European CIIP Newsletter

November 13 – February 14, Volume 7, Number 2

ECN

Contents:

> 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

>Articles to be published can be submitted to:
editor@ciip-newsletter.org

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

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

>Download site for specific issues:
www.ciprnet.eu

>Founders and Editors
Eyal Adar, Founder and CEO, WCK www.wck-grc.com
Christina Alcaraz, University of Malaga, alcaraz@lcc.uma.es
Bernhard M. Hämmerli, HTA, Initiator and Main Editor bmhaemmerli@acris.ch
Eric Luiijf, TNO, eric.luiijf@tno.nl
Erich Rome, Fraunhofer, erich.rome@iais.fraunhofer.de

>Country specific Editors
For France: Michel Riguidel, ENST, riguidel@enst.fr
For Spain: Javier Lopez, UMA, jlm@lcc.uma.es
For Finland: Hannu Kari, HUT, kari@tcs.hut.fi
to be added, please report your interest

> Spelling:
British English is used except for US contributions

Editoral

US Contribution

European Activities

Country Specific Issues

Method and Models

About Associations

Books on C(I)IP

CRITIS 2013 Conference

Links

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 not 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 not 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 optimsed 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 Luiijf

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

e-mail: **eric.luiijf@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

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

He is ECN Editor in Chief

CRITIS 2014

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

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

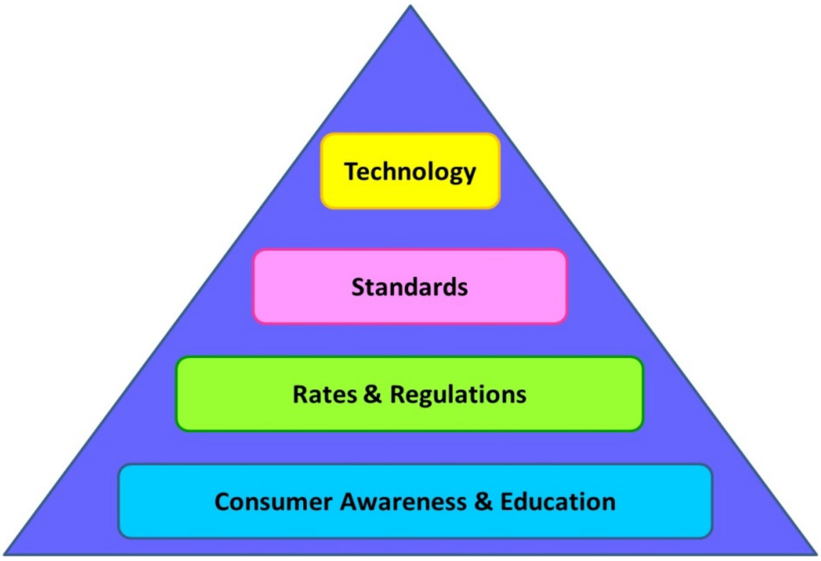


Fig. 1. Building blocks of the Smart Grid

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**

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

- 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 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.

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

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.

