January / February 2007, Volume 3, Number 1

ECN

European CIIP Newsletter

IRRIIS

> 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, ECN is financed by the IRRIIS project
The IRRIIS project is an IST FP6 IP,
funded by the European Commission
under the 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

>Founder 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***

> Graphics and Layout
Florian Widmer florian_widmer@gmx.net

> Spelling:
British English is used except for US contributions

Table of Contents

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events (online Version only)

National CIIP Projects are Starting.

The emphasis if this issue has grown and more articles are available. This fact is just a mirror of the growing activities C(I)IP activities in European Union.

Dr. Bernhard M. Hämmerli

Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
President ISSS
bmhaemmerli@hta.fhz.ch
bmhaemmerli@acris.ch

ECN was intiated with the CACIIRCO Project

Eric Luiijf, Eyal Adar and my self were editing 5 issues of ECN on behalf of the CIIRCO co-ordination action. It was a time with a lot of support; my warmest gratitude is directed to the co-editors, to all CIIRCO project team members and ECN authors.

ECN is now with the IP IRRIIS

ECN has found a new umbrella on behalf which we can continue for three more years. Already in the last numbers the IRRIIS project was introduced. However, mailing lists and editors addresses will remain. We are looking forward to the new period with the support of the very large IRRIIS project team.

About this Issue

The first section consists of two articles about EU funded CIP Projects and the challenging statement of director European Homleand Security Association, ESHA that CIP should be reframed in a holistic way.

The section of national issues is dedicated mainly to one of the largest national C(I)IP research project within EU: The Netherlands “Next Generation Infrastructure” NGI Project. Furthermore a new curriculum with a strong dependability focus (master level) is presented.

Section methods and models discusses decision models in order to get fast automatic vulnerability information, a brief resume of the PhD theses “Network Reliability” of Dr. Mark de Bruijne is given and the interaction between CIP, safety and crises management is discussed. As an unusual topic, legal aspects of early warning are researched. The legal dimension is often too much neglected and it is very good to consider this dimension as well.

Two international conferences are announced in the last section.

About the Link Collection

This issue will first be published in a printed version. The link collection will be published exclusively in the online version of ECN, available form mid February

The complete link collection of all ECN issues can be found on www.irriis.eu (within the download section)

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

This is the first issue, which is published on both, www.irriis.eu and the www.ci2rco.org. Furthermore we hope, that all ECN mirror sites will be maintained further.

Enjoy reading the ECN!

A Survey on ICT Vulnerabilities of Power Systems.

The GRID Coordination Action funded by the IST Programme has recently performed a survey on the needs of the power sector concerning the ICT vulnerabilities of power systems and the relevant defence methodologies

Alberto Stefanini

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.
Alberto.Stefanini@jrc.it

Robert M. Gardner

Robert M. Gardner is working as a Ph.D. student in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His research interests include wide-area monitoring and control of large-scale systems.

Nouredine Hadjsaid

Nouredine Hadjsaid is a full Professor at INPG and the President of the International Institute for Critical Infrastructures (CRIS). He is interested in research on the control and security of the power networks.

Jean Pierre Rognon

Jean Pierre Rognon is a full Professor at INPG and a member of the INPG Presidency team. He is interested in research on availability and predictive maintenance of electrical devices and systems.

Vulnerability of the electrical infrastructure appears to be growing due to growing demand, hectic transactions, growing number of stakeholders, complexity of controls, as made patent by the major recent blackouts over Europe and North America. Although these events do not seem to have been influenced by malicious acts, existing vulnerabilities could be exploited by malicious threats in the future.

GRID is a Coordination Action funded under the Trust and Security objective of the IST Programme of the 6th Framework to achieve consensus at the European level on the key issues involved by power systems ICT vulnerabilities, in view of the challenges driven by the transformation of the European power infrastructure. GRID wants to assess the needs of the EU power sector on these issues, so as to establish a Roadmap for collaborative research in view of the forthcoming 7th Framework Programme. Partners in GRID are mostly European research institutes and organizations from the energy and ICT communities.

The survey involved 600 members of industrial and research communities across Europe. Of those polled, 57 responded

Recently GRID has completed a survey on the opinions of the European industrial and research communities about the challenges raised by ICT power system vulnerabilities. This was started through a stakeholder Conference (held in Stavanger on June 15, 2006 within the Energy Forum) and relied on a questionnaire, which was disseminated to a broad selection of professionals, approximately 600 members of industrial and research communities across Europe and beyond. Of those polled, 57 responded; nearly 10 percent. Of the respondents, 34 are from the industrial community and 22 from the research community. The questionnaire covered three points: Criticality, Vulnerability and Areas of Future Emphasis. Within each point, respondents could rank specific issues. Rankings were based on a scale from 0 to 3. For example, a rating of 3 in the Measurements subsection of the Criticality section would indicate that the respondent considers Measurements to be of highest criticality.

Industry respondents were from six categories: transmission system operators (TSO), power companies, manufacturers, regulators, corporate research, and distribution system operators. TSOs were the single most dominant voice in industry. The survey was not deliberately formulated to generate this imbalance. It merely indicates that a higher level of interest in the ICT vulnerabilities of power systems exists within TSOs.

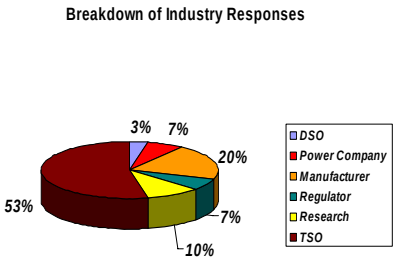


Figure 1: Graphical breakdown of all industry responses.

Criticality

Protection was ranked as the most critical function followed closely by **control**. The reason for such high rankings in these two areas is that a single error in protection and/or control has the potential to lead to larger events of a severe nature (voltage instability, blackout, etc.). The ability of protection systems to both limit damage under normal expected operation and to exacerbate problems under abnormal

operation makes the protection area critical. C**ontrol** comes in a close second with protection. The proper circulation of information in the control loop is the key element in control criticality. The availability of correct incoming and outgoing information is essential in supporting and executing operators' decisions regarding control actions. **Monitoring** criticality is at its highest during events and afterwards in the restoration process. Display clarity is the key in monitoring criticality. **System management and coordination** is critical for its inclusion of energy transactions between neighbouring countries and transmission operators. The telecommunications network is quoted as a critical component of both management and coordination on one hand and measurements on the other. **Measurements** [1] are seen as highly critical collectively and barely critical individually due to the high level of measurement redundancy. **Operator decision support** ranked the lowest in criticality due to the heavy reliance on the sound judgment of experienced operators.

Fig 2 shows the criticality average rankings of each kind of function.

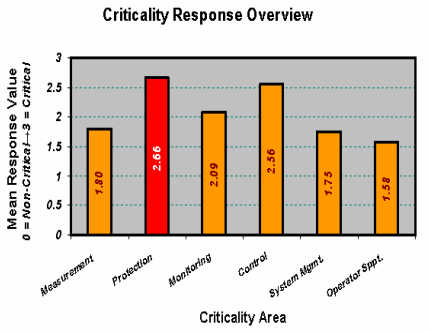


Fig. 2. Functions criticality ranking

Members of the industrial community mentioned redundancy as a key factor in the lower criticality of the measurements. Research communities did not express as much faith in measurement redundancy.

To better understand Fig. 2, the overall rankings by function, Fig. 3 shows the variances of the different responses.

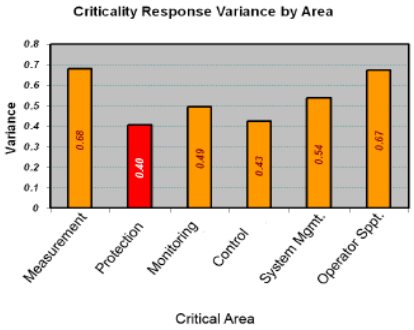


Fig 3. Criticality response variance

There is a large consensus (and therefore the variance is low) on protection and control criticality. Contrarily the high variance on measurements and operation decision support answers reveal important disagreements on these issues. The conclusions are supported by several comments accompanying the answers which express some interesting dualities. Measurements, collectively, are seen as very critical. Without measurement, closed-loop control is impossible. However, individual measurements are seen as much less critical for reasons of redundancy. Disagreement in the operator decision support rankings is caused by two lines of reasoning. Some stated that experienced operators do not rely on sophisticated tools to run the system. Others insist that an operator's job becomes impossible without operator decision support tools.

Vulnerability

Protection, the function with highest criticality ranking, also ranked highest in vulnerability. Hidden failures and configuration/settings errors are of primary concern. Remote access via ICT and sensitivities to ICT failures also cause protection schemes such as wide-area protection and distance relays to have increased levels of vulnerability.

Measurements are seen as highly vulnerable mainly because of the high failure rate of RTUs and the reliance of wide-area measurements on ICT functions. The tendency of data acquisition methods away from privately owned dedicated networks on to potentially less secure systems is a cause for concern. Wide-area monitoring seems to be the key link that makes monitoring both critical and vulnerable. The term "wide-area" suddenly marries measurement devices such as RTUs (with their famously high failure rates) and monitoring functions such as state estimators (with their famously sound robustness) together through the ICT medium. The questionnaire findings indicate that it is the ICT interface with power systems that increases risk and vulnerability. State estimators are not seen as highly vulnerable and are permanently observed, thus monitoring enjoys a lower level of vulnerability.

System management and coordination along with **operator decision support** were the least vulnerable functions owing largely to confidence in operator experience. Fig. 4 shows the average rankings of each function as for vulnerability.

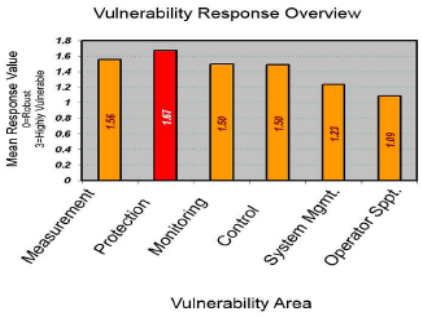


Fig 4. Functions vulnerability ranking

[1] The questionnaire was designed such that elements such as remote terminal units (RTU) and phasor measurement units (PMU) were listed in the measurements area. Also, elements such as state estimation and display functions were included in the monitoring area.

The topic of ICT vulnerability of power systems does not enjoy as much agreement as criticality. There was much more spread in the rankings: the lowest variances in vulnerability are close to the highest variances in criticality (Fig. 5).

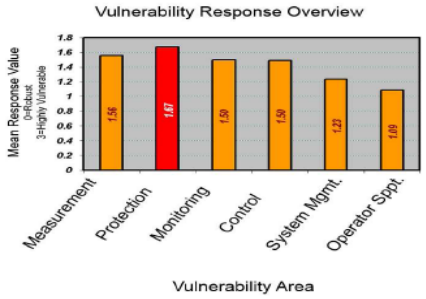


Fig 5. Vulnerability response variance

The rankings for control vulnerability tended towards a ranking of 1 as did monitoring vulnerability. This result is interesting since control functions were, in general, ranked at the highest level criticality. As in measurement vulnerability, the adoption of open communication systems and protocols is seen as a potential for increased vulnerability. Monitoring facilities are seen as a potential target for attacks, especially those heavily relying on ICT. For instance, tampering of alarm settings via an ICT break-in was listed as a concern. The mental balance of experienced operators is seen as a key factor in lowering the vulnerability of control functions: like system monitoring, control functions are seen as easy to supervise and thus less vulnerable.

The rankings for vulnerability in operator decision support area tended strongly towards a ranking of 1. Those that thought this function was not very vulnerable were referring to operators that did not rely on sophisticated tools, whereas those that ranked this function as vulnerable were referring to operators that rely heavily on computerized/software tools. In general, respondents agree that operator support vulnerability increases during system disturbances – when such support is most needed. Those that issued the highest level of vulnerability noted that operators' decisions are supported by the other five kinds of functions. Therefore, the weakest link in the ICT function chain can cascade to the operator decision level.

Protection and control ranked the highest in criticality and vulnerability

Areas of Emphasis

The emphasis on risk and vulnerability tools and methods rises above the rest, considerably. Cyber-security assessment of critical online equipment is needed but there is a lack of appropriate methodologies. The effort to "amalgamate the risk analysis of electrical contingencies with cyber security analysis" is encouraged by those polled. The lack of appropriate risk and vulnerability tools is explained by the lack of a broadly accepted conceptual basis for risk assessment. The redesign of control architectures and technologies is not a popular idea, while the upgrading of control architectures and technology is highly emphasized. The results of the survey suggest that an evolution is in order – not a revolution. A main challenge voiced in the control issue is to "integrate innovative control equipment with the legacy control systems…" The focus is on researching wide-area controls that are impenetrable to hackers.

