

### Focus on EU sponsored Projects:

- CRUTIAL
- CISTRANA
- CI2RCO
- SecurIST

### Infrastructure Security

Safety and security:  
two sides of the same medal

### Crisis Prevention and Planning System

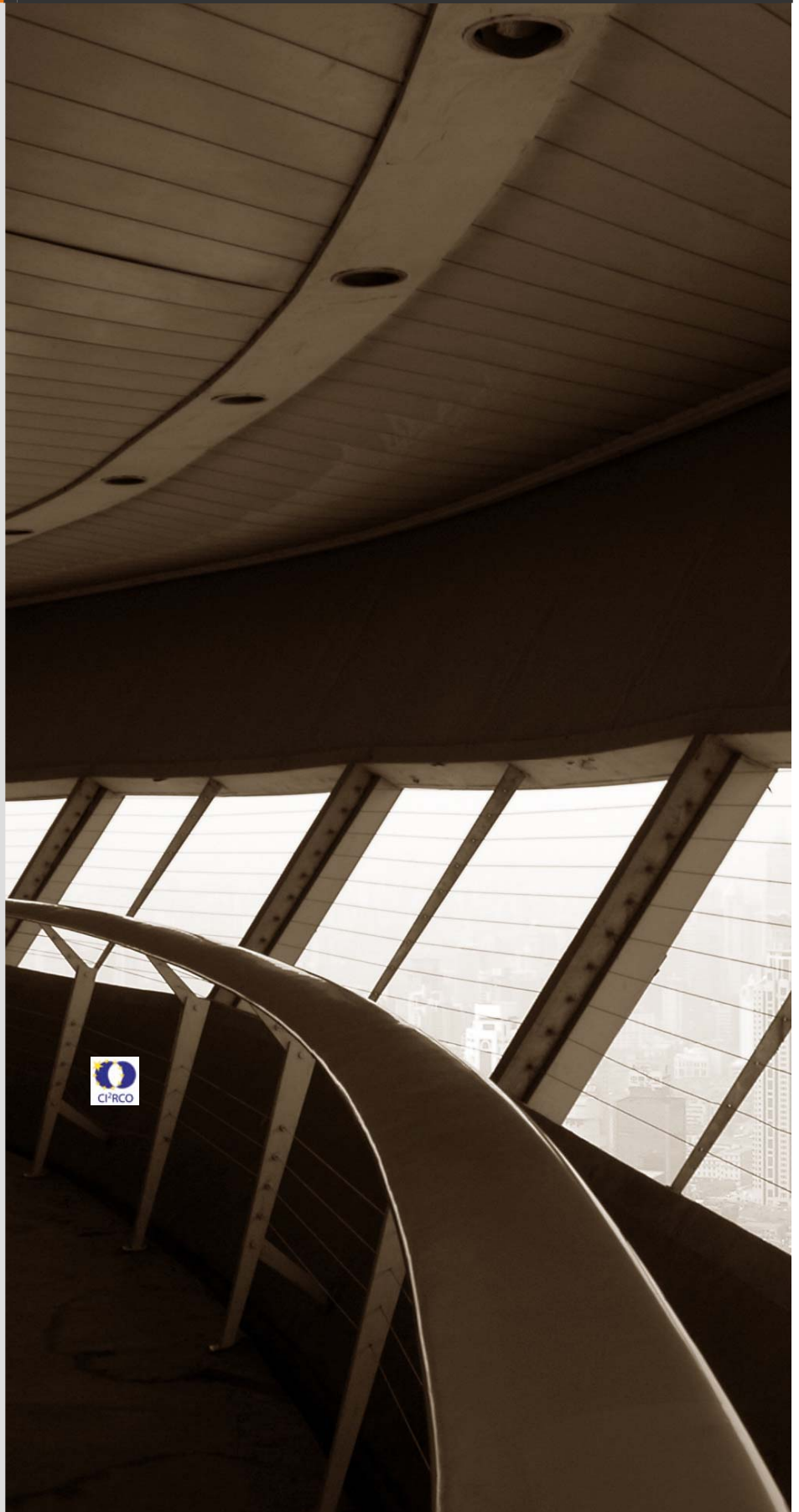
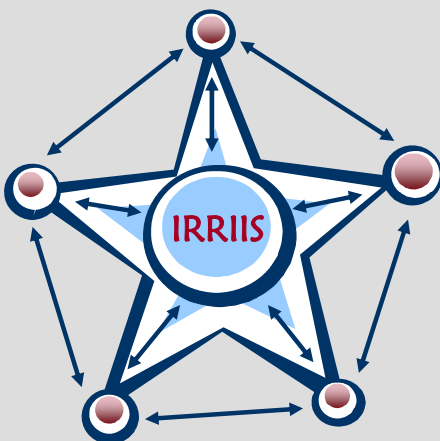
Information security,  
Internet security or  
CIIP

### CESS

### Conferences:

- CRITIS 2007
- ITCIP 2007

### Links



**> 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 IRRIS project  
The IRRIS 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](mailto:subscribe@ciip-newsletter.org)

**>Article can be submitted to be published to:**  
[submit@ciip-newsletter.org](mailto:submit@ciip-newsletter.org)

**>Questions about articles to the editors can be sent to:**  
[editor@ciip-newsletter.org](mailto:editor@ciip-newsletter.org)

**>General comments are directed to:**  
[info@ciip-newsletter.org](mailto:info@ciip-newsletter.org)

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

**The copyright stays with the editors and authors respectively, however  
people are encouraged to distribute this CIIP Newsletter**

**>Founder and Editors**

Eyal Adar CEO iTcon, [eyal@itcon-ltd.com](mailto:eyal@itcon-ltd.com)  
Bernhard M. Hämmerli, HTA, Initiator and Main Editor [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)  
Eric Luijff, TNO, [eric.luijff@tno.nl](mailto:eric.luijff@tno.nl)

**>Country specific Editors**

For Germany: Heinz Thielmann, Prof. emeritus, [heinz.thielmann@t-online.de](mailto:heinz.thielmann@t-online.de)  
For Italy: Louisa Franchina, ISCOM, [luisa.franchina@comunicazioni.it](mailto:luisa.franchina@comunicazioni.it)  
For France: Michel Riguidel, ENST, [riguidel@enst.fr](mailto:riguidel@enst.fr)  
For Spain: Javier Lopez, UMA, [jl@lcc.uma.es](mailto:jl@lcc.uma.es)  
For Finland: Hannu Kari, HUT, [kari@tcs.hut.fi](mailto:kari@tcs.hut.fi)

**> Graphics and Layout**

Florian Widmer [florian\\_widmer@gmx.net](mailto:florian_widmer@gmx.net)

**> Spelling:**

British English is used except for US contributions

# Table of Contents

## Introduction

	<b>Strong EU funded activities in C(I)IP by Bernhard M. Hämmerli</b>	<b>5</b>
--	--	----------

## European Activities

<b>EU CRUTIAL</b>	<b>CRUTIAL: Towards a Reference Critical Information Infrastructure Architecture</b> by Paulo Veríssimo	<b>6</b>
<b>EU CISTRANA</b>	<b>CISTRANA – Coordination of IST Research and National Activities</b> by Agnes Richard	<b>9</b>
<b>EU CA CI2RCO</b>	<b>Analysis of CIIP R&amp;D programmes in Europe and trends for the future</b> by Gwendal Le Grand	<b>12</b>
<b>EU SecurIST</b>	<b>SecurIST - Strategic Research Agenda</b> By James Clarke	<b>16</b>

## Country Specific Issues

	<b>This time empty</b>	
--	------------------------	--

## Methods and Models

<b>Safety and security</b>	<b>Safety and security: two sides of the same medal</b> by Odd Nordland	<b>20</b>
<b>IRRIIS: Tool Emergency Management</b>	<b>Crisis Prevention and Planning System</b> by Hermann Dellwing and Walter Schmitz	<b>23</b>

## **News and Miscellaneous**

<b>Broad IT-Security Approach</b>	<b>Information security, Internet security or critical information infrastructure protection?</b> <i>by Solange Ghernaouti-Hélie</i>	<b>27</b>
<b>CESS</b>	<b>CESS &gt;&gt;&gt; Excellence in Security</b> <i>by Reinhard Hutter</i>	<b>28</b>
<b>Critis 2007 Call for Papers</b>	<b>Critical Information Infrastructures Security</b> <i>by Javier Lopez</i>	<b>29</b>
<b>ITCIP 2007 Call for Participation</b>	<b>Conference on Information Technology for Critical Infrastructure Protection</b> <i>by Felix Flentge</i>	<b>30</b>

## **Selected Links and Events (online Version only)**

<b>Online only</b>	<b>Upcoming CIIP Conferences</b>	
<b>Online only</b>	<b>Selected Links</b> <ul style="list-style-type: none"> <li>• <b>Actual upcoming CIIP conferences in Europe</b></li> <li>• <b>European projects with articles in this issue</b></li> <li>• <b>Links related to articles in this issue</b></li> <li>• <b>Various resources for IT risk, security and disaster management</b></li> </ul>	

# Strong EU funded activities in C(I)IP.

Again, we present four EU funded projects in this issue. And new proposals can be prepared for the Security and Dependability call starting in September 07. The topic is now recognized at large as one of the essential issues in maintaining prosperity and welfare within EU.



**Bernhard M. Hämmerli**

Seconded National Expert  
Joint Research Centre Ispra, European  
Commission

Professor in Information Security  
Founder of the Executive Master Pro-  
gram IT Security, FHZ  
President ISSS  
[bmhaemmerli@hta.fhz.ch](mailto:bmhaemmerli@hta.fhz.ch)  
[bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)

## New C(I)IP= Conferences

For years the C(I)IP was fostered in the research community and now projects are running and delivering. New calls in the FP7 and the security program address the C(I)IP topic and task for proposals. One call will be opened just in the time (October 3-5, 2007) of CRITIS 2007 conference in Benalmadena in Spain. Jacques Bus from European Commission will by there give a keynote "Resilient Critical Infrastructures: a myth or a realistic target?" and also direct a panel related to C(I)IP. The call for papers for CRITIS 2007 conference is at least ten days open. If you are late write to program chair.

## About this Issue

The first section is dedicated to EU funded projects:

- CRUTIAL which is defining a reference architecture for Critical Information Infrastructure (CII) including embedded and SCADA systems
- CA CISTRANA which elaborated a portal for insights into national policies and research programs on ICT
- CA CI2RCO which analyses CII project in Europe and defines a set of research priorities
- CA SecurIST which defines a strategic research agenda in the security and dependability field

The second section on methods and models contains two articles:

- A contribution defining and comparing security and safety including the associated standards
- An introduction in the knowledge based emergency management tool CRIPS which is developed under the IRRIS umbrella. Main features are:
  - Assessment of current situation
  - Support of decision making in emergency management
  - Warning and alerting including the broadcasting of decisions.

## About the Link Collection

The complete link collection of all ECN issues can be found on [www.irriis.eu](http://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](http://www.irriis.eu).

ECN is published on websites, [www.irriis.eu](http://www.irriis.eu) and the [www.ci2rco.org](http://www.ci2rco.org). Furthermore we hope, that all ECN mirror sites will be maintained in future.

Enjoy reading the ECN!

# CRUTIAL: Towards a Reference Critical Information Infrastructure Architecture

**Computerised and interconnected critical infrastructures have generated a hard and fascinating problem for computer science and control engineering: achieving resilience of critical information infrastructures.**



**Paulo Veríssimo**

Professor of the Department of Informatics of the University of Lisboa Faculty of Sciences (FCUL), Director of LASIGE, member of the European Security & Dependability Advisory Board and associate editor of the IEEE Transactions on Dependable and Secure Computing.  
 Email: [pjv@di.fc.ul.pt](mailto:pjv@di.fc.ul.pt);  
 Web: <http://www.di.fc.ul.pt/~pjv/>  
 Address: Faculdade de Ciências da Universidade de Lisboa, Campo Grande, 1749-016 Lisboa, PORTUGAL

Achieving resilience for CII is concerned with ensuring acceptable levels of service and, in last resort, the integrity of systems themselves, when faced with threats of several kinds. In this article we are concerned with threats against computers and control computers, not with the physical infrastructures themselves. These threats range from accidental events like natural faults or wrong manoeuvres, to attacks by hackers or terrorists. The problem affects systems with great socio-economic value, such as utility systems like electrical, gas or water, or telecommunication systems and computer networks like the Internet. In consequence, the high degree of interconnection is causing great concern, given the level of exposure of very high value systems and components to attacks that can be perpetrated in an anonymous and remote way.

