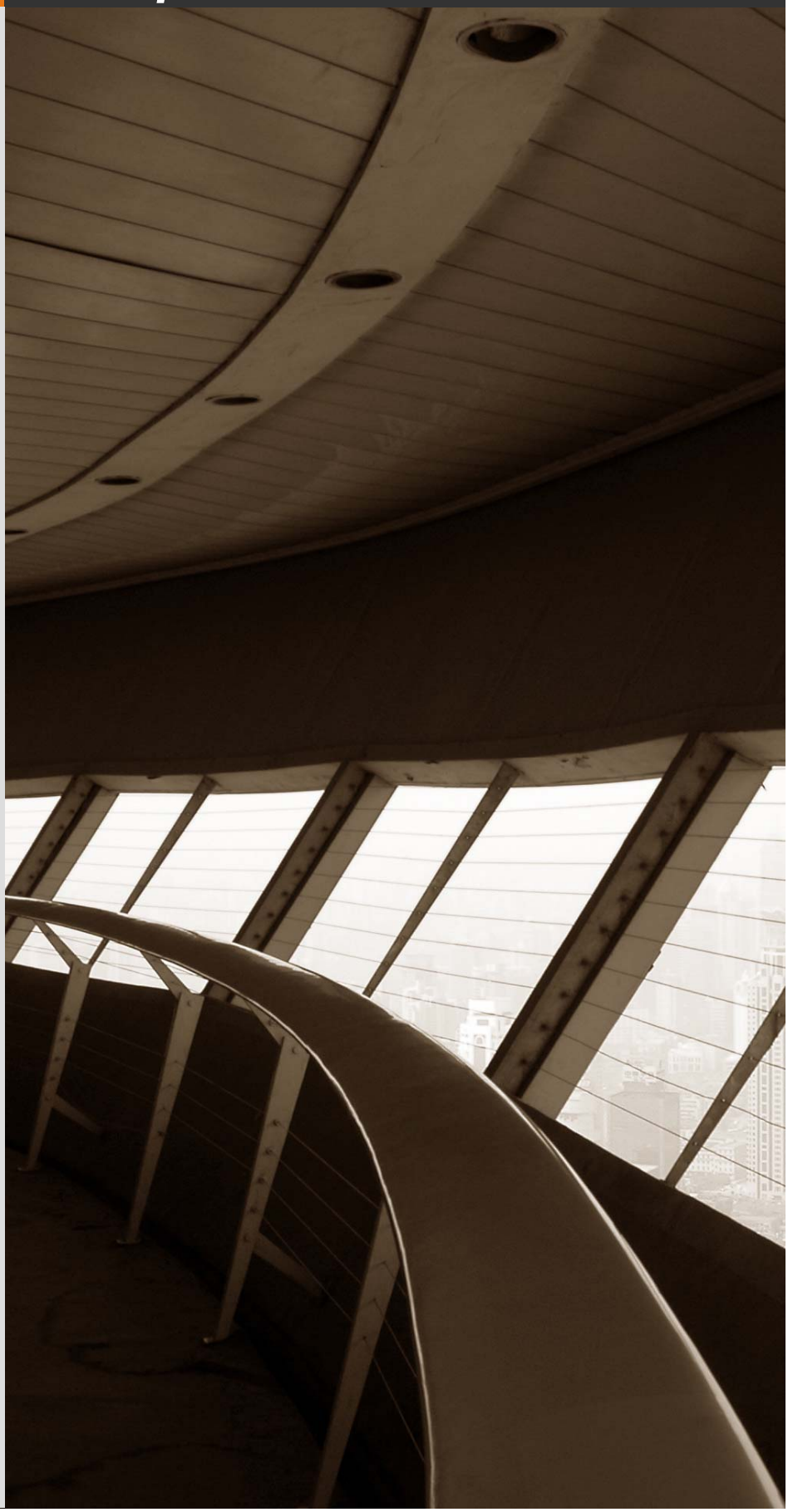
November / December 2008, Volume 4, Number 3

ECN

European CIIP Newsletter



> About ECN

ECN is co-ordinated with
The European Commission, was initiated by Dr. Andrea Servida,
and is now coached and supervised by Angelo Marino.
For 2007-2009, the ECN is financed by the IRRIIS project.
The IRRIIS project is an IST FP6 IP,
funded by the European Commission
under contract no 027568

>For ECN registration send any email to:
subscribe@ciip-newsletter.org

>Article can be submitted to be published to:
submit@ciip-newsletter.org

>Questions about articles to the editors can be sent to:
editor@ciip-newsletter.org

>General comments are directed to:
info@ciip-newsletter.org

>Download site for specific issues:
http://irriis.org
http://www.ci2rco.org

>Founders and Editors
Eyal Adar CEO iTcon, ***eyal@itcon-ltd.com***
Bernhard M. Hämmerli, HTA, Initiator and Main Editor ***bmhaemmerli@acris.ch***
Eric Luiijf, TNO, ***eric.luiijf@tno.nl***

>Country specific Editors
For Germany: Heinz Thielmann, Prof. emeritus, ***heinz.thielmann@t-online.de***
For Italy: Louisa Franchina, ISCOM, ***luisa.franchina@comunicazioni.it***
For France: Michel Riguidel, ENST, ***riguidel@enst.fr***
For Spain: Javier Lopez, UMA, ***jlm@lcc.uma.es***
For Finland: Hannu Kari, HUT, ***kari@tcs.hut.fi***

> Spelling
British English is used except for US contributions

Table of Content

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

Working on C(I)IP implementation:
Integrated Risk Assessment and C(I)IP Middleware have been researched.

C(I)IP policies, resilience and BCM misses its uniting part: The C(I)IP middleware. It communicates risk, system stability, robustness, and redundant capabilities in integrated systems containing diverse infrastructure elements from several sectors and being used across companies and borders.

Bernhard M. Hämmerli
Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
Vice-President ISSS Information Security Society Switzerland and Chair of Scientific and International Affairs

e-mail: bmhaemmerli@acris.ch
bmhaemmerli@hslu.ch

www.acris.ch

CIP and the financial sector

The current financial crisis demonstrates publicly that the financial sector is indeed a critical infrastructure. The question we need to address is, *did ICT cause this crisis?* Most experts are more involved with the business side of this crisis. Their argument and stance naturally revolves around these aspects. However, we can argue with some weight that, at the very least, the level at which the financial sector is "ICT enabled" has contributed to the crisis. Fast communications, fast electronic evaluation of assets, according to a more or less unique, insufficient, and failing model, are just one area of ICT practises that could be connected to this crisis.

What we can learn from this? Stringent application of homogenous ICT models may develop into problems. Diversity, delay, and well thought through human interaction vectors should be considered before national governments spend billions. We should keep in mind these facts before creating more integrated and broader – i.e. dependent infrastructures – electronically integrated risk radars.

About this Issue

Two articles in this issue deal with research into critical infrastructure dependencies:

"Simulating Interdependent Critical Infrastructures with SimCIP" is a report about the simulation component of the EU IRRIIS project.

"UK Interdependency Analysis Feasibility Study" is an article that presents an overview on the present and future state of research and practice in this area.

The EU project "PARSIFAL: Protection and Trust in Critical Financial Infrastructures" investigates ICT research requirements in the EU finance sectors, with a strong stakeholder involvement: The project will develop a new research agenda.

Massoud Amin presents the topic of "Resilient and Self-healing National Critical Infrastructures". Regina Maria De Felice Souza and Sérgio Luís Ribeiro report on the CIP status in Brazil giving an insight into how emergent countries deal with CIP.

"Critical Infrastructure and Industrial Supply Chains" discusses corporate needs and the meaning of CIP and BCM.

"Operations Research and Space Situational Awareness" looks at CIP in space, an often neglected topic.

Also included in this issue are:

A conference Report on "Security and Safety Management and Public Administration" and two announcements of upcoming conferences (4th CRIS and 4th CRITIS) which give community insights on current developments and thought patterns of experts in this field.

About editing books

C(I)IP research and conferences are very active. However, we still require good text books offering a consistent and broad view on C(I)IP. Therefore we have included an IEEE – Wheyly book publishing opportunity.

Enjoy reading this issue of the ECN!

PS. *Authors willing to contribute to future ECN issues are very welcome. Please contact me or one of the national representatives. Further information about the ECN and its publication policies can be found in the introduction of the first ECN, see* www.irriis.eu.

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 infra-structures 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.

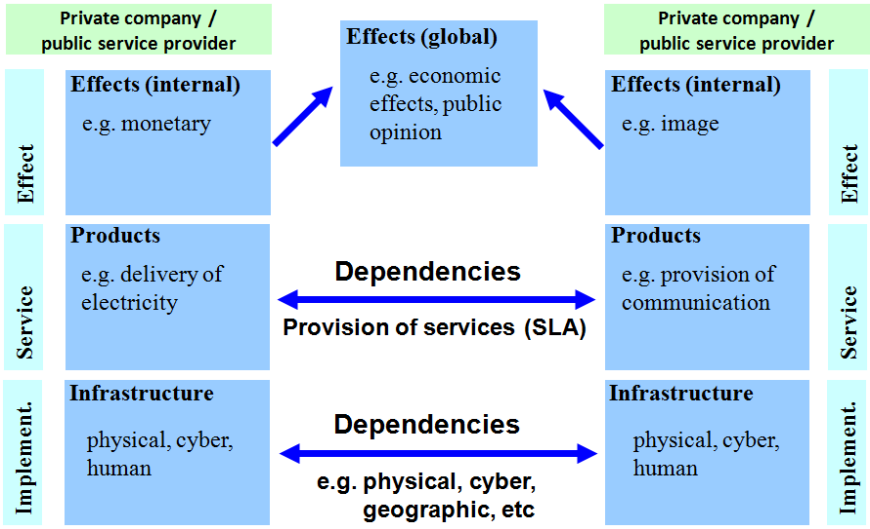


Fig. 1: The Implementation-Service-Effect CI metamodel [9].

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 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.

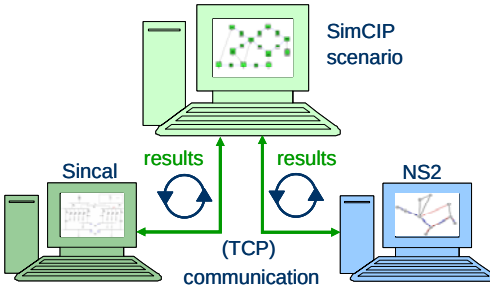


Fig. 2: Federated simulation in SimCIP

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

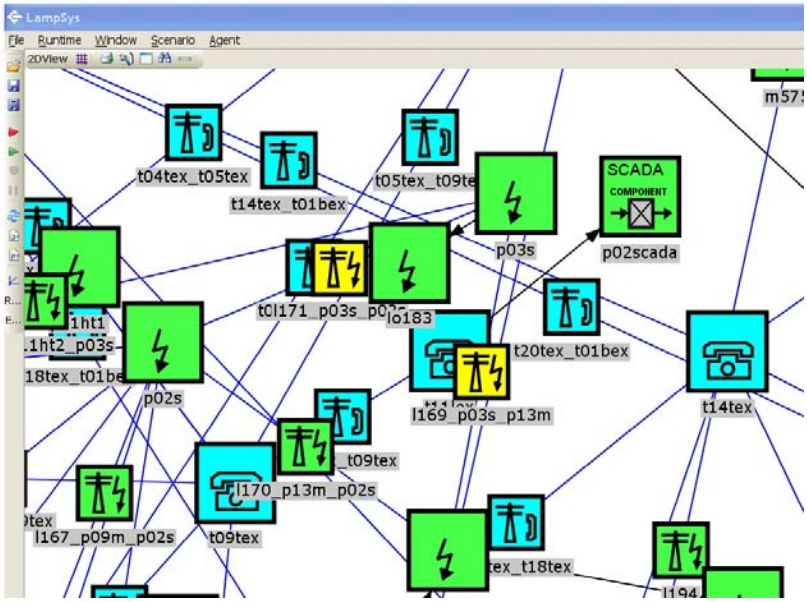


Fig. 3: SimCIP modelling environment.

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

PARSIFAL: Protection and Trust in Critical Financial Infrastructures

The PARSIFAL project is a Coordination Action within the European Programme for Critical Infrastructure Protection, with the ambitious objective of defining how to better protect CFI (Critical Financial Infrastructure) in Europe.

Rafael Llarena

Project Manager
R&D Consultant at Atos Origin Research & Innovation

e-mail: rafael.llarena@atosorigin.com

The PARSIFAL objective is to provide input to future research programmes and further strengthen the engagement between EU, Financial Services Industry with regards to trust, security and dependability of these critical financial ICT infrastructures. The activity of the project will be developed around two main workshops, where different stakeholders will directly exchange their views and discuss future scenarios and challenges from different perspectives. This group of stakeholders will have represented the main actors from CFI protection, industry, academia and government, typical with knowledge in financial products, ICT, R&D, Trust, Security and Dependability (TSD) and service providers.

Background of the initiative

The roots of this project go back to September 2007. On that date, a successful workshop was held in Frankfurt, in order to initiate the dialogue between financial industry stakeholders and Europe's top level research community[1]. The objective of this workshop was to identify research and development challenges for the protection of critical ICT-based financial infrastructures for the next 5 years.

The workshop was a perfect platform to articulate a discussion between the stakeholders on the future of the protection and trust on CI on the European financial sector, and develop scenarios and strategies on haw these CI could be constructed and protected. The workshop addressed global, cross border and multi-member state issues, which may affect the financial infrastructures of the European economy.

The workshop was the first time in history that a reasonable number of high-level financial industry actors addressed security challenges to the research community. As a result, some EU research projects in the view of the EU's 7th Framework Programme were generated. The subject of this article, PARSIFAL, is one of them.