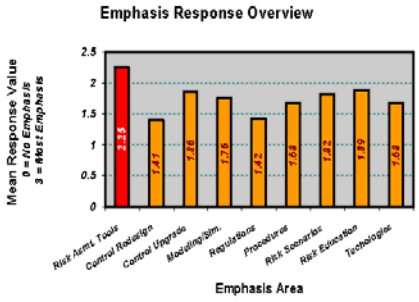


Fig 6. Emphasis response ranking

Risk scenarios and risk education are also highly emphasized. Incorporating ICT risk scenarios into operator training programs is suggested along with the establishment of a risk database to include relevant previous risks. The lack of ICT/cyber-security studies on power systems controls is noted as a problem needing remedy. The incorporation of risk studies at the earliest stages of learning for all power engineers is encouraged. Fig. 6 above shows the overall response breakdown for the emphasis areas. Interestingly, areas of highest emphasis, such as risk scenarios, risk and vulnerability tools, and risk education, corresponded to areas of most agreement.

Conclusions

According to the recent survey performed by GRID with the European industrial and research communities concerned, protection and control were found to be the most critical issues in terms of the interface between ICT and power systems. Protection and measurements were found to be the most vulnerable. Control is perceived to be less vulnerable, because of confidence in operator capabilities. Concerning emphasis areas, risk and vulnerability assessment tools and methods were especially stressed. High emphasis on risk scenarios and risk education support this finding. Finally, the industrial research community supports an upgrade of control technologies, rather than their redesign.

DESEREC: Dependability and Security by Enhanced Reconfigurability.

DESEREC is an integrated project of the Sixth Framework Programme of the European Union in the thematic area "Information Society Technologies", under the Strategic Objective "Towards a global dependability and security framework".

Pedro Pérez

Pedro Pérez is a consultant at GMV Soluciones Globales Internet in Tres Cantos, Spain. He is currently involved in the DESEREC project
pperez@gmv.com

Benoit Bruyère

Benoit Bruyère is the DESEREC Programme Manager.
Benoit.BRUYERE@fr.thalesgroup.com

The fast growth of highly interconnected Communications and Information Systems (CIS), and the use of them to carry out critical activities, has opened an important issue regarding the resilience, reliability and security of these CISs. DESEREC aims at managing the mission-critical Information Systems in order to optimise the use of the CIS resources for the provision of its business services. The strong interdependence increases the consequences of accidents, failures, attacks and implies high vulnerabilities. Only a multi-disciplinary approach is able to leverage dependability of CISs by an alliance of the following three approaches, currently scattered into separated scientific fields:

The multi-disciplinary approach allows DESEREC to respond efficiently to incidents and threats.

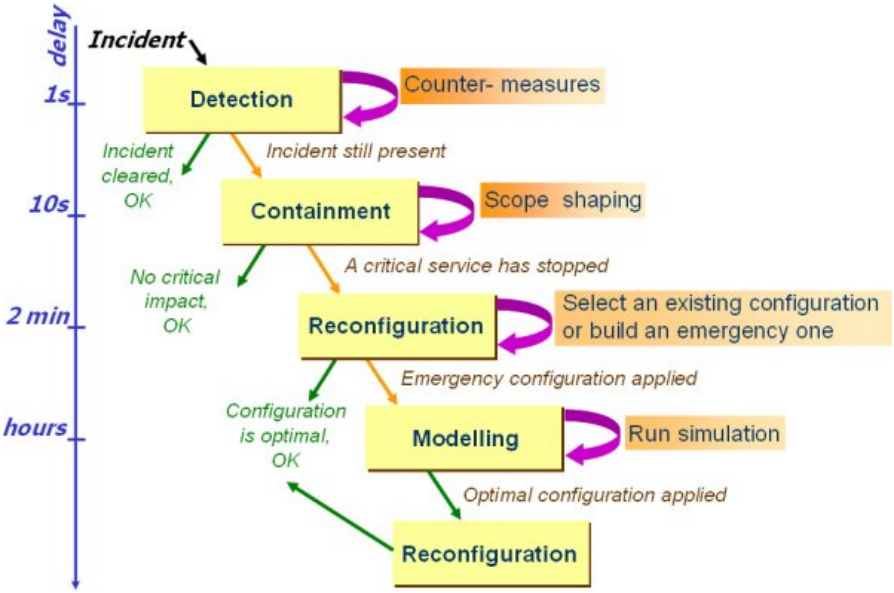
- Modelling and simulation: DESEREC devises and develops innovative approaches and tools to design, model, simulate, and plan critical infrastructures to dramatically improve their resilience.
- Detection: DESEREC integrates various detection mechanisms to ensure fast detection of severe incidents but also to detect complex ones, based on a combination of seemingly unrelated events, or on an abnormal behaviour.
- Response: DESEREC provides a framework for computer-aided counter-measures initiatives to respond in a quick and appropriate way to a large range of incidents to mitigate the threats to the dependability and rapidly thwarts the problem. CIS Re-configuration is the utmost mechanism for their survivability.

Multi-disciplinary Approach

This multi-disciplinary approach allows DESEREC to respond efficiently to the three families of incidents which can occur on a critical system: *Attacks from the outside, Intrinsic failures and Misbehaviour or malicious internal use.*

As incidents act with different time scales and impact levels, DESEREC includes three response loops working on three different answering times to provide a suited answer:

- A few seconds to locally respond to a severe and well-characterized incident and to launch an emergency curative procedure to avoid escalation process or dramatic damage.
- Some minutes to detect a very complex problem and to readjust the system (i.e. through computer aided reactions) in order to maintain the critical business services. The prime objective of DESEREC is to increase the availability of the services provided to end-users of the CIS giving the priority to the critical ones (from the stand point of the service provider).



- Some hours to build a new configuration optimised to resist to a new situation and validated through modelling and simulation

Study Areas

DESEREC targets the Strategic Objective "Towards a global dependability and security framework".

DESEREC aims at providing methods and tools to analyse, design, model, simulate, and plan, the optimised configurations of resilient information systems supporting critical activities. DESEREC improves risk management as well as infrastructure dependability and survivability with reconfiguration methods and automated support tools for incident detection and reaction on different time scales.

To achieve this goal, DESEREC:

- Designs, develops and validates tools for incident detection and decision support. The tools span different time scales and provide solutions for survivability that range from immediate reaction to global and smooth reconfiguration through policy based management for an improved resilience.
- Enhances the self-healing properties of mission-critical infrastructures by planning, designing and simulating optimised architectures tested against several realistic scenarios.
- Improves risk management, crisis management in critical infrastructures with the design of new models, countermeasures, and incident management tools as well as a thorough analysis of several situations (infrastructures and scenarios). Devises, characterizes, models and designs mechanisms to mitigate the cascading and escalading effects induced by inter and intra dependencies.
- Develops decision support tools for critical infrastructures, validated by scenarios for several case studies on infrastructures.

Objectives

The DESEREC project aims at improving resilience of complex mission-critical systems where many European activities rely on them.

DESEREC proposes solutions to ensure coherent and efficient dependability management of such complex systems, relying on an information network by providing solutions on the three domains:

- Planning: Modelling, simulation, and utility tools with a suitable approach to plan optimal operational configurations, detection and reactions scenarios through modelling and simulation of critical system and their potential threats. They allow to define a coherent and homogeneous operational mode and to define the efficient response to an anticipated incident, the process to face unexpected ones and the method to restore an optimal usage of the system after a switch to a degraded configuration.
- Detection and Prevention: Distributed, multi-technology sensors and a set of detection mechanisms to detect all kind of incident that can occur in the system. They ensure fast detection of elementary incidents and in addition, elaborate the detection of distributed incident from a combination of apparently unrelated events or from an abnormal behaviour in the system.
- Reaction: a framework for computer-aided and automated counter-measures initiatives in order to respond in a quick and appropriate way to a large range of incidents. These responses include the identification of the scope of a given incident, the best approach to isolate the "suspected" devices to avoid propagation of threats or a cascading effect.

The methods, tools and utilities are provided with hooks for interactions (notifications, provisions, self-learning and human-aided rules optimization) and share a common repository with the topology, the planned configurations, the rules for activities precedence and any other relevant information.

Project Plan

The DESEREC project will be developed during 3 years from January 2006 to December 2008.

The DESEREC project aims at improving resilience of mission-critical information systems.

So far the system requirements have been defined after the compilation of requirements from end-user scenarios as well as the conclusions extracted from the state of the art reports. The next steps are the design of DESEREC architecture allowing the development of an initial prototype for mid-2007.

In a second phase, DESEREC, based on a refined architecture, will develop a set of modelling tools as well as a final prototype. Such prototype will be demonstrated in one of the test bed environments provided by the end-user partners taking part in the project.

Dissemination

Several dissemination and training activities are planned and will target a various audience. As DESEREC envisages both to work on the relating disciplines and to provide tools, the consortium will present results to academics, researchers, and industrials. These events will cover the mechanisms, case studies, as much as results and concrete outputs of the projects.

End of September, the 1st DESEREC Training Workshop took place at Wroclaw University of Technology, Poland. The workshop presented project aims, analysed test beds and foreseen architecture, focusing on the problem of Information Systems modelling for dependability analysis. It was a very successful event with more than 50 participants: end-users, academia and representatives from partners.

Partners

The partners involved in DESEREC project expect to strengthen their experience in managing dependability of large IT systems and in particular in maintaining their most critical business services.

The list of partners is provided below:

Industrial Partners

- **Thales Communications (France, Project Leader)**
- Canadian Research Center (Canada)
- EADS Defence and Security Systems SA (France, Technical Leader)
- Exaprotect (France)
- IABG (Germany)
- Intracom (Greece)
- Security Evaluation Analysis and Research Laboratory (Hungary)
- GMV- Soluciones Globales Internet (Spain)
- Trusted Logic (France)
- TNO (Netherland)

Academic Partners

- Budapest University of Technology and Economics (Hungary)
- Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni (Italy)
- École Nationale Supérieure des Télécommunications (France)
- Politecnico di Torino (Italy, Scientific Leader)
- Wroclaw University of Technology (Poland)
- University of Murcia (Spain)

End Users

- Renfe Operadora (Spain)
- Hellenic Telecommunications Organization (Greece)

Web site: www.deserec.eu

Latest information may be found easily on the DESEREC web site: public documents, news about project events, references to publications and subscription to the project newsletter are available

Critical Infrastructure: An Expanding Concept.

A proposal to understand CI in a holistic way: prevention, protection, response and post-crisis recovery

Ambassador RICHARD NARICH

Advisor to the Director of the Institut National des Hautes Etudes de Sécurité (Paris) and President of the European Homeland Security Association (Brussels)
richard.narich@e-hsa.org

The protection of critical infrastructure is a topic that can be viewed from the perspective of "business continuity"' or from the perspective of internal or national security.

I will limit myself to a general overview.

The idea of critical infrastructure seems quite clear although it can vary according to the country. It comprises the necessary installations for the normal functioning of a country. This consists of, for example, nuclear plants, ports, roads, etc.

I will look at four points:

a. The expansion of this conception. The term "critical infrastructure" was originally connected with only the physical infrastructure; however, it increasingly includes all of the critical functions of our societies.

b. The importance of the protection of this infrastructure. This is at a primary level, in terms of global security in a world where the risks and threats have only multiplied.

c. The way in which we have attempted to face this challenge. I will briefly comment on the technical approach, but I will primarily focus on the institutional approach.

d. The entirety of vulnerabilities.

1. The expansion of the concept of critical infrastructure.

Currently, an evolution and extension of the vocabulary of this concept is noticeable.

I will give three examples:

Firstly, an infrastructure can be deemed critical because it is important to the overall functioning of a group of activities, for example, an electrical installation. The infrastructure thus becomes 'systemic.'

Secondly, it is important to protect the static infrastructure against all sorts of aggression and damage. However, it is becoming increasingly important to also protect services, the physical and electronic flows of information, and the messages that these are transmitting. Furthermore, next to a barrier, which is a physical infrastructure, we can legitimately place the supply security chains or the transactions effected by financial institutions or banks.

IT-systems are becoming increasingly complex, and consequently, increasingly vulnerable.

Thirdly, an infrastructure can also be deemed critical because it is symbolic. The first example that comes to mind is evidently that of the World Trade Centre in New York. However, we could also mention the Eiffel Tower or the British Parliament.

Another important aspect that has become related to critical infrastructure protection is that of protecting the critical infrastructure also in terms of information and information technology.

The physical protection e.g. of a plant has received much attention over many years, even if necessary precautions are not always taken. .

In contrast, the protection of IT systems is a new concern. It is crucial for three

main reasons: these systems are, as we have already said, at the heart of all economic activity. They are becoming increasingly complex, and consequently, increasingly vulnerable. Moreover, the threats are becoming more and more insidious and more and more effective.

In a general manner, the notion of the critical infrastructure covers not only the physical infrastructure, but the critical functioning of society.

2. The protection of critical infrastructure in a new context of international security

The need to protect critical infrastructure is not a novelty. Natural disasters, human errors, both capable of causing great damage, have always been a major preoccupation of public powers and enterprises.

In the case of a conflict, these infra-structures become strategic assets that must be protected, as they provide prime targets for the aggressor.

Why then has this topic been of primary interest these past few years when dealing with security issues?

Two moments come to mind.

