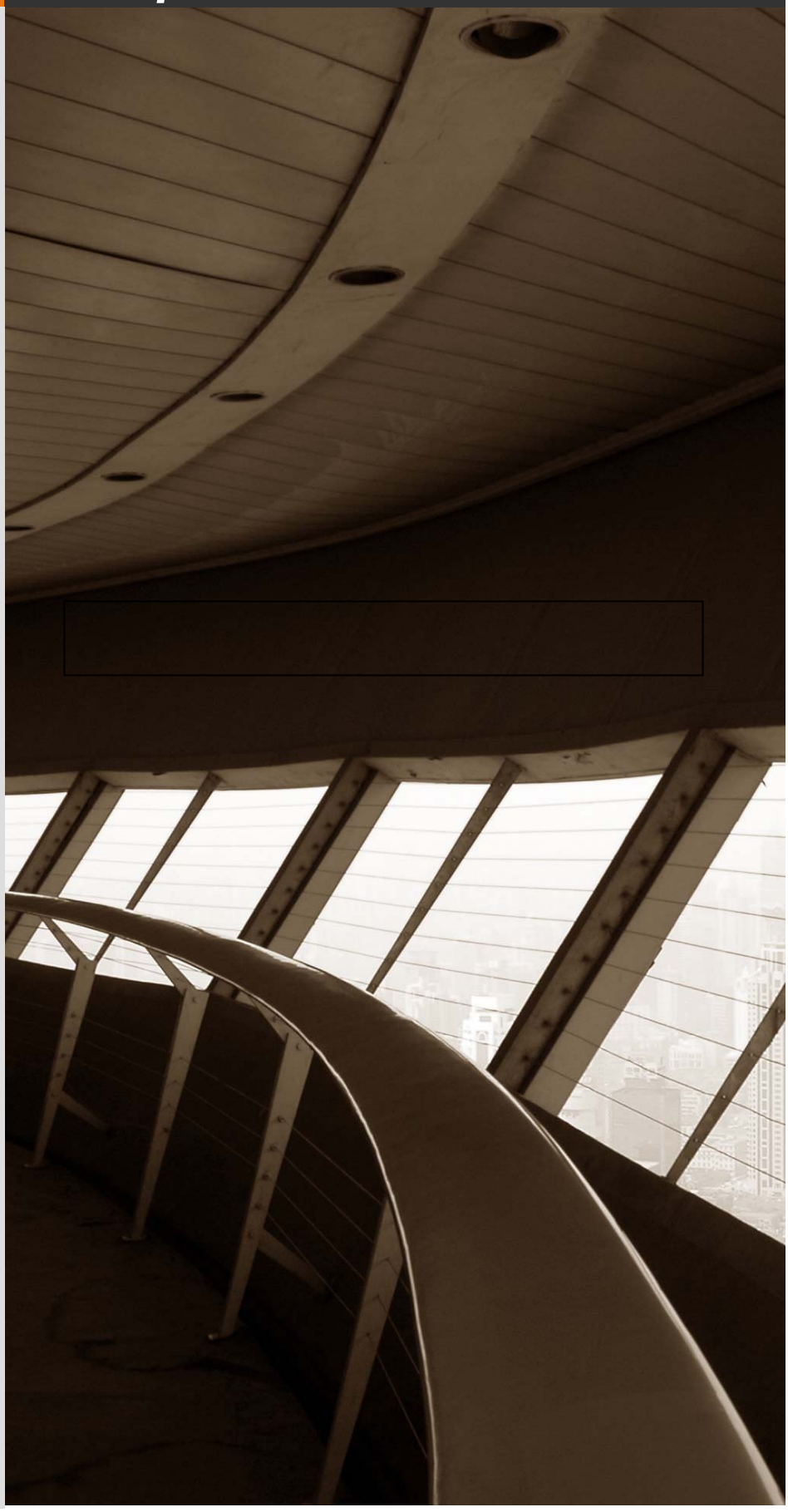
July / August 2008, Volume 4, Number 2

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

Relevant results from long lasting work on C(I)IP will be tangible

With the tenth ECN issue the articles move from awareness to case studies, results of C(I)IP research and conceptual innovations. C(I)IP is now discussed for years at policy and conceptual levels. The policy actors have completed fundamental studies and start to take action.

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

About this Issue

Andrea Servida highlights the background on which an EU policy initiative on Critical Communication and Information Infrastructure Protection (C(I)IP) may grow and gives inside into the action points of this initiative.
Two articles on the Integrated Risk Reduction of Information-based Infrastructure Systems "IRRIIS" project follow:

- An overview on IRRIIS is given, pointing out the SimCIP simulation and the four components of the middleware improved technology MIT.
- Functional principle of MIT middleware improved technology and its four main component give insights on the tool.

The *EUropean Risk Assessment Methodology project EURAM* integrates with the same yardstick risk assessment form corporate level up up to European level. The elaborated results are presented and an outlook for the successor project EURACOM is given.

A report on *The First Dutch Process Control Security Event* is given by Eric Luiijf pointing out the strong need for actions in securing PCS. Three general recommendation discussed during the Event are disclosed to the reader.

The Royal Academy of Engineering published its report *Dilemmas of Privacy and Surveillance* in March 2007. In spite of all securing measures this report demonstrates how to consider urgent demands of our privacy.

Today's risks to the financial sector discloses that "Financial Industry Sector" lost its e-innocence: New e-risk factors have appeared. As a result, the financial sector has to deal with e-espionage, identity theft and the problems of international terrorism.

Cyber Security Assessment of a Power Plant analyses in a true corporate environment the risk of attacking the power process control environment. The results are presented in text and graphs.

Governance and Risk Management in a globally integrated Ecosystem discusses critical information infrastructure assurance and its approach of model-driven risk management presuming robust enterprise architecture (EA).

Furthermore, news on *The International CIIP Handbook 2008/2009*, events such as Critis'08, IMF 08 and ICCR is presented.

First universities start to offer professorships on C(I)IP. See the advertisement of the University of Lisboa Faculty of Sciences FCUL.

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.

Towards an EU Policy Initiative on Critical Communication and Information Infrastructure Protection[1]

Several EU studies on Critical Communication and Information Infrastructure Protection have been completed. CIP strengthening actions are planned based on the preliminary studies, the G8 principles and OECD activities.

Andrea Servida

Deputy Head of Unit
European Commission,
Directorate General Information Society and Media

e-mail:
andrea.servida@ec.europa.eu

Communication and information infrastructures are the nervous system of the Information Society. Many services and processes in our economy and society are increasingly dependent on the proper functioning of these infrastructures. In addition, the processes of liberalisation, deregulation and convergence have brought about a multiplicity of players, while nowadays a large part of these infrastructures are owned and operated by the private sector. At the same time, by their nature, communication and information infrastructures often stretch out well beyond national borders. Their level of security and resilience in any country depends heavily on the level of security and resilience which have been put in place outside its national borders. In this respect, national governments face very similar issues and challenges while the private sector is calling for harmonised protection measures.

Because of this trans-national dimension, a more integrated and co-ordinated approach throughout the European Union may usefully complement and add value to the programmes which are already in place within Member States. It will also contribute to reinforce the wealth creation capabilities of the European single market. To address these issues, in May 2006, the European Commission made proposals to revitalise its strategy for a Secure Information Society[2]. This strategy defines a holistic approach to network and information security (NIS) in Europe, highlighting the respective roles and obligations of each and every stakeholder. In 2007, the main elements of this strategy were endorsed by the European Council in a Resolution[3] that provided a strong political signal of the need to work together towards enhancing the level of NIS in Europe.

One of the main actions announced in the strategy is the multi-stakeholder dialogue on the security and resilience of communication and information infrastructures as the Information and Communication Technology (ICT) sector specific approach under the European Programme for Critical Infrastructure Protection (EPCIP) adopted by the Commission at the end of 2006[4]. In June 2008, the European Council reached a political agreement on a directive on the identification and designation of the European Critical Infrastructures and the assessment of the need to improve their protection[5] that constitutes one of the main elements of

[1] Disclaimer: the views presented in this paper are those of the author and do not necessarily represent those of the European Commission

[2] COM(2006) 251 of 31.05.2006 (http://ec.europa.eu/information_society/policy/nis/index_en.htm)

[33] Council Resolution 2007/C 68/01 of 24.03.2007 (http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:068:SOM:EN:HTML)

[4] See http://europa.eu/scadplus/leg/en/lvb/l33260.htm

[5] See http://register.consilium.europa.eu/pdf/en/08/st09/st09403.en08.pdf

EPCIP. The formal adoption of this directive is expected by the end of the year.

The multi-stakeholder dialogue on the security and resilience of communication and information infrastructures will contribute to shape up the Commission policy initiative on Critical communication and Information Infrastructures Protection (CIIP) planned for the beginning of 2009. The objective of this initiative, which is part of the Commission Legislative Work Programme for 2008, will be to enhance the level of CIIP preparedness and response across the European Union. To achieve this aim, the initiative will build on national and private sector activities and will involve relevant public and private stakeholders in ensuring that adequate and consistent levels of preventive, detection, emergency and recovery measures are put into operation to ensure a high level of security and resilience of critical communication and information infrastructures as well as to guarantee the continuity of services.

The preparatory steps

To prepare the initiative on CIIP, the Directorate General Information Society and Media of the European Commission has launched a number of studies and consultations.

The first study was launched in 2006 to assess the on availability and reliability of electronic communication infrastructures. The study, which is called ARECI and was carried out by Alcatel–Lucent, has identified ten recommendations and addressed to private sector, Member States and the European institutions. The recommendations cover a number of critical areas, such as emergency exercises, critical infrastructure information sharing, inter-infrastructure dependency, formal mutual aid agreements, priority communications on public networks and interoperability testing. The study also highlights the need for a much stronger and effective public private partnership at National and European level. The publication of the ARECI final report was followed by a call for comments that engaged a number of private and public stakeholders in providing comments on the findings and recommendations of ARECI[6].

In 2007, Directorate General Information Society and Media of the European Commission requested the European network and information security agency (ENISA) to investigate the feasibility of a European Information Sharing and Alert Systems (EISAS) that would build on existing national systems, be of benefit for the EU citizens, help share information and pool together expertises. The EISAS final report[7] highlights both the benefit of fostering the dialogue among national information sharing systems as well as the need to take a step-wise approach to realise such a system. To this end, earlier this year the European Commission launched a call for proposals for a prototype of a European multilingual information-sharing and alert system under the EPCIP financing scheme.

In additions to studies, the Directorate General Information Society and Media launched a round of consultation via workshops with Member States and private stakeholders on country code Top Level Domain (ccTLD) Contingency Plans; raising security awareness and strengthening the trust of end-users; on lessons learnt from large scale attacks on the Internet; the definition of ICT sectoral criteria; the role of private sectors in protecting critical communication and information infrastructures. Detailed information on findings and recommendations of these discussions are found on the Directorate General Information Society and Media web page on CIIP[8]. More consultations are planned in the remaining part of the year.

The planned areas for action

The preparatory activities have helped the European Commission to identify both the key issues to be addressed in the planned policy initiative on CIIP as well as the potential synergies to be developed between preventive measures and reactive measures, including those pertaining to the cooperation of law enforcement and judicial services in fighting cyber-crime and cyber terrorism. The main areas for action currently being considered are:

- The definition of the sectoral criteria to identify the European critical infrastructures for the ICT sector, as foreseen by the directive on the identification and designation of European Critical Infrastructure.
- The improvement of the incident response capability at national and Europe level. The intention is to invite Member States to establish/reinforce national incident response capability, possibly built on National/Governmental CERTs/CSIRTs, as a key resource for preparedness, information sharing, coordination and incident response. A central task of such a national incident response capability would be to organise National exercises for contingency planning and disaster recovery whose importance will be highlighted. Member States will also be encouraged to reinforce the pan European cooperation between National/Governmental CERTs/CSIRTs with a view to

[6] See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm

[7] See http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf

[8] See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

facilitate the exchange of information, technical measures and good practices; enhance the preparedness at the European level by organising regional exercises and/or pan European on simulated large-scale network security incidents/attacks; facilitate the contact and cooperation between National capabilities in case of incidents or crises. Lastly, National/Governmental CERTs/CSIRTs may constitute the key component of a multi-lingual European Information Sharing and Alert System (EISAS).

- The development of a trusted public-private partnership at the European level on security and resilience to support information sharing and dissemination of good practices.
- Bridging gaps on national CIIP policies across Europe and reinforcing the cooperation and the information exchange between Member States. To date, only a limited number of Member States has developed policy approach in this area. Building on the existing activities and work, a mechanism will be proposed to support information sharing and transfer of good policy practices between Member States.
- The international dimension of CIIP to reinforce co-operation on global issues, in particular the security and the robustness of the Internet.

Several other issues will require attention among which are the need to plan for recovery and continuity strategies, the definition of cross-sectors proactive information assurance methods, the promotion of risk management culture and tools and the consideration of inter-dependencies.

In shaping up this initiative, internationally recognised principles like the G8 principles on CIIP and the UN General Assembly Resolution on the 'Creation of a global culture of cyber security and the protection of critical information infrastructures', as well as OECD related activities would be taken in due account.

This initiative will constitute a significant step forward in the implementation of the Commission's strategy for a Secure Information Society.

Project IRRIIS – preliminary results to increase dependability of CIs

After two years of project work a set of models and first prototypes of tools are available to support analysis of CI interdependencies and to manage critical events that affect the resilience of networked large complex critical infrastructures.

Rüdiger Klein

Dr. Klein is senior researcher at the Fraunhofer Institute for Intelligent Analysis and Information Systems; Project Coordinator of the EU Integrated Project IRRIIS
Phone +49-2241-14-2608
E-mail: ruediger.klein@iais.fraunhofer.de
Website: www.sit.fraunhofer.de

Mechthild Stöwer

Senior consultant and researcher at the Fraunhofer Institute for Secure Information Technology (SIT)
Department Secure Processes and Infrastructures (SPI)
Phone +49-2241-14-3123
E-mail: m.stoewer@sit.fraunhofer.de
Website: www.sit.fraunhofer.de

Final project year for IRRIIS has begun

The EU-integrated Project "Integrated Risk Reduction of Information-based Infrastructure Systems – IRRIIS" has started in February 2006 with the target to enhance substantially the dependability of Large Complex Critical Infrastructures (LCCIs) by developing appropriate models for interdependency analyses, provide techniques to simulate dependent infrastructures and to deliver Middleware Improved Technology (MIT) components to manage interdependent critical infrastructures.

In focus of the project activities are (inter)dependencies between two different CIs of the same or in different sectors. The electrical power and telecommunication infrastructure are of special interest in this case and have been selected to be the first test cases for IRRIIS analyses and developments.

The project is supported by the European Union's Sixth Framework Programme and brings together partners from research and industry from eight EU countries and Switzerland. Among them are important operators of telecommunication and electrical power infrastructures and technology providers.

