FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013 Duration: 48 months

D8.518 European CIIP Newsletter issues 19–22

Due date of deliverable: 31/10/2015
Actual submission date: 21/10/2015

Revision: Draft version 1

ACRIS GmbH (ACRIS)

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

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

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

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

TABLE OF CONTENTS

1 Introduction – Rationale of this document

This deliverable contains the bundled issues 19, 20, 21 and 22 of the European CIIP Newsletter (ECN). All issues so far have also been published on the CIPRNet website and distributed via the CIPRNet consortium's mailing lists. Issue 22 has been printed and distributed at the CRITIS 2015 conference in Berlin, 5.-7.10.2015.

2 References

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

Appendix: ECN issues 19 (Vol. 8, No. 3), 20 (Vol. 9, No. 1), 21 (Vol. 9, No. 2) and 22 (Vol. 9, No. 3)

European CIIP Newsletter

November 14 – February 15, Volume 8, Number 3

ECN

Contents

CIPR Net

>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

>Spelling:
British English is used except for US contributions

Editoral

European Activities

Country Specific Issues

Method and Models

About Associations

Conferences 2014

Books on C(I)IP

Links

Editorial: Fostering young CIP Talents and Providing CIP Expertise to the Community?

The CIPRNet Young CRITIS Award (CYCA) for outstanding research in Critical Infrastructure Security sponsored by EU FP7 NoE CIPRNet.

Critical Infrastructure Protection (CIP) is a rather recent research topic which began at the end of '90 and gained momentum after 9/11 and the big blackout in the USA of 2003.

The interest regarding CIP has grown during the previous decades and there are now more than nine million webpages dedicated to CIP and an estimated 19.000 scientific publications.

This has contributed to create a CIP community with magazines (e.g., the Elsevier International Journal of Critical Infrastructure Protections (**IJCIP**) and Inderscience International Journal of Critical Infrastructures (**IJCIS**), just to cite the two most relevant) and conferences such as **IFIP WG 11.10** (International Conference on Critical Infrastructure Protection) and, especially, **CRITIS** (International Conference on Critical Information Infrastructures Security).

A large part of the components of the CIP community have very heterogeneous backgrounds. Indeed, there are researchers with experience in computer science, control theory, physics, electrical engineering, telecommunications, et cetera.

The main goal of these pioneering years of work has been to better understand CIP challenges and to recognise its framework. This has been done providing ontological definition of dependencies and interdependencies, cyber-physical systems, all-hazard paradigm, etc.

In other terms, in the past we have been looking to identify the "right" QUESTIONS, now it is time starting to provide ANSWERS.

An important part of this equation is to delegate young researchers to exploit their imagination, innovation, vision and ideas.

Luckily, in the recent years we have witnessed several young researchers complete their PhD on CIP and are now ready to provide their valuable contributions to the CIP community.

With the aim to specifically facilitate the inclusion of young and innovative research ideas into the CIP community, we arranged the ***CIPRNet Young CRITIS Award*** (CYCA).

The final stage of the first edition of this award, funded by the EU FP7 Network of Excellence (NoE) **CIPRNet** (Critical Infrastructure Preparedness and Resilience Research Network - www.ciprnet.eu), will be hosted during the 9 th edition of CRITIS in Cyprus, 13-15 October, 2014.

There, inside a special session, the top five candidate papers will be presented by the young authors and evaluated by the CYCA committee and by CRITIS attendees to select the best paper.

To facilitate the knowledge of young CIP talents to the community, the award is based on the soundness and innovativeness of the paper as well as the quality of the presentation.

The first edition will have ten candidates apply for the CYCA award from seven countries. Notice that even if CIPRNet sponsors the award, the large part of the candidature is outside the NoE.

We plan to announce this award also for the 10th and 11th editions of CRITIS in 2015 and 2016 respectively. Therefore, all young researchers are encouraged to apply for the next editions.

Enjoy reading this issue of the ECN!

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

Roberto Setola

Roberto Setola is professor at University Bio-Medico, Rome and head COSERITY Lab (Complex Systems & Security Lab) and director of the Post Graduate program in Homeland Security.

Email: **r.setola@unicampus.it**

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH

e-mail: **bmhaemmerli@acris.ch**
He is ECN Editor in Chief

(This page is intentionally left blank)

Securing Infrastructures & Services in Europe

ENISA role in protecting European Citizens.

ENISA, the European Union Agency for Network and Information Security, was set up to enhance the capability of the European Union, the Member States and the business community to prevent, address and respond to network and information security problems.

In order to achieve this goal, ENISA, acting as a Centre of Expertise in Network and Information Security, is stimulating the cooperation between the public and private sectors. Helping the Member States and the private sector to secure infrastructure and services is one of the main activities of the Agency, an area at the cross road between private and public domains which directly impacts the life of millions of European citizens. Indeed Critical Information Infrastructures are exposed to risks with repercussions for public welfare and economic stability. The EU Member States have committed to protect critical ICT systems according to the recent EU Cyber Security strategy.

Official Communications from the European Commission have highlighted the importance of network and information security and resilience for the creation of a single European information space. They have stressed the importance of dialogue, partnership and the empowerment of all stakeholders to properly address these threats. Fully recognising this need, ENISA is engaged in several activities with the ultimate objective of collectively evaluating and improving the resilience of networks and services in Europe.

For 2014, ENISA activities and tasks cover the entire spectrum of security issues that can be encountered in securing Infrastructures and Services in Europe, specifically:

- Identifying technological evolution, risks and challenges;
- Supporting Member States' capacity building;
- Supporting private sector capacity building.

In the following text, we present a summary of important areas / activities, for each area within the 2013 results as well as the projects running in 2014.

Threat Landscape

ENISA reports on important changes in the evolving threat situation in the ENISA Threat Landscape document (https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape). The primary goal of this publication is to cover current threats and threat trends in a number of technology areas. This work is based on open source information: ENISA collects publicly available reports, analyses them and consolidates their content in order to identify top cyber-threats.

The assessed top threats make up the current threat landscape. By looking at developments, predictions and trends in emerging technology areas, ENISA issues threat trends. This material is accompanied by a summary on threat agents, including groups, motives, and capabilities of adversaries launching cyber-attacks.

The ENISA Threat Landscape [ETL] is not solely a report. Rather, the report is the outcome of a process: through this process ENISA performs collection, issues statements regarding key events in cyber-security, and injects knowledge on threats to other projects.

Evangelos Ouzounis

Dr. Ouzounis is the head of ENISA's Secure Infrastructure and Services Unit.

Prior to his position at ENISA, Dr. Ouzounis worked several years at the European Commission, DG Information Society and Media (DG INFSO). He contributed significantly to EU Commission's R&D strategy and policies on securing Europe's infrastructures and services.

Rossella Mattioli

is Security and Resilience of Communication Networks Officer in ENISA and focuses on security and resilience of Internet and Critical Information Infrastructures in Europe.

Rossella.Mattioli@enisa.europa.eu

In addition to the publication of the ENISA Threat Landscape 2013 ENISA has also collected information on cyber-threats and cyber-risk, has published three flash notes, issued a mid-year threat report, and produced smart grid specific threat assessment. Lessons learned and conclusions drawn help streamline activities in the stakeholder community. ENISA will capitalise on this knowledge and will use it to support the activities of forthcoming ENISA Work Programs.

In 2014, this work continues with the global threat landscape and two in depth studies: one regards the physical and logical layer of the Internet Infrastructure, and one regarding Smart Homes.

Electronic communications

The 2009 reform of the EU Regulatory Framework for electronic communications added Article 13a to the Framework Directive. Article 13a requires operators to take technical and organisational measures to manage the risk posed to the security of networks and services, as well as to report security incidents to competent National Regulatory Authorities (NRA). Article 13a also asks NRA to send a summary report to the European Commission and ENISA, once per year.

In 2010, ENISA formed an expert group to work together with NRA to achieve a harmonised implementation of Article 13a across the EU and to establish a process for reporting incidents to the European Commission and ENISA. In 2011, the Article 13a Expert Group agreed on two technical guidelines, a Technical Guideline for Minimum Security Measures http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures and a Technical Guideline on Reporting Incidents http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting. In 2012, NRA reported for the first time about security incidents to the European Commission and ENISA, and later that year ENISA published a first summary and aggregate analysis of the reported incidents.

In spring 2013, NRA reported for the second time about security incidents to the European Commission and ENISA. In September 2014 ENISA published the third annual summary report, which aggregates and analyses ninety reports about major telecom outages.

> Security and resilience of the Internet Infrastructure and Critical Information Infrastructures will become more and more important.

ENISA follows up on the annual reporting http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports by focusing on specific areas or topics where providers or regulators could make security improvements. In 2013, ENISA worked on two reports: a study on how national roaming could be used to mitigate large mobile network outages http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience and a study on how to mitigate power supply failures http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies.

Security and resilience of the electronic communications networks and services will become more and more important. Developments like the uptake of cloud computing and smartphones will increase the impact of security incidents in the telecommunication sector. Addressing and improving security of the electronic communication networks and services will remain a top-priority.

In 2013, the European Commission issued the cyber-security strategy for the EU and made a proposal for an EU directive on Network and Information Security (NIS). The NIS directive basically takes the model of Article 13a and extends it to other sectors in society. This means that the pioneering work done in the context of implementing Article 13a in the telecommunications sector will now become relevant beyond this sector. ENISA is actively engaging with the public and the private sector to build on the Article 13a work done so far in these areas.

Network Infrastructure

The Internet infrastructure is the backbone of the information society but as it is every day clearer, various threats, both technical and geopolitical, can hamper its availability. Citizens expect national authorities to be fully aware of the possible interdependencies and to put in place all possible measures to ensure the security and resilience of their communications. Member States need to cooperate more on cross-border (inter)dependencies; at the same time they need to secure and enhance the level of resilience of the infrastructure within their borders. In addition, a part of the electronic data communication networks is vital for Critical Infrastructures and in order to properly assess the criticality of specific assets and services, Member States should be able to develop an insight of the current infrastructure, the Critical Infrastructure (inter)dependencies and have a baseline for future development.

The goal of "Understanding the importance of the Internet Infrastructure in Europe" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks report was to help Member States to understand the importance of the infrastructure within their borders with particular attention to critical assets and cross-border (inter)dependencies and work

together with Internet operational actors to maintain the Internet globally coherent, secure and resilient. To pursue this goal, both the technical and organisational aspects were deepened and good practices were investigated. Based on the desktop research, survey and interviews, an initial step by step guide was proposed to understand the importance of the Internet infrastructure in each Member State. The goal was to provide a baseline of steps to understand the allocation of Internet resources at national level, correlate them to organisations that can be part of Critical Infrastructures and develop indicators regarding the overall security and resilience of the system in each country.

Moreover, considering the multi-stakeholder environment of the Internet, recommendations were developed for Member States, providers of critical services and European Internet operational actors. The goal was to foster infrastructure security and resilience not only for securing European citizens but also the entire Internet.

In 2014, ENISA will focus its efforts on:

- Focusing on the methodologies for the identification of Critical Information Infrastructure assets and services and infrastructure vulnerabilities related to data communication networks.
- Fostering the ENISA's Internet infrastructure security and resilience reference group.
- Developing a threat landscape of the physical and logical layers of the Internet infrastructure.

Cloud Computing

ENISA is involved in almost all European Commission activities implementing the Cloud Strategy. In this light ENISA has been supporting the Certification Selected Industry Group and in detail:

- ENISA published a paper summarising all activities of the SIG since its establishment, putting forward all the reasoning in favour of a common certification scheme for Europe https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy .

In parallel ENISA has been asked to support other activities of the strategy (even though not explicitly referred).

- ENISA is also participating and supporting the ETSI standardisation working group by actively joining in the WG meetings.
- In the Service Level Agreement Selected Industry Group, ENISA is requested to participate and offer technical support and expertise on several deliverables. The objective of this group is to create model terms for contracts between cloud providers and customers.

ENISA has setup an experts group with representatives from the private and public sectors, to exchange knowledge and information on the several studies on Cloud Security.

In 2014, ENISA will continue to support the Commission in the implementation of the EU Cloud Strategy. The Agency will also develop a meta-framework for cloud certification and a good practice guide for procuring cloud computing. Finally, ENISA will continue its efforts to promote its recommendations on governmental clouds.

ICS SCADA and Smart Grids

The cyber security strategy for the EU calls upon Member States, the industry, and ENISA to increase the level of NIS in critical sectors, and to support exchange of best-practices.

ENISA responded to this call by launching several activities on security of Industrial Control Systems and SCADA.

In the report "Can we learn from SCADA security Incidents? http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents set of recommendations are highlighted for developing a proactive environment and an appropriate level of preparedness with respect to ex post incident analysis and learning capability.

ENISA identified several key activities that can contribute to this goal:

- Facilitating the integration of cyber and physical response processes with a greater understanding of where digital evidence may be found and what would be the appropriate actions to preserve it.
- Designing and configuring systems in a way that enables digital evidence retention.
- Complementing the existing skills base with ex post analysis expertise and understanding overlaps between cyber and physical critical incident response teams.

In the White Paper "Window of exposure: A real problem for SCADA systems?" http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems ENISA argues that the EU Member States could proactively deploy patch management to enhance the security of SCADA systems. We have identified several best practices and recommendations regarding patching that can improve the security posture of SCADA environments, from which we would like to mention the following:

- Compensating Controls;
- Broadening defence-in -depth through network segmentation to create trusted zones that communicate using access controls.
- Hardening the SCADA systems by removing unnecessary features;
- Usage of techniques such as "Application White Listing" and "Deep Packet Inspection Patch

Management" program and service contract;
- Asset owners should also establish a patch management service contract to define the responsibilities of both the vendor and the customer in the patch management process;
- Asset owners should always conduct their own tests. This can be done virtually or by maintaining separate systems to test on;
- Certified systems should be re-certified after a patch is applied.

The objective of "Window of exposure: A real problem for SCADA systems?" is to explore how European Union actions can be coordinated so as to reach a level of harmonised, independent and trustworthy ICS testing capabilities, leveraging current initiatives.

This represents a step forward from ENISA's 2011 recommendation for ICS protection, offering guidance about how to design and operate these capacities, taking a broad perspective, including organisational, financial, and technical aspects.

The methodology included desktop research, an online survey and in-depth interviews with 27 experts from the European Union, the USA, Japan, India and Brazil.

In 2014, ENISA will focus its activities in the area of certification of Smart Grids components and systems, as well as skills certification of ICS NIS experts. Also the Agency will continue supporting DG ENER in the establishment of Minimum Security Measures for Smart Grids and the EU Smart Grid Strategy.

The Finance Industry

The evolution of the finance sector towards real time processing of transactions has profoundly changed its dependencies on the telecommunication sector, and impacted how banks, clearing houses, and authorities should apprehend ICT and information system security.

In 2013, ENISA performed a stock taking of the actual state of play in this domain, and the conclusions converge towards the need for a more coordinated, pan-European approach.

The findings of the study are as follows:

- Many different methods are in use for interbank e-communication;
- Security regulation is generally high level, and leaves the responsibility for defining and implementing specific control to the banks and their providers;
- Regulation mostly requires solely that communications must be adequately secured and specific (technical) security controls for interbank e-communications are rarely imposed.

In 2014, ENISA is continuing the work in the area and recently established the ENISA expert group in Finance Resilience & Network Information Security.

National Cyber Security Strategies (NCSS)

Given the complex nature of cyber security, the creation of national cyber security strategies to address issues of improving resilience, reducing cybercrime and developing cyber security capabilities of EU Member States is an acute need. In 2012, ENISA published a practical guide that identifies the most common elements and practices of National Cyber Security Strategies (NCSS) in EU and non-EU countries. In 2013, ENISA built up an information pool http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss and has been following the progress of deployment of cyber security strategies in the EU and across the globe.

Securing Europe's Infrastructure and services

ENISA covers a wide spectrum of security threats in its work. Specifically when it comes to the most important infrastructure and services for the European citizens, it focuses on the pillars of the information society.

Core to ENISA's approach is its role of facilitator of public and private partnerships and the work it is doing in following the global threat landscape.

For ENISA, it is essential to bridge the research community with the private and private sectors. Its mission is to achieve a high and effective level Network and Information Security within the European Union, develop a culture of security and awareness for the benefit of citizens, consumers, business and public sector organisations and help the European Commission, Member States and the business community to address, timely respond and especially to secure European Infrastructure and services.

2nd ERNCIP Operators' Workshop

Assessment, selection & deployment of technological security solutions.

On the 19-20th May 2014, the 2nd ERNCIP Operators' Workshop took place, at the JRC premises in Ispra, Italy. It was organised by the European Reference Network for Critical Infrastructure Protection (ERNCIP)[1]. This was the second workshop, following the 1st ERNCIP Operators' Workshop[1], held in Brussels on 12-13 September 2013.

ERNCIP Mission:

Foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities.

The ERNCIP project was setup by the Institute for the Protection and Security of the Citizen (IPSC) of the European Commission's Joint Research Centre (JRC) in 2009 under the mandate of the Directorate-General for Home Affairs, in the context of the European programme for critical infrastructure protection (EPCIP) and with the agreement of the Member States.

ERNCIP aims to provide a framework within which experimental facilities and laboratories can share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of Critical Infrastructures (CI) against all types of threats and hazards.

ERNCIP addresses several thematic areas, as identified by its sponsors, i.e. the European Commission and the Member States. The work is being undertaken by specific thematic working groups. A work programme is established by each thematic group (TG) and approved by the ERNCIP Office. Currently (September 2014), ERNCIP addresses eight thematic areas [2].

Workshop's Theme & Sessions

The work performed within the ERNCIP network aims to be a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services, which is a barrier for future development and market acceptance of security solutions.

Therefore, this year's workshop focused on the needs and practises of CI Operators regarding the assessment, selection and deployment of **technological security solutions**. The workshop gathered thirty-one professionals representing CI operators from several CI sectors - Energy, Information and Communication Technology (ICT), Transport and Water. The workshop facilitated the exchange among operators and sectors, and provided guidance for ERNCIP in its efforts to develop and leverage its role for the benefit of CI operators.

Marianthi Theocharidou

Marianthi Theocharidou works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), for the CIPRNet and ERNCIP projects.

email:
marianthi.theocharidou@jrc.ec.europa.eu

Carl-Johan Forsberg

Carl-Johan Forsberg works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), for the ERNCIP project.

email:
carl-johan.forsberg@jrc.ec.europa.eu

[1] The 1st ERNCIP Operators' workshop highlighted major operators' needs in terms of:

- Risk Assessment, Protection and Resilience
- Crisis management & Recovery
- Future Technological Challenges, Needs & Solutions

Lessons learnt were focused on the implication for testing of solutions and the relationship between cross-sector vs. sector-specific needs, and above all a strong need for more exchange among operators and sectors.
More info, available at: https://erncip-project.jrc.ec.europa.eu/networks/opworkshops

The workshop was structured into three closely linked sessions during which the operators interacted actively both in the flow of discussions and in the joint work on the questions posed by the three dedicated moderators (one for each session).

Each session was centred on a driving question:

- Session 1: What are today are challenges for operators regarding assessment, selection and deployment of technological security solutions? (moderator: Mr Klaus J Keus)
- Session 2: What tools are available for operators and how can these be best utilised in order to address the above challenges regarding the assessment, selection and deployment of technological security solutions? (moderator: Dr Carmine Rizzo)
- Session 3: How can the ERNCIP network help to address these challenges on an EU level? (moderator: Dr Alois J Sieber)

During Sessions 1 and 2 the operators were initially divided into three sector-specific working groups. The outcome of each working group was thereafter presented by a selected rapporteur (one of each working group) to all participants and followed by a discussion. This approach facilitated for discussion both on the sector level, but also on a horizontal level.

Session 3 addressed the outcomes from session 1 and 2 with a focus on ERNCIP's role and took place in the form of an open discussion among all participants. In addition, during session 3, 'green cards' were distributed to all participants on which they could openly express any topic or suggestion. These green cards were reviewed and taken into account after the workshop by the session moderators.

In the following section, we summarise the main outcomes of the work performed. For more detail, please consult the Workshop Report [3] compiled by the three moderators on:

https://erncip-project.jrc.ec.europa.eu/networks/opworkshops/32-2nd-erncip-operators-workshop-may-19th-and-20th-2014

General observations

While several challenges were identified as common to all sectors, recommendations coming from one sector need to be handled very carefully before applying them to other sectors. For example, the Energy sector requires a more **global** approach; the Transport sector focuses mainly on **safety** rather than security. In the ICT sector there is a strong need to secure the entire supply chain, down to the individual **component**. This is a main concern shared across sectors, as ICT has a direct impact on all other CI sectors. Despite such differences, there were several challenges which emerged commonly among the workgroups.

Harmonised EU Legislation

With regards to **legislation**, an overall framework of existing or upcoming laws and regulations — on national as well as European levels — would offer the basis for a qualified assessment and would support the operators in their decision-making process, with respect to security technological solutions. During the workshop this request was particularly well illustrated in the Transport sector. In this sector, a legislative framework would need to take into account interoperability and inter-modality and to cover different areas and sectors within transport. A more fragmented approach would not benefit the operators as intermodality is required when considering an overall intelligent transport scheme. The Energy sector also highlighted a need for a comprehensive inventory of current legislation due to the uncertainty caused by the lack of harmonised European or international legislation.

Procedures and legislation need to be harmonised on a European level in order to improve coordination both at the European and the global level. Harmonisation legislation is a pre-requisite to reach a common level of security-related requirements within a sector and at the same time provide for a fair financial burden for the operators' business.

Cross-sector approach

The current work performed within the ERNCIP project was presented to the operators. The operators highlighted that the existing thematic areas appear scattered and that a clear structure linking the thematic groups on the basis of sector importance and relevance is missing. As a result, operators encouraged ERNCIP to identify new thematic areas more related to the overall theme of Critical Infrastructure Protection (CIP). Moreover, the operators welcomed the idea of a process for establishing new thematic areas which also takes into account the input of CI operators.

The CI operators proposed that new thematic areas could address, topics like:

- Modelling, Simulation & Analysis (MS&A) of:
  - dependencies between CI;
  - security vulnerability identification, assessment & optimisation;
  - evaluation of security solutions, etcetera;
- Human factors and security culture; and
- The threat landscape in the energy sector, in particular the cybersecurity of smart grids and renewable energy.

> Politicians need strategy, management boards need regulations, and technicians need reference manuals for ... assessment, selection and deployment of technological security solutions.

Harmonised EU-wide Training & Certification

The workshop participants pointed out that EU-wide harmonised training for operators' staff does not exist, nor does a certification scheme for qualified CIP personnel. There is a need to support such efforts through

relevant professional education and training/ research budgets. The implementation of an EU-wide **security** certification of qualified staff was also requested. This would allow experts to work within different CI sectors throughout the EU, and make it easier for the owners of the CI to recruit staff.

The participating CI operators asked ERNCIP to facilitate the creation of such an EU-wide harmonised training scheme for CI operator staff. The training scheme should include training on realistic threat scenarios and vulnerabilities of CI, meaning that an **applied, hands-on approach** should be favoured.

Participants also underlined that the proposed training schemes should be addressed to senior staff (engineers as well as managers). At the same time the creation of **academic curricula** for CIP at an undergraduate and postgraduate level was requested. This request is in line with the obligations and mandate of the Academic Committee of ERNCIP. The ERNCIP Office is asked to keep both operators and academia informed and facilitate the exchange of ideas between these two stakeholder groups. This exchange could be an interesting topic to address in a future ERNCIP operators' workshop.

Also in terms of regulation **policies**, ERNCIP can help in communication among operators aiming at requesting DG Home Affairs to coordinate its CIP policy areas with those in other policy areas. It was stressed that at national levels politicians need strategy, management boards need regulations, and technicians need **reference manuals** for appropriate guidance on the assessment, selection and deployment of technological security solutions. There is also a need to create an EU-wide auditing scheme for operators of critical infrastructures, based on a harmonised methodology.

ERNCIP can also facilitate the efficient and effective bi-directional communication between operators and research bodies, and link the relevant stakeholders within the **standardisation** community to ensure standards are created rapidly and effectively.

Learning from experience

Information sharing regarding threats and vulnerabilities, as well as available/needed tools and instruments, is still a huge challenge because of a missing central reliable point of trust. For example, CI operators recommended the establishment of an EU database of **incidents**, which should be updated on a regular basis. Such a central tool (as a single point of reference) would allow operators to stay informed about potential threats in an effective and timely manner. This activity could also be combined with training programs.

In the same context, operators invited ERNCIP to launch a systematic assessment of **past events** like the earthquake in Haiti, Hurricane Katrina in New Orleans, the oil crisis in the Gulf coast of the United States and the tsunami damage to the Fukushima nuclear plant in Japan. The focus should be placed on cross-sector (inter)dependencies (e.g., between energy, communication, transportation, drinking water supply) and the identified cascade effects.

Information sharing regarding threats and vulnerabilities, as well as available/needed tools and instruments, is still a huge challenge because of a missing central reliable point of trust.

Participants followed an all-hazards approach, discussing various threats ranging from terrorist attacks to natural hazards ranging from high probability/low impact threats to low probability/high impact threats. It was underlined that the probability may be perceived as less important in comparison to the consequences of failures of components of complex systems or CI sectors. Hence guidance is requested regarding low probability but potentially high impact risk. In such **scenarios**, operators may ignore the risk of unavailability for critical services (e.g., lack of energy due to extreme space weather, which would result in an inability to manage water supply).

There was common agreement among participants that **exercises** on a national and EU-wide scale, based on common threat scenarios, would be needed. ERNCIP is invited to facilitate such exercises, as well as support the design of scenarios.

The need for **Modelling, Simulation & Analysis (MS&A)**, based on the assessment of past events and monitoring of threats to CI reported worldwide, was also reported. MS&A efforts could drive the development of scenarios to be used for analysing possible cascade effects.

Learning from research

Operators feel that there is not enough information available about **security** research **efforts** at EU or national level.

CI Operators need information about European and national research results, as well as ongoing research projects, in order to be aware of emerging technologies, validation results concerning existing technologies and gaps in innovation which need to be communicated to the managers of research programmes. It was felt that at best, only promotional project leaflets are available. In particular, operators would like to be informed about the research *results*, and how these can be exploited in order to increase security.

Participants invited ERNCIP to facilitate the production of this information and a dialogue between the managers of the research programmes and CI operators. By doing so, gaps and needs for further research can be established and the innovation process, the core of Horizon 2020, can be promoted.

Risk Assessment

A major challenge consists in **assessing risk**, as well as calculating or estimating related **costs**. Scenario-oriented approaches, related but not limited to risk assessment, would enable a more structured process, as would new models for risk and costs estimation. Financing and related investments are challenges which have a direct impact on the business, and hence also on competiveness.

A significant part of the discussion was related to the risk assessment of CI. Risk factors are not easily quantified, particularly if they concern rare probability events. CI-related risk **definition** and **assessment** have to be reconsidered to ensure that all those involved are speaking the same language (with reference to ISO 31000:2009 and ISO Guide 73: 2009).

Building a **comprehensive risk picture** for CIP should include both accidental and intentional threats, should cover a wide range of security-related objectives (namely availability and safety), should look at multiple dimensions (physical infrastructures, information, technical systems, organisational artefacts and people); and it should follow a scenario-oriented approach, which can assist the operators to perform comprehensive exercises.

New concepts for CIP

The operators underline the need to link security with existing safety efforts. More specifically, the transport sector working group presented the new concept of **'safeurity'**[2] as an example of a concept, being developed within the rail sector and aiming at the protection of infrastructures and operations of any kind.

ERNCIP's role

ERNCIP should build on the very positive feedback from this workshop (the second in a series) and launch a systematic outreach initiative to operators. This might include information meetings at national level facilitated by authorities in the Member States.

It is commonly agreed that it is difficult to validate models in a statistically significant approach. However, ERNCIP focuses on the testing of security solutions. Therefore it is recommended to use such models to disaggregate complex systems (which include security solutions) in order to identify components for testing and validation with subsequent aggregation of the results in order to validate the overall system.

This aspect relates to a further topic which has been discussed, namely the need to involve actively the ERNCIP **network of test facilities**. There is an urgent need to establish common test methodologies and test protocols for security solutions. (It should be noted that this is even part of the ERNCIP mission statement.) Perhaps a more suitable term could be evaluation of security solutions rather than testing. The ERNCIP office is invited to establish a dialogue with the laboratory network and operators of CIs to discuss such methodologies — not only in laboratories but also in the 'real field'. In such context, in particular, collaboration with ETSI (European Telecommunications Standards Institute) would be instrumental.

Acknowledgements

This article summarises the findings as presented by the moderators (Klaus Keus, Carmine Rizzo and Alois Sieber) and the ERNCIP Office in the official workshop report of the 2nd ERNCIP Operators' Workshop [3].