This first is the information revolution, with the new risks that it brings that need mastering. The USA has played a pioneering role in this regard since 1997.

The second reason can be attributed to the terrorist attacks of September 11, 2001, against the USA.

These two moments reflect in their own way, the increasing complexity and interdependence within our modern societies, and, consequently, their fragility.

This complexity, these interdependences and this fragility result from different causes:

- a technical cause being the interconnection of the information network which supports all essential productive activity;
- an economic cause being the process of privatization which has developed in the 1990s in many regions of the globe, primarily Western Europe. This led to many economic activities that were previously controlled by the state to enter into the hands of the private sector. This in turn provoked a fragmentation of the infrastructure and the necessity of coordination of protective actions;
- a geographic cause being the process of globalization, which transgresses all borders and creates interdependences. As such, the critical infrastructure in one country can be controlled by enterprises in its neighbouring country.

Furthermore, the supply chains often greatly depend on external markets.

Finally, the management and protection of this infrastructure are becoming increasingly difficult tasks.

These evolutions are occurring at a moment when international terrorism is exercising its ravaging effects, even though the consequences of natural catastrophes are even direr.

3. How this problematic is taken into account?

We have the technical approach. I will cite three examples.

Firstly, the analysis of risks: Due to the increasing difficulty faced to protect installations and more and more complex systems, it is necessary to turn to a more technical solution. Even if this has not been completely refined, its ambition is to answer the following questions: What could the flaws be? What is the probability that they should occur? What would the consequences be? What can be done? What are the available options? What are the advantages and the disadvantages in terms of cost, benefits and risks? What impact can current management decisions have on future choices?

Second example: the research programs in terms of security that are currently financed by the European Commission are part of susceptible projects aimed at better protecting these infrastructures.

Finally, my third example is that of the European program CI2RCO, launched a couple of months ago, most notably in order to address the inventory of all of the technological and information research centers that exist at the heart of the Union, so that it becomes possible to reinforce their cooperation, eliminate doubles, etc...

When it comes to the institutional approach, absolutely necessary and largely sufficient, the following points have to be addressed: an increasing interdependence between sectors in the same country; a greater dependence of national responses in relation to the international environment; a public / private / organizations / international / civil society cooperation, which is being imposed more and more.

All developed countries and a number of international institutions are seeking to advance these projects.

Here too, I will give three examples.

Firstly, the European Commission launched a program destined to reinforce the critical infrastructure in Europe a couple of months ago, in the context of the fight against terrorism. The latter encourages member states to establish lists of their critical infrastructure constituents where they do not have them, and if they do, to update them. It also seeks to define the critical infrastructure at a European level.

Secondly, the protection of critical infrastructure in terms of information is the subject of an enormous project on the international level. As such, the G-8 made recommendations on this point three years ago. However, this is but one initiative among many others.

Thirdly, this topic has also become current in the developing countries exposed to terrorist threats. Strong diplomatic activity has developed over the last few months on the initiative of certain Western governments, in order to incite particularly threatened states to protect themselves, according to the principle that security is indivisible.

These projects are not easy to deal with. Progress is thus more or less rapid.

In this quest for security, not one person thinks that the protection can be total. This is why experts increasingly prefer to speak of 'robustness' or 'resilience'.

4. Critical infrastructure and other vulnerabilities.

To be concerned solely with critical infrastructure does not suffice to totally secure our societies. The critical infrastructure constitutes but one of their vulnerabilities. To be thorough, it is necessary to add the protection of populations and of borders. These three elements, when taken together, along with the palette of risks and threats we currently face, constitute the true 'new topic' of security for the next few years.

The Governments of the major countries are all concerned, notwithstanding that they have different conceptions and varying approaches.

As such, the American initiative of Homeland Security emphasises on the terrorist threat against which the country is waging a 'war,' and several federal structures have been newly created or regrouped within the country to face the threat.

The Nordic countries have a more decentralized and holistic approach (all hazards approach), which puts all of the threats and risks on the same level, and mobilizes all of the means and citizens (societal security).

The European Union regards the protection of the citizen as the central point. The terrorist threat is but one threat among others, and the political approach is thus favoured.

One can remark that, despite the differing conceptions, the response is practically of the same nature, whether a country is facing a terrorist attack or an epidemic.

It is also more and more acknowledged that civil defence and the armed forces should work more closely within this context. At the decision-making level, the question of knowing whether or not one should distinguish between civil defence operations or military operations is increasingly pondered. The cooperation between these two poles is clearly marked during major crises. Indeed, the systems used for both military and civil means, called dual-use technologies, are expanding more and more. Examples include drones, helicopters, airplanes, etc.

Finally, the boundaries between plain defence and civil defence are becoming increasingly clouded when it comes to nuclear, chemical or biological threats, or even the trafficking of small arms .

5. Conclusions

We are still, no matter what is said, in a largely Westphalian world. The difference is that our societies are threatened also in times of peace.

To face this, the holistic approach is the legitimate one. As mentioned previously, the treatment of these problems is the same whether it concerns a terrorist act, a human error, or a tsunami. Reinforcing the prevention, the protection, the response and the post-crisis recovery is, in effect, reinforcing the whole of the mechanisms by which a society can defend itself. It thus indirectly discourages terrorism “by other means”.

Finally, war and peace still remain in large part, the affairs of the Governments. The treatment of new threats, however, becomes the business of all: Governments, International Organizations, the private sector, research, and civil society.

These are the few points I wanted to close the report with, which has no ambition to go beyond a purely technical expertise.

It nevertheless seems to me that an appropriate forum is missing where these problems could be addressed in their totality, and involving all of the actors that are concerned.

P.S.: This text was delivered in June 2006 during a special meeting dedicated to the so-called „new threats“ at the UN Conference on Disarmament in Geneva.

Infrastructure Security at Carnegie Mellon and Lisboa Universities.

The University of Lisboa Faculty of Sciences (FCUL) takes part in the CMU-Portugal partnership between Carnegie Mellon University and the Portuguese Government, with joint CMU-FCUL Master and PhD programs in Security and Dependability.

Paulo Veríssimo

Professor of the Department of Informatics of the University of Lisboa Faculty of Sciences, Director of LASIGE, member of the European Security & Dependability Advisory Board and associate editor of the IEEE Transactions on Dependable and Secure Computing.

Faculdade de Ciências da Universidade de Lisboa, Campo Grande, 1749-016 Lisboa, PORTUGAL

pjv@di.fc.ul.pt

The University of Lisboa Faculty of Sciences (FCUL) takes part in the CMU-Portugal partnership between Carnegie Mellon University and the Portuguese Government through the Ministry of Science, Technology and Higher Education. The partnership has an initial 5-year phase during 2007-11 and is materialized by a joint "Information and Communication Technologies Institute", ICTI, with poles in CMU and in Portugal. Several Portuguese research and education institutions are involved, with the affiliation of a number of industrial companies.

FCUL has a leading role in one of the initiatives of the program, Information and Infrastructure Security and Dependability, through faculty from the Department of Informatics, and researchers from LaSIGE, the Large-Scale Informatics Systems Laboratory.

There are two graduate programs: MSc and PhD. Either will confer a dual degree, both from CMU and FCUL.

Master and PhD Programs

During the next 5 years, FCUL expects a number of students and researchers from all over the world and from Europe in particular, to enjoy the experience of a transatlantic research and graduate education (MSc and PhD) environment between CMU and FCUL, contacting with researchers and faculty internationally experienced in the extremely attractive and state-of-the-art areas of computer and network security and dependability.

Professionals in search of further specialization, or students or researchers in search of further progress through a Master (MSc) or Doctoral (PhD) degree, should check the opportunities of CMU-FCUL programs with the quality seal of Carnegie Mellon University.

There are two graduate programs in this initiative: MSc and PhD. Either program will confer a dual degree to the successful candidates, both from the Carnegie Mellon University and from the University of Lisboa.

Joint Research

Besides community building actions, two exploratory projects are defined for the first phase, which will serve to: address perceived research problems; establish research relationships and trust relations; better organize global discussions and braining-storming; and promote the definition of more structured ideas leading to focused projects in the second phase. Research will be structured in two working groups: WG1 - Security and Dependability of Large-scale Computer Systems; WG2 - Secure Systems of Embedded-Systems.

More information:

http://cmuportugal.di.fc.ul.pt/

http://www.icti.cmu.edu/

Next Generation Infrastructures: Facing the Complexity Challenge.

Understanding and steering the behaviour of infrastructure systems is a daunting knowledge challenge. Researchers and practitioners have joined forces to secure the future performance of our critical infrastructures.

Prof.dr.ir. Margot Weijnen

Scientific Director of the Next Generation Infrastructures Foundation. Full professor of process and energy systems engineering at the Delft University of Technology, where she heads the Infrastructure Systems & Services Department in the Faculty of Technology, Policy and Management.

M.P.C.Weijnen@tudelft.nl

The Next Generation Infrastructures consortium unites researchers from a variety of disciplines and practitioners from all critical infrastructure sectors in a concerted knowledge effort to improve the reliability, quality and affordability of infrastructure related services. Originally a Dutch national initiative, the consortium is now quickly expanding across national borders. The composition of the consortium reflects the multi-actor complexity of today's infrastructure systems. Besides a variety of knowledge institutes, the consortium involves infrastructure system operators, service providers, technology providers, capital providers, contractors, public policy makers, and regulators.

The current program spans five subprograms and a total of 65 projects, with 85 full time equivalents of research capacity. The number of projects is envisaged to increase to approximately 100 as the 40 million Euro program unfolds over its projected lifetime, from 2004 until 2012. An international Scientific Advisory Board and a User Council supervise research progress from an academic quality and a utilization perspective, respectively.

Dealing with new types of complexity

The need for such a massive knowledge effort is evident from the huge complexity of today's critical infrastructures. The complexities of the physical infrastructure system are evident and could adequately be dealt with in the public monopoly era, when capacity expansion and infrastructure innovation were centrally planned and coordinated. However, the new era of deregulation, market liberalization, value chain unbundling and privatization of public utility functions has brought an unprecedented multi-actor complexity of the social infrastructure system. In the new reality, the development of our critical infrastructure systems is determined by the distributed decision making of a multitude of actors who each strive to optimize their own subsystem. Many new actors have entered the playing field, often in new roles.

Unprecedented multi-actor complexity of critical infrastructure systems

Public policy makers must face new reality

The predominant conceptual frameworks underpinning the design of public policies towards infrastructures, in particular regulatory and network economics, law and engineering are based on methodological assumptions that are at odds with the reality of present and next generation infrastructure systems. These disciplines utilize a mechanistic approach in which the design of optimal policy is seen as a problem of constrained optimization under conditions of uncertainty. While this approach may have been adequate for modelling policy problems during the era of government monopoly, it is inappropriate and potentially leads to wrong policy recommendations in the present environment of multiple service

providers, reliance on market forces, and convergence.

An integrated systems approach

The complexity of the social network mirrors the complexity of the physical network. Both the physical and the social system are characterized by multi-agent, multi-level, multi-objective and dynamic complexity, leading to emergent system properties.

Advanced infrastructure systems are better characterized as complex socio-technical systems, which are composed of several interacting sub-systems. These sub-systems include, but are not limited to, the technical components of the infrastructure, the economic system through which transactions are organized and the political system in which important governance decisions are made. These are, in turn, complex adaptive systems. Governance issues can only be effectively solved if the co-evolution of these systems is properly understood. Thus, a new framework is needed that better reflects the complex evolutionary nature of infrastructures.

The Next Generation Infrastructures program is unique in its ambition to grasp the complexities of both the physical and the social subsystems, to the extent that we can model and understand their interactions and steer the behaviour of the integrated socio-technical infrastructure system.

The challenge is not to come up with a universal model of critical infrastructure systems.

Driven by practical knowledge needs

The variety of disciplinary angles needed to understand the various complexity aspects of infrastructure systems and model their behaviour includes – but is not limited to - mathematical graph theory, game theory, statistical physics, system dynamics, agent-based modelling, simulation gaming, institutional economics, law, and organizational behaviour. The challenge as the Next Generation Infrastructures consortium perceives it is not to come up with a universal model of critical infrastructure systems, but rather to derive a systematic framework and a methodology for combining and confronting the techno-physical and socio-economic modelling perspectives. The ambition is to derive a common framework for all critical infrastructure sectors: telecommunication, transportation, energy and water infrastructures.

This is not an academic quest we embarked on for reasons of scientific elegance; it is essentially driven by very practical needs. In the present world of interconnected and converging infrastructure systems, infrastructure system performance characteristics such as robustness and security are interdependent across infrastructure systems based in different sectors and subject to different market designs and regulatory regimes. If we are to understand their interactions and interdependencies, a common methodological and modelling framework is a *conditio sine qua non*.

Communities of Practice

Another practical reason for a common systematic framework is the development of a common vocabulary. Effective knowledge sharing between researchers from different disciplines and between practitioners from different infrastructure sectors is seriously hampered by a lack of consistent terminology. Even though the programme is still in its infancy, the first promising results of the development of infrastructure system ontology are apparent from the emergence of vibrant Communities of Practice where practitioners exchange knowledge across sectional borders. CoP's have emerged to exchange best practices and lessons learned in infrastructure capacity management, asset life cycle management, innovative contract arrangements, and the safeguarding of public values.