Inclusion of stakeholders view

IRRIIS final target is to achieve a broad utilisation of the project results by the stakeholders from research and industry. Technology components should be included in the portfolio of operators and technology providers as well as the developed methods and models which in particular address the research community.

This requires constant feedback on project activities and results:

- The project is accompanied by an advisory board consisting of representatives of research organisations and relevant companies operating in the field of LCCIs. This board evaluates results and gives advice for promising development paths.
- To include broad feedback three international workshops have been organized so far which were attended by more than 200 participants.
- The feedback process is supported by bilateral discussions with operators of CIs and technology providers to present and evaluate IRRIIS developments.

This close cooperation will guaranty that the results of the projects fit to the specific needs of stakeholders who will use them to increase stability and resilience of CIs and push the progress in scientific research.

Fundamental analysis and future network requirements as basis of IRRIIS developments

The ambitious targets of the project also include the objective that the IRRIIS developments will support requirements

of future networks that already become visible and that may aggravate the effects of interdependencies between CIs. For the electrical power infrastructure these are in particular:

Basic research is necessary to understand CI interdependencies, dynamics and cascading effects

- Smart grids require more flexibility than existing network structures:
- Increased competition in energy market is leading to high cost pressure:
- Infrastructures are aging and required investments often are delayed:
- A lack of experts to operate CIs is emerging:
- A high number of small scale units based on renewable energy sources and combined heat and power plants (CHP) mainly in distribution networks and large offshore wind parks with increasing distance from load centres have to be integrated and managed.

These challenges increase the demand for intelligent management systems which will be considered in the IRRIIS modelling activities and included in the development of the technology components.

IRRIIS methodology: Understanding (inter)dependencies

Though the topic of CI dependencies is of high interest, the variety of methods for analysis is very limited and the current approaches do not provide enough support for analysis of real life-situations. As main deficits the following two factors are identified [1]:

- A sharp definition of dependencies is still missing, and
- Appropriate support for modelling essential real-life influencing factors as quality factors, various states of operations and environmental factors is missing.

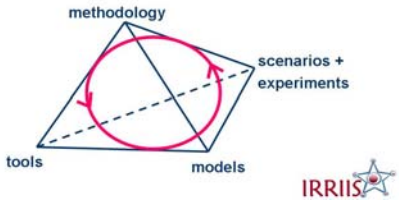
To overcome these deficits a methodology is provided to assess the risk factors to CIs at the various levels of abstraction (management, service, cyber, and physical) including an assessment whether IRRIIS Middleware Improved Technology (MIT) may help to mitigate threats and incidents. The approach is supported by a failure database maintained by an IRRIIS project partner.

Modelling complex network infrastructures

Complex networks are inherently difficult to understand because of their structural complexity, network evolution and component diversity. For research on complex infrastructure networks and as a basis for their reliable management a set of appropriate models is required.

Generic and specific models can be distinguished. For interdependency analyses different models for network behaviour including topology analysis and information models are of special relevance:

IRRIIS is a highly interdisciplinary project



- The IRRIIS Information Model was developed as an expressive common framework for modelling and analysis of systems of dependent critical infrastructures. It provides a “lingua franca” in the tradition of semantic models for structures, behaviours, events and actions which are suitable for models of quite different types. They are needed for the various kinds of networks and their interdependencies to be modelled within IRRIIS. It features a network-of-networks approach where the different networks and their interdependencies can be modelled within a unique framework. The IRRIIS Information Model extends the Implementation-Service-Effect (ISE) Metamodel approach by including additional layers and modes. Target groups are scientific researches but also infrastructure providers. [2]
- Preliminary Interdependency Analysis - PIA and Network Analysis:
Understanding the behaviour and risk of Critical Infrastructure (CI) requires an understanding of the dependencies, and consequently interdependencies, within and between critical infrastructures. Knowing the existence and possible mitigating policies against the effects of interdependencies can be used to increase the dependability and resilience of critical infrastructure. The Preliminary Interdependency Analysis (PIA) and the Network Analysis are methodologies for performing interdependency analysis in critical infrastructures. These models can also be used to support the design and implementation of Middleware Improvement Technology (MIT). [3]

One task for the last project phase will be the consolidation of these different project models to achieve a coherent view on the challenges of networked CIs.

The IRRIIS SimCIP simulation environment

SimCIP is the main IRRIIS simulation tool. It is used to implement network of network models based on the IRRIIS Information Model. It is implemented on the advanced agent based simulation environment LampSys. It allows:

- to model and to simulate systems of Critical Infrastructures,
- to analyse dependencies within complex infrastructure systems and between them,
- to communicate with the MIT tools used in IRRIIS for risk estimation, crisis prevention, and
- communication between CI.

For this purpose, SimCIP has:

- a model editor allowing users to build the simulation models,
- a sophisticated simulation kernel allowing to process simulation models,
- an attractive Graphical User Interface allowing users to control simulations and to visualize simulation results,
- interfaces to external simulators (an interface to Siemens SINCAL simulator is available),
- an interface to import structured data for simulation model building, and
- a Web service interface to the MIT tools.

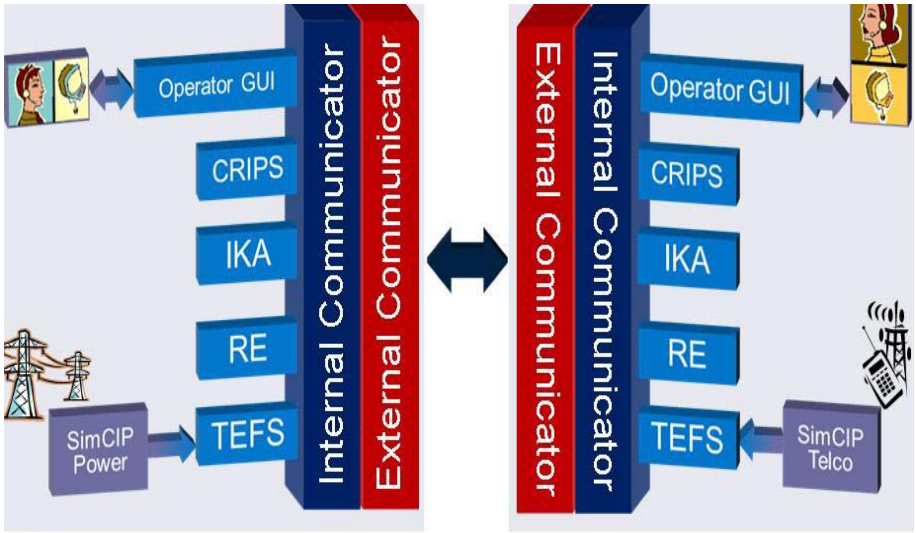
The latter allows using SimCIP as a test bed for the IRRIIS Middleware Improved Technology (MIT) components.

IRRIIS Middleware Improved Technology - MIT

To support and facilitate the communication between different infrastructures, IRRIIS has developed appropriate middleware communication components. All communication between different LCCIs should be handled by this middleware layer in a standard way.

MIT is made up of:

1. the MIT communication component which is created as a common "message layer" to dispatch information CIs can/want to share, and
2. MIT add-on components enhancing the capabilities of already existing tools to improve resilience and to mitigate cascading effects. These are:



- Tool for Extracting Functional Status (TEFS) to identify current functional statuses (in service/out of service and/or quality of service if relevant) and expected ones in the near future. For this, TEFS will carry out fusion of already available and real-time data issued from various tools used by the LCCI operator to monitor the infrastructure.
- Risk Estimator (RE) to evaluate the risk level of degradation/outage of services that are critical for the mission of interconnected external infrastructures. For the realisation of such function RE "correlates" the information about the status of the processes acquired from the local TEFS MIT components together with the analogue information acquired from the MIT systems of the external infrastructures.

Other 'optional' add-on components of MIT are:

- Crisis Prevention and Planning System (CRIPS) to provide knowledge based decision support [4]
- Incident Knowledge Analyser (IKA) aims at making the most of LCCI experience about past failures or critical conditions by properly storing and checking at run-time whether the current situation has any similarity with one which led to a disruption of operations in the past in order to make useful forecast and take proper countermeasures.

Other add-on components may be defined and integrated in the tool set.

Together with SimCIP and other additional system components MIT builds the IRRIIS architecture.

Scenarios and experimentation

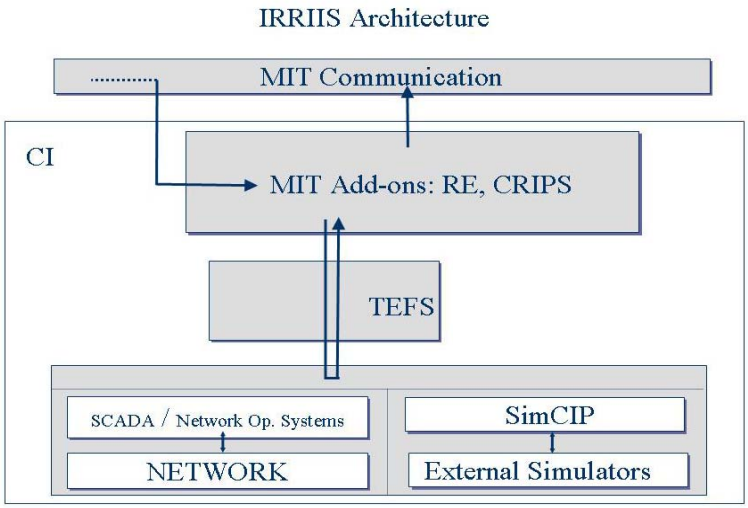
All IRRIIS developments have to be evaluated by realistic scenarios and experimentations. For this purpose scenarios including four types of CIs have been specified and updated for IRRIIS experimentation. Different types of fault and attack scenarios which impact at least a couple of infrastructures will be applied.

To show the adoption of future challenges an appropriate scenario will be built which consists of realistic future networks in the power and/or telecommunication domain.

Use cases for IRRIIS components

The real benefits of the IRRIIS developments will become visible by specifying appropriate use case. There are mainly four use cases to show the impact of the components:

- Using SimCIP to analyse (inter)dependencies of CIs and identify threats caused by disturbance of services from connected CIs and specify related vulnerabilities. Results of these analyses can be used to improve risk assessment including specific risks induced by (inter)dependencies.
- SimCIP and MIT will contribute to a cost effective optimisation of CIs' network infrastructure design by supporting the assessment of different architectural concepts regarding resilience of CIs. This contributes to a mitigation of risks caused by disturbances of services from connected CIs by implementing well targeted investments regarding redundancies and diversities of network components leading to optimised network infrastructures.
- IRRIIS components support the handling of critical events having earlier and better information and appropriate decision support available. This means more time to decide and to make better decisions on a solid basis.
- By rising awareness to (inter)dependency effects IRRIIS can support the training of operators improving their skills of handling of critical events caused by disruption of services from other CIs. As IRRIIS components can be integrated in existing training environments the new components easily can be adopted.



Demonstration and training Events

The system environment and the impacts will be demonstrated to interested LCCI-stakeholders in three demonstration events in Oct/Nov. 2008 in Germany, and in spring 2009 in Italy and Spain.

One additional training event will take place in spring 2009 in Germany to make stakeholders familiar with all IRRIIS components.

Summary

After two years of project work the IRRIIS team has elaborated a set of methods and models to achieve an in-depth understanding of (inter)dependencies CIs. This knowledge is used to provide first prototypes of the simulation environment SimCIP and the IRRIIS MIT communication platform and add-on components. The systems will be evaluated by realistic scenarios and experiments. Within three demonstration events the benefits of the solutions will be shown applying appropriate use cases.

More information about the project approach and results is provided by the IRRIIS web site: www.irriis.org, www.irriis.eu

References

[1] A. Nieuwenhuijs, E. Luiijf, M. Klaver, Modeling Critical Infrastructure Dependencies, Paper presented at: Second Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Arlington, Virginia 22201, March 16-19, 2008

[2] Uwe Beyer, Felix Flentge, Towards a Holistic Metamodel for Systems of Critical Infrastructures preliminary version in European CIIP Newsletter, Volume 2, Number 3

[3] See IRRIIS Deliverable 2.2.4: Report on service-oriented interdependency analysis, available on IRRIIS web site

[4] Dellwing, H., Schmitz, W. CRIPS – Knowledge based Emergency Management tool in European CIIP Newsletter, Volume 3, Number 2

MIT: A software tool to facilitate CIP

Data exchange between interdependent infrastructures is thought to increase the resilience of large complex critical infrastructures. Middleware Improved Technology is being developed by AIS Ltd under the FP6 project, IRRIIS, to facilitate this data exchange.

Mario Schembri

Ing. Mario Schembri is managing Director for AIS Group of Companies, Malta.

Email: mario.schembri@ais.com.mt
Website: www.ais.com.mt

MIT (Middleware Improved Technology) is a software tool which aims to facilitate data exchange and therefore mitigate cascading effects between LCCIs (Large Complex Critical Infrastructures). This software is being developed by AIS Ltd as has been specified in the FP6 project, IRRIIS (Integrated Risk Reduction for Information Based Infrastructure Systems).

Company Background: AIS Ltd.

Advanced Industrial Systems (AIS) Limited is a customer solutions-oriented engineering company with specific expertise in developing and implementing nationwide SCADA systems. AIS is the technology provider in IRRIIS by developing the software tools specified in the project to help mitigate the cascading effects in LCCIs, i.e. MIT.

The aim of this tool is to mitigate cascading effects in LCCIs by facilitating data exchange

Middleware Improved Technology

The aim of this tool is to mitigate the cascading effects in LCCIs. This is done by increasing and facilitating data exchange whilst also providing a means of measuring probabilistic risk values for service failure between interconnecting LCCIs.

The architecture used to develop MIT can be seen in Figure 1. MIT has been developed consisting of the communication components and various add-on components. The communicationcomponents are the basis for the MIT, onto which the add-on components can plug in. Add-on components developed by AIS include the Risk Estimator, the Incident Knowledge Analyser and the Tools to Extract the LCCI Functional Status (TEFS). IABG has developed the Crisis Prevention and Planning System (CRIPS) add-on component. MIT allows for other add-on components to be added to the software in the future. Once an LCCI decides to install and use MIT, the user can select which of the add-on components to install and use. The essential software would include the communication components, the risk estimator and TEFS. Each of these components would need to be customised by an expert to suit the LCCI's individual needs. The user can then select which of the other add-on components to install and use.

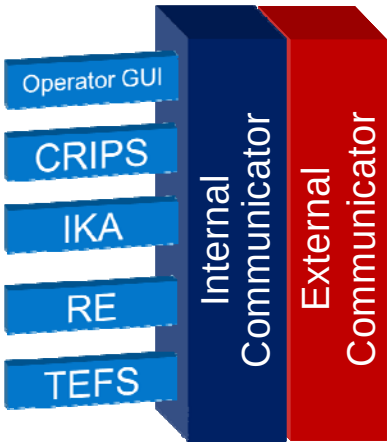


Figure 1 - MIT Architecture

The MIT Communicator

The communication components are made up of four main parts:

• A Sender module, called the Publisher

• A Receiver module, called the Subscriber

• A Graphical Interface to enable operators to view and send messages

• A web interface, called the LCCI Portal, which allows Operators to register for information.