References

[1] ERNCIP, Joint Research Centre, European Commission, https://erncip-project.jrc.ec.europa.eu

[2] ERNCIP Thematic Groups, https://erncip-project.jrc.ec.europa.eu/networks/tgs

[3] K. Keus, C. Rizzo, A. J. Sieber, Second ERNCIP Operators Workshop, Workshop report, EUR 26858 EN, Publications Office of the European Union, 2014

[2] safeurity in this context means just the concept of this group and should not misunderstood as safeurity, a trademark for a product

ENISA: Certification in industrial environments

Incidents demonstrate that our SCADA and Industrial Control Systems (ICS) are really vulnerable and exploited. Discussing various measures ad debate on certification of technology and experts should stimulate security for next generation security.

Security certification schemes are scarce in industrial environments despite the growi ng number of cyber-attacks that affect what i s considered EU Memb er State Cri tical Information Infrastructure (CII). Many actions have been taken i n this direction in recent years, however, the community questions remain unanswered: Are the i ndustrial Control Systems (I CS) often used as part of Critical Infrastructures (CI) secure? How secure are they?

To date, i n the absence of EU approved standards, harmonised testing and correspondi ng certification schemes for ICS, answering these questi ons remains elusive.

Addressing this topic requires understanding the current challenges for security certification. This paper will address som e of these challenges; it will draw the conclusion that the identific ation of an implementation strategy whi ch delivers results in a coor dinated, balanced and cost-effective manner for society and i ndustry alike is needed.

The overall result of introducing a security certificate in ICS depends on the qualitative aspects of t he certificate. Quality-parameters of the security certificate should be defined and monitored. Discreet security certification requirements need to be classified accordingly as mandat ory and optional based on "cer tification zones" which are defi ned by mapping the consequences (t he dominant CII factor) wi th likelihood and risk. Best practices such as ATEX[3], IECEx [4], IEC61508 [5], GMP/GAMP [6], Common Criteria[7] and FIPS[8] need to be examined. Specific implementation points that can be "transferred" to the security certification from a technical and administration framework perspective need to be further identified.

Security certification calls for a holistic and human-centric approach. Security-certified CII systems and components need to be operated by competent organisations and personnel. Security certifications of plant organisations and key personnel should be used to set the minimum accepted level of security for industrial environments and can be further elaborated to m otivate incident reporting and pr oblem solving.

Adrian Pauna

Adrian Pauna is a NI S Expert at ENISA, working in the "Secure Infrastructure & Services" department. His main activity is related to the topics of ICS/SCADA security. In the previous years he managed several projects which finalised with a set of recommendations on the subject of patching, testing and ex-post analysis of SCADA systems. Previously working to ENISA, he was a member of the Romanian Governmental CERT, entity designated to prevent and respond to security incidents related to information and communication systems of the Special Telecommunication Service and its clients. He has a M aster in Information Security and followed several certification programs (CISSP, CEH, ISO27001:2005 Lead Auditor).

Email:
adrian.pauna@enisa.europa.eu

---

3 http://ec.europa.eu/enterprise/sectors/mechanical/atex/index_en.htm

4 http://www.iecex.com/docs/PCIC%20Europe%202010%20Pomme.pdf

5 http://www.iec.ch/functionalsafety/

6 http://www.ispe.org/glossary?term=Good+Automated+Manufacturing+Practice+%28GAMP%29

7 https://www.niap-ccevs.org/evolution/pps/index.cfm?&CFID=18039492&CFTOKEN=daccca7eec09357e-96F7BBA3-9102-80BA-3774A3C10DA9E20E

8 http://www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf

Certification Challenges

Threats and changes within the technology base used in industrial environments may have an impact on the installed ICS. The speed of reaction to those changes is indicative of the degree of resilience of the user community (in the European Union) against those changes. Subsequently a large number of challenges may crop up, examples of which are given hereunder.

ICT drives ICS product lifecycles resulting in the following challenges:

- Security certificates hinder the adoption of new ICT products and services for ICS innovation as certifications are based on standards which typically lag behind technological development.
- ICS manufacturers will have to maintain a stock of ICT components and follow-up on vulnerabilities even if the ICT manufacturer has discontinued support.
- Vulnerabilities in ICT components are found every day rendering "one-off" security certifications short lived.
- ICS component lifecycle becomes shorter and it does not facilitate the traditional long periods to amortize testing and certification costs.

High security certification setup costs, especially for ICS asset owners

Manufacturers take risks upfront when investing in ICS security certification, however, asset owners need to consider:

- more expensive certified ICS components and systems,
- own costs for organisation and personnel certifications,
- interacting with external certification bodies,
- acquiring new equipment such as test beds, and
- having to deal with scheduled production downtimes.

Obstacles based on mentality may delay the security certification process in ICS CII plants

The successful prevention of ICS security threats and the mitigation of ICS security hazards need ICT and ICS/Process experts to work closely together in order to prioritise measures like ICS security certification, see Figure 1. A typical example is found in CI plants, a Process Hazard Analysis (PHA), led by the ICS/Process personnel, needs to be conducted before the cyber security risk assessment; which in turn calls for IT staff leadership (stated also in the working draft of ISA/IEC 62443-3-29). Traditional barriers, knowledge gaps, misconceptions and the different approaches of Control/Automation and ICT staff hinder the communication and cooperation within the asset owner organisation.

Threat-oriented ICS security certification is volatile and uncertain

Hacker attack technique developments, future vulnerabilities and related risk are unpredictable, especially for high-availability systems with the long lifecycle turnover installations such as ICS in CI plants.

Most of ISA/IEC 62443 [8] parts are still under development and not harmonised.

ISA/IEC 62334 focuses on all ICS ecosystem certifiable objects (polices-procedures-system-component) and consists of thirteen distinct parts (standards)[10]. Two parts are currently

published, two other parts are published under review, while seven parts are still under development, and two parts are planned.

Process Hazard Analysis (PHA)

A **"hazard"** is a dangerous situation which can threaten life, health, property, or environment. Potential hazards associated with an industrial process are called "*process hazards*".[7] "**Process Hazard Analysis**" (**PHA**) is a set of organized and systematic assessments of the process hazards in order to improve safety and reduce the **consequences** of harmful **incidents** such as accidents, disrupts of business or community services, society emergencies or disasters. There exist various methods to conduct a PHA such as the Hazard and Operability Study (**HAZOP**) and the Layer of Protection Analysis (**LOPA**).[11]

Recommendations

ENISA concludes that strategies, guidelines and increased competences/skills are necessary to overcome the current challenges related to security certification in order to provide a transparent, balanced and efficient framework regarding the security of CI production plants. In the short-term, the Agency believes that the focus should be on the following:

[9] Zalatynskyi Vasyl Danger - a subjective evaluation of objective reality. Science & Military. – L. Mikulas, Slovak Republik. Armed Forces Academy of General Milan Rastislav Stefanik. No 1, Volume 8, 2013. P. 53-62 EV 2061/08, ISSN 1336-8885

[8] http://isa99.isa.org/Documents/Drafts/ISA-62443-3-2-WD.pdf

[10] http://isa99.isa.org/ISA99%20Wiki/Home.aspx

[11] http://en.wikipedia.org/wiki/Process_Hazard_Analysis

Manage volatility

Certifications – as understood today – have the disadvantage of being static. Once a "traditional" certificate is issued, it remains valid until expiration. The features of a traditional certificate can be applied in areas of "low volatility" e.g., organisational security (ISMS).

ICS component security has two legs: One leg "rests on the land of stability" of the production process and associated process hazards. The hazards normally do not change much over the lifetime of the ICS. The other leg rests in the "land of volatility" caused by technological progress and vulnerabilities, as well as threats evolving on an hourly rate.

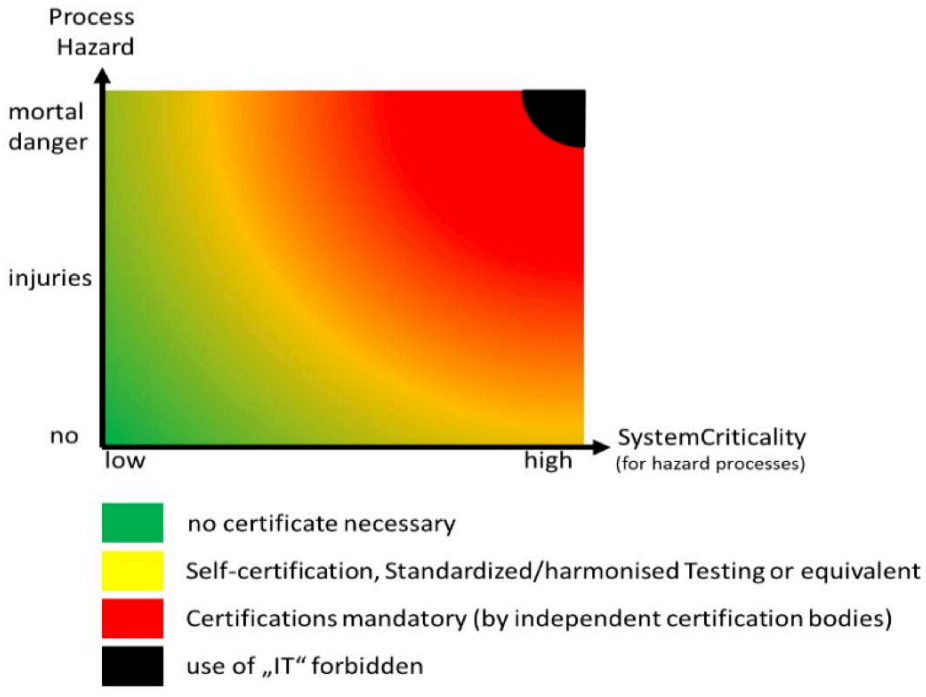
The ENISA recommendation is to certify aspects related to the known process hazards and manage volatility with dynamic certifications.

Focus on the content of certification

Due to their complexity, industrial environments need a certification scheme which covers the complete industrial supply chain to ensure a chain of trust, in other words all the above mentioned elements should be certified against different standards. ICS security certification may depend primarily on the outcome of the Process Hazard Analysis (PHA) taking into account two important factors: a) the costs and b) the criticality of each component which shall be determined by the risk assessment performed by the asset owner.

According to an ICS scheme, in general the following objects could be certified:

- Person
- Production or development of the product (Manufacturer, Integrator, Asset Owner)
- Component
- System



- Certifier

Fig. 1: Zone grouping of Objects for ICS Security Certification zone

Zone grouping of Objects for ICS Security Certification

The working draft of ISA/IEC 62443-3-2 states that: "The asset owner organization needs to determine the financial and health, safety and environmental (HSE) impact and assess the CI plant assets based on function, location and potential consequences. The purpose of the risk assessment is to develop a relative risk ranking of the cyber assets and group them into zones and conduits, in order to develop the appropriate security measures."

The grouping of cyber assets is recommended to follow the identified impact level in the PHA and not the vulnerability of the components. As per the colouring scheme, vulnerable components used in red zones need to be certified, while the certification of the same type of vulnerable component in the yellow zone may be optional. Portable and mobile devices that are temporarily connected to several zones should have the certification requirements that correspond to the highest risk zone.

As depicted in Figure 2, the ICS security certification requirements are prioritised based on the rightmost column and the "Damage Extent" of consequences. Components, systems, organisations and persons involved in the highest hazardous red zone(s) may have mandatory security certification requirements. In moderate hazardous yellow zone(s), security certification may take into account the threat likelihood, in a manner where certification is mandatory for high probability threats and optional for lower probability threats.

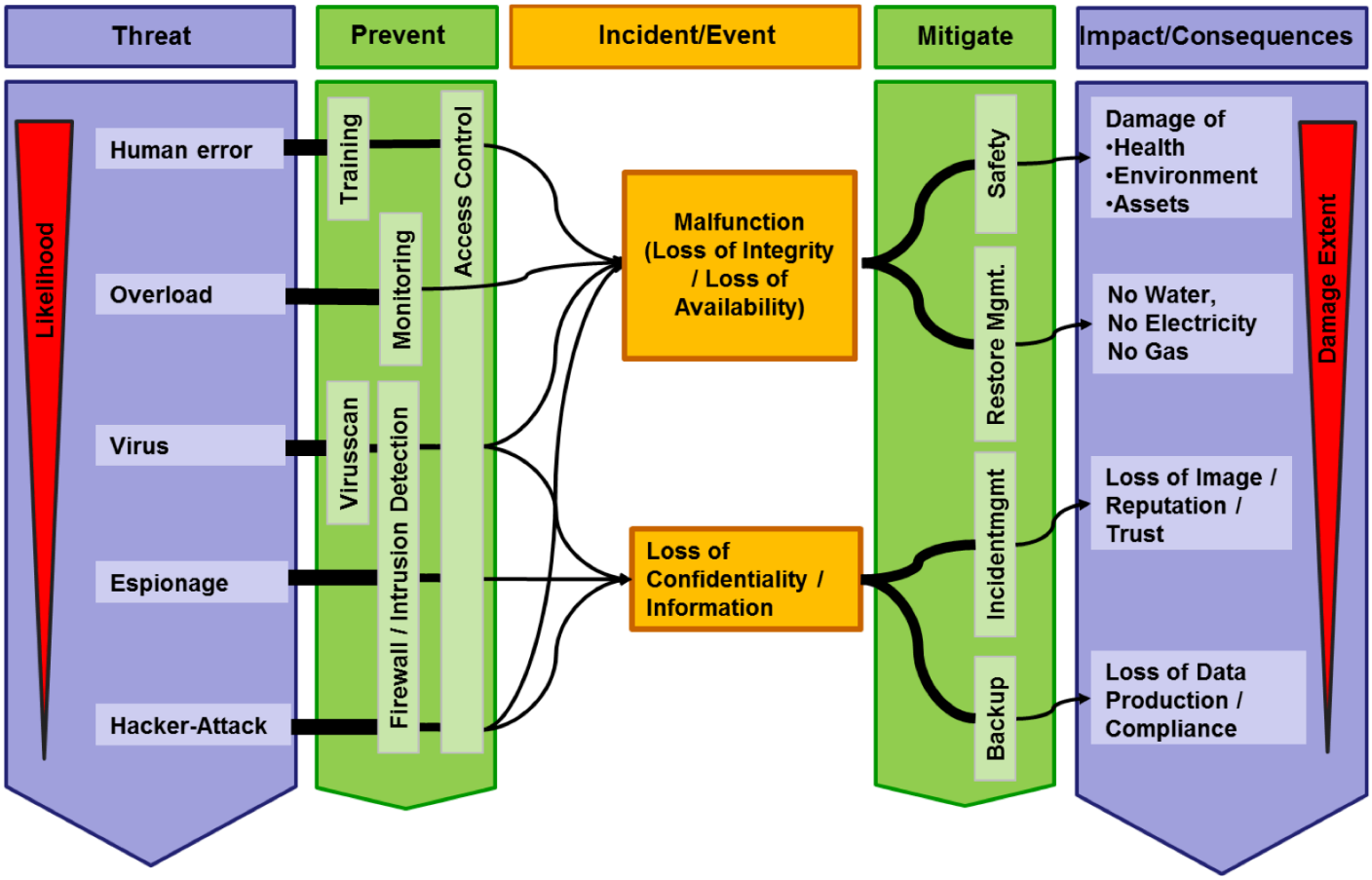


Fig. 2: ICS cybersecurity map

ENISA's 2014 activities on ICS

ENISA initiated a study on the "Certification of Cyber Security Skills of ICS SCADA experts" and the preliminary results were presented and discussed at the validation workshop organised in Heidelberg, Germany on the 30th of September: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components .

In order to strengthen the interaction with its stakeholders, ENISA has also set up an expert group that focuses on the subject matters and invites all the interested experts to join the EICS-SG expert group: https://resilience.enisa.europa.eu/ics-security

Conclusions

For many years SCADA systems were proprietary and isolated but the industry is experiencing massive changes as new network technologies are used. As a result, for the moment, there is no solution that fits all approaches to the security certification of industrial environments. A holistic approach to the problem is needed which covers all the different security levels which have been identified by carrying out a risk assessment with a view to tackle new cyber threats.

IT-Security – A new Challenge for Water and Wastewater Industry?

When discussing security of water supply and of waste water systems in general, we have to reflect what IT-Security means in terms of capacities, resilience, economy and surveillance. Which options should be implemented and which conditions have to be complied with? What is practicable?

Water and waste water servi ces are in general essential and deci sive for the health of the popul ation and the quality standard of l ife. They pr ovide the basis for a sound economy and good development of industry. Water as "Foodstuff Nr.1" is not substitutable, this means i n practice: "Without water no life". First aim , therefore to secure the pr ocesses, plants and resources of w ater and w aste water services.

Considering IT Risks

Water and w aste water services are typical "critical in frastructures" on local and regional level. German water law prescribes explicitly local water supply. Water and waste water services are not transboundary.

> Water and waste water services are typical "critical infrastructures" on local and regional level.

Because of the i mportance of water and waste water services for population and i ndustry in Germany high quality standards are set to protect the health of popul ation and secure water protection. In the last decades the use of advanced control technologies for w ater and waste water services has increased constantly. Risk management may be more and more insufficient looking "only" to the security o f water and waste water plants, netw orks, resources, and compensati ng measures. Even when unti l today many water and was te water services are still w orking without specialised computer aided systems, importance and pr otection of I T will attain more and mor e distinction according to their application.

The Water and Waste Water Sector in Germany

In Germany, water suppl y and waste water disposal are core duti es of public services in the general interest with the competence of munici-palities or other public corporations. In Germany t here are approximately **6065 water supply enterprises and utilities**. These enterpri ses are predominantly small ancillary municipal utilities and owner-operated municipal utilities. In the water supply sector, publ ic and private forms of or ganisation have co-existed for decades. In the w aste water sector there are in to tal more than **6900 waste water disposal utilities** in Germany. The undertaki ngs are predominantly operated by municipalities and owner -operated municipal utilities.

> The importance and protection of water and waste water IT will attain more and more distinction.

The most i mportant regulations for water and waste water i ndustries are the so called "W asserhaushaltsge-setz" and the regul ations of the Länder "Landeswassergesetze", which f.e. implemented the Water Frame Work Di rective, the so-cal led "Trinkwasserverordnung", which im-plemented the Dri nking Water Directive and the so cal led "Ab-wasserverordnung", which imple-mented the Urban Waste Water Treatment Directive into German law.

Michaela Schmitz

Dr. Michaela Schmitz is General Manager of Water Industry at BDEW German Association of Energy and Water Industries, Berlin, Germany and member of the committee "Implementation Plan for Critical Infrastructures - UP-KRITIS" of the German Federal Ministry of Interior.

e-mail: michaela.schmitz@bdew.de

Besides these regulations standardisation rules and minimum standards are established for technical processes of the water and waste water sector. Also security regulations for risk management and crisis management for the water and wastewater industry are established.

Structural and Quality aspects

After the big municipality reforms at the beginning of the seventies in the last century and the decentralisation after the German Reunification in the nineties the trend towards intercommunal cooperation of the water supply industry is growing on. The objectives of these intercommunal cooperations are increase in performance and efficiency and fulfilment of increased requirements towards quality of drinking water and consumer service. The number of water supply companies decreased since the sixties of the last century by more than 60%. Within the municipality reforms between 1967 and 1978 the number of water suppliers decreased from 15,286 to 7,323. After the German Reunification the Eastern German Länder started the process of municipality reforms as well. In some Länder this is still in process. Therefore, it is expected that the number of municipalities in Germany (Spring 2003: more than 13000; October 2006: 12,315) will continue to decrease. After the reunification the unbundling of the water and wastewater units, the so called "Kombinate" in the former DDR, initially caused a slight increase in the number of water suppliers to 6,709. Intercommunal cooperation, however, decreased the number of water suppliers until 2010 to 6,065. (Fig. 1)

Germany is a water-rich country. Public water supply utilises only about 2.7% of the available water resources of 5.1 billion m³. In total only 21% of the renewable water resources in Germany are utilised by all users. (Fig. 2)

Long-term nationwide protection of all waters is a national duty to which water supply and waste water disposal utilities make a substantial contribution. The geological, hydrological and hydro-chemical conditions within the different regions lead to large differences in availability and quality. In a highly industrialised and densely populated country like Germany with areas of intensive agricultural use and chemical production, water resources are subject to a wide variety of utilisation requirements and major pollution. Nationwide protection of water bodies is a matter for the Federal Government. In Germany targets were set to ensure a good status of water bodies according to the European Framework Water Directive (WRRL).

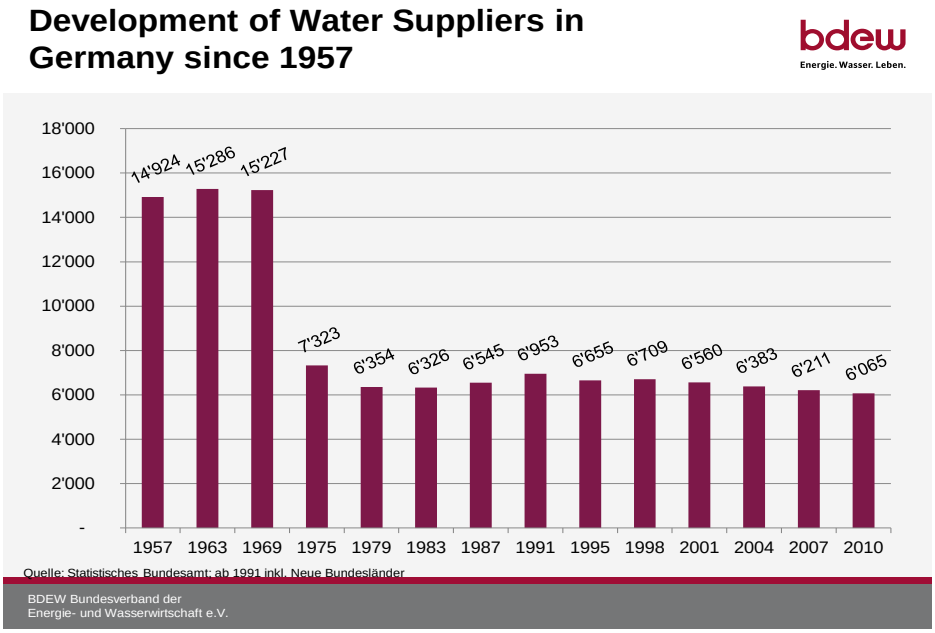


Fig. 1: from 1957 ongoing: Germany's water supply

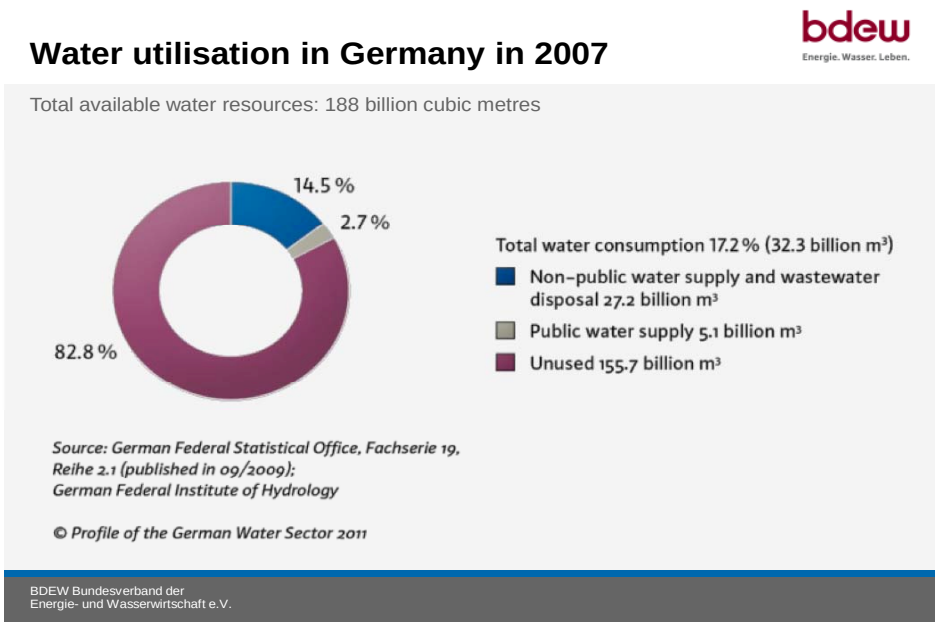


Fig. 2: Water utilisation2007 in Germany

Consumers in Germany are careful with drinking water. A comparison between six European countries shows that the German per capita consumption is lower than in other long-standing EU Member States. Since 1990 water consumption has decreased considerably and continues to decline. Demographic and climate change together with the continuously decreasing water consumption pose great challenges to the German sector. Uniform solutions cannot be adopted due to regional and local differences in impact. (See Figure 3 & 4, next page)

In Germany the degree of connection to the public water supply is

above 99% and thus on a very high level. Drinking water is of excellent quality in Germany. It is available to the population at all times in sufficient quantities. This is the main result of the third report of the Federal Ministry of Health and the Environmental Agency of the quality to the consumers looking to the years 2008 and 2010. Another important indicator of the quality of mains and safety of supply are the low water losses in the public drinking water network. Water losses in Germany continue to decline and are low in comparison with other EU-countries. (See Figure 5)

The population`s share in waste water treated according to the highest EU-standard has increased to 97% at the present time. With a connection degree of 96% to sewage networks and waste water treatment plants Germany holds a top position in comparison to other European countries. (See Figure 6, next page))

Since 1997, the rate of mains failures has decreased to 9. 9 incidents per year and per 100 km of network length. This means a very low rate of damage compared with other European countries (England and Wales 18.7, Scotland 16.6) with a tendency to decrease further. There have been huge improvements particularly in the new German "Bundesländer" since reunification.

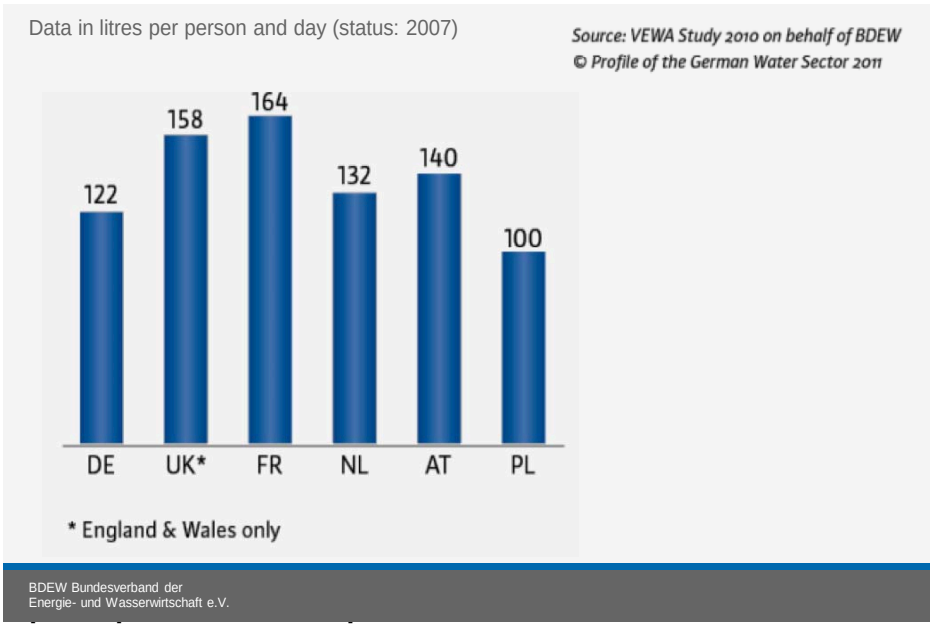
Cost recovery for the water sector is stipulated in Germany by the Local Rates Acts of the German Länder and by the Water Framework Directive at EU level. Cost recovery has been implemented in Germany and is a legal obligation.

IT-Security: National and European Legislation in Progress

The German Government has announced that it will present an IT-security-regulation in 2014. Focal point of this law is explicitly the protection of critical infrastructures including the general services like energy, water supply and waste water disposal. Purpose of this new

Figure 3: Comparison of per-capita water consumption on a European level

bdew
Energie. Wasser. Leben.