**Threats range from accidental events or manoeuvres, to hacker or terrorist attacks.**

## **CRUTIAL, CRITICAL UTILITY INFRASTRUCTURAL RESILIENCE**

These are the challenges to be met by CRUTIAL, CRITICAL UTILITY INFRASTRUCTURAL RESILIENCE, a European FP6-IST research project (<http://crutial.cesiricerca.it/>), through a multinational team that strikes a balance between academia and industry: CESI (IT), CNIT (IT), U. Lisboa (PT), ISTI (IT), K.U. Leuven (BE), LAAS-CNRS (FR). CRUTIAL's innovative approach resides in modelling interdependent infrastructures taking into account the multiple dimensions of interdependen-

cies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks. In short, the objectives of the project are: investigation of models and architectures that cope with openness, heterogeneity and evolvability endured

by electrical utilities infrastructures; analysis of critical scenarios in which faults in

the information infrastructure provoke serious impacts on the controlled electric power infrastructure; investigation of distributed architectures enabling dependable control and management of the power grid. In this note we shortly discuss the last points in architectural work.

## **CURRENT CII ARE HYBRID STRUCTURES**

Although there is an increase in the concern for using security best practices in these systems, we believe that the problem is not completely understood, and cannot be solved with classical methods. Its complexity is mainly due to the hybrid composition of those infrastructures: the operational network, called generically SCADA (Supervisory Control and Data Acquisition), composed of the computer systems that control the physical processes; the corporate intranet, where usual departmental services (e.g., web, email, databases) and clients reside; and the Internet, through which intranet users get to other intranets and/or the outside world, but

to which, and often unwittingly, the SCADA network is sometimes connected to.

### Computer Interconnection: the core of the problem

The problem of critical information infrastructure insecurity is mostly created by the informatics nature of many current infrastructures, and by the generic and non-structured network interconnection of CIIs, which brings several facets of exposure, from internal unprotected wire line or wireless links, to interconnections of SCADA and corporate intranets to the Internet and PSTN. This situation is conspicuous in several of the attacks reported against CIIs. For instance, the attack of the Slammer worm against the Davis-Besse nuclear power plant (US) was due both to the combination of computers with non-structured network interconnections, and to a lack of protection. Although the network was protected by a firewall, the worm entered through a contractor's

computer connected to the CII using a telephone line. If nothing fundamentally changes, we should anticipate failure perspectives go-

ing from unavailability of services supposed to operate 24X7, to physical damage to infrastructures, and corresponding collateral effects on society. In some companies there is a (healthy) reluctance against interconnecting SCADA networks and the corporate network or the Internet. Nevertheless, in practice this interconnection is a reality in many companies all over the world, and will in time become a necessity to the whole CI business segment. Besides CII feature a lot of legacy subsystems and non-computer-standard components (controllers, sensors, actuators, etc.), from where security concerns are largely absent. On the other hand, conventional security and protection techniques, when directly applied to CII controlling devices, sometimes stand in

the way of their effective operation. These facts are research challenges that we are interested to tackle in our project.

### CIIs are large and complex distributed systems

The computer-related operation of a critical utility infrastructure is a distributed systems problem including interconnected SCADA/embedded networks, corporate intranets, and Internet/PSTN (Public Switched Telephone Network) access subsystems. This distributed systems problem is hard, since it simultaneously includes facets of real-time, fault tolerance, and security.

Whilst it seems non-controversial that such a status quo brings a certain level of threat, we don't know any work that has tried to equate the problem by defining a reference model of a critical information infrastructure distributed systems architecture, providing the necessary global resilience against abnormal situations. What can be done at architectural level to achieve resilient operation?

Our point is that interference and threats start at

the level of the macroscopic information flows between these subsystems, and can in consequence be stopped there. This should not prevent the study of techniques at the controller level, which are also pursued in the project. Our approach is equated along three main axes that we explain next.

### Classical security and/or safety techniques not sufficient

There is a recent and positive trend to make SCADA systems and CIIs at large more secure, relying on technologies such as intrusion prevention and detection and ad-hoc recovery or ultimately disconnection. However, classic engineering remedies place real-time and embedded (RTE) systems at most at the current level of commercial systems' security and dependability. Both are

known to be insufficient: systems constantly suffer attacks, intrusions, some of them massive (worms); most defences are dedicated to generic non-targeted attacks; attacks degrade business but only do virtual damage, unlike RTE systems where there is a risk of great social impact and even physical damage. On the other hand, some current IT security techniques can negatively affect RTE system operation, e.g. on. availability and timeliness. For example, if security is based on disconnection, on significant performance degradation, or even defensive restrictions, the capability of actuation or monitoring of the infrastructure may be severely impaired.

### Effective solutions lie on automatic control of information flows

Any solution, to be effective, has to involve automatic control of macroscopic command and information flows, occurring essentially between the physical or virtual LANs composing the critical information infrastructure architecture, with the purpose of securing appropriate system-level properties. We are talking about an architectural model, a set of architectural devices, and key algorithms, capable of achieving the above-mentioned control of the command and information flow, at organisation-level. The devices and algorithms should be capable of securing a set of system-level properties characterising whatever is meant by correct and resilient behaviour.

### Reference CII architecture to represent hybrid structure and risk level

We lack reference architecture of "modern critical information infrastructure" considering different interconnection realms and different kinds of risk, throughout the physical and the information subsystems of a CII. We must consider the physical or virtual LANs composing the operational SCADA/embedded networks, the cor-

**Failure perspectives go from unavailability to physical damage to infrastructures.**

porate intranets, and the Internet/PSTN access networks, as different first order citizens of the architecture. Likewise, the notion that risk factors may be varied and difficult to accurately perceive, brings the need to reconcile uncertainty with predictability in architecture and algorithmic, in order to achieve resilience.

**CRUTIAL Architecture**

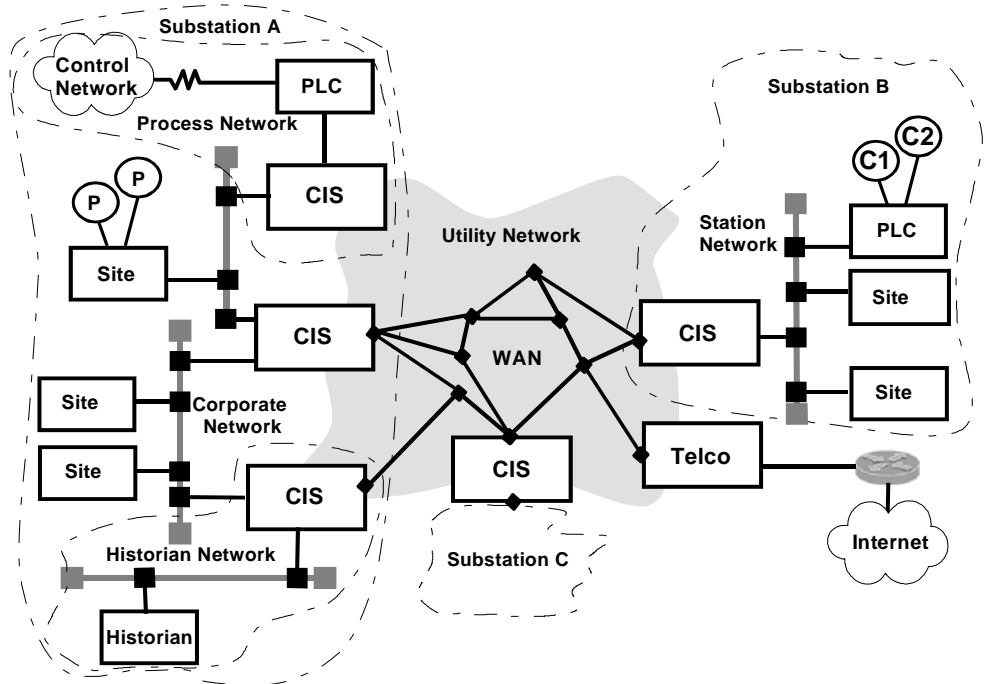
The CRUTIAL architecture embodies a few key concepts helping to meet the objectives above. Architectural configurations featuring trusted components in key places a priori induce prevention of some faults, and of certain attack and vulnerability combinations. Helped by middleware devices that achieve runtime automatic tolerance of remaining faults and intrusions, trusted services end up being supplied out of non-trustworthy components. Intrusion tolerance mechanisms are selectively used in the CRUTIAL architecture, to build layers of progressively more trusted components and middleware subsystems, with baseline un-trusted components (nodes, networks). Since faults keep occurring and systems should work unattended, proactive-resilience achieves exhaustion-safety, ensuring perpetual, non-stop operation despite the continuous production of faults and intrusions. Since assumptions are not perfect but system behaviour is nevertheless critical, trustworthiness monitoring mechanisms detect situations not predicted, and adaptation mechanisms help the system survive those situations. Organisation-level security policies and access control models (OrBAC) secure information flows with different criticality within/in/out of a CII. These basic services support application-related electricity services in a resilient manner.

**Main Architectural devices**

We view the system as WAN-of-LANs: there is a global interconnection network, the WAN, switching packets through generic devices that we call CRUTIAL Information Switches (CIS) which are attachment points for the several LANs of the infrastructure. More

properties.

CIS in a simplistic way could be seen as sophisticated circuit or application level firewalls combined with equally sophisticated intrusion detectors, connected by distributed protocols. This set of servers must be intrusion-tolerant (i.e., must



than one LAN can be connected by the same CIS. The WAN is a logical entity operated by the CII operator companies, which may or may not use parts of public network as physical support. All traffic originates from and goes to a LAN. As example LANs, the reader can envision: the administrative clients and the servers LANs; the operational (SCADA) clients and servers LANs; the engineering clients and servers LANs; the PSTN modem access LANs; the Internet and extranet access LANs, etc. CRUTIAL Information Switches collectively act as a set of servers providing distributed services relevant to solving our problem: achieving control of the command and information flow, and securing a set of necessary system-level

tolerate intrusions), prevent resource exhaustion providing perpetual operation, and be resilient against assumption coverage uncertainty, providing survivability. The services implemented on the servers must also secure the desired properties of flow control, in the presence of malicious traffic and commands, and in consequence be themselves intrusion-tolerant. Since CIS are essentially inserted at LAN edges, this architecture preserves legacy systems inside the latter, as well as the legacy protocols involved in communication within a CII. CRUTIAL intrusion-tolerant node architecting principles are also applicable on a need basis to harden individual control computers.

See more on CRUTIAL at <http://crutial.cesiricerca.it/>



# CISTRANA – Coordination of IST Research and National Activities.

**CISTRANA, a co-ordination action project supported by the EC, analyzes the information and communication technologies landscape to identify fields where strategic, programme-level coordination among EU countries offers significant opportunities**



## CISTRANA Consortium

German Aerospace Agency (DLR)  
E-mail: [cistrana@dlr.de](mailto:cistrana@dlr.de)

Association Nationale de la Recherche  
Technique (ANRT)

Finnish Funding Agency for Technology  
and Innovation (TEKES)

Council for the Central Laboratory of the  
Research Councils (CCLRC)

National Office for Research and Technol-  
ogy (NKTH)

How can Europe overcome the fragmentation of its research and development landscape? What are the common technological/societal challenges faced by European countries? In which of these fields is trans-national R&D cooperation in information and communication technologies (ICT) essential to achieve the critical mass needed for a competitive European ICT industry? What are the

**What are the common technological / societal challenges faced by European countries?**

underlying needs/rationales in these fields for trans-national R&D cooperation? How can actors cooperate to mitigate risks and complement each other's knowledge and resources? What mechanisms are needed to facilitate coherence among national initiatives and deepen strategic co-operation among policy makers and key stakeholders throughout the EU?

It is precisely these types of questions that prompted the concept of CISTRANA in the beginning of the ERA coordination process. CISTRANA is a coordination action project launched under the IST programme in 2004 with the cooperation of five partners and a Steering Committee of 33 national representatives of Member and Associated States.

## Surveying the European R&D Landscape

As the majority of public R&D funding today is allocated from national sources, the first fundamental challenge CISTRANA addressed was the lack of easy access to information about national

R&D policies, programmes, actors and activities. CISTRANA performed an extensive survey in 33 European Members and Associated States to build the ICT R&D portal

(<http://www.portal.cistrana.org>). The portal helps to overcome barriers in accessing information and provides a comparable overview of the ICT R&D landscape in Europe – a valuable starting point when exploring the potential for complementary actions and initiatives.