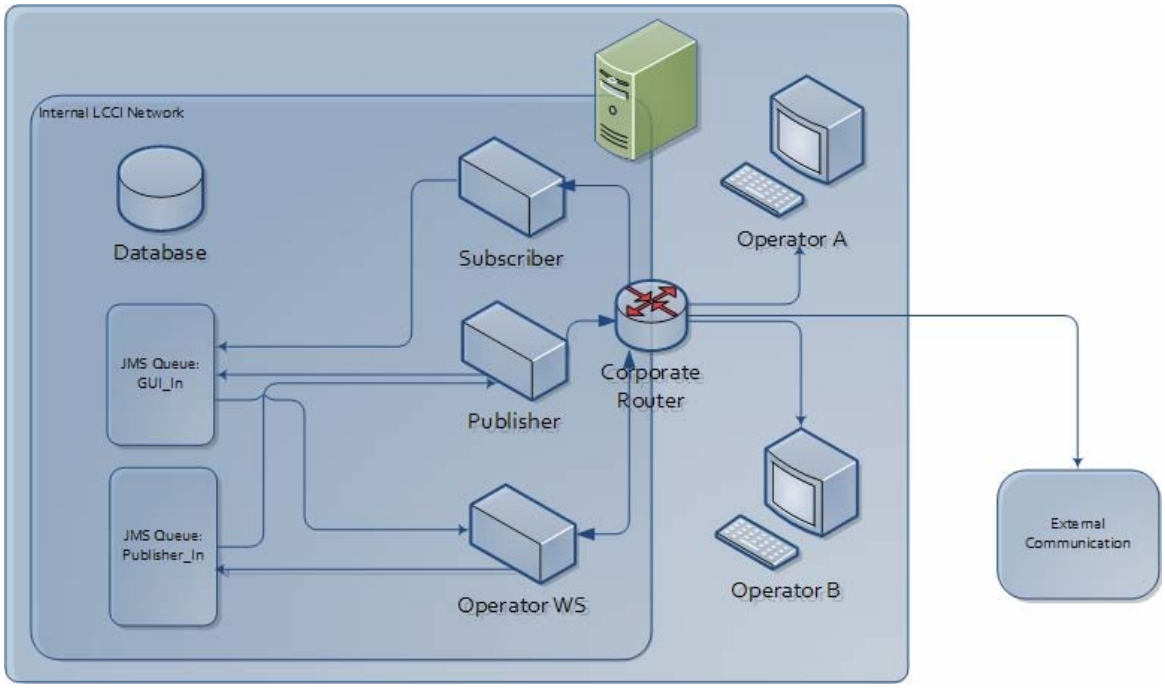


Figure 2 - Schematic Representation of the Communicator in a typical IT Infrastructure setup

A web-based administration tool is available for administering local users, diagnose and view the current configuration and for validating Operator subscriptions. As part of the communication process, an encryption library is used to encrypt and sign all outgoing messages, verify the signatures and decrypts incoming messages.

The layout of a typical operator interface would be as shown in Figure 2. Operators connect to system by means of the operator web service (Operator WS). This web service provides a link between the operators and the server resources. A corporate router will provide the necessary security to keep the infrastructure and the operators safe.

The publisher and subscriber modules are implemented as a web service client and a web service respectively. The publisher has an outbound connection to the web services on other Operators, and it calls a method on the web service that allows it to pass an encrypted XML message. The subscriber has an incoming interface, and provides methods that facilitate communication and key sharing functionality.

The MIT Tools to Extract LCCI Functional Status (TEFS)

TEFS is an essential part of the MIT components. It is basically the tool that will interface the MIT to the LCCI's infrastructure. In the case of a power LCCI, the TEFS component will be the interface to the SCADA system and MIT will read all necessary data through this component.

The MIT Risk Estimator

The Risk Estimator can be seen as a risk evaluation engine with notification capabilities based on an expert system and a Fuzzy Control Language (FCL) approach. It is based on an abstract model of the LCCIs as these are modelled in terms of services and processes.

Services are defined as the delivery of the final product consumed by the infrastructure's customers. Hence in the case of the power industry the service would be the availability of power supply to the customers. Processes on the other hand are defined as the carriers of the services. Hence, in the case of the power industry the process would be the power line availability.

The fundamental building blocks of the system will therefore be represented by the set of entities that define the LCCI in terms of the services and processes described above. Each of these services and processes has associated to it a set of parameters and attributes which will be manipulated by the risk estimator's rules. An expert can program into the software the FCL which applies to the risk calculation for each individual service and process.

One important feature of the Risk Estimator is its focus on the risk values of services supplied by one infrastructure affecting another infrastructure. Hence risk values calculated by risk estimator not only depend on other internal components but also on components and factors which are external to the home LCCI.

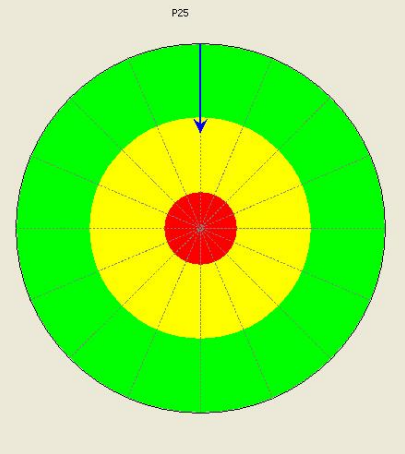


Figure 3 - The Map of Risks

Risk Values are depicted on the Map of Risks Graph shown in Figure 3. In this graph the outer circle shows a zero risk value, the centre is the 1.0 probability of failure. The green area shows a low risk value of between 0 and 0.4, the yellow region shows a medium risk value of between 0.4 and 0.8, whilst the red area shows a high risk value of between 0.8 and 1.0. Individual Services and Processes can be added to this graph in order to view the current risk value. The arrow direction signifies whether the risk value is increasing or decreasing over time.

The MIT Incident Knowledge Analyser (IKA)

The IKA is an optional add-on tool to the MIT components which displays past historic incident data in the form of a mind-map as shown in the screenshot of Figure 4. The mind map represents a series of past experiences, together with related incidents. Experts can add their comments, and also any procedures or additional information that may be useful if another similar situation occurs again.

Using the mind-map tool, the operator can set particular events to indicate that they have occurred. The mind-map tool allows operators to share the same information, and hence, other operators can benefit from getting the latest verified information from colleagues, so that they can react quickly to an evolving crisis.

Besides analysing the consequences of an event, an operator can also see what other events caused the event being examined. For example, a fire might have caused an event to occur in the past. The operator can verify if a fire occurred in the vicinity of a process/service, and take appropriate action based on the LCCI's procedures and/or on the actions taken when the previous incident occurred.

Crisis Prevention and Planning System (CRIPS)

This tool is being developed by IABG and is one of the MIT add-on components. CRIPS is a tool which aims to support and aid the operator in the decision-making process in order to reduce the negative impact of cascading effects and possibly stop major cascading effects which could lead to a blackout. This is done by suggesting actions to take in case a fault occurs.

Further information on the IRRIIS project can be found on the website: http://www.irriis.org /

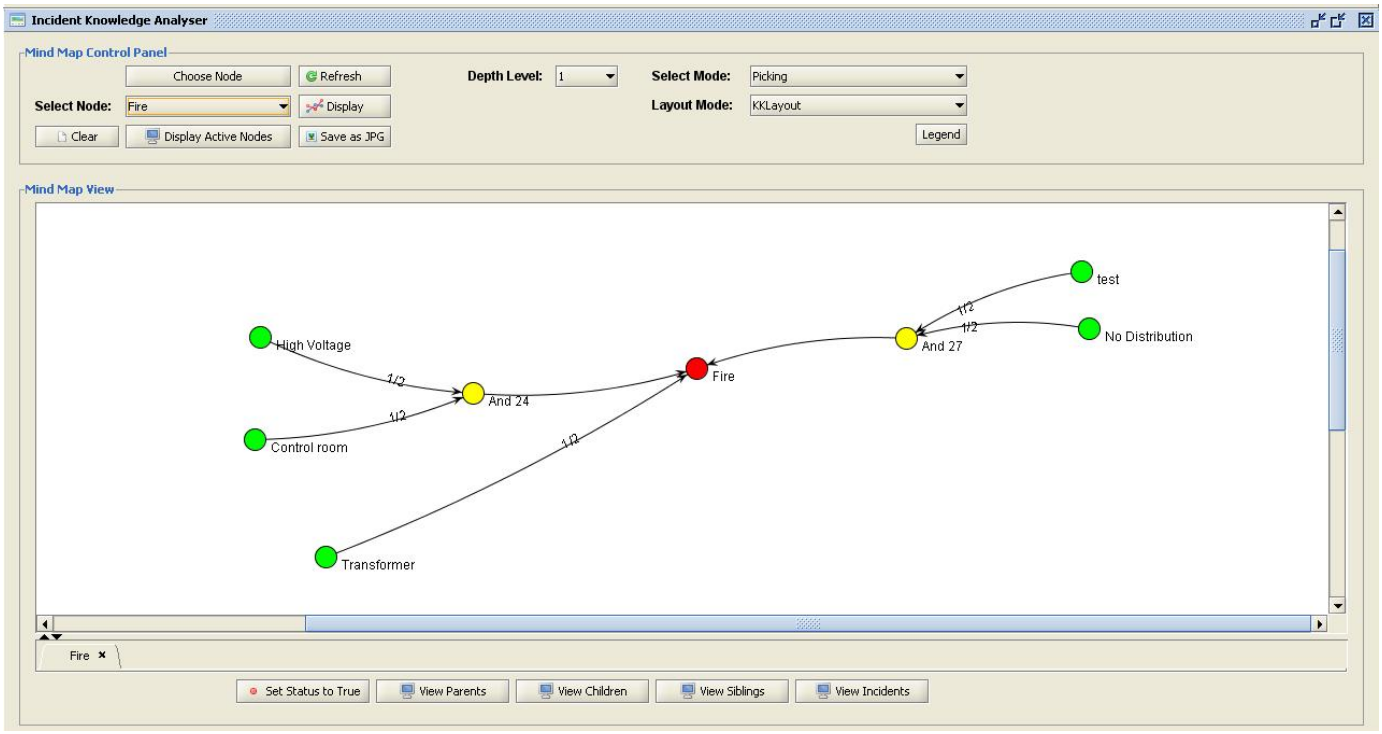


Figure 4 - Screenshot from the MIT Incident Knowledge Analyser

EURAM - EUropean Risk Assessment Methodology project

EURAM developed a uniform risk assessment method for Critical Infrastructures that scales across company, sector, cross-sector and European-wide levels.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl
Website: www.tno.nl

Marieke Klaver PhD

Marieke is Programme manager Security and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0112
e-mail: marieke.klaver@tno.nl

Dealing effectively with threats to and vulnerabilities of critical infrastructures (CI) up to the European level requires methods for CI risk assessment and CI risk management. Risk management processes already exist or are under development for different critical and non-critical sectors in the EU Member States. These processes, however, deal with different sets of threats and different approaches. The European Commission European Programme on Critical Infrastructure Protection (EPCIP) requires a wider co-ordination of these risk management processes with common basic elements and a transversal approach within critical sectors, across critical sectors and/or cross-border while taking into account the (inter)dependencies of CI. To be able to accomplish this, there is a need for a common understanding and information sharing about threats, vulnerabilities and risk by all CI stakeholders, e.g., operators, emergency management centres, policy makers, and independent regulators, both with the CI sectors, cross-sector and at EU-levels.

Re-uses the outcome of existing risk assessment; only align along an agreed 'yardstick' and assess the CI dependencies

The EPCIP sponsored project EURAM - EUropean Risk Assessment Methodology project targeted these issues. EURAM had the following objectives:

- identify basic elements for a EU methodology for general risk assessment,
- identify elements for a common methodology for analysis of (inter)dependencies,
- support information sharing by defining procedures for creating qualified and trusted expert networks.

EURAM ran from December 2006 until November 2007. The work was performed by a TNO Defence, Security and Safety-led consortium consisting of THALES Security (United Kingdom), Ericsson (Sweden), ERTICO (Belgium), and The Netherlands Organisation for Applied Scientific Research TNO (Netherlands).

Business to European-wide

EURAM delivered elements for an overarching risk analysis method. This method allows a holistic approach at different levels of abstraction from the business level, via sector and cross-sector levels up to the European-wide multi-national level. In comparison with other risk methods, EURAM uses an approach that takes the CI dependencies into account and accommodates the outcomes of earlier risk analyses at lower levels of abstraction.

The TNO-led consortium also studied how the various public and private stakeholders, who are involved in providing resilient critical sector services, can share sensitive information on risk in a trusted way ('information sharing').

Based on broad expertise in CI

The EURAM developments are largely based upon the broad expertise of the consortium partners with critical infrastructure protection (CIP). The outcome of the study reflects the background knowledge by the partners stemming from dialogues with the CI operators in sectors like energy, telecommunication, drinking water, transport, and water management as well as with government agencies in various European nations.

Scalable, lean and mean

The EURAM holistic risk approach addresses the risk from a point of view where all expertise at a certain level of abstraction is involved. At the business level one can think of people responsible for and representing process control, information systems, human resources (e.g. awareness processes) and management.

By using a uniform approach with a single list of potential threats, multiple teams can work in parallel in various parts of the organisation on identifying and scoring risk factors. The use of uniform yardsticks (e.g. a five point scale) allows communication across the various teams.

The risk assessment method developed by Thales for a single organisation has been extended by TNO with a comprehensive set of example 'yardsticks' that match the EPCIP definition for CI. These yardsticks allow risk scoring on the axis for seriousness of the effects for the citizens, economic damages, environmental damages, political effects, psychological effects and health effects. This allows a transparent and seamingless use of the scales across all levels of abstraction. When moving up from the business level to the sector level, the cross-sector level and the EU multi-national level, the only additional step to be made is a careful analysis of the dependencies of other CI.

Additionally, a set of steps has been developed by TNO to identify the full set of CI dependencies at a certain level of abstraction. These include the second-level of dependencies which become critical when a primary dependency fails, e.g. after a power failure, the dependency of diesel fuel to run the power backup generators becomes critical.