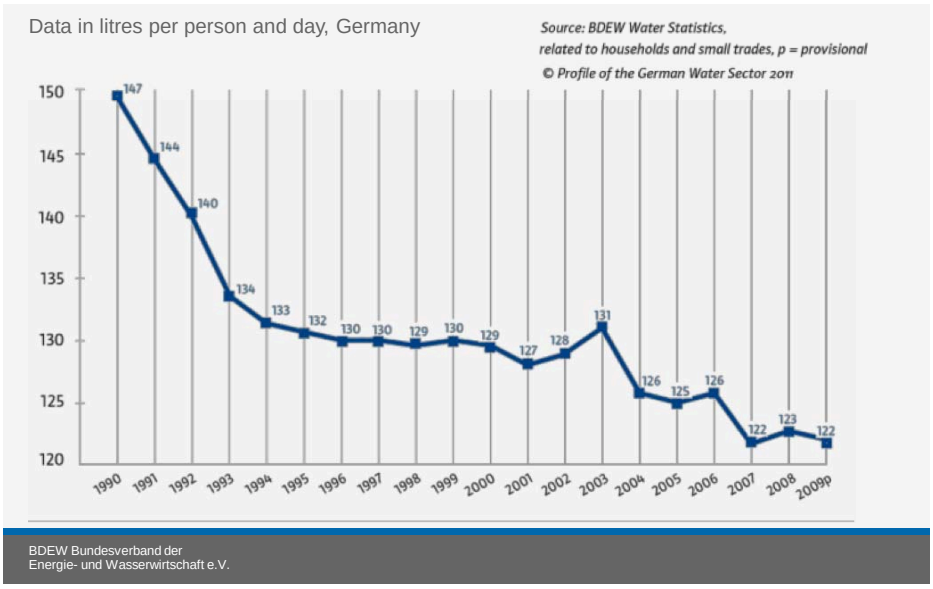
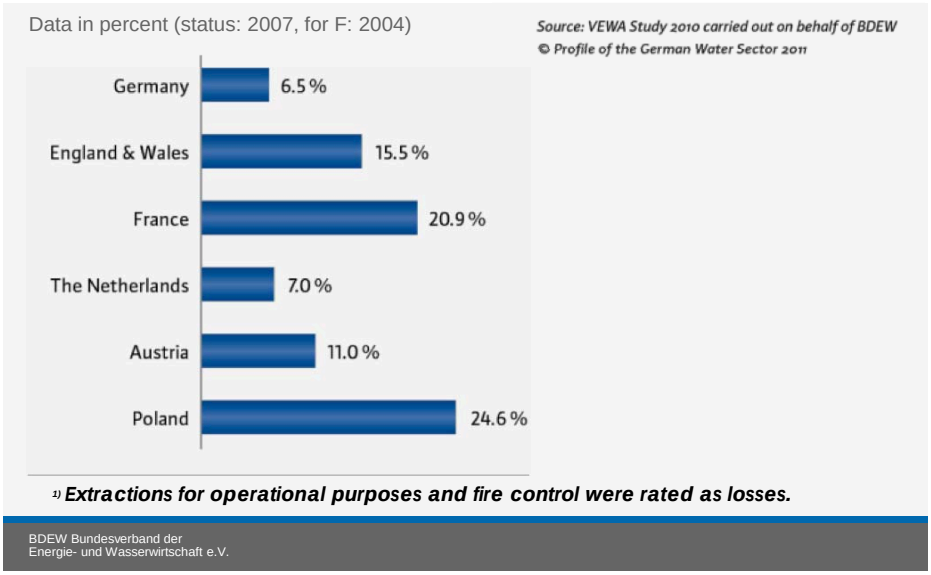


Figure 5: Water losses in the public drinking water network[1]: most important indicator of network quality and safety of supply

bdew
Energie. Wasser. Leben.



[1] *Extractions for operational purposes and fire control were rated as losses.*

regulation is the support of resilience of systems against cyber-attacks.

BDEW explicitly supports this IT-Security Initiative of the German Federal Government. In the frame of a first positioning to pre-proposals of an IT-security-regulation BDEW started this. The significance of functioning IT-security mechanisms is obvious to everybody nowadays when reading about data theft or by effects of hacker attacks. The technical competition of attack and defence of the security of IT-systems should be flanked by legal regulations. The existing optional regulations that were created by industry and public authorities commonly and were initiated by the Federal Ministry of Interior in its implementation plan KRITIS requires a binding legal foundation.

The main objectives of the planned legal regulation include the obligatory introduction of minimum standards and an obligation to report. The operators of critical infrastructures should develop IT-security measures according to the technical standard further on and guarantee their implementation. BDEW supports the development of IT minimum standards within the newly founded committee "Branchenarbeitskreis" for water and waste water of the German Federal Ministry of the Interior together with the German Association for Gas and Water (DVGW), the German Association for Water, Waste water and Waste (DWA) and the German Association of Municipal Industry (VKU). These minimum standards will complete the existing security regulations for risk management and crisis management for the water and waste water industry.

BDEW supports an IT step by step-plan within the sector of water and waste water according to the size and the technical systems of the companies. Fact is, that with regard to good raw and drinking water quality many water suppliers only need basic treatment techniques without complicated electrical and control technologies. Many processes can still be completed in a mechanical way nowadays.

Therefore, for small companies BDEW requires a general exception when missing digital systems.

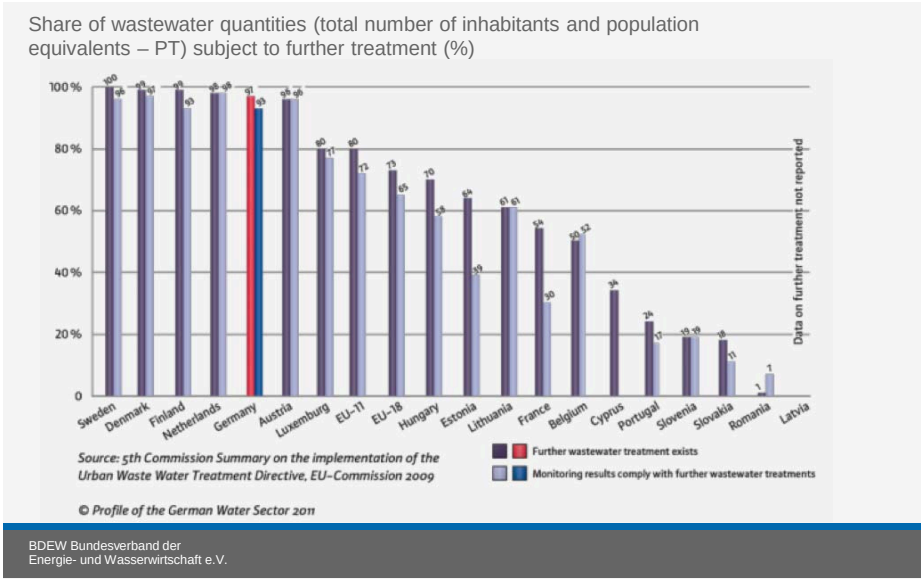
BDEW believes that the projected obligation to report should apply only to serious IT-security incidents with impacts to security of supply or public safety. BDEW also requires observance of existing obligations to report, with no approval of double-point information and extra bureaucracy. As technical IT-authority, institution for certification and approval of industry sector standards and for reporting of attacks on integrity of IT-systems the German Federal Agency for Security in Information Technology (BSI) is designated in the code law. BDEW explicitly approves of this dialog partner of the industry. However, BDEW disapproves of the SPOC (Server) as an external element to collect and forward data within the industry sector which was suggested in the first legal bill.

Parallel to the German national initiative the European Commission presented in 2013, the proposal "Regulation of the European Parliament and Council on actions to guarantee a high standard network and information security within the Union (COM (2013) 48 fin.)" which BDEW also acknowledged. The proposal of the so-cal led NIS-Directive also foresees the establishment of minimum standards, obligations to inform and reporting systems for water and waste water industries. BDEW points out that water and waste water services are national critical infrastructures and not transboundary active, therefore their inclusion within the NISDirective as European Critical Infrastructures should be examined. On these grounds BDEW disagrees with an inclusion of water and waste water in the NISDirective as European Critical Infrastructures. The draft Directive is under consideration and it is planned to pass legislation in 2015. BDEW watches the parallel developments of this legislation both on national and European level. Considering the proceeding development of both legal regulations BDEW believes it to be necessary to support the technical aspects on the one hand and to avoid national over-regulations and extra bureaucracy on the other hand.

References

BDEW, ATT, DBVW, DVGW, DWA, VKU: Profile of the German Water Sector 2011. BDEW: VEWA Study 2010.

Figure 6: Status of further wastewater treatment based on a comparison of EU countries



Intelligent network modeling in the electric power grid

As a result of the electricity evolution, the electricity infrastructure will get more and more inter-linked with network infrastructures. However, the same networking capabilities that can provide these benefits have also introduced vulnerabilities in the operational network. Intelligent control systems are an integral part of the critical infrastructures of power utilities.

Electric power system i s one of the most critical and st rategic infrastructures of in dustrial societies. Power utilities face the challenge of using information and commun-ication networks more effecti vely to manage the demand, generati on, transmission, and di stribution of their commodity services. The capabilities

> "This approach increases energy efficiency, reduce emissions, and transit to renewable energy."

of networking these systems provi de unprecedented opportunities to improve productivity, reduce impacts on the envi ronment, and hel p provide energy i ndependence. Communication network constitutes the core of the el ectric system auto-mation applications, the design of a cost-effective, and r eliable network architecture is c rucial. To resolve this difficulty we study the i ntegration of advanced artificial intelligence technology into existing netw ork management system.

Recent years have seen expl osive growth in the areas of power syst em monitoring using i ntelligent agents and distributed intelligence. This pro-ject differs from previous work because we present a techni que for the design and i mplementation of a security intelligent system that i s designed through the normal isation and integration of knowl edge management. We descr ibe an i n-telligent technique, which processes management knowledge collected by intelligent agents and uses i t to detect and to resol ve the network anomalies and secur ity faults. This work focuses on an intelligent frame-work and a l anguage for formalising knowledge management descr ipt-tions and co mbining them with exis-ting Open Systems I nterconnection (OSI) management model . The goal is the assi gnment and di spersed intelligent control of network resour-ces, pertaining to hardware as well as software, to hel p operators manage their security netw orks more effect-ively and also to promote reliability in network services.

Systems Management Overview

Telecommunication systems are essential elements to i mprove efficiency and economy i n energy operation, transmission, distribution, storage, and utilisation. There are two dominant network management models, which have been used to administration and contr ol the most of existing networks: Tel ecommunica-tions Management Network (TMN) and Simple Network Management Protocol (SNMP). In the public enviro-nment, a more heterogeneous mi x of de facto tel ecommunications indus-try standards has prevai led, with a move toward TMN support. TMN was the first who started, as part of i ts OSI program. OSI architecture for network management involves five major functional areas: fault, configuration, accounting, performance, and secu-rity management, which facilitate rapid and consi stent progress within each category's individual areas [1].

Antonio Martín

is Professor in the Electronic Technology at the Seville University in Spain, researcher and author. He has a Computer Science degree, and Ph.D. in Intelligence Artificial applied in Management Know-ledge. He also serves as editorial board member of several journals and conferences; guest editor for journal special issues; chair of conference tracks; and keynote speaker at conferences. His research interests encompass subject areas including data mining, intelligence artificial, knowledge management, software engineering, and expert systems. Professor Martín has published numerous articles in international journals and conference proceedings in these topics, in addition to two books on artificial intelligence and knowledge management.

mail: **toni@us.es**

According to the International Organization for Standardization (ISO), the OSI network management model defines a conceptual model for managing all communication concepts is the managed object (MO), which is an abstract view of a logical or physical resource to be managed in the network. MOs provide the necessary operations for the administration, monitoring and control of the telecommunications network. For a specific management system, the management process involved will take on one of two possible roles: the Manager Role is an element that provides information to users, and the entities within a network. This main Agent Role is part of a device in the network that monitors and maintains status about that device. MOs are defined according to the Guidelines for the Definition of Managed Objects (GDMO), which has been established as a means to describe logical or physical resources from a management point of view. The guidelines for the definition of managed objects, ITU-T Recommendation X.722, allow for a common data structure for MO in the managed and managing systems. GDMO uses an object-oriented approach to define the standardised functionality in substation devices [2]. A complete agent definition is a combination of a relationship between a managed object class (MOC), package, attribute, group of attributes, action, notification, parameter, connection of name, and behaviour. MOC is the base of the formal definition of an intelligent agent (IA).

Integration of Intelligent Agents

In a heterogeneous and distributed energy context, the application of IA to perform soft real-time control functions for the power grid is a way to introduce new information management techniques and information security functions to the power grid. An IA is an autonomous hardware/software system, which can react intelligently and flexibly on changing operating conditions and demands from the surrounding processes. IA can actively and dynamically cooperate for solving problems by using integrated knowledge and intelligence reasoning. IA required having knowledge management of its own local system and at least partial models of the global system [3]. For this to occur will be necessary to make changes on the templates of the GDMO standard.
We propose to extend the GDMO with the goal of facilitate the normalisation and integration of the knowledge base of expert system into resources specifications. We suggest a new description for the information management definition named GDMO+, which we add a new element named KNOW, as shown in figure 1. wo relationships are essential for the inclusion of knowledge in the component definition of the network: Managed Object Class and Package. These templates allow IA to have properties that provide normalised knowledge of a management dominion [4].

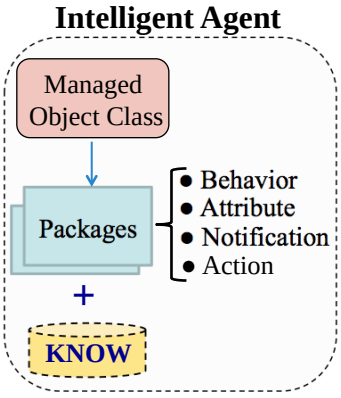


Fig. 1: Template relations in GDMO+ standard

The definition of a MOC is made uniformly in the standard template, eliminating the confusion that may result when different persons define objects of different forms. MOC structure is show here:

<IA-label> MOC
DERIVED FROM <IA-label> [,<IA-label>]*;]
[CHARACTERIZED BY
<IA_propert-label>[,<IA_propert-label>]*;]
[CONDITIONAL PACKAGES
<IA_propert-label> PRESENT IF condition;
REGISTERED AS object-identifier;

The package template specifies the characteristics about an IA, it is a combination of behaviour definitions, attributes, attributes groups, operations, notifications, and parameters. We suggest the incorporation of a new property called KNOWS, which contains all the specifications of the knowledge base for the intelligent system.

<IA-properties-label> PACKAGE
[BEHAVIOUR [,<behavior-label>]*;]
[ATTRIBUTES [<attributes-label>]*
[ACTIONS [<action-labels>]*
[NOTIFICATIONS [<notification-label>]*
[KNOWS [,<know-label>]*;]
REGISTERED AS object-identifier;

KNOWS attribute will define all the aspects related to management knowledge in a specific intelligent system. This new property has an associated template called KNOW. This template allows a particular MOC to have properties that provide a normalised knowledge of a management dominion. We represented the knowledge in production rules, which are relatively simple, very powerful as well as very natural to represent expert knowledge. The structure of the KNOW template is shown here:

<IA_know-label> KNOW
[PRIORITY <priority> ;]
[BEHAVIOR [,<behaviour-label>]*;]
[IF [,occurred-event-pattern]*]
[THEN sentence [, sentence]* ;]
REGISTERED AS object-identifier;

The first element in a definition is the headed. It is the name of the management expert rule <know-label> and a key word that indicates the type of template KNOW. After the head, the following elements compose the archetype:

- BEHAVIOR: This construct describes the behaviour of the rule.
- PRIORITY: This represents the order in which competing management actions will be executed.
- IF: We can add a logical condition that will be applied to the events that have occurred or their parameters.
- THEN: These are actions and diagnoses that the management platform makes as an answer to network events that have occurred.

The application Model

In order to validate our approach, we have developed intelligent control architecture in an el ectric power system. This system i ntegrates the management knowledge into the network resources specifications. We study an example of alarm detection and intelligent resolution of i ncident concerning a pri vate network. W e have used a tel ecommunications network that bel ongs to a company in the electrical sector in Spain.

> "This approach increases energy efficiency, reduce emissions, and transit to renewable energy. We present a technique for the design and implementation of a distributed intelligent system".

The Spanish power grid company has got a net work using wireless on t he regional high-tension power grid. Part of long-distance traffic in this net i s controlled by a wireless intelligent system distributed throughout thi s private network. The use of integrate knowledge in agents can hel p the system administrator in using the maximum capabilities of the intel- ligent network management platform without having to use other speci fi- cation language to customi ze the application [4]. Our system has thr ee major components: an inference engine, a knowl edge base, and a user interface, figure 2.

- The inference engine is the processing unit that sol ves any given problems by maki ng logical inferences on the gi ven facts and rules stored in the knowledge base.
- The knowledge base is the core of the system. This is a collection of facts and i f-then production rules that represent stored knowledge about the problem domain. The knowl edge base contains both static and dynamic information and knowledge about different network resources and com mon failures.
- Human Machine Interface reports to human operators over a specialised computer called Human-Computer Interface (HCI). Each devi ce provides a time-stamped message on events (starting, tripping, activation, etc.) through the bus.

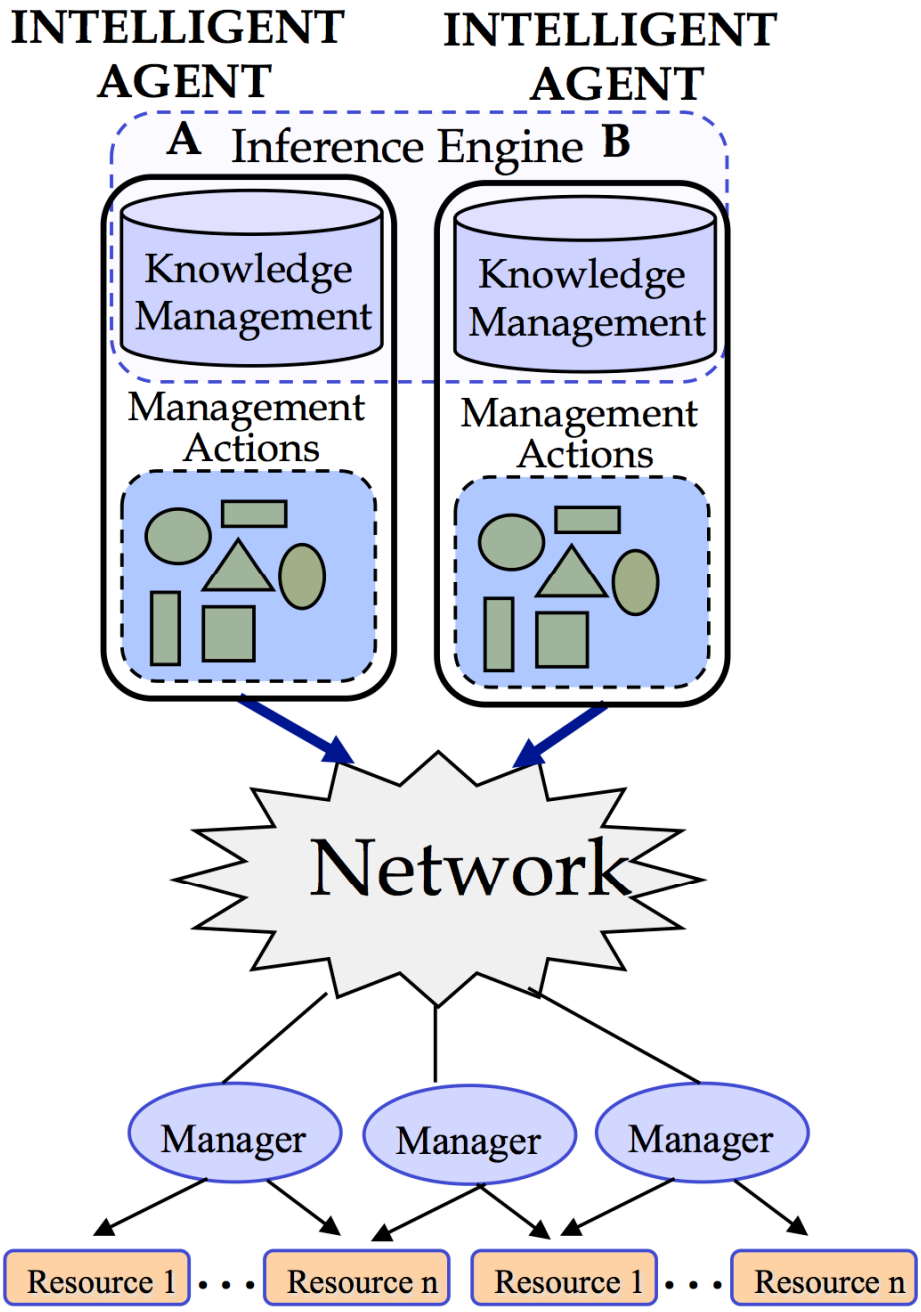


Fig. 2: Architecture System

We have used a SCADA system due to the m anagement limitations of network communication equipment. SCADA systems are configured around standard base functi ons like data acquisition, monitoring and event processing, data storage archiving and anal ysis, etc. [5]. The Remote Terminal Unit (RTU) encodes sensor inputs into protocol format forwards them to the SCADA master. The fundamental role of an RTU is the acquisition of var ious types of data from the power process, the accumulation, packaging, and conversion of data. The RTU communicates back to the m aster, the interpretation and o utputting of commands received from the master, and the performance of l ocal filtering, calculation and processes to allow specific functions to be performed locally [6].

The nerve centre of any power network is the central control and management function, where the coordination of all operational strategies is carried out. Our operations module uses a supervision system called Communication Supervisory System (CSS), figure 3.

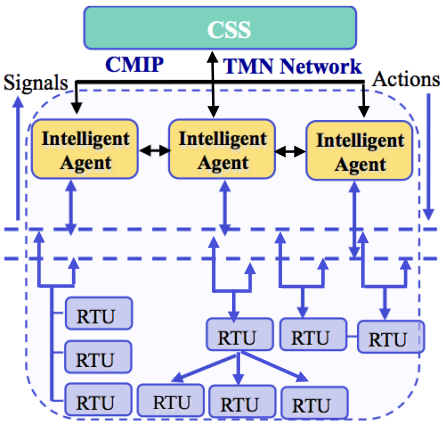


Fig. 3: Communication Supervisory System (CSS)

This system can monitor, in real time, the network's main parameters, making use of the information supplied by the SCADA, placed on the main company building, and the RTUs are installed at different stations. The CSS allows the operator to acquire information, alarms, or digital and analogical parameters of measure, registered on each IA or RTU.

An important aspect of the design and implementation of an intelligent system is determination of the degree of speed in the answer that the network provides. We will discuss the issue of response time for five agents associated to transceiver resources. Every IA is assigned a particular resource repair task. We test the model by inserting some alarms into the system. We compared our results with those we had obtained with a traditional system. We can establish that expert system, with over 500 operation rules, has produced excellent results which, after extensive field-testing, proved to be capable of filtering 93% of produced alarms with a precision of 92, 7% in locating them. The system performs satisfactorily with about a 97,1% rate of success in real cases.

Concluding Remarks

Current networks are very complex and demand ever-increasing levels of quality, making their management a very important aspect to take into account. The intelligent control architecture tries to organize the grid in a flexible way, which allows dynamic aggregation and de-aggregation of resources at different intelligent control levels. The use of IA in network supervision can help the administrator in using the maximum capabilities of the network management platform. These IAs not only have to optimally perform local control within the network resource, but also must comply with responsibilities towards the main grid. Distributing intelligent power system control and analysis is viewed as one of the fastest growing areas of research and new application development in network management. We have investigated the innovative control architecture in electric power systems, in which we are using IA. We conclude by pointing out an important aspect of the obtained integration: the solution not only masks possible faults but also optimises the management functions and efficiency of the distributed services and their resources by using an artificial intelligent strategy, while ensuring a high degree of functionality in power utilities.

References

[1] Goleniewski L. & Jarrett, K.W. Telecommunications Essentials, Second Edition: The Complete Global Source. Addison Wesley Professional. 2006.

[2] ISO/IEC and ITU-T. Information Processing Systems – Open Systems Interconnection – Systems Management Overview. Standard 10040-2, Recommendation X.701. 1998.

[3] Power, Y., Bahri., P. A. Integration techniques in intelligent operational management: a review Knowledge-Based Systems, Volume 18, Issues 2-3, Pages 89-97. 2005.

[4] Ray, P., Parameswaran, N., Lewis, L. Distributed autonomic management: An approach and experiment towards managing service-centric networks, Journal of Network and Computer Applications, Volume 33, Issue 6, Advances on Agent-based Network Management, Pages 653-660. 2010.

[5] Baker, D.; Nodine, M.; Chadha, R.; Chiang, C.J. "Computing diagnostic explanations of network faults from monitoring data," Proc. of IEEE Military Communication Conference, CA, USA, pp. 1-7. 2008.

[6] Doukas, H., Patlitzianas, K. D. Iatropoulos, K., Psarras, J. (2007). Intelligent building energy management system using rule sets. Building and Environment, Volume 42, Issue 10, Pages 3562-3569. 2005.

[7] Chantaraskul, S., Cuthbert, L. An intelligent-agent approach for congestion management in 3G networks, Engineering Applications of Artificial Intelligence, Volume 21, Issue 4, Pages 619-632. 2008

If you would like to find out more about our work please visit our website www.dte.us.es. For any general questions regarding the project, please contact toni@us.es

Creative Modelling of Emergency Management Scenarios

Is creativity needed in modelling emergency management scenarios? How semantic technologies can support experts in defining scenarios.

Coping with unpredictable and unlikely events in emergency management (EM) requires promptness and reactiveness of emergency service providers and institutional operators. Software simulation is a means to prevent and mitigate emergency situations, as it allows definition of recovery plans and training in coordinating the involved people. However, a precondition to simulation is the availability of models that account for all the relevant events causing emergencies, or occurring during their management, and their possible impact on the infrastructures and people lives.

Thus, modelling emergency and management scenarios to the purpose of simulation requires a capability in identifying what to represent and also deciding how to organise the content in a single model. Generally, the modelling activity is human-based and modellers experience a significant difficulty due to the inherent nature of emergency situations. It is relatively easy to model likely situations, perhaps already known, but it is quite hard to even conceive the unlikely and not obvious events that could happen in an emergency scenario. Moreover, the complexity caused by interdependency of involved entities and by the size of the models to be built requires the involvement of an interdisciplinary team, which raises the costs of the modelling project.

Here we propose a framework to provide automatic support to emergency scenarios modellers with the following objective: capability to model unlikely events and their management with **creativity**, i.e., the ability to make or think of new things.

In particular, we propose to automatically generate semantically coherent fragments of emergency management scenario models, called mini-stories [1], to be supplied as input for scenarios creation by composition.

Our approach integrates three types of knowledge: **structural knowledge**, provided by design patterns [2], to support models construction; **domain knowledge**, including emergency knowledge, which is gathered in an ontology [3] and provides the content for the scenarios at conceptual level; and **contextual knowledge**, which is codified through rules and it is related to a specific geographical location or specific regulations to be applied in a given temporal period.

In this contribution we first present some challenging case studies exposing such problems. Then we present a methodology for emergency scenarios modelling and how this is implemented through a software environment we have developed. Finally, we present future work and conclusions.

Challenging Case Studies

This works originates from the difficulties arising during the modelling activities of two different case studies: EM in **supply chains** and EM in **smart cities**.

Supply chains [4] involve networks of interoperable companies where goods are bought and sold, documents and data are shared and physically distributed through cloud technologies, and company services are provided through the web.

Antonio De Nicola

Staff scientist at ENEA. He is member of the UTMEA-CAL Lab. His research activity includes emergency management scenarios modelling, semantic technologies, trusted information sharing, social networks, and decision support systems for low carbon society. He holds a master degree in Physics at the Sapienza University of Rome.

e-mail: antonio.denicola@enea.it

Maria Luisa Villani

Staff scientist at the UTMEA-CAL Lab of ENEA. Her research activity includes emergency management scenarios modelling, discrete-event simulation, semantic technologies, and decision support systems for low carbon society. She holds a PhD in Mathematics from the University of Warwick and a Master in Software technology from University of Sannio.

e-mail: marialuisa.villani@enea.it

Interoperability and collaboration are enabled by infrastructures such as the telecommunication network and the Internet, the energy network, and the transportation system. Such infrastructures are constantly threatened by highly unpredictable events such as natural events (e.g., earthquakes, tsunami, and floods) and anthropic events (e.g., terrorist attacks, environmental disasters). Effects propagation of an emergency, originated from one or more of the companies' sites, to the whole business ecosystem must be carefully accounted for in the simulation scenarios. Also, some emergencies may have disruptive consequences in the overall productive system of a country. An example is the Fukushima nuclear disaster causing victims and damaging also supply and trade chains from automotive to chemical sectors.

Smart cities [5] are characterised by interconnected physical and virtual services aiming at simplification of citizens' activities, consumption of sustainable primary resources, like water and energy, and involvement of people in decisions that could have an impact on their lives. More and more physical services are being operated through ICT services and this dependency leads to new types of emergencies to be handled (e.g., a virus altering the normal functioning of semaphores), but also to new ways an emergency can be faced (e.g., a social network-based set up of voluntary rescue teams). Smart cities ecosystems are threatened by several hazards spanning from natural disasters (e.g., earthquakes) and anthropic events (e.g., terrorist attacks and cyber-attacks).

In the first case, **creativity** is needed in conceiving the impact of **unlikely events**. This would improve preparedness in facing them and, consequently, mitigate the economic losses. The second case is characterised by the need to **model with creativity** new services involved in emergency scenarios and the **currently unknown consequences** of disruptive events happening in smart cities.