## Analysis of National Policies and Programmes

With this central information source established, CISTRANA proceeded to analyze national policies and programmes to pinpoint ICT research topics and strategic themes where co-operation is essential. There already exist today a number of frameworks for trans-national R&D cooperation – such as the EU Framework Programmes, EUREKA for industrial research, and the extensive set of bi- and trilateral research agreements – which have already contributed to building a significant European R&D ecosystem. The European Technology Platforms' involvement of industry in developing strategic research agendas has also contributed to building consensus on long term visions, as did the preparation of the ambient assisted living and the joint technology initiatives.

**CISTRANA Workshop Series**

In addition, CISTRANA organized a series of workshops with programme managers around the EU to gain a better understanding of various national policies and

**What are the underlying needs / rationales for trans-national R&D cooperation in ICT?**

programmes, examine best practices in design, implementation and impact assessment of national and trans-national programmes, as well as on the use of portals and ICT taxonomies to share knowledge and information about national ICT R&D. (Reports on the discussions and findings of these workshops are available on the project website)

**Building the European Research Area in Information and Communication Technologies**

However, there is certainly scope for further strategic collaboration. CISTRANA's analysis has identified focus areas as well as gaps. Discussions with ICT directors throughout Europe have validated needs to complement national capabilities and resources, and have identified a number of ICT fields as candidates for trans-national research cooperation, including fields such as civilian security, language technologies and e-health, among many others.

The 2006 IST Conference has revealed strong common interest among researchers, industrial actors and government representatives in deepening strategic cooperation in these fields. Therefore it is important to capitalize on this momentum and the knowledge accumulated in the ERA process, and to continue to pursue those fields that offer fertile grounds – both in terms of research and economic impact – for deepening cooperation.

Faced with globalisation and increased competition from emerging markets, few EU countries or organisations can now afford the cost of building the know-how and skills to master increasingly complex technologies. Trans-national research

cooperation based on mutual, long-term goals can therefore foster the pan-European industry/academic partnerships needed to integrate ICT goods and services, and to develop the EU and international standards

needed for global markets. The ERA coordination process will continue to contribute to the EU's drive towards the 2010 target of being the most competitive knowledge-driven society in the world.

**CISTRANA publications**

- European ICT R&D Landscape - Report on National Priorities and Programmes
- Consolidated Impact Assessment Reports on IST ERA-NETs
- Workshop Report Series
  - National Policy Priorities and RTD Programmes in the Field of ICT
  - Programme Impact Assessment in National IST Initiatives
  - Best Practice in Multi-national Programme Collaboration
  - Portals for Information Dissemination and Taxonomies for Classification
  - Design of National IST Programmes in the Context of ERA Coordination
- Concept for Impact Assessment on IST ERA Projects
- IST ERA Taxonomy

**Further information:**

CISTRANA website – project information, workshop reports and analyses:

[www.cistrana.org](http://www.cistrana.org)

ICT R&D portal:

[www.portal.cistrana.org](http://www.portal.cistrana.org)

In 2007, CISTRANA will continue engaging stakeholders through a series of topical seminars. These will be of two kinds:

**Addressing specific ICT topics:**

Such seminars will be structured to bring together stakeholders in selected fields, including policy makers, programme managers, researchers and industry.

The first section will discuss the landscape with researchers and industry representatives to confirm key challenges that should be addressed at a trans-national level.

This will be complemented with a round table discussion with key public sector stakeholders interested in pursuing programme-based cooperation.

The first such seminar shall address ICT security.

**Joint calls in the ERA NET scheme:**

The Sixth Framework Programme launched a number of ERA NET initiatives aiming to facilitate trans-national research cooperation around the EU, many of which have led to joint calls between national funding programmes.

The seminar will bring together a small group of experts to take stock of these initiatives.

The event will offer the opportunity to discuss experience with joint calls and exchange best practice on issues such as planning and implementation procedures, earmarking budgets, IPR regulations, efficient administration / slim bureaucracy, common evaluation schemes, etc.

*Keep an eye out for upcoming topical seminar announcements on the CISTRANA website: [www.cistrana.org](http://www.cistrana.org).*

**The CISTRANA ICT Research Portal**

The CISTRANA ICT Research Portal has been designed to help overcome the barriers in accessing information about national research and development activities in the field of information and communications technologies.

The portal provides a view of the landscape of ICT research in Europe, allowing quick and easily understandable access to and comparison of information from different countries about their research policies, programmes and other activities. It complements the other activities of the CISTRANA project by tackling the problem that ICT research information at national level is often difficult to find. The information is provided by a network of National Support Organisations in each participating country.

The portal will be of interest to policy makers, programme managers, researchers and industrial actors.

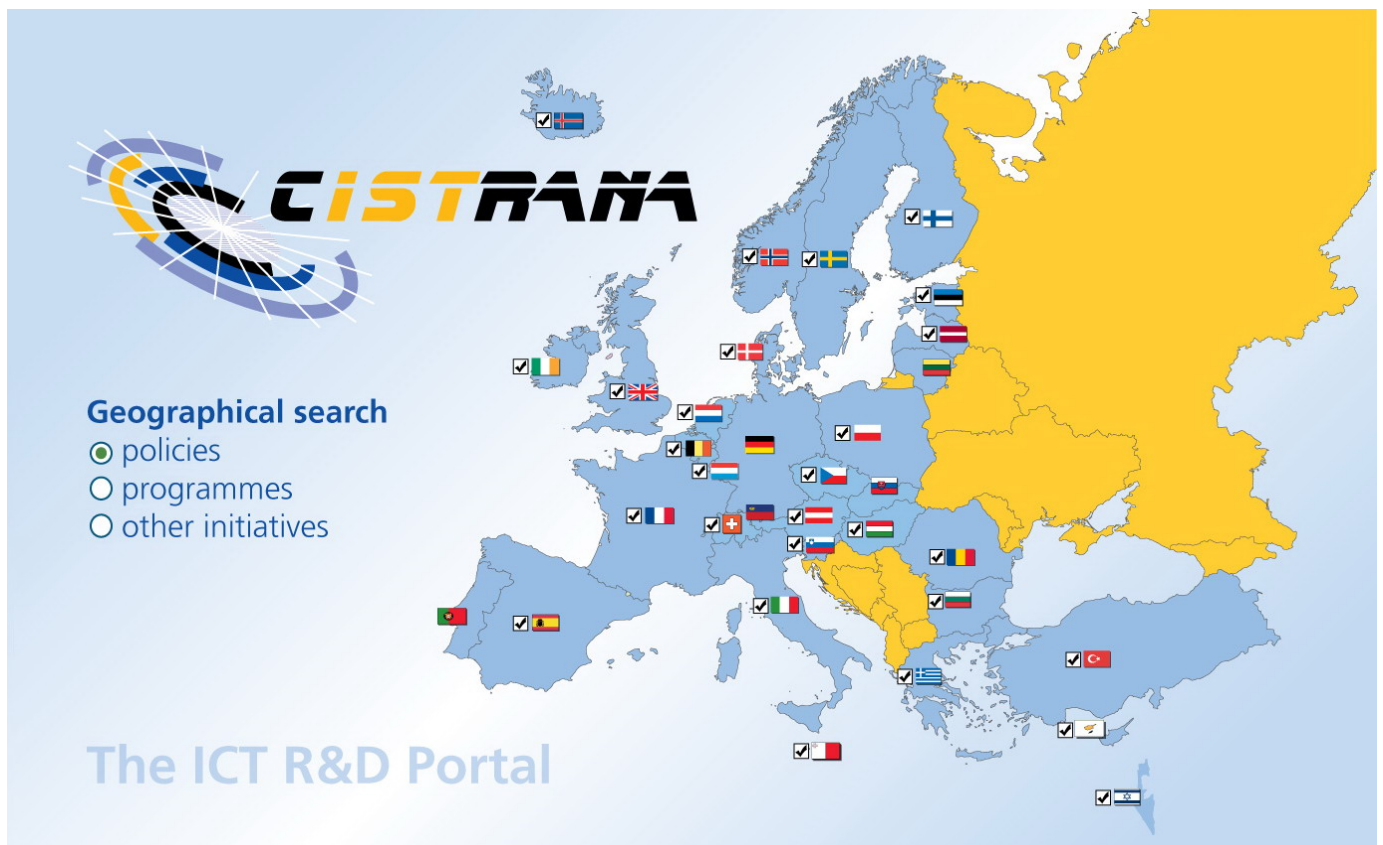
Are you looking for information about national R&D programmes in information and communication technology in Europe? Visit the CISTRANA ICT Research Portal to find the answers to questions like these:

- Which organisations are involved in national R&D policy-making and funding programmes in a particular country?
- Which R&D challenges are European countries addressing in transnational cooperation?
- Where in Europe do you find significant research in ICT security?

- Which are the most recent national research programmes launched in ICT?
- What are the national strategic focus areas for ICT policy in Northern Europe?
- How much R&D funding is available through programmes in your competitor's country?

Visit the ICT R&D Portal at:

<http://www.portal.cistrana.org>



# Analysis of CIIP R&D programmes in Europe and trends for the future.

**We investigate research efforts in the Critical Information Infrastructure Protection area, based on results collected in 2006 within the CI2RCO project. We present several classification methods and then we assess and analyse identified projects. Finally, we conclude by proposing a set of priorities for future CIIP research.**



**Dr. Gwendal Le Grand**

Associate Professor,  
Ecole Nationale Supérieure des Télécommunications, Paris, France,

[gwendal.legrand@enst.fr](mailto:gwendal.legrand@enst.fr)

This article presents work performed within the IST FP6 CI2RCO (<http://www.ci2rco.org>) project. We focus on the analysis of the European CIIP Research Area. For this analysis, in 2006, we have collected data not only from the European Union, but also from major initiatives in the United States, Canada, and Australia. The classification and analysis of projects is therefore done at a broader scale in order to assess European research and its positioning vis-à-vis international efforts. We propose several classification methods to situate European CIIP research in an international context. Finally, we propose a set of priorities in the field of CIIP.

## POSSIBLE CLASSIFICATION METHODS

In order to identify the future needs in the CIIP research area, CIIP projects and initiatives should be classified. Several classifications for CIP are available in the literature [REF, ACIP], or have been proposed in CI2RCO. For instance,

- based on the CI's hierarchy, as shown in Figure 1. (the top level deals with global / general CIP aspects; the Compound of Critical infrastructures represents (in-ter)dependencies between CI's; Critical Infrastructure represents a specific sector or a type of critical infrastructure; Critical System deals with research focused at the system/technical level)

- based on protection method type (High-Level models, Practical models, Tools, Organisational)
- based on the phase of the incident response cycle (Pro-action, Prevention, Preparation, Detection, Early warning, Incident management, Recovery, Post mortem analysis)
- based on the model emphasis (phase in the life-cycle of the CI -- requirement analysis, design, implementation, operation-- Risk typology, Faults, Failures, Incidents)
- based on the maturity status of the research effort (the status of the research is important in order to determine the readiness of the model, and the ability to perform significant improvement in the CI's) and
- based on the phase in the research cycle (Figure 2): a normal research cycle goes through several steps including sector analysis, intra- and inter-dependency analysis, risk analysis, system analysis, and tool design. It also includes a feedback loop to improve existing tools. Note that this research cycle is designed to be clearly oriented towards modeling, simulation and concrete technical solutions. However, policy analysis, organisational measures, and governance, are considered to be included within sector and intra- and inter-dependency analysis.