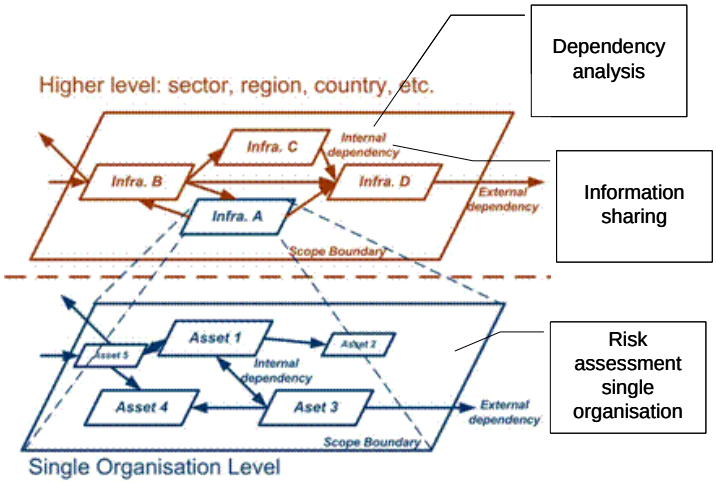
Minimise sensitive exchanges

When moving up to the next level of abstraction, only the identified risk which could not be handled in total at the lower level, needs to be conveyed at the next level. For instance, a business can take care of the risk of power failures and flooding up to a certain extend. The next level needs to take care of the risk which exceeds the business level, e.g. prolonged power outages or major area flooding. At that level, the effects of catastrophic events will be much larger than at the individual business level paired with a much lower probability. On the earlier five-point scale at the business level, one or more risk categories will become of no importance while at the top-end new risk scoring categories will appear. In the same way, when moving up to a next (e.g. multi-national) level, some scoring categories will disappear and new ones will appear.

This approach allows the communication about risk and the handover of risk to the proper higher level of abstraction without additional efforts. As only the risk factors that are not totally controlled are communicated, the sharing of business or sector specific sensitivities is limited to the absolute minimum.

EURAM also encompasses the re-use of the results of an existing risk assessment in an organisation or by a CI sector. Such risk assessments are probably based upon another risk method. The only step required is to map the remaining risk along the EURAM 'yardsticks' and to communicate the CI dependencies which form a risk to the organisation to the next level.

Communicate and share the remaining risk and the CI dependencies with the next level



Conclusions and outlook

EURAM has identified a set of elements for an umbrella-like risk assessment approach covering risk assessments from the business up to the EU-level which include the risk of CI dependencies.

The EURAM elements and method for risk assessment will be put on trial in the energy sector as part of the EURACOM project, which is also sponsored by EPCIP. EURACOM will start in the second half of 2008. Interested stakeholders who are interested in the trial and the method are invited to contact the authors.

First Dutch Process Control Security Event

Many organisations do not manage the information security of their process control systems (PCS). As risk is increasing, there is an urgent need for public-private collaboration against potential cyber crime in this domain.

Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.

Phone +31 70 374 0312

e-mail: eric.luiijf@tno.nl
Website: www.tno.nl

On May 21st, 2008, the Dutch National Infrastructure against Cyber Crime (NICC) organised their first Process Control Security Event. Over 100 representatives of key industry sectors participated in the event.

Mrs. Annemarie Zielstra, the NICC programme manager, opened the event. "Earlier studies in the Netherlands and abroad show that many organisations do not manage the information security aspects of their process control systems (PCS). As risk is increasing, there is an urgent need for public-private collaboration by government, process control system users, and manufacturers against potential cyber crime in the PCS domain. Since these systems monitor and control processes that are critical to society, there may be a major safety and economical impact when they fail."

"Not a free ride! Take the next step: secure your Process Control Systems"

Such processes comprise for instance the supply of power, gas, and drinking water; managing surface water; traffic control, refineries and other chemical industrial processing, automated food processing systems, automated milkers, and security systems.

She continued: "The NICC started discussing and working on the process control security theme with various critical infrastructure sectors. After analysis of information security weaknesses in the PCS of the Dutch drinking water sector, a publication with 39 good practices for PCS security in the drinking water sector was developed [1].

Currently, studies are in progress on the information security posture of PCS in the Rotterdam harbour and the energy Sector."

Join the effort

Foppe Vogd, Program Director Dutch CIO Platform, chaired the event.

He emphasised: "This event is not a free ride. At the end of the day, the participants have a moral obligation to make the next step: enhanced security of their own PCS. This is not easy as it requires a joint effort by people at the technical level as well as management layers. One important question today is how to get to the point that CEOs and/or CIOs will pay attention to the PCS security risk. Or: how do we move the known risk to information security experts towards the board room?"

Opening byAnnemarie Zielstra

Life Hacking

To increase awareness of the audience, the German white hacker Christian Gresser performed a life hack.

Christian Gresser in action …

He explained why most PCS hacks that have been published in the media seem to have happened quite some years ago: "People do not want to get the word out that the processes of critical utilities are vulnerable. However, the reality is that PCS are often 10 to 15 years' old setups connected to office automation environments and also to the Internet. Intrusion is easy and free Internet tools may be of help."

And it is not only about hacking tools! He told the audience about some cases where physical access to PCS and information and communication technologies (ICT) of organisations become easy: "The anti-smoking laws help me and cyber criminals as well".

Integrated environments

The next speaker, Kees Jans, the CIO of the Schiphol Group, outlined the innovative use of ICT at the Schiphol airport and JFK's Terminal 4. Governance requires well-founded decisions, risk management and security auditing. The overall view is left to the CIO.

The view of a CIO (Kees Jans, Schiphol)

"PCS are a new risk factor to take into account. It is not a separated world anymore; increasingly PCS and the administrative and business process ICT are integrated." His worries are that new systems and applications are put in place without proper security considerations by one of the many parties at the airport. The information security awareness is low!

"Anti-smoking laws help the cyber criminals"

He was challenged by the chairman: "who will be on prime time news telling about the hack or virus taking down your baggage handling system, you or the CEO?" His answer showed that the hot potato may be given to a system manager (provided that the press accepts that).

Need for moving faster

Because of other obligations, the discussion between Frank Heemskerk, State Secretary Economic Affairs and André Haket, CIO of Stork, was shown on videotape. The outline of their discussion was about the increased tempo in which critical systems in our society become intertwined with normal ICT, the increased risk and the societal need for reliable infrastructures and safety.

André Haket: "The risk is that we move too slow. The role of government is to boost action by the private industry as the cyber criminals will not wait. Of course, the private industry has to solve the security issues themselves and reduce the risk. That is not a task of the government. The government, however, can help to foster knowledge exchange on risk factors and good practices in reducing vulnerabilities."

Frank Heemskerk: "I agree that tempo is required. Both government and PCS owners need to address the challenges".

Cross-sector governance issue

The next speaker, Peter Hondebrink of the Dutch Ministry of Economic Affairs, stated that his department encourages the use of ICT on the one hand, but has to consider the vulnerabilities on the other hand.

"The majority of the critical and economic sectors use PCS. Incidents in PCS in other nations show that serious PCS security incidents have occurred. But incidents have occurred in The Netherlands as well in multiple sectors as for instance a TNO-KEMA report [2] highlighted."

PCS security requires a cross-sector approach. Multiple sectors working with the NICC are already addressing the PCS security issues. That requires confidentiality and anonymity amongst the participating parties.
"The confidentiality issue, however, makes it a challenge to show that the government actions and the public-private partnership are effective".

He finished by stating that "The Ministry of Economic Affairs wholeheartedly will support the public-private efforts to increase PCS security in all sectors".

One participant was not convinced. He put forward that utilities are privatised without proper governance controls guaranteeing resilience and reliability, in this case a lack of control on information security in critical PCS. "Should the privatisation of utilities policy not be reversed?".
Peter Hondebrink replied that "Security is the owners' own responsibility. If failures regularly occur and it becomes a national issue, the right government department may pick up the escalation process."

Who turned out the lights?

Eric Byres, a well-known PCS security expert, was next: "Who turned out the lights?"

Eric Byers explains the PCS risk

Industrial PCS are vulnerable because many people still believe in myths.

"Myth 1 – PCS aren't vulnerable for hacks and malware. Wrong!" PCS have limited resources but use the same operating systems and CPU as office systems with the same vulnerabilities. "Myth 2 – PCS are not connected to the Internet". A large oil company found that 80% of its PCS are connected to its insecure corporate network, and that aside of the managed connection another seventeen unmanaged connections exist between the PCS and the outside world.

39 good practices for PCS security in the drinking water sector have been developed

Eric showed a list of public examples of PCS security incidents, and some statistics about the way hackers have penetrated into PCS. He discussed the vulnerability of PCS for normal network security tools in the office environment. Security management systems in the office environment cannot be applied to the 24 by 7 environment. "Nevertheless, one can borrow 90% of the ICT security good practices and standards for the office environment, e.g. ISO/IEC 17799. The other 10% requires the same spirit but needs to be specialised due to differences in assumptions about the office and PCS operating environments. This involves issues like patching, asset management (and scanning), access control, standardisation of systems and applications, office hours versus 24 by 7 operations, and incident response.

Perimeter security is not enough; one shall break-up plants into separate zones. Critical is the human factor and the security awareness of all involved in PCS."

During the period for questions, one of the participants stated that "there is a major difference between people responsible for ICT and those operating PCS. PCS users talk about their 'baby', they are passionate to let it perform the process in the best way ever. ICT people do not care much about IT-hardware such as a laptop. He was suggested to refrain of speaking about security to PCS personnel. Instead, one should introduce security as 'this is making your process more safe and reliable'.

Several participants objected to this suggestion as a CIO or CEO needs to take control about reliability and shall require that (office) ICT and PCS work together as a single team.

Five work sessions

After lunch, the audience was split up into five different work sessions dealing with the topics '(No) security solutions for PCS', 'Patching and hardening', 'The way to Secure PCS', and 'Organisation and Management'.

Intense discussions took place in the VIP round circle workshop

There was some time for relaxation ..

A special VIP-track was held in which the vulnerability of PCS was visualised by a life example. The incentives and disincentives for ICT security in general and PCS security in particular were discussed.

The main issues

The day was concluded by a panel consisting of the work session chairmen. The main issues:

- A first dialog between PCS vendors, users and security application vendors started. A joint discussion and information exchange platform about PCS infrastructure security is regarded fruitful. A no-go area is a discussion about business risk and impact aspects.
- Security is still seen as cost factor; not as a risk mitigating factor or insurance; how to come to a business value?
- PCS patching and hardening is a security need; it is not done yet in the right way. Good practices need to be explored and exchanged. Legacy is an issue as very old operating systems are still being used.
- PCS security requirements should be part of procurement, but this is not always the case.
- The drinking water advancements in PCS security and their risk analysis approach are being looked at by other critical sectors that co-operate in the NICC. PCS security policies are needed, but that requires management awareness. How to quantify the risk for the management levels?

- When safety requirements are met, the security requirements for daily operations are often met as well. The remaining security risk is less rational and may hit unexpectedly. How to make this remaining risk quantifiable?
- Information security is good business practice as one can make risk assessment for PCS security comparable with safety risk assessment. PCS and 'office ICT' will converge over time. Education, training and partnering of all involved is required; the earlier the better.
- There are too many PCS security standards; a common international cross-sector view is required.
- Good risk management requires a bottom-up involvement of all people involved in the organisation. That may require another risk management culture in the organisation.
- A number of participants is in favour of an obligation to publically report incidents if consequences are exempted (alike the FAA-model in the airline industry). An anonymous database managed by a trusted party is another alternative to increase the sense of urgency and awareness.
- PCS vendors stated that PCS security requirements are often dropped first by the PCS buyers when the offer exceeds the budget.

Three recommendations

The assembly came up with three recommendations to the NICC to jointly improve the security of PCS:

- Continue and intensify the dialogue about PCS security.
- Discuss the results of the Process Control Event in the NICC sector-specific working groups.
- Develop a database and anonymous reporting scheme for reporting PCS security incidents.

The event was closed by Annemarie Zielstra. She asked all participants to consider their commitment about participation in the next steps. She announced that the next NICC Process Control Security Event will happen on November 20, 2008.

References

[1] Luiijf, H.A.M., SCADA Good Practices for the Dutch Drinking Water sector, TNO DV 2008 C096, March 2008.

[2] Luiijf, H.A.M., Lassche, R., *SCADA (on)veiligheid, een rol voor de overheid?* [SCADA (in)security, a role for the government?], TNO/KEMA rapport, april 2006.

Engineering Privacy: Technologies and Strategies for Protecting Data

The Royal Academy of Engineering published its report *Dilemmas of Privacy and Surveillance* in March 2007. Two parliamentary inquiries into the state of surveillance and data security have followed in its wake, yet the UK has still suffered large-scale losses of citizens' personal data. Here, the lessons of the Academy's report are reiterated.

Nigel Gilbert

Professor Nigel Gilbert chaired the Royal Academy of Engineering group that wrote the report on *Dilemmas of Privacy and Surveillance*. He also served as Specialist Advisor to the Home Affairs Committee's Inquiry. He is Professor of Sociology at the University of Surrey, Guildford, UK.

n.gilbert@surrey.ac.uk

Natasha McCarthy

Dr. Natasha McCarthy is Policy Advisor at The Royal Academy of Engineering. She was secretary to the *Dilemmas of Privacy and Surveillance* working group and also works in the areas of engineering ethics and philosophy of engineering.

natasha.mccarthy@raeng.org.uk

This June, the UK Parliament's Home Affairs Committee published the report of its inquiry 'A Surveillance Society?', which examined the extent of the UK Government's collection of personal data and its responsibility for keeping that data secure. This report is the latest in a number of studies on the impacts of data collection and surveillance on society, one of which was the The Royal Academy of Engineering's report, *Dilemmas of Privacy and Surveillance*, published last year.

Data – less is more

One of the overriding messages of both the Home Affairs Committee and the Academy's reports is that the key way of keeping data secure is ensuring that only essential data is collected in the first place. Excessive harvesting of data increases the risk of loss and thereby threatens individual privacy.

"The key to data security is to limit the amount of data collected in the first place"

Collective trust is also threatened by the excessive collection of personal data. Firstly, if people feel that the amount of data that the government collects on its citizens is unreasonable, this can threaten their trust in government. Secondly, trust is lost if it is believed that a government is not a reliable custodian. This has been shown in the UK as a result of the mislaying of large quantities of personal data by the Inland Revenue and the Driver and Vehicle Licensing Agency. The loss ofprecious personal details such as bank account information and children's names and ages has demonstrated to UK citizens that Government has lessons to learn about the importance of, and strategies for protecting, personalised data.

The Drive for Data

But there are reasons for government wishing to collect data, and benefits can be gained by having access to greater amounts of, and more detailed personal information. The crucial thing is to reach a balance between those benefits and the threats already described.

The kinds of benefits intended are the creation of a more intelligent government that can match policy solutions to real needs; the provision of a more personalised approached to public service delivery and easier access to public services. Another key reason for data collection is the increases in security it promises – greater surveillance and more comprehensive and searchable databases are promised to bring reductions in crime, control of terrorist threats, less opportunity for fraud and greater child protection.

The powers of surveillance

The first step to realising these benefits, however, is to be realistic about the extent to which greater surveillance and data collection can really deliver them. A number of studies, including research

carried out by the UK Home Office, have failed to show that increased camera surveillance results in a reduction in crime. CCTV footage might have a use in identifying the perpetrators of a crime, but there is less evidence that they actually support the safety of members of a community.