The infrastructure system ontology is steadily developing as it is being applied in agent-based modelling of infrastructure system co-evolution. Such modelling efforts have already proven to generate valuable insights into the co-evolution of energy and industrial networks, which are finding their way to the planning processes of a world-scale harbour-industrial complex.

Simulation gaming

Besides through CoP's the Next Generation Infrastructures programme involves practitioners from the infrastructure sectors in numerous other ways. Practitioners actively participate in the research process, e.g. through participation in simulation games. These may be designed to test alternative institutional arrangements: how do individual actors behave under different institutional arrangements and how does their collective decision making work out for the development of the integrated socio-technical system?

Simulation games bridge the gap between social and technical sub-system behaviour and turn out to be a very useful tool for public policy makers in testing the robustness of new institutional designs and intervention strategies. Decision makers from the infrastructure industries use the games to test their business strategies in different institutional environments. Also for them, it is a great learning tool to gain insight into their interdependencies with other sub-systems and into the strategic behaviour of other actors with common and/or conflicting interests.

Although primarily being developed as interactive research models, Next Generation Infrastructures' simulation games are already used abundantly as participative methods for strategy making and policy recommendations. Last but not least, they find their way to education and training programs for practitioners in the public and private sector.

Public values at stake

A substantial subprogram of Next Generation Infrastructures is aimed at identifying the numerous public values at stake in the design, management and governance of infrastructure systems and designing institutional arrangements for safeguarding these public values. It is interesting that certain values are considered to be public in one country and private in another. We argue that public values cannot be defined objectively and unambiguously; rather, public values are emergent. For example, privacy and security are relatively new public values associated with infrastructure systems, which were triggered by the penetration of information and telecom networks into all infrastructure sectors and by the 9-11 terrorist attacks, respectively. As a consequence of technological and societal development and discrete events, the set of public values perceived to be at stake may be changing, as well as the definition of certain public values and their order of priority.

Public values cannot be defined objectively and unambiguously.

As a result of the unbundling and decentralization processes in the critical infrastructure sectors, the responsibility for safeguarding specific public values is not always clear. Neither is it clear which measures and governance models are effective in the liberalized market setting as each of the players in the game - incumbents, entrants and other players, act strategically to reduce, delay, or control competition. This behaviour has not fully been anticipated by orthodox economists, who assumed that disbanding public monopolies and allowing new players in would automatically create a competitive market. In reality, strategic behaviour forces governments to design regulatory regimes and intervene in such a manner that level playing fields are promoted and public interests safeguarded, following Wirick, *"It is naive to believe that such markets would not require ongoing oversight to make certain that exclusionary behavior, tying, monopolization, price-fixing and other anti-competitive behaviors do not occur*".

One of the research questions tackled by the Next Generation Infrastructures consortium is: What types of regulatory regimes (i.e. combinations of regulatory style, instruments and repertoire of interventions) are conceivable, which enable regulators to anticipate and deal with strategic behaviour and to safeguard public interests? In this specific project, the regulators of the Dutch infrastructure-based industries are involved.

It is nothing short of remarkable that the reliability of critical infrastructures has been maintained at such a high level in the liberalized market setting.

The challenge of networked reliability

In contrast with public opinion, the performance of most critical infrastructures has only improved over the last decades. The widespread public dissatisfaction with the reliability and quality of infrastructure related services should apparently be attributed to our increasing dependency and increasingly stringent service quality demands. It is, however, nothing short of remarkable that the reliability of critical infrastructure based services has been maintained at such a high level in the situation of the liberalized market and distributed decision making. On the basis of both normal accident theory and high reliability theory one would have predicted a dwindling reliability performance in the new setting of multi-actor decentralized decision making. However, as case studies with KPN Mobile and the Californian electricity transmission system operator have shown, the deeply distributed intelligence in both the physical and the social subsystem, most notably the expert knowledge and improvisation talents of the system operators, has saved us from quite a few pending outages. This result is encouraging, but not to the extent that we can trust our critical infrastructure systems to self-organize the reliability performance society will need in the future.

On the one side, all critical infrastructure industries are struggling with an aging work force and a pending lack of engineering professionals in the future. It is therefore questionable if they can timely replace their experienced work force and instil the same level of professionalism and professional pride in the next generation of system operators.

On the other side, there is great pressure on the intensity of infrastructure capacity usage, which makes the systems more vulnerable e.g. to fluctuations in demand or to transient flows. To ensure reliability of service in the longer run, sufficient levels of maintenance and (timely) investment in new infrastructure capacity and innovation are needed. In this realm

there is real reason for concern. In e.g. the electricity market, timely investment in new generation capacity is not likely to come about unless a capacity market or an alternative capacity mechanism will be installed. In the absence of such an intervention, a boom-and-bust cycle with prolonged periods of scarcity is likely to develop: in other words, prolonged periods of frequent outages and sky-high prices, which may well lead to disruption of society and the economy.

The quest for flexibility

In the dynamic liberalized market environment of present and next generation infrastructures, investors in new infrastructure and infrastructure capacity have to cope with new uncertainties in addition to the massive uncertainty inherent to the long lifespan of infrastructure systems. Since infrastructures are deeply embedded in society, they are not only subject to technological change but also have to stay in synch with institutional, economic and societal developments. Infrastructures should be able to respond to new opportunities and threats and to changing social requirements, for instance regarding ethical and environmental issues.

Such adaptability or flexibility requires new approaches to the design and management of infrastructures, starting with taxonomy of uncertainties pertaining to infrastructure design and operation and methods to handle the various types of uncertainty. The Next Generation Infrastructure program is amongst others investigating the potential of Exploratory Analysis and Modelling and Real Options Analysis in designing and retrofitting infrastructure systems.

The flexibility concept is less developed for transient modes than for static modes of operation. For dynamic modes of operation a generalized flexibility concept is being developed and tested. In addition, multi-scale models of flexibility are being developed for infrastructure components and for the overall structure, suitable for application in the synthesis and analysis phases of a design, in order to allow for Life Cycle Costing.

For more sophisticated asset management in the infrastructure sectors a risk-based approach is being developed, which dictates a priority of asset management projects that is elegantly aligned with the business logic. In too many infrastructure industries asset management is still considered in terms of costs rather than being recognized for its contribution to strategic business objectives. This risk-based approach to asset management poses a formidable organizational and cultural challenge for the traditional infrastructure industries where the asset management function is dominated by hard core engineers. However, considering the active interest of the infrastructure network owners, they are ready for change.

Risk-based asset management poses a formidable cultural change challenge to the traditional infrastructure industries.

The promise of intelligent infrastructures

The Next Generation Infrastructures Foundation is not only concerned with the long term performance of critical infrastructures: we are also prepared to face imminent operational problems that require new, more intelligent modes of operation for today's infrastructure systems. Many of our infrastructures are being stretched to their limits, as they have to respond to increasing demand in terms of bare capacity and service quality. As the lead time for new infrastructure capacity may range between years and decades, there is enormous pressure to 'milk' existing capacity. It is evident; however, that better capacity utilization may not violate other public values, such as service quality, safety and environmental constraints.

The projects in this line of research are a.o. concerned with multi-level and multi-criteria optimization, with multi-actor dynamic congestion pricing as a road capacity management strategy, and with computer simulation and visualization techniques. An advanced simulation based platform is being developed to support controllers and operators in choosing the right control strategies and making the right operational decisions.

Accelerated knowledge effort

Infrastructures are so deeply embedded into society and the economy that their existence has long been taken for granted, and they were used without specific reflection. It is this characteristic that seems to have caused the neglect of infrastructures as a topic area in academic research, especially in technological research, which generally focuses on specific infrastructure components without questioning the infra-*structure* and the working of an infrastructure as an integrated system.

However, the notion of infrastructure system *criticality*, brought about by terrorist attacks but also by accidents, maintenance and service delays and system outages, has given rise to massive research efforts all over the world. The knowledge quest is further fuelled by the growing concerns voiced by network operators and public policy makers on the vulnerabilities brought about by the links and interdependencies between our critical infrastructures systems.

Combating the fragmentation of knowledge and governance

As a lot of the massive new research effort is focused on CIIP, on

technological solutions and the specific public value of security, the challenge that remains is to ensure an integrated socio-technical systems approach. Only then can we ensure that the technological solution strategies do not create conflicts with other public values (at least not to the extent of social unacceptability) and will be backed up by appropriate governance models. It is precisely the fragmented nature of governance, fragmented as it is over nation states, infrastructure sectors and specific public values that seems to be the greatest obstacle to safeguarding the future quality and reliability of critical infrastructure related services.

Joining forces

It is a necessity therefore to join forces, across disciplines, across sectors, across national borders and across the border between academia and practice. The Next Generation Infrastructures consortium is open to new partners, and in turn is open to joining other critical infrastructure focused knowledge initiatives, whether in research or education and training.

If you want to be on our mailing list for new publications and upcoming events, then visit www.nginfra.nl and leave your address. The Next Generation Infrastructures consortium is not only organizing many national events and seminars, it is also actively disseminating knowledge through a.o. the conferences organized by the IEEE Societies of System, Man & Cyvbernetics (SMC) and Networking, Sensing & Control (NSC).

First International Infrastructure Systems & Services Conference

You are cordially invited to submit your proposals for special sessions or a special conference track at the 1rst International Infrastructure Systems and Services Conference "Building Networks for a Brighter Future" of the IEEE System, Man & Cybernetics Society in Rotterdam, April 7-9, 2008.

Increasing Survivability of Critical Information Systems.

The Medusa project is a project within the Next Generation Infrastructure (NGI) program that applies Biologically Inspired Information Security (BIISec) to resist multiple random failures in critical IT infrastructures and systems.

Dr.ir. Semir Daskapan

Delft University of Technology
Faculty of Technology Policy and Management
Section Information & Communication Technology

S.Daskapan@tudelft.nl

It has been proclaimed by many experts already that we need more novel approaches to protect our critical infrastructures. Traditional methods are simply not sufficient to assure the dependability of our vulnerable complex and large interdependent infrastructures. In the BIISec project we derive novel ideas to deal with this increased vulnerability of Information Technology (IT) infrastructures from the field of complex biological systems. The Medusa protocol set is one of the outcomes of this project.

Infrastructures rely on ICT

Many critical infrastructures, like telecommunications, transportation, banking and transmission and distribution of electrical power rely nowadays for their control heavily on the correct operation of information systems. Such information systems are therefore called critical information system (CIS). A failure to such a CIS can jeopardize the dependability of the infrastructure that it supports. The recent earthquake in Taiwan in December 2006 has shown again how crucial CISs are. For, with the disruption of the Internet some CISs were disconnected. Among others, this interrupted local and international banking transactions for a while. It is obvious that we must increase our effort to protect those CISs, especially now those CISs become more complex and use public (internet) networks. Many critical infrastructures rely on decentralized and sometimes even distributed CISs for their correct operation. Think of the remote traffic control systems in Hong Kong or SWIFT (Society for Worldwide Interbank Financial Telecommunication) for banking. Consequently, in this Internet era these CISs have increasingly become the targets of sophisticated (denial of service) attacks of hackers, which cause random failures. Common technologies designed to improve their resilience will not help sufficiently, since they are based on costly, dedicated and limited redundant hardware systems. The inherent weakness of redundancy as defence principle is that each attacked system will be replaced until there is no spare system to replace with. This is an unacceptable risk for CISs and the critical infrastructures they support.

We can only master complex infrastructures by learning from the complex nature around us

Biology to control Complexity

The goal of the Medusa project was then to develop "middleware" by which the complex CISs can resist endless unforeseen attacks. We were inspired by the mammal immune system. Knowing that the mammal body is immensely complex and that it is mostly capable of controlling this complexity autonomously is something we can use as a model to learn how to master our 'simple' human-made complex systems. The analogy we want to draw is that clustered computers can be used to clear failures, like the mammal immune system is doing with antigens by seamless collaboration of the cells. By attributing similar properties to CISs as those of the mammal cells the different components of a CIS should be able to build and operate a distributed defence system (DDS) autonomously.

The Medusa research project is focused on how to improve the resilience of the security systems of a CISs, since they are primary responsible for the protection of the CISs and indirectly thus of the supported infrastructures. We will call those security systems that provide one or more of the security services, i.e. identification, authentication, confidentiality, integrity and non-repudiation, security distribution centres (SDCs).