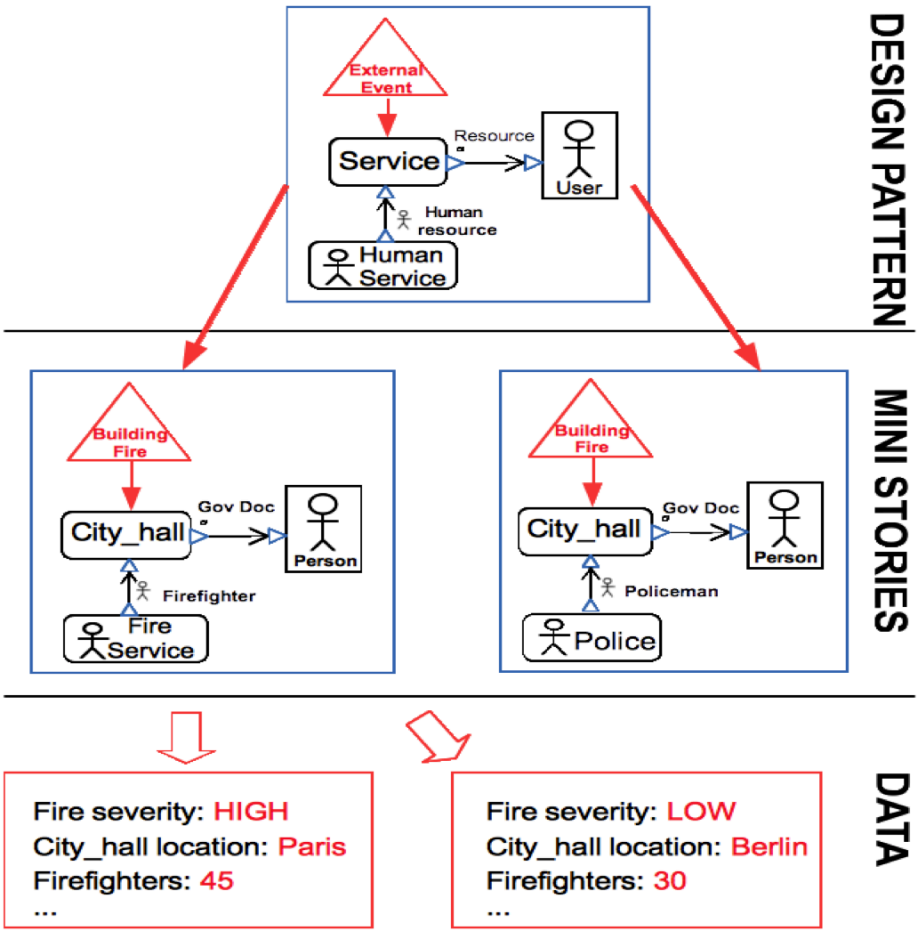


Fig. 1: The three types of knowledge of a EM scenario model

EM Scenarios Modelling and creativity

In this contribution, we face the problem of providing automatic support to the construction of EM *scenario* models to the aim of defining an EM plan for a given emergency situation.

An EM scenario model is a formal representation, through a modelling language, of an emergency situation and of the actions taken to solve it. Such emergency is usually caused by an unpredictable event, occurring in a certain place and impacting one or more specified real worlds objects (e.g., people, infrastructures, institutions, and companies), which must be all represented in the model. To facilitate the modelling activity, this is realised by means of a bottom-up approach starting from simple structures called *design patterns*, encoding an abstract semantics. The design pattern represented in Fig. 1, edited in the CEML language [6] [7], describes a general situation where some external event affects the operation of a service in the provision of some resource to users. Thus, a human service sends human resources to recovery the damaged service.

A specifically built EM and domain ontology (an excerpt is shown in Fig. 2), together with semantic rules, are used to automatically provide more semantics to design patterns, thus generating *mini-stories*.

Mini-stories are the building blocks of an EM scenario model, but they are still *abstract* i.e., they contain general components belonging to the domain, such as earthquake, transportation service and electricity infrastructure. Fig. 1 presents two examples of mini-stories automatically generated from the described pattern. The mini-story on the left represents the natural configuration where firefighters intervene on the

building fire. The other mi ni-story depicted on the ri ght, instead, describes an unusual case where policemen resolve the fire. However, such mini-story can be consi dered as possible in an emergency scenario. Indeed, in case of l arge scale emergencies the availability of the most appropriate human resources cannot be granted si nce they could be occupied elsewhere.

An abstract scenario model is further refined by the modeller with context *data* and simulation parameters (Fig. 1), such a s the id entification of the real objects (e.g., name and location) and thei r characteristics, the severity of the emergency, and/or the response measures (e.g., number of firefighters involved).

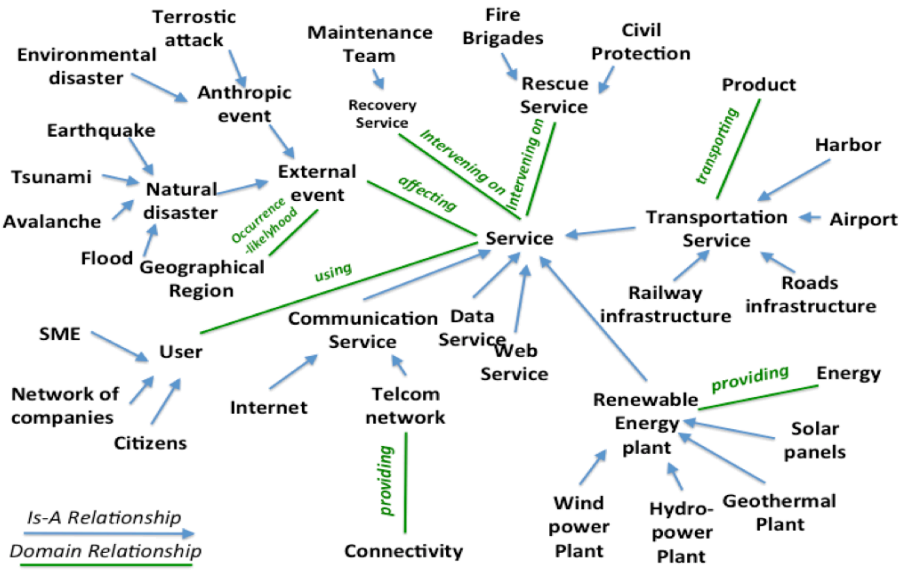


Fig. 2: An excerpt of the EM and domain ontology

Technology support

Our methodology for EM scenari os modelling can be implemented through a suite of tools, as shown i n Fig. 3, interacting with a knowledge base. Some of thes e tools are used in the desi gn phase, for the construction of the knowledge base, and others at run ti me, to generate and validate mini-stories.

An important assumption of the methodology is th e availability of a modelling language and the construction of design patterns with that language. To this aim, we used CEML [6] [7], a dom ain-specific modelling language for EM, formally derived from SysML [8], an UML' s profile widely accepted for systems modelling and which is b ecoming a reference language for interoperability of simulators. CEML has been defi ned to al low domain experts to build formally grounded models in a user-friendly way.

A CEML model is presented with a graphical notation and consi sts of a structural diagram, that is, a representation of a set o f active entities that are linked to exchange objects of some nature. To the diagram, a set of behavi oural specifications has to be attached, describing the computati onal steps that the entities of the model perform during a simulation.

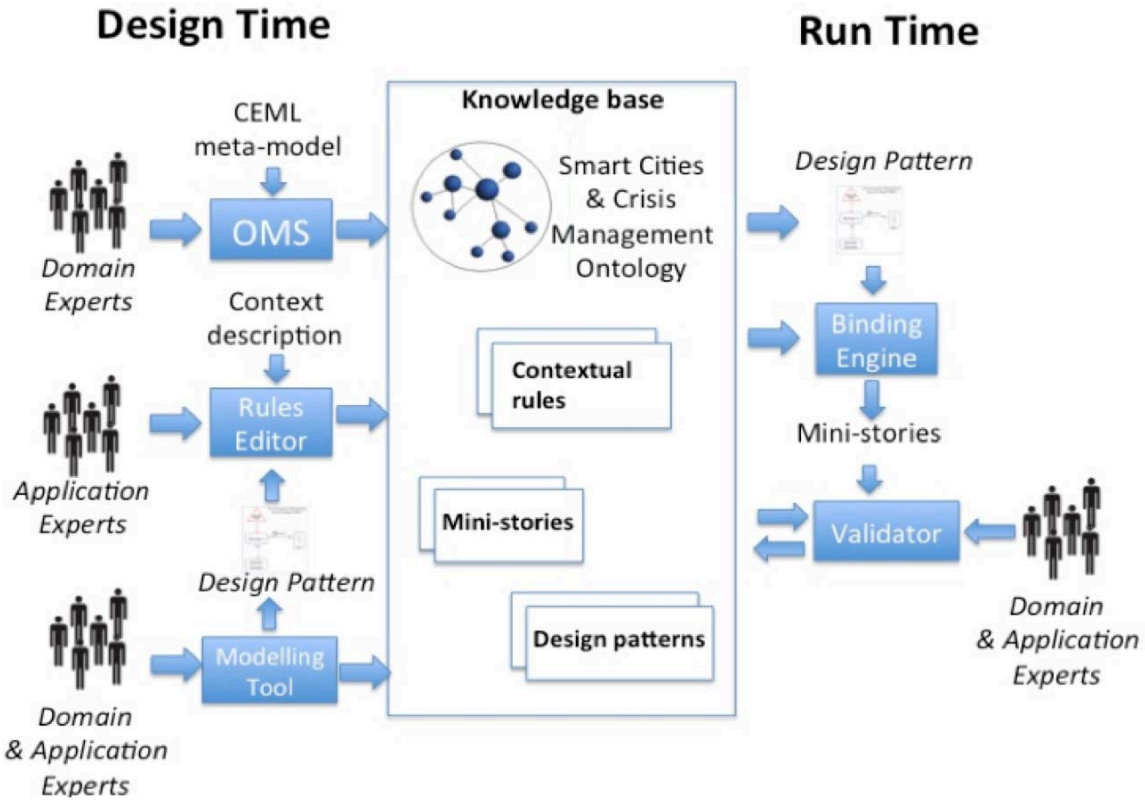


Fig. 3: The architecture for EM Scenarios Modelling

Some domain-specific design patterns have been defined using CEML, including that presented in [5]. They are devoted to facilitate modelling of interaction and communication exchange arising among emergency services providers and citizens to solve the emergency.

Our method towards automatic construction of EM scenarios models starts from the selection of pre-defined design patterns and, by means of mini-stories semantic binding and composition and data assignment, produces concrete EM scenario models. This is achieved through the following activities.

Ontology engineering. Here the ontology covers knowledge about the domain of interest, e.g., business ecosystem or smart city, and the emergencies to be considered with their management. Therefore, such knowledge includes descriptions of hazards and events, critical infrastructures, services provided to companies and citizens, recovery and rescue services, and users. An ontology is built by domain experts by means of an ontology management system (OMS) (e.g., Protégé [9]).

Contextual rules definition. Rules concern the specific context considered such as the location, the temporal period, and the current laws and regulations. These rules are specified by application experts through a rule editor and have to be satisfied by the scenario models and, consequently, by the generated mini-stories.

Model structure definition. The model structure is defined by means of a design patterns approach. Domain and application experts define these patterns through a modelling tool.

Semantics-based generation of mini-stories. Mini-stories, as semantically coherent fragments of scenario models, are automatically generated by a binding engine starting from design patterns and considering the domain and contextual knowledge. The binding engine has been developed in Java. It is based on the Apache Jena framework including the ARQ library [10], which implements a SPARQL 1.1. engine [11]. Then a PostgreSQL [12] database has been developed to persistently save the mini-stories.

Validation of mini-stories. Mini-stories are collected in a repository once domain and application experts have validated them. They can use a validator module conceived to support the voting activity aimed at validation. In case a generated mini-story describes a configuration considered as not valid, the experts can update the knowledge base in order to remove the cause of the non-acceptance. This can be done either by revising the ontology or the contextual rules or even the design patterns.

Conclusions

Creative modelling of emergency management scenarios is a challenging activity requiring an automatic support. Here we face the issue by means of a stepwise approach where mini-stories are fragments of a scenario model. In this contribution we mainly present the part of the work devoted to mini-stories generation. The results of a promising experimentation of the approach are available in [5]. As future work, we intend to study the adoption of methods originally conceived for web services composition, in order to support EM scenario models definition.

Acknowledgements

We wish to thank Michele Melchiori (Università di Brescia) working together with us in this topic.

References

[1] Thalheim B., Tropmann-Frick M. Mini Story Composition for Generic Workflows in Support of Disaster Management. Proc. of 24th Int. Workshop on DEXA, IEEE; 2013.

[2] Gangemi A. and Presutti V., Ontology design patterns, In: Handbook on Ontologies, 2nd edn. Int. Handbooks on Information Systems. Springer, Heidelberg; 2009.

[3] Gruber, T. R. (1993). A translation approach to portable ontology specification, Knowl. Acquis. 5, pp. 199–220, 1993.

[4] De Nicola, A., Melchiori, M., Villani, M.L.: A semantics-based approach to generation of emergency management scenario models. In: Proc. of I-ESA 2014, vol. 7,pp. 163–173. Springer (2014)

[5] De Nicola, A., Melchiori, M., Villani, M.L.: A Lateral Thinking Framework for Semantic Modelling of Emergencies in Smart Cities. Database and Expert Systems Applications (DEXA) Conference. Lecture Notes in Computer Science Volume 8645, pp 334-348, 2014.

[6] De Nicola A., Tofani A., Vicoli G., Villani ML. An MDA-based Approach to Crisis and Emergency Management Modelling. International Journal on Advances in Intelligent Systems 5 (1 & 2), 89-100; 2012.

[7] D'Agostino G., De Nicola A., Di Pietro A., Vicoli G., Villani M.L., and Rosato V., A Domain Specific Language for the Description and the Simulation of Systems of Interacting Systems. Advances in Complex Systems, Vol. 15, Suppl. No. 1; 2012.

[8] OMG-SysML, OMG Systems Modeling Language version 1.2. Available at: http://www.omgsysml.org; 2010.

[9] Protégé. http://protege.stanford.edu

[10] Apache Jena, version 2.11.1, 2013. http://jena.apache.org.

[11] W3C. SPARQL 1.1 Query Language http://www.w3.org/TR/sparql11-query/.

[12] PostgreSQL, version 1.14.2, 2012. http://www.postgresql.org.

CIrcle

Critical Infrastructures: Relations and Consequences for Life and Environment: An interactive touch table application for cascading effects analyses.

Introduction

For two case studies on critical infrastructure in the Netherl ands open data was used for cascading effect analyses. The data alone was not enough t o describe and visualise these effects, but interviews with network owners proved very valuable and gave i nsight in how the open data coul d be used at best.

It became cl ear that when data and knowledge was combined in a smart way, there i s less need to access detailed data from the network owners themsel ves. The results of direct impacts from a flood and cascading effects wer e indicated as roughl y the same or very likely by the network owners we talked to. Figure 1 shows the results of a possi ble electricity black-out during a certain flood scenario at a specific time step based on open data and network knowledge.

Because open data i s widely available but knowl edge is not, we created a st akeholder participation tool that gathers val uable knowledge on net work behaviour and impact.

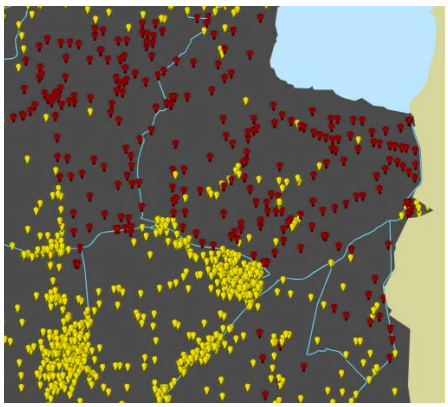


Fig. 1: Result of a possible electricity black-out during a fl ood based on open data.

Cascading Effects

Until now connecti ons between Critical Infrastructure netw orks are hardly identified. Critical infrastructures are dealt with separately, even though di fferent parties are aware of thei r (inter)dependencies and possi ble cascading effects in case of floods or other natural hazards. Still it is n ot clear if cascading effects cause a major part of the to tal impact or If these effects are relatively small. Moreover, data is mostly unavailable and dependenci es are not automated, which makes it difficult to determi ne the effects on a certain location and hi nders an adequate coordination and disaster management.

The reason why data (on for instance the energy networks) are not publicly available is that they are vulnerable for mi suse. Network owners are often aware of t he possibility of cascadi ng effects and their connection with other networks or vulnerable objects, but struggle with the secr ecy of network data. For two case studies, D eltares performed an anal ysis on possi ble cascading effects after a flood with the use of open data and expert knowledge, and tested the results with several netw ork owners. Although detailed data was not used, still th e results were evaluated by network owners to be adequate and close to reality.

Micheline W.A. Hounjet

Team leader of the Deltares Critical Infrastructures Team.

Micheline MSc(Eng) TUDelft is a creative and strong connector between various fields of delta technology. With her background as an engineering geologist, she is not only active in the cross-over between technical disciplines, but also focuses on the link between technology and people. Her main interests are serious gaming, information tools, visualization techniques for crisis management. and to connect critical infrastructure knowledge to create integral impact analyses through cascading effects.

e-mail: micheline.hounjet@deltares.nl

Deltares is an independent institute for applied research in the field of water, subsurface and infrastructure. Throughout the world, we work on smart solutions, innovations and applications for people, environment and society. Our main focus is on deltas, coastal regions and river basins. Managing these densely populated and vulnerable areas is complex, which is why we work closely with governments, businesses, other research institutes and universities at home and abroad. Our motto is *Enabling Delta Life*.

Deltares
Enabling Delta Life

CIrcle

The two cases showed that not all data is needed to perform a cascading effect analysis and that network owners do not need to give all their data. On the other hand, there still is a need for knowledge on the operability of different networks. Because many network owners are aware of the problem, they are willing to cooperate in a different way.

For this purpose CIrcle has been developed, a touch table application for workshops. Within workshops, different network owners, vulnerable object owners or governments can find out and discuss cascading effects together. During the discussion, connections between the networks or objects are drawn and the causal relationships between them are collected in a database.

Examples of these causal relationships are:

- When during a flood the water depth reaches 25 cm, the electricity substations stop functioning (see also Fig. 1).
- When electricity falls out, our industry relies on temporary measures for 3 days.
- When water levels reach 30 cm, the gas network is damaged but can still be repaired.

Fig. 2 shows CIrcle while establishing and defining the connections. For each arrow causal relationships can be collected in the database of CIrcle. These causal relationships are very important for the performance of cascading analyses. Without these, time-dependent analyses and automated GIS analyses are not possible.

Fig. 3 shows the end result where all discussed connections are projected at the same time. Every time such a multi-stakeholder workshop is done and the database of CIrcle fills up with causal relationships, the cascading effect analyses will improve.

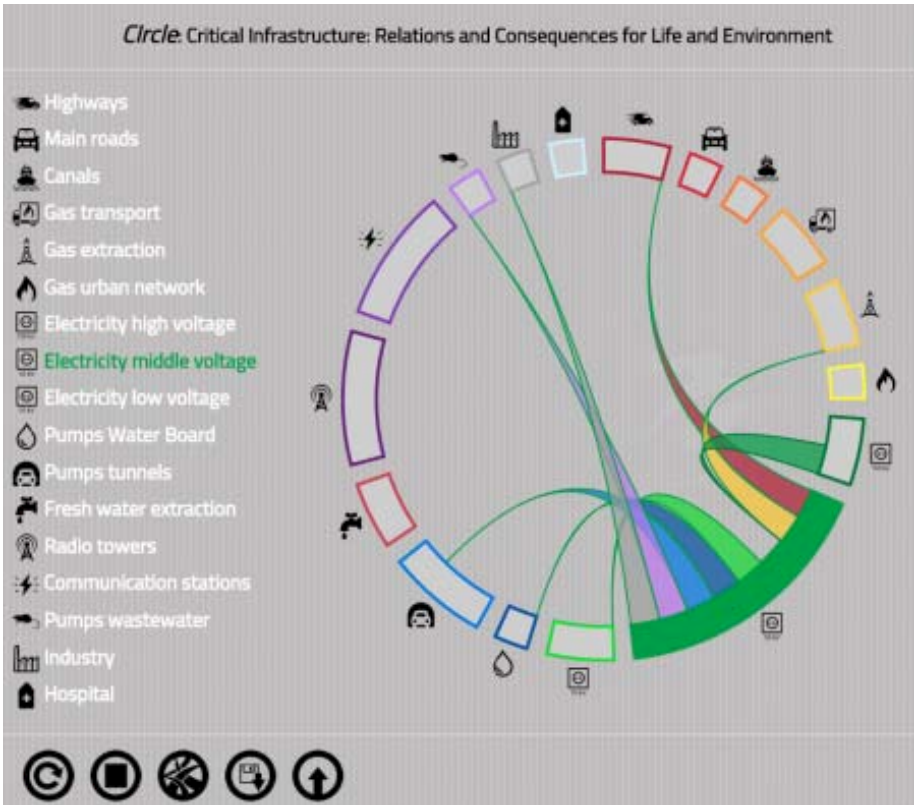


Fig. 2: Drawing of the connections between different Critical Infrastructure networks.

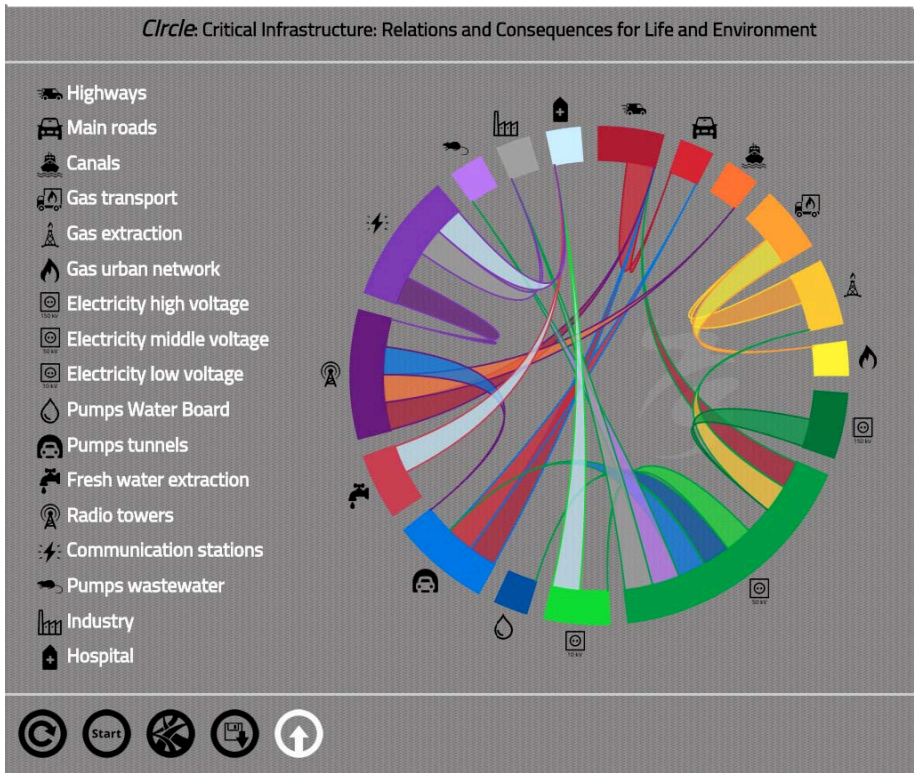


Fig. 3: Final result of the discussion where all the drawn connections are shown in one view.

Floods

The workshops can be organised for different set-ups. It is not strictly necessary to have all the network owners or vulnerable object owners around the table. Every set-up will be interesting for the attenders and valuable for CIrcle and cascading effects analyses as long as everybody voluntarily shares some of their knowledge. At the moment CIrcle is used for flood related cases and connected to state of the art flood and flood risk models like 3Di. Maps and animations are used to show the results of cascading effect analyses obtained with open data. Participants of the workshops (Fig. 4) can comment these existing analyses and indicate if the reality might be different. The causal relationships from the workshop are used to create a second cascading effect analysis as a final result. The differences between these two analyses are valuable for new workshops and the insight in cascading effects.

CIrcle will not only be used to collect cascading effects caused by floods, but is applicable for any natural hazard. Some cascading effects might be universal and not typical for floods, which makes the gathered knowledge very useful.

Fig. 4: Participants of a CIrcle workshop indicate some of the cascading effects.

CIrcle is a simple but effective tool for stakeholder participation in an increasing complex and interdependent society. It performs as a missing link in the insight in cascading effects caused by natural hazards and will be important for robustness and climate change adaptation research in urban areas.

(This page is left blank intentionally)

5th IDRC Davos 2014 – *Building bridges between science, technology, policy and practice*

Already for the fifth time, the biennial International Disaster and Risk Conference IDRC Davos organized by the Global Risk Forum GRF Davos took place in Davos, Switzerland from 24-28 August 2014. Over 700 participants from more than 80 countries representing science, technology, policy and practice gathered in Davos.

The 5th IDRC Davos 2014 was taking stock of the current state of the art on integrative risk management (IRM). By discussing the way forward on IRM participants provided input for the post-2015 Framework for Disaster Risk Reduction (2015 FDRR) which is to be established in March 2015 at the 3rd UN World Conference on Disaster Risk reduction WCDRR in Sendai, Japan. The IDRC Davos 2014 participants represented science, the private sector, a number of UN organisations like UNDP, UNEP, UNESCO, UNISDR, and UNITAR, International Organisations like ILO, WHO, and WMO, The World Bank, governmental agencies from the Philippines, Senegal and Turkey, cities' authorities, as well as many non-governmental organisations.

The focus of the IDRC Davos 2014 was on "Integrative Risk Management – the role of science, technology and practice". With a vital mix of topics and formats, including plenary and parallel sessions, special panels, workshops, exhibitions and networking events, the conference fostered the exchange of information and viewpoints between scientists, practitioners and policy makers.

Conference proceedings, personal The conference proceedings, personal statements from conference participants on the post 2015 framework for Disaster Risk Reduction (DRR), the red chair video statements and other conference outputs are available online at http://idrc.info/

IDRC Davos 2014

- Over 700 participants from 80 countries
- 78 Poster Presentations
- 45 Plenary Speakers
- 311 Presenters
- Risk Award Ceremony
- Best Poster Award
- Photo contest
- Movie Award
- 4 lunch cinemas
- 5 book presentations
- Red Chair Video Statements
- Exhibition
- Post conference expert workshop 9 Keynote Lectures
- 15 Special Panels
- 85 Parallel Sessions
- 5 Workshops

Fig. 1: Red Chair Statements given at IDRC Davos 2014. All statements available online at www.idrc.info

Marc Stal
Senior Project Officer GRF Davos
e-mail:
marc.stal@grforum.org

Andrea Roth
Project Officer GRF Davos
e-mail:
andrea.roth@grforum.org

Jill Portmann
Communication
e-mail:
jill.portmann@grforum.org

Highlights from the IDRC Davos 2014 keynotes

The opening keynote was given by Margareta Wahlström, Special Representative of the United Nations Secretary-General for Disaster Risk Reduction. She presented the current process toward the post 2015 framework for Disaster Risk Reduction including her vision beyond 2015.

She raised the importance of the understanding that disasters have to be seen as long time processes rather than events. Referring to the achievements of the past ten years, such as the building of an international architectural collaboration in DRR, she mentioned that economic losses and mortalities are still increasing.

Science and technology still have to provide important inputs toward the reduction of risks on local, regional, national and international level as more knowledge is needed. By mentioning that the main problem is not necessarily a lack of knowledge but a lack of knowledge management she highlighted the need for an institutional redesign and the responsibilities at the highest political levels.

Ortwin Renn, Professor of Environmental Sociology and Technology Assessment at the University of Stuttgart explained how people behave according to perceptions not facts. His research reveals that the safer people live, the more they are worried about safety, which he refers to as the Risk Paradox.

In his keynote he also referred to perceptions following consistent patterns, but their expression may vary from culture to culture. However, there are dominant perception clusters that govern the intuitive evaluation of risks – even statistics may be biased by perception. He emphasized three major risk challenges of today's society: intensity of human interventions into the natural environment; the lack of adequate governance of collective actions; the side effects of modernisation and globalisation.

Stephan Lechner, Director of the European Commission Joint Research Centre for the Protection and the Security of the Citizen in Ispra warned from the risk of a societal collapse that could arise from complex interdependencies that characterise the modern society, by highlighting that resource depletion, fragile interdependencies, lack of resilience and the end of growth could be drivers of such a collapse.

Fig. 2: Ambassador Michael Gerber on the importance of DRR in the Sustainable Development Goals.

In his keynote, Ambassador **Michael Gerber**, Swiss Special Representative for Global Sustainable Development for the Swiss Development and Cooperation Agency SDC has called for the need to anchor Disaster Risk Reduction and Disaster Risk Management (DRR/M) into the Sustainable Development Goals, dwelling on the Swiss experience.

He highlighted the need to shift from a response only to an integrated risk management approach and highlighted the need to align the targets, monitoring and communities within the sustainable development goals and the post 2015 framework for DRR.

Other keynote presentations have highlighted national experiences and the benefits of sharing such experiences like;

H.E: Nivedita Haran, General Secretary Home Department, Government of Kerala, India, who shared her experience in managing crisis, daily accidents and disasters and explained how to put DRR policies into praxis.