The UK Government is currently in the process of introducing a system of identity cards, which will be implemented alongside an identity register, a database holding the identification details of UK citizens and long term visitors, with records of the circumstances of use of those cards. One of the advertised purposes of the system is to reduce the threat of terrorism, but the efficacy of such a system to identify, track and deter terrorists is yet to be proven.

Engineering Privacy

One of the main messages of The Royal Academy of Engineering's report was that engineers have an important role in helping to strike the balance between the benefits of data collection and the threats to privacy and the security of data. The contribution of engineering does not lie solely in devising technologies to keep data protected. One of the essential skills of the engineer lies in the ability to devise successful systems that comprise both human and technical elements. Be that a railway system, a manufacturing process or a large IT system, it will inevitably feature both technical components and human operators and users. Engineers have to understand how these human elements will function in the system, and will also need to be aware of how the behaviour of those operators and users can jeopardise the system. Thus part of system design is creating clear and intuitive processes that will allow the human elements and technologies to work together. Another key aspect of engineering is ensuring that the requirements of a system are clearly specified so that it is fit for purpose.

In the case of databases that contain personal data, engineers can help to devise both technologies to protect that data, and rules and strategies for operators and users that will maintain security. Therefore, it is important that the organisations that procure these databases utilise engineering skill in designing and implementing them.

"Both technological solutions and under-standing of human factors are essential to protecting data"

Foresight for Failure

One of the main tasks of engineers is to foresee and plan for the failure of the systems they are designing. Identifying failure modes and ensuring both that the likelihood of failure is as low as reasonably practical, and that the system is fail-safe, is essential in every branch of engineering from structural engineering to designing software systems.

When a government body or private sector organisation creates a database of personal information, it is their duty to identify the ways that the database might fail, including illicit access to confidential data and loss as a result of technical failure. It is clear that the UK Government is not blind to the possibility of the failure of the identity databases that it is creating. For example, the proposed children's database, which will hold information about UK children in order to keep track of those who are potentially vulnerable, will not hold the details of the children of celebrities or other public figures. This demonstrates an awareness of the likelihood of failure, and one of the most likely modes of failure – illicit access to the database by individuals attempting to obtain especially valuable information. Since it is more likely that the database will be broken into in order to access this particularly high value data, excluding it from the database reduces the likelihood that there will be illegal access. However, this strategy demonstrates the fact that this failure mode remains open, and that perhaps not enough has been done to protect the information of the rest of the UK's children. Once such a failure mode has been identified, the next step is to design procedures and technologies to reduce the likelihood and impact of those failures.

Technologies for data security

The Academy report distinguished three main strands of technologies in the identity management domain. First, connection technologies allow the movement and communication of data; second, disconnection technologies prevent access to and protect data; and third, processing technologies allow data to be searched or used. Disconnection technologies will be key to the design of databases and of methods for verifying identity. A number of significant technologies in this area should emerge in the next ten to twenty years. First are those that provide secure means of proving one's right to access a database, an online bank account, or similar, which come in the form of *identity tokens.* Options include secure MMC (secure versions of the Multimedia Memory Cards used in mobile phones and palmtop computers) and secure USB (using secure USB keys as a way of authenticating oneself – with access to online services requiring the presence of the USB key in the computer). A combination of these identity tokens with Public Key Cryptography for the security of data offers hope for the secure transmission of data and policed access to that data.

Voice-based interaction is another salient disconnection technology. Voice is attractive as a biometric identifier because it is passive and non-invasive compared with biometrics that require samples or scans of parts of the body. Although these technologies currently are not sufficiently reliable, if voice recognition and speaker identification technologies were to be improved, they could provide an option for ensuring that only authorised users could access valuable data.

Human Factors

Although technical solutions and procedures can be established to protect data, often the weakest point in a system is the human operator. Therefore, systems that hold or process large amounts of personal data must be treated in the same way as other critical systems that engineers deal with. A nuclear power station or a chemical processing plant will be designed in such a way that it is extremely difficult for an operator to make an error that would easily lead to the leaking of radioactive materials or toxic chemicals. Barriers should be put in place to make it extremely difficult for, say, a member of staff to download large amounts of personal information to insecure media such as CDs, or for data to be accessed by anybody but trained personnel.

"*Identification* involves proving who you are, *authentication* involves proving that you have the right to access a service"

Training of staff is essential. Just as workers who deal with hazardous substances are drilled to understand the threats that those substances pose and the ways to control them, staff given access to sensitive data should be encouraged to treat it as if it poses risks of a similar magnitude.

But mistakes and malicious attacks will still occur. The disconnection technologies described above can play a significant role in minimizing the likelihood of such mistakes or attacks, but employing the right procedures for collecting and storing data is also crucial. Data should be stored in such a way that it does not offer a goldmine to data thieves nor threaten catastrophe if it is compromised.

Procedures for protecting privacy

Databases that contain large amounts of personal data about individuals pose the greatest threat. A single database that contains enough data about each individual for a fraudster to be able to perpetrate identity theft will be a honey pot to data thieves. There is also a risk that if it is accidentally compromised there would be potential for opportunist exploitation of the lost data.

Data relevant to different aspects of a person's life, required for different purposes, should be kept on separate databases, or compartmentalised within a database as far as possible. Keeping people's personal information segregated lessens both the opportunity for it to be stolen and used maliciously, and the impact of data collection on a person's privacy. Privacy is threatened when a person's life story is open to the view of an unknown third party, but if different parts of that story are kept separate, then the story is kept secret.

Risks are also lowered if people are not expected to give away identifying information unnecessarily. The Academy's report distinguished identification from authentication. *Identification* involves proving who you are, *authentication* involves proving that you have the right to access a service – for example, proving that you have the right to travel on a train because you have paid the fare, or proving that you have the right to free transport because you are over a certain age. Separating authentication and identification will allow people to access restricted services without giving away personalised data, and without providers of that service having to hold databases of identifying information.

Conclusion – a change of attitude and an embracing of technologies

Through the process of designing socio-technical systems that are fit for purpose, devising new technologies to protect data and identifying processes that minimise the risk to data, engineers can have an important role in securing citizen's privacy. It is key that governments who are collecting data begin to appreciate the critical nature of what they are doing and secure the skills of engineers and technologists to design systems that work, are low-risk and are failsafe.

Today's risks to the financial sector

The CIP Sector "Financial Industry" lost its innocence. The traditional risks have been enhanced and therefore the banks have to deal with e-espionage, identity theft and the problems of international terrorism.

Rolf Schulz

Director, GNS GmbH, Germany
Rolf has been active in the security business for more than 20 years and his vast experience ranges from threat analysis and threat modelling, malware intelligence up to security strategy for operators of critical infrastructure.
He and his team of security veterans continue to serve a range of customers in EMEA as well as the APAC regions, with a strong focus on Critical Infrastructure Protection and strategies for developing application security right from the start.
He is a well known consultant to Governments and a regular speaker and conference host all over Europe and Asia.

Phone : +49 173 957 9661

e-mail: rs@gnsec.com

In May 1998, President Bill Clinton issued Presidential directive PDD-63 on the subject of Critical Infrastructure Protection. This directive acknowledged certain parts of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizens, and required steps to be taken to protect it. This program was under control of the DOD and the FBI.

It was the first time that the term CIP – critical infrastructure protection – was used. This was also the first time that the national infrastructure was broken into 10 defence critical infrastructure sectors. Characteristic CIP Sectors were, beside the government, private services like Energy, Transport or Water – the importance of the financial Industry was in the beginning marginal – with a focus on defence activities related to officially appropriated funds.

Lessons learned from 9/11

After 9/11 a paradigm shift occurred in the world of CIP – and suddenly everybody understood the importance of communication – and what happens, when this communication breaks down. The attack against the World Trade Centre was a physical attack – but one of the side effects was the elimination of a major network node in one of the towers – and the backup of this node in the other tower. As a result, the whole city net went down – and the banks and stock exchange, which were not affected by the primary attack, went offline for more than one week. Only those banks, which had an emergency backup centre in Jersey, were back to business in less than four hours. Weakly secured interlinked Infrastructure - and the impact of the communication breakdown – causes a multibillion dollar loss to the financial world. ---

After 9/11, it became evident, that the financial industry plays an important role in the fight against the international terrorism

Money, Money, Money…

After 9/11, it became evident, that the financial industry plays an important role in the fight against the international terrorism – because Terrorist need money!! And it is a bank's business to collect and transfer money. Investigators almost immediately identified countries or individuals, which invested into questionable funds. Then international special investigation groups concentrated on the money flow, intercepted critical transactions and blocked accounts of known – and not known - terrorist supporters. All this was possible because everything nowadays is online available. To find the data, it is only a question of computer power and some internal know how. Once the FBI arrested al Capone because of tax evasion– today they dry out terrorist with the help of modern communication equipment and computers – by following the international money flow.
The CIP Sector "Financial Industry" lost its innocence…

Today's Risks to the financial sector

The risks have changed. Well, maybe not all the risks, but the methods. E.g., fraud is still a popular threat, but it is more and more ICT based.

Identity Theft

Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. (Source: Wikipedia). The interesting question is, whether this is a direct or indirect risk for the bank.

In 2006, CNN's headline in May said: Identity theft: The new way to rob a bank. HOUSTON, Texas (CNN) -- When Bank One notified Houston veterinarian Mike Janney that he owed $85,000 on his line of credit, he was stunned.

Janney felt victim to fraud when a bank employee sold his personal information to an identity theft ring. His bank had to cover the loss, along with another $12 million stolen from other customer accounts.

That was 2006. Today, Trojans, malicious websites or phishing attacks collect millions of personal data from people all over the world. Sites like darkmarket.com sell these data to everyone, who is interested. The "customer" can buy bank accounts, credit card details with guaranteed balance or detailed information about debtors. He can pay online via faked banks hosted by the Russian Business Network even with a money back guarantee and an escrow mechanism. The amount of personal data, stored on Drop Zones (these are sites, where Trojans or Key-Loggers send the captured data to, is in the Terabyte Range.

Like this bank, which was using life production data on test systems…?

The data are stolen from the customers PC, but there are also targeted attacks to the banks data, like a Trojan that is harvesting data from internal databases or intranet sites.

The internal risk factor

Or the data is simply stolen by employees or external "specialists" and sold to the highest bidder. 10 Years ago a German bank became victim of such an attack – an external programmer found a list of "special" customers. He first started to blackmail them directly, and then he blackmailed the bank. End of day, Fiscal investigation got the list – and this ended up with police searches on some of the major German banks regarding illegal money transfer, money laundering and tax evasion.

Or the data is simply stolen by employees or external "specialists" and sold to the highest bidder ...

And a few months ago similar incidents happened in Luxembourg and Switzerland – also initiated by insider and internal staff.

The interesting question is: If those highly confidential customer data could be disclosed and misused – what is about internal data of the bank, like strategy plans or confidential information from / for the board?

Information Leakages

Information leakage happens whenever a system that is designed to be closed to an eavesdropper reveals some information to unauthorized parties. For example, when designing an encrypted instant messaging network, a network engineer without the capacity to crack your encryption codes could see when you are transmitting messages, even if he could not read them. During the Second World War, the Japanese for a while were using secret codes such as PURPLE; even before such codes were cracked, some basic information could be extracted about the content of the messages by looking at which relay stations sent a message onwards (Source: Wikipedia)

Information Leakage also applies to data deemed confidential, which aren't properly protected by web sites. These data may include account numbers, user identifiers (Drivers license number, Passport number, Social Security Numbers, etc.) and user specific data (account balances, address, and transaction history).

But information Leakage is not limited to applications. Users often are careless in the use of electronic stored information. Critical information is not encrypted; access rights are not tight enough. Sometimes a copy or an attachment is sent cc: to persons, which are not really involved – and the mailbox store of certain users is bigger than their home directory.

This all is a paradise for a malicious person, who wants to collect interesting Data – also, because there are -mostly-no mechanisms available, to prevent or identify such a reconnaissance operation.

Information Leakage Protection is a new trend for the Security Industry – and a new market for the antivirus business. But careful: The term information Leakage is not clearly defined – and available Products differ a lot in functionality and usage. All companies interested in such a solution are strongly advised, to carefully write down their requirements and use this to define the test cases for the comparison of the favoured products - and do not only look on the feature set, but also on the integration capabilities into the existing security processes.

E-espionage, Globalisation and the Wild, Wild East…

Most banks today still see the major risk in fraud or other, similar threats – threats, that are targeting the money…But what about the disclosure of internal data, like strategy information?

Today we talk about globalisation, about the role, the financial industry will play in the international world. New markets are coming up, and the banks see the big business in former member states of EX-Soviet Union or China. But they sometimes forget that these countries are different – in behaviour and business culture.

For some of those countries, it is quite normal, to use all options to gather the necessary information. In other countries, the secret services are still ruling – and working closely together with the local industries.

So the banks have to learn, to be prepared against attacks which they never thought about – attacks from an opponent, who is familiar with all those things, we only see in a James Bond Movie. And of course, the attacks are not only IT based. Yes, in a TV Show, it is always the hacker who is getting all the info. But in the real life it is more complex – it is always a mixture of extortion, social engineering, violence, break-ins and – maybe - some real hacking.

But who is prepared? Which organisation is able to fight a blended attack – using traditional crime methods together with high tech? In most organisations, IT Security and internal security are two different entities, mostly without any communication. One solution is a Cybercrime Incident Response Team or CIRT. It combines the recourses of internal and IT Security and helps to react fast to all kind of attacks – from terrorist to hacker.

A little spy-how-to ….

A few words about e-espionage and how easy collecting information is. Let's assume, there are employees who need some extra money and decided to go for Industrial Espionage. So, what do they need for a successful spy attack? Well, it's easy, and all is available on the internet. First of all, they need a good modern Trojan. It must be flexible and easy to configure – that gives an excellent return on malware investment (ROMI).

They only want to spy, not to manipulate. So they don't need any sophisticated tool to capture sessions or extract forms. But some web based Command Centre would be fine, it's so common…To be on the safe side, they order all this from the friendly Russian Solutions Provider. Investment is between 200US$ and 3000 US$. Delivery is fast and secure, and they will also receive a bill.