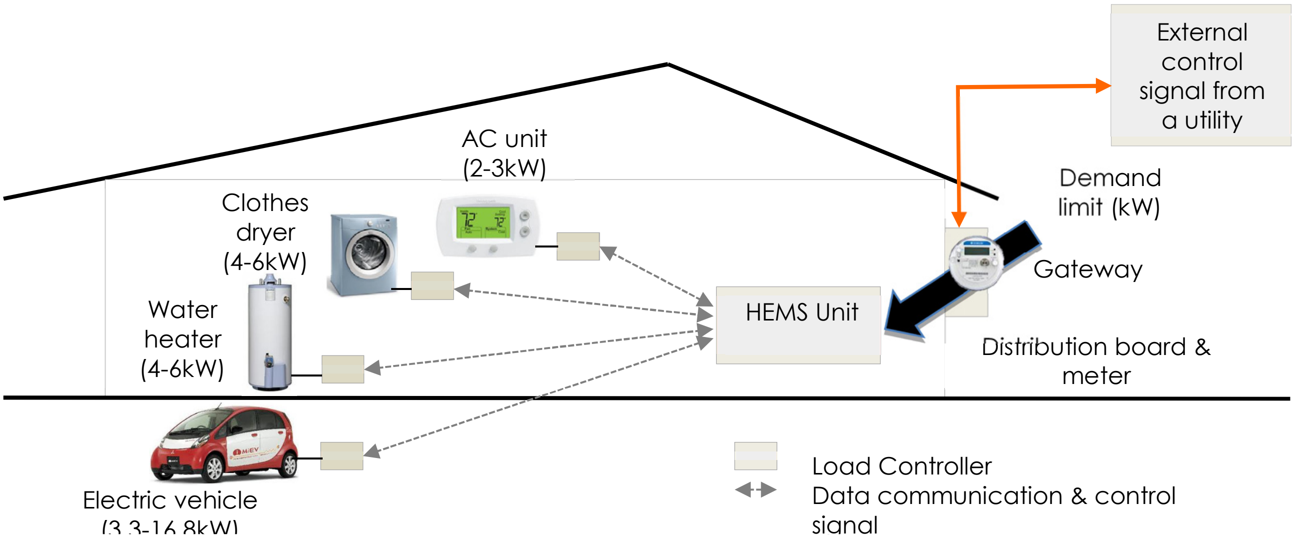

External control signal from a utility
AC unit (2-3kW)
Clothes dryer (4-6kW)
Demand limit (kW)
Gateway
HEMS Unit
Water heater (4-6kW)
Distribution board & meter
Electric vehicle (3.3-16.8kW)
Load Controller
Data communication & control signal

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 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:

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

- 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

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**
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: **jlm@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).

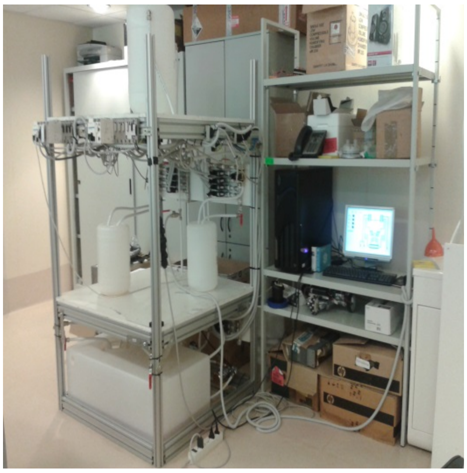


Fig. 1: Testbed for FACIES

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 values/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, Octr/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

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 been 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 stake-holders. 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.

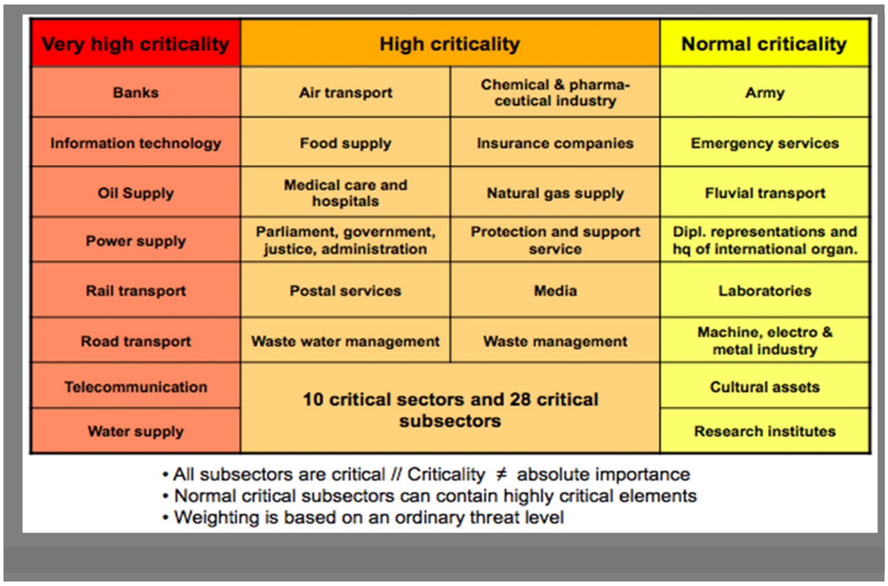
Short review of sub-sector criticality

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).