H.E. Birima Mangara from the Ministry of Economy, Finance and Planning, Dakar, Senegal gave insight into the challenges of sovereign risk financing in Africa.

The Japanese experience in incorporating science and technology in disaster risk reduction was conveyed by **Satoru Nishikawa**, Vice-President of the Japan Water Agency.

Barry Hughes, Director of the Frederick S. Pardee Center for International Futures, Denver, USA talked about the identification of risks by using a long-term global model that detects imbalances.

The IDRC Davos 2014 Plenary Sessions

Plenary Session I offered a platform to present the outcomes of major conferences on DRR, which had been held within the first six months of 2014. A special focus was put on relevant outcomes for the post-2015 framework for DRR. The main goal of these presentations was to examine and evaluate the **latest knowledge and advances for all phases of DRR/M in science, technology, education, policy and**

Fig. 3: Plenary Session III Urban Areas and Critical Infrastructures: Resilience as Key. From left to right: Yang Zhang; Peter Burgherr; John Bircham; Stefan Brem; Stéphane Jacobzone.

implementation with a focus on how they have been supporting the implementation of the HFA.

The panel discussion identified gaps and needs for next steps and further research on DRR/M, in regards to education, capacity building and implementation with the goal of revealing commitments for the implementation of the Post-2015 Framework for DRR.

Fig. 4: H.E. Birima Mangara on risk financing in Africa.

Plenary Session II Building financial resilience - Sovereign disaster risk management and financing was co-hosted and chaired by Swiss Re, Zurich, Switzerland. The plenary focused on why **financial resilience** is a critical component of sovereign disaster risk management and discussed the use of ex-ante disaster risk financing instruments. Particular relevance in this sense had the participation of H.E. Birima Mangara, who overviewed the sovereign risk financing challenges in Africa, and Halil Afsarata, who shared his views on similar challenges in Turkey.

The Plenary Session III Urban Areas and Critical Infrastructures: Resilience as Key was co-hosted and chaired by the Swiss Federal Office for Civil Protection, Berne, Switzerland. The Session addressed the gaps, needs and opportunities for **creating a culture of resiliency in urban areas** as a whole, and to develop more resilient and sustainable infrastructures and services to strengthen urban areas from a social, political, economic, technical and ecological perspective. Examples on how science and new technologies can improve the resiliency of critical infrastructures and services were featured. This identified ways in which national strategies and standards are effectively translated into local actions, and successful practices for incorporating social, technical and cultural elements into frameworks that can improve resiliency at all scales and levels – global, national, and local – and across all sectors.

Plenary Session IV Future Scenarios of Global Risks: The Social, Health and Humanitarian Dimensions was co-hosted and chaired by the University of Denver, Denver, CO, USA. The session introduced some of the latest, **cutting-edge approaches to global risk scenario development**, and demonstrated their value by case studies. Particular emphasis was given on the role of the social sciences in risk scenario development. The session examined a social- ecological approach to risk modelling and scenario development and addressed some of the most relevant social and humanitarian aspects as well as health and environmental dimensions.

The **importance of the role of the Private Sector** has been highlighted in all plenary sessions. **Public-private partnerships** are more important than ever and will hopefully be further enhanced at the WCDRR in Sendai.

The 2014 RISK Award goes to ONG Inclusiva, Chile

The 2014 Munich Re Risk Award held under the topic "Disaster emergency – Resilience for the most vulnerable" honours and funds a project dedicated to improving the **inclusion of people with disabilities in disaster risk management (DRM)**.

The winner of the 2014 RISK Award is ONG Inclusiva, an organisation based in Peñaflor, a town south of Santiago de Chile. The aim of the project is to reduce or eliminate barriers in the city for people with disabilities. People with disabilities are particularly vulnerable to disasters because of health, architectural and technological barriers.

Carlos Kaiser, director of ONG Inclusiva stated: "*We are very proud that we won the 2014 RISK Award. It will encourage the whole project team to carry on, find new partners – also within the government – and make disaster risk management in Peñaflor sustainable and inclusive*".

The Risk award is endowed by the Munich Re Foundation in partnership with the UNISDR and GRF Davos as a biannual prize awarded during the IDRC Davos.

The 2015 RISK Award: "Disaster risk reduction – people-centred, innovative and sustainable" is open for application until 1 November 2014. More information on the 2015 Risk Award is available online at: http://www.risk-award.org.


Fig. 5: The Risk Award Laureate Carlos Kaiser (2nd person from right) with the Risk Award Partners (starting from right to left) Thomas Loster, Munich Re Foundation; Margaretha Wahlström, UNISDR; and Walter J. Ammann, GRF Davos.

The role of science, technology and practice in integrative risk management

The theme of the IDRC Davos 2014 was: "The role of science, technology and practice in integrative risk management." The conference aimed within all the different tracks, presentations, outputs and discussions to gather input towards the role of science and technology for integrative risk management; and respectively input for the Post 2015 framework for DRR.

After the conclusion of the conference and based on the outputs of the conference, a post IDRC Davos 2014 expert workshop has been held to draft an input paper on Science and Technology, Education, Capacity Building, and Implementation. The paper shall serve as the IDRC Davos 2014 outcomes document and an input toward the process for the post 2015 framework for DRR. The paper is still being drafted and shall be available on the conference website (www.idrc.info) by the end of the year. The expert workshop was kindly supported by the Board of the Swiss Federal Institutes of Technology ETH.

The participants invited to the workshop covered representatives from research institutes, international agencies, private sector, implementation, practice and donor agencies. Based on the outputs of the IDRC Davos 2014 and the discussion held during the expert workshop, the following preliminary outcomes can be presented:

- the crucial role of science and technology has been underscored;
- speakers highlighted gaps in knowledge and underlined the need to fill such gaps including better knowledge management;
- participants urged for further progress in research with a special focus on science and technology;
- particularly emphasised was the crucial need to learn how to properly put science into practice and how to feed the results back into science.

IDRC Davos as platform to link decision-makers and policy-makers with the scientific and technical community has proofed to be an important contribution towards this inter- and trans-disciplinary exchange of knowledge:

- there was a common agreement that the global risk landscape is changing and the dynamics in resilience-building are evolving fast;
- the increasing exposure and vulnerability to hazards and risks has been underscored but also recognised the progress made in integrative risk management approaches to reduce the risks from hazards and other threats;
- Integrative risk management is gaining **more and more** importance within the international DRM community;
- links and intersections between DRR, Resiliency, Sustainability and also Humanitarian spheres were widely discussed; and
- the private sector plays a crucial role in international disaster risk reduction activities and public-private partnerships are becoming increasingly important.

Fig. 6: Participants of the IDRC Davos 2014 Post Conference Workshop which was organized by the Global Risk Forum GRF Davos and UNISDR Stag (UNISDR Scientific and Technological Advisory Group) with support of the Board of the Swiss Federal Institutes of Technology ETH.

CIPedia© is here!

www.cipedia.eu

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

> CIPedia© aims to become a common reference point for CIP concepts & definitions.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

Roadmap

In its initial stages of development, CIPedia© resembles more to a glossary, which means it is a collection of pages – one page for each concept with key definitions. It aims to expand more and include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

CIPedia© is now publicly available on http://www.cipedia.eu.

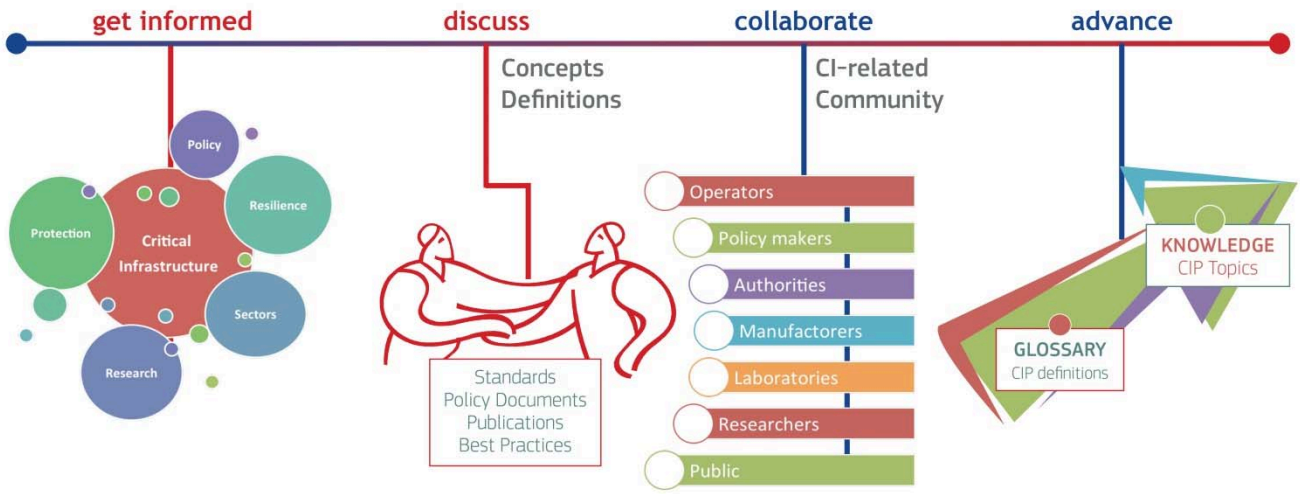
Future versions will be more dynamic; CIPedia© will allow stakeholders to update information capturing the evolution of the CIP domain, as new concepts emerge or receive different meaning.

Marianthi Theocharidou

Marianthi Theocharidou works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), for the CIPRNet and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

> The initial content was provided by the EC-JRC, Fraunhofer, TNO, and the CIPRNet consortium.



Links

ECN home page	www.ciprnet.eu
ECN registration page	free registration on www.ciip-newsletter.org
CIPedia© The upcoming and **new** CIP reference point	www.cipedia.eu

Forthcoming conferences and workshops

ISPEC 2015 11th Information Security Practice and Experience Conference	http://icsd.i2r.a-star.edu.sg/ispec2015/	Call for Paper May 5-8 Bejing China
6th IDRC Davos 2016	www.grforum.org	28. 8.- 01.09. 2016
CfP ESReDA CI Preparedness Seminar	www.esreda.org	May 28-29, 2015, Wroclaw University of Technology, Poland

Exhibitions

Interschutz 2015	ht	tp://www.interschutz.de/86385	8.-13.6.2015	Hannover ,Germany

Associations

Global Risk Forum Davos	www.grforum.org
Swiss Cyber Storm	www.swisscyberstorm.com/

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu

Project home pages

FP7 CIPRNet	www.ciprnet.eu
ERNCIP Project	https://erncip-project.jrc.ec.europa.eu
PREDICT	www.predict-project.eu
Intelligent Network Modelling	www.dte.us.es
ERNCIP	https://erncip-project.jrc.ec.europa.eu/

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other materi al on "Resi lience of Networks and Services and Critical Information Infrastructure Protection" I this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
ENISA information pool on cyber strategy	www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

Websites of Contributors

Joint Research Centre (EC-JRC)	https://ec.europa.eu/jrc/en/institutes/ipsc
Delatres	www.deltares.nl/en
ENEA	www.enea.it/en/home?set_language=en&]http://www.enea.it/en/home?set_language=en&

European CIIP Newsletter

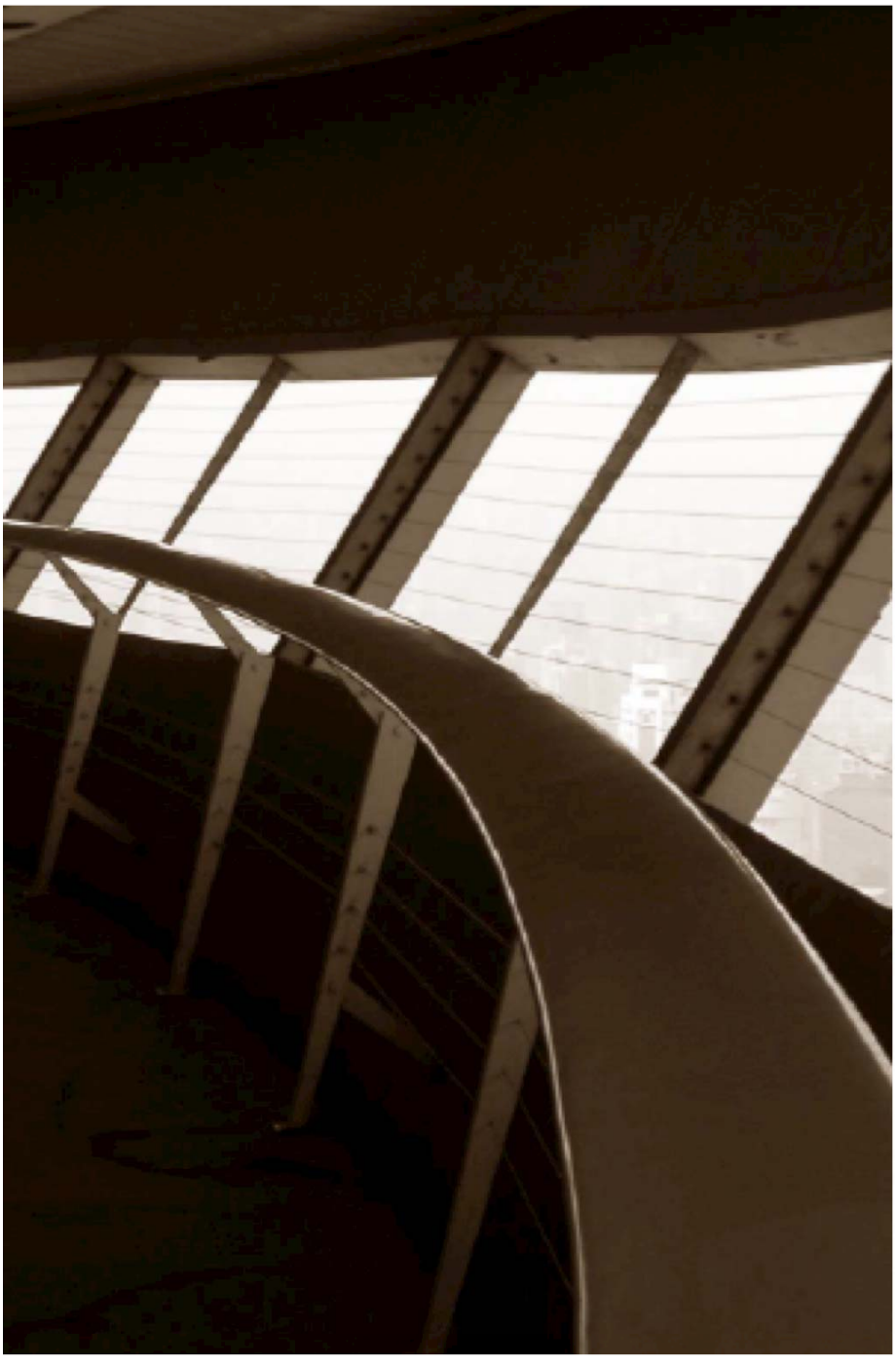
March 15 – June 15, Volume 9, Number 1

CRITIS 2015

Submission deadline
May 10, 2015

2nd Young CRITIS Award

Conference
Oct. 5-7, 2015 Berlin



ECN

Contents

CIPR Net

> 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

Editorial: Fostering synergy between security projects on Critical Infrastructures

There are lots of EU and national CIP projects, but rarely the projects know form each other. CIPRNet and C(I)IP Newsletter ECN support visibility and interaction.

Although Critical Infrastructures Protection (CIP) is a new research topic which began at the end of the 90s and accelerated after the 9/11 terrorist attack on the twin towers in New York, todays the EU has increased the interest on this matter through several security research projects under the 7th framework programme in the period 2006-2013 continuing today through HORIZON 2020.

The issues considered by the EC funded projects are as diverse as security of the citizens, security of infrastructures and utilities, intelligence surveillance and border security, restoring security and safety in case of crisis, security systems integration interconnectivity and interoperability or security and society.

The threats considered rank from natural catastrophes (earthquake, tsunami, volcanic eruptions, extreme weather conditions...) to terrorist attacks (CBRN, explosions, cyber, electromagnetic attacks ...) or organized crime.

The EC is promoting the idea that all these projects should interact together to benefit of the past experience, to avoid the duplication of efforts and to achieve more within the envelope of the available EU contribution.

This issue of the ECN letter series has the ambition to help in developing the synergy between the EC funded projects and even beyond, in extending the contour to the national research projects on the same topic. This is the reason why several project coordinators have been invited to present their projects: INFRARISK, ASTARTE, PROGRESS, BESECURE, DEMOCRITE ... It is anticipated that this will continue in the future issues of the ECN letter series.

The EU FP7 Network of Excellence (NoE) CIPRNet (Critical Infrastructure Preparedness and Resilience Research Network) pioneered in the development of the synergy between the projects by creating on its own website a variety of services to the benefit of the CIP community (visit the CIPRNet website at www.ciprnet.eu and see in particular CIPedia©).

This issue is also hosting more generic papers from the French CIP community: "Societal Resilience" by Alain Coursaget, Director of ACCESS2S, "Pôle RISQUES- The innovative cluster on risk management" by Jean-Michel Dumaz, Security Program Manager at Pôle RISQUES, "Cascading failures: a dynamic model for CIP purposes" by Mohamed Eid, CEA CIP expert, "Critical infrastructures are at risks under electromagnetic attacks" by Dominique Sérafin. These various articles will give some flavour of the French national CIP community activities.

We would like also to remind you that the CIP community has a rendezvous in Berlin at the **10th edition of the CRITIS conference** which is scheduled October 5-7. We announce also that the student award will be delivered at the next CRITIS conferences. Therefore, all young researchers are encouraged to apply for 2015 and 2016 awards:

http://www.critis2015.org/ciprnet-young-critis-award/

Enjoy reading this issue of the ECN!

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

Dominique Sérafin
is in charge of developing security research at CEA-centre de Gramat, France.

e-mail: **dominique.serafin@cea.fr**
CEA,DAM,GRAMAT

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

e-mail: **bmhaemmerli@acris.ch**
He is ECN Editor in Chief

CRITIS 2015

10th International Conference on
Critical Information Infrastructures Security
October 5–7, 2015, Berlin, Germany

www.critis2015.org

With

2nd Young CRITIS Award Competition

http://www.critis2015.org/ciprnet-young-critis-award/

If you are less than 32 years and you contribute
Please apply!

CAPITAL: **C**ybersecurity research **A**genda for **PrI**vacy and Technology ch**AL**lenges

Creating an Integrated Research and Innovation Agenda for Cybersecurity

Cybersecurity is a growing concern worldwide with cloud computing, smart grids, social networks, and Voice over IP telephony as key target domains. Europe's interests, sensitivities, and commitment to liberal values in cybersecurity and privacy are not necessarily aligned to those of other leading world actors. Therefore, leaning back and expecting others to solve the problems is not likely to lead to optimal outcomes for Europe. However, for Europe to move to a pro-active role, it has to exercise its power potential by achieving a sufficient degree of coordination among Member States. In addition, Europe's ability to influence how cybersecurity and privacy issues are handled is also key to the competitiveness of European industries in the field.

CAPITAL is a European Commission FP7 funded Project running from October 2013 to October 2015 for 2 years. CAPITAL will deliver a European integrated Research and Innovation Agenda for cybersecurity and privacy through looking at the emerging areas of information technologies, reference models, identifying threats and solutions. This article describes the process of CAPITAL workflow and explains some of the research already conducted.

The emerging areas of information technology

CAPITAL has identified 8 key emerging areas of information technology which are the following: **1) Future clouds** - new models for the provisioning of infrastructure and software resources by external vendors or by a different IT department over the Internet; **2) Future Security and Privacy Incident Management:** next-generation SIEM-like systems that integrate new layers of business and application for increased intelligence into the status of security and privacy in a target monitored system, and which provide automated proactive and reactive – countermeasures- functionalities for attack detection and incident response; **3) Cybersecurity and Privacy Engineering:** implementation of security and privacy across all phases of the SDLC for more secure and privacy-respecting applications and services; **4) Internet of Things:** the integration of a multitude of new disparate intelligent devices connected and feeding information to the Internet; **5) Mobile Computing:** the fusion of traditional information technology with mobile telecommunications, including new services, applications, and communication infrastructure; **6) Big Data:** the extraction and processing of massive volumes of information available to information systems; **7) Critical Industrial Systems:** the application of IT control systems that are used to monitor and manage industrial and other critical processes, in the advent of other emerging technologies and consequent threats; and, **8) Online Trust and Transparency for Privacy:** the management of digital identities, trust, and privacy in complex infrastructures, including recommendations, rating, reputation, and reasoning for trust in online environments. CAPITAL conducts in-depth research into each of the areas and draws a list of research items based on this research.

The Crystal Ball Reference Model

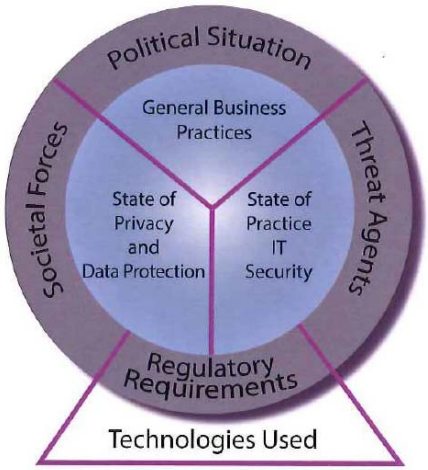
The security and privacy needs associated with an area of information technology are influenced by the business practices of the emerging area, the technology used and environmental forces. Market trends, the societal impact and the evolution of technology determine the future evolution of the emerging area.

Mari Kert

Mari holds a LLB International Law and an LLM Law and Technology. She has experience in the field of cyber defence, cybercrime, privacy, data protection, security and border protection related issues. Her past work includes research conducted at the NATO Co-operative Cyber Defence Centre of Excellence, as well as with the European Commission, DG Home Affairs where she was part of the European Union negotiating team for the Passenger Name Record agreements between the EU, the United States, Canada and Australia. She is working as a Cybersecurity Policy Manager at the European Organisation for Security responsible for coordinating all policy activities between industry and the public sector and is coordinating an FP7 funded project CAPITAL – Cyber Security and Privacy Research Agenda and is also involved with project CYSPA and COURAGE.

e-mail: mari.kert@eos-eu.com

CAPITAL presents a new and innovative reference model called the **Crystal Ball** model consisting of all these forces for each emerging area. These reference models have been used throughout the project to understand how research needs and innovation barriers affect emerging technologies and application domains.



The foundation of each emerging area is the technology. All other entity classes rest on it. Hence, it is placed on the bottom of our model. The crystal ball itself consists of two layers: Business practices and environmental forces. The business is at the core of the model because it defines the needs and goals of products evolving from an emerging area. The environmental forces are the outer ring of the crystal ball. They are an external influence for the business practices and the whole emerging area of technology. Furthermore, the model gives an overview of the maturity of each emerging area and allowing the comparison of each of the emerging areas. Our initial analysis showed that none of the emerging areas seems to be in an extreme condition. However, the maturity level of their entity classes still differs. The crystal ball reference model helps to clarify the situation. Selected influencing forces are highlighted to show certain aspects in detail. The Emerging Area "Online Trust and Transparency for Privacy" exemplarily shows the contrast between outer and inner forces within the reference model.

Threat landscape and gap analysis

CAPITAL also identified current and future threats in cybersecurity and privacy, identified current solutions and performed an initial gap analysis between the emerging areas, the threats and the solutions. The study of the gaps for each emerging area resulted in a set common areas of deficiency which are fundamental for all emerging areas and highlight core topics of cyber security and privacy that require further improvement, namely Foundational Gaps. The following are the 7 foundational gaps identified: 1) Encryption algorithms; 2) Secure network protocols; 3) standard cyber security and privacy metrics and global benchmarks; 4) Usable Security and Privacy by default (zero-configuration); 5) Cyber security risk management process and techniques; 6) Secure, privacy-respectful and usable mechanisms for authentication, and authorization, and; 7) Effective protection of systems' integrity against malware (virus, trojans, worms) and new emerging threats.

> CAPITAL delivers a European integrated Research and Innovation Agenda for cybersecurity and privacy through looking at the emerging areas of information technologies, reference models, identifying threats and solutions by 2015 September.
> CAPITAL also works closely together with the European Commission NIS Platform.

These gaps highlight areas of improvement in today's technological landscape with regards to their preparedness to deal with current and emerging cyber security threats. These areas of improvement can be translated into research topics to further investigate in order to bridge the gaps.

Review of Research Agendas and Market Study

CAPITAL is currently studying all the other research agendas found and deriving information on the research items that were not so far identified in the project. Furthermore, CAPITAL is currently conducting a market study, which aims to validate whether the identified gaps between cyber threats and cyber research challenges is experienced by the main market players. More specifically, the market study tries to assess the market structure and dynamics features determining the innovativeness of the market in the EU in cybersecurity and privacy. Specific activities foreseen for the market study include the identification of clusters specialized in cybersecurity and privacy, identification of the main players: SMEs, MNEs, (semi-) governmental institutions, universities and conducting interviews.

All of this is then pulled together into a list of research items, which will be then integrated into the Final Research and Innovation Agenda for Cybersecurity and Privacy.

In search for evaluators

CAPITAL is currently looking for expert evaluators in each of the emerging areas of information technology in order to evaluate the research items identified so far through participation in our workshops in the first half of 2015 or through our Online Collaboration Tool. If you identify yourself as an expert, feel free to get in touch with Mari Kert (details below).

The CAPITAL Consortium

The CAPITAL Consortium consists of 9 partners: EOS (European Organisation for Security), Engineering, Thales, Fraunhofer, Atos, Ecorys, University Degli Studi di Trento, Conceptivity and TNO. This represents a good mix of large and small industry and the leading academia and research institutions across Europe.
If you would like to find out more about CAPITAL please visit our

Website at http://www.capital-agenda.eu/?Page=home
Collaboration Tool: http://capital.atosresearch.eu/home
Email: mari.kert@eos-eu.com .

CAPITAL
Cybersecurity research Agenda for Privacy and Technology chALlenges

FP7 ASTARTE: **A**ssessment, **ST**rategy **A**nd **R**isk Reduction for **T**sunamis in **E**urope

ASTARTE is organized to foster tsunami resilience in Europe, through innovative research on scientific problems critical to enhance forecast skills in terms of sources, propagation and impact.

Tsunamis are low frequency high impact natural disasters. In 2004, the Boxing Day tsunami killed hundreds of thousands of people from many nations along the coastlines of the Indian Ocean. Seven years later, and in spite of some of the best warning technologies and levels of preparedness in the world, the Tohoku-Oki tsunami in Japan dramatically showed the limitations of scientific knowledge on tsunami sources, coastal impacts and mitigation measures. The experience from Japan raised serious questions on how to improve tsunami warning systems as well as the resilience of coastal communities, to upgrade the performance of coastal defences, to adopt more efficient risk management for existing structures and for the reconstruction of damaged coastal areas. Societal resilience requires the reinforcement of capabilities to manage and reduce risk at national and local scales.

Tsunamis in the NEAM region

Tsunamis may represent an important threat also for European coasts. Several European coasts experienced large tsunamis in historical times (e.g., Crete 365 and 1303; SW Iberian Margin 382 and 1775, the 'Lisbon tsunami'; Chios 1881; Messina 1908; Loen in Norway 1936; Balearic Islands 2003), as well as pre-historical tsunamis (like that generated by the Minoan Santorini eruption or Storegga slide some 8k years BP) killing thousands of people and causing significant damages to coastal economies.

NEAMTWS

In response to the tragic 2004 Indian Ocean tsunami, the Intergovern-mental Coordination Group for the Tsunami Early Warning and Mitigation System in the North-eastern Atlantic, the Mediterranean and connected seas (ICG/NEAMTWS) was formed (http://www.ioc-tsunami.org/index.php?option=com_content&view=article&id=70&Itemid=14&lang=en). National Tsunami Warning Centres (NTWC) in each country are responsible for issuing warnings to the relevant authorities in the Member State. Tsunami Watch Providers (TWP) are those NTWCs willing and able to provide tsunami alert information outside their Member State at designated Forecast Points. To date, that is almost exactly ten years after the 2004 Indian Ocean tsunami, there are 5 candidate TWPs in the NEAMTWS region, France, Greece, Italy, Portugal and Turkey, four of which are operating on a 24/7 basis. They provide alerts to their subscribers if a tsunami may have been generated because of a submarine or coastal earthquake in the region.

ASTARTE Objectives

The ultimate goals of ASTARTE are to reach a higher level of tsunami resilience in the NEAM region, to improve preparedness of coastal populations and, ultimately, to help saving lives and assets. The main objectives are: (i) assessing long-term recurrence of tsunamis; (ii) improving the identification and modelling of tsunami generation mechanisms; (iii) developing new efficient and fast computational tools for short- and long-term hazard assessment; (iv) ameliorating the understanding of tsunami interactions with coastal structures; (v) enhancing tsunami detection capabilities, impact forecast and early warning methods in the NEAM region; (vi) establishing new approaches to quantify hazard, vulnerability and risk related to tsunamis, accounting for inherent uncertainties; (vii) identifying the key components of tsunami resilience and potential implementation in the NEAM region. Such goals will help improving the future management of tsunami risk in Europe, and increasing

Jacopo Selva

Istituto Nazionale di Geofisica e Vulcanologia (INGV)

e-mail: jacopo.selva@ingv.it

Maria Ana Baptista

Coordinator of ASTARTE

Instituto Português do Mar e da Atmosfera (IPMA)

e-mail:
mavbaptista@gmail.com

the efficiency of European tsunami warning centres. Indeed, all the Institutions hosting TWPs in Europe are partners of the ASTARTE project.