Context

The European Programme for Critical Infrastructure Protection (EPCIP) Communication underlines that "since various sectors possess particular experience, expertise and requirements with Critical Infrastructure Protection (CIP), EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors". The European Critical Infrastructure (ECI) 2006 draft Directive puts forward in its Annex 1 a list of 11 critical infra-structure sectors that include the Critical Financial Infrastructures (CFI) sector. This is the context in which PARSIFAL is aiming at defining how to better protect CFI, but also other information infra-structure that link CFI with other sector Critical Infrastructures (CI) in Europe.

What makes this project different from other similar initiatives is its focus on CFI and involvement of stakeholders of the financial sector. Moreover, PARSIFAL will pay special attention to

1. http://www.europeanfinanceforum.org/Workshop.100.8.html?&ftu=a12e170569

the relation between protection of CI (and CFI) and trust, which is the key business requirement in the financial world.

In order to explain PARSIFAL concept, and a summary of CFI trends, it is useful first to describe the financial services provided by financial institutions and financial infrastructure providers, and observe them as two separated categories: "retail services" and "wholesale services". The main ICT characteristics of retail services are:

PARSIFAL focuses on CFI and involvement of stakeholders of the financial sector.

- Changing business channels: migration to wireless connections.
- I/O devices: use of handheld devices such as PDAs and mobile phones.
- End-to-end requirements for confidentiality, integrity, authenticity and non-repudiation.
- Integrated identity management for a broad range of identity proofs.
- Advanced authentication methods and tools (not just a simple password or one-time passphrase calculator).

On the other wholesale side, improvements will be achieved reducing transaction cycles, which imply:

- Higher standards of dependability, due to the risks of failure on a few technical
- System platforms concentrating a big number of applications.
- Need of improved mechanisms for provisioning and assigning access rights to servers.
- Improved behavioural detection and prevention methods to fight malware and malicious code.

PARSIFAL Objectives

The project will study and analyse one or more financial scenarios that involve dependencies on CFI. Derived from the Frankfurt meeting mentioned above, a set of trends and themes will be considered as a starting point of PARSIFAL:

Open infrastructures: we will analyse contradictory elements in a non-perimeter design paradigm for the CFI in which information is shared with customers and third party companies. This can often compromise privacy and competitiveness.

EU Critical Financial Infrastructure Consolidation: ICT infrastructures are generally owned by banks and managed as cost centres. These infrastructures often make use of old technology and there is not much appetite for upgrading the systems or to collaborate to identify better solutions. PARSIFAL will create awareness on benefits of a coordinated approach.

Competitive open EU financial markets: in the coming years, the growing openness of the EU market due to projects such as SEPA (Single Euro Payment) and MiFID (Markets in Financial Instruments Directive) will deliver high competition and increased power of end-users. PARSIFAL will contribute to the development of future infra-structures coordinating research projects in this area with current initiatives in the financial market.

Interconnected CFI and CII: When services and infrastructures become more interconnected, the stability and protection of these inter-connected services becomes crucial in the global UE economy. PARSIFAL will be working on identifying best practices and propagating these to existing or future CFI and CII owners, operators and service providers of these interconnected infrastructures.

Following this selection of trends and themes, PARSIFAL will engage a set of activities aligned with the following *PARSIFAL Objectives*:

1. **Bringing together CFI and TSD research stakeholders** in order to establish and nurture relationships between the financial sector stakeholders and the ICT TSD RTP communities. It is a key activity in PARSIFAL establishing an expert stakeholder group together with specific targeted working groups linked to selected technological challenges and identified financial service scenarios. The objective will be measured by appropriate coverage of relevant stakeholders and organisational structures. An overview of important public actors in the national CIIP organisational framework will be used to characterise the specific responsibilities and involve public actors in CFI scenarios, while links with financial sector are PARSIFAL´s guarantee to include the most relevant private sector stakeholders. The specific working group missions will come from initial work of expert stakeholders and position papers.
2. **Contributing to the understanding of CFI challenges:** the outcomes of the Frankfurt Workshop held in September 2007, mentioned before, will be used as a starting point for the fulfilment of this objective. PARSIFAL actions are structured around analysis on how the situation in the European CFI will evolve over the next 5-10 years. These actions address trends in CFI (critical financial infrastructures) from various perspectives (technological challenges, service

scenario, CFI dependencies etc and (socio-economic, technological, organisational…). Some of these emerging trends include changes in financial service chain and CFI operation outsourcing, use of eID in

3. banking, establishment of trust model, impact of social networking and online reputation, role of privacy in interlinking of CFI with other CII, end-to-end security of composed financial services etc.
4. **Developing longer term visions, research roadmaps, CFI scenarios and best practice guides:** PARSIFAL would bring together relevant research, industry and financial stakeholders that help in understanding on how identity thieves work in different financial operations and scenarios, such as electronic funds transfer, wire transfer, line of credit, check, credit and debit card, bill pay, scheduled automatic withdrawals, loans, or fund transfers between accounts. All these will find place on the PARSIFAL Position Paper and a set of recommendations for further actions will be generated. By describing detailed financial service over CFI scenarios, provision will be made for wider community discussion on the responsibility and accountability of stakeholders.
5. **Coordinating the relevant research work, knowledge and experiences:** the project has the potential to avoid duplication of effort and to quicken the pace of RTD in Europe while addressing common challenges in the development and protection of CFI on a national and international level. PARSIFAL will promote a structured EU wide approach to CFI challenges and scenarios and promotion of common CIIP framework among financial sector stakeholders and other way round (contributions from CFI and financial service resilience standards to general CIIP and ICT TSD research community). The project will also collaborate with related bodies, similar initiatives and even reach out to other areas and explore comparisons and synergies.

Two Workshops (March 2009 and January 2010) will take place to support PARSIFAL's objectives

Workshops

PARSIFAL will organize two workshops which will be crucial in order to achieve all the objectives explained. One workshop will take place in Frankfurt on March 16-17, 2009 and its objectives will be to provide the functional framework and mechanisms to enable a structured and strategic dialogue between stakeholders. Together with position papers, this event will feed directly formation of working groups. The second workshop in January 2010 will have the result of the first workshop as initial position. This workshop aims at getting a common understanding on CFI scenarios and accordingly matching of technological challenges to scenarios.

Current Work

Since the project started, on September 2008, the projects members have contacted a number of stakeholders from trust, security and dependability research community and from the financial sector. These contacts comprise high level actors of the financial sector, covering all the parts of the financial value chain. The response we have obtained from these stakeholders has been very positive and encouraging, given that the success of this project depends heavily on the cooperation and level of involvement that can be achieved from the different stakeholders. The project members have also started to work on the position papers that will serve as a starting point for the working groups and help support the discussion of the different sessions that will make part of the PARSIFAL workshops.

Towards Resilient and Self-healing National Critical Infrastructures

Critical infrastructures have become heavily interconnected with no complete control over them, and without high-confidence early-failure detection and modeling methodology. The solution could be Grid "self-modeling" with a capability to survive emergencies via resilience and adaptivity to new conditions.

S. Massoud Amin

Dr. S. Massoud Amin, Professor of Electrical and Computer Engineering, directs the Center for the Development of Technological Leadership (CDTL), and holds the Honeywell/H. W. Sweatt Chair in Technological Leadership at the University of Minnesota. Before joining the University, in March 2003, he was with the Electric Power Research Institute (EPRI), where he held positions of increased responsibility including Area Manager of Infrastructure Security, Grid Operations/Planning, Markets, Risk and Policy Assessment. In the aftermath of 9/11 he directed all security research and development at EPRI.

e-mail: amin@umn.edu

The Bigger Picture

Energy, telecommunications, transportation and financial infrastructures are becoming increasingly interconnected, thus, posing new challenges for their secure, reliable and efficient operation. All of these infrastructures are complex networks, geographically dispersed, non-linear, and interacting both among themselves and with their human owners, operators, and users. No single entity has complete control of these multi-scale, distributed, highly interactive networks, nor does any such entity have the ability to evaluate, monitor, and manage them in real time. In fact, the conventional mathematical methodologies that underpin today's modeling, simulation, and control paradigms are unable to handle the complexity and interconnectedness of these critical infrastructures.

Virtually every crucial economic and social function depends on the secure, reliable operation of energy, telecommunications, transportation, financial, and other infrastructures. Indeed, they have provided much of the quality of life that the more developed countries enjoy. However, with increased benefit has come increased risk. As these infrastructures have grown more complex to handle a variety of demands, they have become more interdependent. The Internet, computer networks, and our digital economy have increased the demand for reliable and disturbance-free electricity; banking finance depends on the robustness of electric power, cable, and wireless telecommunications. Transportation systems, including military and commercial aircraft as well as land and sea vessels, depend on communication and energy networks. Links between the power grid and telecommunications as well as between electrical power and oil, water, and gas pipelines continue to be lynchpins of energy supply networks. This strong interdependence means that an action in one part of one infrastructure network can rapidly create global effects by cascading throughout the same network and even into other networks.

Modeling interdependent infrastructures (e.g. the electric power, together with telecommunications, oil/gas pipelines, and energy markets) in a control theory context is especially pertinent since the current movement toward deregulation and competition will ultimately be limited only by the physics of electricity and the topology of the grid. In addition, mathematical models of complex networks are typically vague (or may not even exist); existing and classical methods or solution are either unavailable, or are not sufficiently powerful. For the most part, no present methodologies are suitable for predicting true systems' dynamics and understanding their behavior.

There is reasonable concern that national and international, energy and information infrastructures have reached a level of complexity and interconnection which makes them particularly vulnerable to cascading outages, initiated by material failure, natural calamities, intentional attack, or human error. The potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energise and control their

operations. Despite some similarities, the electric power grid is quite different from gas, oil or water networks- phase shifters rather than valves are used, and there is no way to store significant amounts of electricity. To provide the desired flow on one line often results in "loop flows" on several other lines.

In the aftermath of the tragic events of 11 September 2001, and recent natural disasters and major power outages, there are increased national and international concerns about the security, resilience and robustness of critical infrastructures in response to evolving spectra of threats. Secure and reliable operation of these networks is fundamental to national and international economy, security, and quality of life.

The Complex Interactive Networks/Systems Initiative (CIN/SI) and Intelligrid

The pioneering initiative in the area of complex interactive networks and infrastructure interdependency modeling, simulation, control, and management was successfully launched and carried out its goals during 1998-2002. This EPRI/DoD Complex Interactive Networks/Systems Initiative (CIN/SI), investigated challenges to the interdependent electric power grid, energy, sensing/ controls, communications, transportation, and financial infrastructures. CIN/SI was initiated in mid-1998 in response to growing concerns over the vulnerability of our critical national infrastructures. It was a three year, $18 million US Government-Industry Collaborative University Research (GICUR) program funded 60% by EPRI and — through the Army Research Office— 40% by the Deputy Under Secretary of Defense for Science and Technology. Six research consortia have been funded under CIN/SI, and work began in spring 1999. A total of 108 faculty members and over 220 graduate students and post-doctoral researchers from 28 universities in 17 of 50 U.S. States were involved in modeling, simulation, optimisation, and adaptive control of complex interactive networks.

The work showed that the grid can be operated closer to the limit of stability given adequate situational awareness combined with better secure communication and controls. A grid operator is similar to a pilot flying an aircraft, monitoring how the system is being affected, how the "environment" is affecting it, and having a solid sense of how to steer it in a stable fashion.

CIN/SI became the first and only initiative to attract academic research in inter-disciplinary areas of critical and interdependent infrastructures, mathematical underpinnings of cascading effects, and is of mutual benefit to private and public interests.

Ongoing programs at EPRI, DOE are further pursuing these objectives. As an example, EPRI's Intelligrid program has a component which is aimed at enabling grid operators greater look-ahead capability and foresight into the interdependent systems' dynamics to overcome limitations of the current schemes which at best have over 30 seconds' delay in assessing system behavior- analogous to driving a car by looking into the rear-view mirror instead of the road ahead. This tool using advanced sensing, communication and software modules was initiated in 2002 by me while at EPRI under the "Fast Simulation and Modeling" (FSM) program. This advanced simulation and modeling program promotes greater grid self-awareness and resilience in times of crisis in three ways:

Research activity indicated how to reach higher resiliency through simulation and modeling.

- by providing faster-than-real-time, look-ahead simulations (analogous to master chess players rapidly expanding and evaluating their various options under time constraints) avoiding previously unforeseen disturbances;
- by performing what-if analyses for large-regional power systems from both operations and planning points of view;
- and by integrating market, policy, and risk analysis into system models, and quantify their integrated effects on system security and reliability.

For The starting point: The 1996 and 2003 power outage

One event in particular precipitated the creation of the research initiatives: a power outage that cascaded across the western United States and Canada on August 10, 1996. This outage began with two relatively minor transmission-line faults in Oregon. But ripple effects from these faults tripped generators at McNary dam, producing a 500 MW-wave of oscillations on the high-voltage transmission grid that caused separation of one of the primary West Coast transmission lines, the Pacific Intertie, at the California-Oregon border. The result: blackouts in 13 states and provinces costing over $1.5 billion in damages and lost productivity. Subsequent analysis suggests that shedding (dropping) about 0.4% of the total load on the grid for just 30 minutes would have prevented the cascading effects and prevented large-scale regional outages (note that load shedding is not typically a first option for power grid operators faced with problems). Had the results of the CIN/SI been in place at the time of the August 2003 blackout, the events might have unfolded very differently. For example, fault anticipators located at one end of the high-voltage transmission lines would have detected abnormal signals, and making adaptive reconfiguration of the system to sectionalise the disturbance and minimise impact components failures several hours before the line failed.