Medusa

In this section we will briefly explain the main deliverable from this phase: the so-called Medusa protocol set. It provides an adaptive DDS that ensures perpetual availability of security systems when resisting an endless number of failures. Like the mammal

immune system, Medusa distinguishes rare and common security breaches and deals with them in different ways. As is shown in figure 1 three main security processes characterize the SDC life cycle. The most inner cycle depicts security session management (SSM), i.e. the process that takes care of one or more of the security services that the SDC delivers. The continuous SSM process might be the execution and control of any authentication protocol, for example KryptoKnight and Kerberos, but other security services are also possible. The middle and outer cycle protect the SDC itself from any failure. Their efforts are mainly aimed at guaranteeing the availability of the SSM. The middle cycle, called the innate response system, takes care of known and simple failures. When more complex and unknown failures emerge the middle cycle calls the most outer cycle, i.e. the adaptive response system. This system runs then the survivable security management process (SMP) that is based on the execution of three sub protocols: preparation, narcosis and resurrection.

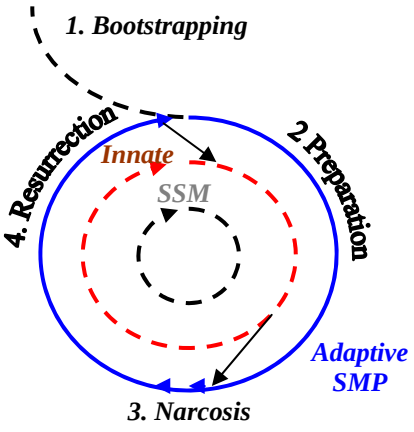


Figure 1 SDC life cycle

Medusa's phases

An SDC starts with *bootstrapping* (1). In this phase we assume a starting point where all the computers of a CIS perform their task independently. The main goal of this phase is to link the several trusted computers within subparts of the CIS with each other by secure self-organization. At the end of this phase each subpart SDC has a list of other computers, i.e. a pool, which are trusted and with whom it will collaborate in the next phases.

In the *preparation* phase (2) measures of precaution are taken by each SDC to anticipate on possible failures. The 'core' components of an SDC are frequently sent to all the members of his pool, like passwords or keys in case of Kerberos, which are exchanged in encrypted form; this is the token. The receiving host does not have the key to decrypt it. The token should be preserved there until the sending SDC collapses. The token can be resurrected then by the host after receiving the appropriate keys from other computers in the pool.

Protocol 3 deals with the *narcosis* of the SDC. In this phase the difference between the innate and adaptive response system becomes evident since the suffering SDC reacts in two ways. An attack is first encountered by deploying immediately the conventional means like firewalls, intrusion detection systems and virus scanners. Whereas those defence systems have the benefit of a quick reaction, they are not always effective, since they rely on known attacks and predefined restrictions. Since the SMP runs continuously as a background process, the adaptive system can be called at any moment the innate system fails to recognize and/or to respond. When at a sudden moment the SDC is suffering from numerous attacks or any other detectable random system failure, the SDC stops sending 'heartbeat messages'. The pool members (in the trust pool) on their turn send requests for heartbeat messages to check the state of the suffering SDC (again). When the suffering SDC has indeed a bad condition (collapsed or bad performance) and cannot reply to requests in a timely manner, the resurrection sub-protocol of the last preserved state of the token of the SDC will be started by the pool members. Roll back mechanisms will take care of uncompleted security transactions.

Protocol 4 deals with the resurrection of the trust token. The token can now be reconstructed by the host, which was appointed earlier in the preparation phase by the former (collapsed) SDC, but only when it collects a majority of secret pieces from other pool members. After the resurrection of the complete token the successor continues the security services on behalf of the previous SDC.

Conclusion and Future Developments

It has been shown in the test phase that Medusa was capable of resisting multiple Denial of Service attacks. The tests were performed up to 100 computers in a WAN topology. This model was exposed to multiple distributed denial of service attacks (DDOS) to cause system failures.

Despite those results, Medusa is still not capable of distinguishing all types of attacks. Neither is it capable of dealing with the condition of the attacked SDC in more detail: so far, it is considered either dead or alive. The reaction on an attack is also not very smooth: it can resurrect or not. In future work we intend to embed such refinements. This requires more systematic knowledge about the working of the mammal immune system.

Practical Decision Support for IT CIP.

IT CIP, a complexity challenge defined by network and human interaction. A new initiative tries to develop a decision support system helping the operational personnel to identify and fight critical situations.

Stefan Burschka

Head Intrusion Management Lab at Swisscom Innovations. CIP, AI, IT-Security, Decision Support, Data Mining.

stefan.burschka@swisscom.com

The introduction of IT to the management layer of our Critical Infrastructure (CI) creates opportunities but also adds dangerous deficiencies, reducing their reliability and fault tolerance thus provoking abnormal network behaviour or even outages. Key players in this game are the following facts:

- No KISS (Keep It Simple Stupid) enabled designs
- The "Banana Principle"
- Legacy design problems in HW
- The Human: Part of a self inflicted and emerging complexity

The basic engineering law of KISS design knowledge is elusive in IT systems, mostly due to historical and commercial reasons. Hence, important factors such as, robustness, fault tolerance and resource regulation, intrinsic qualities of early mechanical and analogue systems are lost. HW redundancy and SW methodology helps but does not prevent the so called "Banana Principle". It denotes multiple product maturation cycles at the customer's side until the product is fully functional even under dynamic conditions.

CI operations need fast and effective decision making

Almost all buffer overflow attacks on system and application level are due to a violation of a golden rule: "The separation of the executable program area and non-executable data area." There are CPUs who comply with that rule but they lost market acceptance, being a bit more expensive, than e.g. Intel designs. Due to technological inappropriate decisions in the past, we pay now the debt with the dependability of our CIs.

The said factors trigger almost all security leaks and provide the ground for self inflicted and emerging complexity in our systems, not curable by any SW methodology or ostentatious major Consulting Companies. All this combined with human beings of limited computational power and data comprehension and the need to decide in minutes or even seconds can create havoc.

Human administrators with their long term experience actually being the immune system of our critical infrastructures try to keep them alive 24/7. This scenario defines one future challenge the telecommunication field of dynamic mobile services and P2P infrastructures has to face. The core problem of failures and outages can be easily evaluated in practice by asking operational personnel.

Boundary Conditions

Provided appropriate perimeter defence and AAA measures exists [1] we have seen in the last years the following causes for outages:

- Cyber Attacks < 0.1%,
- Miss-configurations = 70%,
- HW/SW Failures = 30%

So our primary concern should be on the human side to enhance fast and effective decision making to prevent and troubleshoot outages or failures. In order to achieve that good decision making is

required in all situations, which require the following factors:

- Information
- Preferences
- Knowledge
- The goal and cost estimates for different scenarios

These factors are actually available in abundance but scattered in different locations or heads or not clearly defined at all. Especially the network to business concept relation is still subject to intensive research. In practice the development of scenarios for price and target estimation in large organizations are often too cost intensive and therefore substituted by pragmatic approaches or omitted at all. Standard Decision Support tools, as being used in business decision support, requiring manual data acquisition and modelling are of only limited use IT. The reason is the distributed complex ever changing environment interacting with humans itself. Some practical problems each IT admin or the security personnel has to face are listed below:

DCS requires automated data acquisition

- Dynamic Environment Machines, Services and Responsible change
- Huge number of network elements and machines
- Various and sometimes unknown network interconnections
- Information overload, meaningless Alarms, False Positives
- Fragmentation of knowledge
- Policy compliance
- Temporal criticality of a decision
- Reaction time: Human decision chains

The combination of topological knowledge, complicated human decision chains and last but not least the lack of awareness of the temporal criticality of a certain decision of an operator on the whole functionality of the CIP is the prominent cause for failure. Criticality or the sensitivity of decisions on other system functionality is time dependent. Therefore approaches with static knowledge are insufficient.

Approach to Decision Support (DCS)

There are methods and tools available to automatically acquire e.g. topological and vulnerability information. So an in-depth analysis for IT infrastructures should be done automatically. Characteristics and configuration of its components are theoretically known. What is unknown is its sometimes emergent behaviour, due to human interaction and the "banana principle".

The problem left is to acquire vital parts of information and to store it normalized into centralized databases. An often underestimated problem, otherwise the basis of a good decision, the correlation with other sources, such as Intrusion Detection Systems (IDS), system logs, and firewall logs is not possible.

Nevertheless, automated alarm reduction and correlation is available for IT infrastructures [1] and works if used by skilled personnel. But practice showed that automated hidden models are not accepted by humans because they like to understand and build their own knowledge base to react more quickly.

Humans in IT admin and security are experts. They like simplicity in their complexity to be fast and effective, e.g. the use of own C-shell or Perl scripts instead of complicated GUI's. An approach, which favour low qualified workforce operating intelligent tools must fail in critical situations, when in troubleshooting is required. So the correct approach is the collaboration of computer aided decision support utilized by many human experts.

What is needed is a pragmatic approach utilizing the knowledge of humans combined with automatic interaction of knowledge between machine and human. Also the constant evaluation of productive system component sensitivity and scenario building and most important forgetting is of vital importance in dynamic environments. Drill down features for problem identification, disaster prediction and centralized instant repair and UNDO functions [1] are other necessities for successful outage prevention.

This task is clearly beyond the nowadays available tools of risk management, because static modelling is almost impossible. Moreover risk management focuses on time independent problems and scenarios which are known and before they happen. Decision support has to deal with the unknown time dependent operational risk in real time to prevent an imminent threat to whole or parts of the systems operation.

DCS Model

Research in DCS goes back to the 70'ies. Most of them are essential rule based models or CBR expert systems, or probabilistic models [2,3]. They all require a clear definition of decision paths, goals, and risks. Widely used in risk management for business processes, or in the military regime.

Some interesting approaches are in the area of CBR [4], Cognitive Function Modelling [5] or workflow modelling [6] which might be useful as a start. In our complex "banana principle" systems

the definition of preferences (Policies) and goals (operational parameters) is theoretically possible, but practically very time consuming and often not feasible.

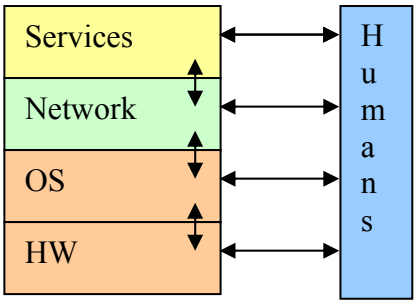


Figure 1 Interaction Model IT CI

Complex systems such as in Fig 1 tend to be high-dimensional, non-linear and hard to model. Even under specific circumstances they may also exhibit low dimensional behaviour, but still be pretty much sensitive to initial conditions, so that even a limited prediction of the systems path is only possible if the complete system is correctly represented and infinite computing accuracy is available.

In order to describe the behaviour of such a system the complexity of environmental variables and actions will defined as C(e) and C(a) respectively. The response is normally described by the response function f, where a = f (e). Without simplifying or heuristic assumptions, specifying the response to each environmental input requires an amount of information that grows exponentially with the complexity of the environment.

$C(f) = C(a) \cdot 2^{C(e)}$

Thus modelling and dynamic scenario building will be a vital part of our research. Combined known heuristics with new ways of sensitivity measurements in productive systems could be a possible approach to beat the exponential limitation.

Challenges of future DCS

The solution of the following unsolved challenges will be vital for a successful completion of the project.

- Human Acceptable Data reduction techniques
- Integration of hidden human knowledge
- Limits of abstraction: High abstraction might be useless in practical environments
- Automated dynamic model parameter acquisition
- Automated Integration of human knowledge and preferences
- Reduction of human biases, Integration of preferences
- System dynamic topology database
- Online sensitivity measurement of productive system
- Central UNDO function as human error compensation
- Short time prediction of outcome in nonlinear systems
- Drill down feature for troubleshooting
- Useful Anomaly detection: Emergent, unpredicted but normal behaviour assessment
- Automated Scenario modelling and adaptation

Simplified rule based scenarios will not work in the telco case, because of its unpredictable dynamic behaviour. The chance and the challenge might be the fact that there is knowledge available from operational personnel. Inspiration from the abilities of trained human minds being capable to sense anomalies could be adopted in AI based approaches.

Decision Support Project

We at swisscom have to focus on helping human operators to prevent incorrect actions, or troubleshoot in a time efficient way. We cannot change the way systems are build today in a few years time. Thus our approach has to be lead by our practical experience in dynamic environments of critical infrastructure operations. The goal is to use as much of existing technologies to be as close to practice as possible and focus the research only on the said unsolved research parts. A solution should then enhance the capability of existing IDS and Management Systems and Static DCS in productive environments.

We currently define a project, where the resulting DCS should be extendable to other types of critical infrastructures.

References

[1] http://www.stns.ch/Safeguard/

[2] http://www.mirrorservice.org/sites/home.ubalt.edu/ntsbarsh/Business-stat/opre/partIX.htm#rtreeinflunc

[3] Howard, Ronald A. Decision Analysis, 1998, o.O.

[4] www.environmental-expert.com/magazine/inderscience/ijram/art2.pdf

[5] http://www.aptima.com/publications/2000_Anastasi_Klinger_Chrenka_Hutton_Miller_Titus.pdf

[6] IDS-Autopilot: Automated Workflow Modelling, Swisscom, Dominic Windisch, Stefan Burschka

Networked Reliability.

Societies' growing dependence on ICT urges us to think about Critical Information Infrastructure Protection (CIIP). But, how do liberalisation and institutional fragmentation affect the reliability of our Critical Infrastructures?