As a Drop Zone (Collector System) they can use a few systems in the victims IT Centre, which was prepared earlier. They only want the Trojan to collect documents and PDF's from the Project "Armageddon", so they use the web based Command & Control System to configure the Trojan. The next step is to infect the targets. That's easy, too. They setup a website for a project, or an info page, or maybe a server with the latest digital pictures from the big party last weekend. They can use WMF exploits directly, but there is some risk, because the Company is updating their AV Pattern quite fast. So they use a modified and outdated Web attacker (that's an attack toolkit), because JavaScript is allowed in our target environment. To be on the safe side, they encrypt the source with tools like HTML Protector. And for those, who will not visit the website, they prepare some fancy USB Sticks with some presentations and the Trojan…

First of all, we need a good Trojan, fitting our needs. ... It's flexible and gives an excellent return on malware investment (ROMI)

That's it. Now they have to wait. At the end of the Week, they use their IPod to copy the Payload from the Drop Zones. Nobody has a problem with a guy and his stylish MP3 Gadget, and the Security Check at the gate only look for Laptops. End of day, there is only one thing to do: To review the data and sort it for potential "Customers"

National Risk Impact

Most of the above mentioned threats are targeting the bank – and not the critical infrastructure of the country. Of course, there are side effects. One example is if a local bank is sold to a foreign investor with questionable goals,–and if this investor could gain advantages in the deal because he had illegal insider information. Another scenario is an electronic attack against the international cash flow by attacking systems like SWIFT. But still one of the most critical things is money laundry. When drug runners and terrorists want to park illicit cash, there may be no better safe place than hedge funds. For more than three years, the Securities & Exchange Commission and the Treasury Dept. have been discussing how to include hedge funds in the USA Patriot Act, the 2001 legislation designed to protect against terrorism. Yet during that time, the $1.3 trillion plus hedge fund industry has collected record amounts of cash, some of which could well be from questionable sources. As it stands, hedge funds have no responsibility to determine the sources of investor funds or to analyze whether they're questionable. This is a perfect mechanism for mafia groups and terrorist.

Risks to the financial sector changed in the last years. Automated electronic attacks like internal Trojans, e-espionage and information Leakage are only a few examples. Together with the globalisation, with international partnerships, other risks occurred – and good selling products like hedge-funds have the potential to turn into a national risk.

Cyber Security Assessment of a Power Plant

Critical Infrastructures are nowadays exposed to a new kind of threats due to the large number of new vulnerabilities and architectural weaknesses introduced by the extensive use of ICT into such complex critical systems. We present the first outcomes of an exhaustive ICT security assessment analysis, targeting a real thermal Power Plant.

Alberto Stefanini graduated in Electronic Engineering in Bologna, 1974. He is working with the JRC where he is involved in studies on critical infrastructure vulnerabilities, and in the coordination of research activities on this subject.

Marcelo Masera is an Electronics & Electrical Engineer (1980), and an Officer of the European Commission at the JRC since Nov. 2000. He is in charge of the Security of Critical Networked Infrastructures action within the Institute for the Security and Protection of the Citizen.

Igor Nai Fovino received the Ph.D. in Computer Science in March 2006.He is a researcher at the JRC and a Contract Professor at the University of Insubria. His main research activities are related to the computer security

e-mail: alberto.stefanini@jrc.it
e-mail: Marcelo.Masera@ec.europa.eu
e-mail: igor.nai@jrc.it

Introduction

Nowadays the process control network of most power plants is integrated with a broader information system including the company business network. Moreover, most maintenance services on process control equipment are remotely performed.

Most power plants are vulnerable to cyber attacks through the business network they are part of

There has been a qualitative leap in the last years in the need to safeguard those installations against malicious activities by actors such as terrorism, organised crime or violent extremism (for instance, radical environmentalists). On the one hand, the security conditions suffered a drastic change after September 11, 2001. On the other, the intensive use of ICT has opened new ways for carrying out attacks.

The paradox is that the more ICT systems are employed, the more opportunities there are for intrusions by external and internal malicious actors. A violation of the integrity, availability or even the confidentiality of data might produce significant damage to assets of the company and be part of a broader aggressive action.

These situations cannot be ignored because the potential consequences of an incident can be severe: the cost of a power plant shut down is huge, and release of pollutants from a plant in the environment can provoke vast damages.

Security assessment

We propose a systematic approach to this problem based on a **Security Framework.** This provides an overall model for a methodical characterisation of the security requirements that a distributed Integrated Control System (ICS) should satisfy. The framework, taking as reference the standard ISO/IEC 17799 (Code of Practice for Information Security Management), has three main purposes:

1. framing the problem (i.e. stating which are the information and communication elements to protect),
2. categorizing the requirements (typically referring to the three security properties to satisfy: confidentiality, integrity and availability); and
3. defining the ICT security policy.

Once the problem is framed, it is possible to conduct a **Security Assessment**, i.e. a risk-oriented analysis of the system for the identification of the assets that could be menaced by internal and external threats, which take advantage of vulnerabilities. The normal sequence of the analysis initiates with the characterisation of the assets, for then evaluating the possibility that the combination of threats and vulnerabilities might pave the way for potential attacks. These attacks are studied making reference to known attack patterns so as to evaluate their capabilities to affect the services and assets of the system under study,

and the potential countermeasures. The assessment finishes with the quantification of the potential impacts and their likelihood.

As soon as the assessment is ready, the identified attacks can be simulated. This **Attack Simulation** can be done either using the ICS of the case studied, or employing a full simulation environment (i.e., where the same SCADA are simulated). The complete architecture comprises: 1.) a simulator of the physical system being controlled (e.g. the power plant or a section of it); 2.) the real-time part of the ICS under study (or a simulation of it); 3.) the rest of the ICS (e.g. database, communication links, etc.); 4.) any remote control system (or their simulation); 5.) the attacker simulator; and 6.) the simulation management.

Results of the preliminary Security Assessment on a target Plant

According to the approach presented above, we carried out a preliminary security assessment of the ICS of a target power plant. Although several features of the real ICS were streamlined, the target system was close to the ICS of the power plant.

The target system and its ICS functions were analyzed in order to identify (**System framing):**

- Asset classification and control (human/organisational actors; hardware, software and information assets, components and subsystems, interfaces);
- Data flows (complete life-cycle of each data package; who can do what on them);
- System operational context (the different usage states, conditions and procedures).

According to this analysis, the ICS includes several main subsystems (fig. 1):

- the Process Control System,

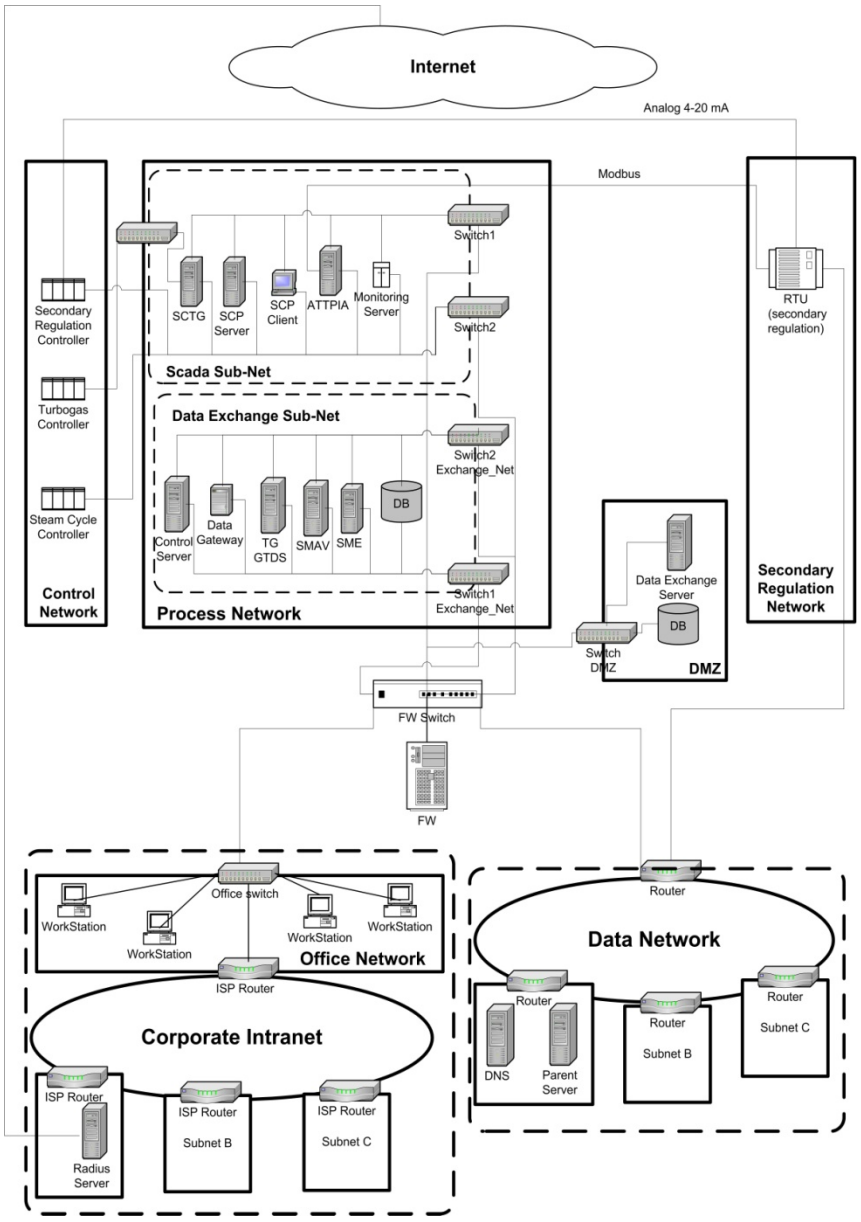


Fig 1. The ICS of the target plant 1

- the Process Control and Data Acquisition System (Process SCADA),
- the Control network,
- a Data network,
- business applications based on the Company Intranet, and
- the main Firewall between the data network and the Intranet.

The results of this framing step were used to perform a **System requirements analysis**, in order to define for the ICS:

- Network security requirements (Architecture requirements, network access control requirements, communications management);
- Node security requirements (node access requirements, operations management).

This set of requirements was employed for the defining the current **Information Security policy**, containing:

- Access control policy;
- Communications and operations management policy (including Data

Authentication Policy, Data flow security policy and Data confidentiality policy).
- System maintenance policy (including a procedural guideline for the secure maintenance of SCTI).

Based on the results of the previous phases, the **Security Assessment** provided a detailed analysis of the potential threats, of the main system vulnerabilities, and the most likely attack scenarios. Countermeasures for opposing the potential security failures were identified:
- To counter vulnerabilities (reporting, changing configuration, patching, etc.)
- To counter threats: which preventive measures to apply for dealing with threats before their actualisation (e.g. preparedness, review of security policies, testing)
- To counter attacks: which instruments to deploy for dealing with cyber incidents, before, during and after an attack occurs (e.g. firewalling, intrusion detection, cyber forensics)

Potential Threats were analysed based on an FBI classification of threat agents which includes:
- Crackers: external agents with certain knowledge about computer and communication systems, which may break into the system violating security measures.
- Insiders: disgruntled employees, or outsourcing vendors and other actors who benefit of permits for physical and cyber access to the system facilities. They do not need a great deal of knowledge about computer intrusion, because their knowledge of a target system allows them to gain unrestricted access to cause damage or to steal system data.
- Malware writers: malicious code writers produce software designed specifically to damage or disrupt systems, such as a virus, a worm or a Trojan horse. These are normally known as Malware. They can be specific (target to particular systems or even organisations), or generic.
- Organised Crime: There is an increased use of cyber intrusions by criminal groups who attack systems, mainly for monetary gain. These groups might try to get internal information for blackmailing the company, or to extort by menacing the dissemination of some sensible information, or to commit different types of fraud (e.g. influencing some prices), or forgery (e.g. changing values in bills).
- Terrorist groups: terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
- Hacktivists: politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
- Information Warfare: several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that can affect infrastructures as one key column of a country.

In our case, five different types of threat agents were considered: *Insiders*, *Crackers*, internal and external *Malware*, *Organised* groups (these include terrorism and **hacktivism**), as *Information Warfare* threats currently appear to be negligible in Europe. These potential actions of threat agents were classified based on their potential actions. The most dangerous are: Insiders, Crackers and Organised Groups. All of them have the same likelihood of occurrence and potential impact severity, although for different reasons. While Insiders have an easier access to internal resources and a better knowledge of assets and potential weaknesses, organised groups have more motivation and own resources (and potential availability of expertise). On the other hand, Crackers are ubiquitous and their hazard grows with the increasing visibility of critical infrastructures.

The Vulnerability Assessment identified 156 major vulnerabilities in the ICS of the target plant. These were classified according to their likelihood of occurrence and potential impact severity. Both were given a numeric value (1, .5, or .1) corresponding respectively to: *Almost Certain*, *Likely* and *Improbable*, and *Vital*, *Heavy* and *Minor* impact. Combining these two factors two weakness indices were computed: a *Weakness Worst Case* and a *Weakness Cumulative Index*. According to this analysis, all main subsystems, and especially the *Process Control System*, the *SCADA*, the *Data network*, and the *Firewall*, resulted heavily vulnerable, as presented in the Radar Charts of Fig 2.

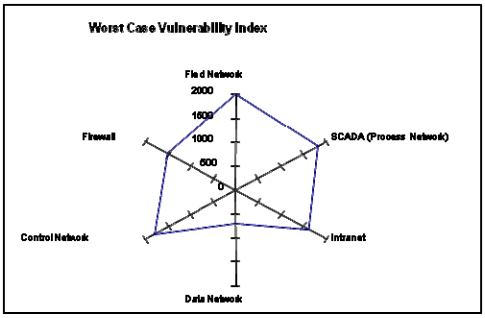


Fig.2: Weakness worst case Radar Chart

Attack scenario analysis

Despite the huge number of different kinds of attacks that can be carried out against a host or a network, they can be classified in a limited number of categories, or scenarios (Reference: Attack modelling for information security and

survivability, A. Moore, R. Ellison, R. Linger, March 2001, SEI). We carried out a systematic review of those attack categories for verifying their feasibility, by checking them against the already identified vulnerabilities. The attacks that were identified to be most likely and dangerous were:

- Radius Server Denial of Service: DOS attacks have the scope of causing damage by drastically limiting, or even denying, access to specific resources, such as the company Intranet and the Power Plant Network thus making them unusable to intended users. Such an attack has a direct impact on the Power Plant maintenance and management routines.
- Domain Credential Stolen/External Connection DoS: this attack scenario has two different goals:
  - to obtain the credential of a user which tries to log itself from Internet to the Radius Server
  - to make an external connection DoS avoiding the user to be remotely logged on the Intranet/Power Plan network.