Very high criticality	High criticality		Normal criticality
Banks	Air transport	Chemical & pharma-ceutical 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

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**

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 or Email: 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**

Ir Thomas Bles

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

e-mail: **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**

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

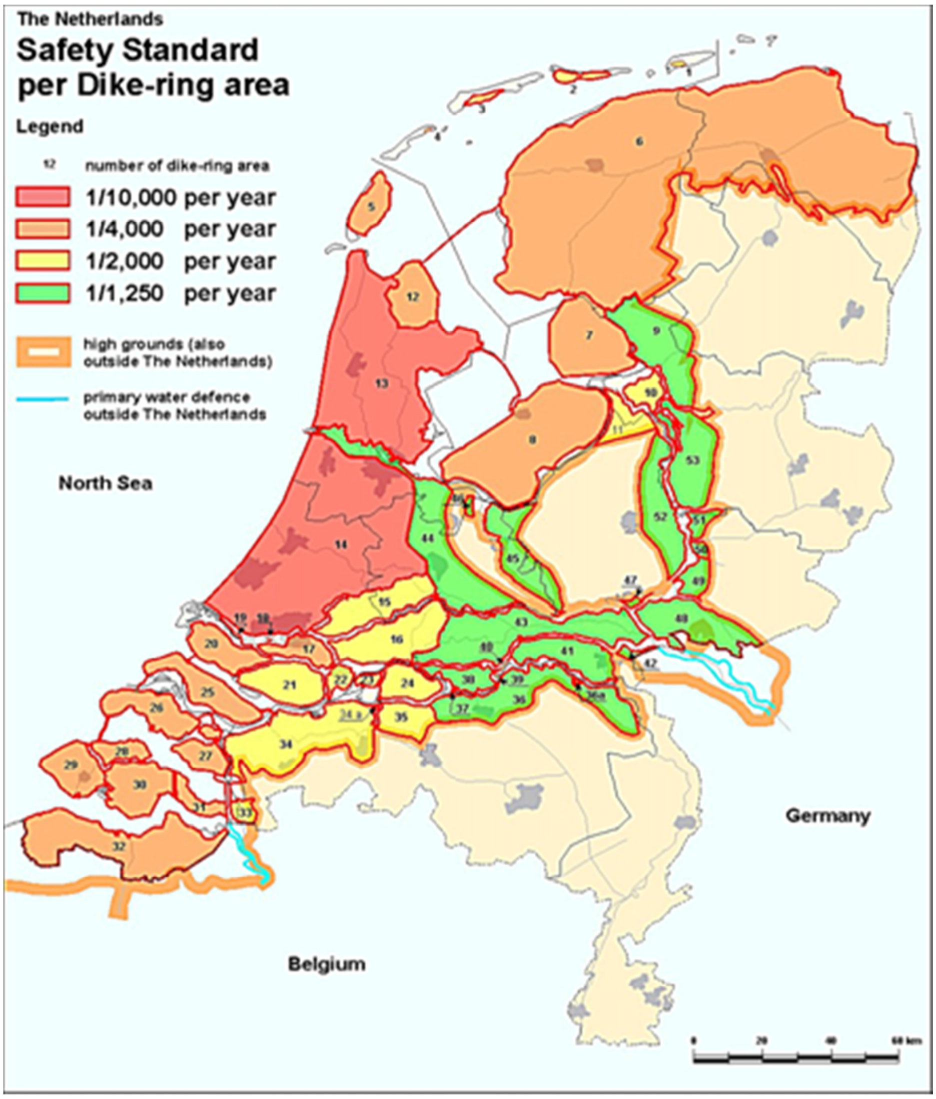

The Netherlands
Safety Standard per Dike-ring area
Legend
12 number of dike-ring area
1/10,000 per year
1/4,000 per year
1/2,000 per year
1/1,250 per year
high grounds (also outside The Netherlands)
primary water defence outside The Netherlands
North Sea
Germany
Belgium
0 20 40 60 km

Fig. 1: Protection levels / safety standards

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 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 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 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 Vlake tunnel (2011), the severe drought that hit the Netherlands (2011) and the failure of a NAFTA pipeline near the Juliana Channel dike (2013).

