



**FP7 Grant Agreement N° 312450**

## **CIPRNet**

**Critical Infrastructure Preparedness and Resilience Research Network**

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013

Duration: 48 months

### **D8.514 European CIIP Newsletter issues 16–18**

Due date of deliverable: 30/06/2014

Actual submission date: 08/07/2014

Revision: Draft version 1

**ACRIS GmbH (ACRIS)**

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Author(s)	Bernhard Hämmerli (ACRIS) Erich Rome (Fraunhofer)
Contributor(s)	

<b>Security Assessment</b>	<b>This deliverable is excluded from security assessment</b>
Approval Date	–
Remarks	See Annex I – DoW. All CIPRNet articles have been security assessed and received clearance.

The project CIPRNet has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

TABLE OF CONTENTS

**1 INTRODUCTION – RATIONALE OF THIS DOCUMENT..... 4**  
**2 REFERENCES ..... 4**  
**APPENDIX: ECN ISSUES 16 (VOL. 7, NO. 2), 17 (VOL. 8, NO. 1) AND 18 (VOL. 8, NO. 2) ..... 5**

## 1 Introduction – Rationale of this document

This deliverable contains the bundled issues 16, 17 and 18 of the European CIIP Newsletter (ECN). ECN issue 16 has been published on the CIPRNet website [CIPRNet] on 14.11.2013, issue 17 has been published on 27.3.2014, and issue 18 on July 8, 2014. All issues so far have also been distributed via the CIPRNet consortium's mailing lists.

## 2 References

[CIPRNet] FP7 NoE CIPRNet homepage: <http://www.ciprnet.eu/ecn.html>

## Appendix: ECN issues 16 (Vol. 7, No. 2), 17 (Vol. 8, No. 1) and 18 (Vol. 8, No. 2)

# European CIIP Newsletter

November 13 – February 14, Volume 7, Number 2

# ECN

## Contents:

Editorial: What is Smart?

The Smart Grid: First Steps  
into its Implementation

EU Project FACIES, CIPRNet &  
ERNICIP

CH: CIP Inventory; NL: Flood  
Management;

NO: Cross-sectorial Crisis  
Management

Smart Soft ID

Impact Analyses

CRITIS 2013 Report

CIP Background Information

Association: TIEMS IFIP WG11



**> About ECN**

ECN is coordinated with The European Commission, was initiated by Dr. Andrea Servida, today funded by the European Commission FP 7 CIP Research Net CIPRNet Project under contract, Ares(2013) 237254

**>For ECN registration ECN registration & de-registration:**

[www.ciip-newsletter.org](http://www.ciip-newsletter.org)

**>Articles to be published can be submitted to:**

[editor@ciip-newsletter.org](mailto:editor@ciip-newsletter.org)

**>Questions to the editors about articles 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:**

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

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

**>Founders and Editors**

Eyal Adar, Founder and CEO, WCK [www.wck-grc.com](http://www.wck-grc.com)  
Christina Alcaraz, University of Malaga, [alcaraz@lcc.uma.es](mailto:alcaraz@lcc.uma.es)  
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)  
Erich Rome, Fraunhofer, [erich.rome@iais.fraunhofer.de](mailto:erich.rome@iais.fraunhofer.de)

**>Country specific Editors**

For France: Michel Riguidel, ENST, [riguidel@enst.fr](mailto:riguidel@enst.fr)  
For Spain: Javier Lopez, UMA, [jlm@lcc.uma.es](mailto:jlm@lcc.uma.es)  
For Finland: Hannu Kari, HUT, [kari@tcs.hut.fi](mailto:kari@tcs.hut.fi)  
to be added, please report your interest

**> Spelling:**

British English is used except for US contributions

## Editorial

Intro	What is Smart? by Eric Luijff & Bernhard Haemmerli	5
-------	---	---

## US Contribution

Smart Grid	The Smart Grid: First Steps into its Implementation by Saifur Rahman	7
------------	---	---

## European Activities

Facies	Online identification of Failure and Attack on interdependent Critical InfrastructurES by Cristina Alcaraz and Javier Lopez	11
CIPRNet & ERNCIP	Testing Critical Infrastructure Protection: Gaps and Challenges by Christer Pursiainen	15

## Country Specific Issues

Switzerland: National CI tools	Swiss National CIP Programme: Establishing the CI Inventory by Stefan Brem	17
Netherlands	CIP and Flood Management by Annette Zijderveld, Thomas Bles and Micheline Hounjet	21
Norway	Cross-sectorial crisis management and the need for robust information services – a Norwegian perspective by Janne Hagen	25



## Method and Models

Smart ID	Soft Identities, the new challenge for the digital citizen by Igor Nai Fovino	27
Impact Analyses	Prediction to CI impact analyses in case of natural hazards by Vittorio Rosato	31

## About Associations

TIEMS	The International Emergency Management Society by K. Harald Drager	35
IFIP TC-11	IFIP TC-11's WG11.10 on Critical Infrastructure Protection by Yuko Murayama	49

## Books on C(I)IP

CRITIS 11 & 12 Proceedings	Are available for ordering: see links	No Page
----------------------------	---------------------------------------	---------

## CRITIS 2013 Conference

CRITIS 2013	CRITIS 2013: Conference Report by Eric Luijff	41
-------------	--	----

## Links

Where to find:	<ul style="list-style-type: none"><li>• Forthcoming conferences and workshops</li><li>• Recent conferences and workshops</li><li>• Exhibitions</li><li>• Project home pages</li><li>• Selected Download Material</li></ul>	43
----------------	--	----

# Editorial: What is Smart?

When discussing Smart Cities, Smart Grid, Smart Mobility and Smart everything, we have to reflect what this means in terms of investment and return. Which options for surveillance and Big Data applications are created? What is really desirable?

Originally, smart technologies comprised digitally enhanced functionality. It was easy to understand what was improved, as in watches the accuracy, in cars the injection, in elevators a clever plan to pick up persons and to accelerate and slow down smoothly.

Today we face an increasingly connected world. The potential for a global and better optimum is always present. However, counter-balances are – if existing at all - hardly considered today: borders of properties, interests, unwanted duplication of data, and decaying privacy are our future needs.

Smart Cities, Smart Mobility, Smart Grids, Smart Home, Smart Car, Smart Socks, Smart Leasing, Smart Configurator, Smart Roadster, Smart Market, Smart Portal, Smart Hotel... today it looks like everything is smart, and if you don't believe it, please double-check with the search engine of your choice.

This resembles the fairy-tale about a robe which is much softer than silk, so soft that you nearly cannot feel it. And this robe, which the smart tailor was in term to sew for the king had another property: only smart people can see the robe, all others don't see that robe at all ...

Smart technologies are wonderful tools to humankind. We have to explore these to understand how to use them in a way which serves us as human beings. With technology and our increasingly interconnected world, many applications and business cases are feasible today:

- We can track anybody's location. We can measure accurately any time how much one is driving and keep this information available for the insurance company. We can use the information to optimise the data traffic flow, to generate advertisements based on one's actual location, and keep all data stored for 20 years for forensic and other investigations. We can collect travel intentions and pool common interests.

- We can measure our consumption on calories, sorted to fat sugar and other ingredients for advising us what to eat, optimising our health, measuring our behaviour and providing that information to insurers. Additionally food distribution could be optimised world-wide.
- We can measure our consumption on energy (electricity, gas and oil) every minute to optimise the balance between supply and demand. Also, we can punish bad behaviour by dynamic pricing mechanisms or by switching off the supply. We can generate personal profiles and categorise individuals in different classes. Based on these classes we can develop new services such that the future need is covered in the best possible way.
- And please add your own visions, how we can make your and our world smarter ...

Reflecting on the above ideas and many additional ones, we can ask ourselves in which world we would like to live in the future? What is desirable? What are the hard boundaries we don't want to cross? Somewhere there is another optimum of smartness with which we are happy to live with.

In engineering, when building such a new smarter world, we have the responsibility to respect one's individual freedom and privacy including the option that we – as human beings – have the right to redefine ourselves according to our will. It is a fascinating time we live in, creating this new and smart world. But we should be careful to avoid ending up naked in front of everybody – just as the king in the fairy tale – without any privacy and self-determination.

As always, selected links – mostly derived from the articles – enhanced with some insider hints, events and exhibitions conclude this issue.

Enjoy reading this issue of the ECN!

*PS. Authors willing to contribute to future ECN issues are very welcome.*



**Eric Luijff**

is Principal Consultant Critical (Information) Infrastructure Protection and Cyber Operations at TNO, The Hague, The Netherlands.

e-mail: [eric.luijff@tno.nl](mailto:eric.luijff@tno.nl)



**Bernhard M. Hämmerli**

is Professor at Lucerne School of Engineering and Architecture and Gjøvik University, CEO of Acris GmbH and President of Swiss Informatics Society SI [www.s-i.ch](http://www.s-i.ch)

e-mail: [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)

He is ECN Editor in Chief

# **CRITIS 2014**

9<sup>th</sup> International Conference on  
Critical Information Infrastructures Security  
October 8-10, 2014, Limassol, Cyprus

[www.critis2014.org](http://www.critis2014.org)

call for papers soon available

(see last page)

# The Smart Grid: First Steps into its Implementation

Simplicity is key issue to reduce cost and engineering risk, when implementing smart grid. Additionally privacy of consumer is to be protected. A practical and cost-effective approach is presented

In today's power grid, with the penetration of renewable energy sources, distributed generation (including storage), and the expected introduction of plug-in electric vehicles (PEV), there is a growing need to balance the load and generation, and thereby alleviate the grid stress conditions. The smart grid – in its initial stages – can provide the necessary technology and sensing / control protocols to achieve the goal of selective load control known as demand response. However, before we talk about deploying the smart grid, let us try to understand what are the building blocks of the smart grid as shown in Figure 1?

At the top of the smart grid pyramid is technology, which is its most visible part. At the present time, the technology mostly exists to deploy the smart grid, if desired. However, for the smart grid to be practical and sustainable, there needs to be international standards such that the technology and software are interoperable allowing multiple vendors to develop its component parts which can be used anywhere in the world. This work is on-going and some standards exist today to deploy at least parts of the smart grid.

In order to incentivize the customer to take part in smart grid deployment, there needs to be rates and regulations to encourage them to do so. This work has just begun in the United States and some other countries, but needs a lot more focus. Since this requires a public debate and regulatory intervention, this is time consuming. Finally, the bottom layer – Consumer Awareness and Education – which is the foundation of any successful smart grid deployment needs a lot more attention. Because, if the consumer – the end user – is not aware and convinced of the benefits of the smart grid, no matter how much technology is developed, standards created and rates/regulations are put in place, the smart grid will not achieve the broad appeal necessary to make it practical. Having said this, let us now look at what benefits the smart grid can provide when deployed. The six most tangible benefits of the smart grid are:

- Renewables integration
- Peak load reduction
- Demand response application
- Remote meter reading & billing
- Transformer/Switchgear loading
- Service monitoring and recovery

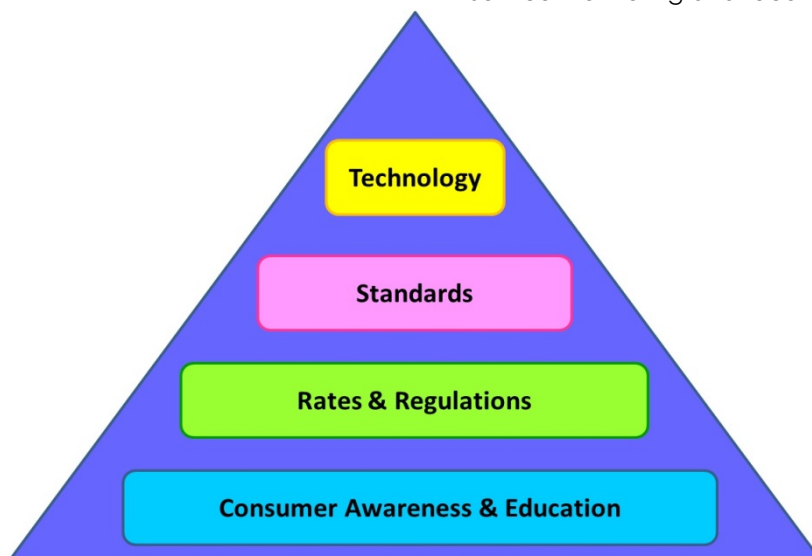


Fig. 1. Building blocks of the Smart Grid



## Saifur Rahman

is the Joseph R. Loring professor of electrical and computer engineering and the director of the Advanced Research Institute at Virginia Tech. He also directs the Centre for Energy and the Global Environment at the university. He is a Fellow of the IEEE, and an IEEE Millennium Medal winner. He is currently serving as the Vice President for Publications of the IEEE Power & Energy Society (PES) and a member of the PES Board of Governors. Dr. Rahman is the founding editor-in-chief of the IEEE Electrification Magazine. He is also a member-at-large of the IEEE-USA Energy Policy Committee. He is the general chair of the IEEE International Smart Grid Conference held annually in Washington DC. His research interests include alternate energy systems, smart grid, infrastructure studies, electric load forecasting and power system planning. He has authored over 300 technical papers in these areas.

email: [srahman@vt.edu](mailto:srahman@vt.edu)

As more and more intermittent sources of generation enter the electric power generation mix, the short-term unavailability of generation from these sources can cause supply disruptions resulting in partial loss of load. The smart grid – with its ability to control short-term load –

In the US 20% of the electricity-generation and vice versa of the load at demand side happens just over 5% of the time!

can provide the necessary load relief to match the generation intermittency. The same capability to control short-term load can also be used to reduce the peak load, which occurs very infrequently. But it is a challenge faced by all electric utilities throughout the world because of the heavy investment necessary to make generation available, when needed, however short-lived the load maybe. . For example,

- In the US 20% of the load happens 5% of the time ;
- In Australia 15% of the load happens less than 1% of the time;
- In Egypt 15% of the load happens 1% of the time;
- In Saudi Arabia 5% of the load happens 0.5% of the time.

With the United States having an installed generation capacity of approximately 1,000,000 megawatts,

if the 20% or 200,000 megawatts of generation capacity and associated transmission and distribution needs can be avoided – because it is only used 5% of the time - that will result in savings of over 300 billion US dollars. Now the question is – how to achieve this short-term load control. The current load control approach (i.e., Demand Side Management, DSM) - which is applied for air conditioner and electric water heater control – works as follows:

- During a power system stress condition, an electric utility sends control signals to shed selected commercial/residential loads.
- The problem is the customer has no control over the load curtailment even if this causes discomfort for them.

At Virginia Tech Advanced Research Institute we have developed a different approach that takes into account the customer convenience and preference by considering more appliances to control for shorter durations as presented below:

- A demand reduction request (kW) is sent by the electric utility to the individual residential/ commercial/ industrial customer through a customer interface device.
- The customer now has a choice and can decide which appliances to control and for how long based on their preference and load priority in order to meet the electric utility requirement.

The platform that has been developed provides algorithms and technologies needed for the customer to achieve their goal of energy conservation while meeting their priority and ensuring their privacy. This helps to encourage customers to participate in demand response programs. By utilizing

Customer data privacy is ensured by storing detailed customer usage data at customer premises under customer's control

such platform technologies, electric power utilities can offer their customers flexible choices of how much power to use and when to use it, all in real-time. These choices can be offered to customers at any time through communication between a substation and the Home Energy Management System (HEMS) at the customer premises as shown in figure 2 below.

The platform technology presented here is suitable for advanced demand response applications with load monitoring and control schemes for 240-V appliances useful for both improved off-peak energy sales, and reducing the peak load under stressed conditions of the power grid. The appliances available for control includes the electric water heater, electric clothes dryer, air conditioner, PEV (plug-in electric vehicle), etc.

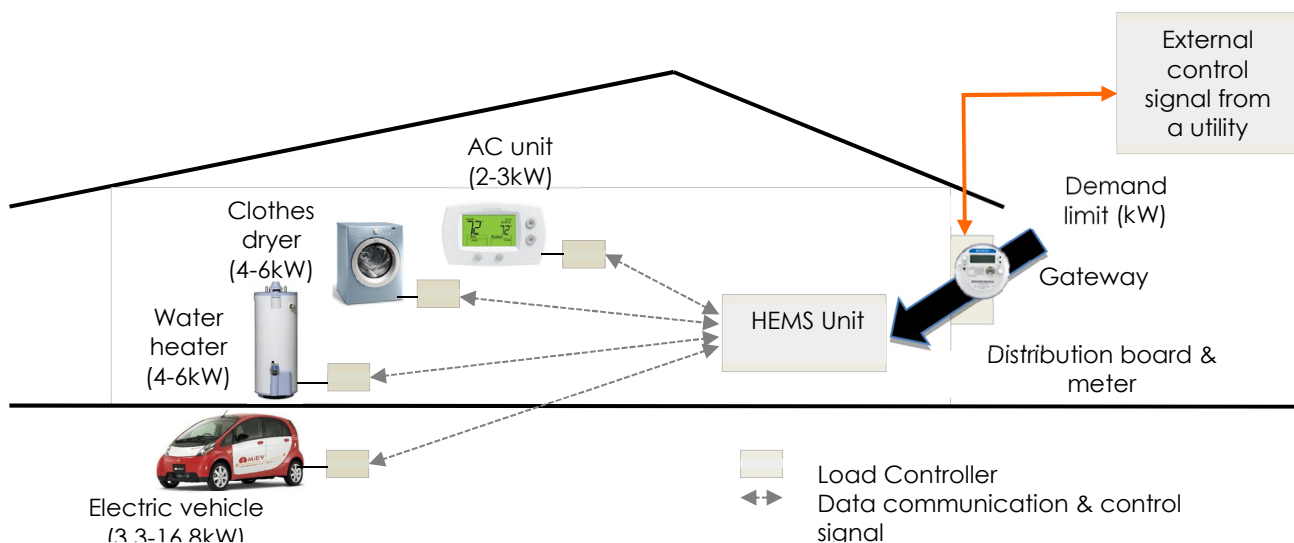


Fig. 2: Load Control Platform with Customer Choice

Since the 240-V appliances are more energy intensive (4 kW or higher), and are not considered critical loads, they can be controlled without causing much inconvenience to the end-user. For the customer, the demand response protocol and associated hardware designs enable intelligent energy conservation applications which are conducted in real-time. This provides them with choices while controlling their power usage, thus ensuring their comfort and privacy. This article targets this issue, and offers a technology solution to achieve this goal under the smart grid environment. Our research shows that in order to achieve this goal it is not necessary to have a smart meter at every house or apartment at the initial stages. The existing internet access - which is almost universal in the United States, western Europe and several other countries - provides the last mile connectivity necessary to achieve smart demand side control, or demand response. Rather than the electric utility sending the load control signal through the smart meter, it can be sent over the internet using web services.

The customer can receive this signal on their tablet device, smart phone, etc. With the electric utility control signal, the customer device can

Unidirectional communication over existing channels lowers cost, reduces complexity, and is by far cheaper to protect.

communicate with the home energy management system (HEMS) and execute the desired load control protocol as seen in fig. 2. There are other benefits of this approach as described below:

- Detailed customer usage data is stored at customer premises,
- Customer data privacy is ensured,
- Customer can pick and choose which appliances to control,
- Unidirectional communication with existing communication channels leads to lower investment and operational costs, reduction in complexity, and therefore lower deployment risk,
- This approach allows the citizen, the regulator, the electric utility and the business partner to gain experience with the smart grid and be convinced of its value without a large up-front investment.

## Additional Information and scientific documentation

Portal for Smart Grid: Information Collection and Archival:

### Smart Grid Information Clearinghouse

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

A commented power point presentation can be downloaded from:

<http://www.saifurrahman.org/sites/default/files/u2/CEPS%20Rahman.pptx>

This presentation plays 22 Minutes, and was presented at Centre for European Policy studies, September 18, 2013 at CEPS Digital Forum Task Force on Smart Grids building the business case for smart and sustainable energy in Europe.

(Left intentionally blank  
for double sided printing)

# FACIES: online identification of Failure and Attack on interdependent Critical InfrastructurES

FACIES aims to protect water treatment systems and their control systems against accidental or intentional incidents such as failures, anomalies and cyber-attacks with a particular emphasis on stealth attacks.

In September 2012, the European online identification of Failure and Attack on interdependent Critical InfrastructurES (FACIES) project was launched to find suitable methodological solutions for cyber and physical defence of Critical Infrastructures (CIs) in general. The project, funded by the European Commission's 7th Research Framework Program (FP7) within the prevention, preparedness and consequence management of terrorism and other security related risks program, highlights the current situation through a set of theoretical analyses and practical experimentation in a testbed.

The testbed, with a particular focus on water treatment systems and their control systems, exhibits how changes in specific CIs can seriously affect other interdependent infrastructures, such as energy systems, dams, market, environment or public health.

## Why the Water Sector?

Water systems are, in common with other critical systems, susceptible to adverse events that can have a dramatic impact on the safety of our society, its social welfare and economy, with a certain degree of emotional repercussion and distrust. Compromising the security of control systems and damaging the underlying infrastructure, is to indirectly attack social sensibility and to put on edge, governments, industries and citizens, who are the main consumers and beneficiaries of water supply. Therefore, they become the main end-victims of cyber or physical attacks.

According to the latest reports published by the Control System Cyber Emergency Response Team (ICS-CERT) in 2009 [1][2][3], the number of

incidents in the respective critical sectors has increased over the last few years. In the particular case of the water sector: 3 incidents were registered in 2009 with 33% compared to other sectors; 2 in 2010 with 4%; 81 in 2011 with 31%; 29 in 2012 with 15%; and this year 8 incidents with 4% in total.

Situational awareness consists of *"the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"*. R. Endsley, 1995.

The spread of a consequent effect depends on a set of factors: (i) scope of the effect measured in terms of geographical extension, loss or unavailability of assets and services; (ii) magnitude of the effect measured according to the degree of the effect or propagation towards other CIs; and (iii) restoration time, which is established, starting from the initial loss of an element until it regains its initial states, whilst preserving its essential properties. The effect on the water sector may not be, a priori, so shocking as a lack of electric power services, but the consequences can become equally drastic in time.

## Situational Awareness

Responses to hardware or software failures, anomalous perturbations or cyber-attacks can require information of a context to understand, at a high-level, what a domain and its infrastructures may be experimenting at a given moment [4]. This degree of knowledge can require the orchestration of small evidences related to the context, to interpret and illustrate a specific situation, such as



**Cristina Alcaraz**

C. Alcaraz is a Marie-Curie Postdoctoral Researcher on CIP at the NICS Lab. of the University of Malaga and at the Royal Holloway, University of London under the Marie-Curie COFUND programme "UMobility" co-financed by UMA and the EU 7th FP (GA 246550).

e-mail: [alcaraz@lcc.uma.es](mailto:alcaraz@lcc.uma.es)

URL: <https://www.nics.uma.es/alcaraz>



**Javier Lopez**

Prof. Lopez is Co-Editor in Chief of IJIS journal, and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.

e-mail: [jlml@lcc.uma.es](mailto:jlml@lcc.uma.es)



location, identity, physical events, time, etc. This information is generally perceived by sensory devices and massively managed by collectors, such as dedicated servers, remote terminal units/Programmable Logic Controllers (PLCs) or gateways.

However, the management of big data is not a trivial task. Depending on the context, the characteristics of such a context and its architectural complexities, it is necessary to carefully select some of the existing methodologies for detection of anomalies and intrusion. In any case, the solutions should be effective, rapid and lightweight since supervision and acquisition requirements cannot be sacrificed or violated at any time. This efficiency degree also means a trade-off between security and operational performance, which should also be questioned at this point and always.

An anomaly is something that deviates from what is standard or expected, and can become the evident symptom to watch for in unrecognized behaviour pattern prototypes, likely linked to specific cyber-attack sequences. Applying anomaly and intrusion detection techniques in critical contexts can become a challenge to be met, where a high degree of knowledge of the situation is needed to exhaustively or perhaps, partially explain a problem.

Most of these problems are primarily caused by deficiencies and vulnerabilities registered in the underlying system. Some common exposures to vulnerabilities in control systems are for example: incomplete or inefficient security policies and access control, deficient protection in the perimeter where security systems (e.g. firewalls or intrusion detection systems) are based on inaccurate rules/patterns, interoperability issues and conflicts, abuse and use of weak security credentials based on username-password with high visibility and low update using insecure cryptosystems, vulnerable TCP/IP-based protocols, implementation bugs, non-segregation of functions, interferences or industrial noise, strong dependence on third-parties' components, and so on.

Any failure or anomaly may open up breaches in security and bring about numerous security risks. Indeed, attackers may take advantage of a given situation to lead a set of non-

iterative or coordinated cyber-threats, such as: false injection, to falsify reading values/alarms, hide real values of signalization, manipulation of assets and configurations, memory corruption, denial of services, impersonation, etc.

Governance, best practices, recommendations, policies, maintenance, training, auditing, and accountability are certainly key elements to mitigate these cyber issues. Still, specification and commissioning of both methodologies and lightweight approaches, and the exploration of new research fields and technologies are also necessary. Investigation on situational awareness could for example complement the majority of these goals, becoming in itself a useful tool for prevention and mitigation.

## Stealth Attack and Mitigation

Being aware of stealth attacks and addressing topics of protection against them is nowadays a challenging exercise. A stealth attack consists of quietly operating a set of techniques to drive a set of malicious actions that compromise critical nodes with a low visibility. The attacker, capable of dynamically moving across the entire system, normally tries to hide evidence that can reveal his/her presence.

An example of precisely this type of threat was the Stuxnet worm in 2010. It was considered the first malware designed specifically for writing, reading and localizing critical sections in the PLCs of Siemens without leaving activity evidences. Although Stuxnet is a clear example of how to beat the system unnoticed, typical stealth attacks have, as their ultimate goal, the manipulation of the state estimation while preventing the control system from being warned of bad data.

Unmasking stealthy and invisible actions is consequently a difficult mission, but not impossible. For example, it is possible to protect a state estimator by applying cryptographic techniques (e.g. to encrypt the number of state variables) or correlation methods. Through FACIES we intend to address all of these cyber issues in addition to considering some other measures to quantify and qualify anomalies, compare physical and software

evidences, manage interdependencies, and quantify situations through weights. Obviously, defining patterns or schemes to ascertain the influence of stealthy actions can become a tricky job since it could require a prior learning phase to understand the context and classify normality settings.

Now that we have the right tools, it's time to learn to defend ourselves, validating defense solutions to face stealth attacks. The time is now. It's our time.

Differentiating a normal (but unrecognized) situation from an abnormal situation involves specifying boundaries/regions. Anomaly detection is an open research area that still faces many investigative problems, especially when it is applied to critical contexts to [5]:

- Appropriately manage high rates of false alarms; either false positives or false negatives.
- Define the concept of normality and adapt it to the application domain. In this case, in contexts related to water treatment and control.
- The normality concept can vary as these types of infrastructures generally work over long time periods.
- Differentiate between anomaly and noise so as to properly remove the noise from the data.
- Differentiate between causal anomalies and anomalies provoked by malicious actions.

Moreover, the prototypes of patterns are in the majority of cases unknown to staff members. They do normally know when and where to establish the limits of the normality concept, how in reality, to apply it, and why. The lack of knowledge of this can even hamper the training procedures and labelling that sometimes requiring an initial investigation to examine the context and determine where, when and how to establish the boundaries. This study could even require an analysis on levels of criticality associated with each subdomain, modelling or simulation of inter-dependencies, valorisation of architectural complexities and analysis of information so as to illustrate a general skeleton of the

context, thereby distinguishing a normal from an abnormal event.

## About Cyber-Physical Exercises in Testbed

In order to implement the objectives of FACIES and experiment with cyber-physical exercises to validate defence solutions, the University Campus Bio-Medico of Rome (UCBM) under the coordination of Professor Roberto Setola, has configured a testbed for FACIES (Figure 1).



Fig. 1: Testbed for FACIES

The testbed, based on four water tanks, a water reservoir, automatic and manual valves, pumps and (flow, pressure and level) sensors, is monitored 24/7 by a Prophecy HMI (Human-Machine Interface)/SCADA (Supervisory Control and Data Acquisition)-iFIX software, offering support to operate 200+ nodes. All the knowledge of the context is centralized in a Modicom M340 PLC, which is responsible for transferring commands from iFIX to valves/pumps, and collecting (flow, pressure and level) reading values from sensors.

Several cyber exercises on the testbed will principally focus on testing the robustness and resilience of the solutions against falsification attacks and integrity of data, availability of resources and stealth attacks, exploring the abilities of the testbed to detect intrusion, warn of the situation and self-heal to continue the services in the worst case scenario.

The FACIES Consortium is based on four partners, each of whom is entrusted with a particular task. For the physical part, those responsible are as follows:

- UCBM as the coordinator of the project and responsible for configuring and maintaining the testbed, in addition to addressing modelled, stealth attacks, and recovery.
- RadioLabs from Italy focuses on topics of analysis and evaluation of impact and consequences in highly interdependent systems, and fault detection.
- University of Cyprus (UCY) in charge of the modelling and simulation of interdependent networks, as well as the analysis of behaviours and impact.

For the cyber part, the entire Consortium heavily relies on:

- The Network, Information and Computer Security (NICS) Lab. at the University of Malaga (UMA) which is responsible for addressing cyber-threats, intrusion and anomaly detection, stealth attacks awareness, and reaction strategies.

For more information about the structure of FACIES, its Consortium, goals and technical documentation, please visit our website at <http://facies.dia.uniroma3.it>

## Are we going in the right direction?

Optimistically, we believe that the direction we are taking is correct, but somewhat pessimistically we also believe that there is still a long way to go. Support from governmental and industrial entities are essential to proceed with these types of practical exercises over the coming years. Ideally the scientific community should be encouraged to expand their research and learn more from these systems, exploring new technologies and exploiting existing/new research fields to evaluate protection measures. These fields could be for example controllability, observability, secure location privacy, trust management, reputation, prevention and reaction through dynamic and intelligent solutions.

The secret to us not deviating from the right path is to stay motivated, but in some way it is also necessary to feel that we are being supported.

Knowledge sharing and motivation are the means to keep on this path, where closer collaboration is, unfortunately, still needed. Trust is the secret to succeeding in overcoming a problem, but certainly this is impossible if such collaboration does not exist.

## References

- [1] U.S DHS, ICS-CERT, incident response summary report, 2009-2011, September 2011, <http://www.uscert.gov>, Last access on Sept., 2013.
- [2] U.S DHS, ICS-CERT, ICS-Monitor – Malware Infections in the Control Environment, Oct/Nov/Dec 2012. <http://www.uscert.gov>, Last access on Sept., 2013.
- [3] U.S DHS, ICS-CERT, ICS-Monitor – Brute Force Attacks on Internet-Facing Control Systems, June 2013, <http://www.uscert.gov>, Last access on Sept., 2013.
- [4] C. Alcaraz, and J. Lopez, Wide-Area Situational Awareness for Critical Infrastructure Protection, IEEE Computer, vol. 46, no. 4, pp. 30-37, 2013
- [5] V. Chandola, A. Banerjee and V. Kumar, Anomaly Detection: A Survey, ACM Computing Surveys, vol. 41, no. 3, Article 15, pp. 15-58, July 2009.

(Left intentionally blank  
for double sided printing)

# Testing Critical Infrastructure Protection: Gaps and Challenges

CIPRNet cooperates closely with other European projects. One of them is ERNCIP, which focuses on common test methodologies for technological security solutions

The Institute for the Protection and the Security of the Citizen of the Joint Research Centre (JRC) of the European Commission set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) project in 2009. This took place under the mandate of the DG Home, in the context of the European Programme for Critical Infrastructure Protection, and with the agreement of Member States.

Currently, manufacturers are often forced to test the security products separately for 28 markets in the EU.

The preparatory phase was successfully completed in November 2010 and the project started its implementation phase in February 2011.

## Why do we need common testing standards?

The specific mission of ERNCIP is to “foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities”. In order to achieve this, ERNCIP has two main approaches. First, it maintains an online inventory of laboratories in Europe, which are specialised in testing technological security solutions. Second, ERNCIP has created networks of experts to identify and promote good test practices to form the basis of common European testing standards, aiming at harmonisation of test methodologies and test protocols, where practical.

Why should we need common testing standards? This is important for two reasons. Firstly, harmonised

test methodologies and protocols throughout Europe will ensure that the security solutions will be properly tested across the EU, according to agreed-upon standards, leading to better and more reliable protection of critical infrastructures.

Secondly, harmonised test protocols are a prerequisite for a mutual acceptance scheme for security solutions, thus enhancing the development of the European security industry and security market and related standardisation efforts.

Currently this is usually not the case. Manufacturers and vendors are often forced to test and certify the security products separately even within the EU for 28 markets in national test laboratories, each following their own testing methodologies and requirements. This state of affairs is not satisfactory for Europe, being overly complex, time-consuming and costly. ERNCIP is thus working towards the goal that a security solution tested in one accredited European laboratory would be given market access to the whole European single market.

## Nine priority areas

Member States have identified some priority testing areas of concern for ERNCIP to address. Currently ERNCIP focuses on nine areas, which cover a wide range of subjects, some sector-specific, while others are cross-cutting.

The current thematic areas include the following: Aviation Security Detection Equipment; Explosives Detection Equipment in non-Aviation; Industrial Automation and Control Systems & Smart Grids; Structural Resistance against Seismic Risks; Resistance of Structures Against Explosion Effects; Chemical and Biological Risks to the Water Sector; Video Analytics and



**Christer Pursiainen**

Dr Pursiainen works at the EC's DG Joint Research Centre in Ispra, Italy. He coordinates the activities of the European Reference Network for Critical Infrastructure Protection and is a member of the CIPRNet Network Governing Body.

e-mail:  
[christer.pursiainen@jrc.ec.europa.eu](mailto:christer.pursiainen@jrc.ec.europa.eu)

Surveillance; Applied Biometrics for CIP; and Radiological and Nuclear Threats to Critical Infrastructure.

Each priority area is dealt with by a thematic group of nominated experts, representing mostly experimental facilities and laboratories but also other stakeholders such as manufacturers and vendors of security solutions, government authorities, academia, and operators of critical infrastructures.

There are only a few European laboratories that have experimental facilities that can work on explosives detection.

Currently, these ERNCIP thematic groups bring together over 180 stakeholders to address the specific problems of each priority area from the perspective of testing related security solutions.

## Explosive detection faces concerns

Let us look at the challenges of some fields in some detail. For instance, experimental work in explosive detection is linked to the national regulations on handling explosives, especially home-made explosives. The actual detection testing is therefore not the only aspect to be considered for testing of explosives detection equipment. Other aspects include preparation of explosives, characterization, and the safe storage of explosive products, which can be extremely dangerous in some cases.

These difficulties limit the number of laboratories involved in this area. Consequently, there are only a few European laboratories that have experimental facilities that can work on explosive detection.

However, the main concern in this field is more clearly related to the lack of regulations and standards, especially in a non-aviation context, rather than lack of testing infrastructure. There are laboratories working on trace detection, for instance, but no common protocols exist for the evaluation and certification of trace detectors. To be sure, the first studies in the field are in progress, but these are only

aimed at aviation security. Outside this area, no work has really been started. ERNCIP offers a platform to face this challenge.

## Water sector should be better prepared for incidents

Or let us consider another field that of chemical and biological risks in water sector. In general, organisational structures and scientific methods today provide a high level control mechanism on environmental water resources and on drinking water. There exist a number of national accredited laboratories, in all EU countries, to test water quality.

Furthermore, there exist also well-developed European regulatory frameworks to both protect environmental water resources from pollution and to guarantee a good chemical and ecological status of environmental water resources, as well as to set quality standards for drinking water at the tap. The regulations define rather carefully the normal substances permitted in drinking water as well as the list of known pollutants, such as heavy metals, and their acceptable limits.

Most laboratories cannot perform a rapid investigation of unknown pollutants in case of an incident.

What is then the problem? The current system is designed for long-term decision making and not for immediate response in case of an incident, caused by a malicious attack or natural or technological hazard. In other words, generally laboratories of the drinking water companies are specialized in routine analysis. The number of parameters analysed by such laboratories is established in accordance with the requirements of the legislation. Water operators and authorities are not interested in analytical methods for substances which are not included in national or EU regulations.

This is one of the reasons why most laboratories are not stimulated to develop respective methods and why they usually cannot perform a

rapid investigation of unknown pollutants, in case of an unexpected event.

However, there are technological solutions available. Innovative water quality monitoring systems, applicable in the event of an incident, have been developed in the last couple of years which allow for real-time control of the overall water quality. These systems react to a number of classes of contaminants and could warn operators and decision makers of potential contamination in the network immediately.

Yet, while several sensors already exist in the market, there is no EU standard approach available which sets out parameters for an overall assessment, thus helping avoiding false alarms and ensuring that the sensors are monitoring what they are meant for. Especially testing of sensors for drinking water and conditions for testing are not standardized yet. Again, this is a task that motivates ERNCIP to deal with the issue.

## Emerging technologies and the problems of data sharing

There are some emerging technologies such as video analytics and biometrics, which are increasingly applied to critical infrastructure protection. In some individual Member States and institutions, especially in the UK, France and Germany, there are considerable capabilities to this effect.

In these fields, specific test-datasets have been developed for the evaluation and validation of commercially available systems, in order to test and compare the applications. The 'European problem' here – a reason why ERNCIP is dealing with these thematic areas – is that the test-datasets are not standardised between the countries and test facilities. This naturally leads to a situation where a system tested in one country is not necessarily tested with the same parameters in another country.

One reason why this is so is that due to the nature of the content of these datasets – video pictures or biometric data of people – there are inhibitors to sharing the datasets

for privacy or other legal reasons. One possible solution, discussed within ERNCIP, is to share the datasets on a metadata level which would make it possible to establish a more harmonised test methodology in the EU within these fields.

## From radiation safety to detecting security risks

When we take a look at the field of radiological and nuclear safety, there are many experimental facilities and test laboratories in the EU. There are, however, only a few labs that have the capabilities and capacities for testing and qualifying technologies and methodologies related to radiological and nuclear security.

Yet technological development, combined with threats arising from security rather than safety concerns, are bringing about new challenges and also new gaps in experimental and testing capabilities.