Another key insight came out of forest fire analyses,, which researchers at CalTech and UC-Santa Barbara, found to have similar "failure-cascade" behavior to electric power grids. In a forest fire the spread of a spark into a conflagration depends on how close together the trees are. If there is just one tree in a barren field and it is hit by lightning, it burns but no big blaze results. But if there are many trees and they are close enough together - which is often the case with trees because Nature is prolific and efficient with its resources - the single lightning strike can result in a forest fire that burns until it reaches a natural barrier such as a rocky ridge, river, or road. If the barrier is narrow enough that a burning tree can fall across it or it includes a burnable flaw such as a wooden bridge, the fire jumps the barrier and burns on. It is the role of first-response firefighters such as smokejumpers to contain a small fire before it spreads by reinforcing an existing barrier or scraping out a defensible fire line barrier around the original blaze.

These preliminary findings suggested approaches by which the natural barriers in power grids may be made more robust by simple design changes in the configuration of the system, and eventually how small failures might be contained by active smokejumper-like controllers before they grow into large problems. Other research into fundamental theory of complex interactive systems explored means of quickly identifying weak links and failures within a system.

CIN/SI developed, among other things, a new vision for the integrated sensing, communications, and control of the power grid. Some of the pertinent issues are why/how to develop controllers for centralised vs. decentralised control and issues involving adaptive operation and robustness to disturbances that include various types of failures. Modern computer and communications technologies now allow us to think beyond the protection systems and the central control systems to a fully distributed system that places intelligent devices at each component, substations, and power plants. This distributed system will enable us to build a smarter grid.

Potential route ahead

A new mega-infrastructure is emerging from the convergence of energy, telecommunications, transportation, Internet, and electronic commerce. Furthermore, in the electric power industry and other critical infra-structures, new ways are being sought to improve network efficiency eliminating congestion problems without seriously diminishing reliability and security.

The electric power grid can be defined as the entire apparatus of wires and machines that connects the sources of electricity, with customers and their myriad needs.

The existing electricity infrastructure evolved to its technology composition today from the convolution of several major forces, only one of which was technologically based. During the past 12 years, we have systematically scanned science and technology, investment and policy dimensions to gain clearer insight on current science and technology assets when looked at from a consumer-centered, future perspective, rather than just incremental contributions to today's electric energy system and services.

Self-healing has become the strategic goal for the transformation of our current infrastructures.

The goal of transforming the current infrastructures to self-healing energy delivery, markets, and computer and communications networks to provide unprecedented robustness, reliability, efficiency, and quality for customers and our society is ambitious.

More specifically, the operation of a modern power system depends on complex systems of sensors and automated and manual controls, all of which are tied together through communication systems. While the direct physical destruction of generators, substations, or power lines, may be the most obvious strategy for causing blackouts, activities that compromise the operation of sensors, communication and control systems by spoofing, jamming, or sending improper commands could also disrupt the system, cause blackouts, and in some cases result in physical damage to key system components. Hacking and cyber attacks are becoming increasingly common.

Many elements of the distributed control systems now in use in power systems are also used in a variety of applications in process control, manufacturing, chemical process controls and refineries, transportation, and other critical infrastructure sectors and are hence vulnerable to similar modes of attack. Dozens of communication and cyber security intrusions, and penetration red-team attacks have been conducted. These "attacks" have uncovered a variety of cyber vulnerabilities such as unauthorised access, penetration, or hijacking of control.

While some of the operations of the system are automatic, ultimately human operators in the system control center make decisions and take actions to control the operation of the system. In addition, to the physical threats to such centers and the communication links that flow in and out of them, but one must also be concerned about two other factors: the reliability of the operators within the center, and the possibility that insecure code has been added to one of the programs in a center computer. The threats posed by "insiders" threats, as

well as the risk of a “Trojan horse” embedded in the software of one or more of the control centers is real. This can only be addressed by careful security measures both within the commercial firms that develop and supply this software and careful security screening of the utility and outside service personnel who perform software maintenance within the center. Today security patches often are not always supplied to end-users, or users are not applying the patches as they fear to impact system performance. Current practice is to apply an upgrade/patch after SCADA vendors thoroughly test and validate patches, sometimes causing a delay in patch deployment of several months.

As an example, related to numerous major outages, narrowly-programmed protection devices have contributed to worsening the severity and impact of the outage- typically performing a simple on/off logic which locally acts as preprogrammed while destabilising a larger regional interconnection. With its millions of relays, controls and other components, the parameter settings and structures of the protection devices and controllers in the electricity infrastructure can be a crucial issue. It is analogous to the poem "for want of a horseshoe nail… the kingdom was lost." i.e. relying on an "inexpensive 25-cent chip" and narrow control logic to operate and protect a multi-billion dollar machine.

As a part of enabling a self-healing grid, we have developed fast look-ahead modeling and simulation, precursor detection, adaptive protection, and coordination methods that minimise impact on the whole system performance (load dropped as well as robust rapid restoration). There is a need to coordinate the protection actions of such relays and controllers with each other to achieve overall stability; single controller or relay cannot do all, and they are often tuned for worst cases, therefore control action may become excessive from a system wide perspective.

On the other hand, they may be tuned for best case, and then the control action may not be adequate. These call for coordinating protection and control - neither agent, using its local signal, can by itself stabilise a system; but with coordination, multiple agents, each using its local signal, can stabilise the overall system.

It is important to note that the key elements and principles of operation for interconnected power systems were established in the 1960s prior to the emergence of extensive computer and communication networks. Computation is now heavily used in all levels of the power network — for planning and optimisation, fast local control of equipment, processing of field data. But coordination across the network happens on a slower time scale. Some coordination occurs under computer control, but much of it is still based on telephone calls between system operators at the utility control centers — even or especially! — during emergencies.

Grid “self-modeling” could survive emergencies and adapt to new conditions quicker than grids that are not self-conscious.

Grid “self-modeling” could survive emergencies and adapt to new conditions quicker than grids that are not self-conscious. Enabled by distributed sensing and measurement and combined with Fast Modeling and Simulation we have developed and pilot tested data-driven control and operation of regional power grids analogous to the continuous self-modeling and compensation of damaged fighter planes and intelligent robots in face of unexpected damage.

From a broader perspective, any critical national infrastructure typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the constituent networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure. In any situation subject to rapid changes, completely centralised control requires multiple, high-data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center. But all of these are liable to disruption at the very time when they are most needed (i.e. when the system is stressed by natural disasters, purposeful attack, or unusually high demand). In case of failures occurring at various locations in such a network, the whole system breaks into isolated "islands," each of which must then fend for itself. With the distributed intelligence and the components acting as independent agents, those in each island have the ability to reorganise themselves and make efficient use of whatever local resources remain to them in ways consonant with the established global goals to minimise adverse impact on the overall network. Local controllers will guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition. A network of local controllers can act as a parallel, distributed computer, communicating via microwaves, optical cables or power lines themselves, and intelligently limiting their messages to only that information necessary to achieve global optimisation and facilitate recovery after failure. Advanced technology now under development or under consideration holds the promise of meeting the electricity needs of a robust digital economy. The architecture for this new

technology framework is evolving through early research on concepts and the necessary enabling platforms. This architectural framework envisions an integrated, self-healing, electronically controlled electricity supply system of extreme resiliency and responsiveness—one that is fully capable of responding in real time to the billions of decisions made by consumers and their increasingly sophisticated agents. The potential exists to create an electricity system that provides the same efficiency, precision and interconnectivity as the billions of microprocessors that it will power.

Cost and benefit

A major outage (affecting 7 million or more customers) occurs about once per decade costing over $2 Billions - smaller disturbances are commonplace with very high cost to the customers and our society - on a given day, there are 500,000 customers without power for 2 hours or more in the United States. The annual losses to the U.S. economy from power outages and disturbances are $75 to $180 billion. The above programs cost about $170-$200M per year for R&D, and up to about $400M per year over a decade for fielding, testing and integration into the system and will save about 5 to 7-fold in prevention and mitigation of disturbances.

Next steps

How to control a heterogeneous, widely dispersed, yet globally interconnected system is a serious technological problem in any case. It is even more complex and difficult to control it for optimal efficiency and maximum benefit to the ultimate consumers while still allowing all its business components to compete fairly and freely. A similar need exists for other infrastructures, where future advanced systems are predicated on the near perfect functioning of today's electricity, communications, transportation, and financial services.

From a national perspective, a key grand challenge before us is how do we redesign, retro-fit and upgrade the nearly 220,000 miles of electro-mechanically controlled system into a smart self-healing grid that is driven by a well-designed market approach. Creating a smart grid with self-healing capabilities is no longer a distant dream; we've made considerable progress. But considerable technical challenges as well as several economic and policy issues remain to be addressed.

Achieving the grid performance, security and reliability are a profitable national investment, not a cost burden on the taxpayer.

Funding and sustaining innovations, such as the self-healing grid, remain a challenge as utilities must meet many competing demands on precious resources while trying to be responsive to their stakeholders, who tend to limit R&D investments to immediate applications and short-term return on investment. In addition, utilities have little incentive to invest in the longer term. For regulated investor–owned utilities there is added pressure caused by Wall Street to increase dividends.

Several reports and studies have estimated that for existing technologies to evolve and for the innovative technologies to be realised, a sustained annual research and development investment of $10-$13 billion is required. However, the current level of R&D funding in the electric industry is at an all-time low. The investment rates for the electricity sector are the lowest rates of any major industrial sector with the exception of the pulp and paper industry. The electricity sector invests at most only a few tenths of a percent of sales in research - this in contrast to fields such as electronics and pharmaceuticals in which R&D investment rates have been running between 8 and 12 percent of net sales - and all of these industry sectors fundamentally depend on reliable electricity. A balanced, cost-effective approach to investments and use of technology can make a sizable difference in mitigating the risk. Electricity shall prevail at the quality, efficiency, and reliability that customers demand and are willing to pay for. On the one hand, the question is, "Who provides it?" on the other hand, it is important to note that achieving the grid performance, security, and reliability are a profitable national investment, not a cost burden on the taxpayer. The economic payback is three to seven times greater than the money invested. Further, the payback starts with the completion of each sequence of grid improvement. The issue is not merely who invests money, because that is ultimately the public, but whether it's invested through taxes or kWh rates. Considering the impact of regulatory agencies, they should be capable of inducing the electricity producers to plan and fund the process; this may be the most efficient way to get it in operation. The current absence of a coordinated national decision-making body is a major obstacle. States ' rights and State PUC regulators have removed the individual State's utility motivation for a national plan. Investor utilities will face either collaboration on a national level or a forced nationalisation of the industry.

Given economic, societal, and quality-of-life issues and the ever-increasing interdependencies among infrastructures, a key challenge before us is whether the electricity infrastructure will evolve to become the primary support for the 21st century's digital society - a smart grid with self-healing capabilities - or be left behind as a 20th century industrial relic!

UK Interdependency Analysis feasibility study: the present and future state of research and practice

The UK Government are funding a feasibility study that explores the state-of-the-art in infrastructure interdependency modelling and analysis, both in terms of research and practice, and considers market, cost and regulatory issues for a future strategy.

Robin Bloomfield

Robin Bloomfield is Professor of Software and System Dependability at the City University London and a founder member of Adelard, an independent specialist Safety and Security consultancy.
Phone +44 20 7490 9453
Email: reb@csr.city.ac.uk and reb@adelard.com
Web: http://www.csr.city.ac.uk/ and www.adelard.com

Nick Chozos

Nick Chozos is a consultant at Adelard, an independent specialist Safety and Security consultancy based in London, UK.
Phone +44 20 7490 9456
e-mail: nc@adelard.com
Web: www.adelard.com

The UK Government is funding a study that explores the state-of-the-art in interdependency modelling and analysis and the potential market opportunities of interdependency analysis as a distinct service, placing much of the focus on Information Infrastructures.

The study is funded by the *Centre for the Protection of National Infrastructure* (CPNI) [3], *the Engineering and Physical Sciences Research Council* (EPSRC) and the *Technology Strategy Board* (TSB) [4]. The study is led by the *Centre for Software Reliability* (CSR), *City University London* [5], and also includes *Adelard* [6], a specialist consultancy in safety and security, and the *UK Defence Academy* [7], part of *Cranfield University*.

The Buncefield explosion and the 2007 UK floods are recent large-scale disasters that highlight the need for more R&D in infrastructure modelling and analysis.

Throughout this study we have consulted widely with service providers, tool suppliers, infrastructure owners and other stakeholders, such as policy makers and simulation validation experts, evaluating the state-of-the-art in terms of research and practice.

In addition, we are also interested in expanding the scope of this study to encompass the challenges posed from implementing the recent EU Directive that defines European Critical Infrastructure (ECI).

This article presents and discusses this study, and some of the findings that have emerged to this stage.

Lack of an evidence base

We began this study with a search for empirical evidence: major incidents that have occurred in the UK with sufficient information for an analysis that would provide insight in terms of vulnerabilities and limitations that would drive our study.

We focused on the Buncefield explosion [1] and the UK floods [2], which are the largest disasters that have affected the country in the last decade if not for longer.

Analysis of this data highlighted some important issues which are discussed here.

Although physical proximity of assets (geographical dependencies) seems an obvious issue, there were many "surprises" during these incidents. For instance, during the floods, power stations had to be shut-down for precaution, an action which was not planned in all cases.

During the Buncefield explosion, a business park hosting offices for 92 companies was destroyed by the blast, one of which was an IT company that hosted patient records for five hospitals and a £1.4 billion payroll scheme, which were all lost, even if temporarily. The Buncefield example highlights the importance of information infrastructures

and some of the risks that are associated with them.

We have also analysed a dataset collected by TNO [8] whom we work with within the EC-funded IRRIIS project (Integrated Risk Reduction of Information-based Infrastructure Systems) 0. The data concerns some 203 infrastructure incidents in the UK which occurred over approximately 6 years. The data is based on news articles which therefore select incidents above a newsworthy threshold. The analysis we have conducted examines the potential of failures cascading across infrastructures.