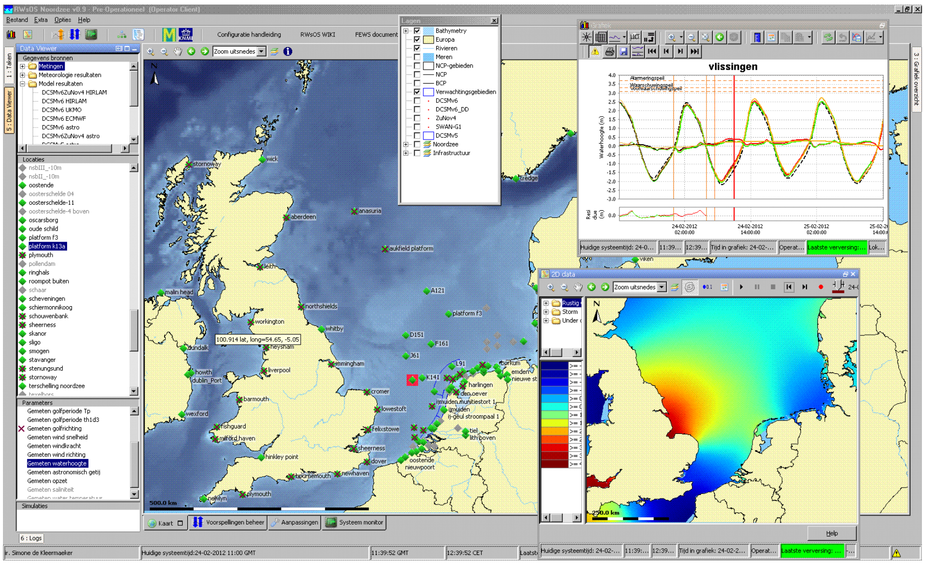


Fig. 2: North Sea forecasting system

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

(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 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.

> 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.

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**

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 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?

> 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).

The Norwegian approach of civil and military emergency preparedness cooperation

The Norwegian Government's policy on national emergency preparedness 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 inter-dependencies 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 FFIs research please visit our

website at www.ffi.no
email: 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).

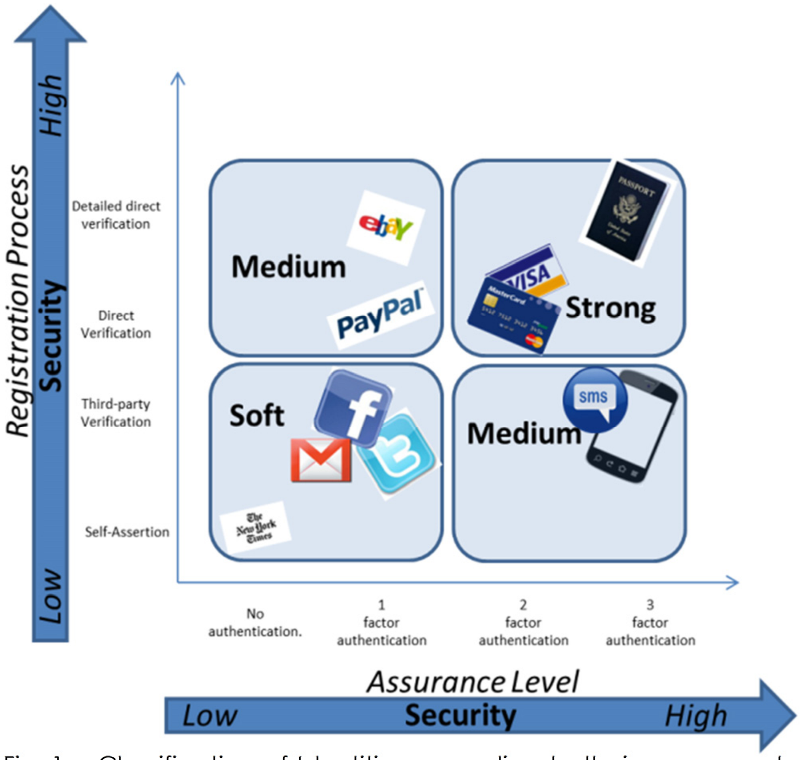


Fig. 1: Classification of Identities according to their assurance level and registration process

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**

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 specified 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 Simulation 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 CIPRNet (Critical Infrastructures Preparedness and Resilience Research Network, see www.ciprnet.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

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

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 Universitè 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 Sacaly (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**

mating the consequences that the loss of the E_x 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.

$$V(E_x,T) = V(E_x, pos(E_x), T, S(T)) \qquad (2)$$

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 E_x 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).