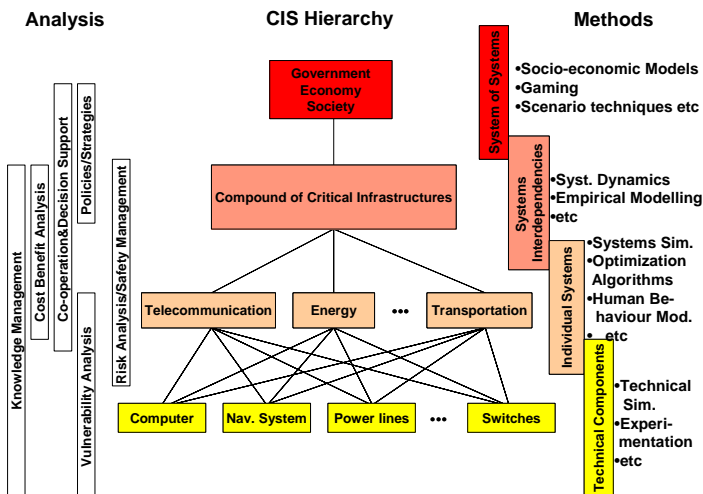


Figure 1: Hierarchy of infrastructures

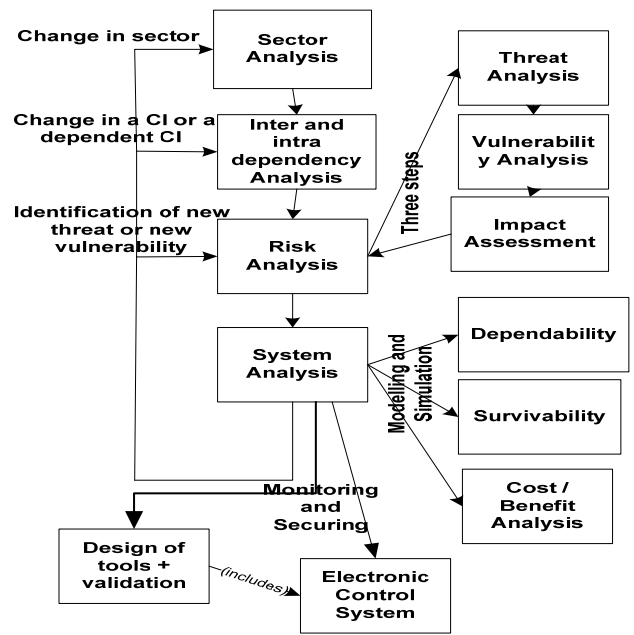


Figure 2. Classification based on research cycle

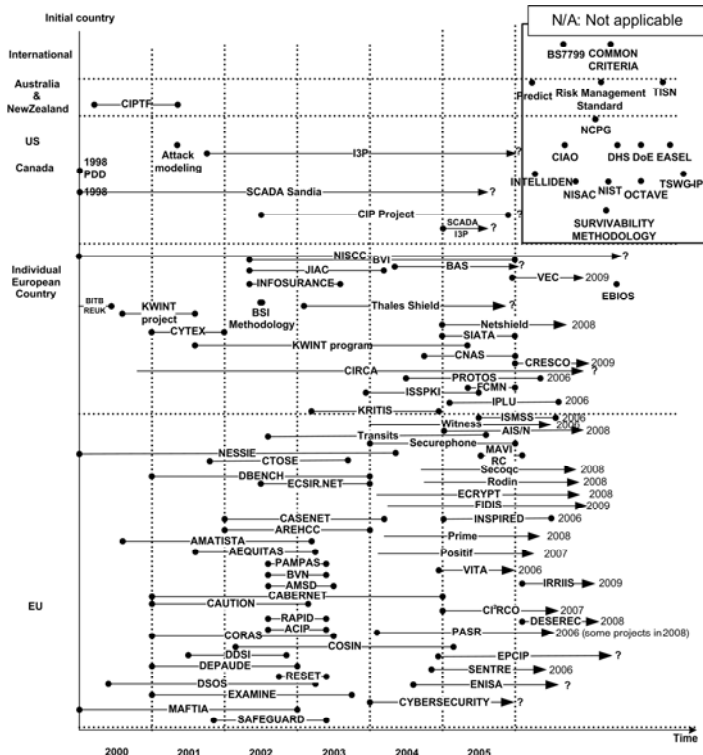


Figure 3. Chronology of CIIP projects

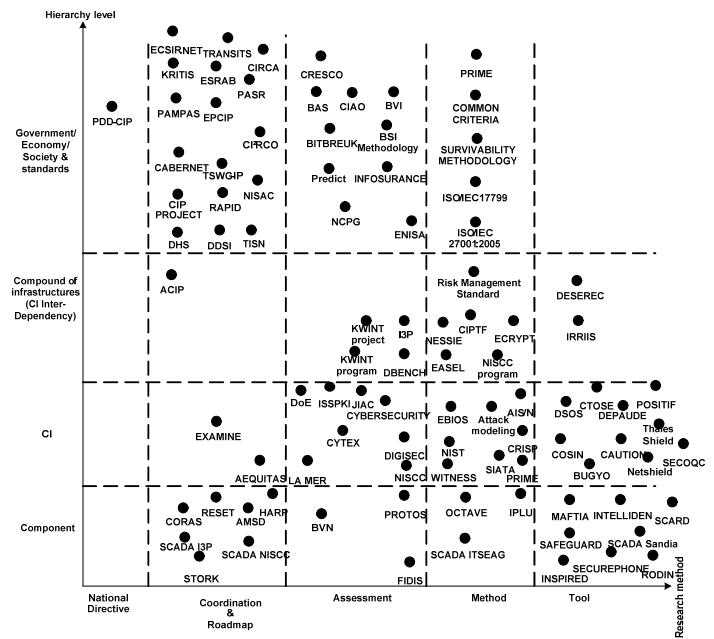


Figure 4: Research method versus hierarchy level

**SCOPE OF THE ANALYSIS**

We restricted our study to projects, programmes, and initiatives that are clearly CIIP<sup>1</sup> and ICT focused, and we included major international programs to situate European research in the international context.

**RESULTS**

We have classified C(I)IP projects or initiatives, completed or on-going, national and international. Using this classification, it is possible to identify methodologies used in projects and assist in identifying gaps in CIIP research. Based on the classification results – a classification matrix was extracted and presented in CI2RCO deliverable D6 (which is publicly downloadable on the CI2RCO website). Moreover, we have extracted the additional results.

Figure 3 shows the programs’ chronology in several countries. We present the start date and end date of each initiative (program, project, action, etc.) when it can be clearly identified or when this information is relevant (otherwise the initiative is classified as not applicable (n/a)).

We observe that US CIP research started in 1998, approximately two years before the EU launched its first project. Several

European initiatives started from the beginning of 2002 and the research effort within the EU is growing. In addition, we have collected funding information on the projects and noticed that increasing efforts are being carried out within Europe. It seems that Europe is definitely trying to bridge the gap in this domain. Indeed, CIIP has become a vital issue in Europe since most of European critical activities rely on highly interconnected networked communication and information systems. The good performance of those infrastructures is clearly threatened by incidents like faults, failures, human errors, and attacks.

Figure 4 classifies the projects based on the CI’s hierarchy levels and their research methods. We observe that only few projects aim at providing tools and methodologies as a final result, especially as the hierarchy level increases. In fact, most of the research efforts consist in a risk and/or vulnerability analysis, a high level design, etc. Many projects deal with the “government / economy / society and standards” level. They are generally initiated by the governments and do not necessarily need an active participation of the CI owners. In practice, most of the analyses have been carried out with the help of the private sector which represents obviously an essential link in this chain. In fact, critical infrastructures can only be efficiently protected if both the infrastructure and the services are reliable. Therefore, even if today’s CIP is essentially a governmental initiated activity, the projects are often conducted with the participation of the CI owners (private companies in most cases).

Currently, most of the identified projects at the European level are co-ordination actions or roadmap projects. This is due to the fact that CIIP is still a young research area. Therefore, the research needs must be clearly identified by an active research community that contributes to the European CIIP research

agenda. Research communities are trying to tackle the problem in order to improve the resilience of the critical (information) infrastructures. One way to reach this objective is to design the operational tools and methodologies that currently are not available and that will not be available in a near future to the required extent (some best practice approaches exist).

**CONCLUSIONS AND RECOMMENDATIONS**

Critical Information Infrastructure Protection or CIIP is still a young research domain even though European R&D in CIIP covers an increasingly comprehensive range of research themes. Although a great attention has been paid to CIIP since the last few years, the fundamental goal that consists in offering resilient, attack-resistant, and self-healing critical infrastructures is far from being achieved.

Several efficient classification methods, risk assessment tools, roadmap projects, etc. have been carried out at the European and national levels to push and coordinate the CIIP research and development efforts. These efforts are presently not only at the national and the European level, but also (marginally) at the international level.

In today’s CIIP field, there are **no efficient tools** for modelling, simulation and operation as well as CIIP policy-analysis that encompasses all the CII levels from the compound level to the component level. In particular, **cascading effects and (inter)dependencies are still hardly studied and understood**, both from technical and the organisational views. However, important steps have been taken to protect individual infrastructures in various nations (and European Member States). For example, electrical grids have accurate models, but the issue of (inter)dependent and cascading effects among different sectors has remained marginal.

---

<sup>1</sup> CII is defined as the information processes supported by information and communication technology (ICT) that are critical infrastructures by themselves or that are critical for the operation of other critical infrastructures. CIIP is defined as the programs and activities of infrastructure owners, manufacturers, users, operators, R&D institutions, governments, and regulatory authorities which aim to keep the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of service and to minimise the recovery time and damage.

The weakness implied by the (inter)dependencies of infrastructures will certainly lead to cascading failures as well as future attack attempts. Therefore, it is critical to **secure the critical infrastructures and their (inter)dependencies** in order to avoid cascading and escalating effects and to guarantee that critical services survive deliberate attempts to break security.

Due to the complexity of our interconnected and (inter)dependent infrastructures and due to the impossibility to design error-free systems, most of the CIIP tools and methodologies proposed today cover the risk assessment area. These do not provide fast-cicatrization, self-healing, and self-learning features. Improved resilience is often provided by *a posterior* action, e.g. by upgrading infrastructures to make them resistant to newly discovered attacks. It is essential to develop relevant and efficient monitoring tools and methodologies that will collect, filter and process data efficiently in order to move one step ahead towards self-healing and self-learning infrastructures. Yet, detection is no cure and it is necessary to develop new security measures and implement redundancy where needed.

Within the framework six program (FP6), several important integrated projects have begun. One of their goals will be to fill the gaps in the EU research in CIIP by proposing global approaches, from concepts to the design, as well as validation and deployment of tools.

We have noticed that most of CIIP research has either been developed independently by private stakeholders, or has been pushed by the governments with

little or no participation by the CI private owners. CI owners often use security by obscurity, and avoid revealing information on its infrastructure. However, improving the resilience of interconnected and interdependent infrastructures naturally leads to the sharing of knowledge, data and intelligence using trusted information sharing platforms.

Therefore, we propose the following recommendations:

- (1) The ambitious goal of CIIP research is to design resilient, **reconfigurable** and **self-healing** interdependent critical information infrastructures that **encompass all the CII levels**. Thus, it is not only necessary to design secure systems at one CII level (which is the approach that is generally adopted today) but also to **secure the interfaces in order to achieve a policy continuum**.
- (2) CIIP aims at assisting and improving the secure design and exploitation of critical infrastructures. Since it is impossible to design 100% secure systems, infrastructure operators spend important efforts in risk assessment and management but also in monitoring and reconfiguration of infrastructures (both in real time and non real-time when unexpected events occur). The general trend is to increase reconfiguration capabilities of infrastructures and the operators' ambition is to manage reconfigurability in a minimal time. Therefore, it is not only necessary to define what component should be reconfigured, how to reconfigure it,

and how to deploy updated security policies, but also to **secure the re-configurability** processes.

- (3) An increasing effort is being put in Europe to design efficient tools and tackle (inter)dependencies. However, (inter)dependencies can only be characterised and modelled if information is available from infrastructures generating those (inter)dependencies. As a consequence, **sharing of knowledge** and **trust** will be crucial issues in the near future. Past experiences have shown how reluctant infrastructure operators are to share data which are potentially confidential and may reveal internal vulnerabilities. Therefore, **secure models for co-operation** as well as **dynamic trust** management models and tools should be studied and developed.

However, those priorities are made complex by the scale and the heterogeneity within the infrastructures: multiple inconsistent security policies over various security domains and communication technologies together with outsourcing increase the difficulty in realising proper vulnerability assessments. Consistent work certainly needs to be carried out to determine the security assurance of the systems.

# SecurIST - Strategic Research Agenda.

**SecurIST is co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D.**



**James Clarke**

James Clarke received a B.E. in Electrical Engineering in 1986 and an MSc. Applied Mathematics in 1992. He works for the Telecommunications Software & Systems Group (TSSG) at the Waterford Institute of Technology in Waterford, Ireland. Mr. Clarke is working as the operations manager on the IST SecurIST project (FP6-004547) and the leader of the Applications Security Initiative (ASI) in the European Security and Dependability.

[Task Force: www.securitytaskforce.org](http://www.securitytaskforce.org).