However, apart from the TNO dataset, there is very little evidence to support systematic analyses e.g. into estimating the costs of interdependencies and potential benefits of greater understanding. There are several reasons for this; one is the rarity of such events. Another is the lack of overall responsibility for this data collection.

Stakeholder perspectives: consultations and questionnaire

Our study is based on extensive consultations with stakeholders, and a questionnaire we are distributing to a larger number of stakeholders, and infrastructure operators in particular. Overall, we have consulted with:

- Government and infrastructure owners: We were interested in their current approaches and in their further needs. The needs of Government and utility companies resulted in a set of initial requirements that were then compared to the state-of-the-art in terms of capabilities.
- Service and tool providers: We explored the state-of-the-art in modelling, simulation and analysis. This resulted in a set of available capabilities. Our consultations with service and tool providers considered the areas presented in figure 1.

Current approaches

In our discussions we found that infrastructure owners place much attention to ensuring close relationships with suppliers and vendors. They believe that close relationships can assist in understanding the various risks associated with their providers' failure and their overall level of resilience. Risks are monitored through internal risk review groups and company boards oversee the results. In some cases, alternative providers have already been sourced as part of contingency planning.

A focus is given on resilience, with business continuity planning, frequent risk assessment and back up systems especially for IT being the most common practices.

We found that utility companies do not have an integrated approach for the assessment and mitigation of vulnerabilities related to infrastructure interdependencies. Responsibilities are distributed across the corresponding departments that deal with each infrastructure. Despite acknowledgement of the cross-infrastructure vulnerabilities, it was not clear how they cooperate/coordinate throughout their organizations.

On the whole there is very limited use of software tool support. In addition, infrastructure owners did not seem to be aware of any technical documentation,

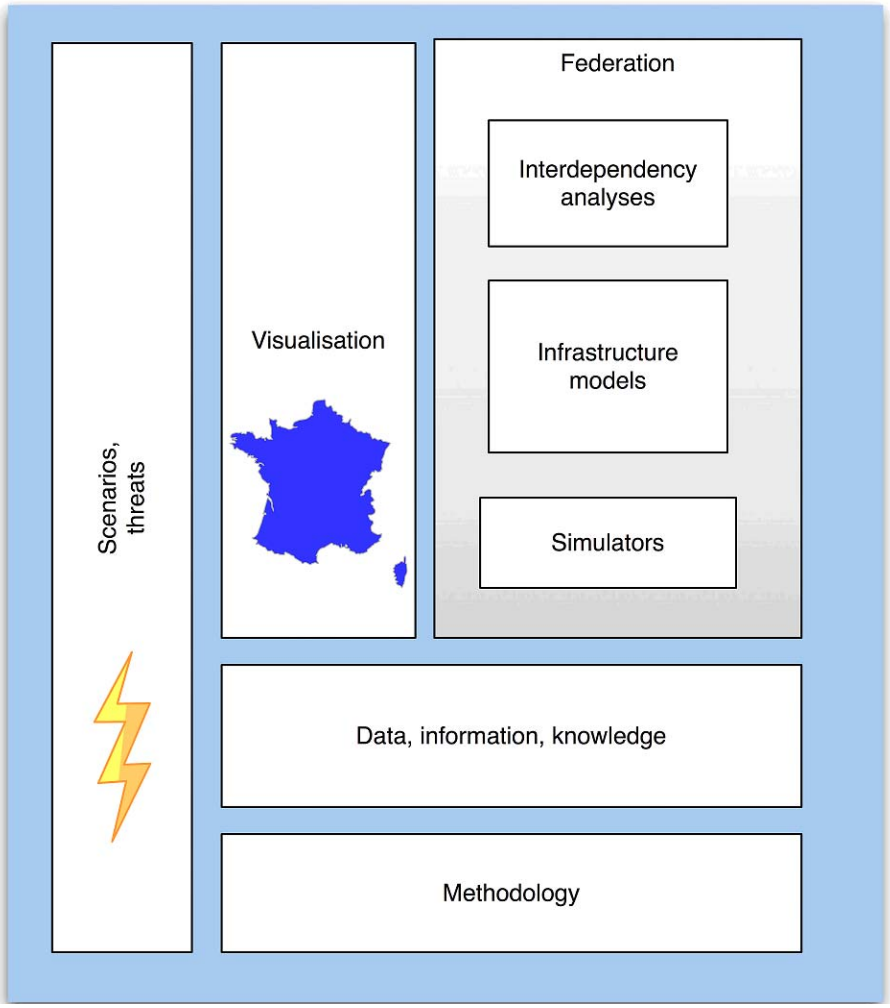


Figure 1 : Scope of consultation

research or conferences in infrastructure interdependency, something which perhaps suggests the presence of a gap between research and practice.

Perspectives on interdependency analysis tools and services

There was some disagreement as to whether there is a market for interdependency analysis as a distinct service, but infrastructure owners suggested they could be interested if it came along with other kinds of risk assessment. The issue of information sensitivity was raised as the major challenge to making interdependency analysis as a feasible service.

Initial requirements for interdependency analysis

The initial requirements that were identified during our consultations with Government agencies and utility companies fall under the following categories:

- **Inherent infrastructure resilience – scope and overall methodology.** This requirement aims at understanding to what level resilience is built in to infrastructures and their normal operation.
- **Infrastructure analysis and support.** Here we identify different kinds of decision-making support, such as off-line risk assessment and real-time infrastructure modelling.
- **Hazard and vulnerability identification and management**. There are various perspectives that need to be considered. I.e. natural hazards, security vulnerabilities or an all-hazards perspective (both natural and malicious)
- **Resilience phases.** Resilience goes through several phases: Normal operation, detection, recovery and long term reconstruction, as well as learning from past incidents.
- **Critical information infrastructures**. There is a need to understand not only Information Communication Technologies (ICT), but also data itself, and in all forms (electronic, paper-based, tacit).
- **Dependability of the modelling** . There are important challenges in achieving and evaluating the correctness, accuracy, and overall dependability of models used and analysis of the results (Validation and Verification).
- **Evidence of costs and potential benefits**. We have a very limited understanding of the relationship between scale of failures, recovery and cost. In order to justify investment in research and the development of tools and services, the relationship between costs and benefits must be considered.

Soft infrastructures

Our consultations highlighted the importance of "soft" critical infra-structures, e.g. trust and confidence within society both in their own right but also as an important component that is essential to the functioning of critical services.

Trust is an asset that can be built–up, destroyed, squandered and undermined as with so many other assets and resources. Assets such as trust and privacy within society are important and can be seen as emergent properties; although they are affected by local aspects of trust they have a complex relationship to localised issues. If we are to assess interdepen-dencies we need to take into account these essential yet softer aspects and their relationship to the more tangible assets. These soft aspects could be just as much the target of security threats as the more obvious physical and cyber systems.

Assets such as trust and privacy within society are important and can be seen as emergent properties. However, if we are to assess interdependencies we need to take into account these essential yet softer aspects and their relationship to more tangible assets.

While in the past the soft infrastructures might have been separable from the more technical infrastructures they are clearly related. Trust in the competence of government and authorities is dependent on how well they cope with crisis and incidents in the physical infrastructure. Trust relationships that citizens have between themselves, organisations, government and is increasingly mediated by the information infrastructure: a trend that is likely to increase.

The importance of "soft" infrastructures has been more than highlighted by the "credit crunch" and associated problems.

Research review

We have also undertaken an extensive researcher review. There is a plethora of research on infrastructure interaction modelling from a variety of diverse research communities. Many of the modelling approaches can be deployed across a wide range of abstractions. For example, the use of Stochastic Activity Nets can be at a fine grain, protocol level or at an abstract service description level. There are some general results from topological analyses that show, for example, the oft cited "small world" properties of certain topologies. There are also some general models of cascade failures and epidemiological spreading that have been applied to infrastructure modelling by the Complex Adaptive Systems community. There research community is fragmented and also rather distant from service providers.

Gap analysis

We performed a gap analysis between capabilities, the requirements, and current research in order to identify the nature and extent of the research and development challenges.

The overall impressions from the gap analysis, the research reviews and consultations are that there are impressive examples of detailed modelling and visualisation that would support the realisation of these capabilities. There is also considerable experience and expertise in the UK and internationally in simulation of domain or platform specific systems. The UK, and by impaction Europe, appears to lag significantly behind the US and Australia in the application of interconnected, multi-infrastructure modelling. In addition, the interaction within and between information infrastructures brings some specific problems.

Innovation

In our consultations, we also considered other potential areas where interdependency analysis could possibly contribute, both in research and practice. One example of such areas of innovation where several of consultees agreed was the calculation of Carbon Footprint.

The accurate calculation of the emissions of a product or service becomes very difficult when considering long and complex dynamically evolving supply chains. This would therefore be a potential area where interdependency analysis could find application in the near future.

A proposed strategy

We are currently developing our proposal for a strategy to address the required capabilities and gaps that we have identified. This strategy overall considers the need for the following activities:

- Trial of state of art and emerging research on realistic studies of significant scale
- Develop more analytical policy support and analysis of the evidence base
- Develop knowledge transfer and co-ordination and address the gap between research and practice

Interdependency analysis in practice
What do you think?

We would appreciate hearing perspectives and experiences (whether anecdotal evidence or analysis tools and applications) of either infrastructure owners or agencies in other countries. Anyone interested could also fill in one of our questionnaires. Your input will help us to better understand what is already possible, but also to contrast UK and other European perspectives in order to identify gaps that are worth further consideration.

In addition, this study has not considered the European Critical Infrastructure per se in much depth, but was only focused on UK priorities.

Finally, we are producing a limited version of our report that will be publicly available in the near future. Feel free to contact us if you would be interested in a copy when it becomes available or if you would like to find out more about our study.

References

[1] Pitt report, http://www.cabinetoffice.gov.uk/thepittreview.aspx

[2] Buncefield investigation website, http://www.buncefieldinvestigation.gov.uk/index.htm

[3] Centre for the Protection of Critical Infrastructure (CPNI), www.cpni.gov.uk

[4] Technology Strategy Board, www.innovateuk.org

[5] Centre for Software Reliability, City University London. cetifs study webpage, http://www.csr.city.ac.uk/projects/cetifs.html

[6] Adelard LLP, www.adelard.com

[7] Cranfield University Defence College of Management and Technology, http://www.cranfield.ac.uk/dcmt/

[8] Dutch TNO, http://www.tno.nl/

[9] IRRIIS project official website: http://www.irriis.org/

Critical Infrastructure Protection in Brazil: An Introduction

Brazil's telecommunications sector is fundamental to the integration of the population, as well as to the government's activities and services. This fact enforces the need to treat the telecommunications infrastructure as being critical.

Regina Maria De Felice Souza

Head technical advisory unit, Anatel's Presidency.

Regina is Telecommunications Engineer and she holds both a M.Sc. and Ph.D. degrees in Telecommunications Engineering from Unicamp, Campinas.

Sérgio Luís Ribeiro

Information Security Researcher, CPqD

Sérgio Ribeiro has published various articles on Information Security at national and international conferences. He holds both a B.Sc. degree in Applied Mathematics and a post-graduation in Information Systems from PUC Campinas, an MBA from FGV and is a CISSP.

e-mail: sribeiro@cpqd.com.br

Introduction

Brazil is developing a long-term program focused on Critical Telecommunication Infrastructure Protection (CTIP). Its objectives are: i) to identify the critical points of Brazil's telecom infrastructure; ii) to propose recommendations intended to prevent security incidents and to guarantee service and operations continuity if they happen; iii) to elaborate strategies and policies to protect Brazil's telecom infrastructure; iv) to analyze interdependency among different infrastructures. This program is being conducted by Anatel, Brazilian telecom regulator, and by CPqD, a private R&D telecom centre, and is sponsored by Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel).

Development

Security incidents in any critical infrastructure have nationwide level consequences that can impact an entire nation socially, politically or economically. This broad scope involving society, government and industry, requires a new approach to understand the related risk and the dependencies in order to develop a suitable program to protect what is critical to a country.

This broad scope, that involves the society, government and industry, requires a new approach to understand the related risk and dependencies…

The Brazilian CTIP project (see Figure 1) is based upon four main points:

- contextualisation,
- a protection strategy,
- a set of methodologies and
- software tools to support them.

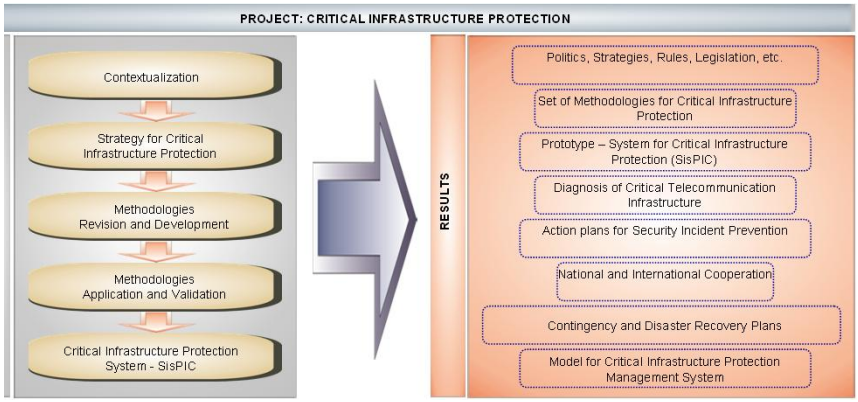


Figure 1 – CTIP project phases

Methodologies

The critical telecommunications infrastructure protection model is implemented by a set of five methodologies (see Figure 2).