  In this scenario, the attacker has already obtained the control of a machine in the same sub-network of the Radius Server. The first goal of the attacker is to be able to capture the authentication request and responses of the users. Once obtained the authentication/response packets, the attacker is able to make a direct cryptanalysis. After having sniffed the authentication and response packet, it is possible to predict the sequence number of the packet responses, impersonate the Radius Server, and reply to the users using ad-hoc forged reject packets.
- Intranet Virus Infection: Viral infections can attack all environments connected to an open network. There are several ways by which viruses can be transmitted, for instance networks, data download and, in general, all data incoming from all sorts of connections and local input streams (e.g. floppy disks, CDROM and other kinds of removable media). Anti Virus software is the most important instrument against viral infection. However, even a fully patched system with an updated antivirus may be vulnerable to virus attacks in the interval between the release of the virus code, and the moment the Anti Virus vendors provide a new updated package. Damages caused by viruses may vary from minor disruption to major malfunction and even service disruption; in some cases, viruses are also programmed to install a backdoor on the infected system, in order to allow the attacker to remotely control the infected workstation.
- Data Network Worm Infection: Computer Worms are self-replicating computer programs that run independently and travel across network connections. The main difference between viruses and worms is the method in which they reproduce and spread: a virus depends on a host file or boot sector and, in order to be transferred between two computer, it needs that a file is transmitted; on the contrary, a worm can run completely independently and spread itself through network connections. Once activated, a worm can behave as a virus, install Trojan horses or execute operations on the infected system.
- ISDN Router Attacks: this scenario is possible due the presence of an ISDN Router in the SCADA Network. Such router is not managed by the operator of the plant, but it is under the direct control of an external company. The Router is used by the external company to control, manage and maintain the SCTG system. When there is any need in that sense, that company produce a telephone call to the Router ISDN, makes a login and then becomes logically connected to the SCADA Network. In our scenario, the attacker starts operating at this point. After a standard system fingerprinting, he identifies the presence of that router. Once the router is online, the attacker, either by brute force or by sniffing, tries to identify a correct login and password.. If the attack is successful, the attacker acquires a direct access to a portion of the SCADA network, the one which contains the router and the SCTG.
- Phishing Attacks: this attack is normally used to gather information from legitimate users leveraging their confidence on the “look & feel” of a web portal; a phishing attack is usually carried out by making the target users connect with a malicious web site, set up in a way to make them believe to be connected with a legitimate website. As a result of this action, a legitimate user might supply sensitive data and/or login credentials to the attacker.

These attack scenarios were analysed according to their Plausibility and Severity: three seem to present a highest risk: **Infection due to virus reaching the Intranet, Infection due to worms in the Data network, and attacks to the ISDN router** employed for external access by suppliers/service providers. The likelihood of occurrence of infections is high, and this calls for maximum attention with respect to prevention and protection mechanisms. In addition, specific procedures are needed to react to evolving infection situations. The attack to the ISDN router is also highly likely, as it is the case of any external Internet access point. Its direct access to critical resources makes it a crucial point for the security of the system.

Governance and Risk Management in a globally integrated Ecosystem

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.

Margarete C. Donovang-Kuhlisch

Dipl.-Math. (MSc)
IBM Deutschland GmbH
Northeast Europe Government Industry Technical Leader

e-mail: mdk@de.ibm.com

Problem Space

Service orientation at the enterprise or ecosystem level has been proven to be the primary enabler by which organisations can become and operate as globally integrated enterprises.

The implementation of service-oriented architectures (SOA) with support for coherent operational processes requires interoperability not only on the network, but all the way up to the procedural level – with integration of both real-lives as well as virtual reality systems for knowledge management as well as decision support.

Frameworks for model-driven architectures (MDA) and product development based on modelling and simulation (M&S) converge

Synergies exist between the leading industry frameworks for simulation systems and IT solutions. The Object Management Group (OMG) specifies and sets the standards around model-driven architecture (MDA).

The Simulation Interoperability Standards Organisation (SISO) is the standardisation organisation for Modelling and Simulation (M&S), especially for the military space. High-level Architecture (HLA) has proven efficiency. Therefore, the introduction and adoption of ideas and concepts of HLA into MDA is subject to ongoing discussions [1].

Interoperability by Semantics

The European study on "advanced technologies for the interoperability of heterogeneous enterprise networks and their applications" [2] defines levels of interoperability and gives guidance on the roadmap to achieve semantic interoperability on all levels:

- an enterprise service bus (ESB) as the backbone needs to provide the core integration, communication and collaboration services to establish connectivity,
- data exchange standards allow for the interoperability of systems or applications with similar functions, e.g. presentation of data in geospatial context,
- ontologies can be used to structure and exploit the information domain and generate knowledge and insight out of data. They are the foundation of semantic interoperability, and
- finally, coherent processes across organisational and systems' boundaries can be governed on base of these ontologies and the use of a process control language defined by a controlled natural language for knowledge representation.

Model-Driven Lifecycle

The Open Group defines the concept of enterprise architecture (EA) as a layered set of models [3]:

- Organisation
- Process
- Information
- Application
- Infrastructure

Governance of this architecture is performed in context with the EA strategy.

The common strategic imperative of all networked ecosystems is the efficient and effect-oriented performance of the critical information infrastructure during a given reference scenario instantiated at a particular time.

Efficiency and effectiveness have to be measured against the current operational capabilities of the organisation. Capability gaps lead to transformation initiatives implementing the next version of the enterprise architecture.

The transformation roadmap is supported by state-of-the-art model-driven development and governance technologies, which allow for efficient lifecycle management (LCM) not only of singular products, but the enterprise architecture itself.

Governed Interoperability can be achieved via the use of ontologies and a process control language

On the strategic business level, key performance indicators model a balanced scorecard which has to be considered when defining the linkages between strategy level metrics and the underpinning process metrics. The composition of a supporting IT solution should be based on abstract business objects (ABO) patterns to allow for flexibility and re-usability in various client environments.

Service component architecture (SCA) focuses on patterns for the development of functional components and their later integration with foundation infrastructure services to define application services using platform independent models to trigger the generation of platform-specific code. Real-time data monitored to capture IT performance needs to be fed back into a business intelligence exploitation backbone and presented in a business performance dashboard to flexibly govern the business optimisation process.

Threat and Risk Models

Organisations and networked ecosystems are facing multiple dimensions of pressure as it relates to successfully operating in an increasingly competitive environment, e.g.:

- CBRNE threat
- external attacks on facility
- cyber warfare
- weaknesses in information assurance
- system failure
- human factors

The governance, risk and compliance (GRC) solution space needs to address three different categories of concerns throughout the ecosystem:

Enterprise GRC:

- Is performance optimal?
- Are the right risks addressed?
- Are we compliant to external regulations and internal policies?
- Is an integrated view applied?

IT Governance:

- Are investments optimized?

IT Risk Mitigation (CIIA):

- Are we addressing the right operational risks?
- Are we compliant to service level agreements?

Models to express risk on the business level can be categorized and used to define proper measures to protect the critical information infrastructure:

- Contextual Risk Specification: subjective opinions about the risk are identified and the perceived leading indicators are leveraged to determine an event has occurred. An event is a complex combination of situational attributes and their geospatial relationships.
- Probabilistic determination: looking at historical performance as well as subjective assessments one can use Bayesian formulas to predict threats and risks.
- Risk management models: by aligning profiles of risk in context to business processes and controls, we can create a more accurate representation of risk based on control execution effectiveness. Risk profile can be used in complex event detection and processing.

Service Orientation and EA

Whereas SOA can be considered an enterprise architecture model, it is not it is not equivalent with the standardized EA definition. Nevertheless, there is a considerable amount of interlock between the two approaches to business transformation.

SOA is an approach, that through a set of methods provides flexibility to treat elements of the organisation and its underlying infrastructure as standard components, which can be reused and combined to address operational priorities as required to enable an enterprise architecture, which can respond with flexibility and speed to any citizen or government demand, military mandate or external or internal threat and risk.

A service-oriented enterprise is primarily about bridging the gap between business and IT infrastructure – for all architecture artefacts: components, services, compositions and value. In the terminology of EA, there needs to be a model for each type and set of artefacts. These models cannot been considered and developed independently, but have to be closely interlocked. In particular, the end-to-end service identification and implementation needs to provide traceability of performance impacts both forwards and backwards between both the functional and operational level of the organisation as well as in the IT-infrastructure domain. Semantic interoperability based on metadata models

(ontologies) and common understanding of abstract business objects is key to service orientation. The integration and exploitation of information from various data sources (e.g. sensors for external conditions, network and application monitoring systems and situation and event detection services as well as searchable, rich knowledge bases) is the enabler for SOA governance and risk management.

Governed Service LCM

Performance and risk models need to guide and govern the SOA implementation in all phases of the services' lifecycle.

The SOA Governance and Service Lifecycle Management Model enable agile infrastructure protection

Service Identification
A business problem or requirement results in the identification of a future service:

- establishment of ownership
- definition of role of intended service
- allocation of funding
- impact analysis and scheduling

Outcome of this phase is the authorisation of procurement.

Service Specification
follows and consists of the following tasks:

- development, assembly and test using best practices for re-use
- leverage of architectural policy adherent to global standards
- design for re-use and effective re-use in implementation
- policy and contract validation during development

Outcome of this phase is a service ready for certification and available for

Service Implementation
according and compliant to:

- change management policies
- production configuration and workload planning
- verification procedures in operational context
- deployment best practices to production systems

Thus approved the service will enter the next stage:

Service Operation
While being operational, the performance of the service is monitored and measured against the scorecard and key performance indicators, finally entering the next optimisation and innovation cycle:

- policy enforcement
- monitoring for IT and business as well as risk management dashboards
- quality-of-service management
- service revision and retiring policy

Summary

Critical information infrastructure assurance can be achieved by taking an approach of model-driven risk management, protection and underpinning the implementation with a robust enterprise architecture and EA transformation strategy.

References

[1] Building and Integrating M&S Components into C4ISR Systems for Supporting Future Military Operations, Dr. Andreas Tolk & Dr. Michael Hieb, Position Paper for the 2003 International Conferences on Grand Challenges for M&S, 2002

[2] www.athena-ip.org

[3] www.opengroup.org/togaf/

The International CIIP Handbook 2008/2009

In September 2008 the Fourth Edition of the Critical Information Infrastructure Handbook will be published. This publication, like its predecessors, will facilitate a review of problems regarding CIIP policy. Below is a summation of themes and trends in CIIP policy.

Manuel Suter, Elgin Brunner, Fraser McArthur (f.r.t.l.)

Centre for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)

Crisis and Risk Network (CRN) Team
www.crn.ethz.ch

e-mail: suter@sipo.gess.ethz.ch

The Continued Need for Critical Information Infrastructure Protection

At present – and as a result of 9/11 – there is a great degree of time and attention expended upon the protection of physical infrastructure. Whilst this attention on physical infrastructure is not unworthy it should not be at the expense of dedication to Critical Information Infrastructure Protection (CIIP). Two recent events highlight the necessity of continued attention to CIIP.

Firstly, on March the 7th 2008 the Hatch Nuclear Power Station (Georgia, US) initiated an automated emergency shutdown after a computer on the plant's business network was rebooted following a software download. The fact that this power station, like most others, operates an internal network which is connected to the internet means that a number of security challenges have been introduced to the system but, problematically, these issues haven't yet been adequately addressed. This event is symptomatic of a wider problem now facing infrastructure in almost every nation and every sector.

Secondly, the unprecedented DDoS (Distributed Denial of Service) attacks upon Estonia's information technology infrastructure over a prolonged period in April/May 2007 highlights the vulnerability of all nation's regarding Critical Information Infrastructure (CII). The Estonian government, and later private installations, were subjected to a barrage of cyber attacks that effectively disabled them for weeks.

These two incidents show the continued relevance of and necessity for CIIP. The *International CIIP Handbook*, first published in 2002 now in its fourth and substantially expanded edition, offers a comparative overview of these protective efforts.

The 2008 Handbook

The CIIP Handbook focuses on *national governmental efforts* to protect critical (information) infrastructure. The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in an increasingly broad range of countries. The initial eight countries from the 2002 edition (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States) were substantially updated and supplemented by six additional surveys in the following 2004 edition (Austria, Finland, France, Italy, New Zealand, and the United Kingdom). In 2006 we added an additional six country surveys to the existing fourteen, with a distinct focus on Asia (India, Japan, Republic of Korea, Malaysia, Russia, and Singapore).

The utility of the Handbook is in offering nations a guide when constructing their own 'best fit' policy

The inclusion of five new states (Brazil, Estonia, Hungary, Poland and Spain) to the repertoire of cases consolidates and further builds upon previous editions of the Critical Information Infrastructure Handbook (CIIP) to bring the total number of states analyzed to 25. The Handbook has served both policy makers and researchers as an invaluable tool and guide to policy on Critical Information Infrastructure Protection.

Format of the 2008 Handbook

The systematic layout of the Handbook facilitates easy navigation and comparison between the various elements of CIIP. There are five focal points identified by the handbook:

The definition of critical sectors: A core definition of what the particular state believes to constitute critical sectors is provided, in terms of both CI and CII where available.

Past and present CIIP initiatives and policies: A brief review of past policy regarding or relevant to CIIP with a description of the various governmental capacities in which these initiatives or policies were implemented.

Organisational structures: The third section is an overview of public sector actors at a national level responsible for provision of various services regarding CIIP. Importantly, due to the extensive private ownership of elements of both CI and CII, public/private partnerships are also reviewed with regards to CIIP.

Early warning approaches and public outreach: The national organisations instrumental in the provision of early warning of threats, namely CIIP-related information-sharing organisations such as Computer Emergency Response Teams (CERTs) or Information Sharing and Analysis Centres (ISACs) are reviewed. Public outreach programs are also documented.

Law and legislation: The final section catalogues relevant legislation enacted in order to ensure CIIP. Law regarding issues such as IT security, fraudulent use of a computer, handling of electronic signatures, damage to data and data protection as well as any legislation bestowing responsibility on particular organisations for CIIP are provided where available.

An extensive appendix is also provided that offers an invaluable reference utility. The 'Countries at a Glance' section concisely summarizes the most important actors, legislation and documents regarding a particular nation, allowing the opportunity to quickly overview current CIIP policy. In addition a bibliography, list of experts consulted and a directory of important and relevant links are also all included.

Frustratingly the problems identified in the U.S. 1997 PCCIP report under the Clinton Administration still exist

Evolution versus Persistent Problems

After six years of publication the CIIP Handbook allows us the opportunity to identify the problems of these varied responses to CIIP policy. Perhaps the most important point to be made regarding CIIP policy is that despite continual innovation regarding initiatives, legislation and policy in general the underlying problems persist. Frustratingly the problems identified in the United States *Presidential Commission's report on Critical Infrastructure Protection* (PCCIP) under the Clinton Administration in 1997 are still prevalent over a decade later.

Policy efforts are caught in a cyclical state due to the difficulty of addressing their underlying factors.

The primary generic problems facing CII, both in 1997 and today, are that of interdependency, the challenges posed by public-private collaboration and the global character of information communication technology (ICT).

Issue One: Interdependency

The interdependency between varying sectors of critical infrastructure is, arguably, one of the most important relationships for CIIP. Interdependency exists between physical infrastructure and Critical Information Infrastructure as well as interdependency between different sectors of infrastructure (communications, energy, transport). For example the 1997 US PCCIP report heralded the Energy sector as the "lifeblood of these interdependent infrastructures" which is to say that incapacitation of energy infrastructure would have a knock-on effect leading to incapacitation of all other infrastructural sectors.