Mark de Bruijne

Assistant Professor, Faculty of Policy, Organisation & Management, Delft University of Technology.

A copy of the dissertation: *Networked reliability, Institutional fragmentation and the reliability of service provision in critical infrastructures* can be obtained by contacting the author. Mail to:

M.L.C.deBruijne@tudelft.nl

Societies' vital services are provided through large complex critical infrastructures. In all of these infrastructures, information and communication Technology (ICT) play an important role. Another, often ill-considered aspect of critical (information) infrastructure, is that they are increasingly provided through networks of organisations.

Networks of organisations and their effect on reliability

Liberalisation – but also technical developments such as the rise of ICT and economic trends such as outsourcing – ensure that the reliability of service provision of critical is no longer the task of single organisations, but networks of organisations. Recent research unveiled how the increasingly networked character of large-scale critical infrastructures affects their ability to provide high levels of reliability. The results were surprising and apparently contradictory.

The networked character of critical infrastructures limits their ability to provide reliable services

Operations in two critical (information) infrastructures (i.e. the electricity and telecommunications industries) were found to be negatively affected as a result of institutional fragmentation. Network operating companies had to ensure high levels of service provision under increasingly unforeseen and highly turbulent circumstances. The networked character of the industry and the lack of central command and control, severely limited the ability of operators to maintain the reliability of service provision in both industries. Nevertheless, despite these difficulties, both industries maintained a highly reliable provision of services.

Real-time management

What can guarantee continuous high levels of reliability when the ability to achieve reliability through central command and control diminishes? Decentralise automated and intelligent operations? The evidence pointed in another direction.

The increased complexity and loss of control that resulted from institutional fragmentation caused critical (information) infrastructures to behave less predictable and less manageable. Planning, control and routines – traditional means to maintain reliability – failed to provide reliable services.

The consequences of institutional fragmentation for central command and control were found to be the least affected in real-time. In real-time, network operators regained control of network operations by using their expertiseas well as ability to improvise.

It can be concluded that, as a result of institutional fragmentation, reliability in networked critical (information) infrastructures shifts to real-time, the domain of control room operators. Researchers, policy makers and companies involved in CI(I)P, would do well to acknowledge this change.

Legal Aspects of IT-Security Warnings by Public Authorities.

The article deals with legal problems of IT-security warnings by public authorities. The main emphasis is put on comments on the German and the Swiss law.

Alexander Koch

works as a lawyer in Bonn, Germany. He is managing director of the Institute for the Law of Network Industries, Information and Communications Technology (Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie, IRNIK)
http://www.irnik.de

ak@irnik.de

Introduction

Official warnings about security gaps in IT-products take place in a complex legal environment. In times of permanent attacks via computer networks, the public – on the one hand – does have a need to get reliable, i.e. official, security warnings. On the other hand, companies whose products have been wrongly said to be dangerous may raise huge claims against the public authority that has issued the (wrong) warning. Generally, there are three different types of warnings, depending on the source the information come from and depending on how the public authority passes on the information to the public. 1. A public authority warns against the products of a certain producer because of information got by the respective producer. 2. A public authority warns the public because of its own investigations. 3. A public authority warns only certain firms – for example the operators of critical infrastructures.

However, warnings can in each case cause serious (legal) problems: A warning can cause a company – whose products were warned against – to suffer a pecuniary loss whereas it makes no difference if the warning is right or wrong. Warnings can also turn out to be wrong and companies as well as private persons who complied with the warning can sustain damage. If only certain companies are warned the companies who were not warned can feel to be discriminated against.

These examples illustrate that warnings can comprise a lot of legal problems: Warnings about security gaps can restrict the constitutional rights of the company that is warned against. If only certain firms are warned this can be an unequal treatment that is not compatible with their constitutional rights. Furthermore, the question arises which public authorities or governmental agencies are allowed to issue warnings. If financial damages are caused the question of the liability of public authorities comes to the fore.

Rights of freedom

IT-warnings do not differ from warnings about wine polluted with glycol or about spoilt meat. The Bundesverfassungsgericht (German Federal Constitutional Court) judges such product warnings at the criterion of the freedom of occupation as laid down in Art. 12 (1) Basic Law. In Switzerland, Art. 27 of the Federal Constitution is addressed. Comparable rules can be found in most European legal systems.

Without a doubt the freedom of occupation covers the production of IT-products as well as the sale of IT-products. But problems are caused by the question if a mere warning or a detached hint can be a restriction of constitutional rights. Assuming that a constitutional right is only restricted by a governmental measure if this measure is final, immediate, formal and binding, the question will be answered in the negative: A mere warning does not comply with these requirements.

However, legal practice and legal writers concede that fundamental rights can not only be threatened by purposeful measures but also by any kind of governmental measure: Modern theory of constitutional rights admits

that any kind of public action which prevents an individual from doing something which is completely or partly protected, by a constitutional right can turn out to be a restriction of this constitutional right.

In the basic constellation, a public authority issues the warning itself. This can usually be seen as a restriction. By contrast, there is no restriction of a fundamental right where a public authority only passes on information about security gaps which it has received from the producer of the ascertained product.

However, problems can arise if security reports which have been written by third parties are passed on since this could be interpreted as the report is approved by the respective public authority. Similar problems may arise when a private CERT is sponsored by public authorities. When it comes down to it, it is likely that a restriction of a fundamental right could be seen in both situations. Public authorities cannot avoid their obligation to respect the individual constitutional rights, even if they use private parties to fulfil their duties.

However, the restriction of a fundamental right does not necessarily violate the respective right. A violation is only given if the restriction is not justified. In this context it has to be checked, inter alia, if there are means that are similarly effective but less burdensome for the individual. For example, it will usually not be necessary to advise the user against a certain product if the security gap can also be closed by deactivating certain functions.

Finally, the German Federal Constitutional Court has established certain criteria warnings have to comply with in order to be appropriate and thereby constitutionally justified: Warnings by public authorities always have to be neutral and extensive. That means, inter alia that the public authority has to abstain from any one-sided warning. Furthermore the public authority has to disclose any uncertainty.

For example, if the public authorities suggest not using the products of a certain producer because they were generally insecure, this advice might not be justifiable by the abovementioned criteria. By contrast, the advice that in certain areas of high security just products that comply with a particular standard should be used and are not offered by a particular producer can fulfil the legal requirements.

Principle of non-discrimination

Art. 3 Basic Law specifically prohibits treating equal things in an unequal way without any justification as well as it prohibits treating unequal things in an equal way without justification.

Comparable regulations are to be found in Art. 8 and 9 of the Swiss Federal Constitution.

As the principle that all people are equal and the principle that the state may not act arbitrarily are part of the common theory of state and law in Europe, comparable regulations should exist in other European legal systems as well.

However, it must be emphasised that an unequal treatment is not generally forbidden. It only violates the principle of non-discrimination if there is no justification for the unequal treatment. First of all, there must be a legitimate aim of differentiation. E.g. this might be “the protection of critical infrastructures “ versus “the protection of infrastructures” is one important public task. In contrast to this, it can never be a legitimate aim to favour a national market leader in a European environment. Furthermore, the criterion of differentiation has to comply with the respective constitutional rights. For example, there will be generally no good reason to inform only large companies about security lacks, but not medium- or small-sized companies. However, it might be legitimate to inform only companies which deal with critical infrastructures because of their specific importance for the public good. Finally, the unequal treatment has to be proportional. For example, it might be less invasive to make a security check of the employees of interested companies if confidential information are passed than warn only certain companies. In each case it is necessary to check if the disadvantages of a public announcement might justify the unequal treatment. The harder those potential consequences would be for the companies which were not warned, the harder it is to justify the unequal treatment.

Special problems arise, if the producers of IT products do only cooperate with public authorities under the condition that only a few chosen addressees are informed about security lacks. In principle public authorities also have to obey constitutional rights when they cooperate with private entities. Consequently, it must be thoroughly checked if such a request for an unequal treatment meets the constitutional requirements.

Tasks and competences of public authorities

Another relevant question is which authority is empowered to issue warnings concerning IT problems. This is a problem because executive, legislative and judicial powers are vertically and horizontally separated. With regard to such separation the administration is only able to act within the legal framework. This means that there must be legal provision empowering the authority with regard to the specific measure. If individual fundamental rights such as the freedom of occupation are affected by the security warning, the existence of such

a provision becomes crucial. It is not sufficient that the tasks of the public authority as such may include warnings about security gaps. Furthermore, the authority requires an explicit competence for restricting constitutional rights. In practice, this problem becomes obvious by taking a look on the existing legislation related to IT security: The relevant law often broadly describes the tasks of a public on the hand and contains a catalogue with specific competences on the other.

Only if IT warnings are subject of both parts of the relevant law, the authority may legally issue warnings which might affect the constitutional rights of individuals.

However, the German Federal Constitutional Court is of the opinion that the German government is allowed to warn the public even if there is no explicit power. According to this legal practice, the government is allowed to spread information in order to be able to react quickly in critical situations and in order to inform the public about important topics.

Liability of the State

Typically, the question of liability of the state becomes relevant in the following two situations: If security warnings turn out to be wrong, the company whose products are affected may suffer a (huge) pecuniary loss. Even more important, the company's reputation can be seriously damaged. Furthermore, the addressee of the warning can be harmed as well, e. g. if the technical instruction to close the respective security gap was wrong. In this case the data loss might be more harmful compared to the situation if the addressee had not done anything.

In such cases, the basis of a claim in Germany is to be found in Sect. 839 (1) of the Civil Code. This provision governs the responsibility of the acting civil servant. Art. 34 Basic Law diverts corresponding claims to the state. As a consequence, the government or the respective public authority is finally liable. “Civil servant” means any person who acts on behalf of a public authority. This includes, for example, employees, granted contractors or even admin clerks. In any case, the relevant action has to be based on public law. Generally, if a public authority announces something, this condition is fulfilled: This means on the one hand, that even if a tax office would issue security warnings – which is a rather far fetched scenario –, this could cause claims based on liability of the state. On the other hand, if the manager of the IT department of a security agency has a private blog in which he warns about security gaps there is generally no connection to an official action so that a claim against the state will not be successful.

Furthermore, the state will only be liable when official duties have been neglected. However, no exhaustive catalogue of official duties exists in written German law. As a consequence, the relevant official duties have to be outlined in each particular case with regard to the duties of the individual civil servant.

If a civil servant issues security warnings, he has to check them carefully beforehand. The basis for this duty lies in the constitutional rights of the companies and individuals which are affected by those warnings while the public authorities and their employees are the addressees of these rights. Furthermore, a claim against the state requires, in principle that a monetary loss has been caused by the failure to comply with the official duties. This condition is not fulfilled if only the reputation of an IT producer is (seriously) damaged unless this damage can be measured financially.

Another condition under German law is that the civil servant must have acted at least negligently. The servant complies generally with his duties and therefore does not act negligently if his recommendations of how to act were checked up carefully beforehand. If only a very specific situation has caused problems and damage, the civil servant and consequently, the public authority will not be liable.

The standard of care is set by an experienced and dutiful ordinary civil servant and not by the individual skills of the civil servant who has issued the warning. This is based on the idea that the public authority is liable in the end and not the acting civil servant himself. As a consequence, the public authority cannot exonerate itself by the fact that the security warning was issued by a beginner of a job who has no experience and does not take into account the consequences of his recommendation or who is even unqualified for the job. In contrast, a claim will not be successful if the mistake would not have been avoidable for other security experts observing the reasonable care, too.

The Swiss law concerning the liability of the state is quite similar to the German law. The basic principles are to be found in the Law of Responsibility (Verantwortlichkeitsgesetz). As in German law the state is liable for the damage which has been caused by one of his civil servants. However, in contrast to German law it is not necessary that the civil servant is to be blamed individually.

As the principle of liability of the state also belongs to the basics of the European understanding of law, it is therefore found in other legal systems within Europe.

Strategy of Critical Infrastructure Protection.

How safety, severe crises management and critical infrastructure protection interrelate.

Dana Procházková

CITYPLAN Ltd. Praha,
Czech Republic
CIIRCO Project

prochazkovad@polac.cz

INTRODUCTION

The security situation in the world, in countries, and in organisations has been changing with the time, and therefore, a safety culture must be built systematically that takes into account existing knowledge and experience.

The safety culture promotion into practice requires both the management and broad participation of all staff of public administration / organisations with emphasising that the top management has biggest responsibility. It understandably leads to the assignment of higher priority to planning and safety management as well as to higher demands to the understanding level of all participants, see e.g. [1-16].

A basic function of each state is to ensure the Human Society Sustainable Development. Therefore, the present main aim is to build the Safe Space for the 21st century. The tool is the safety management the process model of which is in Figure 1.

Figure 1: The sustainable development process model (base and pillars).

SAFETY MANAGEMENT

The safety management is strategic proactive management based on risk analysis. It ensures basic prevention against disasters of all kinds; i.e. natural, technological, environmental, social and those caused by interdependencies in critical infrastructure, including terrorist attacks and existing interactions between the human system and its vicinity.