## Introduction

In November 2004, the Co-ordination Action Project SecurIST (004547) commenced as a 24 month project as part of the Strategic Objective 'Towards a global dependability and security framework' of the 6th Framework Programme, contributing to its vision of 'anywhere anytime natural access to IST services for all' [1].

The purpose of the SecurIST project is to co-ordinate a Strategic Research Agenda for ICT Security and Dependability R&D for Europe. Its main mission is to provide Europe with a clear European level view of the strategic opportunities, strengths, weakness, and threats in the area of Security and Dependability. It set out to identify priorities for Europe, and mechanisms to effectively focus efforts on those priorities, identifying instruments for delivering on those priorities and a coherent time frame for delivery.

- The core objectives from the Description of Work for the project were:
- Drive the creation of an "ICT Security & Dependability Research strategy beyond 2010"
- Establish and co-ordinate a European ICT Security & Dependability Taskforce
- Leverage the knowledge base of existing/future ICT Security and Dependability researchers and projects

Through the use of clustering highly relevant thematic areas, the project will

leverage the knowledge base of projects and people already engaged in ICT Security & Dependability R&D. The thematic areas would enable projects to address how their research activity will contribute to higher-level and broader perspective issues, and to the clear elaboration of the Strategic Research Agenda.

## Project Achievements

As mentioned in the introduction, the SecurIST project has been charged with the co-ordination of a European strategic research agenda in the field of ICT for Security and Dependability, in particular for the timeframe of the 7th research framework programme (FP7, 2007–2013). In order to achieve this objective, the SecurIST project established two fundamental bodies: the European Security and Dependability Task Force (STF), and the SecurIST Advisory Board. The STF is currently comprised of 200 members, spread across fourteen fundamental thematic areas (initiatives) of research. It provides a forum for consolidation and consensus building. The SecurIST Advisory Board is composed of European experts in information security and dependability. The charter of the board is to oversee, review, enhance and promote results from the STF (see [www.securitytaskforce.eu](http://www.securitytaskforce.eu)).



The approach and method taken by the SecurIST project in developing the Strategic Research Agenda for ICT Trust, Security and Dependability can be seen in Figure 1. The interactions between the EU Security and

addition to two large convening workshops in January and April 2005, the project held a special convening workshop in March 2006 to fast track the inclusion of the newly formed Information Society Call 5 ICT for Trust and

sequent output reports. In May 2006, SecurIST held a dedicated Workshop bringing together the Mobile and Wireless and Security and Dependability Communities [4] for the first time to intensively discuss and agree the mutually important challenges and issues for their constituencies. In addition, the project organised an international workshop entitled EU/US Summit Series on "Cyber Trust: System Dependability & Security" was held in Dublin, Ireland on November 15th and 16th, 2006 [5]. It was attended by 60 delegates from the EU and the US, along with representatives from Canada, Australia and Japan. This event was co-organised and hosted by Waterford Institute of Technology (WIT), the project co-ordinator of SecurIST, and also co-organised by the US National Science Foundation (NSF), Department of Homeland Security (DHS), University of Illinois, and the European Commission, Directorate General Information Society and Media, Unit D4 "ICT for Trust and Security". The aim of this workshop, and a planned follow-up workshop to be held in Illinois in April/May 2007, was to gain a shared understanding of critical issues, identifying promising dependability and security research directions, and also to foster collaboration between EU and US research teams.

A large number of detailed challenges and priorities for FP7 were elicited from the EU Security and Dependability Task Force Initiatives and these were presented to the SecurIST Advisory Board for review both in writing and in presentations at Workshops. These detailed challenges can be found in [6]. Some of these research challenges areas encompassed the following (not exhaustive): Ambient Intelligence security and virtual security, resilience, security and dependability of large critical infrastructures, modelling and implementation of security policies, cryptology, biometrics, identification, privacy and authentication, network



Figure 1: SecurIST approach

Dependability Task Force (STF), comprised of mainly members from former FP5 and FP6 projects, and the SecurIST Advisory Board (AB) can best be described throughout the four project phases of the project in Figure 2.

The SecurIST project endeavoured to include as many participants and projects within the STF Initiatives and, in

Security projects [3]. This was a crucial milestone as it enabled the incorporation of a number of other very important challenges not originally captured in the STF work to be included in the analysis by the SecurIST Advisory Board; For example, projects involved in security and dependability in the software and services areas, Service Oriented Architecture (SOA), became involved and were included in the sub-

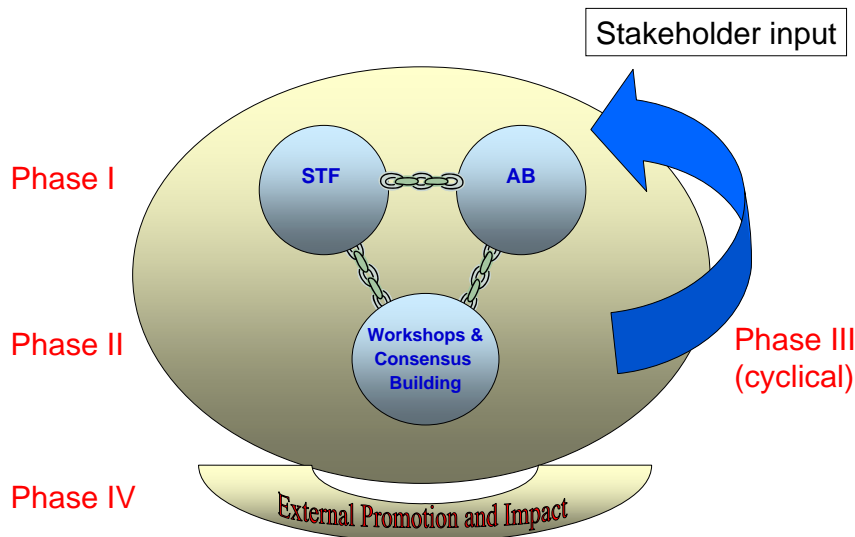


Figure 2: Interactions between STF and Advisory Board throughout SecurIST

security, IS security, software systems and service security, assessment of vulnerabilities, certification, the assurance of security, data assets management, research on new computing, communication and information models, the injection of semantics into these systems, because in a mobile, changing world, information must be validated locally, the creation of interaction models and knowledge models so that independent devices can, during their life cycle, learn how best to interact; also models for creation, acquisition, distribution, sharing of knowledge and trust, research and development on languages and tools in order to inject security and dependability during the design phase, and assess ability (verification and validation) techniques need to be developed. Please visit [6] for the complete list.

Based on the detailed inputs from the STF, the SecurIST Advisory Board issued three versions of reports presenting its recommendations for a future security and dependability research framework in Europe, for the period 2007-2013 [7]. Version 3.0 takes into account a large number of comments made by the TSD community during an open consultation forum held July – September 2006. Under the headline From “Security and Dependability by Central Command and Control” to “Security and Dependability by Empowerment”, the Advisory Board is recommending the following nine key research areas:

- **Empowerment of the Stakeholders:** User awareness/control in all R&D and ensuing functionality: generic usability, security, trust and dependability;
- **Europe-specific Security & Dependability:** Euro-awareness and goals in all R&D and ensuing exploitation;

- **Infrastructure robustness and availability:** Generic dependability and consistency of all aspects of European (and global) ICT infrastructure;
- **Interoperability:** Inter-working and interoperability of security and dependability across a convergent yet heterogeneous digital world;
- **Processes for developing Secure and Dependable systems:** Provision and use of trusted tools, processes and procedures to achieve a secure, and dependable digital environment;
- **Security and Dependability Preservation:** Maintenance of achieved security and dependability states against attack/failure/erosion;
- **User-centric security and dependability standardisation:** Involvement and consideration of human user needs and sensitivities in development of standards;
- **Security and dependability of Service Oriented Architectures (SOA):** Establish basics of trust, security and dependability in new Software Systems and Services architectures and approaches;
- **Technologies for security:** Underlying many of the previous recommendations, relates to ongoing development of existing technologies, and exploration of new possibilities; e.g. cryptology and trusted functionality.

In addition to these nine key research areas, four future grand challenges (covering a 10-20 year vision) were compiled. They illustrate possible longer-term possibilities and implications. These are:

1. Countering vulnerabilities and threats within digital urbanization: This challenge addresses open problems that

we will face in security and dependability from the expansion and globalization of digital convergence by 2010-2015.

2. Duality between digital privacy and collective security: digital dignity and sovereignty: This challenge deals with future privacy issues of all the stakeholders, whether citizens, groups, enterprises or states. It addresses the problem of how to override the "Big Brother" syndrome and "dark security", i.e., the future assurance of digital sovereignty and dignity for the various stakeholders.
3. Objective and automated processes - the Reinforcement of the Science and Technical Foundations of TSD: This challenge addresses the problem of how to attain a controllable and manageable world of complex digital artefacts by 2015 and how to inject regular, quantitative techniques and engineering to make the field truly scientific.
4. Beyond the Horizon: a new convergence – Going beyond the Digital Universe: This last challenge deals with the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum “galaxy” and the new security and dependability challenges that will emerge.

The formal launch event of the work of the SecurIST project was formally held at IST 2006 in Helsinki, Finland. The title of the networking session proposed and organised by the SecurIST project was ‘Security, Dependability and Trust in pervasive networks and services: Towards a Roadmap 2007-2013’. Over 115 people attended the session on 22nd November 2006. There were two strands to the networking session:

1. The SecurIST Advisory Board presented some of the Grand Challenges as identified in their recommendations report;

2. A call for presentations was made by the SecurIST session coordinators and a number of presentations were accepted by researchers on identified gaps in current research in Europe within ICT Trust, Security and Dependability areas and potential project proposals for Call 1 of FP7. WIT/TSSG is facilitating a follow up co-ordination group as we continue preparation for FP7.

All of the reports discussed here can be found at [www.securitytaskforce.eu](http://www.securitytaskforce.eu)

### Annex 1: References

[1] <http://www.cordis.lu/ist>, FP6 Work Programme, Call number 2.

[2] <http://www.securitytaskforce.eu/>

[3] SecurIST Deliverable, D3.2 Validation Workshops report, November 2005.

[4] SecurIST Deliverable, D2.4 Convening's of the Task Force – Joint SecurIST, Mobile and Wireless Workshop report, 11/12th May, 2006.

[http://www.securitytaskforce.org/dmdocs/cu-](http://www.securitytaskforce.org/dmdocs/cu-ments/jointws_report_v1july0707_reportonly.pdf)

[ments/jointws\\_report\\_v1july0707\\_reportonly.pdf](http://www.securitytaskforce.org/dmdocs/cu-ments/jointws_report_v1july0707_reportonly.pdf), plus Annex containing detailed material

[http://www.securitytaskforce.org/dmdocs/cu-](http://www.securitytaskforce.org/dmdocs/cu-ments/JointWS_AnnexOnly.pdf)

[5] SecurIST Deliverable, D2.5 Joint EU US Cyber Summit System Dependability & Security Workshop report, 14-16 November 2006.

[http://www.securitytaskforce.org/dmdocs/cu-](http://www.securitytaskforce.org/dmdocs/cu-ments/JointWS_AnnexOnly.pdf)

[cuments/ D2.4 Joint EU US Cyber Summit WS Report V1.0.pdf](http://www.securitytaskforce.org/dmdocs/cu-ments/JointWS_AnnexOnly.pdf)

[6] SecurIST Deliverable D3.3 – ICT Security & Dependability Research beyond 2010: Final strategy.

[7] Lechner, et. al. Recommendations for a Security and Dependability Research Framework: from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment, Version 3.0, January 2007.

# Safety and security: two sides of the same medal.

**Safety and security have developed into two separate communities, each with their own specific methods, terms and concepts. But in reality they are two sides of the same medal and should be treated together.**



**Odd Nordland**

Studied nuclear physics and computing science and has worked as a safety assessor for over twenty five years. Since 1997 working for SINTEF in Trondheim. [odd.nordland@sintef.no](mailto:odd.nordland@sintef.no)

For a Norwegian, understanding the difference between safety and security is a problem: like other Germanic languages, Norwegian has only one word for both concepts, so some kind of explanation is always necessary. The simplest - and worst - solution is to refer to the English words and hope your audience knows what you mean. It doesn't.

## **Explanations instead of definitions**

There are of course numerous standards and guidelines that contain definitions of the terms, but as the then head of the NASA safety engineering school once put it: the nicest thing about (safety) standards is that they're so incredibly easy to improve!