For instance, in many test cases, high-activity radioactive sources are required. Obtaining them comes with the obligation of secure storage, handling, bookkeeping etc. Lending or moving them between institutes not always feasible. And while some detector manufacturing companies have their own (usually) nationally-accredited laboratories, seldom do they have strong metrological traceable sources in them; in these cases they have to rely on better equipped laboratories.

The testing facilities that the new security-driven developments demand especially concerning radiation detectors, are currently being built by some EU Member States as well as by the International Atomic Energy Agency and the European Commission's JRC.

The EU has recently contributed to making it possible for all EU Member States and their relevant stakeholders to have the necessary access to test facilities within the JRC's new laboratories, exclusively dedicated to face the current challenges in the field of radiation and nuclear security.

In general, one can conclude, however, that these gaps are well

identified and the processes dealing with them are in place. ERNCIP is contributing to this field by filling in the still remaining identified gaps.

## EU self-sufficiency or more international cooperation?

While focussing on the European-wide harmonisation of test methodologies is the current main task of ERNCIP, one of its goals is also to identify gaps in European CIP-related experimental and testing capabilities, such as lack of test infrastructure and know-how.

To this effect ERNCIP has made a survey through an anonymous online questionnaire, completed by 65 respondents representing different types of ERNCIP stakeholders. The survey revealed that while in some sectors the EU has developed impressive capabilities, it still appears to lack some experimental and test capabilities in the field of technological security solutions.

Europe still appears to lack some experimental and test capabilities in the field of technological security solutions.

In some cases manufacturers or operators have to turn to non-EU facilities, most notably to the US big laboratories, to have those tests made they need. In the field of explosives detection, for instance, it may be a question of larger explosive limits in non-EU countries or lack in testing EU facilities on home-made explosives.

The question then is whether the EU should enhance its testing capabilities, striving for self-sufficiency, or whether it should continue to rely on international cooperation in those fields where it does not have enough capabilities. From ERNCIP point of view, the answer is 'both'. While more focussed approach towards European capability building is needed, one should also enhance international cooperation, especially with the US, which in many fields of testing security solutions is ahead of Europe. Emphasis for

greater cooperation should be placed on security areas that require a particularly high degree of international cooperation.

However, for the most critical security technologies, and also for technologies where requirements in Europe are different, the EU should consider an indigenous competitive capability, even if this involves duplication of US capabilities. For more information on ERNCIP:

<http://ipsc.jrc.ec.europa.eu/index.php/ERNCIP/688/0/>

(Left intentionally blank  
for double sided printing)

# Swiss National CIP Programme: Establishing the CI Inventory

Based on previous methodological research and practical experience, Switzerland has established a national inventory covering specific critical infrastructure objects from its 28 critical sub-sectors.

With the Federal Council's approval of the national strategy to protect Switzerland's critical infrastructure (CIP strategy) in June 2012, the establishment and further development of a CI inventory has become a crucial cornerstone in the national CIP programme. Already in 2009, Switzerland has for the first time prioritised its critical infrastructure sub-sectors. Based on this experience and further methodological developments, it was possible to establish a CI inventory from a national perspective by the end of 2012. The classified results from this process are used for various prioritisation and preparation planning activities and are currently supplemented by Cantonal, i.e. sub-national, applications of the methodology.

## Short review of sub-sector criticality

As an important starting point, it was crucial not only to identify the critical infrastructure sectors and sub-sectors on the national level, but also to establish a methodology to prioritize them from a rather generic national

perspective. This allowed for more specific and dedicated analysis in the prioritised critical sub-sectors.

“The main benefit of the inventory is its role in the prioritisation process. As one saying goes: “if you try to protect everything you will end up protecting nothing”

The methodology of the sub-sector criticality considered three main components: the (inter-) dependencies between the critical sub-sectors, the consequences of a loss of service of the respective sub-sector on the population, and the consequences of a loss of service of the respective sub-sector on the economy.

In the dependency analysis both the number of connections between the subsectors, but also their “strength” was assessed. The population impact both included the assessment of the rough number of people affected, but also the seriousness of affectedness (from no disruption of daily life to serious disruption of daily life including deaths and injuries).



**Stefan Brem**

Dr. Stefan Brem has joined the Federal Office for Civil Protection within the Swiss Federal Department of Defense, Civil Protection and Sport in March 2007, where he leads the section on Risk Analysis and Research Coordination. His unit is responsible for the national programme on Critical Infrastructure Protection (CIP) and the disaster risk assessments on the national and Cantonal level. Prior to his current position he served for four years at the Federal Department of Foreign Affairs' Centre for International Security Policy where he was responsible inter alia for CIP, Energy Security, Security Sector Reform, Border Security and Private Military Companies. He completed his dissertation in Political Science with the University of Zurich in 2003.

e-mail: [stefan.brem\[at\]babs.admin.ch](mailto:stefan.brem[at]babs.admin.ch)

Very high criticality	High criticality		Normal criticality
Banks	Air transport	Chemical & pharmaceutical industry	Army
Information technology	Food supply	Insurance companies	Emergency services
Oil Supply	Medical care and hospitals	Natural gas supply	Fluvial transport
Power supply	Parliament, government, justice, administration	Protection and support service	Dipl. representations and hq of international organ.
Rail transport	Postal services	Media	Laboratories
Road transport	Waste water management	Waste management	Machine, electro & metal industry
Telecommunication	10 critical sectors and 28 critical subsectors		Cultural assets
Water supply			Research institutes

- All subsectors are critical // Criticality ≠ absolute importance
- Normal critical subsectors can contain highly critical elements
- Weighting is based on an ordinary threat level



The economic impact, finally, included both the direct economic consequences of a loss of service in the sub-sector itself, but also ripple effects in the dependent sub-sectors.

The results of this first criticality assessment were also included in the basis CIP strategy and approved by the Federal Council in July 2009.

## From sub-sector to object level criticality

In order to not only identify and prioritise the critical infrastructure sub-sectors, but also the specific critical objects, the methodology was further refined and incrementally applied.

The refined methodology includes four steps on the national level.

As a first step, in every of the 28 sub-sectors, a functional mapping highlights the critical processes and "supply chains" of the critical goods and/or services to be produced, managed, stored, distributed (etc.) in the respective sub-sector. On a generic level, the functional mappings include a branch related to the production of the critical good and/or service, process management, task management (incl. crisis management), logistics, R&D, governance.

Based on this mapping, the relevant object groups such as power plants, substations, data centres, train stations, airports etc. are determined in a second step. In a third step, the related threshold levels are defined for every relevant object group previously determined. The methodology in Switzerland differentiates between five levels – from a local level relevant to a municipality up to a national/international level.

In a fourth step, the individual CI objects are compiled and evaluated by their individual output potential (both quantitatively and qualitatively) and hazard potential (for example dams and chemical facilities).

The methodology is compatible with the EU approach, but its focus lies on national importance rather than cross-border effects. Nevertheless, the CI Inventory also considers international aspects.

## Collaboration with CI operators

The Federal Office for Civil Protection (FOCP), which bears the overall responsibility for the national CIP Programme in Switzerland, has developed the methodology and also steered the identification process leading to the CI Inventory.

The FOCP closely worked together with the federal lead agencies of the respective sub-sector, such as the Federal Office of Energy in the area of power supply, for example. Additional federal and Cantonal agencies were included as well as the leading national provider association and the main CI operators and owners of the respective critical sub-sector.

The identification process was launched incrementally in the individual sub-sectors to better include the relevant actors and to further improve the methodology. Overall, however, the methodology proved to be very systematic and pragmatic as it provided reasonable guidance to conduct the identification process in all of the 28 sub-sectors as diverse as cultural assets, fluvial transport, oil supply, and waste management, just to mention four of them.

## Main application of the inventory

The inventory has become a recognised instrument with the CI operators and public agencies for further planning and prioritization activities in the area risk and disaster management. In that respect, it serves preventive as well as preparedness and reactive tasks, including strategic business continuity management.

More particularly, the classified information is shared with trusted partners as appropriate to conduct more specific vulnerability assessments, to

support the prioritisation process in the context of the national economic supply and other federal resources, to support CI operator specific planning activities and CIP activities by the Cantons – to name just a few.

The Cantons are currently also invited to include the findings from the national level in their Cantonal risk and disaster management processes and to complement the national inventory with their Cantonal CI objects.

Even if the CI inventory currently includes specific objects only, it also considers the underlying processes and supply chains. This further increases its value as a planning tool in the context of strategic business continuity and resource management.

## The way forward

By the end of 2012, the CI Inventory was for the first time assembled with the newly established methodology. Currently, the Cantons – as described above – are invited to complement the national inventory. The inventory will be regularly updated with new relevant information and will be thoroughly reviewed every four years.

By then, it will also be fully integrated in the various prioritisation and preparation planning activities. Given the current and on-going discussions on cyber security, data protection and integrity remain high priorities when it comes to data sharing. Finding the right balance between information sharing with relevant partners and – at the same time – protecting sensitive information continues to remain high on the agenda.

## Further information

If you would like to find out more about the Swiss national CIP programme please visit our website at [www.infraprotection.ch](http://www.infraprotection.ch) or Email: [ski\[at\]babs.admin.ch](mailto:ski[at]babs.admin.ch)

# CIP and Flood Management

The Netherlands is a country that is wedged between the large rivers Rhine, Meuse and Scheldt entering the country and the North Sea. As roughly half of the country is below sea level, it is no wonder that CIP is high on the agenda in relation to flooding

In this article we will provide some insight into research and developments in the Netherlands related to CIP and flooding. In the following, examples are given regarding various phases of the disaster management cycle: prevention, preparation and response.

## Prevention - Blue Spots in the Dutch Highway Network

Rijkswaterstaat is the executive arm of the Dutch Ministry of Infrastructure and the Environment which is responsible for the design, construction, management and maintenance of the main infrastructure networks in the Netherlands.

Rijkswaterstaat commissioned a study to identify the vulnerable spots to flooding in the Dutch National Highway Network, the so-called blue spots.

Blue spots are considered the main climate change risk for the Dutch road system which is of great importance to the economy of the country. The RIMAROCC method (Risk Management for Roads in a Changing Climate) was used to establish a risk driven approach to this problem.

Based on different climate change scenarios and using numerical simulations, predictions could be made to determine flood extents, changes in the groundwater regimes and changes in land subsidence. The results were visualised on maps of the Netherlands having the following added value for the stakeholders:

- The identification of areas that, even in the worst scenarios, are not at risk to climate change.
- No-regret measures that can be directly implemented.
- The information provided is the basis for the development of adaptation strategies to deal with climate change, such as mitigating measures, adaptation

of technical design guidelines and cost/benefit analyses.

At this moment Deltares is leading a consortium carrying out a climate adaptation study for the trans-European transport network (TEN-T). ROADAPT (Roads for today, adapted for tomorrow) is funded by the Conference of European Directors of Roads (CEDR).



## Preparedness - Critical Infrastructure in a low lying country

The Netherlands has always been exposed to flood danger both from the sea and the rivers. After many tragic flooding events and the 1953 flood in particular, Dutch authorities increased the protection level over the last decades substantially: large barriers have been built, dykes and levees are designed to withstand flood events with a statistical return periods of up to ten thousand years. This policy is based on the ambition to protect the Dutch citizen as well as the large amount of critical infrastructure in these areas.

After the flooding of Rhine and Meuse in 1993 and 1995 respectively, a new idea grew slowly, but steadily in the mind of the Dutch water authorities: we cannot guarantee complete safety, no matter how high we will set the protection levels.



**Dr ir Annette Zijderveld**

Annette is department head for Hydrodynamics and Operational Systems at Deltares, Delft, The Netherlands

phone: + 31 88 335 8259  
e-mail: [annette.zijderveld@deltares.nl](mailto:annette.zijderveld@deltares.nl)



**Ir Thomas Bles**

Thomas Bles is specialist consultant Geo Engineering at Deltares, Delft, The Netherlands

e-mail: [thomas.bles@deltares.nl](mailto:thomas.bles@deltares.nl)



**Ir Micheline Hounjet**

Micheline Hounjet is specialist consultant flood management at Deltares, Delft, The Netherlands

e-mail: [micheline.hounjet@deltares.nl](mailto:micheline.hounjet@deltares.nl)

Economic flexibility and the necessity to combine different kinds of land use in highly populated areas need new ways of dealing with this problem. While protection levels shown in Figure 1 are still in place Rijkswaterstaat under the Ministry of Infrastructure and the Environment and the Dutch water boards increased the efforts for a proper response system. Modern forecasting systems produce accurate and reliable flood predictions of all main waters at all times, and for all areas. In the last 5 years, all operational forecasting systems for flood fore-

operators at the Afsluitdijk sea barrier. See Fig. 1.

The integrated information system enables a fast and comprehensive countrywide overview of the flood threat at a given time. This overview is used by regional disaster management teams as well as the Ministry of Infrastructure and Environment to coordinate their efforts. The Water Management Centre has recently opened their new Control Room in Lelystad, where the system is hosted; obviously in a flood-proof environment above sea level as this system

still on the drawing table, but it is expected to be implemented in the Dutch disaster management organization over the following years.

## Emergency Response – how can we protect critical infrastructure during a flood?

Obviously critical infrastructure is designed to withstand threats such as flooding in line with standards set for such conditions. However, 100% protection is not possible from an economic as well as technical perspective. Preparations are therefore needed to have a robust set of emergency measures timely in place. These typically relate to monitoring systems, forecasting systems, warning systems and response measures. Regarding the latter, response measures in the case of flooding can be divided into the following categories: water level lowering measures (e.g. diversion of flow, storage of excess water in less harmful areas), flood defence measures (e.g. higher, stronger) and measures related to minimizing damages (e.g. water proofing, isolation, evacuation). Which measures are effective is very much case specific, depending very much on the type of infrastructure, physical conditions and the magnitude (and certainty) of the threat.

## 24/7 National Emergency Response Service

The Ministry of Infrastructure and Environment have an ongoing agreement with Deltares to provide advice during an emergency. A so-called Core Team member is 24-7 contactable and in line with the contractual obligations with the Ministry must be able to mobilise a team of experts to provide specialist advice within 24 hours of receiving the request to mobilise. In total some 120 staff can be called upon to provide their input, covering a broad range of areas such as infrastructure, floods and drought, environment, and subsoil and groundwater. Every year two

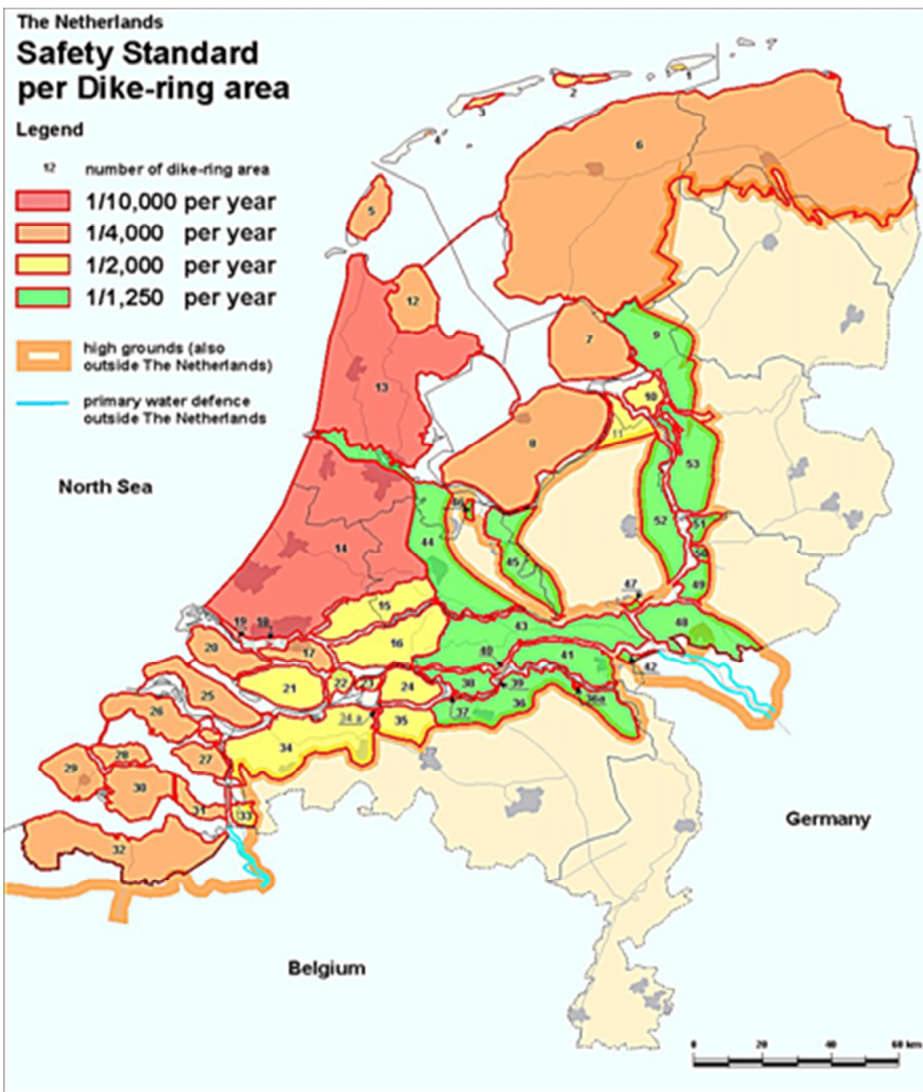


Fig. 1: Protection levels / safety standards

casting have been migrated to one software platform (based on Delft-FEWS), in order to ensure high quality, robustness and flexibility in the information chain: River discharge information is directly coupled with water level forecasting in the estuaries, surge information at the Wadden Sea is available for barrier

too is part of our critical infrastructure! See Fig. 2.

The time that is gained with these new tools and procedures also enables us to look at different possible scenarios of the impact on critical infrastructure and, more important, which measures could be taken to prevent unwanted cascading effects. These studies are

exercises are carried out to test the Deltares team and to ensure Deltares meets requirements regarding mobilisation time, effective crisis management and sound technical advice. Since its establishment in 2008, the Ministry has had three real events that sparked the emergency response service: the failure of the Vlakte tunnel (2011), the severe drought that hit the Netherlands (2011) and the failure of a NAFTA pipeline near the Juliana Channel dike (2013).

on Floods. Their job is to check whether local problems might result in regional or even national problems. If this is the case, they can ask the Deltares Team for help. For this exercise a potential dike breach can cause a flood in one part of the Water Board area. Because of differences in water levels and dike heights, this potentially threatens an equally large area of another Water Board and a flood will endanger at least two medium-sized cities. Given this threat it is important to assess

see how they will communicate about the severity and the possible actions.

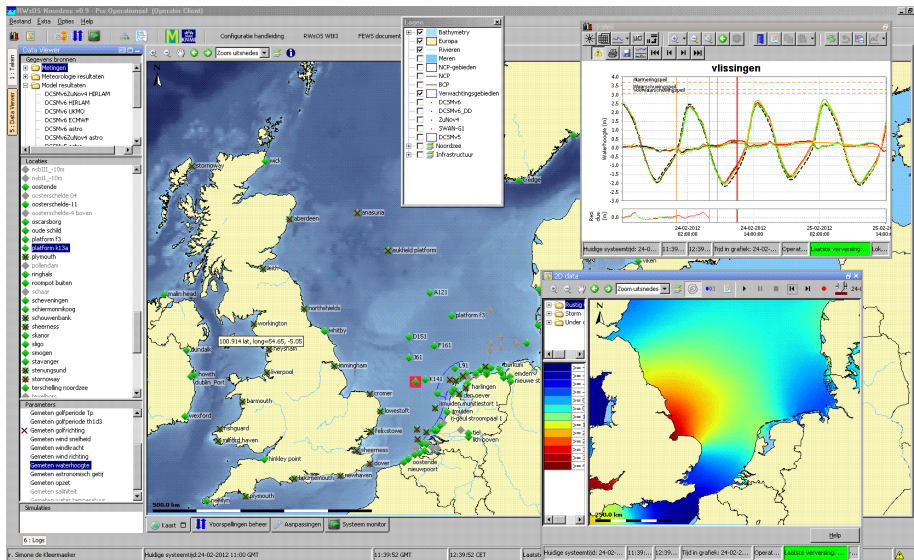


Fig. 2: North Sea forecasting system

## Exercise aimed at protection of critical infrastructure

In December 2013 an exercise aimed at emergency response will be carried out involving three teams: the National Coordination Centre on Floods, a Water Board and the Deltares Team. For each of the teams specific learning objectives have been defined. The script for the scenario has been drafted specifically for the exercise. This particular exercise will focus on the flooding involving the rivers Rhine and Meuse and its (potential) impact on vital infrastructure, in particular a railway connecting Rotterdam with Germany and a highway tunnel.

In the scenario, the Water Board will monitor dike conditions (and failures!) within their area and will register potential problems in so-called situational reports. These reports provide valuable input for the National Coordination Centre

the amount of time that is left once the dike breaches and which options are open for evacuation.

The Deltares Team will only have a few hours to answer questions on the impact of the potential flood, the direction the water will flow, the velocity of the flooding and flood water levels. Also the impact of the water levels on the stability of road and railway embankments and the impact of high groundwater levels on the stability of tunnels will need to be assessed in short period of time.

The Deltares advice should be as comprehensible as possible and right on time as the National Coordination Centre on Floods will use it in their advice to the Water Boards, the Minister and other flood management organisations. One of the objectives of the exercise is to find out how the advice is interpreted by the Water Board. This will be assessed by also requiring the Water Board to carry out a press conference about the situation and

(Left intentionally blank  
for double sided printing)

# Cross-sectorial crisis management and the need for robust information services – a Norwegian perspective

Since 2012, the CIP research at the Norwegian Defence Research Establishment (FFI) has focused on the digitalised society, its vulnerabilities to military information operations and the need for robust information services and information sharing between civilian and military authorities

The Norwegian Defence Research Establishment (FFI) is the prime institution responsible for defence-related research in Norway. It is also the chief adviser on defence-related science and technology to the Ministry of Defence and the Norwegian Armed Forces' military organisation.

## International Cooperation

FFI collaborates with a number of national and international scientific institutions and industry. It leads and participates in several EU projects within EU's Seventh Framework Programme (FP 7) Security addressing protection against electromagnetic threats (HIPOW), learning from handling natural disasters (ELITE) and

According to the Norwegian Computer Crime Survey 2012 the businesses' dependency on Internet services is critical; many will struggle after just a few hours of shutdown.

protection against chemical and biological threats through preparedness and resilience against CBRN terrorism using integrated concepts and equipment (PRACTISE) and two stage rapid biological surveillance and alarm system for airborne threats (TWOBIAS). FFI is also conducting research on CIP. This work has contributed to White Papers and delivered comprehensive and holistic vulnerability and emergency preparedness studies on different sectors, including the telecommunication sector, the electric power supply sector and the critical ICT systems.

Existing emergency preparedness regimes are partly based on the outcome of this research. Since 2012, Critical Information Infrastructure Protection (CIIP) research at FFI has been directed towards the digitalised society, its vulnerabilities to military information operations and civil and military public authorities' need for robust information services and information sharing.

## The Internet has become critical information infrastructure

In Norway, it is a political priority to bring the Internet to the people and build high capacity fibre optic networks, encourage ICT innovation and modernizing of the public sector through digitalisation. It is the ambition of authorities to interact with the citizens on digital platforms including social media. Already in primary school, Norwegian children are offered IT courses, and IT has turned into a skill to be acquired along the same lines as reading, writing and math. Society sectors like banking, power supply, transportation etc. are all highly dependent on electronic infrastructures and the Internet. As a result, the Internet has become one of the most critical of infrastructures to Norwegian citizens, public sector and enterprises. Everyone uses the Internet, and according to the Norwegian Computer Crime Survey 2012 the businesses' dependency on Internet services is critical; many will struggle after just a few hours of shutdown. At the very beginning of the Internet revolution, none could have foreseen such a development with increasing digital vulnerabilities, threats of espionage, hacking and social engineering.



Foto: FFI

## Janne Hagen

Dr. Janne Hagen is a principal scientist working at the Norwegian Defence Research Establishment. She received her MSc degree in industrial economy from the University of Linköping in 1989 and her PhD in information security in 2009. She has been working at different research institutions, and conducted research on emergency preparedness and critical infrastructure protection at FFI since 1996. In 2008-2009 she was a visiting Fulbright scholar at Naval Postgraduate School, Computer Science Department in Monterey. In 2010 she received the ITAKT award from the Norwegian telecom industry for her work on civil emergency preparedness for the telecom sector.

e-mail: [janne.hagen@ffi.no](mailto:janne.hagen@ffi.no)

## The threat from Information Operations (InfoOps)

The fact that Internet services are disseminated throughout the whole society makes the society and the population particularly vulnerable in the area of information operations - InfoOps (i.e. targeted influence activities performed by adversaries' by the use of PsyOps, deception, logical attacks, physical attacks on infrastructure etc.). Recent conflicts in Gaza and northern Africa have reminded us that Internet infrastructure and services are true military targets in conflicts. We have also witnessed

Recent conflicts in Gaza and northern Africa have reminded us that Internet infrastructure and services are true military targets in conflicts. This quote is picked from the paragraph "The threat from Information Operations (InfoOps).

social media being manipulated, aimed at deceiving different target audiences. If you add to this closing down the Internet, performing physical attacks on electric power supply and communication and broadcasting infrastructures with the goal of preventing communication and information exchange, society is paralysed. Yet, in discussions related to CIIP and emergency preparedness, the attention seems to be almost exclusively on cyber threats, which seem to be the biggest concern. If however civil society is attacked by an adversary utilising the full potential of InfoOps, i.e. attacking the physical domain, as well as the social and cognitive domain, including using cyber means, the big question is this: how can the authorities mitigate the threat of an InfoOps attack and, in the worst case, manage such a crisis?

## The Norwegian approach of civil and military emergency preparedness cooperation

The Norwegian Government's policy on national emergency prepared-

ness is based on the following concept of civil-military cooperation: if a disaster or military conflict occurs, all required civilian and military resources are mobilised. The responsibility for crisis management is shared between various Ministries and the associated subordinate public agencies. Public sector crisis management is founded on the following principles: events should be handled by the local authorities as far as practically possible; responsibility, liability and organisational structures within crisis operations should correspond to structures and responsibilities in every day-to-day work; and due to the complexity of crisis situations and the interdependencies of the tasks and problems, collaboration and coordination within and across involved authorities is required. The concept involves public-private partnership and cooperation, which is of critical importance. When it comes to ICT, it is the private sector that possesses the important resources and key knowledge.

## Research challenges on the need for robust information services

Cross-government collaboration in crisis and risk perception among authorities is challenging. First, communication and information collection depends on functions, information services and (critical) infrastructures, such as electricity supply or transportation. Only infrastructures which function efficiently can enable cross-government communication and collaboration. Second, related to this dependency are restrictions stipulated by law. Many pieces of information may be sensitive due to privacy, business strategy or national security concerns. Finally, as documented in several CIP projects, Norwegian information infrastructures are vulnerable.

To sum up, if Norway should ever be subject to an InfoOps attack including physical, logical and social means, then the probability that some information services will not work, or that some information is not reliable or available, would be quite high. The question that arises is this: What can the government do about it?

All these years of researching by FFI have revealed that availability and

integrity of information services are of critical importance. Ideally, the information services should withstand continuous threats posed by nature and humans, and systems and services should be operational for the users despite being under attack. This is what we define as robustness. There is a need for building a digital emergency preparedness that goes beyond the function of Computer Emergency Response Teams (CERTs) and that also covers the cognitive and social domain. We are not there yet. There is also a need for improved cross-sectorial situational awareness and a capability for quick response. This can be achieved inter alia by better information sharing across sectors, though this approach also has its drawback: If the integrity is compromised, then integrity might be compromised across interconnected sectors. However, building ICT systems that enable secured cross-sectorial information sharing will not be sufficient for a rapid reaction. Organisational changes may also be required since conventional bureaucracy might work too slowly. Short-cuts or flat decision structures might be demanded. There is probably no perfect solution, so a major research challenge is to find a sustainable one. FFI will continue to address this challenge in its research.

If you would like to find out more about FFI's research please visit our

website at [www.ffi.no](http://www.ffi.no)  
email: [firmapost@ffi.no](mailto:firmapost@ffi.no)

# Soft Identities, the new challenge for digital citizen

Digital Identities – soft- and strong identities - are keys for the future of Critical Infrastructure. Additionally, means to control and regulate the use of the sensitive information must be given to citizen for privacy reasons.

The role of identity is extremely important in our society. On the basis of our identities we are allowed or denied to perform every day vital operations.

From a philosophical point of view, the identity is the key of every human interaction. We adapt the interaction with a person on the basis of an evaluation of his identity and the surrounding context.

We accept to execute tasks on the basis of the identity of the person requiring that task; we trust on information obtained on the basis of the identity of the information source.

Traditionally the evaluation of the identity of a person involves information related to:

1. What we know about this person
2. What we see and feel about this person
3. What others say about this person (being the "others" provided with some level of trust)

Within the whole "game" of evaluating an identity, establishing a level of trust and acting in consequence, a strong role is played by the possibility of physically verification that the counterpart is with whom we are interacting.

In the digital world, on the other hand, human interactions are indeed extremely limited and the identity evaluation relies obviously less on point (2) and more on points (1) and (3).



**Igor Nai Fovino**

holds a Ph.D. in computer science from the University of Milan. He has deep knowledge in the fields of ICT Security of industrial critical infrastructure, Risk Assessment methodologies, Intrusion Detection Techniques, Secure Network Protocols and Privacy preserving techniques in the cloud. He is author of more than 60 scientific papers; moreover, he serves as reviewer for several international journals in the ICT security field. During his career Igor worked as contractual researcher at the University of Milano in the field of privacy preserving data-mining and computer security and as contractual professor of Operating Systems at the University of Insubria. 2005 - 2011 he served as Scientific Officer at the Joint Research Centre of the European Commission and 2011 - 2013 as Head of the Research Division of the Global Cyber Security Center. From 2013 Igor Nai Fovino serves as scientific project manager of the EU Commission's Joint Research Center.

email: [igor.nai@jrc.it](mailto:igor.nai@jrc.it)

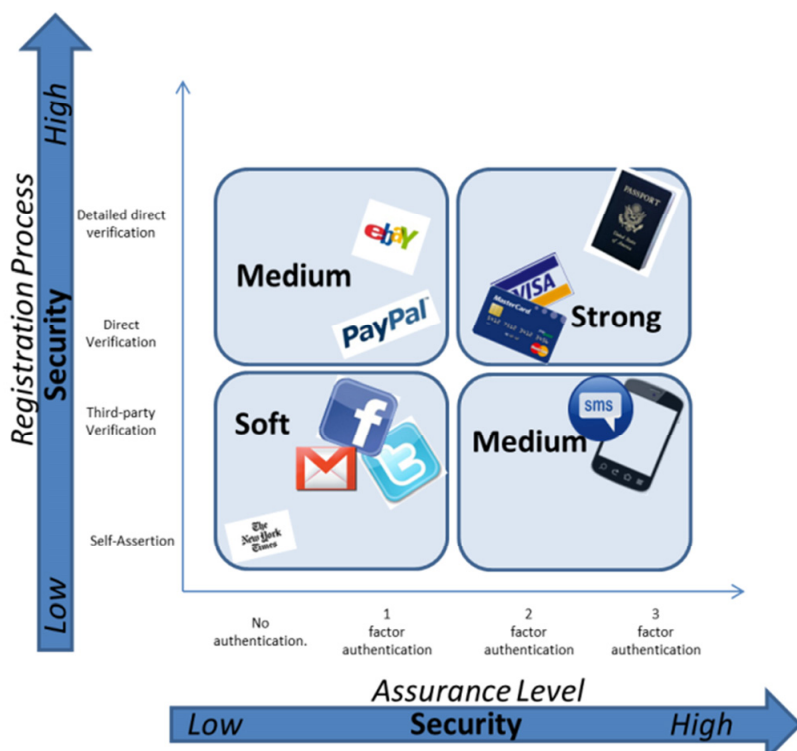


Fig. 1: Classification of Identities according to their assurance level and registration process



According to the standard ISO/IEC 24760 (part 1), a digital identity is defined as "a set of attributes related to an entity", where entity refers to an individual, an organisation, or a device. Attributes are properties of the entity (e.g. address, phone number etc.).

Digital identities can be categorized according to the security level adopted in the registration and authentication phases, i.e. when a digital identity is associated to a target entity. So we can have Hard and Soft electronic identity (e-id).

"We accept to execute tasks on the basis of the electronic identity on behalf a person;

We trust information based on electronic identities."

In our digital society, the concept of digital identity is becoming more and more relevant and in fact, the section 2.1.2 of the "Digital Agenda for Europe" makes an explicit reference to digital identities:

"Electronic identity (eID) technologies and authentication services are essential for transactions on the Internet both in the private and public sectors. [...] As there will be many solutions, industry, supported by policy actions – in particular eGovernment services - should ensure interoperability based on standards and open development platforms".

The problem is that, outside the realm of the so called Strong-eID (e.g. electronic ID cards), the average citizen does not pay enough attention to his digital identity, and, in several cases, he is not even aware of possessing one, or, more commonly, multiple identities.

An e-mail account is a digital identity, the account I use to write on a forum is a digital identity as well as Facebook, Dropbox, Twitter, and Paypal accounts are.

The fact is that a single format for our online identities does not exist, as a set of unified procedures regulating their protection and management is not defined. As spe-

cified in ISO/IEC 24760, everything which can be used to identify myself online in a unique manner is, per se, a digital identity.

## Digital Identity in the IoT and Smart World

The digital identity definition has been extended recently with a sort of "inheritance principle".

Citizens are starting to make massively use of smart-devices and smart-sensors which are connected to the Internet.

To get access to online services they need to configure their devices using their own credentials, giving to these devices rights to operate in their name.

"The management of electronic identities, the way in which they are protected and revoked – if needed - should and must be one of the top priorities for the security of a critical infrastructure."

Let take as example a smart-TV: the citizen, to download and see content should provide to the smart-TV a mean to authenticate itself to the online services. Typically, the authentication will imply the use of some sort of digital-identity linked to the owner of the TV-subscription; in other words, the smart-TV inherits a "portion" of the identity of its owner. The same situation happens when for example the citizen configures his mobile-phone to get synchronized with the company's calendar. To get direct access to this commodity, the smart-phone will need to authenticate itself to the calendar service using some personal credentials; again, the smart-device inherits part of the identity of its owner.

The same principle can be applied considering the more extended scenario of a Smart City, where digital identities or aggregates of digital identities are associated to complex systems used to deliver secure and trusted physical services to the citizen, e.g. public transportation, car to car communication,

remotely monitored Health care devices etc.

However, digital identities do not impact only on the daily life of the citizen, as their role is becoming more and more important also in the industrial sector.

Let consider the world of Industrial Control Systems; the increasing use of general purpose telecommunication networks (i.e. Internet) in these infrastructures, acted as a sort of glue, so that, today, we can say that ICS (and SCADA systems) are remotely controlled and accessed. Also in this case digital identities have a relevant role. To access to certain remote component or control servers, identities with associated roles and rights need to be used. Their management, the way in which they are protected and revoked – if needed, should and must be one of the top priorities for the security of a critical infrastructure.

The same consideration can be done also when thinking about the communication of low level control devices (e.g. PLCs). In this case, especially for those installations spread in geographically remote locations, with scarce or in-existing surveillance (let consider for example a gas or oil pipeline passing through remote regions of the world), the problem of securely manage their digital identities (in this case crypto-material allowing to sign and authenticate their readings and control messages) should be of high relevance.

An interesting playground where citizen identities and industrial infrastructures are quickly converging is that of smart-metering. Smart-meters can be considered the ultimate leafs of the smart-grids. These objects are at the moment those in charge for measuring the energy consumptions of the citizen, and, in some countries, for measuring also the energy production of the citizen.

However, to really benefit from the establishment of a smart-energy grid, soon these meters will need to get more and more integrated, on a side, with the energy-distribution infrastructure, and on the other, with the citizen's home digital infrastructure. Here again the digital identity inheritance principle described before will play a relevant role in the

protection of the privacy of the citizen while guaranteeing the provisioning, in a secure way, of services allowing to improve the optimization of the energy consumption and production.

## Soft Digital Identity Challenges

The concept of digital identity acted, as stated before, as enabler to get the access to a huge amount of different online services. However, a digital identity is also a possible key to get access to a huge amount of citizen's personal information and might be subject to profiling analysis from which additional information on the e-ID owner can be derived. This is especially true for the so called soft-identities, which are, by definition and nature, not standardised and to which, normally, the citizen pay poor attention in term of security despite the fact that they are commonly used indeed to access an incredible amount of personal information (think about the account of a social network).

“Provide the citizen with means to control and regulate the use of the sensitive information made accessible through a certain soft-digital identity”

From what briefly presented before, we can say that the infrastructures managing the digital identities will become more and more critical for the security and privacy of the citizen.

Under this light, generally speaking, three are the real challenges and needs:

1. Identify the right trade-off between level of disclosure (i.e. the amount of information associated to a certain digital identity when used) and the citizen's privacy level. This point assumes a high relevance especially in the context of digital identity inheritance,

where smart-devices uses some piece of their owner's identity to autonomously interact with the external digital world

2. Provide the citizen with means to control and regulate the use of the sensitive information made accessible through a certain soft-digital identity
3. Educate the digital citizen to a better use of their digital identities

Only in this way it would be possible to establish a correct level of trust in the digital world.

(Left intentionally blank  
for double sided printing)

# Prediction to CI impact analyses in case of natural hazards

Resilience of Critical Infrastructures against natural hazards could be significantly increased by efficient and timely events prediction, associated to a reliable consequence analysis of the damages produced on the functioning of infrastructures, on the population and the environment

Critical Infrastructures (CI) are technological systems (gas and water pipelines, telecommunication and electrical networks, roads and railways) at the heart of citizen's life. CI protection, issued to guarantee their physical integrity and the continuity of the services they deliver, is one of the major concern of public authorities and of private operators, whose economic results strictly depend on the way they are able to accomplish this task.

Critical Infrastructure Protection (CIP) is thus a major issue of nations, also due to their trans-national relevance. EU has thus issued directives to member states in favour of an increased level of protection, thus recognising the fact that they constitute a unique, large system covering all the EU area (EU Directive, 2008/114/CE).