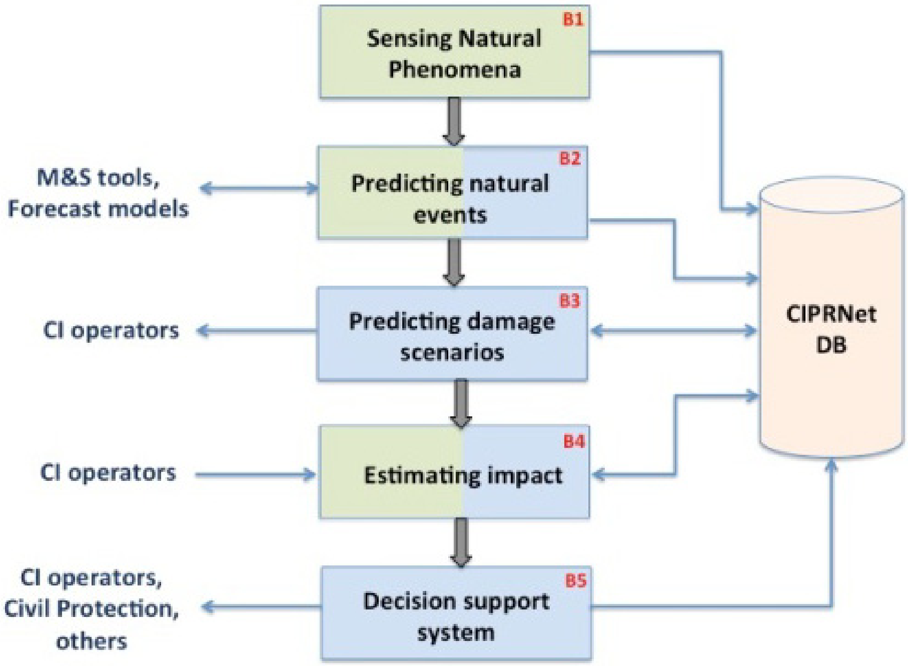

B1
Sensing Natural Phenomena
B2
Predicting natural events
M&S tools, Forecast models
B3
Predicting damage scenarios
CI operators
B4
Estimating impact
CI operators
B5
Decision support system
CI operators, Civil Protection, others
CIPRNet DB

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

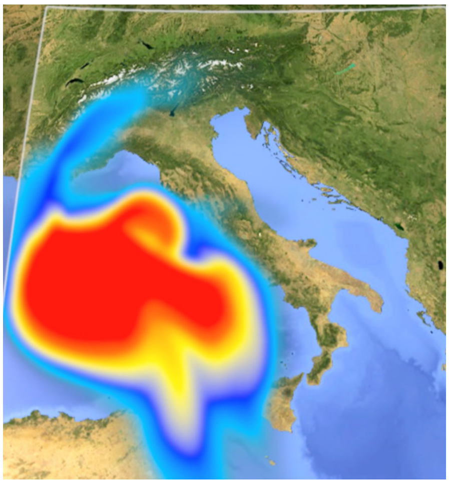
Four different phases are visible in fig.1. In the first (the first term in the right-hand side of eq. (1)), the system collects information from the field (through proximal or remote sensors) and from weather forecast (medium-long term, as weather forecast and short-term by now casting equipment). High 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