The fact is that the standards are a compromise between rivalling factions, and each of those factions wants to have its own definition as the "officially" adopted one. Meine van der Meulen has collected definitions from standards and guidelines and came up with four different definitions of safety and six different definitions of security. Although that was over ten years ago, the standards he quoted still apply and the last thing a standardisation committee updates is the set of definitions that was so difficult to reach an agreement upon.

Now rather than increasing the confusion by introducing even more definitions, let's just agree on a couple of explanations of how the terms are going to be used in the following text. You will probably find definitions in your favourite standard that correspond closely enough to the explanations given here.

In all cases, we are considering a "system" in an "environment". The system can be anything from a reasonably simple device to a complex, critical infrastructure such as a power grid, a railway network or the like. Its environment is the rest of the world, i.e. everything that is not part of the system.

Now a system can possibly have undesired effects on its environment, but the environment can also have undesired effects on the system. We will use the term safety to denote the inability of the system to have an undesired effect on its environment, and security for the inability of the environment to have an undesired effect on the system.

## **Safety is security**

The above explanations already show how close safety and security are to each other. Indeed, many safety measures can equally well be considered as security measures, and vice versa.

**Safety: the inability of the system to have an undesired effect on its environment.**

**Security: the inability of its environment to have an undesired effect on the system.**

In a nuclear power station near a river, there were mounds behind the power station on the land, but a low flying plane coming from the water side would be able to crash into the reactor. So a concrete wedge was installed to deflect an incoming plane away from the reactor. Now was that a safety precaution, or a security precaution?

The wedge certainly protected the reactor from being damaged by an external attack, but it also protected the environment from the radioactive contamination that such an attack could have caused.

And here we see the coupling: security protects your system and in doing so protects the system's environment from the harm that a successful attack could cause. So security is a safety precaution.

### **Safety related concepts can be adapted to security**

Safety experts often claim that the security people are just re-inventing the wheel. Security people not only use attack trees, they have also developed tools - i.e. computer programs - to generate the corresponding diagrams and assist with the analyses. A brief glance at attack trees reveals more than just a resemblance with the fault trees that safety people have been using for decades.

There are, however, significant differences. In fault trees we use the probabilities that items will fail to calculate

the probability of a top event, usually system failure. For an attack tree, using probabilities is more difficult. So we need to translate concepts and parameters in a sensible way.

Demoscopic methods are quite successful in predicting the outcome of an elec-

tion, so they can probably also be used to estimate the probability of an attack being attempted. But an attack is harmless if the attacker does not possess the necessary capabilities to succeed, so just knowing that e.g. one person in ten thousand is a potential attacker is not enough. How many of those potential attackers have the necessary knowledge and resources to actually do damage?

The answer is not easy to find, and it will certainly require a lot of research work to identify which security parameters correspond to which safety parameters and - more important - how to measure them. We can then start thinking about how to interpret things like minimal cut sets.

### **SILs and EALs are not equivalent**

Safety Integrity Levels (SIL) were introduced in the Defence Standard 00-55 in 1991; IEC 61508 adopted the concept, albeit with a somewhat modified definition, and nearly all of the safety related standards that are derived from IEC 61508 have also adopted the concept.

SILs are defined in terms of failure rates of a safety function. In many systems, the safety functions are implemented by dedicated equipment, so the failure rate of the function becomes equivalent to the failure rate of the equipment, but this is not always the case.

A failure of part of the equipment that is used to implement a safety function may not necessarily result in total loss of the safety function, because

the loss may be compensated by another part of the system. For example, the mechanical hand brake of a car can at least partially compensate a failure of the hydraulic brakes. In this case, the safety function will continue to be effective, although possibly more weakly. This ability of a safety function to con-

tinue to be effective in spite of partial break down is Safety Integrity.

Depending on how many measures we use to implement a safety function, how effective they are, how vulnerable they are etc. we will get different levels of safety integrity. In other words, the SIL class (please do NOT talk about SIL levels!) is determined by the way a system has been built.

With EALs the situation is different. The term Evaluation Assurance Level (EAL) is defined in the Common Criteria (CC), a standard for certification of security in IT-systems and products. The concept can be extended to include more than just IT security.

As the name indicates, EALs are determined by the depth to which an evaluation has been performed and a higher EAL can be achieved by simply reassessing the system. This will give greater confidence in the system without changing it in any way. There are some attempts to associate SILs and EALs, but they should be taken with caution. A SIL is a system property; an EAL is an assessment property.

Nevertheless, there is a potential for synergy. Safety integrity levels are determined by the safety requirements on a system, and the standards usually simply state that for a low safety integrity level the amount of safety evidence to be provided may be less than for a system with a higher safety integrity level. It is then left up to the assessor to determine how much evidence is adequate. A set of guidelines, similar to the Common Criteria for security, could certainly help.

On the other hand, the security community could also profit from introducing a concept similar to the safety integrity level, e.g. a "Security Criticality Level".

As mentioned earlier, SILs are determined by the safety requirements on a

**Security related parameters that correspond to safety related parameters - and how to measure them - need to be determined.**

system, based on tolerable hazard rates. For security, tolerable threat levels could be defined, from which the security criticality levels could be derived.

This is not to be confused with the threat levels that security authorities operate with today. When the authorities tell us the threat level is “red”, they are saying something about the current situation, not about the kind of threat we’re assumed to be willing to accept.

### Measuring criticality

The idea of security criticality levels immediately leads us to the problem of measuring criticality. Clearly, a vital infrastructure will have a higher criticality level than a single system that can easily be substituted.

But even with critical infrastructures there will be different levels of criticality. As long as we have cars and trucks, the railway network will have a low criticality, but only as long as the roads are intact and fuel is available. In other words, the criticality of one infrastructure can be dependent on other infrastructures and how intact they are. Thus, in order to measure criticality, we must determine the degree of independence between systems.

This is not unlike the problem of independence of failure modes in safety related systems. There are guidelines to help determine how independent the failure modes of safety related equipment really are, and similar considerations could be used to determine the dependencies of vulnerabilities in the security field.

### Acceptability is a mutual problem

But the problem doesn’t end there. There is also the question of acceptability. For hazards it is already difficult enough to determine what the general public is willing to accept. The nuclear industry assumed that people would be willing to accept the residual risk of a nuclear power plant so long as it was lower than the risks they were exposed to by other accepted systems, such as motor cars.

The discussions and demonstrations that accompanied the introduction of nuclear power plants at least in most western countries revealed the opposite: the more people are aware of a risk, the less willing they are to accept it.

On the other hand, people do accept an astonishingly high hazard rate with motor traffic, even though they are made aware of it almost daily. On the one hand they tend to regard the benefits of mobility that motor cars give them as high enough to justify the risk; on the other hand they believe that they have at least some influence on how big the risk is.

For security and threat levels we can probably expect a similar reaction. If people consider the benefits of an infrastructure as marginal, they will be more willing to tolerate threats against such a system. As long as we can take a car, who needs railways? But cut off the water supply, and people will react.

So for safety and security we need to determine what is acceptable. This is not a trivial problem. Nevertheless, the principles that apply to safety can equally well be applied to security.

### Where are the differences?

One area where safety and security definitely differ is testing. For a security system it is often possible to con-

duct a full scale attack to see if such an attack would have been successful. For example, you can try to smuggle explosives through a security gate without actually detonating them. If you succeed, your security system has a weakness that has to be fixed. But you can’t let a chemical plant emit poisonous gases in order to see if the safety barriers work: if they fail, you will have a major problem!

Nevertheless, there is also a potential for synergy here too. Both safety and security people make extensive use of simulators, so there should be possibilities of combining tools to a more realistic model of a system and its environment.

### Combining approaches

As we have seen, safety and security have a lot in common. Both areas can learn from one another, but more important, it can supplement each other.

The more society becomes dependent on technological solutions, the more important it will

be to regard safety and security as a single issue.

There is still a lot of work to be done before we can fully utilise the experiences that the safety and security communities have gathered. The methods and tools that one community has developed can and should be adapted so that both communities can use them.

The days when a safety expert could say “That’s not my problem, that’s a security issue” are definitely over. Security is a safety issue, just as safety is a security issue.

So those Germanic tribes who only have one word for both safety and security are, in fact, on the right track.

**Security is a safety issue, just as safety is a security issue.**



## Knowledge based Emergency Management Tool



**Hermann Dellwing**



**Walter Schmitz**

H. Dellwing and W. Schmitz are senior consultants of IABG in the field of CIP and military and civil crisis management. Hermann Dellwing was project manager of IT-development projects concerning the support of crisis management.  
Phone: +49 (0)261 / 94729-820  
E-Mail: dellwing@iabg.de

Walter Schmitz was the scientific co-ordinator of the European Commissions ACIP (Assessment of Critical Infrastructure Protection) project and is member of the EC VITA (Vital Infrastructures Threats and Assurance), CI2RCO (Critical Information Infrastructure Research Co-ordination) and IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems) projects.  
Phone: +49 (0)89 / 6088-3331  
E-Mail: schmitz@iabg.de  
Internet : <http://www.iabg.de>

### Introduction

The operation of the electricity and communication networks is supported by various systems. The simulation of different situations in the network provides information about the behaviour of the network in real and planned situations. Supply failures (blackouts) nevertheless cannot always be avoided. The increased interconnection of critical infrastructures via the ICT-backbone increases the danger of cascade effects, which can lead to an area-wide blackout.

The analysis of recent blackouts shows, that a narrow time window is available – in many cases shortly before the blackout. In this time window suitable measures for prevention or mitigation of cascading effects can be taken, provided, that the situation has been assessed well.

It is a precondition, that the necessary information about the situation to be assessed is timely available and the decision-making process is supported by suitable tools.

For this purpose IABG develops the tool

### **Crisis Prevention and Planning System (CRIPS)**

in the context of the IRRIS<sup>2</sup> project.

The aim of CRIPS is to minimize the danger of blackouts by

- Assessment of the current situation
- Support of the decision making in Emergency management
- Warning and Alerting, including the broadcasting of the decisions

### **A „realistic“ Scenario**

To describe the field of application of CRIPS, an artificial Scenario consisting of two actual events, which have taken place in Germany and in Italy years ago, is transferred into the Rome area. In this combination they have happened neither in Germany nor in Italy, but the combi-

nation represents a realistic scenario, in which the functionality of CRIPS can be demonstrated.

The initial event of the scenario is a nightly water pipe burst, and a backbone node of the communication network in Rome is flooded: The power supply is switched off automatically; diesel generators do not start working, so that the complete power supply of the node is coming from the emergency batteries.

The assessment of the damage shows, that the cooling water supply of the air conditioner of the backbone node must be repaired, which means, that the cooling water supply must be interrupted. But this action leads to an overheating of the electronic equipments of the backbone node and most components stop working.

The failure of the communication backbone node impairs the information exchange between the control centres and substations of the electricity network in the Rome area. A part of the substations are operating in “blind flight”. An assessment of the current situation is impossible and nobody has information enough to make the right decisions to stop the spreading of the failures in the networks.

In this combined scenario it is assumed – differing from the real events in Germany and Italy – that there is a failure in electric lines because of a lightning strike, and shortly before the reopening of the communication services the power supply of Rome is interrupted. Due to the incomplete information, the dispatchers can assess the current situation only insufficiently. They want to avoid further blackouts in the Rome area and they try to avoid decisions, which would lead to the switching off of further areas. There is a possibility to guarantee the power supply of Rome under normal conditions: the full capacity of the transformer in the station "Apen-

<sup>2</sup> see <http://www.irris.eu>

nine". Because of the restricted information exchange and pressure of time, a planned maintenance at this transformer is not taken into account, and "the safe solution" is leading to an overload of the transformer, and – consequently – to a full coverage power failure in Middle and South Italy.

Result: Due to the disturbed communication only an incomplete situation assessment was possible, and the decisions and measures, based on it, expand the local blackout to an extensive blackout in Italy.

**Scenario Model**

The Scenario described above is represented graphically in Figure 1, which leads to the task of CRIPS:

1. The failure of the line "Arno" together with the maintenance of the transformers in station "Apennine" proves to be a "critical situation". Wrong decisions lead to a full-coverage blackout in Middle and South Italy.
2. The communication backbone node "Rome" fails because of a flood, which leads to functional failures of further communication stations and impairs strongly the communication services in single regions.
3. Particularly the communication towards the control of the electric power supply is restricted.