CI resilience is thus progressively becoming a keyword. There is a constant recall from EU and Member States (MS) in sustaining actions for increasing CI resilience through the adoption of proper measures either by CI operators or by the specific authorities.

Although from the CI operators side a number of actions related to physical protection has been set in place, from the point of view of the governance of the "system of systems", EU still lacks appropriate answers, still demanding solutions to a "linearization" of the problem (each MS protects its own CI through the actions of single operators activities). However, this solution is not fully appropriate as it is well known the dependence and in some cases, the interdependence between CI and their trans-national interactions. A solution which would comply with this intrinsic character of CI would be thus more appropriate, and for that, more effective. US has provided its system of systems of a National Infrastructures Simula-

tion and Analysis Centre (NISAC) which plays the role of connecting all national-wide CI and performs forecast of high-impact natural hazards and the consequent faults on CI and the environment (see <http://www.sandia.gov/nisac/>).

Much with the same spirit, the EU-funded Network of Excellence CIPNet (Critical Infrastructures Preparedness and Resilience Research Network, see [www.cipnet.eu](http://www.cipnet.eu)) aims at proposing the NISAC experience in Europe by sustaining the technological and institutional growth of an European Infrastructures Simulation and Analysis Centres (EISAC), a constellation of connected national centres enabling a 24/7 risk analysis of the CI elements, providing these data to the appropriate national authorities appointed for CIP.

In this letter, we report the design of a Decision Support System (DSS), a core technological tool which will empower the EISAC capabilities, enabling the Centres to provide useful, timely and reliable CI risk assessments to its end-users, mainly the Civil Protection Offices and the CI operators.

## Risk assessment of CI

The current level of risk  $R(E_x, T)$  due to the possible (partial or complete) loss of a given element  $E_x$  (belonging to the  $x$ -th infrastructure) due to the occurrence of the event  $T$  (a natural hazard but also an attack), could be written, in general terms, as

$$R(E_x, T) = P(T) V(E_x, T) I(E_x) \quad (1)$$

where  $P(T)$  is the probability that the event  $T$  takes place,  $V(E_x, T)$  is the intrinsic vulnerability of the element  $E_x$  to that specific threat, and  $I(E_x)$  is a weighted sum of a number of Impact (consequences) terms estimating and  $(E_x)$  is a weighted sum of a number of Impact (consequences) terms esti-



**Vittorio Rosato**

Dr. Vittorio Rosato is head of the Computing and Technological Infrastructures Lab. at the ENEA Casaccia Research Centre (Roma). He received the Laurea in Physics at Pisa University (1979) and Ph.D. in Physics at the Université de Nancy (F) in 1986. He has been Research Associate at the University College of Wales (UK) and at the Centre d'Etudes Nucleaires de Saclay (F). His expertise is in high performance computing in Condensed Matter Physics. His current interests are in Complexity Science, Risk Analysis and in modeling and simulation of technological infrastructures. He acts as Referees for many international journals and as Project Evaluator. He is co-founder of a spin-off company Ylichron Srl, active in the ICT and bio-ICT domains. He is also one of the co-founders of the Italian Chapter of the International Emergency Management Society (I-TIEMS).

e-mail: [vittorio.rosato@enea.it](mailto:vittorio.rosato@enea.it)

inating the consequences that the loss of the Ex functioning could produce.

The Impact terms could indicate the consequences on:

- the x-th CI (i.e. that stricken by the event)
- other CI whose functioning is depending on the services provided by the x-th CI
- the population (through the lack or the reduction of the corresponding services)
- the industrial sectors, deprived of supply services
- the environment (each time when the loss of a CI element is associated to some secondary effect affecting the environment, such as a gas release from a hit pipeline or the atmospheric or sea pollution due to some spill of toxic contents etc).

For a qualitative and quantitative Risk assessment, one should thus deal with the evaluation of the three terms in the right-hand side of eq.(1) requiring the use of a number of different tools and the availability of many diverse competences.

## DSS workflow and function

The DSS workflow configured by eq. (1) estimates, at the end: 1) the Probability of Occurrence of a given threat (meteorological, meteo-climatic related effects and geophysical events), 2) the intrinsic vulnerability of the different elements of the CI which, in principle, depends on the specific Threat, on its strength and on the geographical position of the element, i.e.

$$V(E_x, T) = V(E_x, \text{pos}(E_x), T, S(T)) \quad (2)$$

and 3) the value of specific metrics defined to quantify the impacts that a fault of a CI could induce in many different domains of public life, from the loss (or reduction) of relevant services to citizens, to the reduction of productivity of the industrial sector, to the environmental damages (e.g. pollution, if the CI damage is associated to environmental one).

The DSS designed in the CIPRNet project, to evaluate the state of Risk of the CI elements in a given area (which, for the national EISAC nodes should coincide with the entire national territories) will make a thorough evaluation of eq. (1) by using existing and *ad-hoc* developed

technological tools (databases, simulation models) integrated with existing technologies (now casting and remote sensing, with High Resolution and/or SAR data).

Fig.1 reports a schematic layout of the different tasks that the designed workflow should accomplish in order to produce a "CI Risk Daily Report" which will constitute the specific outcome of the EISAC nodes in favour of their main end-users: Civil Protection Depts. and/or other Public Authorities committed to CIP.

more of the predicted threats). At this stage, the workflow envisages the communication of the expected Damage Scenarios to CI operators; they will be called to evaluate, with their simulation tools, the impact (in terms of reduction of functionality) on their networks if the predicted outage of the Ex element would occur as predicted. In turn, CI operators will reply by identifying the Impacts on their services that the different damages would produce (in terms, for instance, of reduction of the Quality of Service(QoS)).

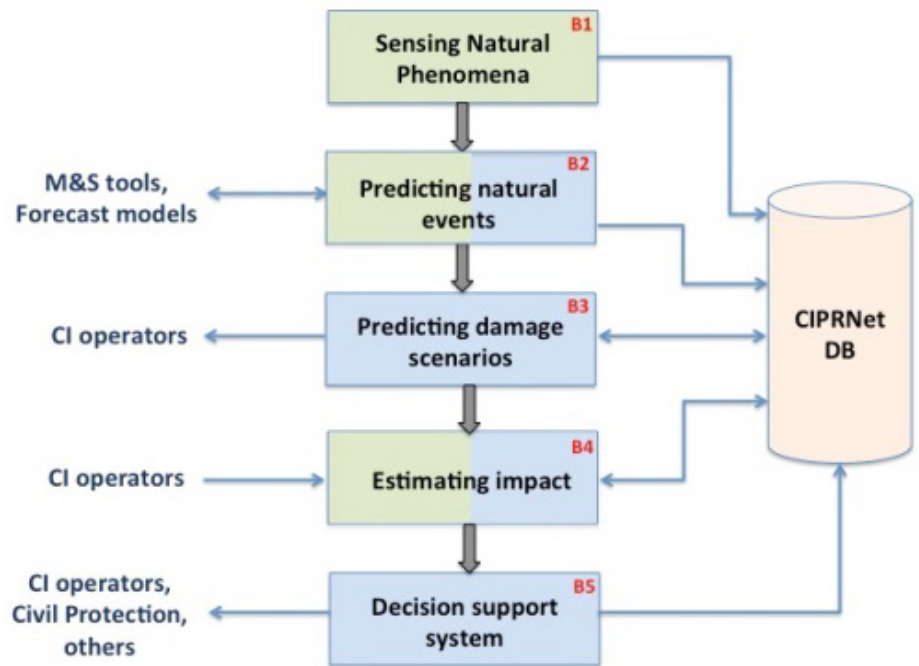


Fig. 1: Workflow of the DSS which is going to be designed and realized within CIPRNet, which will boost the national EISAC nodes.

Four different phases are visible in fig.1. In the first (the first term in the right-hand side of eq. (1)), the system collects information from the field (through proximal or remote sensors) and from weather forecast (medium-long term, as weather forecast and short-term by now casting equipment). High resolution downscaling of weather forecast will be performed in areas where a higher forecast resolution would be relevant for increasing prediction reliability. In the second (the second term at the r.h.s. of eq. (1)), starting from the event prediction, the system analyses its database to establish the probability that a given infrastructural element is hit by the threat and damaged. Intrinsic vulnerabilities of elements are correlated with the event probability and with its predicted strength in order to provide a damage probability. This information will be integrated into a "Damage Scenario" (i.e. the set of all CI elements possibly hit by one or

At this stage, the third phase of the workflow will start. The DSS system will gather the information from the CI operators and, by using specific tools accounting for system's functional dependences (or interdependencies) will evaluate the overall impact of the predicted damages on the whole system of CI (at a level of "system of systems"). This information represents a significant advancement with respect to the current capabilities: (a) the scenario is "predicted", thus it will be delivered to decision-makers in advance to the event's occurrence; (b) the system will also evaluate possible cascading effects due to system's (more or less evident) dependencies, thus increasing impact's predictions made on the bases of single-infrastructures evaluations; (c) other than impacts at the physical and service levels, the DSS could correlate impacts data with different types of information layers (physical, environmental, territorial, industrial, economical, social) and would be

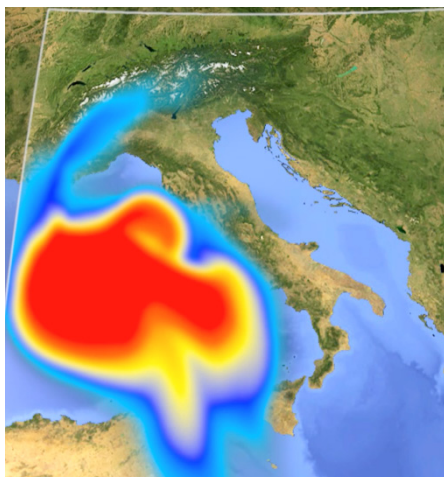
able to establish further types of Impacts, on the population, on the different industrial sectors, on the environment.

“We will never be able to perfectly predict or prevent all extreme events or eventualities. Therefore, we must conserve and develop those systems that can most quickly respond to, and most effectively rebound from, severe weather events and other emergencies.”

NY2100 Commission, 2012

In particular, from the environmental side, the system could also be used for predicting the course of events in the cases where the CI damage scenario would imply some event (such as oil spill, toxic or radioactive releases from plants etc.). In such a case, the DSS could interact with environmental models for the prediction of environmental impacts. Fig.2 reports a snapshot of a simulation enabling the prediction of the diffusion of a radioactive gas release from a nuclear plants and its subsequent ground deposition, affecting, during the course of time, different urban areas.

The DSS functioning will be related to the different operational modes triggered by the issue of Alert (due to specific expected natural threats) from the Authority (like e.g. the Civil Protection, in the case of Italy). When no-Alert is issued, the DSS will perform its current 2/days evaluations starting from the broadcast of large scale weather forecast.



Comune	0h	1h	2h	3h	4h	5h	6h	7h	8h	9h	10h	11h	12h
VFILLE	1716	0.00	0.00	0.00	1.69	42.45	53.10	7296.16	16648.50	17998.10	18001.50	18005.10	
VGOSTA	1448	0.00	0.00	0.00	2.20	50.82	61.54	11457.50	12659.80	14325.70	14328.70	14332.30	
ALBANO LAZIALE	31763	0.00	0.00	0.00	1.12	34.42	350.93	48754.90	87716.30	83026.30	63952.00	43026.70	
ALLUMIERE	4288	0.00	0.00	0.00	0.21	3.13	142.40	20041.30	32979.60	32869.50	32992.90	32994.60	
ANGUILLARA SABAZIA	9728	0.00	0.00	0.00	0.03	1.40	200.10	8576.55	21334.00	21346.70	21349.70	21352.00	
ANTICOLI CORRADO	947	0.00	0.00	0.00	2.20	50.82	61.54	11457.50	12659.80	14325.70	14328.70	14332.30	
ANZIO	34601	0.00	0.00	0.00	2.22	75.98	677.10	2823.00	23820.20	23844.30	23850.30	23854.20	
ARCIANAZZO ROMANO	1422	0.00	0.00	0.00	1.39	27.50	31.31	9790.24	13129.90	13990.10	13993.70	13997.30	
ARDEA	17686	0.00	0.00	0.00	1.44	47.96	530.15	33417.80	50161.30	59313.00	59318.40	59322.20	
ARICCIA	17967	0.00	0.00	0.00	2.24	41.04	247.24	34743.70	81327.60	81735.70	81757.90	81761.00	
ARSOLI	1501	0.00	0.00	0.00	2.20	50.82	61.54	11457.50	12659.80	14325.70	14328.70	14332.30	
ARTENA	10873	0.00	0.00	0.00	1.66	47.46	167.18	27505.80	66528.30	67647.10	67650.80	67654.60	
HELLEGRA	3027	0.00	0.00	0.00	1.99	57.41	74.89	4802.08	20167.10	22006.20	22009.30	22013.00	
IRACCIANO	10970	0.00	0.00	0.00	1.10	2.55	217.21	6557.74	17753.90	17766.10	17772.00	17774.50	
CAMERATA NUOVA	489	0.00	0.00	0.00	1.67	32.19	38.61	8783.99	9479.18	10386.70	10389.50	10392.90	
CAMPAGNANO DI ROMA	6523	0.00	0.00	0.00	0.01	1.05	125.62	24868.50	40748.70	41020.30	41023.00	41025.60	
CANALE MONTERANO	2682	0.00	0.00	0.00	0.13	3.13	181.92	13925.90	25816.70	25829.60	25834.00	25836.50	
CANTERANO	382	0.00	0.00	0.00	2.20	50.82	61.54	11457.50	12659.80	14325.70	14328.70	14332.30	
CAPENA	4474	0.00	0.00	0.00	0.00	0.81	94.39	29229.20	48978.50	49510.30	49512.90	49515.70	
CAPRANICA PRENESTINA	303	0.00	0.00	0.00	1.99	57.41	74.89	4802.08	20167.10	22006.20	22009.30	22013.00	
CARPINETO ROMANO	5237	0.00	0.00	0.00	1.39	57.16	88.52	12357.80	42105.80	43800.60	43904.70	43908.50	
CASAPE	821	0.00	0.00	0.00	1.99	57.41	74.89	4802.08	20167.10	22006.20	22009.30	22013.00	
CASTEL GANDOLFO	7030	0.00	0.00	0.00	2.24	41.04	247.24	34743.70	81327.60	81735.70	81757.90	81761.00	
CASTEL MADAMA	6329	0.00	0.00	0.00	1.74	36.93	64.55	19244.10	28053.00	29755.10	29758.10	29761.60	
CASTELNUOVO DI PORTO	5871	0.00	0.00	0.00	0.00	0.81	94.39	29229.20	48978.50	49510.30	49512.90	49515.70	
CASTEL SAN PIETRO ROMANO	684	0.00	0.00	0.00	1.99	57.41	74.89	4802.08	20167.10	22006.20	22009.30	22013.00	
CAVE	8470	0.00	0.00	0.00	1.99	57.41	74.89	4802.08	20167.10	22006.20	22009.30	22013.00	
ZERRETO LAZIALE	1102	0.00	0.00	0.00	2.20	50.82	61.54	11457.50	12659.80	14325.70	14328.70	14332.30	

Fig. 2 top: snapshot of the simulation of the diffusion of the radioactive cloud in the Mediterranean basin (false colours identify radioactive concentration in Bq/m3);

Bottom: the correlation between deposition data and geographical information layers providing the average dose (Bq/m2) deposited on the ground in the different cities of Regione Lazio (Italy).

The system performs its analysis and provides a Report with “no Damage Scenario” or a “Damage Scenario” predictions. In fact the system could predict the presence of threats and perform a damage prediction on CI I even in absence of alerts (i.e. in small-scale predictions where only a few CI elements could be hit by specific small-scale events such as, e.g., lightning on small, vulnerable areas). When, in turn, an alert is issued by public authorities, the DSS could still produce its prediction by going up to the end of the workflow (Impacts evaluations), by reporting to the end-users its estimates. Moreover, in the Emergency management, the EISAC node (with all its technological assets) could be ready to sustain mitigation and restoring actions by using its tools to support public authority in optimising strategies (for instance by pre-assessing the outcomes of actions by simulating their effects on the crisis scenario).

### The case of earthquakes

In the case of unpredictable threats such as earthquakes, the DSS starts its course of actions as soon as the geophysical data of the event are broadcasted by the public authority. The system is able, in an automatic mode, of getting earthquakes data

from the primary information source and process the event to produce the shake maps in the area around the event epicentre.

Shake maps are relevant for assessing the Intensity of the seismic wave at a given site; this data can be correlated with buildings vulnerability indices providing an empirical assessment of the expected damages.

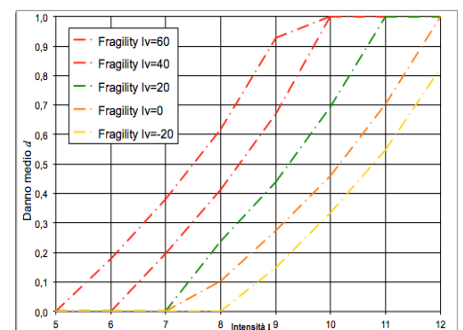


Fig. 3: Expected damage (y axis, empirical scale where 0 is undamaged and 1 has the complete destruction) as a function of the seismic intensity (as evaluated from shake map analysis) for different buildings of different Fragility indices Iv (Iv depends on building types, ages, height etc.). Iv can be deduced by land registers data (Giovinazzi and Lagomarsino, 2001).

Fig.3 reports the expected damages to buildings after an earthquakes producing a given ground acceleration intensity. The shake maps evaluation, correlated with land register data surveying buildings technical properties, allow to produce a damage scenario with a resolution as high as few hundred meters (the current average resolution of land register data). Other than buildings for residential use, the same procedure applies to explore the damage level of technological buildings hosting CI elements, or industrial or energy production plants, or roads, railways etc. Fig.4 reports the expected damages upon a simulated (synthetic) earthquake of magnitude 6.0 (Richter scale) in a point lying in a highly seismic zone close to Naples (Italy). Starting from these data, an Impact analysis made on the bases of the predicted damages suffered by CI elements, the DSS can rapidly provide a first assessment of the expected level of CI services that the first responder should be able to cope with, in order to provide first aids.

The DSS will also be able (by correlating damage scenarios with other information layers) to predict number of affected citizen, the possible impacts on industrial sectors, energy

production plants, thus establishing a comprehensive Impact assessment of the event.

In conclusions, CIPRNet will support the realisation of new tools that, by providing reliable predictions of impacts of natural events on CI, would ultimately increase their resilience. CI operators, emergency managers and responders should benefit of a constant risk assessment of the main CI on which rely most of vital services for citizens. Current web services will allow to broadcast this information not only "desk to desk" but also on the field (through appropriate apps for tablets and smartphones), by reaching also first responders in case of natural disasters.

In conclusions, CIPRNet will support the realisation of new tools that, by providing reliable predictions of impacts of natural events on CI, would ultimately increase their resilience. CI operators, emergency managers and responders should benefit of a constant risk assessment of the main CI on which rely most of vital services for citizens. Current web services will allow to broadcast this information not only "desk to desk" but also on the field (through appropriate apps for tablets and smartphones), by

reaching also first responders in case of natural disasters.

Other than on the technological side, CIPRNet efforts will also be addressed to provide an "institutional location" to EISAC in the different countries, trying to properly fitting its functions to comply with the needs and the workflow of CIP activities.

**Related reference:**

V. Rosato et al. *Risk Analysis and Crisis Scenario Evaluation in Critical Infrastructures Protection* in "Efficient Decision Support Systems - Practice and Challenges in Multidisciplinary Domains", ISBN 978-953-307-441-2, edited by Chiang Jao

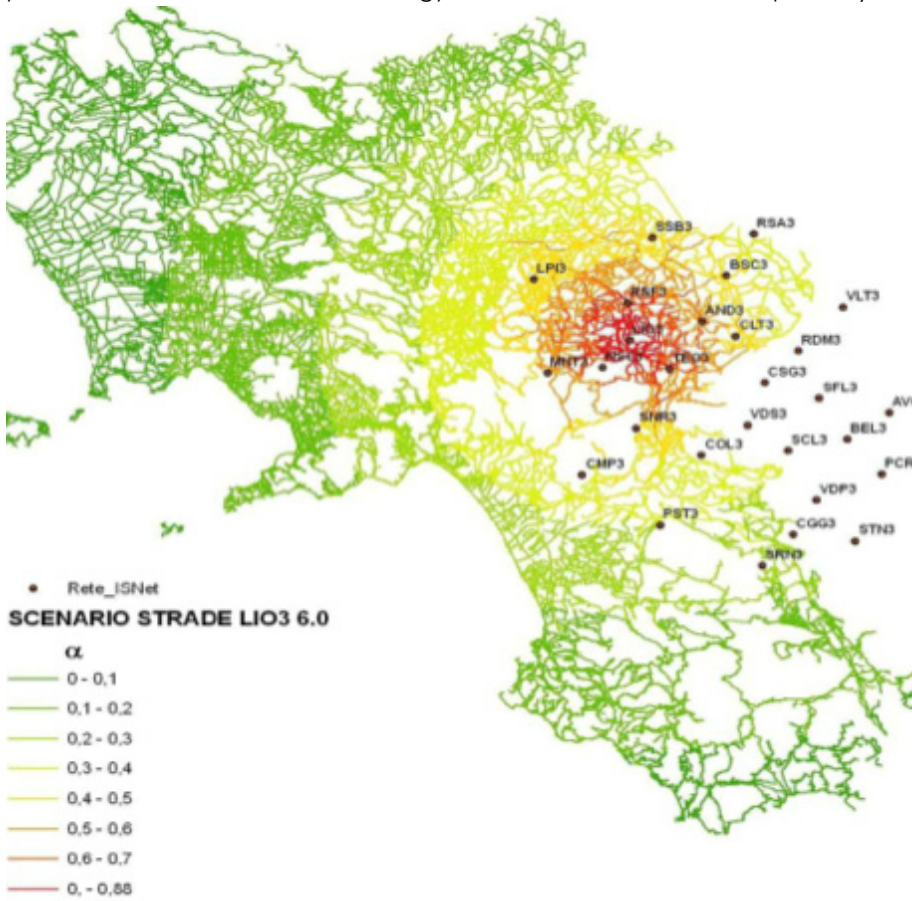


Fig. 4: Expected damages on roads and motorways after the simulation of a (synthetic) earthquake of M=6.0 in the region close to Naples (Italy)

# TIEMS – The International Emergency Management Society

TIEMS is a global forum for education, training, certification and policy in emergency and disaster management, dedicated to developing and bringing the benefits of modern tools, techniques and good industry practices to society for a safer world

TIEMS was established in Washington, USA, as The International Emergency Management and Engineering Society (TIEMES) and registered in Dallas, Texas, USA, as a non-profit organisation in 1993. The Society was reorganized in 1996 and changed its name to The International Emergency Management Society (TIEMS). TIEMS was moved to Belgium in 2006, where TIEMS today is registered as an international, independent and not for profit NGO. TIEMS arranged its first annual conference in Fort Lauderdale, USA in 1994. Since then TIEMS has moved the conference venue around the world, and has developed other important activities and services to its members and the community. TIEMS is today an important communication platform for the international emergency and disaster management community.

## TIEMS Mission

TIEMS is a global forum for education, training, certification and policy in emergency and disaster management. TIEMS is dedicated to developing and bringing the benefits of modern emergency management tools, techniques and good industry practices to society for a safer world. This is accomplished through the exchange of information, methodology innovations and new technologies, to improve society's ability to avoid, mitigate, respond to, and recover from natural and man-made disasters.

TIEMS provides a platform for all stakeholders within the global emergency and disaster management community to meet, network and learn about new technical and operational methodologies. It also aims to exchange experience on good industry practises. The belief is that this will influence policy makers worldwide to improve global cooperation and to establish global

standards within emergency and disaster management.

## TIEMS Chapters

In order to reach out worldwide, TIEMS is building an international expert network, where local chapters play an important role in establishing local TIEMS activity, such that cultural differences are understood and included in TIEMS education and research programs, and other TIEMS activities.

## TIEMS Slogans

For TIEMS Local Chapters:

*"Think Globally and Act Locally"*

For TIEMS Education:

*"Preparedness Saves Lives"*

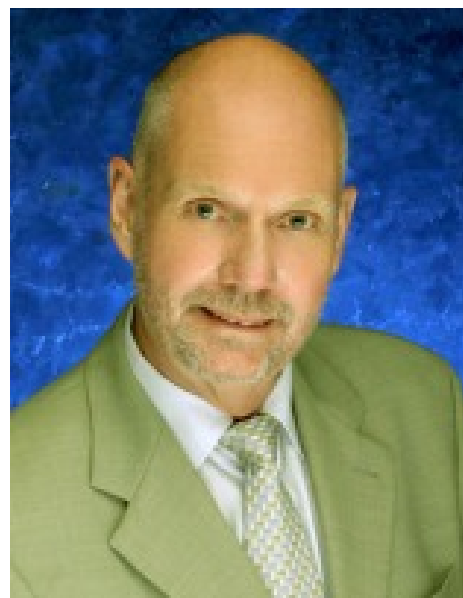
For TIEMS Research:

*"RTD for a Safer World"*

TIEMS chapters are self-governed entities within TIEMS framework. Today chapters are established in Italy, Iraq, Romania, Be/Ne/Lux, India, Finland, Middle East and North Africa, Japan, Korea and China.

Dialogue is also opened with experts in more countries, which see the benefit of TIEMS international expert network of chapters and members, where partnership, education and research in disaster resilience is the focus.

TIEMS Chapters play the main role as host of TIEMS international events, and TIEMS Japan Chapter will be the host of TIEMS next annual conference in 2014, in Niigata, Japan on 21 – 23 October, with the support of Niigata Governor. The date, 23<sup>rd</sup> of October, coincides with the anniversary date of the big 2014 Niigata earthquake.



## K. Harald Drager

is TIEMS President and he was recently re-elected for a 3 year period during TIEMS 2013 annual conference in France. He took the initiative to establish TIEMS in 1993, and was the International Vice President since the start until 2002, when he took over as TIEMS President. TIEMS has under his leadership developed well internationally with local chapters globally and TIEMS arranges each year workshops and conferences around the world with focus on different topics in disaster risk reduction. TIEMS has also initiated a global education, training and certification program and a research initiative service for its members. TIEMS is now in the process of also establishing international task force groups. Mr. Drager as an international consultant has worked for numerous clients worldwide, and he has been project manager of several research and development projects in risk, emergency and disaster management.

e-mail: [khdrager@online.no](mailto:khdrager@online.no)



## TIEMS Activities

TIEMS main activities today comprise:

- International conferences, workshops and exhibitions worldwide
- Newsletter with latest news and articles of interest
- Chapter activity to stimulate local initiatives and activities
- Research & development projects and member service
- International education, training and certification programs
- Global young scientist network
- TIEMS library with proceedings from TIEMS events

However, with an increasing membership constituency and activity worldwide, new activities are continuously added to meet the demand of improved disaster resilience worldwide.

## TIEMS Events

TIEMS arranges conferences and workshops worldwide each year, in order to provide a platform for all stakeholders within the global emergency and disaster management community to meet, network and learn about new technical and operational methodologies, but also to exchange experience and expertise and learn from each other. TIEMS goal is through these events to influence policy makers worldwide to improve global cooperation and to establish global standards within emergency and disaster management.

The main event each year is TIEMS annual conference, where also TIEMS Annual General Meeting takes place with reports on the last year's activities and putting forward plans for the next as well as election of directors to TIEMS Board of Directors. In 2013 the annual conference took place in Velaux, France at the French Fire Service new training centre, and the focus where robotics for increased safety of the first responders. Six leading international robotic companies demonstrated their robots and the potential of these devices, and gave the audience ideas of how to improve and extend the operational ability for those in the field fighting disasters and for search and rescue squads.

In addition to TIEMS annual conference, TIEMS Chapters arrange their local conferences and workshops in their country with focus on local emergency and disaster challenges. TIEMS also cooperate with other partners in making workshops with focus on special topics of interest.

TIEMS events in 2013 comprise:

- **Kyoto, Japan**, on: *Emergency Operation Centre and Common Operational Picture*
- **San Diego, USA**, on: *Collaboration in Emergency Response and Disaster Management*
- **Basrah, Iraq**, on: *Emergency Medicine in Iraq*
- **Espoo, Finland**, on: *Living Lab for Societal Security*
- **Xian, China**, on: *China Chapter Annual Conference and Training*
- **Berlin, Germany**, on: *Public Alerting and Social Media during Crisis and Disasters*
- **Guangzhou, China**, on: *Emergency Medicine*
- **Seoul, Korea**, where subject is to be decided

## TIEMS Education Programs

The motivation behind TIEMS education programs are:

- Put international focus on the profession of emergency and disaster management
- Contribute to an international standard in education, training and certification in emergency and disaster management
- Contribute to the education in Emergency and Disaster Management by promoting the state of the art in technology, systems and methods available
- Contribute to education at all levels, from policy documents to courses in primary school education
- Establish a TIEMS certification of qualifications in international emergency and disaster management
- Contribute to capacity building in countries where little or no education and training in this field is available
- Recruit international instructors to TIEMS pool of international instructors

TIEMS has recognized an increasing worldwide need for qualified

international instructors with up-to-date courses on various subjects in emergency and disaster management. TIEMS has accordingly built up a pool which today counts 20 international well qualified and updated experts, with various courses addressing key issues in emergency and disaster management.

In order to develop TIEMS education programs, reflecting the local needs and adding the different culture aspects, TIEMS has initiated training workshops, arranged by TIEMS chapters locally, engaging TIEMS international instructors together with local instructors. Training workshops have been arranged by:

- TIEMS China Chapter in Shanghai in 2011
- TIEMS Romania Chapter in Dambovitza in 2012
- TIEMS China Chapter in Guangzhou in 2012
- TIEMS Iraq Chapter in Erbil in 2012

TIEMS China Chapter will arrange their next training workshop prior to their annual conference in Xian in October this year.

TIEMS initiative of an international certification is called TIEMS QIEMD. This is a certification of **Qualifications in International Emergency and Disaster Management**

The concept requirements are:

- Candidates need to have sufficient background education and practise in emergency and disaster management
- The QIEMD curriculum is to comprise both theoretical and practical courses and hands on training
- Courses to be offered by TIEMS in cooperation with universities and training institutions worldwide
- The certification exam/test to be passed
- The certification to be given in cooperation with national and international certification authorities
- TIEMS Chapters will be responsible for adding local/national/cultural competences

When surveying available courses and certification in emergency and disaster management worldwide, TIEMS has come across many different approaches, and TIEMS likes to cooperate with existing schemes,

and invites to a joint effort to establish an international standard.

TIEMS therefore invites universities and training institutions worldwide, with available courses and training, meeting TIEMS QIEM curriculum requirements, to cooperate in establishing a worldwide available curriculum in emergency and disaster management.

## TIEMS Research Initiatives

TIEMS research and technology development (RTD) projects and member service, is an initiative to stimulate advancement in technology, methods, operations, systems and organizational aspects of the emergency and disaster management discipline for a safer world.

TIEMS members constitute a large international multidisciplinary group of experts, with different educational background and various experiences in the field of emergency and disaster management. They represent a unique source of expertise and ideas, with different cultural background, which are important assets for research and development activities. TIEMS has therefore launched this initiative with the following goals:

- Based on TIEMS member's needs and ideas, develop a RTD plan and be responsible for the execution of the plan
- Involve TIEMS members in RTD programs and projects
- Initiate RTD consortiums where TIEMS members can participate in RTD proposals
- Inform members of established RTD consortiums and RTD activity where TIEMS members can participate
- Develop and maintain a TIEMS RTD cooperation strategy for TIEMS members
- Maintain and update the website information on RTD opportunities
- Stimulate and encourage TIEMS chapters to take RTD initiatives and establish RTD activity in TIEMS chapters

RTD projects is an excellent way to establish cooperation between TIEMS members and beyond and thus strengthen and extend TIEMS network

and recruit new members and establish new TIEMS chapters

There exist many financial sources and schemes worldwide for supporting RTD activities in emergency and disaster management, amongst others the European Commission. TIEMS encourage its members and chapters to explore and document and exploit these opportunity financing sources and schemes for establishing RTD projects worldwide with TIEMS member involvement to the benefit of a safer world. It should be possible by this initiative to fund good project ideas, anchored in the different cultures, which have a hard time reaching funding today.

## TIEMS Task Force Groups

TIEMS latest initiative, which was launched by TIEMS China Chapter and discussed during TIEMS annual conference in France, is to establish TIEMS Task Force groups.

Each Task Force Group would comprise qualified TIEMS scientists in different fields. These task groups could cooperate with UNOCHA, and/or with local emergency management government agencies and directly join to the operation during the emergency issues occurred.

TIEMS China Chapter suggested, based on their experience in China, the following Task Force groups to be established:

1. Disaster Integrated Risk Assessment Task Force
2. Disaster Scenario Simulation and Preparedness Task Force
3. Emergency Response and On-site Life Rescue Task Force
4. Early Warning and Decision-making Sub-Task Force
5. On-site Communication, Commanding and Coordination Sub-Task Force
6. Emergency Medical Care and Public Health Task Force
7. Emergency Engineer Rescue and Equipment Task Force
8. Allocation of Homeless People and Disaster Recovery Task Force
9. Emergency management and SAR Theory Task Force
10. High-Technology (Robots) and Applications Task Force
11. Disaster Cases Analysis and Database Construction Task Force

12. Training, Exercise and Certification Task Force

This initiative will be further discussed during TIEMS China Chapter Symposium on Emergency Medical Care to be hold in Guangzhou, China during 15-17, Nov. 2013.

The goal is to form the Emergency Medical Care and Public Health Task Force Group during this event, where experts from USA, Italy, France, and Iraq on Emergency medical care will participate in addition to Chinese experts.

## TIEMS Membership and Partnerships

TIEMS membership and partnership benefits are listed in the following:

- Personal and institutional membership
- Partnerships with complimentary organisations and Institutions
- Sponsorships to support TIEMS activities
- Financial support to students to take part in TIEMS activities
- Recognize excellence in emergency and disaster management by awards
- International education, training and certification
- Joining TIEMS international pool of instructors
- Research and development service to TIEMS members

If you would like to find out more about TIEMS, please visit our website at:

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

or send an email to TIEMS Secretariat:

[r.miskuf@squaris.com](mailto:r.miskuf@squaris.com)

(Left intentionally blank  
for double sided printing)

# IFIP TC-11's WG11.10 on Critical Infrastructure Protection

IFIP Technical Committee 11 on Security and Privacy Protection in Information Processing Systems has been promoting the areas of security and privacy since it was founded in 1983. It has an active working group on critical infrastructure protection

Established in 1960 under the auspices of UNESCO, the International Federation for Information Processing (IFIP) is a multinational federation of professional and technical organizations in the area of information processing. Currently, IFIP includes organizations from more than 40 countries. Details about IFIP and its activities are available at [www.ifip.org](http://www.ifip.org).

IFIP Technical Committee 11 (TC-11) on Security and Privacy Protection in Information Processing Systems was founded in 1983. It has fourteen working groups (WGs), each of which focuses on a specific area of security or privacy.

Founded in 2006, the IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of more than 150 researchers, infrastructure operators and policy-makers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in infrastructure protection.

## TC-11

TC-11 aims are: (i) to increase the trustworthiness and general confidence in information processing; and (ii) to act as a forum for security and privacy protection experts and others professionally active in the field.

TC-11 works towards:

- the establishment of a common frame of reference for security and privacy protection in organizations, professions and the public domain;
- the exchange of practical experience;
- the dissemination of information on and the evaluation of current and future protective techniques;
- the promotion of security and privacy protection as essential elements of information processing systems;

- the clarification of the relation between security and privacy protection.

The TC-11 membership is composed of national representatives from its member societies (currently, more than thirty countries) and individual WG chairs.

TC-11 organizes an annual International conference, IFIP SEC ([www.ifipsec.org](http://www.ifipsec.org)), which provides researchers and practitioners with an opportunity to present their most recent work. TC-11 also has an official journal, Computers and Security (COSE), which is published by Elsevier (Amsterdam, The Netherlands).

The WGs are a vital part of TC-11. Each WG organizes events such as conferences and summer schools. Some WGs have their own journals. Since its inception in 1983, TC-11 has strived to accommodate the latest technical areas in the scope of its working groups. Currently, TC-11 has fourteen working groups:

- WG11.1: Information Security Management
- WG 11.2: Pervasive Systems Security
- WG 11.3: Data and Application Security
- WG 11.4: Network & Distributed Systems Security
- WG 11.5: IT Assurance and Audit
- WG 11.6: Identity Management
- WG 9.6/11.7: Information Technology Misuse and the Law
- WG 11.8: Information Security Education
- WG 11.9: Digital Forensics
- WG 11.10: Critical Infrastructure Protection
- WG 11.11: Trust Management
- WG 11.12: Human Aspects of Information Security and Assurance
- WG 8.11/11.13: Information Systems Security Research
- WG 11.14: Secure Engineering

For details see [www.ifiptc11.org](http://www.ifiptc11.org)



**Yuko Murayama**

TC-11 Chair  
Professor  
Faculty of Software and Information  
Science, Iwate Prefecture University,  
Japan

e-mail: [murayama@iwate-pu.ac.jp](mailto:murayama@iwate-pu.ac.jp)

## WG 11.10 on Critical Infrastructure Protection

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to day-to-day operations in every sector: agriculture, food, water, public health, emergency services, government, defence, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Global business and industry, governments, indeed society itself, cannot function effectively if major components of the critical information infrastructure are degraded, disabled or destroyed.

IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of more than 150 scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in the important field of critical infrastructure protection. IFIP WG 11.10 engages the international information security research community to work together on applying scientific principles and engineering techniques to address current and future problems in information infrastructure protection. In addition, IFIP WG 11.10 draws interested parties (government agencies, infrastructure owners, operators and vendors, and policy makers) in a constructive dialog on critical infrastructure protection.

The mission of IFIP WG 11.10 is to weave science, technology and policy in developing and implementing sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. Information infrastructure protection efforts at all levels – local, regional, national and international – are advanced by leveraging the WG 11.10 membership's strengths in sustained research and development, educational and outreach initiatives.