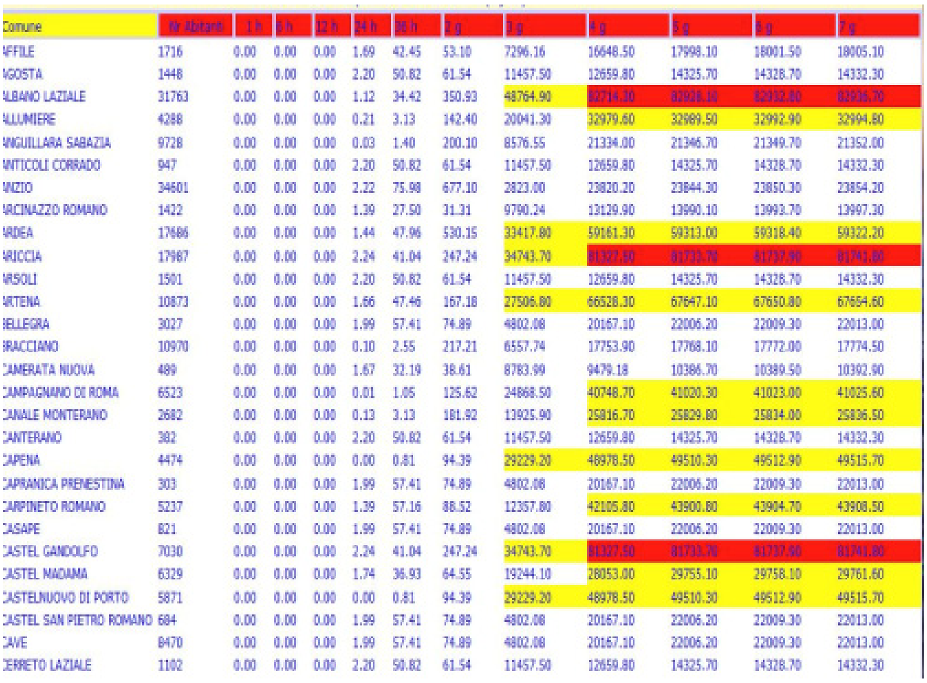
At this stage, the third phase of the workflow will start. The DSS system will gather the information from the CI operators and, by using specific tools accounting for system's functional dependences (or interdependencies) will evaluate the overall impact of the predicted damages on the whole system 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	Nr Abitanti	1 h	6 h	12 h	24 h	36 h	2 g	3 g	4 g	5 g	6 g	7 g
AFFILE	1716	0.00	0.00	0.00	1.69	42.45	53.10	7296.16	16648.50	17998.10	18001.50	18005.10
AGOSTA	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	48764.90	82714.30	82928.10	82932.80	82936.70
ALLUMIERE	4288	0.00	0.00	0.00	0.21	3.13	142.40	20041.30	32979.60	32989.50	32992.90	32994.80
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
ARCINAZZO 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	59161.30	59313.00	59318.40	59322.20
ARICCIA	17987	0.00	0.00	0.00	2.24	41.04	247.24	34743.70	81327.50	81733.70	81737.90	81741.80
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	27506.80	66528.30	67647.10	67650.80	67654.60
BELLEGRA	3027	0.00	0.00	0.00	1.99	57.41	74.89	4802.08	20167.10	22006.20	22009.30	22013.00
BRACCIANO	10970	0.00	0.00	0.00	0.10	2.55	217.21	6557.74	17753.90	17768.10	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	25829.80	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	43900.80	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	81327.50	81733.70	81737.90	81741.80
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
CERRETO 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 l 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.

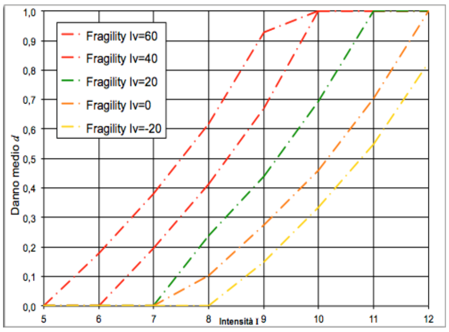


Fig. 3: Expected damage (y axis, empirical scale where 0 is undamaged and 1 has the complete destruction) as a function of the seismic intensity (as evaluated from shake map analysis) for different buildings of different Fragility indices Iv (Iv depends on building types, ages, height etc.). Iv can be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