Attempts to eradicate vulnerabilities in one infrastructural sector (such as energy) are flawed if attempts aren't made to address vulnerabilities in other infrastructural sectors (such as telecommunications) due to the mutual dependency between these two sectors. Infrastructure is comparable to a chain with all infrastructure being only as strong as the weakest of its links.

Little progress has been made in addressing this interdependency, which has in fact been exacerbated over time due to the growth of Information Communication Technology (ICT). As highlighted above in the case of the Hatch Nuclear Power Station there are numerous weak links between different sectors.

Initiatives promoting cross-sector collaboration were formulated as a solution to avoid autonomous weak links and create a sense of a vulnerable cohesive whole; however deficiencies in some sectors continue to plague the entire system.

Issue Two: Challenges to Public-Private Collaboration

The large degree of private ownership of infrastructural components essential to the state necessitates collaboration between the private and public realms to ensure Critical Information Infrastructure Protection. Over the years that the CIIP Handbook has been published there has been evidence of an increasing trend towards public-private partnerships (PPP). However, a number of problems remain. One of the most prominent issues regarding public-private partnership is the role of trust. In order for a PPP to work there must be a basis of mutual trust when passing sensitive information. Cultivation of a system of trust takes time furthermore trust can only be formed by collaboration, while such collaboration itself depends on trust (this is akin to the Chicken-Egg paradox).

CIIP requires cross-sectoral as well as public-private collaboration and a consistent global framework regarding ICT

Another issue that is yet to be substantially addressed regarding public-private partnerships is the lack of incentive on the part of the private sector to invest in the protection of the nation's entire infrastructure, which would inevitably lead to the incurring of great costs. Obviously the lack of incentive and method of protection isn't uniform, a business in commerce or finance is more predisposed to protect itself and its sector than one in transport and it is this disparity that remains a problem today.

Determining the design for PPP's in CIIP is not an easy task. The CIIP Handbook documents the varied responses of 25 nations regarding their believed 'best practice' approaches to these difficult issues.

Issue Three: The Global Character of Information Communications Technology

Another problem is presented to the end of CIIP via the inherently global nature of Information Communication Technology (ICT). The lack of a cohesive multilateral framework to unite currently fragmented nations efforts means that borders still serve as a barrier of immunity from prosecution. Whilst Information Communication Technology transcends borders, legislation regarding ICT does not; this inconsistency is open to manipulation by those fomenting malice.

At present there is little legislative prescription that endeavours to address the global extent of ICT and regulate international incidents. The difficulty of constructing a pragmatic solution to this problem is clear, every nation is at a different stage of ICT development and as such uniform regulative policy seems unfeasible. The CIIP Handbook offers an analysis of the beginnings of some regional and international organisations that could, in the future, offer a potential forum to address this problem. In addition the International Telecommunication Union through its 'Global Cybersecurity Agenda' (GCA) has made substantial progress in proposing what an international framework for organizing national cyber security efforts might look like.

Future Projects

The numerous difficulties facing those developing CIIP policy, as highlighted above, mean that it is imperative to identify successful approaches and 'best practices' in this field. The newest edition of the CIIP Handbook continues to offer a useful monitoring function and a consequent forum for comparative analysis between an ever-increasing number of nations.

However, the purpose of the CIIP Handbook is not to compile a framework for practitioners about the proposed 'best' policy regarding CIIP but, instead, to offer an objective analysis of past and contemporary CIIP policy. The utility of the handbook is in its ability to offer expert-verified analysis as well as a forum for reference and comparison.

The Centre for Security Studies further plans to establish a "special interest community" in the field of CIIP in order to foster increased collaboration between subject matter experts in CIIP in 2009. An online version of the CIIP Handbook will be part of this community.

(*The 2008 CIIP Handbook will be available online at* www.crn.ethz.ch from September).

The Handbook was written by Elgin Brunner and Manuel Suter, researchers at the Centre for Security Studies at the ETH Zurich.

CRITIS'08 - 3rd International Workshop on Critical Information Infrastructures Security

The 3rd international Workshop on CIs and their ICT from 13th to 15th of October 2008 in Rome wants to continue the success of its predecessors and seeks to attract researchers and professionals from all kinds of large critical Infrastructures.

Program Co-Chairs

Stefan Geretshuber

IABG mbH, Germany
InfoCom, Safety & Security,
Dept. for Critical Infrastructures
e-mail: Geretshuber@iabg.de

Roberto Setola

University Campus BioMedico, Italy
Complex System & Security Lab
e-mail: r.setola@unicampus.it

Modern society's dependency on infrastructure services has been widely recognized. The abundance of these services is no more thinkable without ICT that therefore became a key-resource. At the same time ICT is considered as being one of the most vulnerable elements of the whole system.

To continue with the success of its previous editions in 2006 and 2007, CRITIS´08 for the third time will bring together experts from science, industry and public authorities to provide an interdisciplinary and multi-faced dialogue about the third millennium security strategies for Critical Information Infrastructures and their protection.

CRITIS'08 is co-organised by ENEA and by the Italian Association of Critical Infrastructures Experts (AIIC).

The Program Committee received a great number of articles that illustrate research results, R&D projects, surveying works and industrial experiences related to the subjects of the work-shop and conducted a thoroughly peer review process.

Program

Within three days CRITIS´08 will present the 25 most attractive high-quality papers from science and industry arranged in the following six sessions:

- Modelling and Simulation
- Dependency analysis and modelling
- Increasing resilience and self-healing
- Vulnerability and risk analysis
- Cyber threats & SCADA
- Security and Crisis Management

Each session will be chaired and introduced by invited talks from very well known research personalities of the international CI domain. Additional introductive speeches from the national Prime Minister Office and the European Commission will underline the importance and significance of the workshop issues.

One highlight will be as well the round table on the current and future challenges of Critical (Information) Infrastructure Protection attended by recognised international experts from industry, research and politics.

A complementary poster session and a special session on the result of the FP6 research project IRRIIS will complete the broad program.

Location & more

The marvellous workshop location of "Villa Mondragone" and the elegant Gala Dinner in Rome will contribute in making the outstanding event memorable for a long time. Beautiful situated near Rome, Villa Mondragone has been the residence of Popes and famous families of the ancient nobility over the course of its long history. Today it offers with its wonderful gardens and magnificent view towards Rome an excellent and exclusive surrounding for CRITIS'08.

Organisational

The workshop fee includes catering, gala dinner and one copy of the workshop post-proceedings published by Springer in the Lecture Notes in Computer Science series.

The CRITIS'08 organisation committee very gladly welcomes you at CRITIS'08 Workshop. For detailed information and registration please visit:

http://critis08.dia.uniroma3.it

Invited Professor Positions – Univ. of Lisboa Faculty of Sciences FCUL

The challenge for PhD wanting an academic career.

Invited Professor Positions – Univ. of Lisboa Faculty of Sciences (FCUL)

The Department of Informatics of Univ. Lisboa Faculty of Sciences (FCUL) welcomes applications from candidates of any nationality with a PhD, for two positions of *Professor Auxiliar and/or Professor Associado, Convidado em Dedicação Exclusiva* (Full-time Invited Assistant and/or Associate Professor).

The selected candidates will partake the Department's teaching and research activities in Computer Science and Engineering, in the area of Organisation of Computational Systems (OSC, www.di.fc.ul.pt, including the programs of the international partnership with Carnegie Mellon University cmuportugal.di.fc.ul.pt.

The Department of Informatics is very well ranked in the national evaluations www.di.fc.ul.pt/candidatos_licenciatura/?curso, and has a strong international standing in the research activities in the area http://lasige.di.fc.ul.pt.

Conditions:
Up to 4 years contract, salary according to category.

Criteria of preference in order of importance:

- Graduate and/or post-graduate studies in the area of OSC or similar (including operating systems, networking, distributed systems, security, dependability, real-time).
- Track record of research, namely in the area.
- Experience in university-level teaching.
- Fluency in the Portuguese language.

Candidates must provide, until the 31st July 2008:
Curriculum vitae (name, address, degrees, work/research experience, publications, citations, achievements, etc.)

- Transcripts of grades and proofs of the capabilities stated by the candidate. Copies allowed. Legal originals required in case of selection.
- Letter of intent (up to one page) mentioning the personal motivations for applying to the Univ. of Lisboa.
- Two letters of reference, sealed, together with application, or sent by referees directly to the organisation contact, in plain ASCII or PDF or paper, by fax/mail or email (Subject: Concurso Professores Convidados).

Organisation contact data:
Concurso Professores Convidados

Departamento de Informática - Faculdade de Ciências da Universidade de Lisboa

Bloco C6 Piso III, Campo Grande

Lisboa - 1749 – 016

Portugal

Email: secretaria@di.fc.ul.pt

Internet: www.di.fc.ul.pt

ECN-10 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*
- *1st International Conference on Critical Infrastructure Protection and Resilience (ICCR 2008), August 26 and 27, 2008 in Davos, Switzerland: www.tinyurl.com/ICCR-2008*
- *4th International Conference on IT-Incident Management & IT-Forensics www.imf-conference.org*
- *3rd International Workshop on Critical Information Infrastructures Security, critis08.dia.uniroma3.it*
- *INFSO D4 events, http://cordis.europa.eu/ist/trust-security/events.htm*
- *Conference is sponsored by the Next Generations Infrastructures Foundation and the IEEE Systems, Man & Cybernetics Society: "Building Networks for a Brighter Future, 10-12 November 2008, De Doelen Congress Centre, Rotterdam, The Netherlands: http://www.nginfra.nl/conference2008/*

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*

European Projects or Projects with Articles in this Issue

- *IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems: www.irriis.eu*
- *Institute for the Protection and Security of the Citizen: http://ipsc.jrc.it http://ec.europa.eu/dgs/jrc/index.cfm?id=1630&lang=en http://ec.europa.eu/dgs/jrc/index.cfm?id=2360&obj_id=PROJECTS00000000030002AA&dt_code=ACT&lang=en*
- *Governance and Risk Management in a globally integrated Ecosystem: References: www.athena-ip.org www.opengroup.org/togaf/*
- *The International CIIP Handbook 2008/2009: (available 4Q2008): www.crn.ethz.ch*
- *Invited Professorship /MSc in Information Secuirty: www.di.fc.ul.pt_cmuportugal.di.fc.ul.pt*

E-Reports

- The Royal Academy of Engineering published its report *Dilemmas of Privacy and Surveillance* in March 2007: *www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf*

Series of new Reports

- *Martin Rudner, Protecting Canada's Energy Infrastructure Against Terrorism: Mapping a Proactive Strategy, CEIPPR Research Series No. 1 – 2008*
- *Jacques J.M. Shore , The Legal Imperative to Protect Critical Energy Infrastructure, CEIPPR Research Series No. 2 – 2008.*
- *Jack F. Williams, Al-Qaida Threats and Strategies: The Religious Justification for Targeting the International Energy Economy, CEIPPR Research Series No.3 – 2008.*
- *Sean Burges, Jean Daudelin, & Roy Fuller, Latin America's Energy Infrastructure and Terrorism: A Tentative Vulnerability Assessment, CEIPPR Series No. 4 – 2008*

IMF 2008
4th International Conference on
IT-Incident Management & IT-Forensics

September 23 - 25, 2008
Mannheim, Germany

www.imf-conference.org/
mailto:2008@imf-conference.org

Conference of **SIG SIDAR**
of the **German Informatics Society (GI)**.

Call for Participation: see www.imf-conference.org

Information technology has become crucial to almost every part of society. IT infrastructures have become critical in the world-wide economy, the financial sector the health sector, the government's administration, the military, and the educational sector. Although security usually gets involved into the design process of IT systems nowadays, the process of maintaining security in the operation of IT infrastructures, in most cases, still lacks the appropriate attention. The capability to manage and respond to IT security incidents and their forensic analysis are not well established. The quickly rising number of security incidents worldwide makes the implementation of incident management capabilities essential.

Program with Keynotes held by:

Dr. Udo Helmbrecht

Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

John L. Cole

US Army Research Laboratory
Chair, IEEE Task Force on Information Assurance (TFIA)

Fred-Mario Silberbach

Bundeskriminalamt (BKA) LS - Stab der Amtsleitung
Felix Lindner ('FX') Recurity Labs GmbH

Preliminary Program 2008

- Using Observations of Invariant Behaviour to Detect Malicious Agency in Distributed Environments
- Network Forensics of Partial SSL/TLS Encrypted Traffic Classification Using Clustering Algorithms
- Forensic Computing Framework to fit any Legal System
- File Type Analysis Using Signal Processing Techniques and Machine Learning versus file Unix Utility for Forensic Analysis
- Reconstructing People's Lives: A Case Study in Teaching Forensic Computing
- Live Forensic Acquisition as Alternative to Traditional Forensic Processes
- 6Foren: Online Forensics in IPv6 Network Environment
- IPv6 Attacking Test Using ICMPv6 Messages
- Building a state tracing Linux Kernel
- Network Flow Security Baselining

IMPORTANT DATES

September 8, 2008:	Early registration will end
September 23-25, 2008:	IMF 2008 Conference

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection

ICCR 2008
1st International Conference on Critical Infrastructure Protection and Resilience (ICCR)

an Associated Conference to the International Disaster & Risk Conference
(IDRC Davos 2008)
Davos, August 26-27, 2008

Organised and co-chaired by the Swiss Federal Office for Civil Protection
and IDRC Davos 2008

mailto:ski@babs.admin.ch

Call for Participation: see www.tinyurl.com / ICCR-2008

The theme of the ICCR 2008 is "Expanding the Concept of Critical Infrastructure Protection: From Protection to Resilience." The conference will take an integrated, multidisciplinary approach when addressing the different aspects of CIP and resilience. It particularly makes the point that it does not suffice to physically protect critical infrastructures, but that a holistic approach including an integrated risk management cycle and risk governance is necessary by specifically including measures that increase the systemic and social resilience.

The conference builds on the five EAPC/PfP Workshops on Critical Infrastructure Protection (CIP) and Civil Emergency Planning (CEP) between 2003 and 2007 and further expands on its network and information platform as well as deepens its knowledge and expertise.

Program Chair:
Dr. Stefan Brem, Head of Risk Analysis and Research Coordination, Federal Office for Civil Protection, Switzerland

Speakers include:

- Michel Bruneau, Buffalo University, New York, US
- Jost-A. Studer, Studer Engineering, CH
- Wolfgang Kröger, ETH Zurich, CH
- Jean-Pierre Nordvik, JRC, Ispra, I
- Ortwin Renn, University of Stuttgart, GE
- Adrian Gheorghe, Old Dominion University, Norfolk, US
- Ivo Menzinger, Swiss Re, CH
- Eric Luiijf, TNO, The Hague, NL

Programme Highlights:

- Integrated Risk Management in a CIP Context
- From Protection to Resilience
- From Defining Critical Sectors to Establishing Criticality Criteria
- Public Private Partnerships: Concepts and Applications
- Planning and Disaster Response

Registration:

There is no limitation of participation per country or institution. Registration is possible directly on the website:
tinyurl.com/IDRC-2008-registration