IFIP WG 11.10 organizes its Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection every March. The annual conferences provide international forums for presenting original, unpublished research results and innovative ideas related to all aspects of critical infrastructure protection. The conferences are typically limited to seventy participants to facilitate interactions among researchers and intense discussions of research and implementation issues. The Eighth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will be held at SRI International in Arlington, Virginia, USA on March 17 - 19, 2014.

IFIP WG 11.10 produces two important publications in the discipline of critical infrastructure protection. The first is the Critical Infrastructure Protection book series, which is published by Springer (Heidelberg, Germany).

Each book in the annual series contains a selection of edited papers from the IFIP WG 11.10 International Conference on Critical Infrastructure Protection. The book series is an important resource for researchers, faculty members and graduate students, as well as for policy makers, practitioners and other individuals with interests in homeland security.

The second major IFIP WG 11.10 publication is the International Journal of Critical Infrastructure Protection (IJCIP), which is published every quarter by Elsevier (Amsterdam, The Netherlands). Launched in 2008, IJCIP publishes scholarly papers of the highest quality in all areas of critical infrastructure protection. Of particular interest are articles that weave science, technology, law and policy to craft sophisticated yet practical solutions for securing assets in the various critical infrastructure sectors. A unique aspect of the journal is the publication of opinion pieces from leading international scholars and high-ranking government officials that tackle controversial issues related to critical infrastructure protection that are of global significance.

Details about IFIP Working Group 11.10 on Critical Infrastructure Protection and its many activities and initiatives are available at: [www.ifip1110.org](http://www.ifip1110.org)

# CRITIS 2013: Conference Report

CRITIS 2013 took place in Amsterdam, The Netherlands,  
September 16-18, 2013.  
Key topic: Resilience of Smart Cities

## CRITIS 2013

The eighth International Workshop on Critical Information Infrastructures Security (CRITIS 2013) was held in the EYE and the Shell Technology Centre Amsterdam, September 16 to 18, 2013. The conference was organised by The Netherlands Organisation for Applied Scientific Research TNO.

Critis'11 proceedings were sent out on Oct 13. The Critis'12 proceeding are in print now. If you are interested in acquiring a copy, visit the Springer LNCS series website.

CRITIS 2013 proceedings are in the initial typesetting phase aiming for an early 2014 release.

CRITIS 2013 continued the series of successful CRITIS conferences. This conference started with an additional half day of keynote speeches which intended to broaden the view of critical (information) infrastructure (C(I)I) stakeholders such as policymakers, CI operators, and researchers. The focus of the keynote speeches was on Resilient Smart Cities which require resilient and reliable information and communication networks. Related notions are resilient smart grids and smart mobility. The topics of these keynote speeches were:

- Amsterdam, A Smart City (Ton Jonker, Amsterdam Economic Board),
- A Hyperconnected World: EYE on the Past, Present and Future (Henk Geveke, TNO),
- From Requirements for Critical Industry Sectors... Towards... Jointly Protecting our Critical

Service Chains (Ben Krutzen, Shell),

- Smart City, A Vision on 2030 (Max Remerie, Siemens), and
- Future Visions of Super Intelligent Transportation (prepared by Marie-Pauline van Voorst tot Voorst, Netherlands Study Centre for Technology Trends).

During the remainder of the conference keynote speeches took place on:

- Future C(I)IP challenges – a view from the financial sector (Leon Strous, DNB),
- Smart Cities, a View on Developments (Giampiero Nanni, Symantec/EMEA),
- European Critical Internet Infrastructure: Past, Present and Future Research (Rossella Mattioli, ENISA), and
- From R&D to an International Operational Monitoring Centre: Monitoring the State of Critical Infrastructure(s) using Sensor Systems (Robert Meijer; Stichting IJkdijk, University of Amsterdam, and TNO).

All keynote speeches stimulated the debate between CI domain stakeholders on the nearby and long-term organisational and R&D challenges during the remainder of the conference and hopefully thereafter. A House-of-Commons style debate, which actively involved all conference participants, took the debate another step forward while bridging the views of the CI policymakers, CI operators, and the various research communities.

As in previous years, the technical Program Committee received a large set of paper submissions. The Program Committee provided insightful reviews and comments to the submitters of 57 papers. At least three independent and blind reviews per submission took place resulting in the selection of 16 full papers, which means an acceptance rate of 28%.



### Eric Luijff

Eric Luijff is Principal Consultant Critical (Information) Infrastructure Protection and Cyber Operations at TNO, The Hague, The Netherlands.

Local co-chair CRITIS 2013.

e-mail: [eric.luijff@tno.nl](mailto:eric.luijff@tno.nl)

[www.critis2013.nl](http://www.critis2013.nl)

Another four submissions were accepted as short papers. All these papers are published in this volume of the Springer LNCS series.

The selected papers and their presentations were grouped in the conference program as New Challenges, Natural Disasters, Smart Grids, Threats and Risk, SCADA/ICS and Sensors, and Short Papers. The same grouping can be found in the CRITIS 2014 proceedings which are expected to be published by Springer as LNCS 8328 early next year. The pdfs of all the presentations in Amsterdam can be found on the CRITIS 2013.nl website under the program tab.

9th International Conference on Critical Information Infrastructure Protection

**CRITIS 2014**

will be held  
in Limassol Cyprus, visit  
[www.critis2014.org](http://www.critis2014.org)

To stimulate international collaboration and exchange of ideas, the CRITIS 2013 program chairs handpicked a couple of other submissions which broach interesting subjects for the C(I)I protection domain. These contributions were discussed in an interactive parallel work-in-progress session. To stimulate collaboration even more, the conference organisers started the building of a Critical Information Infrastructures Security LinkedIn community for young (of mind) researchers: Young CRITIS. The intention is building a virtual international community that allows (young) researchers in the C(I)I domain to ask questions to peers and experienced researchers in the C(I)I domain about specific topics, e.g. help to find relevant literature, availability of data, and which research approaches are successful and which are not. This will enable to reach faster and better research results. Understanding each other's interests may help to develop joint international research proposals. At CRITIS 2013 a short brainstorm took place with Young CRITIS members (to be) on the need for such a network, how to expand the network further, and how to embed Young CRITIS in CRITIS 2014.

Organising a conference like CRITIS entails an effort that is largely invisible

to the participants. With gratitude I like to thank the local organising team, general chairs, the Technical Program Committee members whom voluntary did their review work and provided insightful reviews and comments to the authors of the submitted papers, the contributions by the keynote speakers, and the support of the host organisation TNO, the City of Amsterdam, The University of Twente, The Hague Security Delta (HSD), and the Shell Technology Centre Amsterdam (STCA). Together with the contributions to the discussions and interactions between all conference participants, this resulted in a very successful and stimulating CRITIS 2013 conference which laid the foundation for the upcoming CRITIS 2014 conference.

## Links

ECN home page <http://www.ciprnet.eu>

### Forthcoming conferences and workshops

CIPRE [www.cipre-expo.com](http://www.cipre-expo.com) 12.-13.2.2014 London, UK  
CRITIS 2014 [www.critis2014.org](http://www.critis2014.org) 8-10.10,14 Limassol Cyprus

TIEMS Forthcoming conferences, workshops and reports from previous events:  
<http://tiems.info/About-TIEMS/TIEMS-2013-Events/index.php>

### Exhibitions

Interschutz 2015 <http://www.interschutz.de/86385> 8.-13.6.2015 Hannover ,Germany  
CIPRE [www.cipre-expo.com](http://www.cipre-expo.com) 12.-13.2.2014 London, UK

### Associations

International Federation  
for Information Processing: [www.ifip1110.org](http://www.ifip1110.org)  
RTD activities and services: <http://tiems.info/About-TIEMS/tiems-projects.html>  
Education Programs: <http://tiems.info/About-TIEMS/diverse.html>  
TIEMS Library: <http://tiems.info/About-TIEMS/tiems-library.html>  
TIEMS Newsletter: <http://tiems.info/About-TIEMS/tiems-newsletter.html>

### Project home pages

FP7 CIPRNet [www.ciprnet.eu](http://www.ciprnet.eu)  
FP7 ValueSec [www.valuesec.eu](http://www.valuesec.eu)  
HIPOW [www.hipow-project.eu/hipow](http://www.hipow-project.eu/hipow)  
ELITE [www.elite-eu.org](http://www.elite-eu.org)  
TWOBIAS <http://twobias.com>  
PRACTICE <http://practice.fp7security.eu>  
ERNICIP <http://ipsc.jrc.ec.europa.eu/index.php/ERNICIP/688/0/>

### Interesting Downloads

Critis' 11 Conference Proceedings: <http://link.springer.com/book/10.1007%2F978-3-642-41485-5>  
Critis' 12 Conference Proceedings: [www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8](http://www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8)

European Network and Information Security Agency [www.ENISA.eu](http://www.ENISA.eu)  
Publish reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection"  
[www.enisa.europa.eu/activities/Resilience-and-CIIP](http://www.enisa.europa.eu/activities/Resilience-and-CIIP)

Dutch National Cyber Security Strategy 2: [www.government.nl/ministries/venj/news/2013/10/28/collaboration-between-government-and-business-strengthened-in-new-cyber-security-strategy.html](http://www.government.nl/ministries/venj/news/2013/10/28/collaboration-between-government-and-business-strengthened-in-new-cyber-security-strategy.html)

Swiss Infrastructure Protection: [www.infraprotection.ch](http://www.infraprotection.ch)

Collection of Smart Grid related publications: [www.SGIClearinghouse.org](http://www.SGIClearinghouse.org)

Commented Power point presentation on Smart Grid (prof. Saifur Rahman:  
<http://www.saifurrahman.org/sites/default/files/u2/CEPS%20Rahman.pptx>

### Websites of Contributors

Norwegian Defence Research Establishment (FFI) [www.ffi.no](http://www.ffi.no)



# CRITIS 2014

9<sup>th</sup> International Conference on  
Critical Information Infrastructures Security  
October 8-10, 2014, Limassol, Cyprus  
[www.critis2014.org](http://www.critis2014.org)



# European CIIP Newsletter

March 14 – June 14, Volume 8, Number 1



# ECN

## Contents:

Editorial

CIPRNet Master Class EU

Austria: National  
CIP Inventory

Coincidence in Crisis

GRF / IDRC 2014

Books

EAIS 2014

CRITIS 2014



**> About ECN**

ECN is coordinated with  
The European Commission, was initiated by Dr. Andrea Servida,  
today funded by the European Commission  
FP 7 CIP Research Net CIPRNet Project  
under contract, Ares(2013) 237254

**>For ECN registration ECN registration & de-registration:**  
[www.ciip-newsletter.org](http://www.ciip-newsletter.org)

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

**>Questions to the editors about articles 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:**  
[www.ciprnet.eu](http://www.ciprnet.eu)

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

**>Founders and Editors**

Eyal Adar, Founder and CEO, WCK [www.wck-grc.com](http://www.wck-grc.com)  
Christina Alcaraz, University of Malaga, [alcaraz@lcc.uma.es](mailto:alcaraz@lcc.uma.es)  
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)  
Erich Rome, Fraunhofer, [erich.rome@iais.fraunhofer.de](mailto:erich.rome@iais.fraunhofer.de)

**>Country specific Editors**

For France: Michel Riguidel, ENST, [riguidel@enst.fr](mailto:riguidel@enst.fr)  
For Spain: Javier Lopez, UMA, [jlm@lcc.uma.es](mailto:jlm@lcc.uma.es)  
For Finland: Hannu Kari, HUT, [kari@tcs.hut.fi](mailto:kari@tcs.hut.fi)  
to be added, please report your interest

**> Spelling:**

British English is used except for US contributions

## Editorial

Intro	Cyber-attacks with physical impact: reality? by Elias Kyriakides & Bernhard Haemmerli	5
-------	--	---

## European Activities

CIPRNet Master Class	CIPRNet Master Class on ModSim of CI by Roberto Setola	7
-------------------------	---	---

## Country Specific Issues

Austria: National CIP Inventory	The Austrian approach to Critical Infrastructure Protection (CIP) Establishing the CI Inventory by Beate Wegscheider	11
------------------------------------	--	----

## Method and Models

Coincidence in Crisis	Simulation and Reality: Coincidence in Crisis happening by Mohamed Eid	13
Impact Analyses	Economic Perspectives on Security Management by Gebhard Geiger	17

## About Associations

GRF / IDRC 2014	Global Risk Forum Davos and IDRC Conference by Walter Ammann	21
-----------------	---	----

## Books on C(I)IP

None in this issue	No Page
--------------------	------------

## Conferences 2014

EAIS 2014	EAIS 2014: Emerging Aspects in Information Security by Andrzej Białas	25
CRITIS 2014	CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security by Elias Kyriakides	27

## Links

Where to find:	<ul style="list-style-type: none"><li>• Forthcoming conferences and workshops</li><li>• Recent conferences and workshops</li><li>• Exhibitions</li><li>• Project home pages</li><li>• Selected download material</li></ul>	30
----------------	--	----

# Editorial: Cyber-attacks with physical impact: reality?

After Snowden's disclosure we know how often systems are under control by others than the owner: is this real and what does this mean for CIP?

Eduard Snowden has given us references to facts that an Information Infrastructure insider knew before. With the references given by Snowden we can start a broader community discussion on what this means for us, when we operate systems that we cannot rely on, or not trust. In everyday ICT we depend on the services; however, we can build a trade-off between how much more efficient we work with these marvellous ICT tools, and the small likelihood that sometimes the system does not do what we want.

In Critical Infrastructures and its critical services by definition we care for best availability and resilience: if this fails, large economic damage, high negative impact on citizens and society is presumed. The name "Critical" is descriptive for what could happen and indicates a zero failure policy.

In crises situations with potential harm to critical infrastructures we depend on our monitoring systems. There are two cases that we would like to share with you:

- Fukushima Nuclear Power Station, March 16, 2011 case: When the catastrophe was evolving, the power went off. As a reaction the engineers went for batteries to supply the most important instruments in the control room. Connecting these to power, the personnel obtained measurements from the reactor. At this time nobody thought that these measurements could be erroneous, and personnel in the control room believed, that water in the reactor is still sufficient. Later investigation disclosed that the water was at this time nearly completely exhausted.
- During the Honours Colloquium 2011 "Cyber Warfare" min 45-47 [www.youtube.com/watch?v=wRttZgeTrZQ](http://www.youtube.com/watch?v=wRttZgeTrZQ), Richard Clarke – a long year security advisor of the White House explains how Israeli Air Forces attacked Syria without being attacked by air

defence weapons. This worked as follows: The Israeli hackers penetrated the air control room software, such that they could make the system see a clear airspace during the bombing attack operation. Literally, Israeli hackers switched off air control systems of Syria.

With this hack, the control room of a critical infrastructure preserving the air space of Syria was under control of Israel: a fact that we could not explain that well to the public before Snowden.

Reflecting on cyber depending infrastructures, the CRITIS community has to engage even more than before to:

1. Promote C(I)IP on national level as well as universities.
2. Work towards diversity in the C(I)IP community by including the younger generation because they have a different perception of ICT and were completely, differently, systematically and profoundly educated in ICT.
3. Work towards architecture with fallback positions on minimum operational level, when the cyber dimension is harmed.

The EU FP7 NoE project CIPRNet has initiated a **Young CRITIS Award (CYCA)** exactly for attracting young researcher to this very interesting interdisciplinary work domain. It is a unique chance for young experts to be recognised. Young experts are encouraged to participate in this competition, where useful feedback will be provided by established community experts. For more information:

[cyca.critis2014.org](http://cyca.critis2014.org)

As always, selected links – mostly derived from the articles – enhanced with some insider hints, events and exhibitions conclude this issue.

Enjoy reading this issue of the ECN!

*PS. Authors willing to contribute to future ECN issues are very welcome.*



**Elias Kyriakides**

is an Assistant Professor at the Dept of Electrical and Computer Engineering and the Associate Director for Research at the KIOS Research Center for Intelligent Systems and Networks, University of Cyprus

e-mail [ellas@ucy.ac.cy](mailto:ellas@ucy.ac.cy)



**Bernhard M. Hämmerli**

is Professor at Lucerne University of Applied Sciences and Gjøvik University, CEO of Acris GmbH and President of Swiss Informatics Society SI [www.s-i.ch](http://www.s-i.ch)

e-mail: [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)

He is ECN Editor in Chief

# **CRITIS 2014**

9<sup>th</sup> International Conference on  
Critical Information Infrastructures Security  
October 13-15, 2014, Limassol, Cyprus

[www.critis2014.org](http://www.critis2014.org)

With

## **Young CRITIS Award Competition**

[cyca.critis2014.org](http://cyca.critis2014.org)

(see last article  
and last page)

# Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (CI)

On 24-25 April, in Paris, the first edition of the training course arranged inside the FP7/ NoE CIPRNet will be held, to contribute towards the CIP community in Europe and as a step towards the creation of the EISAC (European Infrastructure Simulation and Analysis Center)

The European Council Directive 2008/114/EC pushed the EU and Member States to address the CIP topic, but there is still a lack of common taxonomies, ontologies, metrics, and risk management frameworks for CIP-related risks and threats that represent serious barriers which need to be overcome. Moreover, the capabilities towards better understanding CI dependencies, cascading failure, and subsequent societal impact are still limited and need to be improved. This is because the CI in European countries form a gradually changing and increasingly complex system; as their interconnectivity continues to increase, so too do their vulnerabilities. To name just two: (1) CIs are becoming increasingly vulnerable to cyber threats and (2) the disaster risk due to natural hazards (e.g. floods) is increasing due to land use expansion and climate change. In addition, disasters involving or affecting CI may be caused by a wide variety of trigger events, (e.g., earthquakes, terrorist attacks, forest fires, human errors and technical failure). Each disaster has its individual course of events, a fact that makes effective responses difficult to plan, train for and subsequently apply. To effectively respond to a large disaster, it is mandatory to perform an adequate pre-event analysis of the threats, possible impacts, and the design, deployment and test of emergency plans, to include the training of the different operators.

Hence there is a need to “bust-up” the capability of emergency management response centres to assess the consequences of potential courses of action (CoA) in order to make well-informed decisions. Assessment of the (possible) effects of concurrent CI disruptions and cascading failure (electricity, drinking water, transportation, etc.) via “what-if” analysis and serious crisis gaming is of increasing importance to the CoA analysis. These comprise the prevention, preparation, response, and recovery/restoration phases of emergency management. The analysis of the CoA consequences on the short and long term shall be based upon real-time and statistical data, current CI status, meteorological and economic data, and more.

For these reasons, in the last two decades the world has seen an increase in the research of computer-based Modelling, Simulation and Analysis (MS&A) of Critical Infrastructures (CI). This multi-disciplinary field of Critical Infrastructure Protection is both an essential method for analysing the complexity of CI systems and an additional means of training crisis managers in complex scenarios involving disruptions of multiple CI. MS&A is reaching a level of maturity which is graduating out of the research centre and into the actual design and management of complex systems for stakeholders.

In this framework, the CIPRNet consortium would like to contribute towards the growth of the CIP community via a series of training events with the focus to **remove**



## Roberto Setola

Roberto Setola is professor of Automatic Control at University Campus Bio-Medico of Rome and head of the COSERITY Lab (Complex Systems & Security Lab). He is also the director of the Post Graduate program in 'Homeland Security, Systems and methods and tools for security and crisis management'.

He is the coordinator of the EU DG HOME project FACIES on the automatic identification of failure / attack in critical infrastructures, and the EU DG HOME project SLO on the professional figure of the Security Liaison Officer. He has been the coordinator of the EU DG JLS project SecuFood on security of the food supply chain, and was involved in many other CIP projects.

e-mail: [r.setola@unicampus.it](mailto:r.setola@unicampus.it)



**some of the barriers for faster progress in CIP.** For example, addressing the lack of comprehensive 'repositories' (i.e., the results are dispersed among several sources) and the absence of a common vocabulary / language.

The main goal of the Master Class is to illustrate methodological instruments to forecast the behaviour of Critical Infrastructure during their nominal operational conditions and during crisis situations. This will allow us to estimate the direct and indirect impact(s) on other infrastructures, the environment and the population.

The Modelling Simulation and & Analysis tools of CI have matured out of the research centre and into the field to become a valuable tool capable of supporting design, management and supervision of CI

During the 1.5-day training event to be held inside the UIC headquarters on 24-25 April in Paris, top-class experts in Europe in the field of CIP will provide a strong multi-disciplinary and stimulating environment where

they will share valuable knowledge about several topics related to CIP.

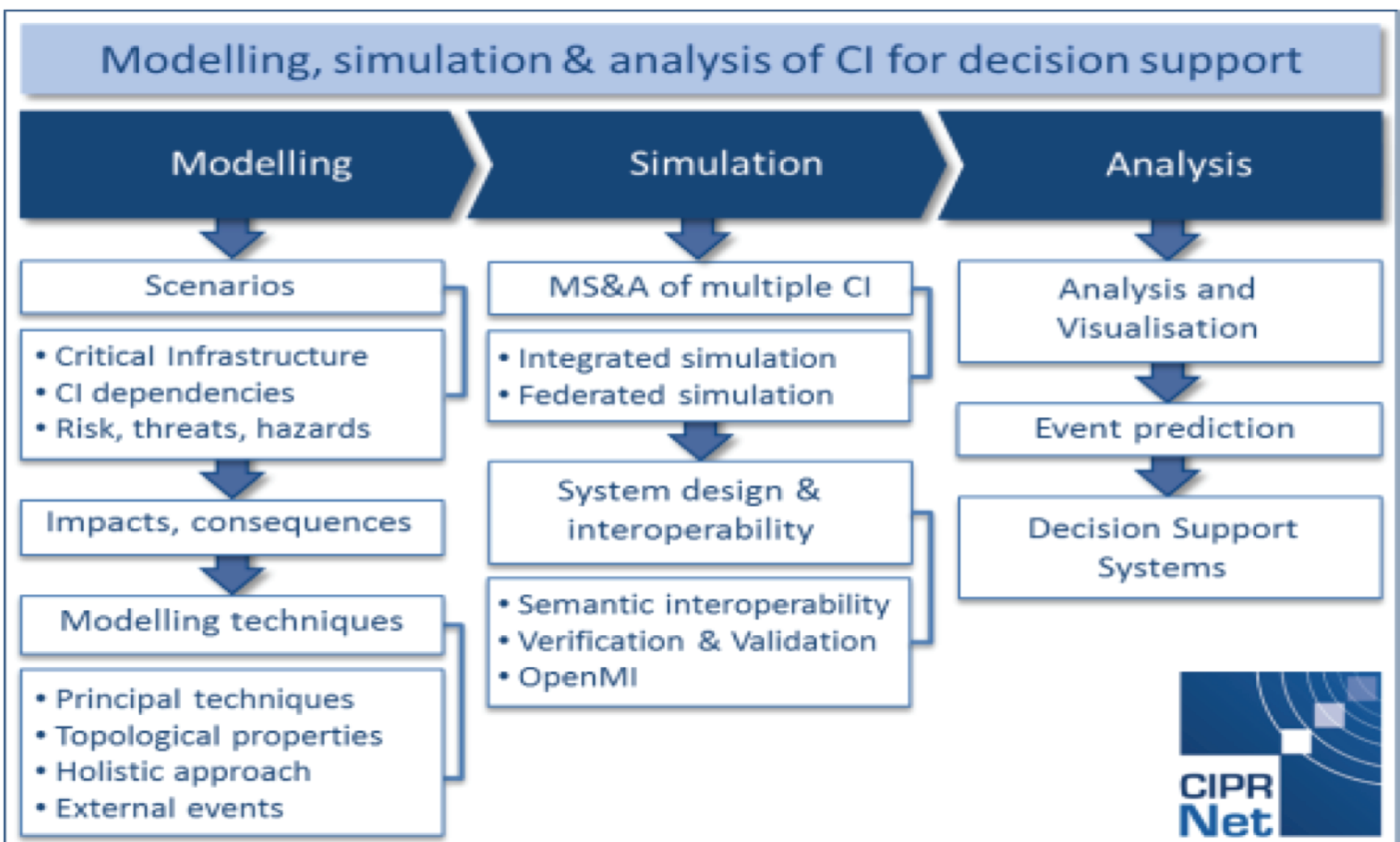
Specifically the Master Class will illustrate the different methodologies and tools developed to model CI and their specific phenomena as dependencies and interdependencies. The class will further illustrate the effectiveness of the different approaches, in terms of capabilities, and provide the necessary information needed to set-up the different models. Finally, the class will demonstrate how external events, such as natural disasters, may be described and integrated into CI models.

Successively the Master Class will illustrate how the CI models have to be implemented into a simulation framework considering the aspects related with the verification & validation of the solutions. It will analyse the different simulation schemas with a strong focus on the federated simulation, which allows one to make interoperable CI specific simulators. Such a solution is possible thanks to the capability to re-use the existing code and minimize the need to share information. In this structure, a specific attention will be

given to the OpenMi framework which recently acquired large interest from several specific domains.

The availability of a simulation tool is the basic element needed to design a DSS (Decision Support System) capable of providing an estimation of possible consequences to adverse events and comparing the effectiveness of different contingency strategies. Indeed the complexity of actual scenarios makes it impossible to correctly predict the impact of any event. The Master Class will illustrate the basic features of a DSS to be used for improved management of CI during a crisis. It will also illustrate schemas on how to relay real-time information on external conditions during a crisis.

The topics will range from the basic concepts of MS&A to advanced aspects related to federated simulation, Decision Support Systems (DSS), and the use of the Open Modelling Interface (OpenMI)



The Master Class will be repeated next year in Rome where additional focus on the design problem of DSS will be explored, allowing the attenders to perform real-scenario analysis exploiting the features of the CIPRNet DSS. The last edition of the Master Class is scheduled for 2016 in Bonn, where the focus will be on "what-if" analysis.

For more information on the program and for registration please visit the following website:

The participation to the Master Class is free of charge, but for logistic reasons it is limited to 40 participants.

<http://www.ciprnet.eu/endusertraining.html>

For any general questions regarding the Master Class, please contact:  
[c.romani@unicampus.it](mailto:c.romani@unicampus.it)

# Modelling, Simulation and Analysis of Critical Infrastructures



**International Union of Railways – UIC, Headquarters  
Paris, 24-25 April 2014**

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

This Master Class is the first edition in a series of training events organised within the European Project **CIPRNet – Critical Infrastructure Preparedness and Resilience Research Network**, with the aim to perform training and activities for the *Critical Infrastructures Protection* community, in order to strengthen the links between different research institutions and create common views. In this two-day master class, basic concepts about MS&A (Modelling, Simulation and Analysis) of Critical Infrastructures and advanced aspects related to federated simulation, Decision Support System (DSS) and the use of the Open Modelling Interface (OpenMI) will be illustrated in a multi-disciplinary framework. Top experts from various backgrounds coming from all Europe will be presenting lectures. The master class is addressed to both researchers and technicians from different research communities and experts from CI operators and Public Authorities.

The event is free but limited to a maximum of 40 participants with a first-come, first-served basis. The application must be sent **no later than 9 April 2014**.

Detailed program and application <http://www.ciprnet.eu/training.html>

For more information and specific requirements [c.romani@unicampus.it](mailto:c.romani@unicampus.it)

## Information about the Venue:

International Union of Railways – UIC  
16 Rue Jean Rey, 75015 Paris (France)

How to get there: <http://www.uic.org/spip.php?article2689>



The Master Class is organized by:

University Campus Bio-Medico of Rome, International Union of Railways,  
and French Alternative Energies and Atomic Energy Commission

# The Austrian approach to Critical Infrastructure Protection (CIP)

As one of the leading countries in the implementation and the support for the development of the European Programme on Critical Infrastructure Austria is now drafting a new Programme on CIP on the national level.

Following the terrorist attacks in London and Spain in 2004, the European Union started with the development of a "European Programme for Critical Infrastructure Protection" (EPCIP). Since then, the importance of this topic as well as the awareness on governmental level have simultaneously increased.

Consequently, the EU Member States launched their corresponding national programs as encouraged by the European Commission.

The starting signal for the "Austrian Programme on Critical Infrastructure Protection" (APCIP) was in 2008 with a resolution of the Council of Ministers. The resolution accompanies the so-called "Masterplan" which sets forth the APCIP. The Austrian Programme is characterized by being based on the principles of EPCIP and being complementary to it.

Critical Infrastructures are infrastructures, or parts of it, which are of strategic importance for the maintenance of fundamental social functions. The disruption or destruction of these infrastructures has severe implications on the health, security or the economic and social welfare of the society or the effective functionality of the public facilities.

The primary objective of APCIP is prevention. Contrary to other EU Member States, Austria has chosen a systemic approach for its programme. Therefore, it is not key if the infrastructure (e.g., electricity) is available, but if the system as a whole works. In addition, Austria abstains from a legal approach and

seeks for cooperation between the administration, economy and academia. Hereby, the creation of mutual confidence is of particular importance and APCIP-partnerships are pursued.

Since 2008 Austria has implemented the measures as well as the action plan of the APCIP Masterplan of 2008. Hence, the further development of the Austrian approach was necessary, wherefore the APCIP Masterplan 2014 is now being drafted.

On the one hand, the new Masterplan is supposed to display the changed setting for CIP in Austria through the implemented measures and objectives of the 2008 Masterplan. On the other hand, it will take into consideration the acquired knowledge of the last years as well as intersecting themes like Cyber Security.

The most essential aims Austria has reached with the implementation of its Masterplan 2008 are the following:

## Identification of Austrian Critical Infrastructure

The protection of Critical Infrastructures is vitally important for the Austrian Security Agencies in order to secure the maintenance of services for the public and with it the internal security. A crucial step therefore was the identification and designation of Austrian Critical Infrastructure (ACI). Significant criteria for the identification of ACI were

- the relevance of the infrastructure for life and health, public security, economic and social welfare of the population, as well as for the ecology;
- the avoidance of loss of service;
- the business location Austria and specialized services.



### Beate Wegscheider

Beate Wegscheider is a Security Policy Officer at the Security Policy Centre in the Austrian Federal Ministry of the Interior in Vienna.

She received her Masters degree from the University of Vienna in 2008. Beate is currently in the process of finishing her PhD thesis in Political Science. In addition, she has completed several trainings in the field of Common Security and Defense Policy, Security Sector Reform, Peacebuilding and Peacekeeping as well as Election Observation. Her fields of interests include the demographic change and its implications for internal security, conflict transformation and management and European security policy.

She regularly participates at national and international conferences and workshops in the field of security and international politics.

e-mail:  
[beate.wegscheider@bmi.gv.at](mailto:beate.wegscheider@bmi.gv.at)

For the allocation of the strategic infrastructures the ÖNACE-classification was used which enables national and international comparability.

The compiled list of ACI is a living document which needs to be evaluated and updated frequently.

## Guideline for CIP Infrastructure

After having identified the Austrian Critical Infrastructures, a guideline was developed for operators and owners of ACI. The guideline is meant to raise awareness at the CEO level and to support the setting up of comprehensive security architecture within the Infrastructure.

Furthermore, it aims to increase the availability of services and products of vital importance for the public. For this reason the guideline is supposed to assist in

- the identification of risks for strategic infrastructures;
- the implementation of risk reducing measures and
- the implementation of preventive and reactive measures against extraordinary events causing damage.

On the one hand, the guideline describes international norms and standards relevant for risk management processes and indications for national and international best practice models and corporate security management. On the other hand, it also offers a self-evaluation in the form of a structured questionnaire to assist with the identification of risks and possible preventive and reactive security measures. Furthermore, it offers recommendations for improvement.

All identified ACIs have received the guideline for self-evaluation and were requested to announce a point of contact within the enterprise to attend the CIP public-private partnership.

## Public-Private Partnership

In 2008, the European Commission also submitted a proposal on a Warning and Information Network for Critical Infrastructures (CIWIN<sup>1</sup>). After

an intensive consultation process the European information platform finally went live in 2013. The platform offers registered members of the CIP-community the possibility to discuss and exchange relevant information, surveys and best-practice models. In addition, each EU member state was offered the opportunity to set up a national page on CIWIN-EU.

Austria has taken this opportunity and established a national CIWIN page for the Austrian CIP-community which will serve as an information platform on CIP.

Up to date Austria is the only EU Member State that has established a national CIWIN information platform.

## The new Critical Infrastructure Unit

On the operational level, the Federal Agency for State Protection and Counter Terrorism has established the new unit "Critical Infrastructure Protection and Cybersecurity". Primarily, the unit supports strategic infrastructures with the implementation of comprehensive security architecture. For this purpose it offers concerted consultations, identification of risks and threats and provides information about current threats.

Moreover, specific situation reports as well as information regarding available products, mentoring and trainings in the areas of e.g. physical protection, risk management, IT-security, business crime, economic and industrial espionage, terrorism and extremism will be provided.

Supplementary, a contact and reporting point for operators of critical infrastructure has been installed.

## Nexus Cyber Security

A close content-related correlation exists between Cyber Security and the Protection of Critical Infrastructure. The Austrian Cyber Security Strategy provides measures for the protection of critical infrastructures in the field of action 4 and other areas. The Operational Coordination Structure (OCS) will support the ACIs on operational level and in particular in the event of failure of information and communication structures. Through the OCS they will also be

provided with information on the dangers of the Internet. According to the Austrian Cyber-Security Strategy, cyber-safety standards for ACI need to be defined and crisis and continuity plans for the common overall cyber crisis management compiled.

Furthermore, the Austrian Cyber Security Platform will be established as a public-private partnership. The aim of the platform is to facilitate ongoing communication with all relevant stakeholders of the administration, economy and academia.

A legal regulation on the notification requirement for severe incidents for strategically important infrastructure needs to be prepared.

The corresponding task forces are currently incorporating these requirements in their work.

As outlined, Austria has made some considerable steps forward in the enhancement of the protection of its critical infrastructures. With the new Masterplan of 2014 the renovation of the Austrian programme will be brought forward.

If you would like to find out more about the work of the Federal Ministry of the Interior please visit our website [www.bmi.gv.at](http://www.bmi.gv.at).

<sup>1</sup> Critical Infrastructure Warning and Information Network

# Simulation and Reality: Coincidence in Crisis happening

Severe accidents and crises are the result of the unlikely accumulation of many random hazardous events. Some would call that “black series” or “bad coincidences”. But coincidences are unlikely to happen twice!

Formal sciences ultimate target is to represent the reality of our surrounding world. Many philosophers and scientists believe that the reality revealed by Science offers only a “veiled” view of an underlying reality that Science cannot access. These are mainly because of two reasons: formal sciences are imperfect and what we call “reality” is the projection of the inaccessible “Reality” on our world. We will call this projection on our world “the reality”. It is the only reality we are talking about through our article. More interesting points of views may be found in ([1],[2])

Struggling to approach their ultimate target, formal sciences construct objects in which small parts of the reality are grasped and formalised. These objects could be called “models”. Because we are limiting our interest only to formal sciences and engineering, these objects are mathematical models. That covers both conceptual and phenomenological models. Models are first validated before being admitted in the global modal of the reality.

Engineering sciences are amongst the most active in producing, validating and applying mathematical models in different aspects of our daily life. Based on the models, engineers and researches are developing robust simulation capabilities of the reality making use of the modern capabilities of performing intensive and coupled calculations. The ambition is to simulate not only independent isolated phenomenon but also of interacting phenomenon belonging to different physics at varying scales.

Regarding our main concerns of protecting critical infrastructures and helping in decision-making in case of severe accidents or crises, advanced simulation capabilities play a decisive role. The simulation of well-defined sequences of events leading to major potential crises is of great help in:

- Decision making in order to elaborate the best strategies in managing crises and severe accidents.
- Helping operators to prioritize actions in real situation facing systems' primary failures and their propagation.
- Helping designers to improve systems' design in view of minimizing failures' frequency and failures propagation and of maximizing consequences mitigation.
- Training future technical staff and qualified persons who will be engaged in systems design, systems operation and crisis management.

Developing powerful integrated simulation capabilities is a serious challenge to all the scientists and the engineers in the field. This ambition gives birth to two major challenges:

- Developing and validating models considering dependencies and interfacing between different physics at varying scales.
- Integrating stochastic and random phenomenon in a global coupled modelling process.

Both challenges are of the same importance but we will focus on the stochastic aspects of events initiating severe accidents. Major crises result very often from the occurrence of some sequences of random events that are combined with some systems' failures, resulting at the end of the sequence serious hazards.

We can mention some examples such as: the Concorde crash (AF4590, Paris-New York, 25 July, 2000) [3][3], the EU Blackout (Saturday-Sunday 4-5/11/2006, EU) [4] or the Fukushima accident (11 March, 2011, Japan) [5]. All are cross-border accidents. In all these cases, it was the sequential accumulation of independent random events that led to the severe accident. Let's take the crash of the Concorde in order to identify the sequence of the



**Mohamed Eid**

Mohamed Eid is a Senior Expert in the French Commissariat of Atomic Energy & Alternative Energies (CEA) and an Associated Professor in the National Institute of Applied Science (INSA) of Rouen. His research and teaching activities cover fields such as: Probabilistic Risk Analysis, System Reliability and Safety, Monte-Carlo simulation, Multi-States System Modelling, Systems Dependency and Interdependency. He is the author of some 50 scientific papers in the field of systems safety, reliability and stochastic modelling.

He is a member of many editorial boards of scientific journals in the field of system reliability, safety and maintenance.

An active member in many EU networks: ESReDA, CIPRNet, ...  
An active member in many EU conference series programme committees: ESRel, ESReDA, SSARS, Lambda-Mu etc.

email: [mohamed.eid@cea.fr](mailto:mohamed.eid@cea.fr)

independent random events that led to the major event. We will not go through the details of the accident analysis report, [3]. We will only underline the sequence of these random events.

The post-accident investigations revealed that:

- The aircraft was over the maximum take-off weight for the ambient temperature and the other conditions, and 810 kg over the maximum structural weight. (It is useful to underline that the total fuel capacity is 95 680 kg and the max take-off weight is 185 065 kg).
- The load was distributed such that the centre of gravity was excessively far to the rare.
- Fuel transfer may have overfilled the wing tank number five.
- Five minutes before the Concorde, a Continental Airlines DC-10 departing for Newark, New Jersey, had lost a titanium alloy strip, 435 millimetres long and about 29 to 34 millimetres wide, during take-off from the same runway.
- This piece of debris, still lying on the runway, cut a tyre, rupturing it, during the Concorde's subsequent take-off run.
- A large chunk of tyre debris (4.5 kilograms) struck the underside of the aircraft's wing at an estimated speed of 140 metres per second. The strike sent out a pressure shockwave that ruptured the number five fuel tank at the weakest point, just above the undercarriage.
- Leaking fuel was most likely to have been ignited by an electric arc in the landing gear bay or through contact with severed electrical cables.
- The flame before the Concorde was airborne.
- With only 2 km of runway remaining and travelling at a speed of 328 km/h, the only option was to take off. The Concorde would have needed at least 3 km of runway to abort safely.