Disasters are divided into:

- *natural disasters:* landslides, hot summer days, drought, dam rupture, floods, tsunamis, earthquakes, volcanic eruptions, slope sliding, rock sliding, wild fires, winds, tornadoes, hurricanes, extreme rainy or snowfall precipitations, or gas releases from the earth's interior,
- *technological disasters:* incidents and accidents in chemical and other industry, induced earthquakes (rock-bursts, shocks induced by dams, by injection of fluids into the earth's interior, pumping liquids from the earth's interior, artificial explosions), accidents when transporting and stocking the chemical materials, traffic accidents, radiation accidents and big environment pollutions,
- *disasters directly influencing the balance of human population and society, environment and critical infrastructure:*
  - *defects in the environment:* collective pestilences of field culture, collective pestilences of animals,
  - *defects in human population:* epidemic and pandemic, human faults,
  - *defects in human society:* the defects in public security and public order, abasement, discrimination, criminality, terrorism, wars, armed conflicts,
  - *defects in critical infrastructure:* the defects in economic sphere, territorial, organisational and social infrastructures, in information technologies, communication, energy sector and banking.

The groundwork for safety management is near the same as for the risk management plus precaution principle.

Safety management aim is to enhance safety and not only to minimise risks as in the risk management. In the frame-work of this tool, there are performed measures in the land-use planning, designing, building and operation of objects and infrastructures. The measu-res are technical, legal, organisational, economical etc. The most effective are

technical measures in the land-use planning, building and operation. For this, it is necessary:

1. To consider all disasters that can occur in the area under account.
2. At possible disasters, to take into account hazards of the 10th, 100th and may be more yr disasters.
3. To carry out measures for vulnerability (and risks) reduction against disasters that can have unacceptable impacts on the protected interests.
4. To carry out mitigation measures against unacceptable impacts on the protected interests, the occurrence of which cannot be prevented.
5. To concentrate the attention to critical assets, critical functions and critical activities in the territory that create the base for human survive.
6. From the economical viewpoint, to implement only measures suitable for the given locality and effective not only for a short time but for a reasonable time period.

CRITICAL INFRASTRUCTURE PROTECTION

Owing to the diversity of disasters that are sources of risks, the different territory, technology and infrastructure characteristics, ***the investigated problem is complex, multidisciplinary and interdisciplinary in its nature***. It has a lot of aspects: technological, organisational, legal, financial, managerial, commanding, educational, international etc.

From the system theory, it is evident that an integral system such as the human system, including the humans, human society, property, environment, critical infrastructures and technologies (Fig. 1), is functional only if its subsystems are functional and reliable and if links and flows among them, including those cross its individual facilities and networks of subsystems, are in demand, i.e. they do not lead to wrong phenomena that can cause to happen unacceptable impacts on protected interests or cause full or partial system disintegration. Provisions of functionality of systems and subsystems of the human system are created by the historical development of human society (legislation, standards and norms of different kinds). ***Instructions, principals and rules are usually held out to subsystem elements and only in minimum to links and flows going cross the system and its subsystems.***

A general critical infrastructure definition has not been proposed yet. In concord with the professional literature, it is possible to use e.g. the definition "the critical infrastructures are physical (technological and material), cyber and organisational subsystems of the human system that are necessary for preserving the human lives, health and security, property and minimum operation of state economy and administration". I.e. ***the critical infrastructure in a country is the infrastructure that is very important for human life in the country and simultaneously is very vulnerable against expected disasters in this country***. The selection is performed by application of special mathematical methods, e.g. multi-criteria analysis methods (deciding matrix) or operational analysis methods based on searching the critical way.

The multi-criteria analysis methods mostly use the criticality matrix, i.e. the matrix comparing the infrastructure vulnerability with regard to expected disasters and the infrastructure importance for a given territory, Figure 2.

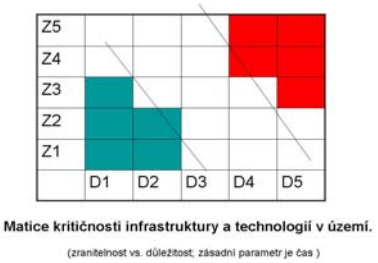


Fig. 2. Criticality matrix for infrastructures and technologies in a territory / country, i.e. the vulnerability vs. importance for infrastructure in the territory / country.

From the human safety viewpoint, it is necessary to take into account that all existing standards and norms ensure the human system safety only to a given disaster size (denoted usually as design disaster). If the disaster size or disaster impact size in a given site is higher than this limit, i.e. after extreme / beyond design (severe) disaster, extreme primary impacts and many secondary impacts will occur that are mostly just mediated by links and flows going across the human system. ***These secondary impacts are mostly induced by infrastructures and technologies.*** Figure 3 shows that at present only nuclear facilities are protected against extreme / beyond design disasters due to high effort of the IAEA and the NEA / OECD.

Lacking sufficient standards for cyber infrastructure at present, there are also a lot of problems related to the impacts of design disasters. Remote technological object control, data transfer and internet communication mean a high benefit for human society on one side, but on the other side, their incorrect functioning connected with possible operational failure or with human intent can induce or start disasters and emergencies with huge impacts. At present, the cyber infrastructure and technology protection has a special role for several reasons. The first one is the non-existence of qualified standards for reducing the cyber (IT) systems vulnerability. The second one is ease of inducing the causal chains of harmful events because they affect the control systems of many facilities and systems. The next one is that the present situation analyses show that terrorists have been prepared to perform the attacks, namely simultaneously to control systems and physical infrastructure together with disinformation of intervention forces with the aim to prolong the panic and chaos in a region.

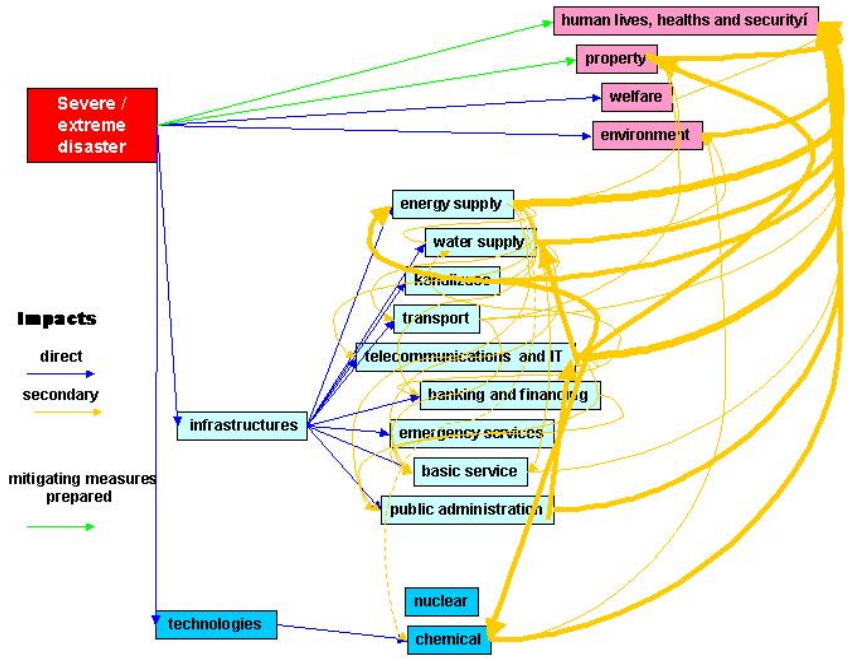


Figure 3: Extreme disaster impacts with marked infrastructure roles (yellow arrows denote secondary impacts induced by critical infrastructures).

CONCEPT OF CRITICAL INFRASTRUCTURE PROTECTION

The strategy of critical infrastructure protection consists in the following concept. The process model for critical infrastructure and technology protection is based on principals, methods and procedures of risk engineering [17]**.**

Because of limited sources, we are only capable to apply the safety management with a preliminary precaution principle in priority domains, i.e. in the cases with high vulnerability and high losses and damages. To arrange the problem in an understandable and transparent way, it is necessary to use the further ranking of primary disasters:

a) Technological accidents (internal) of critical elements, links and flows in the system. It is necessary to take into account material defects, aging, insufficient maintenance etc.

b) Errors or failures of control systems.

c) Human errors.

d) Natural disasters or technological accidents (external) of other systems.

e) Terrorist attacks, criminal acts or war.

The 17 steps of assessment process based on the all hazard approach [15] is described e.g. in [18].

STATE TOOLS

The present critical infrastructure problems deal with interdependencies across the critical infrastructure subsystems that occur at several levels, namely physical, cyber, and organisational. By other words, they are induced by financial flows, energy flows, information flows, and guided operation of management. Incorrect management interventions (namely top one) lead to incorrigible losses.

As critical infrastructure protection means to ensure the preservation of economical and social state life continuity, and to provide the response in case of a hazard or disruption of vital life conditions, services and systems the continuity of which is important for state, there are important critical infrastructure concepts and targets for its protection from the managerial view on the state level. It is necessary to divide the tasks among the public administration and private sectors and to respect the stipulated professional principals. Requirements are delimited in respect to the top management of critical infrastructure and technology owners.

The basic state tools are according to [1]**:**

- management (strategic, tactical, operational) based on qualified data, professional assessments, qualified decision-making methods, land-use planning, correct location, designing, building, operation, maintenance, reparation and renovation of buildings, technologies and infrastructures,
- citizens education, schooling and training,
- specific education of technical and management staff,
- technical standards and norms including the best practice procedures, i.e. tools for control / regulation of processes that may lead to disaster occurrences or to increase its impact,
- inspections and audits,
- executive forces for qualified response,
- systems for defeating critical situations,
- land-use, emergency, continuity, crisis and contingency planning,
- safety, continuity and crisis management; the crisis management is understood as a specific management type for crisis defeating.

Each country must build an effective Safety Management System (SMS) that is founded on safety standards being improved in time. In the SMS, the human failures must be especially considered in all aspects. Attention must also be engaged to the risk accep-

tance. The acceptable risk is a risk level that either it is not recorded by stakeholders or all self-imposed receive it. According to the management theory, the risk acceptance level might be a result of professional territory management including the communication of government / public authority with the public.

SELECTED RESULTS

The selected results of the Czech research in the framework of the Ministry for Regional Development that is responsible for renovation of territory afflicted by disaster were obtained from [19]. At territory renovation, the critical infrastructure and territory have the highest priority. At operation of critical infrastructures and technologies in a territory, a lot of factors must be considered, among basic ones operational costs, maintenance costs during the life cycle, costs for preventive maintenance and corrective measures at response and renovation. For each item considered, the criteria must be stipulated for physical condition judgement (respecting the properties and demands on physical infrastructure), capacity and service demand, and for functionality judgement. With regard to these criteria, the item condition is qualitatively assessed by a verbal scale with five degrees from "very good" to "critical / very bad". Its proposal is given in text. From the territory functionality, it is necessary to evaluate the time during which the injured infrastructure can be repaired or replaced.

Although there are legal acts that can be used for critical infrastructure protection, e.g. for the protection of supply of electricity, heat, oil, gas etc., that are supplemented by directives and regulations of Central Public Administration and Government, there is a necessity to establish an act of codifying the coordination of stipulations of individual legal rules and adjusting the important domains that are without rules. Into practice, it is necessary to include the awareness that failure of critical infrastructures and technologies must be included at each risk assessment of business / territory / state level, because the losses induced by their failure highly affect both the performance of each business and its further existence. The system tool for protection is a continuity plan. It might be compiled for all priority objects and networks of critical infrastructure and technologies. In conclusion, ***the list of 14 basic questions (checklist) that must be considered in connection with critical infrastructure and technology protection is presented:***

1. What kind of disasters can occur in a country with a given infrastructure and what impacts do they have?
2. Where can disasters occur and how can their impacts spread in a country with a given infrastructure?
3. Under what conditions can disasters occur in a country with a given infrastructure and what conditions can cause the escalation of their impacts?
4. How often can disasters occur in a country with a given infrastructure?
5. From what disaster size will disasters in a given infrastructure have unacceptable impacts that cause losses, harms and damages on protected interests (i.e. also on property and assets)?
6. What maximum sizes could disasters reach in a country with a given infrastructure?
7. What property and asset damages can be caused by maximum possible disaster on a specified credibility level in a given infrastructure and what are its impacts on a given infrastructure and in particular on property and assets?
8. What is possible to do in a given infrastructure against unacceptable disaster impacts on sections of land-use planning, design, construction and operation of civil and technological objects and infrastructure, and may be in other domains as monitoring, inspection, education etc. with the aim to prevent the occurrence of disasters or at least to prevent or to mitigate unacceptable impacts by preventive measures, preparedness, fit response to disaster and by renovation, at which there must be respected losses, prevention losses and targets of sustainable development?
9. What are necessary measures against real disasters in a given infrastructure in the technical, organisational, financial, social, legal, education and training domains?
10. What are unacceptable and residual risks (i.e. undesirable impacts with probability occurrence superior to a limit stipulated) with regard to possible disasters in a given infrastructure, when rational measures are ensured by the public administration in the technical, organisational, financial, social, legal, education and training domains?
11. How does the response to disaster perform with respect to stabilising the infrastructure state and to start reconstruction.
12. How does the renovation of infrastructure and its property and assets perform with respect to to a rational use of resources, forces and means for the prohibition of further losses, the upgrade of resistance against possible disasters and for the start of further infrastructure development with all items (environment, property and assets, infrastructure, services etc.) on which it is dependent?
13. What is the suitable form of management and of infrastructure renovation and its assets and property performance after disaster in organisation and how is it possible to realise it?
14. How is the financial / monetary reserve created for rational renovation of infrastructure and of its assets and property after disaster?