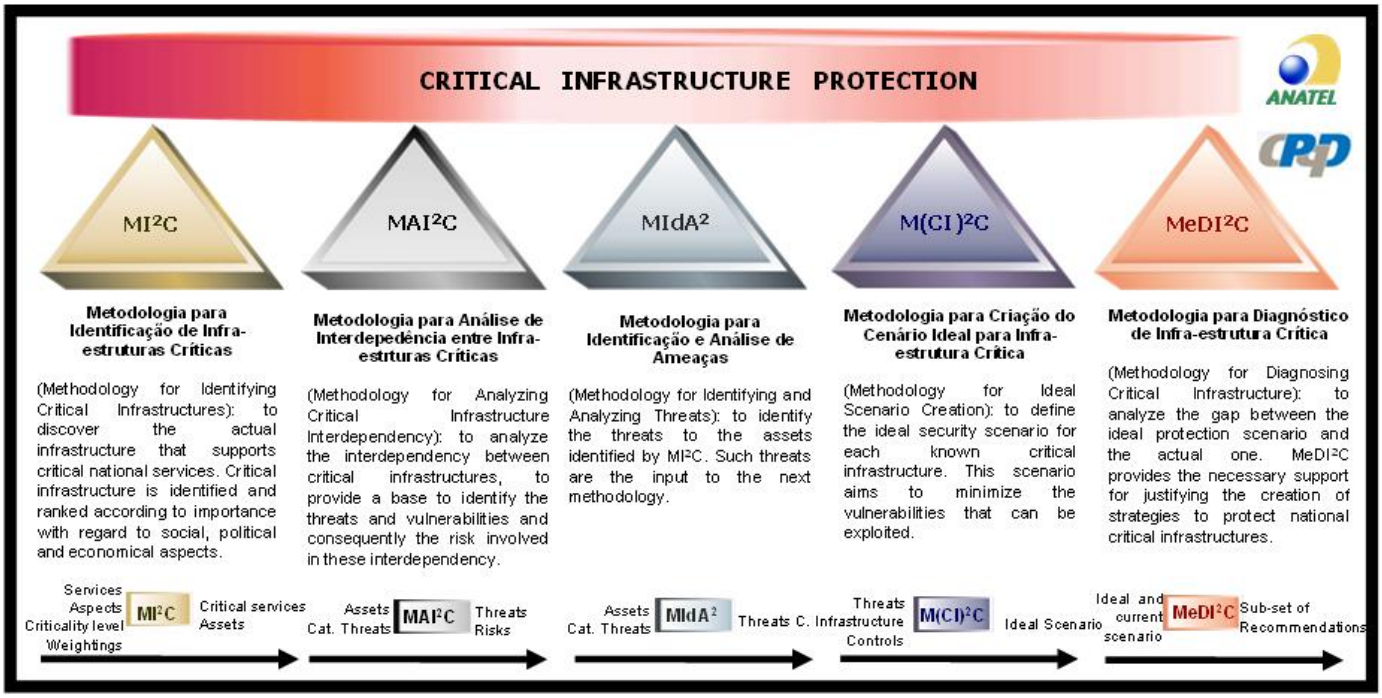


Figure 2 – Set of methodologies used in CTIP project

Although each methodology covers a specific part of the model, they are interdependent, since the output of one could be the input of other. The set of methodologies for CTIP is composed by:

- Methodology for Critical Infra-structure Identification (MI²C) defining the critical portion of the infrastructure, based on social, political and economical aspects;
- Methodology for Analyzing Critical Infrastructure Interdependency (MAI²C) – analyzing the interdependency between critical infrastructures. The results provide a base to identify the threats and vulnerabilities and consequently the risk involved in these interdependencies.
- Methodology for Identifying and Analyzing Threats (MIdA²) mapping threats related to each portion of the critical infrastructure identified by MI²C;
- Methodology for Ideal Scenario Creation (M(CI)²C) – creating the ideal scenario for critical infrastructure protection, based on the results of both MI²C and MIdA²;
- Methodology for Diagnosing Critical Infra-structure (MeDI2²) – diagnosing a portion of a determined critical infrastructure, revealing the actual situation and developing recommendations and action plan.

The approach adopted includes the evaluation of a variety of aspects related to social, economic and political factors to create a particular national context. Some results that had been achieved by the project include the critical telecommunication infrastructure identification needed by the XV Pan American Games (Pan2007) and Parapan American Games (Parapan2007) that was held in Rio de Janeiro from July 13th- 29th /August 12th-19th, using the MI²C application.

The approach adopted includes the evaluation of a variety of aspects related to social, economic and political factors to create a particular national context.

The efforts are now being directed towards the entire national Brazilian telecom infrastructure. Preliminary results achieved so far are the telecom services involved, the aspects to be evaluated for each service, the criticality levels with weighting factors assigned for each aspect, the analysis of the criticality levels and the prioritisation of the most important ("critical") telecom services. Future

phases will en-compass an inter-dependency analysis, the identification of threats and vulnerabilities, the creation of ideal CTIP scenarios and the critical telecom infrastructure diagnosis based on a gap analysis between ideal and actual scenarios with the purpose to elaborate strategies and policies for protection.

…the cooperation and information interchange between countries could result in a greater payoff in terms of results and experiences.

Conclusions

This paper has presented an overview of Brazilian Critical Infra-structure Protection Project with the scope of Telecommunications sector, and subsequently the set of methodologies that support the project.

Critical Infrastructure Protection (CIP) is a difficult task not only due to the complexity of the systems, networks and assets that provide essential services in our daily life but also due to the high interdependence among those infrastructures.

By virtue of economic and technological globalisation, some infrastructures such as telecom, are of global nature in the sense that a problem occurring within one country may affect other countries as well.

In this respect, CIP and consequently CTIP can be viewed as a strategic area for any country. The possibility of creating a context that inherently changes is a strategic goal, since risk levels will change and investments can be adequately prioritised. For instance, during a financial crisis, some parts of the critical infra-structure may have to be considered more important than others, whilst some public services can be put in second place due to the change in priorities.

For this reason, the cooperation and information exchange between countries could result in a greater payoff in terms of results and experiences.

Critical Infrastructure and Industrial Supply Chains

Industrial Business Continuity Planning for Critical Infrastructure Disruptions.

Michael Hiete

Dr. Michael Hiete is head of the research group risk management and technique assessment at the Institute for Industrial Production, Universität Karlsruhe (TH).

e-mail: michael.hiete@kit.edu

Mirjam Merz

Mirjam Merz is research assistant in the research group risk management and technique assessment at the Institute for Industrial Production, Universität Karlsruhe (TH).

e-mail: mirjam.merz@kit.edu

Introduction

Modern societies largely depend on the safe and secured operation of critical infrastructures (CI) like

- Electricity Supply
- Transport
- Communication
- Water Supply
- Banking and Finance
- Primary Industry
- Emergency Services
- Administration.

Failure of CI would have a "serious impact on the health, safety, security or economic well-being of a country or the effective functioning of its government" (Murray and Grubesic, 2007).

As most CI show a complex network structure, they are highly vulnerable and can be severely damaged, destroyed or disrupted by technical or human failure, natural disasters, criminal activity or acts of terrorism. Furthermore the level of interdependencies between the different CI increases possibly leading to a cascading failure across CI in the event of system failures and network breakdowns in a single CI (Murray and Grubesic, 2007).

Importance of Critical Infrastructures for Industrial Production

The secured availability of critical infrastructures is not only essential for modern societies as a whole but also for the continuity of most industrial production processes. The relevance of the various CI is sector specific and depends e.g. on the characteristics of the manufactured products and the different production processes (Merz, 2008).

CI	Dependent Company Function
Electricity Supply	Production processes Process control Measuring systems Administration/Management Service Installations
Transport	Supply of raw materials Supply of vendor parts Distribution of finished products Waste disposal
Water Supply	Process water Cooling Water Solvent Cleaning Sanitary services
IT and Communication	Data management Administration Process control Communication Sales & Ordering
Primary Industry	Raw materials Energy sources
Banking & Finance	Payments
Administration	Licences Surveillance
Emergency Services	Medical care for employees

Table 1: Dependence of Company Functions in Industrial Production on CI

Table 1 shows the various functions in a company depending on a specific CI. The transport sector, for example, is indispensable for the supply of raw materials and vendor parts, the distribution of finished products and the disposal of waste, especially in times where storage capacities have been reduced to a minimum. As a result of an increasing automation of production processes, Information and communication technologies become more and more important.

Power supply, however, takes a special role as not only production processes but also most auxiliary services (e.g. process control, measuring systems, administration) and other CI depend on the continuous supply of electricity.

Thus, within industrial production sites, electricity supply interruptions may trigger significant business interruptions, leading to large production losses. In some industrial sectors (e.g. the chemical industry), due to the breakdown of control and cooling units, secondary hazards might be induced by power blackouts. Therefore, especially for the industrial sector, disruptions of electricity supply pose a special challenge.

CI disruptions rank among the most important categories of supply chain risks.

Cascading Effects in Industrial Supply Chains

Due to the complex structure and the high degree of interdependency of modern supply chains, negative consequences of CI disruptions (e.g. production downtimes, material losses, secondary hazards) are rarely limited to single companies. The induced perturbations can be propagated via cascading effects into far-off supply chain links and may result in long lasting disruptions in global supply chains and substantial economic losses worldwide. Consequently, CI disruptions rank among the most important categories of supply chain risks.

There is a growing interest in this topic as a result of some prominent power blackouts in the last few years. For example, in 2007 the Samsung chip production in South Korea was affected by a power blackout which caused economic losses of more than 60 Mio US $ worldwide (Murray and Grubesic, 2007). Other examples are the large-scale blackouts in the U.S.A. and Canada in 2003. Also European power blackouts with negative effects are known (e.g. Germany in 2005; Germany and France 1999)

However, the prediction of the consequences and cascading effects caused by a power blackout or a supply chain interruption in general is a difficult task. For example, in one part of the supply chain a disruption lessens from one link of the supply chain to the next one, while within another part the negative consequences might increase (Figure 1).

Possible reasons for this behaviour could be:

- different geographical conditions,
- different supply strategies of the companies (e.g. lean supply chains, just-in-time concept and reduced inventories) or
- the general risk prevention and risk awareness politics of the involved companies.

In order to better understand and predict the cascading effects caused by supply disruptions which are prerequisites for effective prevention and mitigation measures more research is needed on this topic.

Industrial Business Continuity Planning

The risks and negative impacts of CI disruptions within single production sites and entire supply chains can be reduced or even prevented. To minimise the negative consequences of cascading supply disruptions, robust supply chains with alternative suppliers and redundant inventories are useful (Christopher and Peck, 2004). For the reduction of direct damages and secondary hazards technical protection measures as well as organisational actions can be effective.

Therefore, it is important for industrial companies to have well structured and sophisticated crisis management strategies which increase the overall capacity levels of a company and support the fast recovery from the potential impacts of CI interruptions and the subsequent supply chain disruptions (Smith, 2006).

Although a sophisticated crisis management would allow to reduce the risks and negative effects of CI disruptions and other accidents to a minimum level possible, there is always an economic trade-off between avoided damages and the costs for counter-measures. Thus, a reasonable level has to be identified for each production site and company needs to take into account that in tightly coupled networks accidents become inevitable due to the complexity of the interconnected systems.

In recent years many companies have implemented Business Continuity Plans (BCPs). BCPs help to increase a company's reactivity during crisis and after failures and to reduce production down times and the associated costs. This also increases the overall robustness of supply chains.

Therefore, BCPs should take effect in two points. Firstly, the vulnerability of production systems must be reduced and secondly the negative effects and therefore the severity of the disruption must be minimised.

In Europe, currently there is no regulation which prescribes the implementation of BCP but there are some legal regulations and standards which motivate for industrial BCP (e.g. Basel II, Sarbanes Oxley Act, ISO/IEC 17799, PAS 56).

Methods for BCP-Design

Formally, the BCP process consists of a four-part framework with the following consecutive steps:

- Step 1: Impact assessment
- Step 2: Risk analysis
- Step 3: Plan design
- Step 4: Plan audit.

Figure 1: Cascading effects within industrial supply chains

Within the first step of the process, potential consequences of CI disruptions for the business processes are analysed and particularly vulnerable and critical production processes and installations are identified. The second step assesses the probability of occurrence of supply or infrastructure disruptions. The third and main step of the BCP development is the structured identification and evaluation of emergency and recovery measures, the determination of responsibilities and communication strategies as well as a proper planning of resources, needed for the restoration of normal production and business processes. In step 4, finally, the plans are revised periodically and tested for their consistency and actuality.

While for the risk analysis (step 1) various quantitative and qualitative methods can be used, for the impact assessment (step 2) there are currently only qualitative methods like scenario-based workshops and interviews in use. For the plan design (step 3) currently only descriptive and qualitative methods are described which originate mainly from the practitioners field (Zsidisin, 2005).

However, the development and selection of adequate crisis management measures can be a complex task as various stake-holders are involved in the development of continuity plans. Therefore, a quantitative approach allowing well-structured emergency, recovery and continuity plans would be very helpful. Furthermore, transparency and trace-ability are important for risk awareness and the overall acceptance of BCP.

Multi-Criteria Decision Analysis in BCP-Design

In order to enable a structured identification and assessment of crisis and recovery measures in the BCP design, methods from the field of multi-criteria decision analysis (MCDA) can be applied. An MCDA method which has proved suitable in the field of emergency and crisis management is the multi attribute value theory (MAVT) (Bertsch, 2008). MAVT allows for example to compare several alternatives (like different emergency or BCP measures) on the basis of several, often conflicting criteria in a structured and traceable way. E.g. for emergency and recovery measures in BCP not only economic and technical aspects but also ecological and social criteria play an important role. MAVT may also support the involvement of public and private stakeholders from diverse disciplines (Bertsch, 2008).

Case Study Application and Conclusion

In an ongoing project a handbook for decision support for crisis management in the event of large-area power disruptions is developed. Focal area is the federal German state of Baden-Württemberg. Within the project negative effects of power blackouts on selected CI (industrial production processes, health services, water supply and communication) are assessed and potential BCP and emergency measures are identified and evaluated. The project makes use of the results of the national crisis management exercise LÜKEX 2004 as a starting point and includes numerous expert interviews and several workshops to get for additional information. Project partners are an electricity supplier as well as federal state and central governmental authorities.