Let's now identify the random events that led to the major accident event. In that very succinct description of the sequence development, one may identify the random/stochastic independent events as following:

- Overloading: what is the probability for the Concorde to be overloaded by a factor less than or equal to 0.5% of its take-off

weight, considering the ambient temperature and other conditions? Knowing that the ambient temperature and the other meteorological conditions are themselves stochastic (random with time).

- Load distribution: what is the probability that the load (overloaded or not) is not correctly distributed and results in an excessive offset of the plane gravity centre?
- Foreign objects on the runway: what is the probability of introducing a metallic object on the runway between two successive runway inspections?
- Detecting objects on the runway: what is the probability of not detecting a metallic strip (40x30cm) on the runway in 5 minutes?
- Tire collision with a metallic object on the runway: what is the probability that one of the tires of an airplane hits a metallic object on the runway during take-off?
- Tyre blow out: what is the probability that the hit tyre blow out?
- Heavy chunks production as a result of a tyre blow out: what is the probability that the blown tyre sends out heavy chunks (> 2-3kg)?
- Collision with a fuel tank: What is the probability that the flying heavy chunk strikes violently (> 100 m/s) any of the wing fuel tanks?
- Tank puncture by direct impact of a heavy chunk at high speed: what is the probability that the violent strike punctures the tank?
- Tank rupture by shockwave propagation: what is the probability that the violent strike produces a shockwave capable to rupture the tank at any of its weak points, if the tank was not punctured first?
- Fuel fast ignition: what is the probability that the leaked fuel could be ignited within a very short time (~ few seconds after leak)?
- No abortion possibility: what is the probability of a successful abortion as function of the run distance and airplane speed?
- Fuel slow ignition: what is the probability that the leaked fuel could be ignited within a longer time (~ the first 30 minutes, hour, 2 hours, ...)? After taking off and attending heights where the ignition conditions are not favourable!

The sequence of interest is then defined by 11 independent events: airplane overloading (~0.5%), inadequate load distribution, introduction

of a large foreign object on the runway, non-detection of large foreign object on the runway within 5 minutes, collision of an existing object on the runway with one of the tyres during take-off run, tyre blow out as a result of a collision with a large metallic object (435 mm long and 29 to 34mm wide), fragmentation of a blowing tyre into heavy chunks (> 2-3 kg), collision of a heavy flying chunk with one of the fuel tanks, rupture of the collided tank (directly or indirectly) following the collision, immediate ignition of the leaked fuel and no more enough distance on the runway to abort safely. This is a sequence of 11 independent and random / stochastic events (coincidence?).

The same demarche of analysis can be performed for the EU Blackout (Saturday-Sunday 4-5/11/2006) and for the Fukushima accident (11 March, 2011, Japan) in order to identify the sequence of independent random/stochastic events that led to the final hazard. However, we will only recall succinctly the description of the final hazard in both accidents.

In the case of EU Blackout (Saturday-Sunday 4-5/11/2006), [4]: A power imbalance in the Western area induced a severe frequency drop that caused an interruption of supply for more than 15 million European households (for about 2 hours). The detailed analysis of the events and the sequence identification are given in [4].

In the case of the Fukushima accident (11 March, 2011, Japan), [5], following a strong earthquake and a strong tsunami. The nuclear power plant of Fukushima (4 reactors) had lost the electrical supply from the grid and the emergency electrical supply units on the site. Subsequently, that resulted in a significant loss on different control capabilities and the loss of the reactor cooling systems of three reactors. The overheating of the reactors lead to the production of a significant quantity of hydrogen in one of the reactors which exploded on 12 March resulting in the blowing out of the ceiling of the reactor building number one. A significant release of radioactive materials had subsequently been monitored. The detailed analysis of the events and the sequence identification are given in [5]. Some analysts may think that strong earthquakes result always in strong tsunamis. This full

correlation between these two events is not proven. A probabilistic correlation exists however less stronger earthquakes can still result in strong tsunamis, ([6],[7]). In all cases of severe accidents and crises it is a matter of a sequence of ordered well-defined random / stochastic events.

## Coincidence?

Severe accidents and crises are the result of the unlikely accumulation of many random hazardous events. Some would call that "bad coincidences" or "black series".

In the case of the Concorde crash, we have too many unlike and independent random and stochastic events in one sequence! Even if some are highly probable such as: the blowing out of a tyre after the collision with a heavy metallic object and the tank rupture following a violent collision with a heavy object flying at high speed. Others are not, such as: the introduction of a large foreign object on the runway between 2 successive take-offs runs and the collision of a heavy chunk with one of the fuel tanks.

In these long sequences of random events, it is enough that a few events show low occurrence probabilities so that the occurrence probability of the whole sequence becomes very low. For example we may imagine that if the occurrence probability of the event "inadequate load distribution" was knowing that the overloading was within a very low range ( $< 0,5\%$ ) and if the occurrence probability of the event "non-detection of a large foreign object on the runway within 5 minutes" was in the range of  $10^{-3}$ - $10^{-4}$ , the occurrence probability of the sequence would already be in the range  $10^{-6}$ - $10^{-7}$  per take-off run, assuming that all the other 9 events had occurrence probabilities close to one ( $\sim 100\%$ ).

What is "Coincidence"? I would answer "Coincidence" would be underlined in two manners:

- Objectively: when some random unlikely events included in a well - defined sequence occur in a given order. Here, we are more interested in the occurrence probabilities of the individual events and less interested in the sequence occurrence probability itself.
- Subjectively: when a sequence with a very low occurrence probability occurs to "Me".

We will be interested in the object (mathematical) perception of the "Coincidence". Coincidences do objectively occur whatever is the low occurrence probability of the whole sequence. Coincidences have a sense when it is a matter of: many events (not only one event), random (/stochastic) and in a given occurrence order.

## Probabilistic Modelling

More complex are the systems man designs, more complex are the hazardous sequences in case of severe accidents and crises. Integrating probabilistic approaches would allow constructing global models in order to deal with phenomenon of different nature at varying scales.

## Mitigation

Analysing sequences of events lead systematically to improving the mitigation of the consequences of each individual random/stochastic event involved in.

Back to the Concorde crash, analysing the sequence of the individual events would suggest to:

- Improve the detection of foreign objects on the runway (this is not out of reach of our modern technology)
- Improve the resistance of tyres for collision with metallic heavy objects at high speed ( $\sim 300$  km/h)
- Improve the tyre's materials and fabrication process such that only small and very small chunks would be produced when blowing out.
- Improve the shielding against and the resistance of the fuel tank structure to the collision with heavy objects at high speeds.
- Find out design modifications to prevent the ignition of the spelled fuel during take-off.

## What if?

One way to cope with hazardous sequences is to question systematically us, what if:

- Such or such occurrence probability was less or higher?
- Such or such occurrence order was followed?
- Such or such component was lighter or heavier?
- Such or such shielder was thinner or thicker?

## Models & Simulation

Models and simulation do not describe exactly the reality. But they are perpetually in improvement to come closer and closer to the reality. We still talk about our local reality (the projection on our world) not the real Reality, which is certainly inaccessible. However, models and simulation help us to improve the quality of life and make it safer, every day

Robust models and powerful simulation capabilities are necessary in order to perform efficient "What if" analysis and to verify the validity of the different mitigation measures. We recall that we consider both conceptual and phenomenological models. It is the only way to perform, a priori, investigations of accidents and crises. Otherwise, we are condemned to perform posteriori investigations to come up with the same improvements. It is to say to wait for the occurrence of severe accidents and crises. But coincidences are unlikely to happen twice.

## References

- [1] Christian Hennig, "Mathematical Models and Reality – a Constructivist Perspective." Research Report No.304, Department of Statistical Science, University College London, June 2009. <http://www.ucl.ac.uk/statistics/research/pdfs/r304.pdf>.
- [2] John Byl, "Mathematical Models and Reality." Proceedings of the 2003 Conference of the Association for Christians in the Mathematical Sciences.
- [3] BEA final report, 'Accident on 25 July 2000 at La Patte d'Oie in Gonesse (95) to the Concorde registered F-BTSC operated by Air France.' F-BTSC - 25 July 2000.
- [4] UCTE Investigation Committee report, "Final Report System Disturbance on 4 November 2006." Union for the Coordination of Transmission of Electricity, 30 January 2007. <https://www.entsoe.eu/news-events/former-associations/ucte/other-reports/>
- [5] NAIIC report, "The Official Report of Fukushima Nuclear Accident Independent Investigation Commission – Executive Summary." The National Diet of Japan, 2012. [http://www.nirs.org/fukushima/naaic\\_report.pdf](http://www.nirs.org/fukushima/naaic_report.pdf)
- [6] Hiroo Kanamori, "Mechanism of Tsunami Earthquakes." physics of



the earth and planetary interiors journal, 6, 346-359, 1972, North Holland Publishing Company.

[7] Eric L. Geist and Uri S. Ten Brink  
"NRC/USGS Workshop Report: Landslide Tsunami Probability."  
U.S. Department of the Interior

U.S. Geological Survey,  
Administrative Report, 2012



**46<sup>th</sup> ESReDA Seminar on  
Reliability Assessment and Life Cycle Analysis of  
Structures and Infrastructures  
(May 29<sup>th</sup> - 30<sup>th</sup>, 2014)**

**Politecnico di Torino, Torino, Italy**



## **ESReDA Reliability Assessment and Life Cycle Analysis of Structures and Infrastructures**

The aim of the 46th ESReDA seminar is to bring together scientists, engineers and decision makers in the field of structural safety and risk management, in order to present and discuss innovative methodologies and practical applications related to structural reliability and life cycle cost: assessment, testing, analysis, design, monitoring, maintenance and optimization. Scientific methodologies, theoretical issues and practical case studies are expected to cover all the range from academic to industrial applications, including mechanical and civil engineering. A selection from seminar papers will be published in the book edited by ESReDA on Reliability based Life Cycle Cost Optimization of Structures and Infrastructures.

### **ABOUT EUROPEAN SAFETY, RELIABILITY & DATA ASSOCIATION**

European Safety, Reliability & Data Association (ESReDA) is a European Association established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability.

For more information please visit the ESReDA home page: <http://www.esreda.org/>

# Economic Perspectives on Security Management

## Critical Infrastructure Security and Return on Security Investment (ROSI)

In view of growing threats to public safety and security and increasing budgetary restraints, risk management in government and industry must be both effective and cost-efficient. To this goal, recent advance in the econometric and operational sciences can be exploited to develop and apply a generic quantitative risk assessment methodology as a security planning and management device to protect public infrastructures and large-scale industrial systems. The concept of quantitative risk assessment thereby means the coherent intrinsic, or "fair", pricing of risks. It implies considerably more than risk measurement in the sense of statistical risk analysis ("intrinsic" refers to risk quantification within a given accounting system rather than to risk prices extrinsically determined by the market for risky goods or services).

It is evident that the practical use and public policy implications of a coherent approach to measure the intrinsic value of any given risk would be considerable. It could help to determine, in a realistic and systematic way, the amount of risk reduction achieved per euro invested in technologies and management efforts to prevent safety and security incidents in large-scale systems and public infrastructures, or mitigate the damage arising from such incidents. As for security management, this is exactly what is otherwise known, though largely missing in practical applications, as calculating the Return on Security Investment (ROSI).

### Quantitative risk assessment and the pricing of risk

Risk management has long been suffering from the fact that risk is an elusive concept. Correspondingly, existing methods to assess risks and risk reduction measures tend to be ambiguous and controversial, if not

manifestly inconsistent, for one of the following two reasons. They are either *ad hoc* rather than systematic, meaning that they lack theoretical coherence, or hard to operationalise. In either case, they may not provide the reliable information decision makers need to solve their problems.

Advance has recently been made on the basis of novel methodological approaches to economic utility theory and the statistical foundations of quantitative risk assessment [1, 2, 3, 4].

It is evident that the practical use and public policy implications of a coherent approach to measure the intrinsic value of any given risk would be considerable.

These approaches have in part been developed and applied within research projects on infrastructure security and security economics co-funded by the German government (SiVe, 2008-2011) and the European Union (ValueSec, 2011-2014). More details can be respectively found at <http://www.bmbf.de/en/13086.php> and <http://www.valuesec.eu>

The methodology for optimal, cost-efficient risk and security management employed in these projects involved concepts of "generalised expected utility" that have been demonstrated to be able to admit coherent, explicit numerical representations of risk preferences, while accommodating basic empirical, individual and social attitudes towards risk. Most importantly, however, they have proven to be sufficiently simple for operational use in applied risk research. Meanwhile, "utility" has nothing to do with naïve views of "degree of individual satisfaction", "desirability" and the like: it is a technical term simply meaning a behavioural risk preference score.



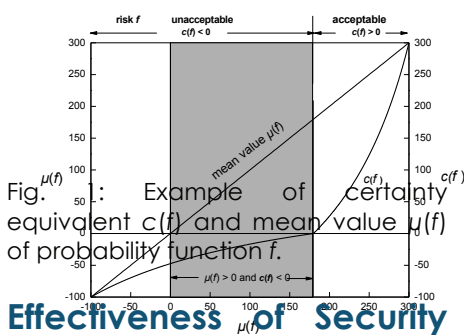
**Gebhard Geiger**

Gebhard Geiger is a professor of methodology and philosophy of science in the Technical University of Munich, Germany (TUM). He is specialising in foundational problems of the operational sciences, especially mathematical methods in risk and security research. He holds doctoral degrees in theoretical physics (Ludwig-Maximilians-Universität München, LMU) and philosophy of science (Habilitation, TUM), and an MA in political science (UCLA).

e-mail: [g.geiger@ws.tum.de](mailto:g.geiger@ws.tum.de)

The core concept of quantitative risk assessment is the pricing of risk. Risks can be formally represented as probability functions  $f(x)$  of the likely gains or losses  $x$  (in monetary terms or otherwise) obtained from safety or security incidents with uncertain consequences. A real number  $c(f)$  is called the *certainty equivalent* of the risk  $f(x)$ , if  $f(x)$  and the certain amount  $c(f)$  of gain or loss are indifferent in preference terms. The certainty equivalent of a given risk can accordingly be viewed as the fair, or "intrinsic" price of that risk, considering that  $f$  and  $c(f)$  are equal in preference. In practice, it can be explicitly calculated for every given probability function  $f$ .

Figure 1 illustrates important realistic features of the quantitative account of risk assessment. One such feature is the marked deviation of the fair price (curved line in Fig. 1) from the probabilistic mean value of a risk (straight line), thus expressing widely observed, non-neutral human attitudes towards risk. Another feature is the capacity of the present approach to accommodate patterns of variability of risk attitude across various dimensions of risk. Finally, this simple and straightforward concept of intrinsic pricing of risks provides a powerful management tool, admitting direct assessments to be made of the effectiveness and cost-efficiency of planning and decision-making under risk.



## Effectiveness of Security Risk Management

Real systems can generally be assumed to be operated with larger or smaller risk management effort. Two risks  $f$  and  $g$  linked to the effort aiming to mitigate them can be estimated, considering the likely consequences of security incidents affecting any such system considered. Furthermore, the risk prices  $c(f)$  and  $c(g)$  of the risks with and without appreciable risk management arrangements, respectively, can be calculated and compared. For example, the comparison  $c(f) \geq c(g)$  shows the effectiveness of the measures planned or taken to reduce the risk  $g$  to  $f$ . In this example, the price difference  $c(f) - c(g)$  is positive. It measures the Return on Security Investment (ROSI) that can be gained when the system changes from the risky state  $g$  to the less risky state  $f$ . If, on the other hand, the difference  $c(f) - c(g)$  is small or even turns out negative, the risk management proves ineffective.

## Cost-Efficiency of Security Risk Management

Let  $k(f, g)$  be the cost incurred by security managers to reduce the risk  $g$  to  $f$ . The ratio of ROSI to cost of the security arrangements made gives the amount of risk reduction per euro invested. It measures the cost-efficiency of the risk reduction achieved. Risk management is optimal if for given "status quo risk"  $g$ ,

Without the scanning machine in operation,  $x$  is the number of passengers killed or lives saved with probability  $g(x)$  if a terrorist smuggles an explosive device into the check-in area of the airport where he detonates his bomb. The equivalent number of lives saved or lost increases from the status quo with  $c(g) = 0$  and  $q = 0\%$  to  $c(f)$ , if money is invested to adjust  $q$  optimally. The cost-efficiency ratio  $c(f)/k$  reaches its maximum approximately at  $q = 58\%$  in this example.

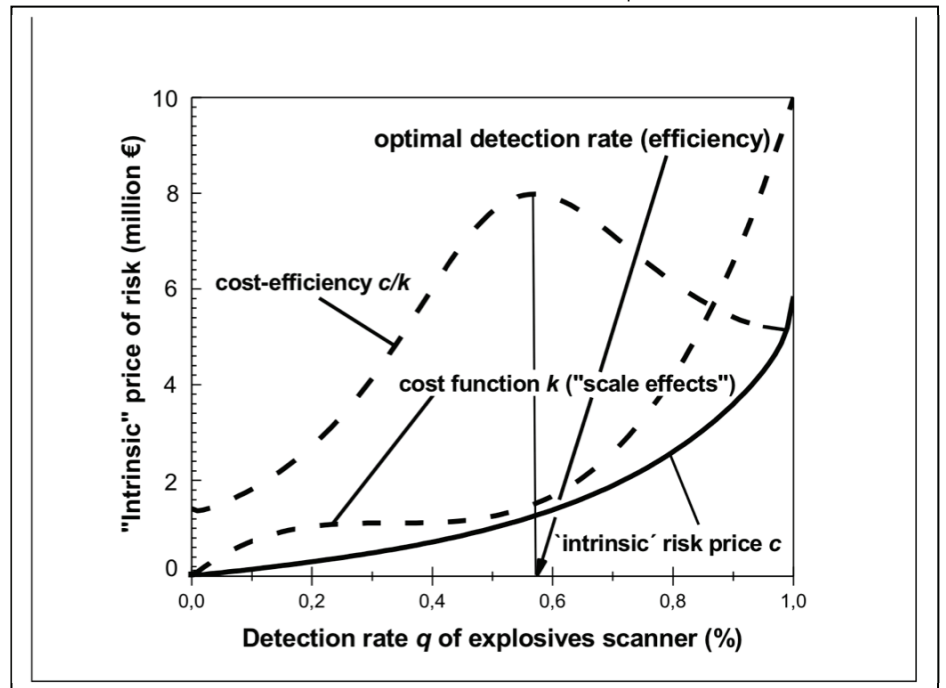


Fig. 2: Example of cost-efficiency of airport security management. After Goldner *et al.* [3].

the target risk level  $f$  is chosen so that the cost-efficiency ratio is at maximum within a given set of alternative risk mitigation choices.

A numerical example is shown in Figure 2. In the example,  $q$  is the rate with which a scanning technology detects explosives at the passenger and luggage checkpoint of an airport.

This simple and straightforward concept of intrinsic pricing of risk provides a powerful management tool, admitting direct assessments to be made of the effectiveness and cost-efficiency of planning and decision-making under risk.

## Modelling Airport Security Management

Safety and security planning in large-scale systems can be made very effective by combining scenario-based computer simulations of systems and processes (e. g., Monte Carlo simulations) with numerical estimates of damage probabilities in simulated safety and security incidents. The effectiveness and cost-efficiency of technical, organisational and procedural risk management provisions can thus be assessed quantitatively prior to their implementation.

Risk and security management as well as attacks can be modelled as processes. A process model may, in turn, help to identify all the relevant risks attached to a process itself or any further actions triggered by it. In airport security analyses, it is therefore important to develop a generic process model of terrorist attacks against airports first (Fig. 3).

Safety and security planning in large-scale systems can be made very effective by combining scenario-based computer simulations of systems and processes with numerical estimates of damage probabilities.

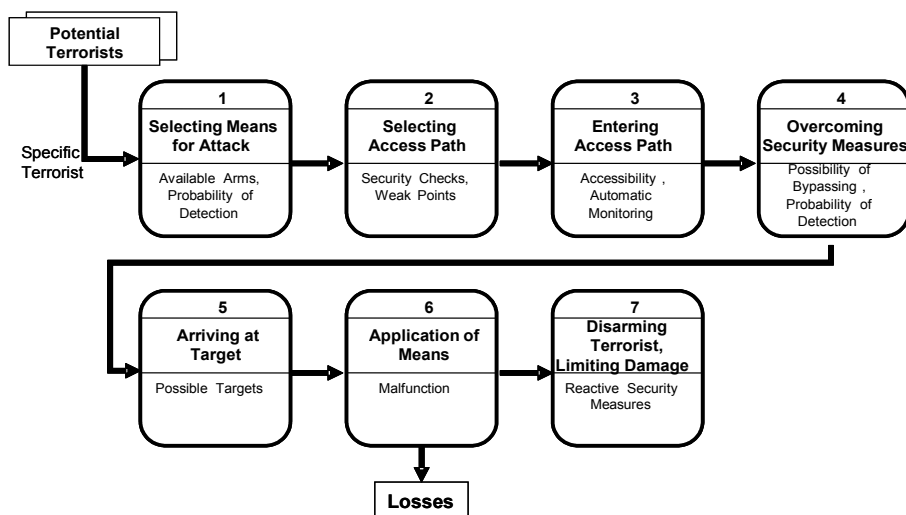


Fig. 3: Generic process model of a terrorist attack on an airport. After Geiger *et al.* [1]

If, for example, a terrorist attack on airport security using liquid explosives (liquids, aerosols and gels, LAG) is considered, the analysis must be carried out considering the following possibilities.

1. A terrorist (suicide bomber) is assumed to arrive at the airport security check. The probability of attack = 1 (i. e., a "What if" scenario is used). The terrorist carries a liquid explosive to be detected with probability  $q$  ("detection rate", see Fig. 2) or else passes the security check undetected with probability  $1-q$ . When detected he tries to detonate the explosive at the check point and kill himself and as many passengers as possible.
2. The situation is characterised by a number of parameters such as false clear rate, false alarm rate and other attributes of the operational performance of the LAG explosives scanning technology and staff such as quota  $q$ , if any, throughput time per passenger, number of passengers to be checked per hour operation time, etc.

3. If the terrorist succeeds to enter the aeroplane, with his liquid bomb undetected, the events occurring aboard generally depend on random factors: the terrorist attempts, more or less successfully, to mix components of liquid explosive; he may fail to get his bomb ready for use; he may be tackled and overpowered by passengers or crew (by an air marshal, if any); the bomb may fail to detonate; alternatively, it may be

4. Most importantly, the screening for LAGs makes impact (imposes limits) on terrorist's success: type and/or amount of usable LAG is restricted, detonator suboptimal or restricted (e. g., contains no metal parts), etc.
5. The possible courses of action aboard the plane are treated as outcomes of a random experiment. As such, they are assigned to (known, estimated, etc.) numbers of fatalities. The frequencies with which the fatalities occur are obtained in repeated (Monte-Carlo-like) trials of the experiment (in fact, each course of action is modelled as a "business process", using modern software-based processes modelling techniques).
6. The random simulations give the particular probabilistic distribution of fatalities involved in an incident. The extreme case is the detonation of the liquid bomb followed by an aeroplane crash, with all passengers and crew killed.
7. Using different fatality risk distributions  $f(x)$ ,  $g(x)$ , ... obtained

in the simulation experiments, the effectiveness and cost-efficiency of the alternative LAG screening technologies to prevent or mitigate these risks can be directly estimated and analysed in quantitative terms, as outlined above.

## Concluding Remarks

In view of the immense complexity of the infrastructures of modern society, incident simulation techniques and methods of quantitative risk assessment can be employed to prevent or mitigate damage from catastrophic events in systematic, practical, effective and cost-efficient ways. Some of the core problems involved here can be successfully addressed, combining methodological perspectives of modern systems analysis and simulation and econometric approaches to risk assessment.

## References

- [1] G. Geiger, E. Petzel and M. Breiing, "Process-Based Identification and Pricing of Risks: Methodological Foundation and Applications to Risk and Security Management". In P. Elsner (Ed.): Future Security – 4<sup>th</sup> Security Research Conference. Fraunhofer Verlag, Stuttgart 2009, pp. 208-220.
- [2] M. Breiing, M. Cole, J. D'Avanzo, G. Geiger, S. Goldner, A. Kuhlmann, C. Lorenz, A. Papproth, E. Petzel and O. Schwetje, "Optimisation of Critical Infrastructure Protection: The SiVe Project on Airport Security". In E. Rome and R. Bloomfield (Eds.): CRITIS 2009. Lecture Notes in Computer Science 6027, Springer-Verlag, Berlin-Heidelberg 2010, pp. 73-84.
- [3] S. Goldner, A. Papproth, E. Petzel and G. Geiger, "Improving the Security of Critical Transport Infrastructures - New Methods and Results". In J. Ender und J. Fiege (Eds.): 6<sup>th</sup> Future Security Research Conference – Proceedings. Fraunhofer Verlag, Stuttgart 2011, pp. 545-554.
- [4] R. Hutter and C. Blobner, "How to rationalise and economically justify security for CIP". European CIIP Newsletter Vol. 7, No. 1, 2013, pp. 9-11.

(Left intentionally blank  
for double sided printing)

# The Global Risk Forum GRF Davos

The Global Risk Forum GRF Davos promotes the worldwide exchange of know-how and expertise, creates solutions and fosters good practices in integrative risk management including climate change adaptation.

The foundation aims to improve the understanding, assessment and management of disasters and risks that affect human safety, security, health, the environment, critical infrastructures, the economy and society at large.

Through its various activities GRF Davos aims at serving as a centre of knowledge and know-how exchange for the application of contemporary risk management strategies, tools and practical solutions. Thus, GRF Davos aims at reducing vulnerability for all types of risks and disasters to protect life, property, environment, critical infrastructure and all means of business for the worldwide community on a sustainable basis.

As recent mega-disasters and crises have shown, risk management from a single perspective is no longer adequate to address the complex threats to today's society. A truly integrated and participative approach is necessary. This approach ensures that lessons learned in risk reduction are covered interdisciplinary and applied correctly. This will create safer, more resilient and thus sustainable societies for the benefit of communities, countries and regions.

## Integrative Risk Management

Integrative risk management stands for risk reduction and disaster management, and at the same time means vulnerability reduction and resilience increase. A multi-measures approach along the risk cycle including prevention, intervention and recovery is required. Preventive measures like land-use

planning, or technical and biological measures serve to reduce vulnerabilities.

Organisational measures such as early warning, contingency planning, emergency preparedness and emergency exercises, ICT and leadership in crisis response management are essential for resilience increase. Resilience measures are important for people and communities to render social groups more adaptable to disasters. The recovery process has to focus on build-back measures reducing vulnerability

### GRF Davos Slogan

From Thoughts to Action

*„We are bridging the gap between science and practice in the search for sustainable solutions.“*

## International Disaster and Risk Conference IDRC Davos – Call for Abstracts

**IDRC Davos builds bridges between science, technology, policy and practice.**

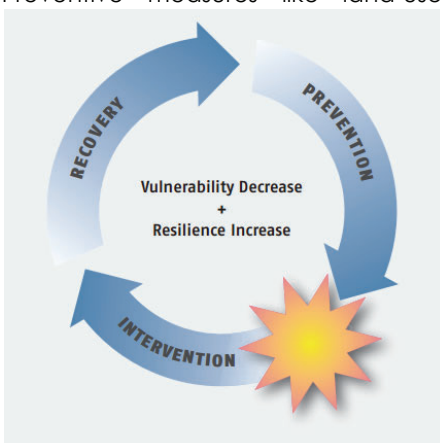
IDRC, the International Disaster and Risk Conferences and workshops, organized by the Global Risk Forum GRF Davos, are the ideal platform for assessment and dissemination activities, and in particular for networking activities. IDRC is the interface for experts, practitioners and institutions from science, technology, business, politics, and civil society to create transparency and encourage synergies to reduce and manage risks worldwide.



**Walter J. Ammann**

Dr Walter J. Ammann, Founder and President of the Global Risk Forum GRF Davos obtained his MSc in Civil Engineering and his PhD in structural dynamics and earthquake engineering both at ETH Zurich. He is an expert in integrative risk management and its applications to all kinds of natural hazards and technical risks, in particular by considering the entire risk cycle with prevention, preparedness, intervention and recovery. He has additional interest in risk financing tools, critical infrastructures, and resilience, for emergency management and communication tools with a focus on early warning, and crisis management. He is author and co-author of over 250 papers, books and scientific reports and is a member of various national and international professional associations and expert consulting groups like the UN-ISDR Scientific and Technical Advisory Group, and is Visiting Professor at HIT in Harbin, China and at Michigan State University, East Lansing, USA.

e-mail:  
[walter.ammann@grforum.org](mailto:walter.ammann@grforum.org)



IDRC attempts to find solutions to today's challenges by managing risks, reducing disasters and adapting to climate change. It helps build stronger ties with adequate public private partnership models among risk management communities and sectors, enabling a move towards a truly integrative way of thinking about risks and disasters.

The 5<sup>th</sup> Edition of the IDRC conferences, the IDRC Davos 2014 will be held from 24 - 28 August 2014 in Davos, Switzerland and will focus on "Integrative Risk Management - The role of science, technology & practice". The conference will yet again cover topics in disaster and risk management amongst others also in cyber security as a major emerging risk, but also about the role of Information and Communication technologies within Disaster and Risk Management. A major obstacle for the Disaster Risk Reduction Community is the management of knowledge and information and its provision. New database management structures to ease the access and the sharing of knowledge would benefit the international DRR community.



**24-28 August 2014**

**Davos • Switzerland**

### Call for Abstracts:

**The call for abstracts for papers for the 5<sup>th</sup> IDRC Davos 2014 is open until 15. April 2014 and contributions are welcome.** To submit abstracts, please follow:

<http://idrc.info/programme/call-for-abstracts>

### IDRC Davos Conference Topics:

- Disaster Preparedness, Response
- ICT in DRR
- Country Risk Management
- Environmental & Ecological Risks
- Thinking the Unthinkable
- Technical Risks
- Urban Risks /Megacities
- Societal / Political Risks
- Resilience & Vulnerability

- Health Impacts and Medical Response
- Economic Disasters
- Business Continuity
- Financial Tools for Risk Management
- Communication & Outreach in DRR
- Education, Research & Capacity Building

The outcomes of the IDRC Davos 2014 will be presented at the UN World Conference WCDRR in Sendai, Japan in March 2015 and aim to influence the post 2015 agenda such as the Post-2015 Framework for Disaster Risk Reduction (HFA2), the Sustainable Development Goals (SDGs) or the successor of the UNFCCC Kyoto Protocol.

## GRF One Health Summit

For many years One Health was limited to an interdisciplinary collaboration in human and veterinary medicine with substantial added value in disease control. Most recently One Health has evolved to a broad and holistic paradigm which includes an environmental dimension, and also addresses economic and social challenges.

In 2012 GRF Davos launched an annual conference, the GRF One Health Summit to promote and foster such an integrative approach in managing health risks at the interface of human-, animal- and environmental health with a strong link to food safety and security. The upcoming GRF One Health Summit 2014 aims to strengthen an international research and education strategy for One Health.

GRF Davos promotes knowledge and best practices based on the One Health approach in to the UN Sustainable Development Goals.



The GRF One Health Summits is an annual conference that promotes and fosters an integrative approach in managing health risks at the interface of human-, animal- and environmental health with a strong link to food safety and security and to agriculture. Striving for intensified collaboration among experts and practitioners from the different sectors and disciplines tangent to such a comprehensive health perspective, in particular the pharmaceutical and food industry as well as health insurers' engagement, will provide significant added value to identify cost-effective measures.

### The 3rd GRF One Health Summit 2014 will be held from 05 - 08 October 2014 at the Davos Congress Centre in Davos, Switzerland.

The Summit will further develop and strengthen the One Health paradigm and its global movement. In particular this 3rd global gathering will focus on the added value of a global One Health approach and a stronger involvement of the private sector and policy.



**The call for abstracts for papers for the 3rd GRF One Health Summit 2014 is open until 31 March 2014 and contributions are welcome.** To submit abstracts, please follow: <http://onehealth.grforum.org/programme/call-for-abstracts/?L=>

## Disaster Surgery Workshop

Disasters in recent years have revealed the crucial role of embedded medical teams providing disaster surgeries during the primary search and rescue operations, and the response phase as a whole. These operations are often additionally aggravated by extreme environmental conditions (cold, heat, high altitude, dust, heavy precipitation, etc.). Many of those people rescued after an earthquake or after an explosion as examples have life-threatening contrasting with a wider

move in recent years to improve humanitarian intervention standards. GRF Davos addresses this issue during its annual Disaster Surgery Workshop Davos

The workshop is jointly organised by GRF Davos, AO Trauma and the AO Foundation.

<http://www.grforum.org/risk-academy/disaster-surgery-workshop-2013/>

## Research Projects

We place a particular focus on applied research and offer experience in Integrative Risk Management in various areas. Profound capacity for dissemination and knowledge transfer activities is also given. We facilitate the formation of efficient international project teams, link scientific institutions with practice and provide the necessary project management tools and support.

We are currently involved in two European research projects which cover different aspects of Risk Management.

The aim of the project **Public Empowerment Policies for Crisis Management PEP** is to investigate how the crisis response abilities of the public can be enhanced and what public empowerment policies are successful in realising this aim.



Public Empowerment Policies enhance crisis management as a coproduction of response organizations and citizens. The project will identify best practices in the community approach to crisis resilience and give directions for future research and implementation, including the use of social media and mobile services, to further citizen response. The input of the experts in the field of crisis management and communication is a key element in pursuing the goals of this project.

PEP offers authorities and other non-governmental organisations a comprehensive information package about key enablers for public empowerment in the form of guides concen-

trating on best practices, community approach and human technology enhancing citizen response.

The Project DITAC (Disaster Training Curriculum) proposes to develop a holistic Training Curriculum for first responders and strategic crisis managers dealing with international crises. The DITAC Curriculum will address the key challenges for the management of disaster incidents. It will develop a standardised strong, comprehensive and efficient EU-wide approach to crises and disasters to feature the added value by EU coordinated actions in the field of crisis response. The Curriculum will also improve the preparedness and availability of trained personnel by providing a common language, common objectives and common tools leading to better results in the protection and assistance of people confronted with large-scale crises.



The focus lies on international crisis management, but the benefit of a standardised training programme in crisis and disaster response can also be used to increase Europe's resilience in facing disasters and crises within the European Union.

We additionally offer risk assessment and analysis for national, regional and local project; conduct research on regional climate change adaptation strategies and methodologies for the protection goal target settings in critical infrastructure protection.

## GRF Davos e-Journals

GRF Davos publishes two online journals.

GRF Davos' **Planet@Risk** contributes to bridging the gaps between science, practice, and different sectors of academia. It fosters a multidisciplinary approach and presents the results of interdisciplinary and transdisciplinary research with a special emphasis on their application to practical problems. Information from data and reports which has been difficult or impossible to access, and whose quality has perhaps been

hard to judge, can finally be put to use. Please submit your papers at: <http://www.planet-risk.org/>.



The **International Journal of Disaster Risk Reduction (IJDRR)** is peer-reviewed journal that is published in close cooperation Elsevier. IJDRR publishes fundamental and applied research, critical reviews, policy papers and case studies focusing on multidisciplinary research aiming to reduce the impact of natural and technological disasters. IJDRR stimulates exchange of ideas and knowledge transfer on disaster research, mitigation, adaptation, prevention and risk reduction at all geographical scales: local, national and international.



<http://www.journals.elsevier.com/international-journal-of-disaster-risk-reduction>

## Partnerships, Alliances and Initiatives

Meaningful partnerships are the foundation for success. GRF Davos takes the lead in partnering with international organizations and universities and in implementing innovative collaborations that enhance risk reduction and disaster management research and cooperation in combating climate change and desertification, land degradation and drought (DLDD).

If you would like to find out more about our UN Agreements, MoUs, and Alliances or GRF Davos in general please visit our website at: [www.grforum.org](http://www.grforum.org) or send an email to the GRF Davos secretariat: [info@grforum.org](mailto:info@grforum.org)





## 5<sup>th</sup> International Disaster and Risk Conference

Integrative Risk Management  
The role of science, technology & practice  
24-28 August 2014 • Davos • Switzerland

**Special call for papers & sessions  
Information & Communication  
Technologies (ICT)  
in Risk Management**



Special call topics include amongst others:  
mobile phone apps • risk communication  
modelling and support of mass evacuation  
supporting technologies for disabled  
information/database management  
crowd sourcing • cyber security  
disaster response technologies



**Submit your abstract  
by 15. April 2014  
[www.idrc.info](http://www.idrc.info)  
> call for abstracts**

Organised by:



# EAIS 2014: Emerging Aspects in Information Security

Special event of the international FedCSIS Multiconference is announced. ECN readers are invited to submit papers or participate in this event and the conference.

It would be difficult to point out a domain of social or economic life which is not dependent on the Information and Communication Technologies (ICT). ICT are broadly used to drive businesses, public, financial and health sectors, and industry. Individual citizens use ICT in their everyday lives.

ICT are used to produce, process, store and exchange a huge amount of information of crucial importance for the society and individuals. This information should be protected in the interests of its owners and consumers (stakeholders). Information security is identified with the protection of information integrity, availability and sometimes confidentiality.

ICT provide services, including transactions, for individuals, organizations and society. They should be available when needed and provided at the assumed quality level. ICT are a backbone of business, industry and society to secure the use of ICT. Other aspects are considered too, such as authenticity, reliability, accountability, nonrepudiation, privacy, anonymity, etc.

All these issues are encompassed within the security term. All factors breaching information assets or disturbing provided services should be identified and controlled. These activities are related to security management. The foundation of this management is risk management. Organizational and personal aspects play an important role in the security management.