The proactive strategy of critical infrastructure protection consists in:

- ***special standards*** in land-use planning, location, designing, building, operation, maintenance, reparation, modification and renovation (it is considered that emergencies are closely connected with system existence, and therefore, the prevention must be performed, e.g. special location, designing, building and operation approaches, the safety and safety relevant systems with 4 x 100% redundancy are necessary in some cases, based on different physical principles and being specially distributed in territory etc.),
- ***continuity plans*** for critical infrastructure compilation (the aim of the plan is to ensure a limited function, to stabilize the situation and start renovation with the perspective to reach normal function in an acceptable time frame – countermeasures are e.g. beyond standard safety systems),
- ***crisis plans*** for emergency if all or a big number of security countermeasures fail through an extreme disaster size or a non-expected combination of random phenomena that escalate the disaster impacts (countermeasures are e.g. cold, warm and hot infrastructures that could ensure human survival during critical time).

REFERENCES

[1] D. Procházková: Safety and Crisis Management (in Czech). ISBN 80-86477-35-5. POLICE ISTORY, Praha 2006, 255p.

[2] Green Paper on European Programme for Critical Intrastructure Protection, Brusel 17.11.2005, COM(2005) 576.

[3] US Critical Infrastructure Conception. Washington 2001.

[4] GAO: Critical Infrastructure Protection. Dept. Of Homeland Security, Washington 2005, 78p.

[5] M. Dunn, I. Wiegert: Critical Information Infrastructure Protection. International IIP Handbook. ETH, Zuerich 2004, 405p.

[6] Office of Energy Assurance: Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities. U.S. Department of Energy, Washington 2002.

[7] Qiao Linag, Wang Xiangsui: Unrestricted Warfare (trans. Foreign Broadcast Information Service). Beijing, China, February 1999.

[8] J. Moteff, C. Copeland, J. Fischer: Critical Infrastrures: What makes an Infrastrucuture Critical Report for Congress, 2003, CRS Web, Order Code RL31556.

[9] W. Stein, B. Hammerli, H. Pohl, R. Posch (eds): Critical Infrastructure Protection – Status and Perspectives. Workshop on CIP, Frankfurt am Main, www.informatik2003.de

[10] A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. National Cooperative Highway Research Program Project 20-07/Task 151B, Science Applications International Corporation–Transportation Policy and Analysis Center, Vinna 2002.

[11] Critical Infrastructure Emergency Risk Management and Assurance.Handbook Emergency Management Australia, 2003, www.ema.gov.au

[12] Worksheets for Electric Utility Vulnerability and Risk Assessment. www.esisac.com

[13] Workshop on Critical Infrastructure Protection and Civil Emergency Planning-Dependable Structures, Cybersecurity, Commnon Standard. Zurich 2005, Centre for International Security Policy, www.eda.admin.ch

[14] Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters“, Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards“, Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters“. ASCE, Washington 2001.

[15] Guide for All-Hazard Emergency Operations Planning. State and Local Guide (SLG) 101. FEMA 1996.

[16] J. F. Gustin: Disaster & Recovery Planning: a Guide for Facility Managers. The Fairmont Press, Inc., ISBN 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn 2002, 304p.

[17] D. Procházková: Problem of Critical Infrastructure Protection (In Czech). In: Sborník MV-GŘ HZS ČR. Praha 2006, 26p.¨

[18] D. Procházková: Emergency Management Principles. In: Proceeding PIARC C18 – Risk Management for Roads. CD-ROM. Budapest 2002.

[19] D. Procházková et al.: Asset Renovation Plan in Territories Afflicted by Natural or Other Disaster Taking into Account the Providing the Critical Infrastructure Continuity. Methodological Handbook for Public Administration (In: Czech). ISBN 80-239-8285-0. CITYPLAN, spol. s r.o., Praha 2006, 40p.

Conference on Information Technology for Critical Infrastructure Protection.

The first international conference on Information Technology for Critical Infrastructure Protection on 6-7 September 2007 at the Petersberg Hotel (near Bonn, Germany) seeks to attract researchers, professionals and practitioners from all kinds of critical infrastructures.

Felix Flentge

Felix Flentge is in charge of all activities related to the EU Integrated Project IRRIIS at the Fraunhofer Institute for Intelligent Analysis and Information systems (IAIS). He leads one of the IRRIIS subprojects and several work packages and is responsible for the organisation of ITCIP 2007.

felix.flentge@iais.fraunhofer.de

Contact & Information:

The complete Call for Papers as well as additional information on the conference can be found at the conference website www.itcip.eu

Important Dates:

15 March 2007:
Full Paper Submission deadline

6-7 September 2007:
ITCP 2007 International Conference

ITCIP 2007 (Information Technology for Critical Infrastructure Protection) is the first conference of an annual series of conferences related to critical infrastructure protection. The conference is organised within the frame of the European Union funded project IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems). ITCIP 2007 especially addresses dependencies between infrastructures in critical sectors, across different sectors, and across national borders. One of the main topics is the use of Information and Communication Technology to enhance dependability, security and resilience of critical infrastructures. This involves the whole range of topics related to critical infrastructure protection from analysis, modelling and simulation up to specific technical solutions.

ITCIP 2007 is still looking for high-quality papers.

The conference will take place at the famous Petersberg Hotel (former guesthouse of the German government) and seeks to attract researchers, professionals and practitioners from all kinds of critical infrastructures with a special focus on telecommunication and electricity. The aim is to find the right balance between scientific research and practicable industrial solutions. The conference will host attractive invited talks, present high-quality, peer-reviewed papers and arrange international workshops dealing with current research questions of critical infrastructures in a complex environment. A distinguished program committee with key persons from industry and academic research has been set-up and is still looking for high-quality papers concerning:

- Analysis of critical infrastructure dependencies
- Modelling & simulation of critical infrastructures
- Information and Communication Technologies (ICT) for resilient and dependable critical infrastructures
- Tools for critical infrastructure modelling, assessment and management
- Security and safety for ICT-based critical infrastructures
- Trusted information sharing between critical infrastructure stakeholders including early warning systems
- Critical (Information) Infrastructure Protection requirements by infrastructure operators and other stakeholders, economy and society
- Risk mitigation strategies and decision support systems for critical infrastructures
- Ensuring reliable service delivery (continuity of services, business continuity)
- Threat, vulnerability and risk analysis for critical infrastructures
- High quality benchmarks scenarios with high practical relevance to compare prevention and mitigation approaches
- Scenarios and case studies concerning present and future critical infrastructures.

CI²RCO

Information Society Technologies

CI²RCO
Final Conference
ROME 7 February 2007
Holiday Inn Rome West, S.S. 1 – Via Aurelia Km 8, 400
00163 Rome, Italy

CI²RCO (Critical Information Infrastructure Research Co-ordination) is a co-ordination action co-funded by the Information Society Technologies (IST) Priority of the 6th Framework Programme by the European Commission.

The objective of the project is to create and co-ordinate a European Taskforce to

- *encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP),*
- *develop a CIIP R&D agenda, and*
- *establish a European Research Area (ERA) on CIIP.*

The main objective of the conference is to present the final results of the CI²RCO project and to foster collaborations to strengthen the European Research Area on CIIP.

To this end the conference aims at establishing a consensus on the findings of the CI²RCO project achieved during the last two years with regards to the determination of CIIP R&D priorities, likelihood of R&D success and the timeframe in which R&D activities should occur.

The conference will conclude the project and thus seeks to produce concrete consent on:

- *Which are the most urgent and significant R&D challenges regarding CIIP to be tackled at the European level?*
- *How to raise awareness on the CIIP concerns at the policy, industrial and academic level?*
- *How to promote a network of CIIP-related R&D activities and a community of experts for providing an answer to the European needs?*

The conference addresses a wide international audience composed of critical infrastructure operators and providers, CIIP policy makers, best practitioners and researchers.

For further information and registration please refer to http://www.ci2rco.org/ or contact directly:

ENEA - Centro Ricerche Casaccia
Dr. Sandro Bologna
Via Anguillarese 301
00060 S. Maria di Galeria (Roma), Italy
e-mail: bologna@casaccia.enea.it

ENEA
Italian National Agency for New Technologies, Energy and the Environment

	MORNING SESSION
8:30	**Registration**
9:00	**Opening / Welcome** Sandro Bologna, ENEA, Italy
9:15	**Key note: CIIP R&D in FP 7** Angelo Marino, European Commission
9:45	**Key note: ESRAB Report "Meeting the challenge: The European Security Research Area"** Jean-Marc Suchier, Sagem, France
10:15	**Security, dependability and trust in pervasive networks and services: Towards a roadmap 2007-2013 – Results from the SecurIST project** Mícheál Ó Foghlú, TSSG, Ireland
10:45	Coffee break
11:15	**CI²RCO: Main results of the CIIP R&D analysis** Uwe Bendisch, Fraunhofer SIT, Germany
11:45	**CI²RCO: Stakeholder CIIP R&D requirement gaps** Eric Luiijf, TNO, The Netherlands
12:15	**CI²RCO: The Critical Information Infrastructure R&D Agenda** Sandro Bologna, ENEA, Italy
12:45	**DISCUSSION**
13:00	Lunch break
	AFTERNOON SESSION
14:30	**Key note: from ENISA *(title to be fixed)*** Dr. Alain Esterle, ENISA, Greece
15:00	**CIIP in Germany –** **The perspective of the German Ministry of the Interior** Andreas Schmidt, German Ministry of the Interior, Germany
15:30	**Coordination of national and European ICT R&D programmes – Results of the CISTRANA project** Agnes Richard, PT-DLR, Germany
16:00	Coffee break
16:30	**Scenario building for Next Generation Infrastructures** Roberto Saracco and Roberto Minerva, TELECOM Italia, Italy
17:00	**Round Table and Conference Wrap Up** Moderator: Eric Luiijf, TNO, The Netherlands
17:30	End of Conference

Selected links and events

Actual upcoming CIIP conferences mainly in Europe

- Defending Against Insider Threats Best Practices For Defending Against Insider Threats to Proprietary Data For Government & Commercial Legal, Privacy, Facility, IT & Security Managers, Learn the Latest Research into Sensitive and/or Private Data Loss and Best Practices for Internal Security, February 28, 2007, NRECA Executive Conference Center Arlington, Virginia, contact via fax: 001 703 807-2728
- European Conference on Security Research SRC '07, March 26-27, 2007, Berlin, Germany http://www.src07.de/index.php?lang=en
- Large Critical Complex Infrastructures – Key Challenges and Evaluation of existing CIIP technologies, St. Augustine, Germany, April 26, 2007 http://www.irriis.eu/File.aspx?lang=2&oiid=8794&pid=644
- Peace, Stability, Security Transition & Reconstruction EU conference Executive Agenda, being held in Central London UK, on April 24th - 25th 2007
- The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, June 25 - June 28 2007 Where: Edinburgh International Conference Centre, Edinburgh, UK http://www.dsn.org
- Fourth International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) in Lucerne, Switzerland on July 12-13, 2007 www.dimva2007.org
- ITCIP 2007 (Information Technology for Critical Infrastructure Protection), 6-7 September 2007, Petersberg (near Bonn, Germany), information at: www.itcip.eu

European or large projects with articles in this issue

- IRRIIS: www.irriis.eu
- CIIRCO www.ci2rco.org
- DESEREC: www.deserec.eu
- GRID http://grid.jrc.it
- NGI www.nginfra.nl
- Safeguard www.stns.ch/Safeguard
- CA Reliance http://www.ca-reliance.org
- CRUTIAL: http://crutial.cesiricerca.it

Links related to articles in this issue

- European Homeland Assoction www.e-hsa.org
- Links related to Dependability Master and PhD http://cmuportugal.di.fc.ul.pt and http://www.icti.cmu.edu/
- Technology, Policy and Management Uni Delft http://www.tbm.tudelft.nl
- 4th EAPC/PfP Workshop on CIP and CEP 2006 pforum.isn.ethz.ch/events/index.cfm?action=detail&eventid=265
- IT Security Made in Germany http://www.itsmig.de/messekalender/suche_en.php

Various resources for IT risk, security and disaster management

- EU ICT Trust and Security Publications: http://cordis.europa.eu/ist/trust-security/publications.htm
- OECD Culture of Security for Information Systems and Networks http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
- The integrated Security Hanbook, DoD www.physicalsecurityhandbook.com