Methodology

ASTARTE consists of ten Work Packages (WPs). WP1 is devoted to Project coordination and management. WPs 2-5 focus on the analysis of tsunami recurrence, generation mechanism, modelling of tsunami nucleation, propagation and coastal impacts. Altogether these WPs will develop an up-to-date knowledge background to the Project. They also involve dedicated fieldwork, including research cruises, in locations that are considered highly significant to obtain new critical background information. Most ship time costs will be provided in kind by the Consortium partners, with only a very small amount charged to the Project. WPs 6-8 focus on detection and communication infrastructures for early warning systems, as well as, on the development of innovative methods for short- to long-term hazard and risk assessments. In all these WPs, from 2 to 8, specific developments beyond the state-of-the-art are expected, along with explicit evaluations about related uncertainties. These WPs open into WP9, which aims at building tsunami resilient societies in Europe, and WP10, which is devoted to the dissemination and exploitation of results. ASTARTE considers 9 test sites in the Mediterranean and Northeast Atlantic, which are under the threat of tsunamis of different origin, such those that might be generated by earthquakes, landslide and volcano sources, and where interactions with stakeholders and the society at large will take place, and practical applications will be tested.

Expected Results

ASTARTE will result in: (i) an improved knowledge on tsunami generation involving novel empirical data and statistical analyses so that the long-term recurrence and associated hazards of large events in sensitive areas of NEAM could be established; (ii) the development of numerical techniques for tsunami simulation concentrating in real-time codes and novel statistical emulations, and (iii) refined methods for the assessment of tsunami hazard, vulnerability and risk. ASTARTE will also provide better forecast and warning tools for candidate tsunami watch providers (CTWPs) and national tsunami warming centres (NTWCs), and guidelines for tsunami Euro Codes and decision makers so that sustainability and resilience of coastal communities could be increased. In summary, ASTARTE will develop critical scientific and technical elements required for a significant enhancement of the Tsunami Warning System (TWS) in the NEAM region in terms of monitoring, early warning and forecast, governance and resilience, and it will provide innovative methods and results on which to base future policies aiming to tsunami long-term risk reduction. Overall, this will lead to the goal of the European/NEAM Horizon 2020 strategy: to foster tsunami resilient communities.

Toward the first SPTHA for NEAM region

Probabilistic Tsunami Hazard Analysis (PTHA) is one of the main scientific contributions to risk reduction of coastal areas. PTHA is the first step of quantitative risk assessment and guidance for risk mitigation, both for long-term planning and for improving early warning strategies. The aim of PTHA is to assess, over a given exposure time, and at a specific target site or coastline, the exceedance probability of a hazard intensity threshold, as a function of the threshold value, from any potential tsunami source. The analysis can be performed choosing different tsunami metrics, such as maximum wave height or current speed offshore, the maximum flow depth inland, or the maximum runup, depending on the goal of the application. Any PTHA includes a series of challenging steps, at which practical choices and approximations are typically necessary. A full assessment of the associated uncertainty is also critical, and it is indeed a main requirement for PTHA applicable for regulatory concerns. Within ASTARTE, it has been established a working group for developing the first consensus PTHA from tsunamis with Seismic origin (SPTHA) for the NEAM region, which will represent a reference regional assessment for future applications, at European, national and local scales.

ASTARTE at glance

Assessment, **ST**rategy **A**nd **R**isk Reduction for **T**sunamis in **E**urope:
www.astarte-project.eu
FP7 – Collaborative Project

Total Cost: 7,884,882.47 EUR
EC Contribution: 5,999,677.80 EUR
Duration: 3 years (2013-2016)
Start Date: 01 November 2013

Consortium:
26 partners, from 16 countries
Project Coordinator:
Prof. Maria Ana Baptista, Instituto Português do Mar e da Atmosfera, IPMA

Key Words:
Tsunamis; social resilience; early warning; coastal impacts; structural performance; source mechanisms

The ASTARTE Consortium

The ASTARTE Consortium consists of 26 partners: Instituto Portugues do mar e da atmosfera (PT), Fundacao da Faculdade de Ciencias da Universidade de Lisboa (PT); Middle East Technical University (TR); Bogazici Universitesi (TR); Commissariat a l'energie atomique et aux energies alternatives (FR); Centre National de la Recherche Scientifique (FR); Alma Mater Studiorum – Università di Bologna (IT); Istituto Nazionale di Geofisica e Vulcanologia (IT); Universidad de Cantabria (ES); Universitat de Barcelona (ES); Technical University of Crete (GR); National Observatory of Athens (GR); Universitaet Hamburg (DE); Helmholtz Zentrum Potsdam–Deutsches Geoforschunszentrum (DE); Universitaet Bremen (DE); Stiftelsen Norges Geotekniske Institutt (NO); University College Dublin, National University of Ireland (IE); Natural Environment Research Council (GB); Danmarks Tekniske Universitet (DK); Nstitul National de Certcetare Dezvoltare Pentru Fizica Pamantului (RO); Special Research Bureau for Automation of Marine Researches Far East Branch Russian Academy of Science (RU); Centre National pour la Recherche Scientifique et Technique (MO); U.S. Department of Commerce (US); Port and Airport Research Institute (JP); University of Sourthern California (US); University of Tokyo (JP)..

INFRARISK: Novel indicators for identifying critical INFRAstructure at RISK from Natural Hazards

The goal of the FP7 INFRARISK project is to develop a stress test framework to tackle the coupled impacts of natural hazards on interdependent infrastructure networks.

The INFRARISK project is a new research project of the FP7 environment call topic ENV.2013.6.4-4: Towards stress tests for critical infrastructures against Natural hazards. The INFRARISK project started on October 3rd 2013 and runs until September 2016.

The EU funded FP7 project INFRARISK is a three-year collaborative project to develop a stress test framework to tackle the coupled impacts of natural hazards on interdependent infrastructure networks.

The coordinator of INFRARISK project is Prof. O'Brien, Director and Chairman of the Board of Roughan & O' Donovan's Innovative Solutions Subsidiary(ROD/RODIS).

Extreme, low probability, natural hazard events can have a devastating impact on critical infrastructure (CI) systems in Europe. The EU project INFRARISK (Novel Indicators for identifying critical INFRAstructure at RISK from natural hazards) aims to develop reliable stress tests to establish the resilience of European CI to rare low frequency extreme events and to aid decision making in the long term regarding robust infrastructure development and protection of existing infrastructure. The project will focus on road and rail network infrastructure.

Objectives

INFRARISK will focus on:

1. Developing a stress test structure for specific natural hazards on CI networks and a framework for linear infrastructure systems with wider extents and many nodal points.

2. Considering the impacts of earthquakes, slope failure, mass movement, and flooding on European roads, highways and railroads (Ten-T Core network).

3. Facilitating implementation through the development of GIS based and web based stress test algorithms for complex infrastructure networks.

4. Testing the framework developed through the simulation of complex case studies.

5. Exploitation strategies aimed at disseminating the 'knowledge' and not just the results.

Risk profiling of extreme impacts

Rare low-frequency natural hazard events, which have the potential to have extreme impacts on critical infrastructure, will be identified.

Robust modeling of spatio-temporal processes with propagated dynamic uncertainties in multiple risk complexity scenarios will be developed.

Maria-Jose Jimenez

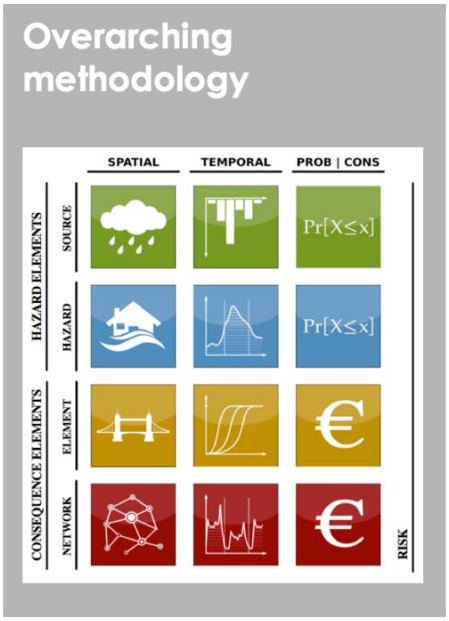
Dr. Maria-Jose Jimenez is physicist and senior research seismologist. She is staff scientist at the Spanish National Council for Scientific Research-CSIC (Consejo Superior de Investigaciones Científicas). She is currently involved in different EU projects and she is member of the Executive Committee of the European Seismological Commission.
Within INFRARISK Consortium she leads WP 9 "Dissemination and Exploitation Activities" and she is co-responsible for the seismic hazard approach in the project.

e-mail: mj.jimenez@csic.es
Institute of Geosciences/ CSIC
Jose Guetiérrez Abascal, 2
E-28006 Madrid
Spain

Overarching methodology

The methodological core of the project is based on the establishment of an "overarching methodology", a harmonised risk assessment process to evaluate the risks associated with multiple infrastructure networks for various hazards with spatial and temporal correlation.

The overarching methodology will capture and incorporate, into a GIS platform, outputs from the extensive profiling of natural hazards and infrastructure, the analysis of single event risk for multiple hazards and the space-time variability analysis of a CI network.



Integrated approach to hazard assessment

An integrated approach to hazard assessment will be developed considering the interdependencies of infrastructure networks, the correlated nature of natural hazards, cascading hazards and cascading effects, and spatial and temporal vulnerability.

Stress test framework

Development of a stress test structure for multi-risk scenarios coupled with a tool for decision-making based on the outcome of the stress test.

Implementation

Development of an Operational Analysis Framework considering cascading hazards, impacts and dependent geospatial vulnerabilities with practical software tools and guidelines to provide greater support to the next generation of European infrastructure managers is the implementation strategy.

Development of a collaborative integrated platform where risk management professionals access and share data, information and risk scenarios results efficiently and intuitively.

INFRARISK works for safer European Critical Infrastructures

In Europe, extreme natural hazard events are not frequent but due to the complex interdependency of our critical infrastructure systems these events can have a devastating impact in any part of Europe.

Protection against the impacts of natural hazards must be guaranteed for people to work and live in a secure and resilient environment. No activity, including emergencies and rescue operations, can be carried out with the loss of key buildings and facilities, transport networks and an interruption of essential supplies.

INFRARISK will develop reliable stress tests to establish the resilience of European Critical Infrastructures (CI) to rare low frequency extreme events, thus contributing to the decision making process on how to build safer in the future. INFRARISK will focus on road and rail infrastructure in Europe.

INFRARISK will enable infrastructure managers to minimise the impact of extreme events by providing them with the necessary tools to develop robust mitigation and response strategies.

Essential in the INFRARISK approach is the dissemination aspect, which involves several targets levels and the development of focused materials and products to reach the widest audience possible.

INFRARISK Consortium

The INFRARISK Consortium consists of 11 members from seven different countries: Ireland, Switzerland, Spain, Netherlands, Norway, Sweden, United Kingdom.

The consortium represents a well-balanced and strong partnership among universities, research institutions, SME's, and Large Enterprise (LE).

The eleven partners in INFRARISK Consortium are:

- ROUGHAN & O'DONOVAN LIMITED (Ireland),
- EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZURICH (Switzerland),
- DRAGADOS SA (Spain),
- GAVIN AND DOHERTY GEOSOLUTIONS LTD (Ireland),
- PROBABILISTIC SOLUTIONS CONSULT AND TRAINING (The Netherlands),
- AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTIFICAS (Spain),
- UNIVERSITY COLLEGE LONDON (UK),
- PRAK (The Netherlands)
- STIFTELSEN SINTEF (Norway),
- RITCHEY CONSULTING AB (Sweden),
- UNIVERSITY OF SOUTHAMPTON (UK)

If you would like to know more about INFRARISK please visit our website: http://www.infrarisk-fp7.eu
watch our video: " The project in 3' ": http://www.infrarisk-fp7.eu/the-project-3-mins

This project has received funding from the European Union's Seventh Programme for research, technological development and demonstration under grant agreement No. 603960 .

PROGRESS: **P**rotection and **R**esilience **O**f **G**round based inf**R**astructures for **E**uropean **S**pace **S**ystems

The FP7 PROGRESS project focuses on the security and resilience of ground based assets of Global Navigation Satellite Systems (GNSS)

The PROGRESS project is a new research project co-funded by the European Union under the EU 7th framework programme. The project is related to the security call topic SEC-2013.2.2-5: "Security of ground based infrastructure and assets operating space systems". The PROGRESS project started on May 1st 2014 and is due to be completed by the end of April 2017.

Abstract

PROGRESS will focus on improving the security and resilience of Global Navigation Satellite Systems (GNSS) and its results will also be applicable to earth observation infrastructure and assets.

At the start of the project a generic GNSS system will be designed and its associated augmentation system will be assessed with regards to vulnerability from intentional malicious threats. In focus are threats, which are generally considered to have a low risk of occurrence but potentially very large impacts.

PROGRESS will concentrate on those threats that have the potential to increase in the coming years. The resulting prioritization of threats and scenarios will be used as input to develop a prototype Security Management Solution (SMS). PROGRESS SMS will be a centralized solution able to automatically detect malicious actions with a built-in reconfiguration capability to ensure the overall system Quality of Service.

The PROGRESS SMS will be composed of an Integrated Ground Station Security Monitoring System (IGSSMS) and a Security Control Centre (SCC). The IGSSMS will be an innovative monitoring solution for the detection of specific malicious types of attacks. The Security Control Centre will analyse the impact of the reported disturbances to the system performance and Quality of Service (QoS) and will propose mitigation strategies, including automatic system reconfiguration.

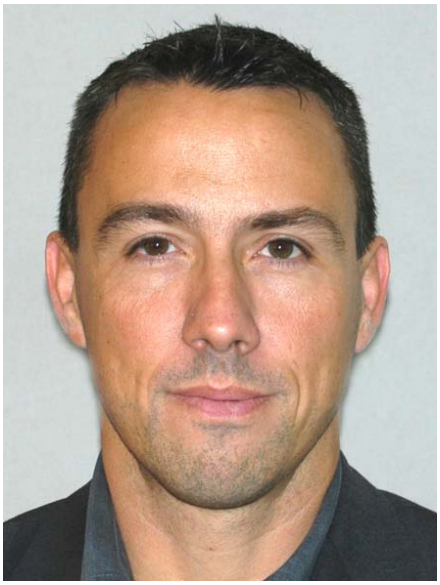
The SMS will be developed with full consideration of present methods and measures for the security and resilience of complex interconnected space control ground station networks by present operators.

The high quality of the developed solutions will be assured by a consortium consisting of a number of experienced partners joining:

- The operator of the Galileo Control Centre in Oberpfaffenhofen,
- The EU leader for satellite systems,
- A manufacturer and world distributor of security solutions,
- Leading applied research institutes,
- Specialized SMEs,
- And a research institution specialized both in security and social aspects.

Context

The main ideas leading to the PROGRESS project is related to the critical importance of GNSS to global society as Global Navigation Satellite Systems (GNSS) based services are used in an ever increasing number of applications, including a large number of critical applications for positioning, navigation and timing (PNT) services.
GNSS time references that are used for example to precisely synchronise critical networked infrastructures, such as: power distribution; fixed and wireless networks, including broadband access networks to the Internet; transportation networks - sea, air, rail and road e.g. for automatic tolls; and financial services e.g. for banking and the stock markets. A number of reports point towards the conclusion that GNSS should be classified as a critical infrastructure itself with the appropriate level of protection.



Nicolas Ribière-Tharaud

Nicolas Ribière-Tharaud is the PROGRESS project coordinator. He is involved in the field of critical infrastructure vulnerability and protection. He is also an expert in the field of electromagnetic effects and their consequences.

e-mail:
nicolas.ribiere-tharaud@cea.fr

CEA,DAM,GRAMAT,
F-46500 Gramat, France

Based on the experience and needs of ground station operators and architects, the following main threats have been identified in [1]:

- Data corruption
- Ground facility physical attack
- Spoofing (Masquerade)
- Jamming
- Replay
- Software/HW threats
- Unauthorized access
- Natural disasters

The consortium plan to focus on threat assessment, detection, protection and mitigation strategies, which can be grouped into three categories: cyber-attacks, RF Interference attacks and physical attacks.

These threats have been focused on because:

a. New technologies are available on the market or technical evolutions in general which are currently evaluated at research level, but require further assessment with specific focus from the security point of view.
b. In the past, threats, which were previously analysed as having a low probability of occurrence, were potentially not taken into account in the system design to a large extent, regardless of the impact they could potentially have on the system or on the service provided to end-users. This is particularly true in the case of terrorism.
c. Europe needs to have the methods and tools to protect its GNSS critical infrastructure and the services expected by its citizens from the threats focused on.

Objectives

PROGRESS has 7 main objectives that are described below:

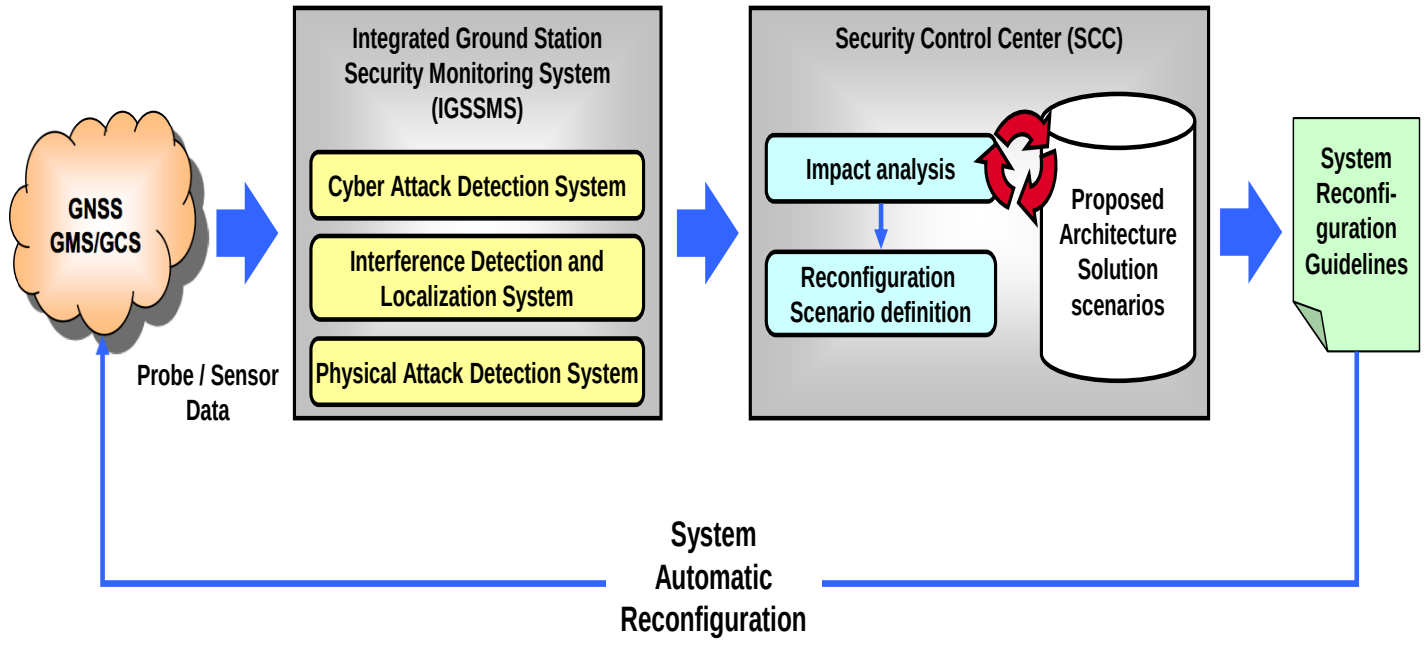
1. Development of risk assessment methodology and tools to assess threats on generic GNSS ground based infrastructure and assets operating space systems and their secure communication links to satellites and a prioritization of the threats for which detection, protection and mitigation solutions should be developed
2. Development of detection solutions for: Cyber-attacks (DoS attacks and spoofing); RF interference (Jamming and Spoofing) detection and localization; and physical attacks (explosive and high power microwaves). These detectors will be integrated in an Integrated Ground Station Security Monitoring System (IGSSMS).
3. Development of threat protection and mitigation solutions for the cyber, RF interferences and physical attacks: guidelines and proposed best practices; architecture solutions; and specific countermeasures and

The PROGRESS project aims at delivering a **prototype Security Management Solution** (PROGRESS solution) composed of an Integrated Ground Station Security Monitoring System and a Security Control Centre. The prototype will be developed on the basis of a generic architecture but with full consideration of present methods and measures for the security and resilience of complex interconnected space control ground station networks

The project will lead to a limitation of the impact of accidents/attacks by providing knowledge for more resilient future GNSS systems and ground stations.

PROGRESS has received funding from EU FP7 under grant agreement Contract No. 607679

PROGRESS main concept



procedures to be implemented once an attack(s) is identified.

4. Development of a Security Control Centre (SCC) to analyse the impact of detected threats and to propose mitigation procedures, including system reconfiguration.
5. Development and integration of a prototype to prove the PROGRESS innovative security concepts, including the IGSSMS and SCC. This aspect includes the development of tools to generate the attack scenario addressed in the project.
6. Testing and evaluation of the prototype Security Management Solution through the PROGRESS prototype testbeds.
7. Further development of strategies to exploit the results of the project in commercial products and services.

PROGRESS objectives include the development of a risk assessment methodology, attack detection and protection means, with respect to threats that have the potential to increase in the coming year.

The innovative concepts are assessed through tests carried on the PROGRESS solution prototype.

The Partners

CEA (France), THALES ALENIA SPACE (France, Italy, Spain), Fraunhofer EMI (Germany), DLR-GfR (Germany), CRABBE CONSULTING LTD (Germany), SECURITON (Germany), DECISIO (The Netherlands), University of Ljubljana (Slovenia), QASCOM (Italy).

If you would like to know more about PROGRESS please visit regularly our website at www.progress-satellite.eu

References

[1] CCSDS 350.1-G-1, Security Threats against Space Missions, Informational Report, Issue 1, October 2006

ARES Conference
The International Dependability Conference

Call for Papers

The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism (FCCT 2015)

To be held in conjunction with the ARES EU Projects Symposium 2015, held at the 10th International Conference on Availability, Reliability and Security (ARES 2015 – www.ares-conference.eu) and organized by the FP7 project CyberRoad (http://www.cyberroad-project.eu/),

August 24th – 28th 2015
Université Paul Sabatier
Toulouse, France

With the constant rise of bandwidth available and with more and more services shifting into the connected world, criminals as well as political organizations are increasingly active in the virtual world. While Spam and Phishing, as well as Botnets are of concern on the cybercrime side, recruiting, as well as destructive attacks against critical infrastructures are becoming an increasing threat to our modern societies. Although reactive strategies are useful to mitigate the intensity of cyber-criminal activities, the benefits of proactive strategies aimed to anticipate emerging threats, future crimes, and to devise the corresponding countermeasures are evident.

The aim of **the First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism** is to anticipate the future of cyber-criminal activities, enabling governments, businesses and citizens to prepare themselves for the risks and challenges of the coming years.

SUBMISSIONS AND REGISTRATION
Authors are invited to submit Regular Papers (maximum 8 pages) via ConfDriver.

IMPORTANT DATES
April 10, 2015: Regular Paper Submission
May 10, 2015: Notification Date
June 8, 2015: Camera-Ready Paper Deadline

CONTACTS
Peter Kieseberg (SBA Research) pkieseberg@sba-research.org

RAPID-N: Assessing the impact of natural hazards on industrial installations

RAPID-N is a web-based decision-support tool for Natech risk management that allows the assessment and mapping of the risk of potential natural-hazard impact on industrial facilities.

The impact of natural hazards, such as floods, high winds, earthquakes, etc., on industrial installations that process or store hazardous materials can cause fires, explosions and toxic releases. These so-called "Natech" accidents have often had significant social, environmental and economic impacts. For example, in 2011 the Tohoku earthquake and tsunami led to one of the worst nuclear accidents in human history. In addition, six refineries suffered severe damage effectively shutting in over 30% of Japan's refining capacity. Similarly, in 2005 Hurricanes Katrina and Rita wreaked havoc on the US on- and offshore oil and gas infrastructure, which led to enormous damage and a hike in global oil prices.

A recent survey among competent authorities highlighted that Natech risk is a concrete threat in European Union and OECD Member States where numerous Natech accidents have occurred. The most important accident triggers were found to be floods, low temperatures and lightning. Interestingly, these natural hazards were not always the ones believed to be of major concern in that specific region. This indicates a discrepancy between risk perception and actual accident causes.

The survey also identified gaps in the development of methodologies and tools for analysing and mapping Natech risks. RAPID-N was developed in response to calls by governments for a decision-support tool for Natech risk management, considering that climate change and increasing industrialisation will change the risk landscape in the future.

The RAPID-N framework

The primary aim of RAPID-N is rapid local or regional Natech risk assessment and mapping with minimum data requirements. RAPID-N features an on-line and user-friendly interface with advanced data entry, visualization, and analysis tools. It does not depend on any commercial risk-analysis applications.

In order to preserve confidentiality, RAPID-N supports data protection and access restriction for critical information, such as industrial plant data and associated risk assessments. User registration is needed for data entry, and further authorization is required for carrying out Natech risk assessment. All other data supporting the risk assessment process is public.

RAPID-N does not contain hard-coded functions for risk assessment. Based on the Natech scenario, models required for risk assessment are created on-demand by using the modelling functions available in the database. The users can enter their own data and models to customize the calculations according to their needs. The data protection feature of the framework prevents user-specific modifications to affect other users. This allows the users to experiment with different analysis methods if so desired.

> Natural-hazard impacts can cause major accidents at hazardous installations. This so-called Natech risk is expected to increase in the future due to climate change

Current capabilities

RAPID-N supports different natural hazards and industrial equipment types. It currently focuses on earthquake impact and contains worldwide earthquake data with M > 5.5. It also monitors the EMSC and USGS earthquake catalogues and automatically updates its database once changes are detected, including ShakeMaps from the USGS.

Elisabeth Krausmann

Dr. Krausmann leads the Natech risk management activities at the Joint Research Centre (JRC) of the European Commission. Her research experience includes risk analysis of natural hazard impact on chemical infrastructures, nuclear reactor safety, severe accident management and consequence analysis. Recently, she has started to work on space-weather impacts on the power grid.

elisabeth.krausmann@jrc.ec.europa.eu

Serkan Girgin

Dr. Girgin is a research fellow at the JRC. His research experience includes Natech risk assessment, industrial accident data analysis, accident consequence modelling, and software development. Recently, his has started working on natural hazard impacts on pipeline systems.

e-mail: serkan.girgin@jrc.ec.europa.eu

From an industrial-installation point of view, RAPID-N contains worldwide information on over 5,500 facilities (refineries, power plants) and 64,000 plant units (mostly storage tanks) collected from public sources.

For assessing the natural-hazard damage, a set of on-site ground motion parameter estimation equations, damage classifications and fragility curves for earthquakes is provided. Currently, the framework contains the most frequently used damage classifications and fragility curves for storage tanks available in the scientific literature. For consequence analysis, RAPID-N includes the complete set of parameters and equations of the Risk Management Programme Guidance for Offsite Consequence Analysis methodology of US EPA.

A modular approach

RAPID-N features a modular structure in which four self-contained but interconnected subsystems focus on the individual aspects related to Natech risk assessment and mapping. These are 1) the scientific module, 2) the natural hazards module, 3) the industrial plants module, and 4) the Natech risk assessment module.

The *scientific module* supports scientific tasks and calculations but it also provides the property definition and estimation framework upon which RAPID-N's risk assessment functionality is built. Due to the complexity of a multi-disciplinary problem like Natech risk assessment, the property definition and estimation framework was created to reduce the amount of data to be entered by the users, to provide default values for missing data, to estimate required damage and consequence parameters, and to guarantee a higher flexibility of the risk assessment by allowing the definition of alternative calculation methods by the users.

The *natural hazard module* provides the source and on-site natural hazard data required for the Natech risk assessment. Both historical and scenario natural hazards are supported. For earthquakes, it estimates the earthquake hazard parameters at the site of the hazardous installations of interest using location-specific attenuation relationships, which are subsequently needed for the risk assessment. For example, RAPID-N determines the distance of each plant unit (e.g. storage tank) to the epicentre of the earthquake, and it calculates on-site peak-ground acceleration (PGA) values by using the appropriate attenuation equation, which is selected automatically. If a ShakeMap is available, the hazard parameters are extracted by interpolation of the map data.