Apart from organizational and procedural aspects, technical aspects are important. It is unquestionable that the applied technology should be modern and proven. This issue concerns hardware, software and composed systems. Communication aspects are important too – everything functions in a network today, with the omnipresent Internet. Reputable stakeholders as

well as individuals entrust their information assets to ICT systems or use different IT services. They all require assurance from these technologies. It means that in the critical situation the users can rely on their ICT and no negative impacts will be exercised by the users. Assurance methods assume rigorous development, manufacturing and maintenance processes of ICT.

For the organizations strongly dependent on ICT, information security and business continuity are connected with each other. The integrated business continuity and information security management systems ensure the following:

- monitoring factors which cause crisis situations in institutions, i.e. when the continuity of business processes is disturbed or information security is breached by threats which exploit certain vulnerabilities,
- ability to reduce negative impact of business continuity disturbances or information security breaches (consequences),
- ability to recover business processes to their original form after different types of incidents.

The security issue concerns individuals, social groups, societies, and governments. In each country there are complex technical infrastructures. Some of these infrastructures have crucial significance to societies, like: energy, fuel, gas, water, food, telecommunications services, financial services, etc. They are classified as critical infrastructures (CIs). In today's world information and communication technologies support all critical infrastructures. What is more, societies develop distinguished infrastructures of strategic importance considered the Critical Information Infrastructures (CII).



**Andrzej Białas**

Institute of Innovative Technologies  
EMAG, Katowice, Poland

Andrzej Białas: PhD, graduated from the Silesian University of Technology, Fac. of Automatic Control, Electronics and Computer Science in 1979. He has been in charge of numerous R&D projects and has carried out ICT trainings.

He is Associate Professor at the Institute of Innovative Technologies EMAG, leading R&D projects (national and EU FP6 CI<sup>2</sup>RCO, FP7 ValueSec) on information security management, design and evaluation of IT security, business continuity, risk management.

He is also Associate Professor at the University of Economics in Katowice, providing lectures on software testing & quality, network information security management, cryptography and its applications.

Dr. Białas is an author of a vast collection of articles and other publications. He is a member of the IFIP WG11.1 Information Security Management group.

He is a Co-Chair of EAIS'2014.

e-mail: [a.bialas@emag.pl](mailto:a.bialas@emag.pl)

The broader the use of ICT is the stronger is dependence on it. All ICT issues (threats, vulnerabilities) can be transferred to business, public or social lives. For this reason, security issues are a matter of the utmost importance.

Security has a multidisciplinary character. Apart from technological, organizational and procedural issues, it takes into consideration human aspects (social, psychological, cultural, etc.).

Security cannot be bought as a miracle box taken down from the shelf. It is a time-related process. We should plan it, implement, check and maintain – security needs permanent care, i.e. the right management.

Complex technical systems, including ICT, are related to both security and safety. These issues are bound with each other – security can influence safety and vice versa.

Information security has many relations with other security domains. Methods, tools and techniques from one domain are checked in others. Researchers try to find synergy in this respect. Together they try to solve big multidisciplinary issues. This job requires knowledge exchange and common understanding. Knowledge engineering in the security domain is getting more and more important.

## FedCSIS Multiconference

Security has emerged as an important scientific field of a multidisciplinary character. To review achievements, exchange experience and knowledge, and to set co-operation, a special event of the international FedCSIS Multiconference will be organized. It is called "Emerging Aspects in Information Security" (EAIS'2014).

FedCSIS – Federated Conference on Computer Science and Information Systems will be held in Warsaw, Poland, 7 – 10 September, 2014. This year's FedCSIS Multiconference features 28 different events: conferences, symposia, workshops, special sessions, each running over any span of time within the conference dates (from half-day to three days). The FedCSIS events bring together researchers, practitioners, and academia to present and discuss ideas, challenges and

potential solutions on established or emerging topics related to research and practice in computer science and information systems. The proceedings of the FedCSIS conference have been indexed in the Thomson Reuters Web of Science since 2012.

Detailed information about FedCSIS multiconference:

<https://fedcsis.org/>

## EAIS'2014 Event

EAIS'2014 is one of the events focused on different aspects of security.

The Emerging Aspects in Information Security (EAIS'2014) workshop deals with the diversity of the information security developments and deployments in order to highlight the most recent challenges and report the most recent researches. The objective of the workshop is to explore all information security technical aspects. Yet, it covers some emerging topics too, such as social and organizational security research directions. EAIS 2014 is to attract researchers and practitioners from academia and industry. It will provide an international discussion forum where experiences and ideas will be shared about emerging aspects in information security in different application domains. This way it will be possible to take up new research directions and respond to modern research challenges.

The objectives of the EAIS'2014 workshop can be summarized as follows:

- To review and conclude researches in information security and other security domains, focused on the protection of different kinds of assets and processes, and to identify approaches that may be useful in the application domains of information security.
- To find synergy between different approaches, allowing to elaborate integrated security solutions, e.g. integrate different risk-based management systems.
- To exchange security-related knowledge and experience between experts to improve existing methods and tools and adopt them to new application areas

- To present latest security challenges, especially with respect to EC Horizon 2020.

Topics of interest include but are not limited to:

- Biometric technologies
- Human factor in security
- Cryptography and cryptanalysis
- Critical infrastructure protection
- Hardware-oriented information security
- Social theories in information security
- Organization-related information security
- Pedagogical approaches for information security
- Individual identification and privacy protection
- Information security and business continuity management
- Decision support systems for information security
- Digital right management and data protection
- Cyber and physical security infrastructures
- Risk assessment and risk management in different application domains
- Tools supporting security management and development
- Emerging technologies and applications
- Digital forensics and crime science
- Misuse and intrusion detection
- Security knowledge management
- Data hide and watermarking
- Cloud and big data security
- Computer network security
- Security and safety
- Assurance methods
- Security statistics

Detailed information about EAIS'2014: <https://fedcsis.org/2014/eais>

I would like to encourage the ECN readers to submit papers to this event and to participate in the conference.

# CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security

Bringing together researchers and professionals from academia, industry and governmental organizations working in the field of the security of critical infrastructure systems. Announcing the **1<sup>st</sup> CIPRNet Young Critis Award CYCA**.

On behalf of the Steering Committee and the Local Organizing Committee we are excited to invite you to submit papers and attend the CRITIS 2014 conference. CRITIS 2014 will be held in October 2014 in Limassol, Cyprus and it continues a well-established tradition of successful annual conferences. It aims at bringing together researchers and professionals from academia, industry and governmental organizations working in the field of the security of critical infrastructure systems.

Modern society relies on the availability and smooth operation of a variety of complex engineering systems. These systems are termed Critical Infrastructure Systems (CIS). Some of the most prominent examples of critical infrastructure systems are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, and oil / natural gas pipelines.

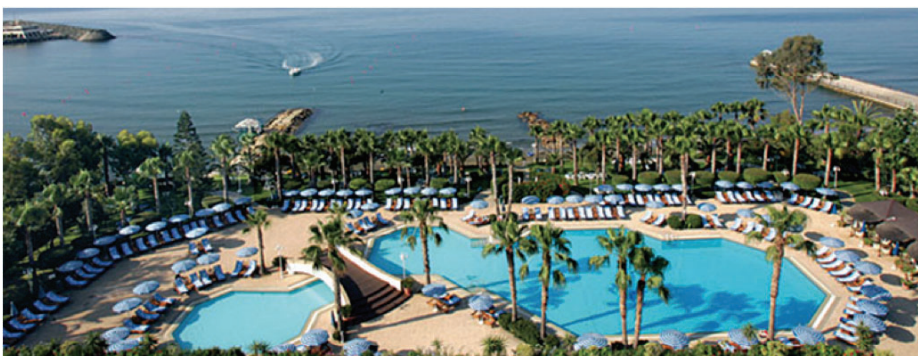
Our everyday life and well-being depend heavily on the reliable operation and efficient management of these critical infrastructures. The citizens expect that critical infrastructure systems will always be available

and that, at the same time, they will be managed efficiently (i.e., they will have a low cost). Experience has shown that this is most often true. Nevertheless, critical infrastructure systems fail occasionally. Their failure may be due to natural disasters (e.g., earthquakes and floods), accidental failures (e.g., equipment failures, software bugs, and human errors), or malicious attacks (either direct or remote). When critical infrastructures fail, the consequences are tremendous. These consequences may be classified into societal, health, and economic.

Conference web site:  
<http://www.critis2014.org>

Conference dates  
13-15 October 2014

The venue of the CRITIS 2014 conference will be the magnificent Grand Resort Hotel, in Limassol, Cyprus. The hotel is set in over 20,000 square meters of beautifully landscaped gardens with exotic trees and subtropical plants, which extend right down to the seashore.



**Elias Kyriakides**

is an Assistant Professor at the Dept of Electrical and Computer Engineering and the Associate Director for Research at the KIOS Research Center for Intelligent Systems and Networks, University of Cyprus



**Left: Marios Polycarpou,**  
[mpolycar@ucy.ac.cy](mailto:mpolycar@ucy.ac.cy)  
Director KIOS Research Center (RC)

**Right: Demetrios Eliades**  
@: [eliades.demetrios@ucy.ac.cy](mailto:eliades.demetrios@ucy.ac.cy)  
Research fellow at the KIOS (RC)

Both: University of Cyprus

## 1. Conference Topics

- Infrastructure resilience and survivability
- Security and protection of complex cyber-physical systems
- Self-healing, self-protection, and self-management architectures
- Cyber security in critical infrastructure systems
- Critical (information-based) infrastructures exercises and contingency plans
- Advanced forensic methodologies for critical information infrastructures
- Economics, investments and incentives of critical infrastructure protection
- Infrastructure dependencies: modeling, simulation, analysis and validation
- Critical infrastructure network and organizational vulnerability analysis

### Important dates

Deadline for invited session proposals: March 26, 2014

Deadline for submission of papers: April 2, 2014

Notification to authors: June 1, 2014

Camera-ready papers: June 25, 2014

- Critical infrastructure threat and attack modeling
- Public-private partnership for critical infrastructure resilience
- Critical infrastructure protection polices at national and cross-border levels
- Fault diagnosis for critical infrastructures
- Fault tolerant control for critical infrastructures
- Security and protection of smart buildings
- Detection and management of incidents/attacks on critical infrastructures
- Preparedness, prevention, mitigation and planning

## 2. Call for Special Sessions

Proposals for organizing special sessions during CRITIS 2014 are cordially invited. Special sessions will comprise 4-6 papers presenting a unifying theme of interest to the conference attendees from a diversity of viewpoints. Special Session

proposals from active research projects are particularly welcomed. Proposals for special sessions must include the title of the session, a paragraph describing the theme of the session, names and affiliation of the contributing authors, and tentative titles of the contributions.



The component papers must be submitted separately, by the respective authors, as per the regular submission procedure. Each paper in a proposed invited session will be individually reviewed.

Any rejected papers submitted as part of an invited session will be removed and appropriate contributed papers may be substituted, at the discretion of the Program Committee. Likewise, selected papers from rejected invited sessions may be placed into other sessions. Further exchanges may be made to ensure coherence of the sessions, at the discretion of the Program Committee.



**CIPRNet Young Critis Award 2014: Are you the Winner?**

## Organisers and Contact Information

### General Co-Chairs:

- Marios Polycarpou, University of Cyprus
- Elias Kyriakides University of Cyprus

### Program Chair

- Christos Panayiotou, University of Cyprus

### Program Co-Chairs

- Vicenç Puig, Universitat Politècnica de Catalunya
- Erich Rome, Fraunhofer Institute for Intelligent Analysis and Information Systems

### Publications Chair

- Georgios Ellinas, University of Cyprus

### Publicity Co-Chairs

- Demetrios Eliades, University of Cyprus
- Cristina Alcaraz, University of Malaga

### For more information

Elias Kyriakides, [elias@ucy.ac.cy](mailto:elias@ucy.ac.cy)

### Conference Webpage:

[www.critis2014.org](http://www.critis2014.org)

## 3. CIPRNet Young CRITIS Award (CYCA)

**An award for outstanding research in Critical Infrastructure Security (CRITIS) and protection sponsored by EU FP7 NoE CIPRNet will honour winners at CRITIS 2014.**

## Who should apply?

Every young engineer / scientist interested in CRITIS and in CRITIS community and is less than 32 year old by May 1<sup>st</sup>, 2014 is invited to apply. We explicitly invite junior experts and researchers from universities, research organisations and industry to apply.

In general, a mature piece of work is expected such as a PhD thesis in final or near final status, as well as outstanding works from young industry or research organisations researchers.

## 3.1 General information

Junior experts less than 32 years old may apply for the CIPRNet Young CRITIS Award CYCA. Three CYCA applicants per year will be selected for presenting their work at CRITIS conference (in 2014 in Cyprus) in the CYCA award session.

The ranking of up to three winners (depending on the number of applications and the paper quality) will be done at the conference itself, and the awards will be presented to the winners at a closing ceremony.

Limited travel funding opportunities are possible under conditions (please contact the organiser for details and conditions).

CIPRNet Young CRITIS Award 2014

There is never a better point in time to apply than right now!

## 3.2 Evaluation process

- The CYCA papers will be rated by at least three experts from the CYCA award committee according to the same evaluation criteria as the papers proposed in the conference.
- Up to five highest rated papers will be reviewed by the experts.

They will select who will qualify for the CYCA award slot, but limited to three papers maximum.

**Note:** If you get a positive evaluation, but you are not selected for CYCA award, your paper will be presented at the conference in the regular slots as all other papers. Therefore, you can only win by applying for CYCA.

- The total available award money is around 2000 Euro.

The ranking of the first three papers will be done at the conference, as follows:

- a) All in the audience vote on the ranking of the presentations → 40% weight
- b) CYCA award committee (written paper) rating → 40% weight
- c) CYCA award committee (oral presentation and interactivity) rating: → 20%
- d) The CYCA award committee will have a meeting after the session, where the final ranking will be made.

## 3.3 Evaluation Committee

The Evaluation Committee consists of the Award Committee and Experts from the CRITIS Steering Committee according to the needs and the number of submitted papers

## 3.4 How to apply?

CYCA papers are normally submitted as other papers through the EasyChair conference system of CRITIS.

Additionally, a CIPRNet Young CRITIS Award questionnaire should be submitted (available from April 15, 2004 on the website). This questionnaire has the following purpose:

- Contact details
- Info on birth data of all the authors
- To provide a statement of honesty: You declare that all citations are declared correctly (anti plagiarism)

The questionnaire and the CV must be sent to the moderator of CYCA: Prof. Dr. Bernhard M. Hämmerli

Please send as soon as possible, but no later than June 15, 2014

e-mail: [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)  
usually your delivery is preferred with cc to: [Bernhard.Haemmerli@HSLU.ch](mailto:Bernhard.Haemmerli@HSLU.ch)

post mail: Bodenhofstrasse 29, CH-6005 Lucerne, Switzerland

If you do not get a confirmation of receipt, please try to resend or call on +41 79 541 7787 in order to exclude transfer problems.

## 3.5 Award Committee

### CIPRNet Young CRITIS Award

#### Moderation

- Bernhard Hämmerli University of Applied Sciences Lucerne School of Engineering and Architecture
- Javier Lopez, University of Malaga

#### Committee

- Jose Marti, University of British Columbia
- Mohamed Eid, French Commissariat of Atomic Energy & Alternative Energies
- Elias Kyriakides University of Cyprus
- Roberto Setola, University Campus Bio-Medico of Rome

#### See also:

[cyca.critis2014.org](http://cyca.critis2014.org)

## Links

ECN home page <http://www.ciprnet.eu>  
ECN registration page free registration on [www.ciip-newsletter.org](http://www.ciip-newsletter.org)

### **CIPRNet Young CRITIS Award: Unique opportunity to jump into a CRITIS Career!**

Award for talents below 32 years [cyca.critis2014.org](http://cyca.critis2014.org)

### **Forthcoming conferences and workshops**

Master Class ModSim & Analysis [www.ciprnet.eu/training.html](http://www.ciprnet.eu/training.html) : A CIPRNet community support effort  
ESReDA <http://www.esreda.org/Events/tabid/1489/Default.aspx> 29-30.05.14 Torino, Italy  
IDRC 2014 <http://idrc.info/programme/call-for-abstracts> 24-28.08.14 Davos, Switzerland  
Call for abstracts open till 15.4.2014  
EAIS 2014 <https://fedcsis.org/2014/eais> 7-10.09. 14 Warsaw, Poland,  
Call for papers open till 11.4.2014  
CRITIS 2014 [www.critis2014.org](http://www.critis2014.org) 13-15.10.14 Limassol Cyprus  
Call for papers open till 26.4.2014  
CIPRNet Young Critis Award see [www.critis2014.org](http://www.critis2014.org)  
open till 26.4. 2014

### **Exhibitions**

Interschutz 2015 <http://www.interschutz.de/86385> 8.-13.6.2015 Hannover, Germany

### **Associations**

European Safety, Reliability &  
Data Association [www.esreda.org](http://www.esreda.org)  
Global Risk Forum Davos [www.grforum.org](http://www.grforum.org)  
FedCSIS – Federated  
Conference on Computer... <https://fedcsis.org>

### **Project home pages**

FP7 CIPRNet [www.ciprnet.eu](http://www.ciprnet.eu)  
FP7 ValueSec [www.valuesec.eu](http://www.valuesec.eu)  
FP 7 PoSecCo <http://www.posecco.eu/?id=354>  
ERNICIP <http://ipsc.jrc.ec.europa.eu/index.php/ERNICIP/688/0/>

### **Interesting Downloads**

Critis' 12 Conf. Proceedings: [www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8](http://www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8)  
Critis' 13 Conf. Proceedings: <http://link.springer.com/book/10.1007/978-3-319-03964-0>

European Network and Information Security Agency [www.ENISA.eu](http://www.ENISA.eu) publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection"  
ENISA [www.enisa.europa.eu/activities/Resilience-and-CIIP](http://www.enisa.europa.eu/activities/Resilience-and-CIIP)

Dutch Intersectional Study (in Dutch): <http://www.wodc.nl/onderzoeksdatabase/vertaling-afhankelijkheden-van-zweedse-methode-naar-nederlandse-situatie.aspx?cp=44&cs=6796#publicatiegegevens>

### **Websites of Contributors**

Austrian Security Policy Centre [www.bmi.gv.at](http://www.bmi.gv.at)

# **CIPRNet Young Critis Award 14: Are you the Winner?**

Less than 32 years by May 1, 2014?

Attractive prizes,  
A lot fun to join!

Please see details on:

[cyca.critis2014.org](http://cyca.critis2014.org)



All participants get qualified coaching by European leading experts on C(I)IP

Don't miss this chance!



# CRITIS 2014

9<sup>th</sup> International Conference on  
Critical Information Infrastructures Security  
October 13-15, 2014, Limassol, Cyprus  
[www.critis2014.org](http://www.critis2014.org)



# European CIIP Newsletter

July 14 – October 14, Volume 8, Number 2

# ECN

## Contents:

Editorial

EU Projects  
INTACT and PREDICT

EU SLO Project

EU Exercises and CIP  
Scenarios

Data Management and  
Information Sharing in  
CIPRNet DSS

Cyber Storm

New Books Netonets

CIPRNet Master Class EU

CRITIS 2014



**> About ECN**

ECN is coordinated with  
The European Commission, was initiated by Dr. Andrea Servida,  
today funded by the European Commission  
FP 7 CIP Research Net CIPRNet Project  
under contract, Ares(2013) 237254

**>For ECN registration ECN registration & de-registration:**  
[www.ciip-newsletter.org](http://www.ciip-newsletter.org)

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

**>Questions to the editors about articles 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:**  
[www.ciprnet.eu](http://www.ciprnet.eu)

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

**>Founders and Editors**

Eyal Adar, Founder and CEO, WCK [www.wck-grc.com](http://www.wck-grc.com)  
Christina Alcaraz, University of Malaga, [alcaraz@lcc.uma.es](mailto:alcaraz@lcc.uma.es)  
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)  
Erich Rome, Fraunhofer, [erich.rome@iais.fraunhofer.de](mailto:erich.rome@iais.fraunhofer.de)

**>Country specific Editors**

For France: Michel Riguidel, ENST, [riguidel@enst.fr](mailto:riguidel@enst.fr)  
For Spain: Javier Lopez, UMA, [jlm@lcc.uma.es](mailto:jlm@lcc.uma.es)  
For Finland: Hannu Kari, HUT, [kari@tcs.hut.fi](mailto:kari@tcs.hut.fi)  
to be added, please report your interest

**> Spelling:**

British English is used except for US contributions

## Editorial

Intro	Community Building: Why is it that important, and what do we get? by Gregorio D'Agostino and Bernhard Hämmerli	5
-------	--	---

## European Activities

INTACT EU Project	EU project on the Impact of Extreme Weather on Critical Infrastructures by Rene Willems	7
PREDICT EU Project	PREparing for the Domino effect In Crisis siTuations by Dominique Sérafin	9

## Country Specific Issues

no		No Page
----	--	------------

## Method and Models

EU SLO Project	The Security Liaison Officer as a part of the European Critical Infrastructure Protection Strategy by Maria Carla De Maggio	11
EU Exercises and CIP Scenarios	CIP Scenarios: Lessons learnt from EU Exercises by Marianthi Theocharidou	15
Information Sha- ring and Data Management	Data management and Information sharing in CIPRNet DSS by Alberto Tofani, Antonio De Nicola, Antonio Di Pietro, Maurizio Pollino and Luigi La Porta	19

## About Associations

Cyber Storm	Cyber Storm Association by Bernhard Tellenbach	23
-------------	---	----

## Books on C(I)IP

Netonets	Netonets: Critical Infrastructures as Network of Networks by Gregorio D'Agostino	25
----------	---	----

## Conferences 2014

CIP Master Class	Experiences from the CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (CI) by Elena Polykarpou	29
CRITIS 2014	CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security by Elias Kyriakides	33

## Links

Where to find:	<ul style="list-style-type: none"><li>• Forthcoming conferences and workshops</li><li>• Recent conferences and workshops</li><li>• Exhibitions</li><li>• Project home pages</li><li>• Selected Download Material</li></ul>	35
----------------	--	----

# Editorial: Community Building: Why is it that important, and what do we get?

In CIP we need local communities, national, European and worldwide communities. Also it is important that all these communities remain in exchange. And what is the role of journals and books?

The world of research is changing very rapidly from huge governmental after war projects like Manhattan (nuclear bomb) and Apollo (Space, reaching moon) project and peaceful use of nuclear energy to dynamically allocated specific aim projects with dynamically changing teams and, of course, still military projects. In line with this tendency, European countries established high level scientific institution supported with large financial budgets.

Meanwhile we saw a huge increase in the publications far beyond the genuine need for sharing results within the scientific community. This is basically due to the criteria applied for fund allocation and for personal scientific careers that are mostly targeted on literature production and participation to official events.

As a new field of applied research, Critical Infrastructure Protection (CIP) had no community, no allocated budget, no funding schema and no publication channel dedicated to this terrific strategic subject. Initial important work like the paper by Rinaldi et al. – "Identifying, understanding, and analysing critical infrastructure interdependencies, Control Systems, IEEE, 2001" – appeared in a journal on "Control Systems" because dedicated CIP journals were lacking.

After five years of an ad hoc expert group promoting CIP, the European Commission released a Communication of December 12, 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007] and two years thereafter the EU started to rule the field on legal level by the Directive of Dec 2008.

CIP Newsletter were made available in the US (CIP Report) and in the EU (European CI(I)IP Newsletter from 2002 respectively 2006 and more followed.

National efforts in CIP (conferences and exercises) started late 90ies and have been growing with emerging awareness.

The scarcity of literature has been recognized and we are happy to observe today more than a dozen available books and even more will be edited in the next period. CIP Journals from Elsevier and Inderscience are available, and IEEE provides a journal on dependability. Still, CIP issues are being discussed in journals dedicated to other more classical topics, but this is about to change.

The dissemination framework of CIP is complemented by international conferences such as CRITIS, the International Conference on Critical Infrastructure (CRIS), and recently CIPRE.

Although CIP is of public interest, some achievements have to be kept secret because of national defense, Transparency, otherwise typical in science, is not always first priority in the field of CIP. NISAC in the US represents a compromise between the need for secrets and synergic capability of open scientific communities. The concept of EISAC might be good for Europe as well.

And finally, we are happy that the CIP community, besides researchers, includes also stakeholders like policy makers, suppliers and operators. Their trustful collaboration is a prerequisite for leveraging the R&D investments made in CIP.

We are very happy to announce CRITIS'14 with over seventy submissions on the next page, and offering a coming together of the CIP community.

[www.critis2014.org](http://www.critis2014.org)

Enjoy reading this issue of the ECN!

*PS: Authors willing to contribute to future ECN issues are very welcome, just drop an email.*



**Gregorio D'Agostino**

Gregorio is a theoretical physicist that received his "laurea" and PhD in Physics at University of Rome "La Sapienza".

email: [gregorio.dagostino@enea.it](mailto:gregorio.dagostino@enea.it)  
Phone +39 06 30484776  
web: [gordion.casaccia.enea.it](http://gordion.casaccia.enea.it)



**Bernhard M. Hämmerli**

is Professor at Lucerne University of Applied Sciences and Gjøvik University, CEO of Acris GmbH

e-mail: [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)  
He is ECN Editor in Chief

# **Call for Participation**

## **CRITIS 2014**

9<sup>th</sup> International Conference on  
Critical Information Infrastructures Security  
October 13-15, 2014, Limassol, Cyprus

[www.critis2014.org](http://www.critis2014.org)

(see last article  
and last page)

# The Security Liaison Officer as a part of the European Critical Infrastructure Protection Strategy

The Directive 114/2008/EC is the starting point for a European strategy for the Critical Infrastructure Protection. The SLO project aims to overcome the regulatory gap related to the profile of the Security Liaison Officer.

The conference on "Security Liaison Officer as a part of Critical Infrastructure Protection strategy", held the 25th June at the Italian Chamber of Deputies in Rome, has been the final act of the European project "SLO - Security Liaison Officer". The project, co-funded by the "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme" (CIPS) of the DG Home Affairs of the European Commission, is ending after a 14-month activity. The project has been developed with the cooperation of two main partners, Complex Systems and Security Lab of University Campus Bio-Medico of Rome (Coordinator), supervised by Prof. Roberto Setola, and the Romanian Association for Critical Infrastructures and Services Protection (ARPIC), with the support of the Italian Association of Critical Infrastructure Experts (AIC), BC Manager, ASIS International Chapter Italy, and Transelectrica, as associate partners.

The Security Liaison Officer figure is mentioned in the Article 6 of the Council Directive 2008/114/EC as the contact point between the Critical Infrastructure operators and the public authorities in charge for Critical Infrastructure protection. As stated in the Directive "Security Liaison Officers (SLO) should be identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated ECIs already possess a Security Liaison Officer or equivalent. Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in

place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers". The Directive overlooks many aspects which should characterize the figure of the SLO, namely his background, his tasks and responsibilities, his position inside the company, his role in a critical situation (before, during, or after a crisis), and his relationships with the other European Security Liaison Officers.

The project, aiming to define a common framework regarding the Security Liaison Officer duties, collected the points of view of several countries, in order to achieve a possible standardization of the SLO profile. This research has been carried out through the data acquisition by means of three different sources: review of the most popular standards and regulations on the subject, acquisition of specific information about actual facts and aspects via online questionnaires and interviews, elicitation of ideas via brainstorming activities during workshop cafés.

The data collection from open-sources and most popular standards has revealed the diversity of ideas regarding the Security Liaison Officer figure. While a new Romanian resolution is very clear regarding the role and the background (military) of the SLO, other European Countries have a different implementation of the security-related roles in their organizations, whether recognized as critical or not, sometimes having a clear implementation of a profile similar or corresponding to the SLO.

To find out the opinions of people involved in the security issues, four different online questionnaires have been devised, depending on the role of the responder (Public Authority, Chief Security Officer, Staff Security Officer, Academia).



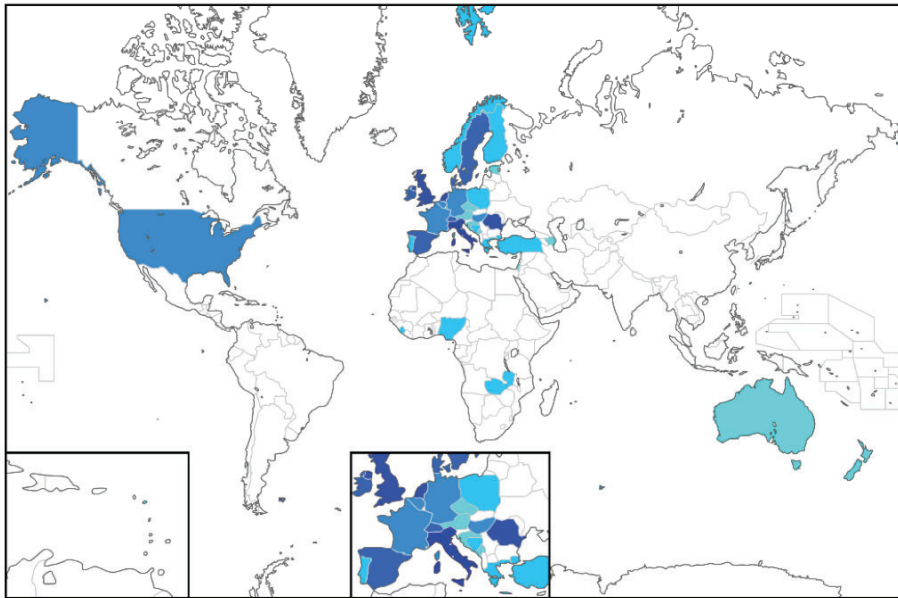
**Maria Carla De Maggio**

She belongs to the Complex Systems and Security Laboratory of the University Campus Bio-Medico of Rome since 2009, after a working period as junior consultant for a company involved in several European Projects in the ICT, e-inclusion and ethics areas. She currently manages several National and European projects of which the group is coordinator or partner, in both scientific and administrative aspects.

Eng. De Maggio holds a Master Degree in Biomedical Engineering (2007) and a Post Graduate Master in Homeland Security (2011), both from the University Campus Bio-Medico of Rome. She is now studying for a Degree in Economics.

email: [m.demaggio@unicampus.it](mailto:m.demaggio@unicampus.it)



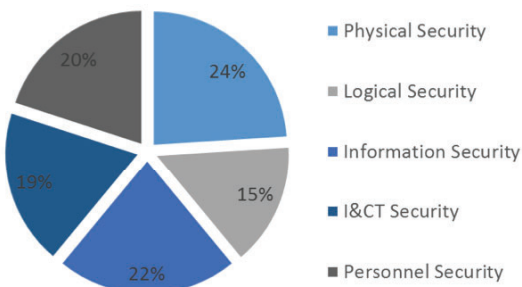


**Participation to the SLO survey.**

In the period from October 2013 to May 2014, more than 200 questionnaires have been collected, from 34 different countries (19 Member States and 15 non-Member States).

The main objective of the SLO survey is to perform a snapshot of the current organizations' security context and to identify the most relevant trends.

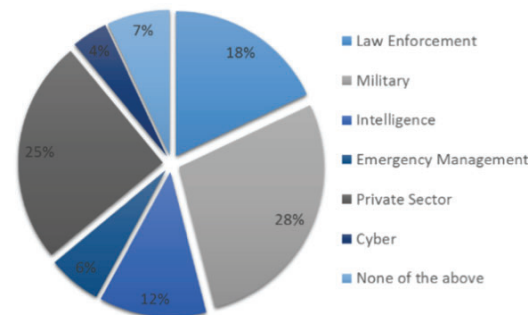
From the collected data, it appears that the security budget for the next five years will be aligned with those experienced in the past. Given the current budgetary constraints within the EU and abroad, this continuing upward trend of funding is further evidence of the sizeable attention that security is garnering. This increase in attention towards security is further emphasized by the data showing an incremental growth in the number of persons involved within the security division.



**CSO budget allocation.**

Considering the different dimensions of security, the most important aspect results to be personnel security: nearly a quarter of respondents considered personnel security as the most essential domain, stressing the utmost importance attributed to the person-

nel inside a company (a large relevance is also attributed to safety).



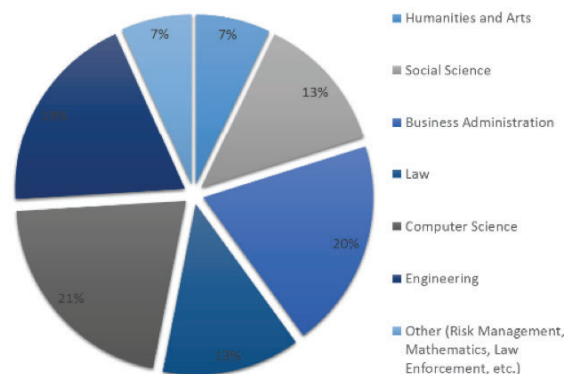
**Background of CSOs.**

However, the collected data shows that in the last five years there was a considerable boost in the security standards for the physical and cyber security domains, while personnel security standards received much less attention.

The result is a balanced approach towards security, further confirmed by the CSO category answers regarding resource allocation, as showed in the figure.

Another interesting aspect analysed is the background of the personnel involved in security. Indeed, even if 46% of the CSOs have a

background in the law enforcement or military fields, the actual composition of a security team is more articulated with a prevalence of competence in Computer Science, Business Administration and Engineering. This stresses the



**Background of Security staff.**

importance to complement the education with managerial and process-based competencies.

The SLO project survey shows an increased attention through all aspects of the security in the Critical Infrastructure organizations

Going more in-depth on the aspects directly related to the Council Directive 114/08/EC, there is only moderate familiarity with it (less than 50% of CSOs have knowledge of the EPCIP programme). Even more resounding is our analysis regarding the CIWIN network, which was evaluated as "unknown", "not relevant" or simply unused by the majority of responders. This limited knowledge regarding the EPCIP programme represents a partial contradiction with respect to the conclusions of the European Commission Working Document SWD(2013)318. This discrepancy can be partially explained taking into account that our questionnaires were mainly oriented toward private sector, while the primary customers for the European Commission are the governments (in fact the PAs involved in the questionnaire have a discrete knowledge of the programme).

The SLO questionnaire results have been completed and deepened by several interviews with Critical Infrastructures Security Managers and Public Authorities, which common request is for a regulatory standardization of the Security Liaison Officer professional profile, in order to establish common and cogent guidelines in case of critical situations which can involve European Critical Infrastructures.

A further important mean for elicit

information and opinions from security experts has been the organization of three Workshop Cafés in three different European Countries (Bucharest, Romania – October 2013, Rome, Italy – February 2014, The Hague, The Netherlands – May 2014) in order to collect opinions reflecting Member States' different regulations and cultural business schemes.

The workshop cafés (WSCs) focused on three separate elements of the SLO profile: Skills, Role and Tasks. These elements were analyzed during brainstorming activities and resulted in numerous innovative ideas and future elements for consideration. These results have been achieved thanks to the participation in the WSCs from about 100 Security experts from Academia, Public Authorities and Critical Infrastructure Companies from different countries.

According to most of the WSC attendees, the SLO must have the function of connecting not only structures, but also tasks and persons, playing a fundamental role to integrate the company activities and coordinate the personnel.

He/she must be able to communicate to all directions within the company and to connect all the divisions/departments of the company. Additionally, they must also be in contact with the other Security Liaison Officers, authorities and law enforcement officers. His/her main role must be, therefore, a link between the organization and both the National and European Public Authorities and other Critical Infrastructures.

To carry out these tasks, the SLO must be a person with good communication skills, able to motivate people, and in particular have a strong commitment from the top management. In this perspective,

being primarily a coordinator/facilitator able to effectively communicate inside and outside the organization, the SLO needs to be at a top management level into the company, referring preferably to the company board of directors. The SLO should have experience in management, though not necessarily former experience in the law-enforcement or military field. However, the SLO should have a wide competence on his own organization and his sector, along with knowledge regarding other sectors, technologies and legislations in security matters, and a mandatory continuing training process should be aligned with context changes. He/she must have a security clearance and it is preferable if he/she also had some professional certificate or adequate academic degree. During the WSCs, also novel vulnerabilities stemming from the implementation of dramatically differing policies, particularly difficult for companies operating in many Member States, were analyzed.



The results of the data acquisition has been integrated during the gap analysis phase, where all the information has been merged in order to define common features for the SLO and for his relationships with

the Public Authorities and the other European SLOs.

The first evidence coming from the SLO project data is that the SLO figure is considered, from both CI operators and PA, an effective element to manage the complex relationships existing between CI and PA, where the SLO could allow them to use a common vocabulary, simplify the procedures and construct more effective strategies and solutions.

This is also due to the change of paradigm of the security, that now deals with service continuity, company reputation, management of crisis situations, etc. This imposes to have a multi-disciplinary security team whose numerical dimension has also continued to increase in the last years. Consequently our data illustrates the existence of a strong motivation to establish a standard profile of the SLO figure, and to introduce a more cogent and specific regulation on the subject to allow the cooperation of Security Liaison Officers.

The SLO should have visibility on all security aspects and a very good knowledge of the organization.

From the amount of data collected during the project, it emerged that the term "OFFICER" is quite inappropriate. Several experts expressed some concerns about the term because it could apply a "military-oriented" connotation that might induce a wrong bias with respect to his/her essential role. Indeed the SLO is primarily a "LIAISON", to serve as an interface between the CI organization the PA or other operators. To effectively perform his/her work, the SLO should be familiar with all the threats that are impacting the organization. Hence it is a largely shared opinion to appoint a person already within the company having, then, a deep knowledge of the corporate processes and activities.

However, a mandatory continuing training process should be aligned with contextual changes and an adequate academic background is more and more required.

The majority of data identified a good collocation of the SLO in the Security Department or as member of the Board of Directors.

There is an important debate



regarding the opportunity for the existing CSOs to also serve as the SLO. This is because there are overlapping knowledge/skillsets between these two professional profiles. However, our data stressed that it should be preferable to have two separate professional figures.

To operate effectively, also the Public Authorities should introduce figure similar to the SLO in order to facilitate the information exchange.

A final consideration is on the word "SECURITY" in the SLO label. From the project, the need emerges to mandatorily consider All-Hazard approaches to guarantee the

capability of the different infrastructures to supply their essential services to the citizens. With this vision in mind, it appears more suitable to use the meaning of the Italian term "SICUREZZA", which embraces a holistic vision of both the accidental and malicious threats, hence Safety & Security.