Figure 1 shows the "main components" of the scenario:

- The transformer stations "Apennine", "Rome", and "Tiber" are primarily involved in the power supply of Rome. Furthermore the station "Apennine" is also an important component in the high voltage network, the failure of which can have far-reaching consequences.

- The communication nodes "backbone Rome", "Tiber" and "Umbra" represent components of the communication network, and failures in this nodes are very dangerous for the communication supply and can have dangerous effects on the operation of the electricity networks.

**Interpretation of the Scenario Model**

Disturbances in networks are possible at any time: planned disturbances (e.g. caused by maintenances) and unplanned disturbances (e.g. caused by thunderstorms), but the networks are designed in a way – for example taking into account the "n-1-rule" of the UCTE –, that alternatives are possible and critical situations can be avoided.

The networks are permanently checked by simulations in order to discover and avoid those critical situations. But the numerous examples of blackouts show, that not all critical situations are discovered in time or the importance of such disturbances is not clear.






Such an emergency situation is shown in the scenario: the example of the unplanned failure of the line "Arno" together with the planned transformer maintenance in the station "Apennine" together with a critical situation in the communication network.

Figure 1 does not represent any technical outline of an energy supply or communication network; it is a graphic representation of special views of decision makers on the network:

- The electricity lines "Arno", "Latium" and "Tiber" guarantee the power supply of Rome. Further lines – directly and indirectly connected to the station "Apennine" – are

- important components of the high-voltage network and a failure can have far-reaching consequences.
- The regions "South Italy", "San Marino" and "Tuscany" represent geographical areas, which are affected by the critical situations described in this scenario.
- The regions "Tiber" and "Umbria" are affected by disturbances into the described components of the communication network.
- The transformer station "Naples" and the electricity line "Apennine" are not involved directly into the power supply of Rome. Depending on the exploitation of the other lines they can, however, contribute to the supply of Rome. This also applies to the station "Po" as well as to the power station "Caesar" and the line "Lagoon", which are alternatives to the power supply of Rome.

The components of Figure 1 are

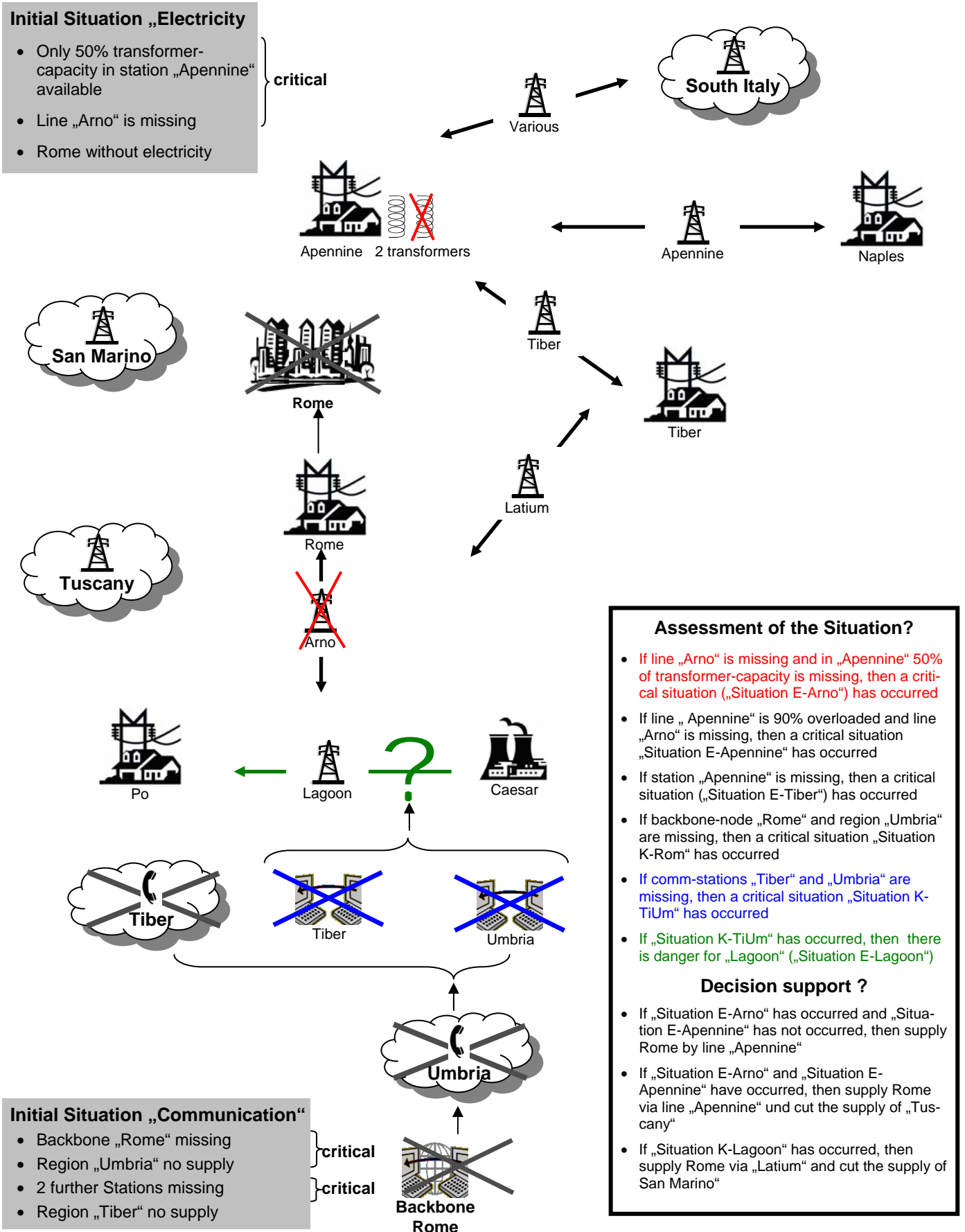
- Electricity Lines 
- Transformation stations 
- Generators 
- Kommunikation codes 
- Regions to be supplied 

The support of CRIPS in this scenario is demonstrated in the text box:

The text box contains a formal description of rules. According to the figure it will be described, how this rules (part of the knowledge base of the expert system CRIPS) can help to make an assessment of the situation together with a decision support, which could help to avoid critical situations and blackouts.



Figure 1: Model of the Scenario



### What has to be done in the scenario?

- All indicators for a judgement of the situation must be taken into account. That means all interfaces to information and communication systems have to be used for the acquisition of information.
- The responsible people in control stations as well as at the management level must know which consequences a failure of certain network components can have. This means, the ability for the comprehensive situation evaluating must be strengthened.
- The right decisions for prevention of the blackout in the Rome area should have been taken on the basis of this evaluation of the situation. It means that any decision support must be based on a situation assessment.
- In the case of the not prevented blackout "Rome", one would have assessed the consequences – in particular those on South Italy's energy supply – and started suitable measures. This means, that alternatives must be elaborated.

### The support of CRIPS in the scenario

- CRIPS would have given an assessment of the situation e.g. after the failure of the line "Arno". Have a look at the rule in Figure 1 (text box): „If line „Arno“ is missing and in „Apennine“ 50% of transformer-capacity is missing, then a critical situation („Situation E-Arno“) has occurred“. This assessment may be contained in emergency plans.
- CRIPS would have suggested the alternative "switch to station"Apennine"". Responsible for this decision-support is the rule "If „Situation E-Arno“ has occurred and „Situation E-Apennine“ has not occurred, then supply Rome by line „Apennine““. So the alternative "Supply via line "Apennine" would have been proposed and not the "switch to station "Apennine" and station "Naples". But – depending on a certain development of the situation in the network – other rules would have forbidden this alter-

native and would have proposed other possibilities or emergency measures – described in emergency plans.

- If a switch to station "Apennine" would have been done, then CRIPS would have prevented the great blackout in Middle and South Italy by suggesting a cut of supply of Tuscany according to damage containment. Furthermore CRIPS would have suggested an alternative to the supply for Tuscany. No rule in Figure 1 would have allowed the switch to the station "Apennine" without suggesting alternatives.
- CRIPS would have known that there were problems in the communication network and would have suggested alternatives in the area of the communication and the energy supply to guarantee the necessary communication concerning the realisation of an alternative supply for Tuscany. A rule is outlined exemplarily in Figure 1 ("situation "K Rome")  
Figure 1 shows only an exemplary choice of rules. It is important to point out, that the decision support is normally based on emergency measures which are described in emergency plans. In this case, CRIPS can use interfaces to those plans.

### Emergency Management

In emergency situations CRIPS has to support the staff concerning the assessment of the current situation and the decision making. CRIPS develops primarily its abilities, if

- there is a high complexity in the subject area
- there is a complex dependency structure in the subject area
- know-how coming from experience (gaming, real situations) is necessary
- an emergency plan (with emergency measures as decision options) exists
- there is a big pressure of time concerning the decision-making process

### CRIPS Method

CRIPS is an expert system and the method is suitable to fulfil the following requirements:

- In addition to results of simulations of the network, know-how coming from lessons learned gained by exercises and real situation can be used
- ☞ CRIPS completes simulations
- CRIPS assesses the current situation with regard to critical situations and to cascading effects, which can lead to blackouts
- ☞ CRIPS makes an assessment of the current situation
- The indicators for the assessment of the situation are coming from all available and reliable sources
- ☞ CRIPS puts the assessments on a broad basis
- The assessment of the current situation is a continuous process over time and basis for an actual decision support
- ☞ CRIPS supports the decision making
- Decisions concerning prevention or limitation of consequences of blackouts have to be selected
- ☞ CRIPS helps to prevent or to mitigate blackouts
- Decisions must be broadcasted
- ☞ CRIPS has an interface to alert systems.

CRIPS is based on a set of „if-then-else-rules“ – characteristic for an expert system – with the following advantages:

- The complexity of the problem definition is dissolved in form of "simple rules".
- Higher complexity only leads to a larger number of rules.
- The Rules and their evaluation (inference) are separated; so an easy maintenance of the knowledge base is possible.
- An explanation component explains the rationale of the assessment and of the proposed decision options.
- The inference strategies (forward and backward chaining) simulate very well the thought-process of experts (e.g. members of a staff) with regard to "assessment of situations" and "generating of decision options".

# Information security, Internet security or critical information infrastructure protection?

ICT security challenges for citizens, organisations and states.



**Solange Ghernaouti-Hélie**

HEC - University of Lausanne  
[sgh@unil.ch](mailto:sgh@unil.ch)

<http://www.hec.unil.ch/sgh/>

Professor Ghernaouti-Hélie has published over 15 books related to telecommunication and security strategies and technologies issues. As an international expert on Cyber security and Cyber crime issues, she writes for the International Telecommunication Union the "Cyber security guide for developing countries" presented at the World Telecommunication Development Conference in Doha (ITU 2006). She is cofounder of the interdisciplinary Master in Law, Crime and IT Security (University of Lausanne).

Availability, reliability, confidentiality, integrity, quality and confidence seem to be criteria that one wishes to be able to associate with any type of electronic services whether in the context of the cyber-administration or in that of the trade and finance for example. Thus, the information security becomes the essential basis in the success of Internet for the use of the citizens, the organizations and of the States.

Insofar as Internet is on the way to become, quite rightly or not, a must of the information society, we have the right to ask us if it constitute a critical infrastructure, as necessary as the electric distribution systems.

The concept of criticality associated to digital technologies, information or, more generally to ICT infrastructure, is function of the level of its importance for those who rely on and depend on it to survive, to be in safety or to be efficient and competitive. It could be evaluated by a risk assessment process and impacts analysis in case of lost or unavailability.

Indeed, the capacity of companies to produce and carry out services is increasingly related to technologies and services provided by the Internet. However, the data-processing and telecommunication infrastructures belong only partially to those who depend on it for every day activities. Even the so-called "state" infrastructures belong to a large extent to private companies. In this context of dependence and interdependence

of ICT infrastructures, and of electric infrastructures, what about their security? Therefore, is it better to speak about infrastructure security than only about information security or Internet security?

Nowadays, a trend is emerging concerning the evolution of the apprehension related to information security, ICT security, Internet security or cyber security, towards a term much more badly defined and complex relating to the critical information infrastructures protection. This modification of terminology without a real definition, so as if it were natural, introduces more complexity, more blur and it doesn't look at the Internet security problem under the angle of the protection of individuals, their private data, the respect of the basic human rights, the informational assets of the organizations, but seems to focus only on the security of the state and on homeland security.

Is it strictly a question of terminology or is it a displacement of the issues, the challenges, the market, or the field of application of ICT security?