RAPID-N is a tool for rapid local or regional Natech risk assessment and mapping. It is available at:

http://rapidn.jrc.ec.europa.

It can support users with land-use and emergency planning, as well as real-time damage assessment and early warning.

The *industrial plants module* collects physical data on industrial facilities and equipment present on the site. This information includes location, unit types and operating conditions, and hazardous-substance properties. A special mapping tool is provided with RAPID-N to easily locate and delineate plant boundaries, and to identify their units using publicly available satellite imagery.

The *Natech risk assessment module* calculates the natural hazard damage to industrial units, performs the consequence analysis, and maps the results. It includes:

- Damage classifications to define the damage states of plant units due to natural-hazard impact;
- Fragility curves to estimate the damage occurrence probabilities as a function of natural-hazard severity;
- Risk states to define Natech scenarios triggered by the damage states;
- Risk assessment framework to calculate Natech risk and to present the output as risk summary reports and impact maps.

Depending on plant unit properties and the available on-site hazard parameters, RAPID-N automatically selects for each plant unit an appropriate fragility curve, which is a best fit with the available data. For each damage state of the selected fragility curve, case-specific Natech scenarios are generated by using the appropriate risk states, and their consequences are analysed by using the available consequence model functions in the database.

Although the US EPA consequence analysis methodology, which is currently included in the Natech risk assessment module, is not a full-fledged quantitative risk analysis methodology, it is a functional approach to assessing impacts. It allows the calculation of consequence-specific endpoint distances for toxic releases, fires and explosions. These endpoints delineate the distance from the point of hazardous-materials release to where a certain adverse effect is predicted to be experienced. These effects are toxic concentration (ERPG-2 or IDLH), overpressure (7 kPa) or radiant heat (5 kW/m^2 for 40 s - equivalent to second-degree burns). The users can modify the model parameters, substitute calculation functions with alternatives, and even introduce a completely new consequence model by using the property definition and estimation framework of the scientific module, which is connected to the risk assessment module.

RAPID-N allows its users to enter their own data and models to customize their risk assessment according to their needs and requirements.

RAPID-N risk output

The output of the assessment is a risk summary report and interactive risk maps.

Risk summary reports provide detailed information on the parameters used by the user and/or RAPID-N for the simulation, as well as on the end-point consequence distances and the scenario probabilities.

RAPID-N risk maps show the scenario-specific calculated impact areas for overpressure, heat radiation and toxic concentrations (Figure 1). Consequence probabilities are indicated by the opacity of the circles, which range linearly from fully

transparent to opaque as the consequence probability increases. Since the majority of the fragility curves used for the damage assessment include more than one damage state, usually multiple concentric circles are displayed for each plant unit. If the risk assessment involves multiple plant units, areas, which might be affected by releases from several units can be easily identified. The degree of opaqueness increases where endpoint circles overlap, therefore areas at higher risk become evident.

Furthermore, as the risk of cascading effects during Natech events is high, RAPID-N can also be used as a screening tool for identifying potential problem areas due to cascading effects. For example, in case of release of flammable substances that ignite, RAPID-N shows if other infrastructures fall within the fire's impact zone. This gives an indication of where attention should be paid and where further in-depth analysis might be warranted.

The RAPID-N framework supports different natural hazards and industrial-equipment types. It has currently been implemented for earthquake impact on industrial facilities.

Next steps are the inclusion into RAPID-N of floods as additional accident trigger and oil and gas pipelines as a new target critical infrastructure.

Application of RAPID-N

RAPID-N can be used for different stages during the Natech risk-management process. For prevention and preparedness, it can assess the potential consequences of different Natech scenarios to develop Natech risk maps for use in land-use and emergency planning. In the response phase, it can be used for rapidly locating facilities where Natech accidents may have occurred based on up-to-date natural-hazard information, so that first responders and the population in the vicinity of the facilities can receive timely warning.

Extension underway

The RAPID-N framework is in principle applicable to any kind of natural hazard. It is currently implemented for earthquake impact on industrial facilities. Work is underway to extend the system to include floods as additional natural-hazard trigger, and oil and gas pipelines as a new target critical infrastructure.

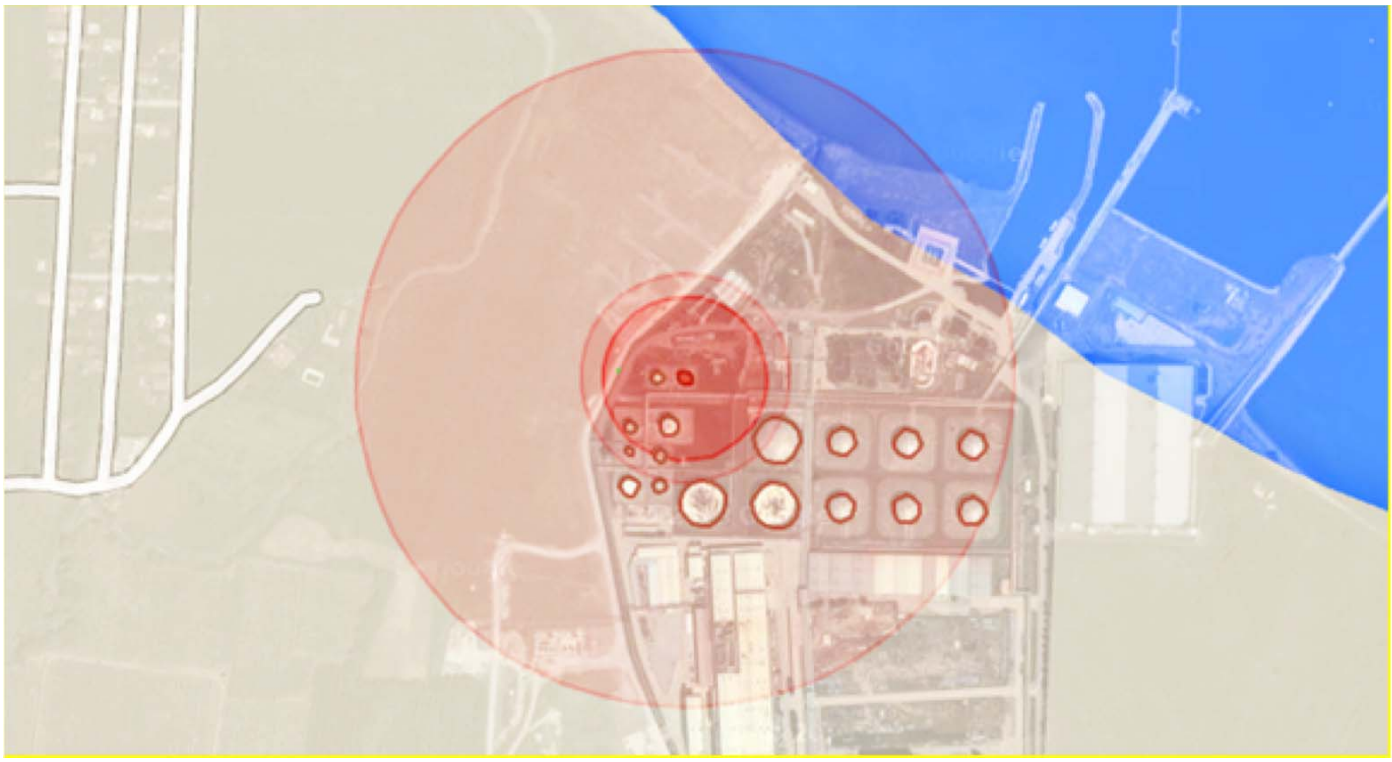


Figure 1: RAPID-N output for the release of a flammable substance from a storage tank upon earthquake impact.

IMF 2015

9th International Conference on IT Security Incident Management & IT Forensics

May 18th - 20th, 2015
Magdeburg, Germany

www.imf-conference.org/
mailto:2015@imf-conference.org

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

About IMF Conference

IT security is an integral aspect in operating IT systems today. Yet, as even high-end precautionary measures cannot prevent every attack or security mishap, the capability to quickly respond to IT security incidents, to secure infrastructure operations and data, as well as forensic capabilities in investigating such incidents in both technical and legal aspects are paramount. Capable incident response and forensic procedures have thus gained essential relevance in IT infrastructure operations and in law-enforcement, and there is ample need for research and standardization in this area.

Since 2003, the IMF conference has established itself as one of the premier European venues for presenting research on IT security incident response and management and IT forensics. The conference provides a platform for experts from throughout the world to present and discuss recent technical and methodical advances in the field. It shall enable collaboration and exchange of ideas between industry (both as users and solution providers), academia, law-enforcement and other government bodies.

Conference Goals

IMF's intent is to gather experts from throughout the world in order to present and discuss recent technical and methodical advances in the fields of IT security incident response and management and IT forensics. The conference provides a platform for collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

IMF 2015 Conference Program

www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2015/program.html

BESECURE: Best practice Enhancers for Security in Urban Regions

The goal of the FP7 BESECURE project is to improve urban security policy making by sharing European best practices and providing visualization and assessment tools.

BESECURE is a research and technological development (RTD) project under the topic FP7-SEC-2011.6.2-1 - Best practices for enhancing security policy in urban zones". The BESECURE started on 1st April 2012 and finishes on 31st March 2015.

Abstract

Urban security is a complex multi-dimensional process that results from the interaction of an increasingly diverse collection of stakeholders. Many factors influence urban security, including the physical layout to the social and economic makeup of urban zones. Enhancing urban security is a complicated problem: causes of crime and social tensions are often unclear and hard to isolate. Furthermore, policy and intervention design processes can be messy and prone to biases because of time and resource limitations, high expectations and involvement of many stakeholders. There is also a common challenge to trace the effects of interventions. We are also faced with limited use of available sources of evidence, such as data, established knowledge and proven practices.

Europe has seen many severe instances of urban unrest in recent times but also the rapid expansion of urban environments with new types of communities through for example migration and the economic crisis. These developments underline the need to understand the factors and their interaction which impact on urban security throughout Europe in order to enable enhanced policy development to create safer urban environments and prevent undesirable security scenarios.

Approach

The BESECURE project works towards a better understanding of urban security through examination of different European urban areas. BESECURE *collects and analyses best practices* in the area of urban security through case studies in eight urban areas within Europe and literature review. By building a *comprehensive set of indicators for urban security,* along with consideration of best practices from different urban areas, important cues about the state of security in urban regions using factors such as social makeup, economic state, crime numbers and the public perception of security become apparent. The eight urban area case studies are: Belfast (UK), London Tower Hamlets (UK), London Lewisham (UK), The Hague (NL), Poznan (PL), Freiburg (DE), Arghilla (IT), Napels (IT).

BESECURE objectives:

- Knowledge – develop a knowledge base on the state of the art in urban security enhancement, identify problems and examine best practices.
- Understand – facilitate an understanding of how context factors influence the security of an urban area.
- Develop – develop a suite of tools and methods to aid policy makers.
- Transfer – transfer knowledge on different methods to assist policy makers in enhancing urban security.

Stephen Crabbe

Stephen Crabbe is the managing director of Crabbe Consulting Ltd. He is an expert in initiating and managing multi-disciplinary RTD projects having worked since 1997 with the European framework programmes 4 to 7 and now Horizon 2020.

e-mail: **stephen.crabbe@crabbe-consulting.com**

CCLD, Allerheiligenstr. 17, 99084 Erfurt, Germany

Based on this valuable knowledge, BESECURE is creating *a resource database that supports local policy makers to assess the impact of their practices and improve their decision-making*. One of the core aims of BESECURE is to create an accessible and communicable background of knowledge that enables policymakers to assert why their policies will be successful, what their impact will be in the long term and how the effect of the policies can be assessed. BESECURE will not however prescribe policies or automate the policymaking process.

Figure 1: Screenshot of BESECURE Platform Interface

BESECURE uses an iterative concept development and experimentation (CD&E) approach, consisting of several cycles that are used to continuously develop test and refine the knowledge and materials that emerge throughout the project. At the start of a cycle, the results and conclusions of the previous cycle are incorporated into the working material. This leads to gradual refinement. Through continuous empirical evaluation sessions, the results are geared towards practical use and are rooted in the everyday practices of our study areas.

In implementing its objectives, BESECURE develops a versatile support platform that provides information, inspiration and innovation to policymakers, consisting of three integrated platforms that help build strong evidence-bases for policy proposals (Fig. 1).

1. Inspirational Platform

The Inspirational Platform contains a wide range of material that is inspiring for policy design or initiatives to address different types of crime and instability in the city (Fig. 2). It encourages policy makers to look at the bigger picture and explore how a wide range of contextual factors, from the quality of city streets, to the provision of education, or the level of investment in an area, interact to influence for example crime and anti-social behaviour. The platform helps frame ideas and direct policy makers to real life approaches that have worked to reduce crime and instability in similar situations from other European best practices. The Inspirational Platform also assists policy makers to get in touch with experts involved in the design and implementation of urban security enhancement approaches.

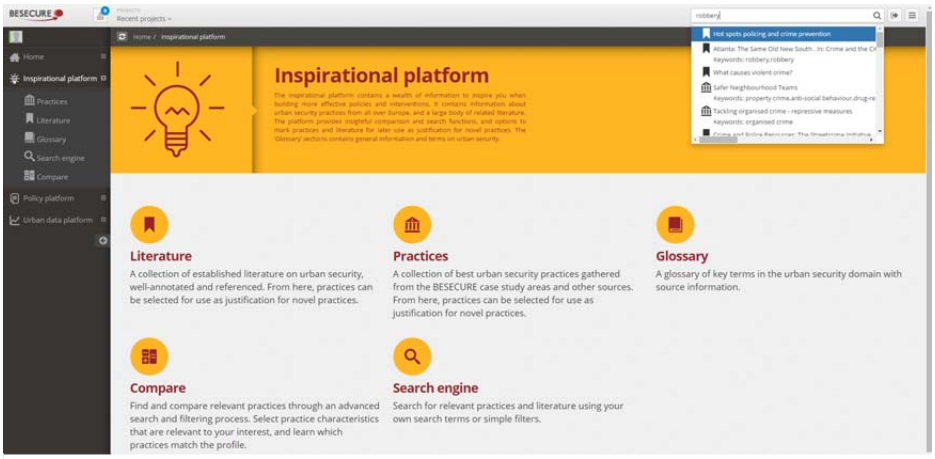


Figure 2: Screenshot of the Inspirational Platform

2. The Policy Platform

The Policy Platform guides policy makers through a comprehensive process to identify some of the most promising solutions for the security challenges in their areas (Fig. 3). The steps challenge policy makers to explore what is needed and some different options to reach their objectives. The steps in the policy support process draw from the other BESECURE tools (the Inspirational Platform and Urban Data Platform) to combine data and experiences from the relevant area with information from other cities across Europe. The results of the Policy Platform include a one-page policy of the most important evidence and promising findings to support the decisions (Fig.4).

3. Urban Data Platform

Urban data is a powerful asset in the development of urban security interventions. However, policy makers normally use just a fraction of the data that is available and typically do not take full advantage of the information that data can provide. The aim of the Urban Data Platform is to provide easy-to-use and understandable visualization to generate specific area profiles. These are visualised in geographic information system (GIS) maps, graphics and tables to enable accessible and relevant interpretation (Fig. 5). GIS is a powerful analytical tool for informing on the choice of sites for interventions and a reporting mechanism for effective and efficient communication with decision makers and relevant stakeholders.

Figure 3: Screenshot of Policy Platform

Figure 4: Example of One Page Policy

The BESECURE team works closely together with stakeholders (city councils, citizen groups, and social organisations, domain experts) to identify relevant and practical practices, indicators and measures that convey information about the state of security in an urban area and that can be used by other policymaker stakeholders to improve their decision making. By structuring this body of knowledge and making it accessible to further practitioners, BESECURE essentially provides an evidence-base for policymakers.

BESECURE is at present focussed on the urban security issues of general crime and instability its integrated platform approach could however be extended towards critical infra-structure.

The Partners

TNO (The Netherlands), UU (United Kingdom), EMI (Germany), ALU (Germany), ITTI (Poland), SLCT (United Kingdom), FAC (Ireland), JVM (United Kingdom), CCLD (United Kingdom), CNR (Italy), UMRC (Italy), EXP (The Netherlands), VJI (The Netherlands),

More information

If you would like to know more about BESECURE please visit our website at http://www.besecure-project.eu/ or our Facebook and Twitter accounts @besecure_fp7

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 285222.

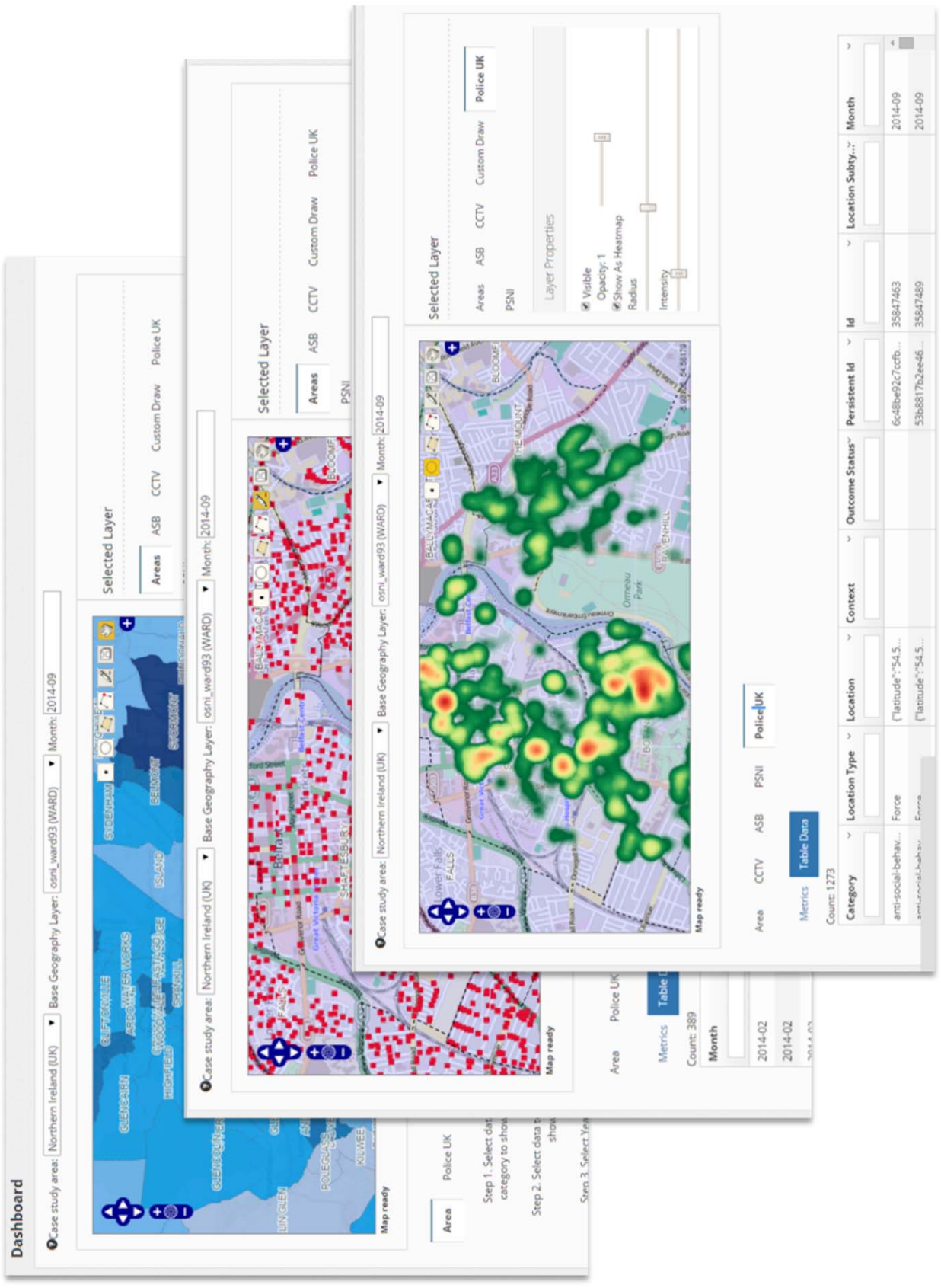


Figure 5: Screenshot of Urban Data Platform with GIS

Societal Resilience

Socio-economical consideration of resilience requires including social-dynamic based collective will in planning. Forming this will is essential for acceptance.

Specific challenge

Resilience to crisis and disasters is a topic of highest political concern. It concerns both man-made threats (accidents, terrorism) and natural hazards (e.g. floods, storms, earthquakes, volcanoes and tsunamis).

Resilience reflects a fundamental aspiration of the human being: continuing to live and adapt in and after a traumatic environment. The term covers different meanings depending on the disciplines and areas of activity to which it refers etymologically or has been adopted by analogy. Homeland security has naturally adopted this term making it a strategic goal for the achievement of which States and all segments of the civil society must organize themselves to be able to act collectively in a highly interconnected and media oriented world, where every major crisis quickly creates large consequences.

The term "resilience" originated in the 1970s in the field of ecology from the research of C.S. Holling, who defined resilience as "*a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables*" (Holling, 1973, p. 14). Clearly Resilience should address the capacity of an organization (both public or private) to be able to limit the effects of a destruction or malfunction of critical activities to a maximum acceptable outage level or maximum tolerable period of disruption, taking into account the existing or created interdependencies, in order to maintain a minimum predefined business continuity objective and to restore the activity to an acceptable level within a predefined timeframe.
This approach (consistent with the ISO standards 22300 series and the organizational resilience) needs to add the societal dynamics and societal impacts in order to safeguard societal objectives. This addition highlights the existence of a social dynamic based on a collective will through which it is possible to mobilize resources in an organised manner in order to meet immediate needs, bearing malfunction or destruction of essential resources, and to guarantee the "*socially acceptable*" level of functioning to an organization, an industry or an entire country.[1] It requires a collective approach that brings the State and civil society to organize collectively by developing four capacities that are developed further down:

- **Risk management, interdependencies analysis and business continuity planning** through a cost/benefit process performed upstream and adapted to the context, which can be evaluated through key performance indicators;
- **Interoperability in crisis management**, including semantic, communication and systems interoperability, interoperability of command and control, organizational interoperability, as well as mass notification of the population;
- **Effective collaboration between all stakeholders**, with the definition of the minimum level of information that must be shared (before, during and after a crisis) and a culture of communication, listening, deliberation, aversion for the "*misleading apparent consensus*", warning, mobilization of people, and regular feedback, allowing progress.

[1] This understanding is supported by the French definition. The Government White Paper on Defence and National Security has defined Resilience as "the willingness and ability of a country, society and government to withstand the consequences of an attack or major disaster, and then quickly restore their ability to function normally, or at least in a socially acceptable way. In Livre Blanc pour la Défense et la Sécurité Nationale, juin 2008, page 64 http://www.ladocumentationfrancaise.fr/rapports-publics/084000341/

Alain Coursaget

is the President of ACCESS2S Risk Management consulting firm for the last 2 years. He managed major projects on risk and crisis management, including the writing of guidance to business continuity plan that has been disseminated by the French Prime Minister Office and the elaboration for the EC of a roadmap for the European Standardization concerning interoperability in Crisis Management.

For the previous 10 years, Alain Coursaget had been Deputy Director for the State Protection and Security at the French Prime Minister's General Secretariat for Defense and National Security (SGDSN).

alain.coursaget@orange.fr

ACCESS2S 13 rue Guynemer 78150 Le Chesnay, France

www.cercle-k2.fr/users/single/296/Alain-Coursaget

Agile Management of crisis in uncertain situation

Collectively built responses can contribute to the reduction of uncertainty, the improvement of the decision making process and the allocation, the mobilization of resources according to priorities, the coordination efficiency as well as better monitoring of actions and to maintain agility in a changing environment.

While the term 'resilience' is also described, in a more "technical" approach, as "*the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.*" (UNISDR, 2009), it is necessary to break down and practically apply this definition to the different security sectors or domains. Resilience concepts namely need to be developed for critical infrastructures (supply of basic services like water, food, energy, transport, housing/ shelter, communications, finance, health), but also for the wider public to integrate and address human and social dynamics in crises and disaster situations, including the role of the population, the media, rescuers (staff, volunteers and ad-hoc volunteers) at the community, regional, national and International levels. Resilience concepts need also to take into account the necessity to anticipate, to plan and to implement in the crises time a substitution process aiming to deal with a lack of material, technical or human resources or capacities necessary to assume the continuity of basic functions and services until recovery from negative effects and until return to the nominal position.

Moreover, as resilience management and vulnerability reduction are closely related, it is necessary to link the on-going efforts and approaches with relevant resilience management approaches, to ensure that risk assessment is followed by the development of resilience concepts in the various security sectors or domains, based on the results of the risk management and treatment.

The scope of societal resilience

The scope of societal resilience needs to cover risk management, interdependencies analysis, business continuity planning, interface and crisis management, collaborative processes, governance practices and societal decision-making. Linkage with the EU Risk Assessment Guidelines[2] can be useful.

Based on experience and previous research, it is more efficient to address resilience at a small organization level, where inter-dependencies that can be more easily managed, and aggregate it at a city, regional or national level, including societal objectives.

It is important to identify the driving forces or obstacles (e.g. awareness, training, guidelines, legal frameworks, standards, financing, etc.) which can be adapted to one or more of the above mentioned critical infrastructures, domains and/or the public and assessed regarding their potential to serve as a basis for resilience assessment and implementation.

> The existence of a social dynamic based on a collective will through which it is possible to mobilize resources in an organised manner makes it feasible to guarantee accordingly the "socially acceptable" level of functioning to an organisation, an industry or an entire country.

Societal resilience needs to cover three major types of stakeholders:

- The Public Authorities, given their importance in preparedness, major decisions making, communication, allocation of scare resources and crisis management,
- Critical Infrastructure Operators, which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people; the possible disruption or destruction of which having a significant societal impact as a result of the failure to maintain those functions, and
- The General Public, whose active participation is more and more critical for the societal cohesion.

[2] SEC(2010) 1626 final, Risk Assessment and Mapping Guidelines for Disaster Management http://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

Concept and approach

As explained earlier, resilience assumes the existence of a social dynamic based on a collective will through which it is possible to mobilize resources in an organized manner in order to meet immediate needs, bearing malfunction or destruction of essential resources, and to guarantee the "acceptable" level of functioning to an organization, an industry or an entire country. It requires a collective approach at the local, regional, national and European level, according to the dimension of the crisis, which brings the public authorities, private organisations and civil society to organize collectively by developing four capacities:

1. Risk management, interdependencies analysis and business continuity planning

Risk management, interdependencies analysis and business continuity planning are performed upstream, and adapted to the context, which can be evaluated through key performance indicators. Planning ahead is needed to get prepared and have contingency plans at the individual level and at the collective level. For an organization, it is the object of the business continuity plan in order to reach the best cost / benefit objective. Business continuity planning, combined with analysis and risk management, allows the best decisions for security investments within a constrained budget. It must also take into account the management of interdependencies to understand, avoid and mitigate cascading effects. The upstream preparation, however, should not lead to a set of rigid work. A good plan should indeed be seen as a toolbox for rapid response, quick procedures and organizations adjustments to fit a specific situation and context.

2. Interoperability in emergency / crisis management

Interoperability in emergency / crisis management includes semantic, communication and systems interoperability, interoperability of command and control, organizational interoperability, as well as mass notification of the population. This topic has already been addressed by the EU Mandate M/487 [3]. It is necessary to improve interoperability between stakeholders, to enable the organization to better know its environment (the missions of the various entities and partners, updated directories, having right points of contact using a model of organizational crisis management structure to facilitate organizational interoperability, etc.), to have communication tools (available and interoperable means of communication, including in secure mode), to understand each other (semantic interoperability, interoperability of map and iconic information, interoperability of models and information systems) and to help each other (interoperability of means, resources and command systems). Interoperability facilitates network operation, and the use of specific tools (mapping, simulation, decision support in an uncertain environment). It also facilitates mobility and intervention of experts, at local, national and international levels.

Interoperability with the general public means to reinforce citizen and local territorial community awareness and involvement with increased knowledge of risks and available channels for information and advice for appropriate actions (before, during and after the incident / emergency) and for warning (alert and notification) dissemination understanding. It requires training of end-users and the general public for better reactions during disasters; developing improved reporting and mass warning systems, ways of acquiring digital information from victims/public and sending it to the whole command & control system, and procedures in order to let citizens actively bring in their resources into the relieve effort.

[3] Mandate M/487 to Establish Security Standards, Final Report Phase 2, Proposed standardization work programmes and road maps http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/default.aspx

3. Effective collaboration between all stakeholders

Effective collaboration between all stakeholders, with the definition of the minimum level of information that must be shared (before, during and after a crisis) and a culture of communication, deliberation, aversion for the "misleading apparent consensus", and regular feedback, allowing progress. If interoperability provides the container and the links, there must also have content and therefore the desire to communicate, listen and share information. But every organization has sensitive information, the sharing of which can cause problems (competition, loss of autonomy, creating vulnerabilities, etc.).