It is highly desirable for the SLO figure to have a unified framework facilitating the definition of his/her role inside a company, for that which concerns his/her relationships with PA and other CIs, and to facilitate information sharing. In this way, the PA can participate in the process of

designating a SLO inside CIs releasing guidelines and criteria for eligibility.

A synthesis of the collected data and results can be found in the Final Report of the SLO project, released during the Final Conference of the project that can be now downloaded at [www.coseritylab.it](http://www.coseritylab.it). More information and results about the project can be requested to the project coordinator mailing to [contacts@coseritylab.it](mailto:contacts@coseritylab.it).



On 1st of May 2014, a new EU project started on the Impact of Extreme Weather on Critical Infrastructures

## Critical Infrastructures and Extreme Weather

Resilience of Critical Infrastructure (CI) to Extreme Weather Events (EWE) is one of the most demanding challenges for both government and society. Extreme Weather (EW) is a key phenomenon that can cause severe threats to the well-functioning of CI. The effects of various levels of EW on CI will vary throughout Europe. These effects are witnessed through changes in seasonal means and extreme value frequencies of regional extreme temperatures (high and low), humidity (high and low), extreme or prolonged precipitation (rain, fog, snow, ice, etc.) or prolonged lack thereof (drought), extreme wind or lack of wind, and thunderstorms. The increased frequency and intensity of EW can cause events such as flooding, drought, ice formation, wild fires etc. which present a range of complex challenges to the operational resilience of CI.

**The Challenge: Planning for Extreme Weather (EW) and economic life time 50+ years!**

The economic and societal relevance of the dependability and resilience of CI is obvious: infrastructure malfunctioning and outages can have far reaching consequences and impacts. The cost of developing and maintaining CI is capital intensive if they are expected to have a realistic functional and economic life (i.e. 50+ years). Hence, future EW has to be taken into account when considering protective measures, mitigation measures and adaptation measures to reflect actual and predicted instances of CI failures.

## The INTACT project

The INTACT project will address these challenges and bring together innovative and cutting edge

knowledge and experience in Europe in order to develop and demonstrate best practices in engineering, materials, construction, planning and designing protective measures as well as crisis response and recovery capabilities. All this will culminate in the INTACT Reference Guide, the decision support system that facilitates cross-disciplinary and cross-border data sharing and provides for a forum for evidence based policy formulation.

The objectives of the INTACT project are to:

- assess regionally differentiated risk throughout Europe associated with extreme weather;
- to identify and classify on a Europe wide basis CI and to assess the resilience of such CI to the impact of EWE;
- raise awareness of decision-makers and CI operators about the challenges (current and future) EW conditions may pose to their CI; and,
- identify potential measures and technologies to consider and implement, be it for planning, designing and protecting CI or for effectively preparing for crisis response and recovery.

Findings of the project will be accumulated in the INTACT Reference Guide. This guide will support decision makers and CI operators with best practices and methodological approaches to protect their CI against EWE

The INTACT project has been launched on May 01, 2014 and will deliver its final results in 2017. TNO is coordinator of the project consortium with eleven partners from eight countries: CMCC (IT), DELTARES (NL), FAC (IRE), DRAGADOS (SP), HR Wallingford (UK), PANTEIA (NL), NGI (NO), CSIC (SP), UN University (GE), Un Ulster (UK), VTT (FI)

INTACT receives funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° FP7-SEC-2013-606799.



### Rene Willems

Rene Willems holds a Master of Science form Eindhoven. He is Senior Policy Advisor Business and Network Development at Defence and Security of TNO in the Hague, The Netherlands.

Amongst others he was head of the division Operations Research and Business Management at TNO-FEL. He chaired the NATO RTO SAS Panel on Systems Analysis and Simulation.

He set up and acted as deputy director of the Hague Centre for Strategic Studies (HCSS), a TNO subsidiary.

He co-created and developed the Hague Security Delta (HSD), the Netherlands' national security cluster.

e-mail: [rene.willems@tno.nl](mailto:rene.willems@tno.nl)  
Phone +31 888 66 3224

This page I intentionally left blank.

# PREDICT: PREparing for the Domino effect In Crisis situations

The goal of the FP7 PREDICT project is to provide a solution for dealing with cascading effects in multi-sectorial crisis situations.

The PREDICT project is a new research project of the FP7 security call topic SEC-2013.4.1-2: Better understanding of the cascading effect in crisis situations in order to improve future response and preparedness and contribute to lower damages and unfortunate consequences. The PREDICT project has started on April 1<sup>st</sup> 2014.

## Abstract

PREDICT will provide a comprehensive solution for dealing with cascading effects in multi-sectorial crisis situations covering aspects of critical infrastructures. The PREDICT solution will be composed of the following three pillars: methodologies, models and software tools. Their integrated use will increase the awareness and understanding of cascading effects by crisis response organizations, enhances their preparedness and improves their response capability to respond in case of cascading failures.

PREDICT project will start from a deep analysis of recent cases (over 8500 incidents worldwide), which will be accompanied with scenarios of potential crisis. Project partners will set up a generic approach (common framework) to prevent or mitigate cascading effects which will be applied in selected cases agreed with end-users.

As modelling each phenomenon separately in a specific environment is not effective, PREDICT project will propose cohesive and comprehensive models of dependencies, cascading effects and common mode failure which will include causal relations, multi-sectorial infrastructure elements and environment parameters, as well as the human factor aspects.

PREDICT will deliver software tools bundled in PREDICT Incident Evolution Tool, which will consist of two core components: a Foresight and

Prediction Tool (for simulation of the evolution of cascading effect and impact on multi-sectorial dependencies) and a Decision-Support Tool (for determining the best course of action and to calculate the risk associated with them).

The high quality of the developed solutions will be assured by a consortium consisting of a number of experienced partners joining research, industrial (incl. SME), and end-users approaches. End-users will be deeply involved in PREDICT at three levels: as partners of the consortium (there are three end-users in the consortium), members of the Advisory Board, and representatives from relevant organisations across Europe invited to regular workshops.

## Objectives

The PREDICT project aims at delivering a comprehensive solution (PREDICT solution) for dealing with cascading effects in multi-sectorial crisis situations covering aspects of critical infrastructures.

The PREDICT solution is composed of the following three pillars: methodologies, models and software tools, which – when used together – will increase the awareness and understanding of cascading effects in crisis situations. It will enhance the preparedness for such effects and improve the capability to respond of various levels (local, regional, national, international) decision makers in case of a crisis.



**Dominique Sérafin**

Dominique Sérafin (PREDICT project coordinator) is a business developer at CEA in the field of critical infrastructure protection. He is also an expert in the field of electromagnetic effects and their consequences.

e-mail: [dominique.serafin@cea.fr](mailto:dominique.serafin@cea.fr)

CEA,DAM,GRAMAT,F-46500  
Gramat, France

The new methods and tools developed within the PREDICT project may reduce the negative impact of possible, future cascading effects and the improve planning of civil protection and crisis management operations. The PREDICT results will help lowering losses and damages in various fields, including economic or social safety and security. In order to bring this new quality into the cascading effects and crisis management domain, the proposed project will achieve the following detailed operational and technical objectives:

1- Gather and analyse available domain knowledge (e.g. historical data, crisis situation scenarios, policies, and procedures, expert knowledge) in order to create a solid, empirically proven background for the project and explore newly discovered information on cascading effects. Carrying out extensive and detailed analyses will enable investigating currently known and identifying new triggers (originating incidents, purpose acts or natural disasters) of cascading effects in crisis situations. Moreover, taking into consideration dependencies among various interconnected critical infrastructure sector elements and other not considered to be critical under existing policies, together with such triggers will help to determine probable cascade paths. Cascade paths (possible, different chain of events triggered by a single incident or act) will be used to study the influence of the crisis incidents, cascading through specific components of the dependent system (different sectors, products, services etc.). The gathered knowledge will also help identifying and measuring the strongest relationships, assessing threats, risks and magnitude of possible impact associated with the cascading effects and taking into account cross-border effect.

2- Develop a common framework that will be an organised set of definitions, methodologies, scenarios, typologies, best practices etc., building a common base for each specific PREDICT solution end-user, but also for cooperation of various actors. The common framework for understanding cascading effect will gather and structure all of the factors affecting cascading effect and results of the carried analysis. This framework will be also used to define a set of quantitative and qualitative

metrics and indicators for measuring the influence of cascading effect, taking into account econometric information about value of goods and services.

3- Create models of cascading effects and interdependencies being a structured and formal way of describing such effects. These models will include causal relations, multi-sectorial infrastructure elements and environment parameters and possible human influence (human factor) on the state of crisis situation. Moreover, they will identify the key points in the incident evolution where decisions are needed, and the need for specific dependency and cascading risk information from stakeholders. These models also need to identify the type of decisions required, including preventive and preparation decisions. Executable versions of such models will be used for cascading effect simulation purposes.

4- Develop a suite of software tools for the simulation of cascading effects, decision support and creating collaborative expert networks and personnel training. These tools will help the PREDICT solution end-users to introduce new scenarios, simulate them and assess the potential decision-makers procedures in terms of their efficiency and effectiveness during a crisis. Continuous evaluation of the PREDICT solution outputs will be ensured by a dedicated expert network support tool. The developed suite of tools will be used in both preparedness and reaction phase of a crisis, allowing extensive virtual trainings and near real-time analysis of the situation. The developed tools will be suitable for assessing vulnerability of contingency plans, foreseeing consequences of complex crisis situations and determining the preconditions for failure of critical infrastructure.

5- Validate the solution through running simulations based on existing and developed cascading effects scenarios and using the developed models and tools. Such simulations will take into account infrastructure elements and relationships between them, environmental conditions, economic parameters, human behaviour and many other factors directly or indirectly affecting the course of the crisis situation. These simulations will be used to perform models behaviour test, which aim at comparing the simulation-generated

states of crisis situation with the observed reference behaviour. This will ensure the validity of developed solutions and help to improve results of the project. Moreover, such simulation might be used to generate a set of different, possible cascading effect scenarios. Due to a close cooperation with potential end-users, the PREDICT solution is considered to be deployed for them, for testing purposes and possible operational use.

6- Disseminate project results and build appropriate liaisons among various project stakeholders starting from end-users involved in the project (at various levels), members of Advisory Board, other end-users' representatives (five workshops will be organised with end-users external to the project), as well as general public. Moreover, the project results will be presented on forums and conferences related to crisis management and critical infrastructure topics. Additionally, the consortium will build connections between the PREDICT project and other, related initiatives, projects and programmes.

## The Partners

CEA (France), ITI (Poland), Fraunhofer (Germany), THALES (France), CEIS (Belgium), TNO (The Netherlands), VTT (Finland), VRZHZ (The Netherlands), SYKE (Finland), UIC (France), TRT-NL (The Netherlands).

If you would like to know more about PREDICT please visit regularly our website at [www.predict-project.eu](http://www.predict-project.eu)

*"Any publicity made by the beneficiaries in respect of the project, in whatever form and on or by whatever medium, must specify that it reflects only the author's views and that the [the Union] [Euratom] is not liable for any use that may be made of the information contained therein."*

*"PREDICT has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement no 607697".*

# CIP Scenarios: Lessons learnt from EU Exercises

In the CIPRNet project, we explore how to design a threat scenario for CIP.

On the 19-20th May 2014, CIP operators from the Energy, Transport, ICT and Water sectors met in Ispra (Italy) for the 2<sup>nd</sup> ERNCIP Operators' Workshop, organized by the European Reference Network for Critical Infrastructure Protection (ERNCIP) [1].

Critical Infrastructure operators highlight the need for CIP exercises based on threat scenarios.

Operators highlighted the need for templates of **scenario-based exercises** so as to exercise on hypothetical scenarios where practical decisions are needed. Exercises at national and EU wide scale, based on common threat scenarios, would be needed. Moreover, modelling efforts could drive the development of scenarios to be used for analysing possible cascading effects. While cost and confidentiality are a concern, operators value the opportunity to test their people and systems and to discover problems.

## Scenarios in CIPRNet

The CIPRNet project [2] currently designs such scenarios in order to develop, test and train users on the novel capabilities offered by the project. An example scenario is a flood-related, cross-border emergency in a densely populated region of the border between The Netherlands and Germany. In order to design the scenario, existing approaches were reviewed.

While pure CIP exercises on an EU level are quite rare, several exercises are performed annually under DG-ECHO's civil protection mechanism [3]. We explored publicly available information and exercise reports, focusing mainly on flood-related scenarios.

The exercises found were international; several Member States (MS) are participating as players to the

exercise. In most cases though, the actual incident affects a limited geographical area of one MS, which requests assistance by neighbouring MS.

Having a cross-boundary effect in terms of consequences is increasing the complexity of the exercises. It requires the coordination of operations across various countries and it exhausts available resources for international assistance. It also introduces communication problems. Communication and interoperability are identified as key factors in most exercises, even if these are limited within one region.

## How to design CIP scenarios?

Most exercises mention **key assets** and their condition. This information is important because (a) infrastructure disruptions affect the population and modify the needs for evacuation, medical care or rescue (water contamination, power disruption etc.) and (b) because they may be a resource for the command control and crews of the exercise. Therefore, it is also important to identify whether the centre of operations and the deployed teams have resources independent of the public and for how long they can maintain functions, without the need for resupplying.

CIP scenarios should identify whether an infrastructure is **critical for rescue or repair operations** (such as a main transportation node, an airport, or a fuel or water supply station needed in order for teams to be deployed or supplied).

One of the most important parameter to model in a CIP scenario is the condition of the **directly affected infrastructures** (e.g. water-related defences, in the threat of a flood). The type of damage or failure on these infrastructures can alter the scenario plot significantly but also the degree of damage it can cause.



Marianthi Theocharidou (JRC)

Marianthi Theocharidou works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), located in Ispra, Italy. She participates in the activities of the CIPRNet project and the European Reference Network for Critical Infrastructure Protection (ERNCIP).

email:  
[marianthi.theocharidou@jrc.ec.europa.eu](mailto:marianthi.theocharidou@jrc.ec.europa.eu)



## Scenarios in CIPRNet

The CIPRNet project [2] currently designs such scenarios in order to develop, test and train users on the novel capabilities offered by the project. An example scenario is a flood-related, **cross-border** emergency in a densely populated region of the border between The Netherlands and Germany. In order to design the scenario, existing approaches were reviewed.

While pure CIP exercises on an EU level are quite rare, several exercises are performed annually under DG-ECHO's civil protection mechanism [3]. We explored publicly available information and exercise reports, focusing mainly on flood-related scenarios.

The exercises found were international; several Member States (MS) are participating as players to the exercise. In most cases though, the actual incident affects a limited geographical area of one MS, which requests assistance by neighbouring MS.

Having a cross-boundary effect in terms of consequences is increasing the complexity of the exercises. It requires the coordination of operations across various countries and it exhausts available resources for international assistance. It also introduces communication problems. Communication and interoperability are identified as key factors in most exercises, even if these are limited within one region.

## How to design CIP scenarios?

Most exercises mention **key assets** and their condition. This information is important because (a) infrastructure disruptions affect the population and modify the needs for evacuation, medical care or rescue (water contamination, power disruption etc.) and (b) because they may be a resource for the command control and crews of the exercise. Therefore, it is also important to identify whether the center of operations and the deployed teams have resources independent of the public and for how long they can maintain functions, without the need for resupplying.

CIP scenarios should identify whether an infrastructure is **critical for rescue or repair operations** (such as a main transportation node, an airport, or a fuel or water supply station needed in order for teams to be deployed or supplied).

One of the most important parameter to model in a CIP scenario is the condition of the **directly affected infrastructures** (e.g. water-related defences, in the threat of a flood). The type of damage or failure on these infrastructures can alter the scenario plot significantly but also the degree of damage it can cause.

CIP scenarios can serve as a tool to identify the affected infrastructures within the geographic region where the threat scenario is realized. The next step is to identify disruptions that may occur in other infrastructures due to common-cause or cascading effects.

Moreover, several other infrastructures may face **common-cause or cascading disruptions** that augment the impact and complexity of the scenario. In the case of a flood scenario, we identified the following possible disruptions:

- transport disruptions due to flood-related accidents (derailment, collision of road vehicles, collision of maritime vehicles, structural elements collapse or overflow, e.g. tunnels, bridges, airports etc.)
- transport disruptions due to large scale evacuation of civilian causing traffic congestion
- disruptions of water supply or contamination of drinking water or other health hazards
- hazardous substances (CBRN) incidents due to structural damages/flooding on facilities
- hazardous substances (CBRN) incidents due to accidents to transporting vehicles,
- collapse of sewage systems
- electrical power supply disruptions
- telecommunications disruptions
- medical care facilities disruptions, due to power shortage, flooding, increased number of patients or inability of the personnel or supplies to reach the location

- industrial or business disruptions, due to power or communication disruptions.

Such disruptions, related to the threat scenario studied, should be included in the storyline. To increase the difficulty of the scenario, they can also be accompanied by other **unrelated events**, such as natural disasters, accidents or man-made incidents that modify the capacity of infrastructures.

The modelling of **dependencies** between infrastructures also indicates points of **information flow** required between different infrastructures and among different sectors.

Each scenario would be helpful if it is supported with **historical data** on previous, similar experiences in the geographic area. Such sources can provide useful information on the impact of the scenario and whether critical infrastructures can be affected. The scenario can also draw on **similar experiences** in neighbouring countries or regions. If such information is not available, other resources can be used, such as **risk assessments** that support the development of such a scenario in the specific region. CIP scenarios can also be used in order to examine **unprecedented or unlikely events** or **complex scenarios**, as this may also provide useful insight to decision makers, especially in terms of resources and critical infrastructure resilience.

A parameter examined in several scenarios is the introduction of conditions where **resources** are **stressed or exhausted** from previous incidents. Such incidents can be of similar nature but of a smaller scale (smaller scale floods, other incidents caused by the severe weather) or unrelated incidents in neighbouring regions (such as fire accidents, man-made attacks, etc.). Two alternative, but similar storylines can be exercised, where the difference lies on the availability of key resources in a specific point in time.

Most scenarios were supported by maps and screenshots of various phases of the incident. In some cases, the maps were limited, difficult to comprehend or read and with limited explanation. Each designed scenario should aim for **clear and comprehensive visualizations**, as this will enable to demonstrate clearly the

storyline and simulation results of the scenario.

Such visualizations can depict a screenshot of each phase (day, hour, etc.) of the scenario, marking affected infrastructures and other points of interest. For example, in most EU exercises the field exercise areas and the Center of Operations are marked clearly on the map. Other examples, include, locations where manned teams are needed for search and rescue, for repairing key infrastructures, etc.

In several cases, the **timeline** of events remained unclear and time periods were mixed. It would be useful if textual and graphical representation is used in order to describe the situation (state of operation on key infrastructures, location of deployed teams, extent of a natural phenomenon or accident etc.) for **specific, clear and distinct points of time**, in a structured way.

The scenarios can range from **early prognosis** or **alert signs**, several days before the actual initiating event occurs. In some cases, **preceding events** of previous months were described<sup>1</sup>. Important points of time are major changes in the development of scenario, e.g. changes in weather conditions, man-made incidents or infrastructure disruptions.

The **time of occurrence** can also alter significantly the outcome of a scenario. For example, the scenario can be affected by **daily** or **seasonal** or **miscellaneous** parameters. For example, an event in the area that increases the population (e.g. a festival, conference or convention) can increase the population affected. Similarly, the time of an event may alter the location of most vulnerable individuals or communities (e.g. event during school hours).

Moreover, a realistic scenario should reflect the interaction and decision-making needed both by **public and private CI operators**. Since public-private cooperation structures differ from country to country, the selection of varying cases or models of cooperation could be interesting to investigate among different scenarios.

Another parameter which needs to be taken into account is the **scalability** of the scenario, as the number of countries, operators and institutions is increasing. Therefore, it would be useful if the scenarios have a **varied level of complexity**, so as to identify the point where the use of the modelling capabilities poses limitations or on the contrary helps decision makers to overcome this obstacle.

When designing scenarios for CIP, a clear timeline is needed.

Each phase should clearly describe the evolution of the threat event over time, coupled with information on the operation status of all affected infrastructures at a given point of time.

One of the few table-top exercises focused on Critical Infrastructure Protection [4] also highlights the fact that the participants in such exercises share **different levels of CIP expertise**, which is a parameter that one needs to take into account when designing CIP scenarios. This means that the exercises should pose **gradual, increasing difficulty** to participants. For example, the scenario should firstly ask the participants to recognize the CIs present, identify their dependencies and then examine the international or cross-sectorial dimension of them.

## Summary

In summary, a scenario should serve a clear goal. A threat or a combination of threats (phenomena) needs to be selected for study. Then the scope of the exercise needs to be decided. This may refer to the geographical region, the timeframe, the involved stakeholders or the resources available. Creating a clear timeline is very important and for this reason, in the CIPNet project, we decided to describe each phase according to a specific template which covers the following information:

- **Timeframe / Duration:** This can be marked with specific points of time or specific events
- **Incident description:** This reflects the current situation of the phenomenon/threat studied
- **Affected infrastructure(s):** Information to be included is the name, the sector, the location, the operational status and the mode of operation (e.g. normal, stressed, recovery, etc.) for each affected infrastructure.
- **Maps:** This is needed in order to depict visually the status of each phase.

## References

- [1] ERNCIP, Joint Research Center, European Commission: [http://ipsc.jrc.ec.europa.eu/index.php/ERN\\_CIP/688/0/](http://ipsc.jrc.ec.europa.eu/index.php/ERN_CIP/688/0/)
- [2] CIPNet Project, <http://www.cipnet.eu/>
- [3] The Community mechanism for civil protection, [http://ec.europa.eu/echo/policies/disaster\\_response/mechanism\\_en.htm](http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm)
- [4] H.A.M. Luijff, D.J. Stolk, "An international tabletop exercise on critical infrastructure protection: the lessons identified", *Int. J. Critical Infrastructures*, Vol. 6, No. 3, pp.293-303, (2010)

<sup>1</sup> The selection of the **day zero** of a scenario can vary from the EU exercises, as it is usually marked by the activation of the mechanism for requesting international assistance.

This page is intentionally left blank.

# Data management and Information sharing in CIPRNet DSS

The CIPRNet DSS enables a 24/7 risk analysis of the CI elements, providing these data to the appropriate national authorities appointed for CIP and CI operators. The nature of the 1) exchanged data and 2) the involved DSS end-users requires a well-defined security plan.

One of the main technological outcomes of the EU-FP7 CIPRNet project[1] will be a Decision Support System (DSS) able to provide a 24/7 service to CI operators and emergency (crisis) decision-makers providing a continuous risk assessment of CI elements due to natural threats. The proposed DSS will encompass the whole workflow of actions ranging from the forecast of natural hazards to the prediction of the physical damages expected for the CI elements as a consequence of the threats manifestations, to the evaluation of the impacts that the physical damages will produce on the services delivered by the CI and the ultimate consequences that the reduction (or loss) of services will produce on citizens, primary services, industrial sectors and the environment.

The architectural design of the DSS has been performed by taking into account security issues. These have been considered at three different levels: physical, informational (IT) and organizational. At the physical level, security concerns with the protection of equipment and resources from damage and harms. Protective barriers and access control protocols are typical physical security measures. The information security concerns with data and information protection against unintended and / or unauthorized access. Organizational security level is, in turn, related to policies, procedures allowing users sharing sensitive information.

In this contribution we will initially recall the CIPRNet Risk Assessment Loop and the DSS architecture. Then, we will focus on some security aspects (i.e. physical and network access security, data and services availability and trusted information sharing) related to the above mentioned security levels.

## Risk Assessment Loop and DSS architecture

The CIPRNet Risk Assessment Loop (RAL) is composed of 5 Functional "Bricks" (Bn):

B1 - Monitor natural phenomena. B1 actions feed the DSS Risk Assessment Loop with external data coming from natural events monitoring sensor networks (e.g. geo-seismic, meteorological data) and data resulting from simulation model for natural events forecasting;

B2 - Prediction of natural events. The output of this phase is the prediction of the intensity of the different threats manifestations on a given area. For example, B2 may indicate that, in a given time frame, a particular region and/or city will be impacted by heavy rain and strong wind of specific intensities;

B3 - Prediction of harm scenarios. B3 will compare the B2 output with CI vulnerability data, in order to estimate the CI elements that will be affected (with a given probability) by the predicted natural threats. "Affected" means that the CI elements will be set in off-state or in a state of reduced functionality;

B4 - Impacts and consequences estimation. B4 represents the most complex task as it performs a number of different evaluations and will be performed by a tight collaboration between CIP experts and CI operators. B4 will initially provide the expected impacts on the CI (in terms of reduction or loss of functionality) and then the consequences, due to CI impacts, expected on citizens, industrial sectors, environment and the primary services (e.g. hospitals, schools);

B5 - Design of efficient strategies to cope with crisis scenarios and Reporting.



**Alberto Tofani** is a staff scientist at ENEA. He is member of the UTMEA-CAL Lab.  
e-mail: [alberto.tofani@enea.it](mailto:alberto.tofani@enea.it)



**Antonio De Nicola** is a staff scientist at ENEA. He is member of the UTMEA-CAL Lab.  
e-mail: [antonio.denicola@enea.it](mailto:antonio.denicola@enea.it)



**Antonio Di Pietro** is a staff scientist at ENEA. He is member of the UTMEA-CAL Lab.  
e-mail: [antonio.dipietro@enea.it](mailto:antonio.dipietro@enea.it)



**Maurizio Pollino** is a staff scientist at ENEA. He is member of the UTMEA-TER Lab.  
e-mail: [maurizio.pollino@enea.it](mailto:maurizio.pollino@enea.it)



**Luigi La Porta** is a staff scientist at ENEA. He is member of the UTMEA-TER Lab.  
e-mail: [luigi.laporta@enea.it](mailto:luigi.laporta@enea.it)

On the bases of Impacts and Consequences, the DSS could also, in some specific cases, develop optimized strategies to solve critical situations; these strategies could be prompted to the operator's attention, serving as a basis to develop real actions, to take over critical situations.

RAL is implemented through the 4-tier architecture as shown in Figure 1

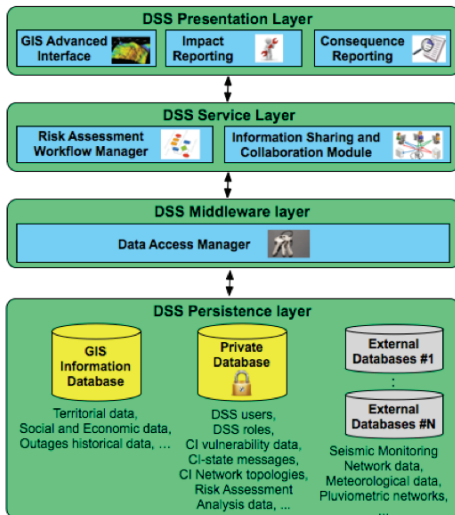


Figure 1 The DSS 4-tier architecture

The *Presentation Layer* contains the different components used to visualize the RAL results in an friendly user interface. In particular, the GIS advanced interface allows the end users to visualize CI elements risk maps and overlay this information with other information as, for example, impacts and consequences analysis results.

The *Service Layer* contains the different modules that realize the DSS business logic. In particular, this layer contains the RAL and the Information Sharing and Collaborative (ISC) platform. Other services are for example DSS System Admin services to manage the platform, DSS Analysis services to manage analysis tasks on the available data/simulations and DSS simulation service to manage and control simulation tasks.

The *Middleware Layer* implements procedures to gather, on a 24/7 basis, data coming from external sources as, for example meteorological data in order to get information to feed models and simulations enabling the prediction of future extreme natural events (e.g. flooding). In particular, the Data Access Manager will implement solutions to make the CIPRNet Persistence Layer compliant with the basic requirements for database and

network security. The first part of this contribution describes the proposed servers and databases configuration (related to the CIPRNet DSS Italian instance) to ensure the physical database integrity and network access control requirements.

The DSS Knowledge Base Layer is composed of different sub components:

-*CIPRNet data*. These are stored and managed using CIPRNet systems and applications. In turn, CIPRNet data will be further categorized as Public (i.e. data that can be accessed by generic end users using web applications and/or web services) that will be stored within the Private CIPRNet DB. Examples of private data are: users, identities and roles data, CI vulnerability data, Information Sharing and Collaborative (ISC) data, CI network topologies data and CIPRNet analysis results data. Private data will be stored within the Private CIPRNet DB. The CIPRNet security plan envisages two network and database different security levels for the two categories of databases;

-*External data*. In general, external data are stored in external databases. The DSS may rely on external data in different phases of the Risk Assessment Loop. For example, B1 relies on external sources of data. In B1, the DSS continuously receives data form different sources: seismic monitoring networks (e.g. in Italy these data are stored and managed by the Italian

-*Data and information shared with DSS end users* (e.g. CI operators, Crisis Management, Local Authorities). For example, the DSS RAL requires that CI operators exchange with CIPRnet experts data and information regarding the possible reduction of the QoS of their CI network related to an expected harm scenario (e.g. the DSS builds an expected harm scenario related to a future flooding event in a specific city area). The CIPRNet experts will use these data within the impact assessment phase in order to update the expected harm scenario considering possible cascading and dependency phenomena. As described in the following, the CIPRNet DSS will rely on a secure ISC platform to share and exchange data and information with the CIPRNet end-users.

## IT and Physical Security

Figure 2 shows the CIPRNet servers and databases configuration of the Italian CIPRNet DSS instance. The DSS server (running the Risk Assessment Loop, the Data Access Service, GIS modules), the ISC server as well as the CIPRNet Private DB will be hosted in the ENEA UTMEA Computer Centre. The UTMEA Computer Centre has the following characteristics: 1) the hardware and frameworks are hosted in a locked room (only authorized ENEA staff members can access the room), 2) the computer centre is

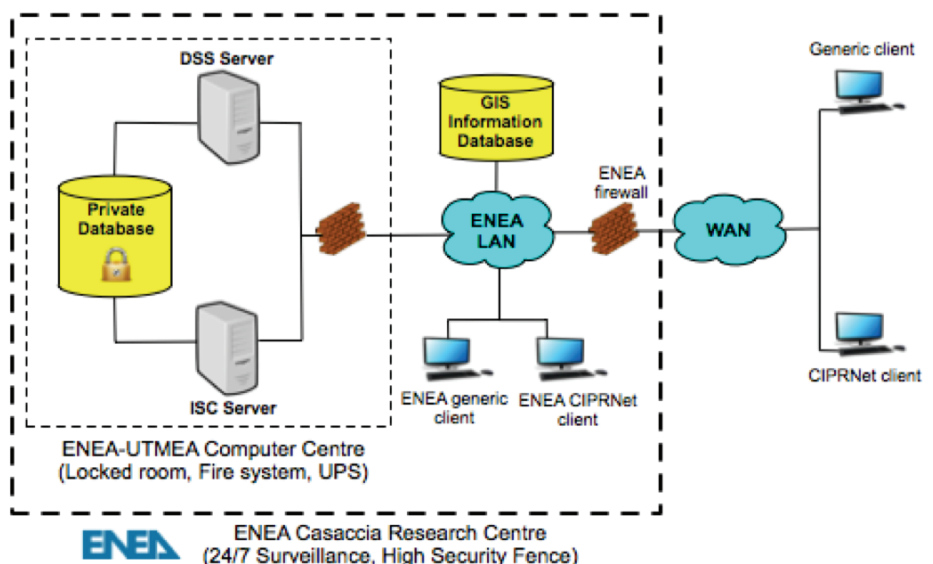


Figure 2 CIPRNet servers and database configuration

Geophysics and Volcanology Institute), meteorological stations (e.g. in Italy the stations are controlled by the Italian Air Force Met Office), pluviometric networks and so on;

equipped with a fire system and UPS system. Moreover, as shown in the Figure 2, ENEA UTMEA building (where CIPRNet servers will be located) is located inside the ENEA Casaccia Research Centre, a 24/7 access controlled Centre equipped with a

system of doubled high security fence. Then, the ENEA server configuration is compliant with the basic physical security requirements.

Regarding network access control requirements, the DSS servers and the CIPRNet Private DB are protected by two firewalls: a) the CIPRNet servers software-based firewalls and b) by the ENEA Casaccia firewall and monitoring systems that constitutes the main barrier to ensure access control to CIPRNet data and systems. Another relevant aspect in information security is the availability requirements to ensure that DSS services and data will be accessible as much as possible (in general the availability requirements are specified through minimum acceptable thresholds percentage of the time the service is available) to final end users even in case of equipment failures. In the following, the solution adopted for the Italian CIPRNet DSS instance for data and services replication will be described. In particular, this second part of the contribution concentrates on the technological solutions adopted to ensure a High Available server system.

slave is managed as a warm standby server, that is, it cannot be accessed until it is promoted master (another possible solution would be to have hot standby server, that is, it can accept connections and serves read-only queries). In order to guarantee the synchronization and the coherence of the database replica, the adopted solution will make use of Transaction Log Shipping [2]. Using this technique, the warm server is kept current by reading a stream of write-ahead log (WAL) records. In particular, the master server sends to the slave server log files containing all transactions that have been performed in the master database. In case of failure, the slave database server can use the log file to update the slave database with the last logged transactions. In general, this replica solution can be applied to manage redundant distributed geographically database servers (Figure 3). For example, for the Italian DSS instance the standby servers may be hosted in the Deltares (The Netherlands) research centre. Then, the Italian DSS may be operative even in the case the ENEA UTMEA Computer Centre is totally not operative.

share sensitive documents and information in order to increase the confidence level about a future extreme natural events prediction and share this information with other actors like Civil Protection, Police Force, Crisis Managers and DSS operators.

During the B3 and B4 phases, DSS operators and CI operators will exchange sensitive information in order to build an Expected CI Harm Scenario is the result of an extreme natural event (e.g. flooding). Figure 4 shows the information sharing process involved in the CI Harm Scenario Impact Assessment Loop that produces as result the Expected CI Harm Scenario.

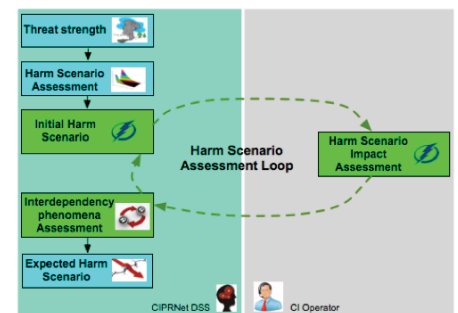


Figure 4 CI Harm Scenario Impact Assessment Loop

For example, let suppose that within the B2 phase the DSS predicts a flooding (the threat) of a certain intensity on a particular area of the city of Rome. The flooding intensity data and the CI elements vulnerability data w.r.t to flooding events will be used in B3 in order to build the so called Initial CI Harm Scenario. In this initial scenario some CI elements of different CI networks may be in failure state. The DSS operator will send this information to all involved CI operators. In turn, the CI operators are requested to provide to the DSS the expected impact (in term of the reduction of the QoS) induced by these failures on their networks. This information will feed an "system of systems" simulator to evaluate possible cascading effects induced by dependency and interdependency phenomena among CI. These phenomena, in general, may change the CI Harm Scenario and this information will be circulated with the CI operators within the CI Harm Scenario Assessment Loop until the Expected CI Harm Scenario is produced when a predefined equilibrium criteria is reached.

Last but not least, the DSS operator would need to share sensitive information with crisis decision makers

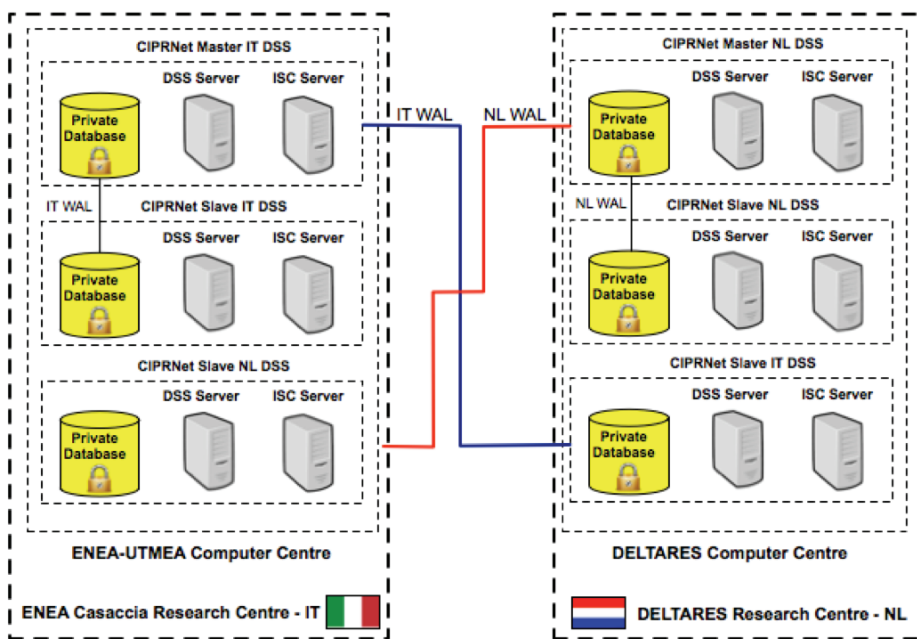


Figure 3 CIPRNet Master/Slave configuration and geographically distributed replication schema

Figure 3 shows the master/Slave CIPRNet DSS configuration. In particular, this configuration envisages the set-up of a replica of database servers, file system as well as the other main DSS services (Risk Assessment Loop, ISC and GIS services). In the described configuration, only the master or the primary server can modify data. The

### Trusted Information Sharing

Within the DSS RAL there are different phases where there will be the need of exchanging trusted and confidential information among different players. For instance, during the B1 and B2 phases, scientists can

during the B5 phase in order to distribute the Risk Assessment and Consequences Report to the involved actors.

At the end, the CIPRNet DSS needs to share information of various types with different players. In general, the process of sharing information in different DSS RAL phases would require the application of different policies and different security constraints. To meet these requirements, we have designed the "CIPRNet Information Sharing & Collaboration (ISC) Module" that will be inserted into the DSS RAL by purposely customizing the outcome of a previous EU project (NEISAS, National & European Information Sharing & Alerting System [3]). NEISAS project aimed at increasing security and trust in the exchange of information between CI operators and stakeholders. To this aim, NEISAS developed a framework consisting of a model and a platform for information sharing, attempting to ensure data integrity, confidentiality (anonymity) and trust, security and service availability.