Difficult in the first attempt to answer and identify in this semantic slip the challenges the people in charge of a company are faced with in terms of information and operational risks, whether they are from criminal origin or not?

Changing the object of the ICT security approach contributes to remain unanswered the fundamental question inherent to any security action, that is to say, “Who controls the security?”

In fact, the chief information security officer of a company cannot respond directly to this essential question and he must address many more open issues, as:

Which level of confidence can he have in security solutions and security services produced by third parties?

On what kind of operational and business metrics he could rely upon to measure information security effectiveness?

What are the competences, tools, methodologies necessary to evaluate the information risk? How insuring the information risk? How transforming the IT risks into business opportunities?

How to be in compliance with standards or regulations? How justifying ICT security investments?

How set up effective and coherent measures of ICT security? How evaluate them in regards of vulnerabilities, threats and costs? How to guarantee security? How are certified ICT security products?

Only transparent and controllable security solutions and a real universal know-how can bring a maturity level to the security market, in adequacy with the issues that it has to satisfy in order to build an inclusive information society.

We must be careful to continue to make a distinction between the information security in the context of ICT security, and Internet security, and the critical information infrastructure protection and the homeland security, because it could be possible to forget to analyze the needs of ICT security from the end-user

point of view and in terms of respect towards democratic principles.

An amalgam, that those who hold the Internet technology and the marketed security solutions, and who are slightly imposing their legal framework at the international level, could not hesitate to do.

So many open questions concerning ICT security and Internet governance still remain. These issues go past the purely technological dimension of the Internet and its security, without having been preceded by true society debate and people awareness concerning security challenges for citizens, organisations and states.

# CESS >>> Excellence in Security

**CESS is a group of scientists and managers specialised in security. It provides independent quality services and support in security and related problem areas. Its focus is on integrated interdisciplinary holistic concepts.**



**Reinhard Hutter**

Director CESS.  
[Reinhar.Hutter@gmx.de](mailto:Reinhar.Hutter@gmx.de)

Senior Vice President, European Security Analyses, IABG, until 2005, and Information & Communications Division, IABG, until 2003.



Centre for European Security Strategies

The new and evolving security challenges require a novel type of strategic expertise on a European level. Even after years of research and community building much is still in its infancy. CESS is based in Germany, with outreach across Europe and beyond. The cornerstones of the Centre are development of concepts, structures and capabilities for strategic and operational security planning and implementation.

### **Safety, Security and Defence**

CESS is specialised in security, safety and defence consultancy for private and public bodies. It has the expertise, organisational capabilities and networks to provide high level concepts and decision support across the safety and security domain. It focuses on sustainable security strategies in a dynamically changing threat environment, on integration of security and defence capabilities, on harmonisation of policies and concepts, on analysis and protection of critical, infrastructures as well as on interoperability and standards for security systems, procedures and technologies.

### **Early Roadmap Projects**

Protection of highly interdependent critical infrastructures requires novel approaches. Ownership and interdependencies are heterogeneous. Effective solutions to protect these assets require shared responsibility of the

various public and private stakeholders. Commonly agreed solutions need to integrate strategic thinking, new models from research, industrial and technological potential as well as institutional competence in an atmosphere of trust and confidence. CESS functions as a catalyst and mediator. Its core members were the initiators of early EU projects on critical infrastructure protection (CIP) as well as of a national working committee on critical infrastructures, both providing role models for the safety and security domain. CESS is involved in establishing regional centres of excellence for “homeland” security combining strategic thinking, threat analysis and scenario development, risk management concepts, demonstration and exercising and evaluation of technologies.

**CESS – an incubator of ideas in the Safety and Security domain.**

### **A Portfolio for Tomorrow’s Security Challenges**

Cooperation of public bodies, research institutes and universities and industries are the key to successful solutions. The portfolio of CESS is focused on four areas: Strategies and concepts, planning and decision support, competence enhancement and benchmarking and assessment. This integrated view from different angles is a prerequisite for achieving the required flexibility, enhanced emergency preparedness and response, reduction of threats and risks as well as improved protection of people, assets and resources.

# CRITIS 2007 Call for Papers and Participation

## 2nd International Workshop on Critical Information Infrastructures Security Benalmadena-Costa, Málaga, 3 – 5 October, 2007



**Javier Lopez**

**CRITIS'07 Program Chair**

**University of Malaga  
Computer Science Department**

**Tel: +34-952131327**

[jlm@lcc.uma.es](mailto:jlm@lcc.uma.es)

<http://critis07.lcc.uma.es>

Nowadays, key sectors of economies depend highly on ICT. The information flowing through the resulting technological super-infrastructure as well as the information processed by the complex computing systems that underpin it becomes crucial because its disruption, disturbance or loss can lead to high economical, material and, sometimes, human loss. As a consequence, the security and dependability of this infrastructure becomes critical and its protection a major objective for determined sectors. Last year - the First

International Workshop on Critical Information Infrastructure Security (CRITIS'06) - successfully served as a platform for discussing these issues. This year, the second edition of the workshop will be held in Málaga (Spain).

The main objective of this workshop is to bring together researchers and professionals from universities, private companies and Public Administrations interested or involved in all security-related aspects of Critical Infrastructure Protection (CIP), and therefore, they can learn about the new advancements in the security of CIP, while discuss about issues and problems in the area, identifying common research interests and establishing co-operation networks.

**The focus of CRITIS'07 is to gather together researchers and professionals interested in all security-related aspects of Critical Information Infrastructures**

CRITIS'07 is co-sponsored by IFIP WG 11.10 on CIP, IEEE Computer Society Task Force on Information Assurance, and Joint Research Centre Ispra of the European Commission.

### **Conference Scope**

The following (non-exclusive) areas of CIP will be covered in several sessions: Code of Practice and Metrics, Communication Risk & Assurance,

Early Warning Systems, Economics on CIP, R&D Agenda, SCADA and Embedded Security, National and Cross Border Issues, Information Sharing and Exchange, Policy Options Elaboration

Threats and Attacks Modelling, Continuity of Services and Resiliency, Dependable Infrastructure Communications, Internet-based remote control, Forensic Techniques, Incident Response, Network Survivability, Trust Models in Critical Scenarios and Security Logistics.

### **Paper Submission**

We look forward to receive research papers or industrial experiences related with CIP. Submissions will be thoroughly evaluated by reviewers and the accepted papers will be presented at the Workshop. Post-proceeding will be published by Springer in the Lecture Notes in Computer Science series. The deadline for paper submission is July 2nd, 2007. For specific submission instructions and general information of the event, see: <http://critis07.lcc.uma.es/>



# Conference on Information Technology for Critical Infrastructure Protection

The first international conference on Information Technology for Critical Infrastructure Protection on 4-5 September 2007 at Königshof Hotel (in Bonn, Germany) seeks to attract researchers, professionals and practitioners from all kinds of critical infrastructures.

## Programme Chair

Stefan Wrobel (Fraunhofer IAIS)

## Programme Committee

Eyal Adar (ITCON Ltd.)  
 Robin Bloomfield (City University)  
 Sandro Bologna (ENEA)  
 Claude Chaudet (ENST)  
 Donald D. Dudenhoefter (Idaho National Laboratory)  
 Claudia Eckert (Fraunhofer SIT)  
 Nouredine Hadjsaid (L.E.G.)  
 Bernhard M. Hämmerli (HTA Luzern)  
 Claus Kern (Siemens)  
 Raija Koivisto (VTT)  
 Eric Luijff (TNO)  
 Gerard Maas (TenneT / ETSO / UCTE)  
 Angelo Marino (EU-IST)  
 Marcelo Masera (EU Joint Research Centre)  
 Saifur Rahman (Virginia Tech)  
 William H. Sanders (University of Illinois)  
 Walter Schmitz (IABG)

## Contact & Information:

Information on the conference can be found at the conference website

[www.itcip.eu](http://www.itcip.eu)

## Important Dates:

4-5 September 2007:  
ITCP 2007 International Conference

6 September 2007:  
Public IRRIS Workshop

The vulnerability of critical infrastructures due to dependencies between them and the need for proper protection has been recognised widely. However, it is still an open issue how to describe, model, analyse and simulate them and how to mitigate the risk. While infrastructure providers have taken measures to protect their infrastructures from the inside, the protection against negative effects of their own and of other infrastructures due to dependencies (e.g. cascading, escalating and common cause failures and attacks) is still a problem to be solved. Further in-depth analysis has to be provided and supporting modelling and simulation tools are still in their infancy.

ITCIP 2007 is organised by the EU Integrated Project IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems, [www.irriis.eu](http://www.irriis.eu)) to present and discuss the challenges described above and look into possible solutions. ITCIP 2007 will establish a world-wide network of industrial stakeholders, technology providers, and researchers addressing these challenges.

The scope of ITCIP 2007 specifically addresses dependencies between infrastructures in critical sectors, across different sectors, and across national borders. Special attention is paid to electric power and to telecommunication infrastructures including the internet as almost all other critical infrastructures are dependent on the services they deliver.

The conference will host attractive, invited talks and present high-quality peer-reviewed papers. The conference sessions comprise topics as

- modelling and simulation of critical infrastructures
- security and safety for ICT-based critical infrastructures
- analysis of critical infrastructure interdependencies
- tools for critical infrastructure modelling, assessment and management
- threat, vulnerability and risk analysis for critical infrastructures
- trusted information sharing between critical infrastructure stakeholders including early warning systems
- information and communication technologies (ICT) for resilient and dependable critical infrastructures
- risk mitigation strategies and decision support for critical infrastructures
- critical infrastructure protection requirements by infrastructure operators and other stakeholders, economy and society
- ensuring reliable service delivery (continuity of services, business continuity)

A workshop for international cooperation and benchmarking will establish measures to compare mitigation and prevention approaches.

The ITCIP organization committee would be glad to welcome you to the ITCIP conference.

The conference is followed by a public IRRIS Workshop on the next morning, 6 September. Details will be announced soon on the IRRIS webpage ([www.irriis.eu](http://www.irriis.eu)) and the ITCIP webpage ([www.itcip.eu](http://www.itcip.eu)).

## Selected links and events

### Actual upcoming CIIP conferences mainly in Europe

- Fourth International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) in Lucerne, Switzerland on July 12-13, 2007 [www.dimva2007.org](http://www.dimva2007.org)
- ITCIP 2007 (Information Technology for Critical Infrastructure Protection), 4-5 September 2007, (Bonn, Germany), and Public IRRIS Workshop 6 September 2007, information at: [www.itcip.eu](http://www.itcip.eu)
- Call for Papers: CRITIS 2007, 2nd International Workshop on Critical Information Infrastructures Security, Benalmadena-Costa, Málaga, 3 – 5 October, 2007, <http://critis07.lcc.uma.es/>

### European or large projects with articles in this issue

- CRUTIAL Reference Architecture: <http://crutial.cesiricerca.it>
- Survey in 33 European Member and Associated States to build the ICT R&D portal: [www.portal.cistrana.org](http://www.portal.cistrana.org)
- CISTRANA website – project information, workshop reports and analyses: [www.cistrana.org](http://www.cistrana.org)
- [www.securitytaskforce.eu](http://www.securitytaskforce.eu)
- Mobile and Wireless Workshop report, 11/12th May, 2006:  
[http://www.securitytaskforce.org/dmdocuments/jointws\\_report\\_v1july0707\\_reportonly.pdf](http://www.securitytaskforce.org/dmdocuments/jointws_report_v1july0707_reportonly.pdf)
- Joint EU US Cyber Summit System Dependability & Security Workshop report, 14-16 November 2006:  
[http://www.securitytaskforce.org/dmdocuments/D2.4\\_Joint\\_EU\\_US\\_Cyber\\_Summit\\_WS\\_Report\\_V1.0.pdf](http://www.securitytaskforce.org/dmdocuments/D2.4_Joint_EU_US_Cyber_Summit_WS_Report_V1.0.pdf)
- CIIRCO [www.ci2rco.org](http://www.ci2rco.org)
- DESEREC: [www.deserec.eu](http://www.deserec.eu)
- SECOQC - Development of a Global Network for Secure Communication based on Quantum Cryptography  
[www.secoqc.net](http://www.secoqc.net)
- GRID <http://grid.jrc.it>
- NGI [www.nginfra.nl](http://www.nginfra.nl)
- Safeguard [www.stns.ch/Safeguard](http://www.stns.ch/Safeguard)
- CA Reliance <http://www.ca-reliance.org>
- IRRIS: [www.irriis.eu](http://www.irriis.eu)