Conclusion

Several infrastructures are critical for the functioning of a society. The interruption of these critical infrastructures (CI) and in particular power blackouts may cause high economic losses - as a result of cascading effects in today's supply chains even in far off regions and in originally unaffected sectors. Business continuity plans (BCP) serve companies to reduce their vulnerability and to minimise negative effects in case of a disruption of production. Methods of multi-criteria decision analysis may support the development of BCP by providing a structured and traceable approach to integrate various and in particular conflicting criteria.

References

Bertsch, V. (2008) *Uncertainty Handling in Multi-Attribute Decision Support for Industrial Risk Management*, Karlsruhe University Press.

Christopher, M. and Peck, H. (2004) Building the resilient supply chain, *International Journal of Logistics Management*, 15, 2, 388-396.

Merz, M., Hiete, M., Rostal, D. and Bertsch, V. (2008) Multi-Criteria Decision Support for Business Continuity Planning in the Event of Critical Infrastructure Disruptions, *International Journal of Critical Infrastructures* (accepted).

Murray, A.T. and Grubesic, T.H. (2007) Overview of Reliability and Vulnerability in Critical Infrastructure, in: A.T. Murray and T.H. Grubesic (Eds.) *Critical Infrastructure - Reliability and Vulnerability*, Springer, 1-8.

Zsidisin, G.A., Melnyk, S.A. and Ragatz, G.L. (2005) An institutional theory perspective of business continuity planning for purchasing and supply management, Int. J. Prod. Res., 43, 16, 3401-3420

Space Situational Awareness, National Assistance, and Crisis Management

How Operations Research and Space Situational Awareness may help to support the IT-based Protection of Critical Infrastructures

Guido Bartsch

Dr. Bartsch is senior researcher at the FGAN Research Institute for High Frequency Physics and Radar Techniques (FHR), Department Radar Techniques for Space Reconnaissance (RWA).
email: Bartsch@FGAN.de
www.FGAN.de

Stefan Pickl

Prof. Dr. Pickl is Chair of the Operations Research Department of Computer Science at University of the Federal Armed Forces Munich.
email: Stefan.Pickl@UniBw.de
www.unibw.de/stefan.pickl

1. Critical Infrastructures and Decision Support Systems

The protection of critical infrastructures demands for the design and optimisation of comfortable decision support systems. One disadvantage of many complex systems (we will see later on which complex system is a critical infrastructure) is that they often consist of a large amount of heterogeneous single applications that are inefficiently integrated into the overall process. This happens as such processes tend to grow over time, caused by an increase of complexity and supplementary demands by users for further functionalities, which leads to demands of new applications that are added to the system and need not always be compatible to the legacy applications. This results in process inefficiencies such as breakings in the media chain, high coordination effort, redundancy and an inefficient handling of information as the processing time increases. In case of threat on such a critical infrastructure element, a fast and flexible acquisition, processing, and allocation of information are crucial. Flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture (SOA) which qualifies it to be used in the context of OR procedures in order to optimally protect the critical infrastructure.

This contribution which is based on Bugheanu et. al. (2008) gives an introduction into complex operational analysis within such risk assessment and risk management processes. The authors elaborate in a first step the role of “Operations Research” and especially methods of “System Dynamics”. Furthermore, an overview of a (possible) integration of SOA-elements within such (complex) optimisation processes is indicated: We combine the approach from an operational point of view together within a service-orientated framework in order to develop a comfortable complex decision support procedure. At the end we embed our approach within a concrete and challenging example: Space and the systems within space.

By now, space holds a significant part of the nation's critical infrastructure. Besides basic essentials of today's telecommunication, timing, and navigation systems, indispensable parts of Earth monitoring systems for environment and security are located in space, too. The capabilities of those space assets are utilised by industry as well as by governmental and military users. In particular for the latter ones, round-the-clock availability of services provided by satellites is mandatory since the desired formation of situational awareness demands for fusing data of every integrated system to provide a holistic picture. However, monitoring space is a quite complex and highly dynamic task. For instance, the Space Surveillance Network (SSN) operated by the Joint Space Operations Center (JSpOC) of the United States Strategic Command (USSTRATCOM) performs up to 400,000 observations per day to detect and keep track of more than 17,000 objects orbiting Earth. The underlying technical architecture consists of 29 worldwide distributed space surveillance sensors as well as computation centres and a highly qualified crew which task is to correlate measurement data for a potentially still unknown object with the descriptive data for/of of already registered objects. This work at the JSpOC is done to support the “protection of US and friendly space systems, prevention of an adversary’s ability to use space systems and services for purposes hostile to US national security interests, and direct support to battle management, command, control, communications, and

intelligence" as documented in the USSTRATCOM Space Control and Space Surveillance Fact Sheet[2]. In Europe several communities on national and supranational level have started their own initiatives, programs or studies to identify and close capability gaps concerning the European space situational awareness (cf. Bartsch 2008, Keil et. al. 2007).

2. Critical Infrastructures as Complex Systems: The Need for OR and System Dynamics

As we learned so far and as it is summarised in Bugheanu et. al. (2008), critical infrastructures are vital elements on which our daily live and society are based on, therefore it is of great importance to pay a special attention to the protection of these elements. The following sectors can be identified as being critical infrastructure elements[3]:

Banking and Finance, Chemical Industry; Commercial Facilities; Commercial Nuclear Reactors, Materials, and Waste; Dams; Defence Industrial Base; Drinking Water and Wastewater Treatment Systems; Emergency Services; Energy; Food and Agriculture; Government Facilities; Information Technology; National Monuments and Icons; Postal and Shipping; Public Health and Healthcare; Telecommunications; and Transportation Systems.

Break-downs or disturbances of such critical systems as a result of e.g. war, disaster, civil unrest, vandalism, or sabotage, may cause severe damage in the supply of a wide part of users linked to these systems and can have severe consequences to vital functions of the society. A definition is given in the "Patriot Act 2001 of the USA" that describes cirtical infrastructures as[4]

> *"systems and assets, whether physical or virtual, so vital […] that the incapacity or destruction of such systems and assets would have a debilitation impact on security, national economic security, national public health or safety, or any combination of those matters."*

Further definitions emphasise the interrelationship of the critical infrastructure elements[5]:

> *"Critical infrastructures are the complex and highly interdependent systems, networks, and assets that provide the services essential in our daily life."*

Thus, certain sections of critical infrastructure elements depend on each other and threats or risks that concern the one can influence the other. In order to understand and to protect such complex (interdependent) systems, system theoretic approaches are therefore necessary. In this contribution we will elaborate the following statements:

The protection of critical infrastructures is a major task of Operations Research

- System Dynamics may help to master the complexity, especially within the network structures
- New technical instruments should be integrated in these complex decision support management systems
- Service orientated optimisation might be a future framework for the algorithmic and procedural solutions

3. Identification Processes and Risk Management – Vulnerability Analysis Role of Operations Research

Which methods and processes will be considered? The following description is only a rough collection of possible instruments and procedures.

- Design of early-warning- or precautionary- and recovery systems:
  How many sensors do we need;
  where should we locate them;
  can we estimate the detection time?
- Emergency planning processes:
  How many emergency units are necessary;
  how much time do we need to evacuate a certain place?
- Sensitivity of networks and places:
  Which patterns or situations are critical?
- Identification, tracking and monitorring procedures: Can we forecast a certain danger or threat?
- Computational Intelligence:
  Can we embed smart technologies in the protection plans?

These tasks of Operations Research lead to complex identification and monitoring problems. We will focus especially on the monitoring aspect in the last part where space surveillance and space reconnaissance can greatly mitigate the system endangerment by human- or technological-caused hazards as well as by hazards with natural origin.

The identification process should be linked to a risk management process, to determine e.g. the vulnerability of certain infrastructure elements and to develop special protection plans. The Department of Defence (DoD) of the U.S.A, which is the responsible authority in the protection of the national sectors: Financial Services; Transportation; Public Works; Global Information Grid Command Control; Intelligence Surveillance, and Reconnaissance; Health Affairs; Personnel; Space; Logistics; and Defence Industrial Base, has developed a "Critical Infrastructure Protection Lifecycle" (CIP) that details the above statements and consists of six phases[6]. This is described in detail in the extended version of this survey which the interested reader may find in Bugheanu et. al. (2008). These six phases underlines the necessity of an integration of Operations Research and

[2] USSTRATCOM Space Control and Space Surveillance Fact Sheet, http://www.stratcom.mil/fact_sheets/STRATCOM Space and Control Fact Sheet -- 25 Feb 08.doc

[3] George Mason University, "What is CIP", School of Law, December 2006, http://cipp.gmu.edu/cip/, accessed 30 March 2008

[4] "USA PATRIOT ACT OF 2001", October 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf, accessed 30 March 2008

[5] George Mason University, "What is CIP", School of Law, December 2006, http://cipp.gmu.edu/cip/, accessed 30 March 2008

[6] Department of Defense, "The Department of Defense Critical Infrastructure Protection (CIP) Plan", November 1998, www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm, accessed 30 March 2008

System Dynamics in this context. We may summarise that

"... the analysis and assessment phase is the crucial part of the CIP life cycle; the identification of the vulnerability and the characteristics of critical elements such as their interrelationship to other elements are central elements of an OR and system-orientated analytic process."

In the following the integration of certain IT-based systems, namely systems to provide complementary pictures of the situation in space is introduced. We call the overall system - a system of systems - SSA system since its goal is to support the formation of Space Situational Awareness as an enabler for the protection of space based services. Referring to this, Nicolas Bobrinsky, Head of the ESA Ground Station Systems Division, stated in a recent interview[7]:

"Any shut-down or loss of services from these systems would seriously affect a wide range of commercial and civil activities, including land and air travel, maritime navigation, telecommunications, climate monitoring and weather forecasting, to name just a few. For example a loss of space-based services could considerably impair the delivery of national emergency services, such as air/sea rescue or disaster recovery, in the event of any concurrent natural or man-made disaster, such as flooding or a chemical spill."

To get the knowledge, or to be more precise to form awareness about the situation in space, one needs an SSA system which provides and integrates different space situational pictures. These pictures will be based on the two building blocks Space Surveillance and Space Reconnaissance as well as on the mapping of Space Weather related data, data about Near Earth Objects (NEOs), data about Non-individually Trackable Objects (NTOs), and data w.r.t. Space Missions. Each of the situational pictures can be obtained by well-defined services to analyse and represent the fused data taken from the corresponding subsystem, e.g. from the Space Surveillance Subsystem. The complexity of each service is hidden from potential customers who only need to know the specific service interface to utilise the service.

4. Integration of IT-based Systems (Identification, Monitoring and Tracking)

The usage of IT-based Systems in order to satisfy the demand on information that is needed to achieve a sufficient situational awareness -within an Operational Analytic approach- at the particular phases is advised. One disadvantage of many systems that are in use to support the CIP life-cycle is that they often consist of a large amount of heterogeneous single applications that are inefficiently integrated into the overall process. In case of threat on a critical infrastructure element, a fast and flexible acquisition, processing, and allocation of information are crucial. Flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture (SOA) which qualifies it to be used in the context of the protection of critical infrastructure. First results are contained in Bugheanu et. al. (2008). We will state that Service-Oriented Architecture is a design concept and an suitable architecture for the protection of critical infrastructures. The design concept in SOA is about designing systems that have well-defined self-describing access interfaces, having services composed into complex processes. The architecture is about having simple mechanisms to use these access-interfaces for integration purposes:8 The advantages of a SOA-based integration will become obvious.

Imagine the potential threat (for example) of a terrorist vehicle carrying a hazardous load possibly heading towards an identified element of critical infrastructure, demands for a system that reports the current position of this vehicle to the authorities capable of escalating this potential threat. A system that is satisfying this demand is referred to as "tracking and monitoring system". This system is vital for several phases mentioned in the first part of this paper. Indications and warning phase that implies monitoring of the critical infrastructure elements to reveal possible threats and to inform authorities about the potential danger:

- Optimise the tracking system in order to minimise the overall threat
- Identify critical edges and nodes in the complex network
- Identification of critical actions
- Analysis of behavioural patterns

This leads to the central question: Which situations are critical and how can we detect those situations?

5. The Space Object Impact Risk, a risk which endangers space assets at the most

While sounding trivial, the reduction of the space object impact risk is a complex goal. One reason for the complexity is the dynamic of space itself. In consequence satellite orbits are only temporarily stable and thus, orbital data of any object has to be updated periodically to ensure that every object is retrievable at any time. Moreover, operational space objects may change their orbit autonomously and without any notice. This means for the monitoring system that its update rate has to be adjusted to a level which ensures not to lose any of those objects. To quantify the reacquisition rate, detailed knowledge about the system dynamics is necessary. In particular, one has to know if an object is passive or can actively change its orbit. But how can we achieve this knowledge?

As mentioned in the previous paragraph, an SSA system will consists of several subsystems, namely sensors but non-sensor data sources as well. From these sources any available information on space objects and their environment is

[7] SSA: Five questions with ESA's Nicolas Bobrinsky, Interview dated 2008/11/23, www.esa.int/esaMI/Operations/SEMFSG6EJLF_1_iv.html

[8] Juric, Loganathan, Sarang, Jennings, *SOA Approach to Integration* (Birmingham: Packt Publishing, 2007), 57

gathered, synthesised and interpreted. Building blocks are the following subsystems:

- *Space Surveillance Subsystem*

The task of this subsystem is to detect and track space objects. It supports the formation of situational awareness since it provides orbital information of any object which position can be tracked at least for a certain period to enable re-acquisition.

- *Space Reconnaissance Subsystem*

The task of this subsystem is to gather data about the space objects themselves. It supports the formation of situational awareness by providing object descriptive information, e.g. the type of object.