The NEISAS information-sharing model guarantees information sharing by means of "trust circles".

A trust circle consists in a group of people exchanging information using the NEISAS platform. It is composed of users with trustmaster and member role. The former role has management functionalities, as the ability to define advanced sharing rules between different trust circles, which are not enabled to the latter. The trustmaster is seen as a trusted

coordinator and manager of a trusted information-sharing group. She/he is a member of a government agency or a trusted member elected as a representative of the group.

**Fehler! Verweisquelle konnte nicht gefunden werden.** shows possible trust circles sharing sensitive information within the CIPRNet DSS.

The NEISAS platform provides the following advanced functionalities:

- Traffic-light protocol for alerts [4]. It is a policy used to categorise information as white (unrestricted information), green (community-wide, but not released outside the community); amber (limited distribution on a need-to-know basis), and red (personal, for named recipients only).
- Information sharing on a one-to-one basis or with a specific group of members or other trust-circles
- Anonymous posts [5]. If sensitive information to be shared could potentially cause embarrassment to the originator's organization from a business perspective, the trustmaster could play a key role. The originator of the information may ask the trustmaster to advise other members about a specific topic, but to conceal her/his identity.
- Information Rights Management [6]. It offers a further level of security, as the content of an IRM protected alert cannot be copied or printed

Finally, besides the security aspects (at technical and organizational level), the NEISAS platform has been conceived as a Web 2.0 platform in the critical infrastructures domain by managing users (with their roles and digital identities), content and data to be shared.

## CIPRNet DSS Security Plan

In this contribution some aspects related to computer security have been described in the context of the CIPRNet DSS implementation. In particular, the contribution described the solutions and configurations adopted for the Italian instance of the DSS. The CIPRNet security plan encompasses many security aspects ranging from data base security to network security. In general, the CIPRNet security plan will drive the choice of every technologies and/or system that will be adopted. In this contribution we described in detail: Physical Database Security, Database and services availability, Network Security (Access control) and Organizational Security (Based on the NEISAS trust-circles).

## Acknowledgement

This work developed from the FP7 Network of Excellence CIPRNet, which is being partly funded by the European Commission under grant number FP7-312450-CIPRNet. The European Commission's support is gratefully acknowledged.

## References

- [1] CIPRNet FP7 EU Project – [www.ciprnet.eu](http://www.ciprnet.eu)
- [2] PostgreSQL 9.3 manual
- [3] NEISAS (National & European Information Sharing & Alerting System) European Research Project (Project ref: JLS/2008/CIPS/016)
- [4] Sutton, D., Cappelli M., Das-Purkayastha A., Bologna S., De Nicola A., Rosato V., Garwood A., Harrison J., Pollard D., Skellorn W. (2011). NEISAS Dissemination – Final Report.
- [5] Sutton, D., Harrison, J., Bologna, S., & Rosato, V. (2013). The Contribution of NEISAS to EP3R. In Critical Information Infrastructure Security (pp. 175-186). Springer Berlin Heidelberg.
- [6] Information Rights Management. [http://technet.microsoft.com/it-it/library/dd638140\(v=exchg.150\).asp](http://technet.microsoft.com/it-it/library/dd638140(v=exchg.150).asp)

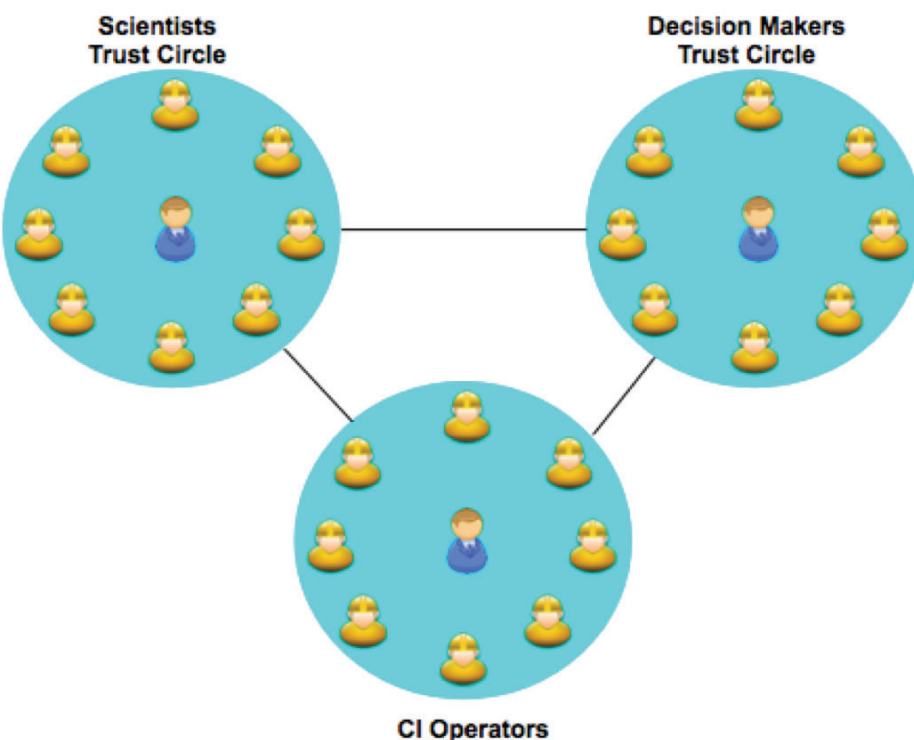


Figure 5 Example of CIPRNet DSS trust circles

# Meet the Future Cyber Talent

## Swiss Cyber Storm is performing a National Cyber Security Competition

With national concern about cyber security greater than ever, what can we do to help the public and private sector to stay ahead of today's and tomorrow's cyber security threats?

There is a huge demand for cyber security professionals willing to put their energy and passion into the field of cyber security research and defense. We need professionals who will network, who are willing to further their education and do not shy away from political discussions.

We, the Swiss Cyber Storm association, believe that it is the community's own responsibility to find, train and coach the most talented people for now and the future. That's why Swiss Cyber Storm is providing a suitable platform where security professionals can obtain and exchange information with regard to current cyber risks and cyber-attacks and defense topics.

However, another, maybe even more important point is to motivate enough young talents to pursue a career in IT security to meet the growing demand for cyber security professionals.

### Getting involved

One problem with this is that there are so many "cool" opportunities in IT which are much more visible to young talents than a career in IT security. To improve the odds, we have to make IT security more visible and tangible to both scholars and students.

And that's exactly where Swiss Cyber Storm comes in. Its purpose is:

- Encouraging young talents to pursue a career in IT security and to promote this topic among scholars and students
- To organize an international IT security conference on Cyber Attacks and Defense at which decision makers, IT security professionals and young talents meet to discuss current and future challenges in IT security.

### Security Challenges

Inspired by the success of the Cyber Security Austria association, who initially performed their first national cyber security challenge back in 2012, we decided to adapt the concept for Switzerland. The first Swiss challenges were then performed back in 2013. Suddenly the topic became quite a lot of attention not only among scholars and students but also in the media publishing reports and stories about the challenge.

### A simple receipt

Organizing a challenge following the model of CSA is quite straightforward. First, you need a platform that can provide and run a wide variety of different security puzzles. Challenges include many different disciplines, for example web application security, crypto, forensics, penetration testing or reverse engineering tasks.

Fortunately, the provider of the challenge platform (Hacking-Lab) being used by CSA was willing to support Swiss Cyber Storm on its way to organizing a similar event to those in Austria.

Using Hacking-Lab, we then invited the most talented scholars and students to participate in the Swiss Cyber Storm Security Challenge final run in parallel to the Swiss Cyber Storm IT security conference in Lucerne.

### Crossing borders

Since cyber security requires cooperation and trust,



#### Bernhard Tellenbach

Bernhard Tellenbach is a lecturer and researcher at Zurich University of Applied Sciences. His interests are focused on IT security, coarsely ranging across network security, system security and network monitoring.

Prior to being appointed by ZHAW he was with ETH Zurich, University of Applied Sciences Rapperswil, Consecom AG, and ran his own IT consultancy business. He was a visiting scholar at Microsoft Research Cambridge and Institut Eurécom.

His works have been published in several journals, and conferences. He serves as a technical reviewer for several international journals and conferences.

e-mail:  
[president@swisscyberstorm.com](mailto:president@swisscyberstorm.com)



we wanted to reflect this by partnering with Cyber Security Austria. Together we set up the "Security Alpen Cup" where the most talented contestants from Austria and Switzerland "fought" against each other. This cooperation boosted the visibility of this initiative considerably and was for the benefit of both CSA and Swiss Cyber Storm, even though the Swiss team won the first Security Alpen Cup.

### Thinking big

The next step now is to internationalize the idea and the event even further. A first step has

been taken this year by inviting Germany to participate in this cross-border event. Since the name "Security Alpen Cup" is no longer appropriate for an internationalized competition, the name has been changed to "European Cyber Security Challenge".


To make the challenges even more interesting and to foster international collaboration among young cyber talents, we invite other European countries to join the European Cyber Security competition.

### Becoming part of it

If you now feel like doing the same in your country or if you just want to have a closer look at the next Swiss Cyber Storm Security Challenge, please do not hesitate to contact us at [president@swisscyberstorm.com](mailto:president@swisscyberstorm.com).

Please save the date and visit the upcoming Swiss Cyber Storm conference and award ceremony on October 22<sup>nd</sup>, 2014 at the KKL in Lucerne. For more details, please visit [www.swisscyberstorm.com](http://www.swisscyberstorm.com)



 Schweizer Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB  
Nachrichtendienst des Bundes NDB  
Melde- und Analysestelle Informationssicherung MELANI



# Netonets: Critical Infrastructures as Network of Networks

During last years a new community was born aimed at combining experts from the Critical Infrastructures Protection and the Complexity Science. A book reviewing the state of the art of the field has recently appeared

During last decades the complexity of the full developed society has been steadily increasing. Any modern device is now endowed with some intelligent tools to improve its capabilities, to enhance its robustness and resilience, to reduce energy consumption, to moderate its price, to ease its recycling and optimize other characteristics such as size, portability etc. The introduction of the intelligent layer is not limited to the tools or devices, it extends to small or even large infrastructures. Any Museum, library or other public place is usually endowed with SCADA system for safety (anti-fire, anti-intrusion etc.) and governance reasons. Those SCADA systems allow for a constant monitoring and real time governance of the activities. The most dwelling and relevant systems that are presently permeated by intelligent devices are the large infrastructures such as pipelines, gas-ducts, power plants, data centres, aqueducts, etc. All full developed infrastructures do strongly rely on the communication network, the electronic control system and automation software. Moreover almost all other infrastructures depend on others such as the Electric System, the Transport (at least for employs availability and maintenance) and most of them on water supply. The owners of the Infrastructures are normally able to handle the majority of undesired situations by means of suitable measures (often also organic contingency plans) and in several cases the resilience of the service they provide is assured. However even the actuation of measures requires the availability of (at least some) other infrastructures they depend on. Therefore, a "systemic approach" is required to build up global measures and contingency plans implying the synergistic cooperation of the different infrastructures. In other words one has to deal with the "System of Systems" as a holomorphic unique entity. Due to the advent of the "smart society" the complexity of this "system of system" is destined to

increase and hence the role of the systemic framework is expected to become central.

As commonly understood, the "Systemic Risk" is a concept employed in the world of finance to refer to the danger related to a potential collapse of an entire financial sector (or a market) due to its global structure and not to a specific weakness of one of its components. The same concept can be extended to full developed societies which functioning depends on a multitude of different interdependent infrastructures. The most important infrastructures, that is those providing vital resources and sustaining the "quality of life" in the full developed countries, are often referred to as "Critical Infrastructures" (CI) and represent the core of such a complex organism that is human society.

The functioning of CI's requires a strong control of several technologies and management capabilities that are essential for providing the service or good they are devised for. Those technicalities do deeply depend on the type of infrastructure and represent a fundamental know-how that needs a constant upgrade. Despite these differences, all the infrastructures share some common characteristics. The most relevant is their partition into units (components) that are geographically and functionally separated and connected by cables, pipes or other links that allow transfer of the primary good or service. This characteristic is very special as it leads to a conceptualization of those systems as "networks" or, from the mathematical point of view, "graphs". Moving steps from this fundamental observation at the end of the past century a novel discipline was born: the "Complexity Science" [1]. This branch of the human knowledge results from the combination of the Statistical Mechanics and the Graph Theory.



**Gregorio D'Agostino**

Gregorio is a theoretical physicist that received his "laurea" and PhD in Physics at University of Rome "La Sapienza". He is presently Senior Researcher at ENEA (Italian National Agency for the New Technology the Innovation and the Sustainable Economic Development); Visitor Researcher at Boston University and Visitor Scientist at LIMS (The London Institute for Mathematical Sciences). He is President of the AIIC (The Italian Association of Experts in Critical Infrastructures) and a member of the OSN (Observatory for National Security). He has been project manager and coordinator of the European project MOTIA aimed at Modeling Interdependencies among ICT critical Infrastructures and is currently involved in different EU projects. In collaboration with Antonio Scala he is leader of the international organization Netonets.

Phone +39 06 30484776  
website: [gordion.casaccia.enea.it](http://gordion.casaccia.enea.it)  
email: [gregorio.dagostino@enea.it](mailto:gregorio.dagostino@enea.it)

The underlying idea is that when the number of components of a system increases (strictly speaking going to infinity) a collective "emergent behavior" is observed and simple rules start governing its temporal evolution. Similarly to what happens to gases, we can disregard the details of interaction between molecules and the system is governed by simple thermodynamic equations. Analogously, when a, large enough, system of computers is attacked by a malware, its epidemic spread does not depend on the details of the propagation mechanism, but on the topology of the system and on the mere infection rate.

The complexity Science paradigms has been successfully applied to several field from the biology to the social Science. However, as explained above, to study the CI's one has to deal with systems of systems, that is, according to the complexity science paradigm, with "Networks of Networks" or "Netonets". It is worth stressing that netonets may result not only from the interdependences between networks of different types, but also from the aggregation of homogeneous

is represented by the ENTSOE (European Network of Transmission System Operators for Electricity). In this case each of the TSO's governs a high voltage (400kV) transmission electric infrastructure while receiving or providing power to other networks.

All critical infrastructures share some common characteristics: Most relevant is their partition into units (components) that are geographically and functionally separated and interconnected ...

The ENTSOE system provides energy to some 500 millions people, assuring a complete phase synchronization all over the "Old Continent". For this reason, it has been named the European "Beating Heart". Another example of network of homogeneous networks is given by the Autonomous Systems (AS's) of the Internet. The owner of each autonomous system provides names and IP numbers

Fig. 1 represents the graph of all AS's on Internet as it appeared on April 2012: the system consisted of some 30,000 AS's linked by some 300,000 different connections.

Despite the huge development of the Complexity Science, the technological community for the Protection of Critical Infrastructures has not yet fully benefit of that discipline. The Netonets community and its relative website ([www.netonets.org](http://www.netonets.org)) were born to fulfill the need of a bridge between the Complexity Science community and that of CIP (Critical Infrastructure Protection). Netonets rises from the coordinated efforts by Gregorio D'Agostino and Antonio Scala, aimed at inspecting the potentiality of such a hybrid community. Netonets has its own international committee formed by Raissa D'Souza, Shlomo Havlin, Wolfgang Kroeger and Gene Stanley that are among the most outstanding personalities in this emerging field.

Under the egida of the Netonets community, several conferences on "Network of Networks" have been organized. Among them it is worth noting the series carrying the same name: Netonets that took place



**Figure 6:** Internet represents a prototype of "Network of homogeneous Networks": each point represents an autonomous IP networks which color depends on the nationality of the owner. The picture has been obtained within the European Project "MOTIA" coordinated by ENEA

and 2014 (in Berkeley (CA)) and the COINETs series: 2012 (in Bruxelles) and 2014 (in Lucca). During the former events the majority of scientist involved in the Netonets research have been invited, thus covering a great part of the whole subject. The network of excellence CIPRNET ([www.ciprnet.eu](http://www.ciprnet.eu)) and the European project Multiplex ([www.multiplex.eu](http://www.multiplex.eu)) are among the most important European activities on the subject, moving from the CIP and the Complexity perspectives, respectively. They both have endorsed different initiatives such as Netonets and Coinets, and have contributed significant presentations to the conferences.

Several information on the different activities performed under the Netonets behalf are available on the website. To be kept informed on main improvement and events in netonets community, one may register in the website.

## The last frontier of Complexity Science

Quite recently, the Netonets community has produced a book that represents an attempt to provide an organic presentation of the state of the art of the discipline. It presents most of the different applications of the "Network of Networks" paradigm to different fields from Physiology to CIP. This book has been entitled "Network of Networks: the Last Frontier of Complexity" [2] as it represents one of the most recent challenges of the Complexity Science. The book tries to present and combine the efforts from both the Complexity and the CIP community. Several theoretical models are presented, starting from the percolation of interdependent networks by the Boston University Group that has imposed the subject of "Network of Networks" to the wide scientific audience attention [3]. However the first real attempt to apply Complexity to Netonets was due to Ian Dobson, Carreras and David Newman [4] that dealt with the problem of failures propagation on interdependent networks (Hawaii conferences). Moreover an other important step toward the application to real networks (in his case the North America inter-connected electric systems) is due to Raissa D'Souza's group [5].

Beside this leading activities, quite recently, the problem of epidemics

on Network of Networks has been also dealt with by a mere spectral approach at topological level [6] thus proving interesting exact inequalities to predict the behavior of the global system. The influence of topology on synchronizability of netonets has been recently investigated [7]. These further develops are not presented in the book.

The book is a good reference point for members of the novel hybrid community...

Other approaches to interdependent networks at basically topological level have been presented in the book. Among others it is worth mentioning the "Multiplex" approach that is the oldest one (coming from early works in sociology) and has been applied to social and financial netonets. The slight difference with the previous approach is that the set of nodes is common to all nets while the type of links have different types.

All the former theoretical works show that some emergent behaviors are observed and even the mere topology of the systems play a non trivial role for its robustness. This could provide important advices for future network expansions and re-designing. However to achieve improvements in different directions, such as assessing contingency plans, dynamical risk assessment and "what if" analysis, the pure topological approach is not enough and some details on the actual functioning of the different systems and their interdependencies need to be introduced. To this purpose, the book provides best practices for risk assessment, agent base modeling and the software federation approach. As for the workshops, several authors from both the CIPRNET and Multiplex contributed to the book

The book also provides realistic risk estimates for interacting networks (included financial systems), significant applications to transport and even to physiology. Also a human body can be conceptualized to a system of systems and the techniques of analysis of signals in interacting system do represent an other useful tool that deserves more inspection also for technological infrastructures.

We do believe that the book represents a good reference point for

members of the novel hybrid community; however it can not be considered exhaustive: several other theoretical approaches have not been treated or deserve some further treatments. Certainly the I/O models should have been included among the most abstract conceptualizations and the systemic risk analysis is under-rated.

## Future develops and needs

From the mathematical point of view a very important field needs to be developed, that is the Statistical Mechanics of systems with finite or even small size. This is actually a critical point as real systems do exhibit a finite number of degrees of freedom. On the other side, there is a very important problem that is central and yet not appropriately treated that is the role of human arbitry. Decision makers and the collective behavior of operators and customers upon undesired events or unexpected situations should account for this issue in order to provide prediction for both the management of the different infrastructures. Understanding and modeling those critical elements requires the synergistic application of different disciplines such as Sociology, Psychology, Economy and the domain knowledge required to predict the consequences of the potential measures. Most of people or groups share similar interests and hence they are expected to exhibit common behaviors; therefore, again, netonets paradigm may represent a versatile tool to predict collective emergent behaviors.

## References

- [1] A. L. Barabasi, R. Albert Science 285 (1999) 509
- [2] "Networks of Networks: The Last Frontier of Complexity" G D'Agostino, A Scala - Springer Berlin Heidelberg (2014).
- [3] Buldyrev et al Nature 464, (2010) 1025-1028
- [4] I Dobson, B.A. Carreras, DE Newman Probability in the Engineering and Informational Sciences 19 (1), 15-32
- [5] C.D. Brummitt, RM D'Souza, EA Leicht PNAS 109 (2012), E680--E689
- [6] H. Wang et al. Physical Review E 88 (2), 022801
- [7] J. Martin Hernandez et al. Physica A 404, 92 (2014)

Understanding Complex Systems

Springer:  
COMPLEXITY

Gregorio D'Agostino  
Antonio Scala *Editors*

# Networks of Networks: The Last Frontier of Complexity

 Springer

# Experiences from the CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (CI)

The Critical Infrastructure Community from multiple countries was reunited in Paris with the occasion of the first edition training event of CIPRNet.

The Master Class on Modelling, Simulation and Analysis of Critical Infrastructure was held on 24-25 April 2014 at the International Union of Railways (UIC) Headquarters in Paris, France. The aim was to perform training and activities for the Critical Infrastructure Protection community. This 1.5 day training event is the first edition of a series of training events organised within the European FP7 Project CIPRNet – Critical Infrastructure Preparedness and Resilience Research Network. The Master Class was successfully organised by the University Campus Bio-Medico of Rome in coordination with the International Union of Railways – UIC and the French Alternative Energies and Atomic Energy Commission – CEA.

This meeting gave the opportunity to different research institutions to talk, exchange ideas, better know each other and create common views. The training attracted about 40 experts from CI operators, Public Authorities and researchers and experts from the Critical Infrastructure Protection research communities. The participants had the chance to learn about modelling, simulation and analysis of Critical Infrastructure. They were informed of its applications in analysis, decision support and training. Experts from the CIPRNet's network presented lectures in order to explain basic concepts and advanced aspects related to federated simulation and the use of the Open Modelling Interface (OpenMI).

The event was announced via the CIPRNet website and the registration was online. The number of participants was limited to 40 but was free of charge.

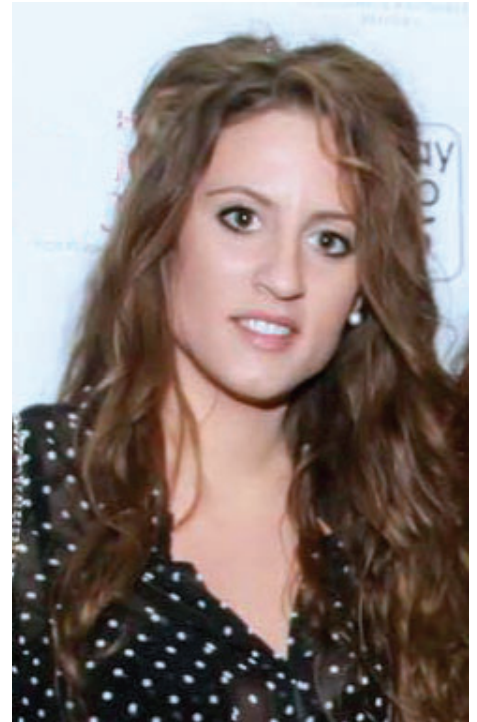
## Master Class: Day One

The Master Class was opened with a warm welcome to the event by J. Pires from UIC who hosted the event. The entire Master Class was organized into 14 sessions. In the first session, E. Rome, from Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS), Germany introduced us to CIPRNet. He started by describing CIPRNet and defining Critical Infrastructures. He stated all the capabilities, benefits and goals of CIPRNet and how they will be achieved.

Participants of the Master Class had the chance to interact with experts from diverse areas of Critical Infrastructures, share their opinion on problems and their solutions and create the first contacts for future collaborations.

The second session focused on critical infrastructure protection and critical infrastructure resilience. C. Pursiainen from the Joint Research Centre of the European Commission presented this session. Through his talk he explained everything about the concept of critical infrastructure resilience. Origin, approaches, dimensions, definitions, enhancement and how to measure and test technological resilience.

The next session "Simulation of Critical Infrastructures (CI): relevant applications", by E. Luijff, from Netherlands Organisation for Applied Scientific Research (TNO) explained



### Elena Polykarpou

Elena Polykarpou is a Research Associate at the KIOS Research Center for Intelligent Systems and Networks at the University of Cyprus. She is also working towards her PhD degree.

Elena received her BSc with Honors in 2010 and her MEng in 2012 from the Department of Electrical and Computer Engineering at the University of Cyprus. Her research interests include monitoring, security and control of power systems, modeling and parameter estimation of loads.

e-mail:  
[polykarpou.elena@ucy.ac.cy](mailto:polykarpou.elena@ucy.ac.cy)

where CI Protection MS&A can be applied and the added value for stakeholders. He also outlined some existing activities all over the world and what we are looking forward to.

Principal modelling techniques was the focus of the fourth session. M. Eid from Atomic Energy and Alternative Energies Commission explained modelling of complex systems and what solutions we can have. We were also showed CI as a collection of heterogeneous interacting components.

Modelling and investigating dependencies was the next topic presented by R. Setola from University Campus Bio-Medico of Rome. In this session we learned the importance of (inter)dependencies and how the most common phenomena can be modelled. We were showed some events and failures so that we could understand the consequences that can result if we neglect to capture them.

V. Rosato from Italian National Agency for New Technologies, Energy and Sustainable Economic Development analysed us the topological properties of complex networks and their relevance for CI. In his talk Dr. Rosato introduced us to graph theory and explained how it is related with complex system properties. It was showed that functioning properties of complex networks can be found by the topological properties and for specific topological shapes of networks that represent CI, robustness and functionality criteria can be met.

The seventh session, "Hybrid engineering/phenomenological approach to simulate systems of systems" was presented by J. Marti, from the University of British Columbia, Vancouver. Prof. Marti discussed how multiple CIs interact in case of disaster response and other critical applications. I2Sim multi-system engineering/phenomenological modelling was also presented. The i2Sim modelling framework allows the integration of both engineering and human systems. I2Sim allows real-time solutions of large multi-CI system of systems. The objective is to have a real-time disaster response optimization. Partitioning of the solution may be used for large and complex systems.

The first day sessions were closed by B. Becker and A. Burzel from Stichting Deltares who introduced us to OpenMI (Open Modelling Interface). We were showed the basic concepts and a life demonstration example. OpenMI is an open model interface standard. It is designed for hydro-related models and is already used by several institutions. With OpenMI time-dependent models can exchange data during runtime at each time step. OpenMI is used for coupling models either of different processes either of the same type allowing this way to simulate interaction processes. We were demonstrated how an open channel flow model is coupled with a real-time control model.

The first day was closed by a welcome cocktail at the UIC grand hall. This cocktail gave the participants the opportunity to know each other better and share their thoughts after attending the first eight sessions. It was a nice and warm break for the attendees giving them the opportunity for networking. Since the Master Class attracted experts from various fields they could discuss their different opinions so that they can overtake any issues that may arise and head to the goal of CIPRNet to create new capabilities, build the required capacities and provide knowledge and technology.

## Master Class: Day Two

The Master Class continued the second day with the ninth session presented by W. Huiskamp from the Netherlands Organisation for Applied Scientific Research. This session focused on the federated approach for the simulation of complex systems. Mr. Huiskamp outlined the available

architectures and standards. He explained High Level Architecture (HLA) and Distributed Simulation Engineering and Execution Process (DSEEP).

Modelling, simulation and analysis techniques for CIP were described by A. Usov from Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS). Following the previous session for federated simulation a comparison was made with integrated modelling and simulation. For a better understanding, an example for both approaches was analysed, i2Sim framework for the integrated approach and DIESIS architectural approach for the federated. In this session it was showed that for many CIP applications modelling and simulation is very useful and the analysis of multi-CI is challenging.

E. van Veldhoven from the Netherlands Organisation for Applied Scientific Research highlighted the importance of verification and validation. In this talk Mr. Van Veldhoven convinced us for the need of verification and validation in a structured way and with the right technique. He explained that more benefits are gained by V&V in comparison to the cost. An overview of the techniques was presented and how we should choose the right one for our CI models. In the end, we were outlined the four basic categories of tests that can be used.

The eleventh session was presented by M. Pollino from the Italian National Agency for New Technologies, Energy and Sustainable Economic Development. Mr. Pollino discussed the Geographical information systems for visualisation and analysis. The basic concepts and functionalities of Geomatics were



outlined. We were presented examples of applications, integration of the technique and computational modules. In addition, the case of an earthquake event was analysed to show us the resulting impact and the consequences.

Real-time event prediction was described in the twelfth session by A. Zijderveld from Stichting Deltares. Mrs. Zijderveld explained that measurements and sensors enhance the accuracy and reliability of forecasting whereas probabilistic forecasting can create uncertainties. Hazard prediction may result by combining the available measured data and model simulations. In addition, we were also showed some examples for better illustration. Nowadays, the real-time services are increasing both in quality and lead-time.

The sessions closed V. Rosato from Italian National Agency for New Technologies, Energy and Sustainable Economic Development. The focus was on the Decision Support system (DSS) in the area of risk management of CI. We were presented the DSS and how it is used in the risk management of CI. A DSS must be able to observe and predict an event, the harm scenario, the impacts and consequences from damages and help decision makers to compile useful information, identify critical situations and take decisions.

The Master Class finished with a very interesting discussion by everyone. With the final comments it was obvious that the goal of the Master

Class to strengthen the links and create common views was achieved. Various opinions from many sides were expressed.

## Master Class Summary

The Master Class was very well organized and accomplished all its initial goals. It attracted people from various areas making the discussions particularly interesting. The participants consisted of people from multiple countries all over the world giving the opportunity to each one expressing their opinion based on their own experiences and points of view. It achieved to give the chance for networking, bring diverse communities together and give the chance for future collaborations. The attendees had also the chance to learn about modelling, simulation and analysis of CI from the best in the field experts. By having people of

all ages and levels of expertise it was like a baptism for entering the professional community. The event surpassed everyone's expectations.

## Further Information

More info along with the full program of the Master Class can be found at the official website of the event <https://www.ciprnet.eu/endusertraining.html>. All the presentations are archived at <https://www.ciprnet.eu/login.html> and are available to all the participants.

The next Master Class will be held in Rome, Italy where the focus will be on DSS. Keeping the high level of the training schools of CIPRNet, experts will be invited to talk and share their knowledge to everyone that will attend the Master Class.





This Page is intentionally left blank.

# CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security

Bringing together researchers and professionals from academia, industry and governmental organizations working in the field of the security of critical infrastructure systems.

On behalf of the Steering Committee and the Local Organising Committee we are excited to invite you to submit papers and attend the CRITIS 2014 conference. CRITIS 2014 will be held in October 2014 in Limassol, Cyprus and it continues a well-established tradition of successful annual conferences. It aims at bringing together researchers and professionals from academia, industry and governmental organisations working in the field of the security of critical infrastructure systems.

Modern society relies on the availability and smooth operation of a variety of complex engineering systems. These systems are termed Critical Infrastructure Systems (CIS). Some of the most prominent examples of critical infrastructure systems are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, and oil / natural gas pipelines.

Our everyday life and well-being depend heavily on the reliable operation and efficient management of these critical infrastructures. The citizens expect that critical infrastructure systems will always be available and that, at the same time, they will

be managed efficiently (i.e., they will have a low cost). Experience has shown that this is most often true. Nevertheless, critical infrastructure systems fail occasionally. Their failure may be due to natural disasters (e.g., earthquakes and floods), accidental failures (e.g., equipment failures, software bugs, and human errors), or malicious attacks (either direct or remote). When critical infrastructures fail, the consequences are tremendous. These consequences may be classified into societal, health, and economic.

Conference web site:  
<http://www.critis2014.org>

Conference dates  
13-15 October 2014

The venue of the CRITIS 2014 conference will be the magnificent Grand Resort Hotel, in Limassol, Cyprus. The hotel is set in over 20,000 square meters of beautifully landscaped gardens with exotic trees and subtropical plants, which extend right down to the seashore.



**Elias Kyriakides**

is an Assistant Professor at the Dept of Electrical and Computer Engineering and the Associate Director for Research at the KIOS Research Center for Intelligent Systems and Networks, University of Cyprus

e-mail: [elias@ucy.ac.cy](mailto:elias@ucy.ac.cy)



## Conference Topics

- Infrastructure resilience and survivability
- Security and protection of complex cyber-physical systems
- Self-healing, self-protection, and self-management architectures
- Cyber security in critical infrastructure systems
- Critical (information-based) infrastructures exercises and contingency plans
- Advanced forensic methodologies for critical information infrastructures
- Economics, investments and incentives of critical infrastructure protection
- Infrastructure dependencies: modelling, simulation, analysis and validation
- Critical infrastructure network and organizational vulnerability analysis
- Critical infrastructure threat and attack modelling
- Public-private partnership for critical infrastructure resilience
- Critical infrastructure protection policies at national and cross-border levels
- Fault diagnosis for critical infrastructures
- Fault tolerant control for critical infrastructures
- Security and protection of smart buildings
- Detection and management of incidents/attacks on critical infrastructures
- Preparedness, prevention, mitigation and planning

## Sponsorship and Exhibition Opportunities

The CRITIS 2014 Conference is a unique opportunity for organizations to connect with up to 150 leading experts in the fields of security and protection of critical infrastructure and critical information systems who work in a variety of government, academic, and private sectors. This would be a wonderful opportunity for your organization to have significant visibility in front of an audience who could benefit and value from your participation at this conference.

We are delighted to invite you to sponsor and/or exhibit at the CRITIS 2014 Conference. The Organizing Committee is committed to providing an exciting and informative program

of speakers, and facilitating networking and business opportunities for sponsors.

Sponsors and exhibitors will receive acknowledgement prior to, during and after the conference through conference materials, the web site, and the plenary sessions, and enjoy significant contact with delegates during the exhibition and social events. The exhibition will be open for the duration of the conference. Our sponsorship and exhibitor packages are very attractive and cost-efficient.

Please do not hesitate to contact us to discuss how we can customize a package that meets your marketing objectives. We are happy to work together with you to create an individual offer to ensuring the best result for your company.

CRITIS 14 is where the CIP expert and researchers meet and exchange. Align with newest trends and get inspired: Don't miss this chance!

## Conference Proceedings

All accepted papers will be included in the conference proceedings which will be distributed during the conference. Selected papers will also be included in a special volume and published by Springer-Verlag Lecture Notes in Computer Science.

## Conference Program

The Conference Program and registration details will be announced along the announcement of the accepted papers. Please stay tuned at the conference web site.

## CIPRNet Young CRITIS Award (CYCA)

An award for outstanding research in Critical Infrastructure Security and Protection sponsored by the EU FP7 NoE CIPRNet will honour winners at CRITIS 2014. It is a unique chance for young researchers to be recognised. For more information: [cyca.critis2014.org](http://cyca.critis2014.org)



## Organisers and Contact Information

### General Chairs:

Marios Polycarpou (University of Cyprus)  
Elias Kyriakides (University of Cyprus)

### Program Chair

Christos Panayiotou (University of Cyprus)

### Program Co-Chairs

Vicenç Puig (Universitat Politècnica de Catalunya)  
Erich Rome (Fraunhofer Institute for Intelligent Analysis and Information Systems)

### Publications Chair

Georgios Ellinas (University of Cyprus)

### Publicity Chairs

Demetrios Eliades (University of Cyprus)  
Cristina Alcaraz (University of Malaga)

For more information:

Elias Kyriakides ([elias@ucy.ac.cy](mailto:elias@ucy.ac.cy))  
Or visit <http://www.critis2014.org>

## Links

ECN home page <http://www.ciprnet.eu>  
ECN registration page free registration on [www.ciip-newsletter.org](http://www.ciip-newsletter.org)

### Forthcoming conferences and workshops

IDRC 2014	<a href="http://idrc.info/programme/call-for-abstracts">http://idrc.info/programme/call-for-abstracts</a>	24-28.08.14	Davos, Switzerland
EAIS 2014	<a href="https://fedcsis.org/2014/eais">https://fedcsis.org/2014/eais</a>	7-10.09. 14	Warsaw, Poland,
CRITIS 2014	<a href="http://www.critis2014.org">www.critis2014.org</a>	13-15.10.14	Limassol Cyprus
Swiss Cyber Storm	<a href="http://www.swisscyberstorm.com">www.swisscyberstorm.com</a>	22. 08.14	Lucerne Switzerland

### Exhibitions

Interschutz 2015 <http://www.interschutz.de/86385> 8.-13.6.2015 Hannover ,Germany

### Master Class

Program and info <https://www.ciprnet.eu/endusertraining.html>  
Presentations (on request only: <https://www.ciprnet.eu/login.html>)

### Associations

Global Risk Forum Davos [www.grforum.org](http://www.grforum.org)  
Swiss Cyber Storm [www.swisscyberstorm.com/](http://www.swisscyberstorm.com/)

### Institutions

National and European [www.neisas.eu](http://www.neisas.eu)  
Information Sharing & Alerting System  
Networks of Networks <http://gordion.casaccia.enea.it>  
Mechanism for civil protection, [http://ec.europa.eu/echo/policies/disaster\\_response/mechanism\\_en.htm](http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm)

### Project home pages

FP7 CIPRNet [www.ciprnet.eu](http://www.ciprnet.eu)  
EU Security Liaison Officer [www.slo-project.eu](http://www.slo-project.eu)  
Conference contributions: [www.coseritylab.it](http://www.coseritylab.it) (for download)  
FP 7 INTACT [www.meteo.unican.es/projects/intact](http://www.meteo.unican.es/projects/intact)  
PREDICT [www.predict-project.eu](http://www.predict-project.eu)

### Interesting Downloads

Critis' 12 Conf. Proceedings: [www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8](http://www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8)  
Critis' 13 Conf. Proceedings: <http://link.springer.com/book/10.1007/978-3-319-03964-0>

European Network and Information Security Agency [www.ENISA.eu](http://www.ENISA.eu) publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection"  
ENISA [www.enisa.europa.eu/activities/Resilience-and-CIIP](http://www.enisa.europa.eu/activities/Resilience-and-CIIP)

### Websites of Contributors

Joint Research Centre <http://ipsc.jrc.ec.europa.eu>

# CRITIS 2014

9<sup>th</sup> International Conference on  
Critical Information Infrastructures Security  
October 13-15, 2014, Limassol, Cyprus  
[www.critis2014.org](http://www.critis2014.org)