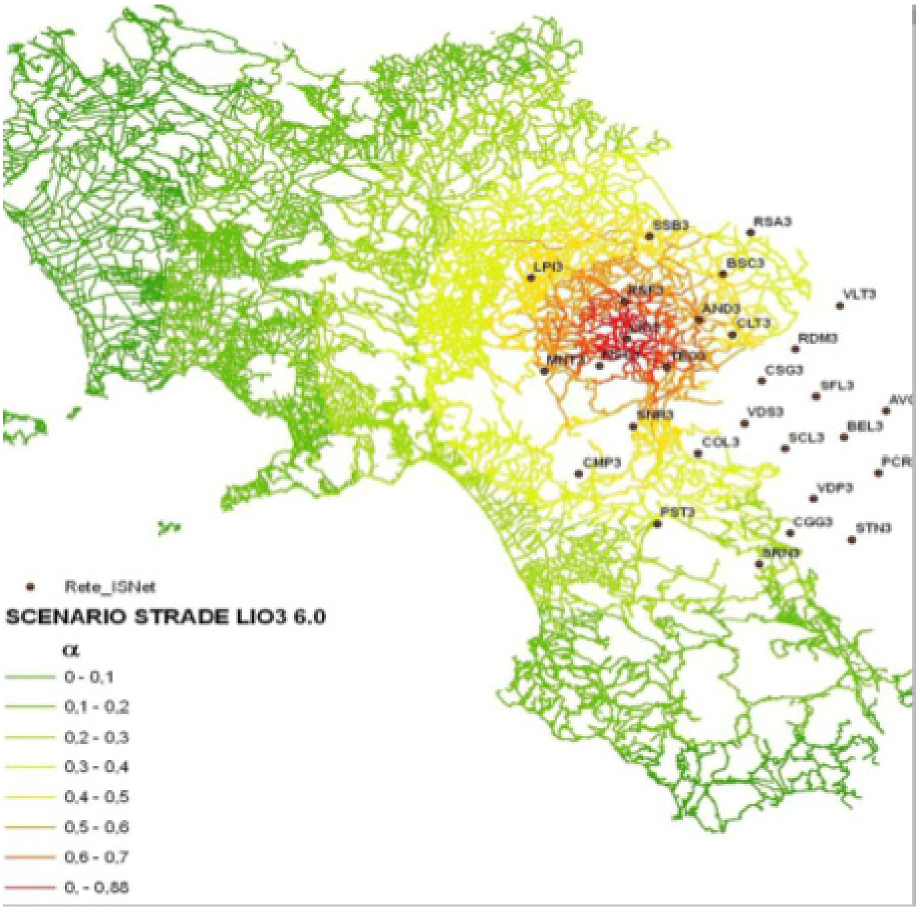


Fig. 4: Expected damages on roads and motorways after the simulation of a (synthetic) earthquake of M=6.0 in the region close to Naples (Italy)

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, 23rd 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**

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 Dambovita 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 QIEDM. This is a certification of **Q**ualifications in **I**nternational **E**mergency and **D**isaster **M**anagement

The concept requirements are:

- Candidates need to have sufficient background education and practise in emergency and disaster management
- The QIEDM 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 QIEDM 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 web-site 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

or send an email to TIEMS Secretariat:

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 in1983. 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.

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), which provides researchers and practitioners with an opportunity to present their most recent work. TC-11also 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

Yuko Murayama

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

e-mail: **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

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 a 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 Luiijf

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

Local co-chair CRITIS 2013.

e-mail: **eric.luiijf@tno.nl**

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 Spinger 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

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	12.-13.2.2014	London, UK
CRITIS 2014	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	12.-13.2.2014	London, UK

Associations

International Federation for Information Processing:	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
FP7 ValueSec	www.valuesec.eu
HIPOW	www.hipow-project.eu/hipow
ELITE	www.elite-eu.org
TWOBIAS	http://twobias.com
PRACTICE	http://practice.fp7security.eu
ERNCIP	http://ipsc.jrc.ec.europa.eu/index.php/ERNCIP/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

European Network and Information Security Agency 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

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

Swiss Infrastructure Protection: www.infraprotection.ch

Collection of Smart Grid related publications: 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

CRITIS 2014

9th International Conference on
Critical Information Infrastructures Security
October 8-10, 2014, Limassol, Cyprus
www.critis2014.org