- *Space Weather Subsystem*

The task of this subsystem is to measure the electromagnetic radiation as well as the low- and high-energy particle fluxes generated by solar or cosmic activity. It supports the formation of situational awareness since it provides information about the space weather including its future.

- N*ear Earth Objects Subsystem*

The task of this subsystem is to gather data about Near Earth Objects, such as asteroids. It supports the formation of situational awareness by providing the object's orbital information and information about the objects themselves.

- *Non-individually Trackable Objects Subsystem*

The task of this subsystem is to detect and track clouds of such objects. It supports the formation of situational awareness since it provides information about the orbital distribution of space debris fragments and natural particulates.

- *Space Mission Subsystem*

The task of this subsystem is to gather available data incurred during the planning and execution of a launch, the object's early orbit phase, its mission, and its controlled ditch or return. Moreover, this subsystem may also support the aforementioned planning and execution phases.

These subsystems are an enabler to mitigate hazards, since they set up the necessary knowledge base to assess potential risks in different operation scenarios. Recalling the goal to reduce the space object impact risk, one can provide as the basis of calculation for each object:

A) Its collision probability by the knowledge of orbital data

- provided by the Space Surveillance Subsystem for preferably all man-made objects
- provided by the Near Earth Objects Subsystem for natural objects, e.g. asteroids

and

B) The expected extent of (collateral) damage by the help of

- the Space Reconnaissance Subsystem which provides a characterisation of the collision partner
- the Space Mission Subsystem which provides a characterisation of an impact
- on ground,
- within the air transport corridor, and
- on the way to or from its orbit for a launched object or an object with a scheduled ditch or return.

Thus, several highly complex services have to be utilised to achieve the objective.

6. Concluding remarks

The future protection of global and national critical infrastructure cannot neglect the holistic aspect that the complexity of space and systems therein demand for integrated approaches. System dynamics and service oriented optimisations are supposed to support the design of effective processes to fulfil the needs w.r.t. SSA. For that reason the authors propose a new way of service integration within these complex challenges to protect critical infrastructures.

REFERENCES

Aidala, V. J and Hammel, S. E , "Observability Requirements for Three-Dimensional Tracking Via Angle Measurements," *IEEE Transactions on Aerospace and Electronic Systems, AES-21*, 2 (Mar. 1985): 200-207.

Bartsch, G. and Letsch, K. (2008), "Space Situational Awareness as a Key to Safeguard Space Assets", Proceedings of the International Disaster and Risk Conference (IDRC) / Global Risk Forum Davos, 2008, Extended Abstract, pp. 807-809 , Invited Talk

Bugheanu, R., Dumitrascu, M., Mihelcic, G., Pickl, S. (2008), Monitoring and Controlling an International Experiment: Optimization of Sensor Allocation and Operations in MIO Scenario, Proceedings of the 2008 Networking and Electronic Commerce Research Conference NAEC 2008, Riva del Garda, 362-371

Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices* (Prentice Hall PTR, 2004), Ch 2.2-2.4

Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices* (Prentice Hall PTR, 2004), Ch 11.1

Keil, K.-H., Weber, H., Foth, W.-P., Bartsch, G., Wagner, A., von Chiari, M., Crescence, P. et al. (2007): ESA Study on "Capability Gaps concerning European Space Situational Awareness", Study Report

Juric, Loganathan, Sarang, Jennings, *SOA Approach to Integration* (Birmingham: Packt Publishing, 2007), 57

Parkinson, B.W. ,*Global Positioning System: Theory and Applications* (1996) ch 1

Department of Defense, "The Department of Defense Critical Infrastructure Protection (CIP) Plan", November 1998, http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm, accessed 30 March 2008

George Mason University, "What is CIP", School of Law, December 2006, http://cipp.gmu.edu/cip/, accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying", http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap12/1233.htm , accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying", http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/311.htm , accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying", http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/312.htm , accessed 30 March 2008

Security and Safety Management and Public Administration

Service orientation and event- and model-driven process management will deliver critical information infrastructure security – provided that well-designed governance, risk and lifecycle management models are applied.

Dana Procházková

Police Academy of the Czech Republic, Praha.

e-mail: prochazkovad@polac.cz

The conference „Security and Safety Management and Public Administration“ took place in Praha (Czech Republic) on September 16-18, 2008 with 153 participants from 5 European countries. The conference programme consisted of four parts:

- Good governance, security and sustainable development;
- Critical infrastructure safety;
- Grounds for safety management;
- Selected aspects of safety management.

The proceedings „Security and Safety Management and Public Administration“ with 54 papers in English were published by the Police Academy of the Czech Republic. All materials and discussions during the conference reflect the paradigm that **the State is responsible for promotion of safe and sustainable development of human society at its territory**, i.e. that security and safety management are of public interest and through this an inherent part of public administration.

The basic tools for reaching security and sustainable development are:

- management (strategic, tactical, operational) based on qualified data, knowledge, professional assessments, qualified decision-making methods, land-use planning, correct placement, designing, building, operation and maintenance of buildings, technologies and infrastructures,
- citizen’s education and training,
- specific education of technical and management workers,
- technical standards and norms including the best practice procedures, i.e. tools for control / regulation of processes that may or might lead to disaster occurrence or to its impact increase,
- inspections and audits,
- executive security forces for qualified response,
- response systems for critical situations,
- land-use, emergency, continuity, crisis and contingency planning,
- safety, emergency, continuity and crisis management.

The safety culture must be developed in a systematic fashion taking the current knowledge and experience into account. The supportive tool (called “s*afety management*“) is the strategic, proactive and process management based on risk management and on results of science and advanced technologies. It ensures:

- prevention against disasters of all kinds; i.e. natural, technological, environmental, social and caused by interdependencies in critical infrastructure, including the terrorist attacks and the existing interactions between the Human system and its vicinity,
- preparedness to put all emergency and critical situations under the control and the capability to renovate affected part of the Human system,
- emergency response if a part of the society is affected,

- recovery after each emergency or critical situation.

The safety management has three basic phases: ***the current management*** (the attention is focused on the development, prevention and preparedness); ***the emergency management*** (the attention is focused on mastering the emergency situations with help of standard sources, forces and means); ***the crisis management*** (the attention is focused on mastering the critical situations, human survival and stabilisation of situation in order to start restoration and follow up development, namely with help of standard and beyond standard sources, forces and means).

The professional results may be summarised as follows:

1. Safety today is understood as a set of measures for preservation, protection and development of protected interests that creates a base for the security and sustainable development of societies.
2. Disasters are the causes of disruptions of people's security and sustainable development. The preventive measures applied at safety management try to address such scenarios and their characteristics.
3. Because *the flood is the most frequent type of disaster* in Central Europe, there is a description of big floods, the flood prevention system and an integrated warning service system being in operation.
4. The disaster management may only be effective if it is based on the assessment of cause impact, the vulnerability related to the cause and the likelihood of the event occuring.
5. In practice there are two models of disasters management, namely the risk management and the safety management. Both management types start with an analysis and assessment of hazard and risk, safety management however includes an additional precaution principle.
6. The term hazard expresses the potential to cause detriments, losses and harm on protected interests at a given site. The term risk expresses the likelihood and probable size of undesirable and unacceptable hazard impacts (losses, harm and detriment) on protected interests of system or subsystem in a given period (e.g. 1 year) at a given site (it is always site specific). Risk has many forms. In addition to economic risks – encountered in the insurance business there are physical risks, social risks and their subdivisions (political, sexual, medical, career, artistic, military, motoring, legal….). These forms can be combined and traded. Human activities should eliminate risk when possible, however the cost of risk reduction can grow immensely. Therefore, the optimum level of safety is when the risk has been reduced up to the point where the cost for reduction just equals to its benefits.
7. For management support there are at present set up the process models, the project models, the scenarios and there are used special methodological tools as e.g. the statistical methods (normal, robust and extreme), the case studies, deterministic methods as the CPM (Critical Path Method), stochastic method as the PERT (Program Evaluation and Review Technique) etc.
8. The quality of each management is based on the quality of data, on the quality of their processing and on competence of methods that are used for decision-making. This is confirmed by results of some monitoring networks that are in operation, e.g. hydro, meteorological, geological, ionising and non-ionising radiation, environmental, human health, animal health, human behaviour (camera systems) etc. In many domains there are used for data image the advanced technologies as the GIS.
9. Today's crucial management problem is about critical infrastructure safety provision. The critical infrastructure is a set of mutually interconnected networks, i.e. the systems of various sectors of economy and society. For a decision support system, the requirement to ensure the continuity of critical infrastructure during recovery in a country affected by disaster is a good guide for the determination of critical elements, critical processes, critical functions, critical infrastructures and critical technologies in a region.
10. Research of critical infrastructure so far clearly shows that the problem of critical infrastructure safety is very complex and both, multibranched and multidisciplinary. It has technical, organizational, legislative, financial, managerial, knowledge, educational, national and international aspects.
11. Co-operation between public and private entities in the field of prevention and consequence management is very important to ensure the critical infrastructure security.
12. The solution of several practical problems are related to:
    - mass disaster victim identification,
    - property criminality,
    - physical Protection Systems of the Dukovany and Temelin NPPs,
    - tools of fight against terrorism (including a finance domain),
    - application of a forensic biomechanics in investigation processes, particularly for violent criminal acts,
    - norms and regulations for tunnel transport fire safety,
    - a compilation and use of business continuity plans,
    - legal responsibility of licensee in the domain of prevention, preparedness, response and renovation,
    - principles of co-operation among the police units, the public administration on all levels and all involved parties (one of the main missions of the European Framework Programme 7).

- All priority areas of the eighteen-month EU programme (France, the Czech Republic and Sweden) for the civil protection tasks fulfilment.

The results summarised below help to extend the generally valid knowledge to the problems mentioned above. The recommendations for further research and for practical application are as follows:

1. The effort to ensure security and sustainable development means that the public administration shall be interested in:
   - the evaluation of properties and the assessment of potential of natural and other disasters causing detriment, harm, damage and losses of preserved interests,
   - the analysis and the assessment of risks in a territory taking into account both, the territory and the human society vulnerability,
   - the qualified determination of short, medium and long term measures that lead to the growth of security and to sustainable development,
   - the preparation of eventual corrective measures for growth of safety in a territory,
   - the capabilities to control the consequences of emergency situations that lean on both, the quality preparedness of safety units, public administration, legal entities and citizens, as well as the creation of sufficient response capacity,
   - the capability to carry out the recovery of affected territory and to ensure the further development,
   - a qualified decision support system.
2. All involved parties shall concentrate their effort to global disaster reduction activities by using the modern technology and science, the efficient organization of early warning and all parts of the disaster risk reduction processes. This should include support for risk reduction activities in post-disaster recovery and processes as well as sharing of good practices, knowledge and technical support with relevant countries and experts.
3. Co-operation is required on national and international level and involvement of all possible stakeholders beginning with governmental, regional and local administration as well as any supporting services down to community and citizen levels.
4. The risk identification effort shall concentrate to obtain vulnerability knowledge of protected interests, which in many countries is not necessarily considered against individual disasters scenarios.
5. It is necessary to work in a theoretical domain with the aim to establish the methodology for integral risk determination, because the sum of partial risks, called integrated risk, does not correspond to real conditions (it does not reflect the influence of interconnections among elements in the system). Only after such excercise we shall be capable to determine an integral safety and security management which will enable our dream of a society with security and sustainable development.
6. A case study could work as a tool for identification of solution contents and general opportunities concerning a great range of complex social and technological problems. The outcome can be a good practice guide of problem solving related to safety management and crisis management.
7. An interconnection of systems addresses the mutual dependence of critical infrastructures. The linkage is required to solve several problems namely the safety of partial infrastructures and the safety of a set of mutually dependent infrastructures and will achieve a safe critical infrastructure and will harvest the sustainable development potential. With regard to the present knowledge we know that the optimum safety of the combined infrastructures is not equal to the set of optimum safeties for partial infrastructures. Therefore we must search for a solution through other means considering the system theory (so called the systems system safety).
8. For ensuring the critical infrastructure safety the following shall be implemented:
   - special solutions in land use planning, placement, design, build up, operation, maintenance, repair, upgrade, renovation, procedure changes and in case of operation disruption,
   - emergency and continuity plans to ensure the survival of critical infrastructures during possible emergency situations,
   - crisis plans for cases in which all or most of the security countermeasures fail because of an extreme disaster size or an unforeseen combination of random phenomena that intensify the disaster impacts.
9. For public administration safety management support the research shall answer the questions “What might happen?”, “Why?”, “What can we do against dangerous situations?” and “How?”
10. The public administration would analyse the risks not only from the viewpoint of social impacts but also from the viewpoint of the public administration governance system, so that decision making might even worsen can the risk event impacts.

The obligation of public administration is the management of security and safety. For the development of quality management in this domain the existing gaps demand for active research in favour of practice. **In order to master disastrous situations it is indispensable for a public administration to transfer the outcome of such research into the domain of security politics and the security system.**

Call for papers 4th International CRIS conference on Critical Infrastructures

The conference will have as the key subject: Critical infrastructures - Migration from existing technologies to future platforms. Deadline for submissions is the 1st of January, 2009.

Simin Nadjm-Tehrani

Professor Simin Nadjm-Tehrani is Director of Real-time Systems Laboratory Dept. of Computer & Information Science Linköping University, Sweden

www.ida.liu.se/~rtslab

e-mail: snt@ida.liu.se

Homepage CRIS 2009
www.ida.liu.se/conferences/CRIS2009

For a timely delivery of critical services to citizens and decision makers, two types of competences are needed: (1) protecting existing infrastructures so that we can continue to enjoy the delivery of reliable services despite the increasing threat picture (locally and globally), (2) moving forward to study the issue of reliability and security in new networked infrastructures that represent a new paradigm in service delivery. The main character of these new networks is the loosely connected nature, in some cases combined with mobility, and generally with several actors as opposed to a single owner/administrator. One example of such an ”infrastructure-less” network is described by the notion of hastily formed networks built-up in response to disasters.

The next CRIS conference will be devoted to the theme of emerging infrastructures and the issues associated with the migration from the existing infrastructures to the future decentralized and heterogeneous ones.

The 4th CRIS conference follows a series of successful international conferences on the theme of critical infrastructures (Bejing 2002, Grenoble 2004, Virginia 2006) in which actors from several communities come together to discuss the latest studies of vulnerabilities, research challenges, and results within the area of critical infrastructures. Presentation of state-of-the-art research is combined with discussion forums in which a range of stakeholders from the industry and government organisations to vendors and technology providers exchange their latest findings.

Being an international network with participants in Europe, Americas and Asia, the ambition of the forthcoming CRIS conference will be to provide a natural forum to bring together speakers from different continents in both *power networks* and *information infrastructures*, including computer and communication networks. Other critical infrastructures, such as water management systems, transport systems, banking and finance, as well as networks for defence and security are of course highly dependent on the above networks and novel analyses of their interdependencies are highly recommended. The goal is to provide a networking occasion for local cooperation as well as international exchange.

SYNOPSIS:

The special theme of the 2009 conference is:
“Critical infrastructures: Migration from existing technologies to future platforms”

The theme reflects the fact that there is a major technology shift in the 21st century with an unprecedented pace affecting all major infrastructures on which the society depends. Energy and climate concerns have brought about a wide range of new technologies for energy generation and distribution with associated decentralised regimes. Progress in microelectronics has made wireless networking a basic tenet of everyday life, and enables mobile networking with no fixed infrastructure a possibility in future scenarios. Spontaneous networks are already being promoted as a potential in disaster relief scenarios.

At the same time, the vulnerabilities and threats to the existing (traditional) infrastructures follows an exponential development, both due to wider deployment of software-intensive components and global political-economic factors that make automated and sophisticated attacks much more widespread than a decade ago.

We specifically encourage contributions that address the migration path between the old and the new; specifically, the sound and healthy transition from a protection strategy that is built around the notion of defence-in-depth, to the novel ideas of self-organising and self-managing networks with built-in resilience; or a realistic transition from a centralised power system control to open, autonomic, decentralised control architecture.

The conference will (non-exclusively) address the following research areas:

- Inherently resilient infrastructures and their scalability
- Quality of service assurance: migration to emerging infrastructures
- Monitoring and mitigation of threats: reusable components
- Socio-economic factors affecting the migration to new technologies
- Management of risk in migration to emerging infrastructures
- Resilience to failures and attacks: migration strategies
- Information network management, monitoring and configuration
- Power trading and its impact on resilience of the network
- From brittle to ductile power networks
- Wide Area Measurement System Applications
- Studies related to recent protocols (e.g. IEC 61850 in power)
- Power System Monitoring, Protection, and Control
- Distributed power generation and infrastructure change
- The changing role of energy end users
- Open information architecture for critical infrastructures
- Quantitative evaluation of infrastructure interdependencies

SUBMISSIONS:

Manuscripts that describe original unpublished work (not submitted elsewhere) in the above and related areas are solicited for post conference publications in a proceeding that will appear in IEEE explore (approval pending). The papers should be submitted in electronic form, pdf format, and have a maximum length of 8 pages in standard IEEE format. Selected papers will be published in the international journal of critical infrastructure protection (Elsevier publishers) as a fast track submission.

Important dates:

Deadline for submission: 1 January 2009
Notification of acceptance/rejection: 15th February 2009
Camera ready copy for preprints: 1rst March 2009
Final manuscript deadline: 31rst March 2009

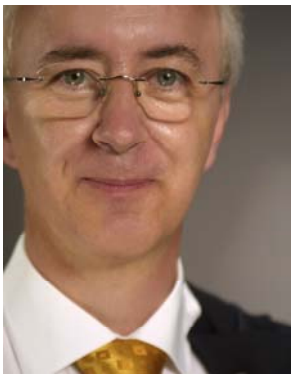
Homepage CRIS 2009
www.ida.liu.se/conferences/CRIS2009

CRITIS International Workshop Series continues 2009 and 2010

After the successful workshop in Italy the next CRITIS Conferences will take place in Bonn, Germany and Lucerne, Switzerland. Preliminary date for the next conference is September 30th to October 2nd, 2009.

Robin Bloomfield, PC Co-Chair

Robin Bloomfield is Professor of Software and System Dependability at the City University, London and a founder member of Adelard, an independent specialist Safety and Security consultancy.
email: reb@csr.city.ac.uk and reb@adelard.com
Web: http://www.csr.city.ac.uk and www.adelard.com



Erich Rome, PC Co-Chair

Erich Rome is a senior researcher at Fraunhofer IAIS, St. Augustin, Germany. He has a PhD in Computer Science and is co-ordinator of the EU project DIESIS.
e-mail: erich.rome@iais.fraunhofer.de

CRITIS 2008, the 3rd International Workshop on Critical Information Infrastructures Security, took place in Frascati, Italy, in Mid-October 2008. It attracted an even larger audience than its two predecessors. The CRITIS steering committee is happy to announce that medium-term continuity of the CRITIS workshop series is granted. CRITIS 2009 is planned to take place in Bonn, Germany, and CRITIS 2010 in Lucerne, Switzerland.

Background and Scope

Critical infrastructures (CI) found the basis of developed countries. In the last years, we observed dramatic changes in CIs. For economical, social, political and technological reasons, CIs become more and more interoperable, integrated and interdependent. These phenomena and the actual socio-political instability pose new and hard challenges for the management and protection of these systems and, more specifically, requires the development of innovative strategies to guarantee their service continuity.

The focus of CRITIS is to bring together researchers and professionals interested in CIIP and CIP.

The abundance of services of modern infrastructures is no longer thinkable without ICT that therefore has become a key-resource. At the same time ICT is considered one of the most vulnerable elements of the whole system.

The main objective of CRITIS is to bring together researchers and professionals from academia, industry and Public Offices interested or involved in all security-related aspects of Critical (Information) Infrastructure Protection (CIP / CIIP), in order to inform about new advances in CI(I)P and to foster the identification of common research interests and the establishing of co-operation networks.

Venue

The city of Bonn is located in the heart of Europe with excellent reachability. The former German capital still hosts half of the German federal ministries, plus many security related offices, including the German Federal Network Agency and the German Federal Office for Information Security (BSI). Bonn is also the headquarters of German Telekom, T-Mobile, and the German Post. All in all, Bonn is an ideal location for a workshop like CRITIS. The venue of CRITIS will be the Günnewig Bristol Hotel, located in Bonn's city centre, just a three minutes walk from the main railway station and bus terminal.

Information

General Co-Chairs: Stefan Wrobel, Fraunhofer IAIS and University of Bonn, Germany, and Costas Lambrinoudakis of the University of the Aegean, Greece.

Preliminary dates: Sep 30 – Oct 2, 2009

More information will be made available at the CRITIS 2009 web site:

http://www.critis09.org

ECN-11 Selected Links and Events

Actual Upcoming CIIP Conferences in Europe

- *IST events, http://europa.eu.int/information_society/newsroom/cf/newsbytheme.cfm?displayType=calendar&tpa_id=7*
- *INFSO D4 events, http://cordis.europa.eu/ist/trust-security/events.htm*
- *Conference CRITIS'2009 website: http://www.critis09.org*
- *CRIS Conference 2009, CRIS website:* http://www.cris.vt.edu/
- *3rd Process Control Security event (international edition), tentatively scheduled on April 23, 2009, Amsterdam, Netherlands.*

Studies on EU Policy Initiative on Critical Communication and Information Infrastructure Protection

- *Promoting a secure Information Society: http://ec.europa.eu/information_society/policy/nis/index_en.htm*
- *The main elements of the Secure Information Society strategy were endorsed by the European Council in a Resolution http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:068:SOM:EN:HTML*
- *European Programme for Critical Infrastructure Protection: http://europa.eu/scadplus/leg/en/lvb/l33260.htm*
- *Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection: http://register.consilium.europa.eu/pdf/en/08/st09/st09403.en08.pdf*
- *ARECI Study: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm*
- *EISAS–European Information Sharing and Alert System: http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf*
- *Critical information Infrastructure Protection (CIIP) : http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm*
- *The International CIIP Handbook 2008/2009: www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663*
- *SCADA Security Good Practices for the Drinking Water Sector: www.samentegencybercrime.nl/Nieuws_over_cybercrime/Good_practices_drinkwater?p=content*

European Projects or Projects with Articles in this Issue

- *IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems: www.irriis.eu*
- *The Möbius Modelling tool: www.mobius.uiuc.edu*
- *Network Simulator: www.isi.edu/nsnam/ns*
- *The DIESIS Project: Design of an Interoperable European federated Simulation network for critical InfraStructures, project web page: www.diesis-eu.org*
- *Dutch TNO: www.tno.nl*
- *Governance and Risk Management in a globally integrated Ecosystem: References: www.athena-ip.org www.opengroup.org/togaf/*

The IEEE Press, a leader in publishing for the Engineering professions, has teamed with John Wiley & Sons, a pre-eminent publisher of non-fiction and educational texts to create the Wiley-IEEE Press.

CALL FOR PUBLISHING PROPOSALS

The Wiley-IEEE Press is seeking publishing proposals in all the Electrical Engineering subject areas, but most particularly in:

- Power Engineering
- Alternative Energy
- Biomedical Engineering
- Digital and Mobile Communications
- Nanotechnology
- Computational Intelligence
- Microelectronic Systems
- Microwave Technology
- Electronics Technology
- Telecommunications
- Engineering Management

CONTACT US

www.ieee.org/press

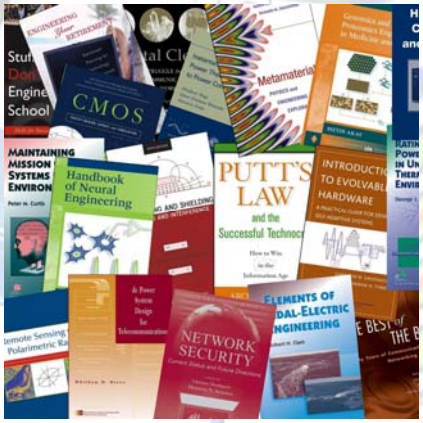
Jeanne Audino, Project Editor
445 Hoes Lane
Piscataway, NJ 08854 USA
Phone +1 732 465 5830
Fax +1 732 562 1746
s.m.welch@ieee.org
www.ieee.org/press
www.wiley.com/ieee

Lajos Hanzo, Editor in Chief
University of Southampton
Dept. of Electronics & Computer Science
Highfield, Southampton, UK
SO17 1BJ
lh@ecs.soton.ac.uk

IEEE
IEEE PRESS

CALL FOR AUTHORS

Frequently asked questions and answers for prospective book authors



IEEE
IEEE PRESS

WILEY
1807-2007
KNOWLEDGE FOR GENERATIONS

PUBLISHING WITH THE WILEY-IEEE PRESS

Frequently Asked Questions

WHEN SHOULD I TRY TO FIND A PUBLISHER FOR MY BOOK?

As soon as you have a clear idea of what your book project should be. Identify an area in which you have expertise. Then, find something new or better to contribute than what is already in other published books. Your next step is to prepare a proposal. Follow the IEEE Press Proposal Guidelines found at www.ieee.org/press.

HOW LONG DOES IT TAKE TO MAKE A PUBLISHING DECISION?

Once the proposal and sample materials are received it takes about 4-6 weeks to secure proposal reviews, another 2-3 weeks for author's response to the reviews and project financial/marketing prep and presentation, and another 2 weeks for contract negotiation/signing. From beginning to end the process takes about 2-3 months, although time frames vary.

WILL I BE PAID A ROYALTY?

Royalty rates are competitive with the rest of the publishing industry. They are determined during contract negotiation.

WHAT KINDS OF BOOKS ARE YOU LOOKING FOR?

The better question is: "What are *you* qualified to write and interested in writing?" IEEE Press staff and volunteers collaborate on a list of "hot" topics—cutting-edge or under-served areas where we think there is both an interest and need for new books. The list is prepared to generate discussion and motivate volunteers who help us identify projects. Since it is highly subjective, it should not exclude other topics. We welcome input on new topics that should be added to the list. See the current list of topics on the back of this FAQ.

WHO HOLDS THE COPYRIGHT IN THE BOOK? HOW IS IT "BRANDED"?

Authors contract with the IEEE Press to grant the IEEE copyright on the published work. The IEEE Master Brand appears at the top of the spine and the Wiley Colophon at the bottom. Both brands appear elsewhere on the cover and inside the book. If the book is in a series, the series brand and identification appears on the cover and title page. If an IEEE Society sponsors the book, that information appears on the title page.

WILL MY BOOK HAVE AN EDITOR?

Writing a book can be a daunting task, especially for a first-time author. That's why we give you a lot of advice. The first step to receiving that advice is to complete the proposal, along with a detailed table of contents and a representative chapter.

You'll receive feedback every step of the way from our Editor in Chief, Series Editor, staff editors, and reviewers from the IEEE volunteer community. All IEEE Press books are technically reviewed prior to acceptance for publication.

DO YOU OFFER FULL PRODUCTION SERVICES OR DOES THE AUTHOR TYPESET THE BOOK?

Through our relationship with John Wiley and Sons, we offer our authors full production services: copyediting, art preparation, page make-up, and collaboration on all aspects that affect the aesthetics of the final, printed book.

HOW ARE THE BOOKS PROMOTED?

Wiley is primarily responsible for the marketing of our books through its worldwide sales & marketing channels. IEEE and individual Societies include our books in member marketing and advertising. Press books can be purchased through IEEE Xplore and the IEEE Store. Wiley has created a special for our books at www.wiley.com/ieee