Societal resilience assumes the existence of a social dynamic based on a collective will through which it is possible to mobilize resources in an organized manner in order to meet immediate needs to guarantee the "acceptable" level of functioning to an organization, an industry or an entire country. It requires a collective approach which brings the public authorities, private organisations and civil society to organize collectively

It is therefore useful to define the minimum level of information that must be shared. This applies equally between the partners (public / private) organizations, between public authorities and citizens when these are intended to be actors of resilience. This also applies to the detection of weak signals to anticipate an emergency/crisis situation and the management of vertical and horizontal information flows. In the latter case, the organization of the communication must limit human filters that delete, often unconsciously, important information (as embedded in a large flow of messages), and must enable expert advice to help decision-making.

4. Agile Management of emergency/crisis uncertain situation

Collectively built responses can contribute to many positive aspects, such as reducing uncertainty, bringing better decision making, maintaining agility in a changing environment, allowing better allocation of resources according to priorities and greater coordination efficiency, as well as better monitoring of actions. It applies at the level of local critical infrastructure operator as well as at the decision-making "Ops-crisis" centre at a State level. The uncertainty can be reduced, but rarely eliminated; command and control managers must know how to recognize and manage it in order to limit the consequences of a crisis, allow functioning in a degraded mode, better anticipate what may occur and restore normal activities. Good governance and organization of crisis management must be adapted to each situation (frequency of meetings based on the kinetics of the crisis and issues, people presence according to their potential contributions, etc.) and must include resilience objectives from the very beginning of the crisis. Finally, governance must overcome the usual management framework focusing on internal issues in order to take into account the effects of a crisis in the whole environment of the organization (impact on customers/users, but also on the state and civil society: citizens, national and foreigners).

Conclusion

In conclusion, societal resilience assumes the existence of a social dynamic based on a collective will through which it is possible to mobilize resources in an organized manner in order to meet immediate needs to guarantee the "acceptable" level of functioning to an organization, an industry or an entire country. It requires a collective approach that brings the public authorities, private organisations and civil society to organize collectively

18th IEEE Mediterranean Electrotechnical Conference

MELECON 2016 April 18 - 20, 2016, Limassol, Cyprus

Call for Papers, closing September 15, 2015

Aim & Scope

Melecon 2016 is an IEEE Region 8 flagship conference with a long standing history of excellence both in electrotechnology and in recent years in information and communication technologies as well. Melecon 2016 covers complementary thematic areas that hold great promise for the advancement of research and technological development in the solution of complex engineering systems. In this context, Melecon 2016 foresees to attract high quality papers and provide a platform for the cross fertilization of new ideas and know-how under the special theme of the conference that is Intelligent & Efficient Technologies & Services for the Citizen. To achieve this, the conference encompasses the following thematic areas:

Themes and Theme Chairs

Conference chairs

C. Pattichis, Univ. of Cyprus, Cyprus
E. Kyriakides, Univ. of Cyprus, Cyprus

Electric Power Systems and Renewable Energy Sources

Chairs: A. Poullikkas, Cyprus University of Technology, Cyprus
C. Sourkounis, Ruhr-University Bochum, Germany

Information and Communication Technologies

Chairs: S. Louca, University of Nicosia, Cyprus
D. Banciu, National Institute for Research & Development in Informatics, Romania

Internet of Things, Cloud-Based Systems and Big Data Analytics

Chairs: C. Mavromoustakis, University of Nicosia, Cyprus
G. Mastorakis, Technological Educational Institute of Crete, Greece
C. Dobre, University Politehnica of Bucharest, Romania

Virtual Environments, 3D Simulations & Serious Games

Chairs: D. Michael, Cyprus University of Technology, Cyprus
P. Charalambous, Inria Rennes-Bretagne Atlantique, France

Security and Networking

Chairs: V. Vassiliou, University of Cyprus, Cyprus
S. Sargento, Institute of Telecommunications, University of Aveiro, Portugal

Micro & Nano Electronic Systems

Chairs: J. Georgiou, University of Cyprus, Cyprus
A. Fish, Bar-Ilan University, Israel

Smart, Green and Integrated Transport

Chair: C. Panayiotou, University of Cyprus, Cyprus
N. Geroliminis, EPFL, Switzerland

Emerging Environmental Systems & Applications

Chairs: A. Paschalidou Democritus University of Thrace, Greece
A.N. Skouloudis, European Commission, JRC, Italy

DEMOCRITE: Demonstration of a Risk coverage Engine on a Territory

The goal of the French ANR DEMOCRITE is to provide a solution for dealing with risk coverage of the French Firemen of Paris.

The DEMOCRITE project is a new research project of the French national Agency ANR. It belongs to the category «Concepts, Systèmes et Outils pour la Sécurité Globale (CSOSG)» which means «Concepts, Systems and Tools for the Global Security». DEMOCRITE has started on March 1st 2013 for duration of three years.

Abstract

DEMOCRITE is a software platform which integrates tools for the analysis and coverage of risks on a territory. It could be used in cold planning mode or in crisis management, and will be used to optimize the rescue response (nature, number, location) given a risk coverage level agreed by the Authority. Some tools will be tested on a limited territory (2,5 km²) but the extension at larger scale will be studied. These tools are meant to map risk probabilities and potential consequences as well as intrinsic vulnerabilities. Techniques for the optimization of resources will be studied.

Models for the development of complex risks:

These low probability risks imply a level 3 operational answer. They are likely to cause large scale consequences and may require the engagement of numerous vehicles and crews. DEMOCRITE tackles two risks: urban fire and explosion. Others (flood, epidemic...) will be studied in a future version. Fire propagation will be based on an urban representation given by a GIS. The propagation will be handled by a cellular automaton whose transition rules will be based on numerical simulations. A local model will be able to replicate the different phases of an indoor fire for different kinds of buildings. Explosion effects (accident, bombing ...) will be first computed.

Simplified approaches will be tested against the reference results in order to select the best one for DEMOCRITE. The explosion will be allowed to be either the cause or the consequence of a fire.

Risk propensity maps:

High probability risks (such as first aid to persons, representing more than 80% of the BSPP actions) may require a level 1/2 operational setup. The analysis of past events shows that risk propensities are far from being isotropic. Optimizing risk coverage thus requires a precise mapping of risks. The aggregation of unitary risks will be studied. Experience feedback will be coupled to statistical approaches in order to predict land use planning impact on territory risks. For instance, car-crash intervention statistics are not sufficient to predict risk evolution due to the creation of new roads: they must first be correlated to other data (traffic density, average velocity, meteorological conditions, etc.).

DEMOCRITE aims to provide an integrated platform for risk analysis as operational decision support system. A first restricted area will be studied during the project and extension to a large-scale up will be studied. The intrinsic vulnerabilities, giving the potential consequences of an adverse phenomenon will also be mapped. DEMOCRITE addresses two risks (fire and explosion) and involves urban GIS environment (urban geometry).

Emmanuel Lapebie

Emmanuel Lapébie (coordinator) is a senior expert at CEA-Gramat and works in the areas of physical explosives and terms unsteady sources. He holds an engineering degree from ENSTA Bretagne, Pyrotechnics Chemistry option and a Master of Fine Chemistry / Theoretical Chemistry

e-mail: emmanuel.lapebie@cea.fr

CEA,DAM,GRAMAT,
F-46500 Gramat, France

The functional vulnerability, describes the functions (government, education ...) performed by a society and how they could be threatened. These functions rely on mappable items. Sometimes the localization of a vulnerable item (a transformer substation) may differ from the affected zone in case of failure (a whole district). Human and functional vulnerabilities will be mapped, and the vulnerability of networks will be tackled. Theses operational maps will aid in decision making (priority evacuation zones, safety perimeters ...).

Intrinsic vulnerability map

Intrinsic vulnerabilities are linked with the characteristics of a territory. They may also vary with space and time. For instance, public access buildings with a high density of people (stadium during a sport meeting) will increase the local human vulnerability during a few hours.

Objectives

The DEMOCRITE project aims to develop an operational tool, providing assistance to cold or warm planning phase. It targets to model complex risks (such as the spread of a fire or explosion in urban areas) must be made at the appropriate level to ensure accuracy of the results. We associate this "upstream" scientific work and operational experience feedback

1- The innovative principle of DEMOCRITE project is based on the scientific work to ensure an accurate risk mapping. It involves the lessons learnt capitalized by the Paris Firefighters (BSPP, Brigade des Sapeurs Pompiers de Paris (500 000 interventions per year). Simplified models that will result will have a solid physical basis and adequately represent the phenomena observed in the field.
The demonstrator must raise a number of scientific and technological obstacles to demonstrate the importance of developing an operational tool on this basis:

- Ability to take into account the complex and dynamic risks, using a rigorous mathematical formalism (lifting of scientific barriers).
- Ability to handle multi-source data, multi-format to assess current risks (lift locks on the processing of information).
- Interoperability with other formats, platforms and tools, dialogue between multiple tools within DEMOCRITE, synthetic presentation of specified outcomes to achieve the operational functions (lifting of integration locks).
- Ability to treat analysis and coverage of risk in a legal and regulatory defined framework (lifting of use locks).

2. The risk analysis part is addressed by the development of tools dedicated for "cold" or "hot" planning. Advanced tools to optimize risk coverage will be studied in task 10 (generalization) by INRIA / X.

The scientific dimension of DEMOCRITE project is organized in a detailed framework.

- With respect to the state-of-the-art, there is not, to our knowledge in France fast simulation of operational tools, simplified, realistic and not empirical for the propagation of an urban fire (Task 3), or urban explosion (Task 4) in connection with a GIS (Geographic Information System).

3- Intensive use of interventions experience feedback, coupled with multi-source data to develop an accurate risk mapping propensities (Task 5), is also an originality of the project. Mathematical approaches will be chosen according to the recommendations of the INRIA / X partner.
- The use of GIS-based tools to identify vulnerabilities maps (human, functional,) has been proposed for the first time by both partners ARMINES-LGEI and CEA-G. The extension of this approach (Task 6), will improve the spatial resolution of the results. It will provide information suitable for the assessment of the vulnerability of networks and critical infrastructure.

4. Finally, the ambitious nature of the project also depends on the features of the study area (the exclusive or shared competence area of the BSPP the number and the diversity of possible interventions, and the complexity of issues [BSPP 2011], [BSPP 2012]:

- Competence area covers 4 regions and three airports.
- The presence of multiple dense networks (transport, energy-related and information).
- The presence of numerous structures related to the functioning of the state.
- The resident population, which represents more than 10% of the French population.
- Defended the population, which includes many non-residents (tourists and others).
- The BSPP carries more than 200 types of different interventions, including rescue people (82%), technological and urban risk (12%) and the fight against fire (4%).

The Partners

- CEA Commissariat à l'énergie atomique et aux énergies alternatives
- BSPP Brigade de Sapeurs-Pompiers de Paris
- PPRIME Institut P' - UPR 3346 CNRS
- Société IPSIS
- Société SYSTEL
- ARMINES LGEI ARMINES Laboratoire de Génie de l'Environnement Industriel de l'Ecole des Mines d'Alès
- CERDACC Centre Européen de Recherche sur le Risque, le droit des Accidents Collectifs et des Catastrophes
- INRIA - EPI MAXPLUS Inira - Centre de recherche INRIA - Saclay-Île-de-France

If you would like to know more about DEMOCRITE please contact the coordinator through the address mail: anr.DEMOCRITE@gmail.com

"DEMOCRITE has received funding from the French national Agency for research; technological development and demonstration under grant agreement no ANR-13-SECU-0007".

POLE RISQUES – The INNOVATIVE CLUSTER ON RISK MANAGEMENT

"Pole Risques", the French cluster dedicated to research and technology in the field of security. Presentation of its organization and innovative activities on critical infrastructures security and crisis management

Pôle Risques is a cluster combining a network of 300 members and supporting various research and technology (R&T) projects in the field of security. It aims at helping industries and researchers to develop the best innovation, based on the user's needs and the potential developments in the market.

History and organization

Pôle Risques was created in 2005 by an initiative from the French government and the regions of the south of France (Languedoc Roussillon and Provence Alpes Côte d'Azur). Those last territories, regularly affected by both natural and man-made large disasters, decided to use these specificities to support the local expertise for disasters prevention, preparedness and response.

2005 ongoing Pôle Risques' network has grown, and now includes 300 entities. Involving initially the local research networks, it now gathers a large national network with only 60% members based in south of France, and an international network through partnerships with clusters or research centres. Pôle Risques works for example with EU-VRI (http://www.eu-vri.eu) in Germany on technological risk, and with the BNHCRC - Bushfire and Natural Disasters Collaborative Research Centre www.bnhcrc.com.au in Australia on large forest fire prevention and reduction. It continuously enlarges international networks through research cooperation with several entities or end-users.

This network enlargement is directed to and driven by its member's needs. Pôle Risques proposes them to work as a portal, able to provide and make the right connections for the best research and the best solutions developments.

Pôle Risques' network includes three types of entities: the academics, including research centres and universities, the industries and solution providers, with a large part of SMEs and start-ups, and the users, from plant and network operators, to public bodies (civil protection, police, local authorities, environment protection services).

In addition, Pôle Risques' network includes several members that propose experiments facilities and test beds, available for testing innovative security solutions: fire and rescue areas, crisis rooms, 3D based simulation platforms, drones and robots tests zones.

Pôle Risques is a cluster combining a network of 300 members and supporting various research and technology (R&T) projects in the field of security.

It includes testing of innovative security solutions: fire and rescue areas, crisis rooms, 3D based simulation platforms, drones and robots tests zones.

Several critical infrastructures operators work closely with Pôle Risques and propose their facilities as experimental platforms for testing security technologies. Pôle Risques' partnership offers the perspective to reinforce the collaboration between the users and the solutions providers and reduce feedback loop and time constraints for specifications integration and final validation.

Jean-Michel Dumaz

Security program manager at Pôle Risques and NCP for H2020 Secure Societies

jean-michel.dumaz@pole-risques.com

POLE RISQUES
Avenue Louis Philibert
13100 AIX EN PROVENCE
FRANCE

Research and Technology programs

The topics addressed by the Pôle enlarged progressively to reach the entire security field spectrum, from crisis management to climate change, and from infrastructures security, to human factors, except digital security.

Pôle Risques organizes its activities in several programs: Air Quality, Critical Infrastructures Protection, Civil Protection and crisis management, Environment protection and climate change. This paper focuses on the last three topics.

Pôle Risques' **critical infrastructures protections program** is dedicated to all the aspects of critical infrastructures security. It includes infrastructures design (facilities and process), inspection and maintenance, decommissioning, recycling of waste, and people safety. Pôle Risques supports several R&T projects in that program. These projects lead to concrete results. We can for example mention the development by the SME Alcrys of a new generation of fluid and control systems increasing the security in the gas installation; the experiments of inspection by drones in nuclear power plants, made by the SME Novadem; deconstruction planning and simulation software developed by the SME Oreka; new generation of gas detector and monitoring designed by the SME Nexvision; inspection optimization by the use of RFID tags, solution proposed by the SME Beweis.

In addition, Pôle Risques supports several projects based on platform developments. We will detail two examples of platforms:

- The Copernic platform, which was created by few partners, all experts in structure fire models. It aims at proposing a large expertise on fire and a panel of infrastructures dedicated to experiments. From small tests to house size test, the Copernic test beds could be used for all the experiments on material, PPEs, and extinguishing systems testing.
- The Air Quality platform, which was created in 2014 by a partnership coordinated by the Ecole des Mines d'Alès. It offers a global expertise and testing solutions on air quality, from monitoring to large evaluations and experiments.

> Pôle Risques is cluster supported innovation in Risk management.
>
> The Scope: is reaching from Air Quality, Critical Infrastructures Protection, Civil Protection and crisis management, Environment protection to climate change.

The Pôle Risques' **Civil Protection and Crisis Management program** aims at developing new solutions for responders and executive managers. It includes several R&T work items:

- New personal protective equipment designs, as technical textile, helmets, individual sensors and exoskeleton
- New response vehicles including unmanned ground systems
- New fire extinguishing solutions, including new foams concepts or water hoses
- New tools for situation evaluation and intelligence through videos and pictures analysis, video-mosaicking, big data and data fusion, social media tracking, new air surveillance platforms
- Sense-making research, based on human behaviours and cognition, in order to build tools and training solutions for response or crisis management teams resilience improvement
- Citizen and territories resilience trough training and learning, new emergency and warning technologies, new applications and new use of social medias
- New tools for response coordination, from teams tasking and localization, to response scenarios model and evaluation

I

n the last years, Pôle Risques supported for instance the following R&T projects :

- Target (H2020-FCT7): Serious Game for crisis management teams training
- INACHUS (FP7): tools for search and rescue operations
- Techforfire (FUI): Forest Fire monitoring by air surveillance, fire behaviour modelling and damage evaluation
- Extrem_owl (FUI): new generation of helmets for helicopters night flight
- Ambucom (FUI): connected ambulance
- SOSPedro (FUI): localization of people in emergency by drones
- DIDRO (FUI): Dams monitoring by drones

In addition, Pôle Risques was involved in the project conception and pre-evaluation phase for French drones detection and interception R&T call. Five projects have been supported in order to propose solutions for critical infrastructures protection again these emerging threats.

The civil protection and crisis management program involves a large panel of end users including the National Fire Officer Academy, the National CBRNE training centre, the National Natural Disasters training and research centre, Fire and Rescue and Police services, command and coordination centres, NGOs.

These partners propose a large panel of facilities that are available for experiments hosting. It includes firehouses, car crash areas, CBRNE platforms, UAV air space, operational centres, 3D based simulation platforms. These facilities can be interconnected in order to provide a large experiment site and they provide access to key and ad hoc experts, dedicated to each project.

How Pôle Risques organizes the R&D support?

The SMEs and laboratories or the users generally initiate the projects. However, Pôle Risques seeks to bring out new R&T project by the coordination of national working groups and workshops. In 2014, Pôle Risques hosted two groups, the first focusing on new air solutions, drones and balloons and the second on emergencies management solutions. After a few months those groups produced recommendations and requirements to identify more clearly the technological development's needs.

The third Pôle Risques program is dedicated to **environment protection and climate change**. It includes innovative technologies for natural disasters prevention and protection solutions. The associated R&T projects cover the design of new sensors for

weather analysis, improvements of weather forecast, extreme events prediction and evaluation systems. Some example of applications:

- SAVaS® : a model for rogue waves prediction worldwide developed by Noveltis
- HYDRIX® weather radar developed by NOVIMET for the rainfall measurement instead of rain gauges
- AirFireTRACK®: Lidar and sensor-based system developed to current state and forecast of local meteorology, used for forest fire smoke plume contamination evaluation.

Pôle Risques in the DRIVER-EU project

Pôle Risques is involved in the DRIVER-EU project implementing the Aftermath Crisis Management System-of-Systems Demonstration Programme funded under the FP7 by the European Commission.
DRIVER activities focus on two main dimensions:

- Propose a pan-European test-bed enabling the testing and iterative refinement of new crisis management solutions
- Integrate a Portfolio of Tools that improves crisis management at Member State and EU level

> Pole Risques involves a comprehensive panel of end-users and experts in order to design efficient solutions for environment protection, public safety and infrastructures resilience.
>
> Pole Risques has the philosophy of efficiency for a safer and more sustainable world.

The project covers the following topics:

- Civil resilience solutions: from individual to community resilience
- Evolved learning: harmonized competence and lessons learned framework; training for high-level decision making
- Recommendations for crisis management structures, governance, standards

Within the DRIVER framework, Pôle Risques contributes to the Test-beds specifications, design, organization and preparation, and to the experiment hosting, in a close cooperation with the end-users community.

In conclusion

Pôle Risques is a cluster that supports research and technology projects in the field of security. It involves a comprehensive panel of end-users and experts in order to design efficient solutions for environment protection, public safety and infrastructures resilience.

It aims at building a solid network of national and international partners working on the same topics, following the philosophy of efficiency for a safer and more sustainable world.

FEDERATED CONFERENCE ON COMPUTER SCIENCE AND INFORMATION SYSTEMS

Lodz, Poland 13-16 September, 2015

Call for Papers:

The FedCSIS Events provide a platform for bringing together researchers and practitioners to present and discuss ideas, challenges, and new solutions in computer science and information systems. Topics of interest are defined by Events constituting FedCSIS and listed on **http://www.fedcsis.org**
The papers should be submitted to the chosen Event by April, 24, 2015 using the FedCSIS submission system available at **http://www.fedcsis.org**

Accepted and presented papers will be published in the IEEE Xplore Digital Library proceedings entitled "*2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*". Because the IEEE proceedings will be published under nonexclusive copyright, the Events' organizers will endeavor to arrange quality journals, edited volumes, etc. and will invite extended and revised papers for post-conference publications.

INDUSE-2-SAFETY - QUANTIFYING SEISMIC RISKS IN PETROCHEMICAL PLANTS

The aim of INDUSE-2-SAFETY project is to develop a quantitative risk assessment methodology for seismic loss prevention of "special risk" petrochemical plants and components.

Abstract

The INDUSE-2-SAFETY (***Component Fragility Evaluation and Seismic Safety Assessment of "Special Risk" Petrochemical Plants under Design Basis and Beyond Design Basis Accidents***) project aims to develop a quantitative risk assessment methodology for seismic loss prevention of "special risk" petrochemical plants and components, e.g., support structures, piping systems, tanks and pressure vessels, flange and Tee joints. The proposed probabilistic-based methodology will ensure safe functioning / shutdown underground motions of increasing spectral acceleration through analytical, FE and experimental investigations. Finally, related harmonized importance factors γ_I and limit state probabilities will provide a uniform hazard versus a uniform risk for EN 1990/EN 1998.

Consortium

The Consortium of INDUSE-2-SAFETY consists of the following 9 partners:

1. University of Trento, Italy
2. Centro Sviluppo Materiali Spa, Italy
3. Commissariat à l'Energie Atomique et Aux Energies Alternatives, France
4. Rheinisch-Westfälische Technische Hochschule Aachen, Germany
5. University of Thessaly, Greece
6. University of Roma Tre, Italy
7. The University of Liverpool, UK
8. Walter Tosto Spa, Italy
9. Ing.-ges. Dr.-Ing. Fischbach mbH, Germany

Objectives

1. INDUSE-2-SAFETY intends to achieve the following main goals: Quantification of actual risk for seismic loss prevention of potentially dangerous "special risk" petrochemical plants.
2. Development of a Seismic Probabilistic Risk-based Evaluation (SPRE) procedure capable of providing damage exceed occurrence frequency for a representative prototype case study of a "special risk" petrochemical installation.

INDUSE-2-SAFETY aims at developing a probabilistic quantitative risk assessment methodology for seismic loss prevention of "special risk" petrochemical plants and components, e.g., support structures, piping systems, tanks and pressure vessels, flange and tee joints, etc.

Grant Nr.: RFS-PR-13056

3. Evaluation of fragility curves of main structures and components needed for the SPRE analysis, e.g. for support structures, piping systems, tanks, slim vessels, vertical cylinders, spherical storage tanks, flange and tee joints, etc.
4. Experimental investigation of steel storage tanks without/with floating roofs, piping network substructures, flange joints and tee joints by means of cyclic, real-time/pseudo-dynamic and shaking table tests.
5. Issuing of risk assessment provisions for seismic loss prevention of onshore "special risk" petrochemical facilities within the scope of EN 1998.
6. Enhanced design recommendations for the improvement of several European standards and codes, including EN 1990, EN 1998, EN 13480-3 and EN 1591.

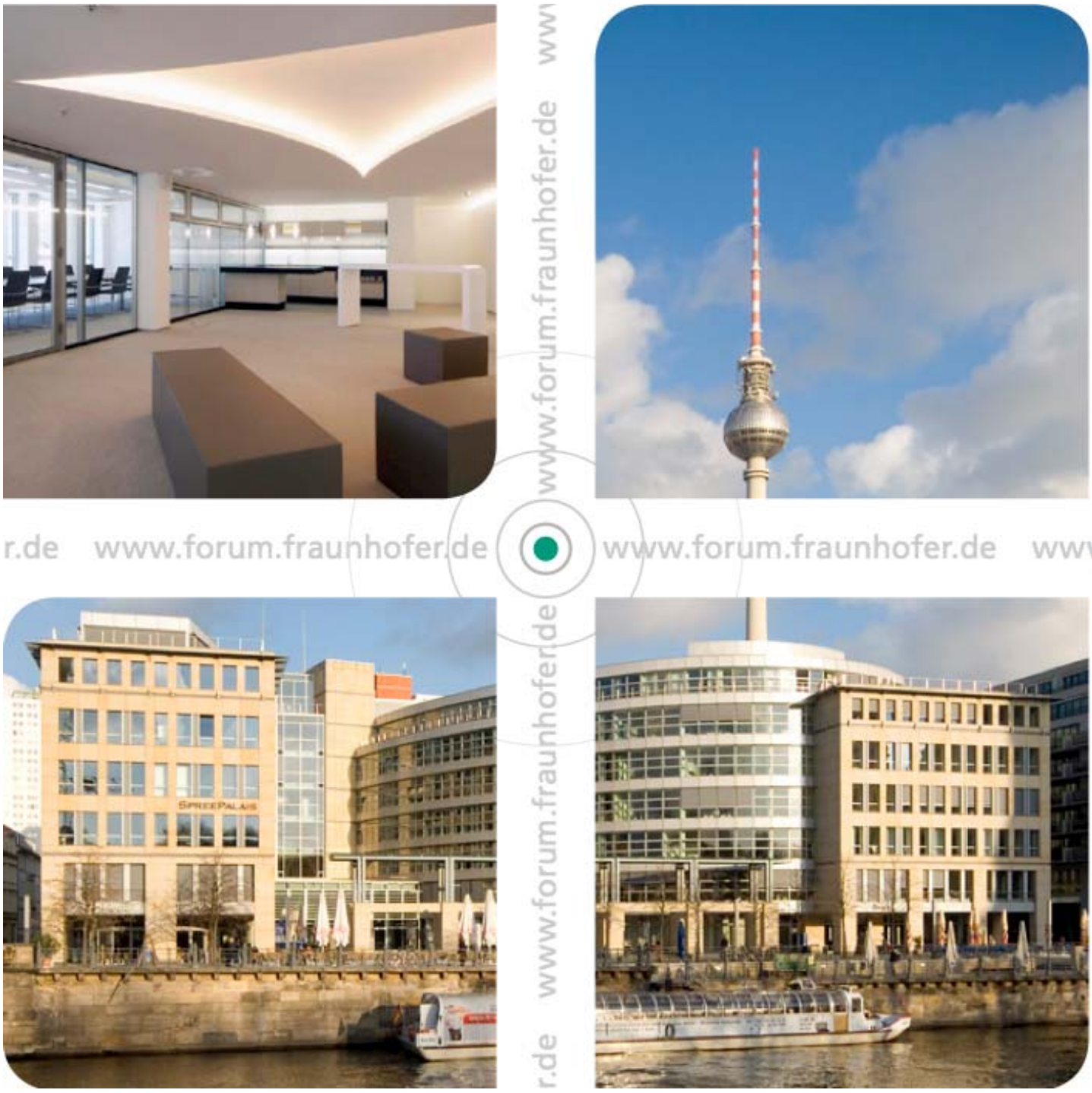
Oreste S. Bursi

Dr. Oreste S. Bursi is a Professor at the University of Trento – Italy. He graduated in Mechanical Engineering at the University of Padua, and earned his PhD in Mechanical Engineering at the University of Bristol, UK. The research activity is mainly devoted to the pseudo-dynamic test method, non-linear dynamics, control, structural identification and seismic risk assessment of industrial plants.

e-mail: oreste.bursi@unitn.it
www.ing.unitn.it/~bursi
http://r.unitn.it/en/dicam/nhmsdc

Project-website
www.induse2safety.unitn.it

CRITIS 2015 – 10th International Conference on Critical Information Infrastructures Security



Where CRITIS 2015 will take place: see **www.critis2015.org**

Driving vendor security capability in readiness for a more complex world

Regulators, governments, buyers, consumers and the ICT industry must challenge each other to drive increases in the inherent security of vendor products ahead of the product or service that they launch

Imagine a future world

Imagine a world in ten years' time Telecommunications continues to become more and more widespread as we connect the next billion citizens, and then the next. The concept of the Internet of Things becomes more real as "devices" connect to "devices" and people to everything.

A range of sources from Informa, IDC, Huawei, Gartner and ovum *et al.* make various growth predictions. Imagine two times more Internet users; imagine twenty times more data or ten times more cloud services; imagine ten times faster broadband speed and five times more smart devices.

Imagine a world where we have moved from a position where there is "an app for that" to a position of "an API for that" – anyone can connect almost anything to anything.

Superimpose on top of this the rise of big data, smart devices, smart applications, smart networks, smart grids, smart cities and probably not, but it is worth mentioning, a smarter world, all interplaying with each other.

Imagine an economic world that has also been changed by this technological rampage through every walk of mankind – the existing rich might not be so rich, the existing poor and less developed might be richer and more developed. Global supply chains based on major continents continue to become fragmented to countries, regions, cities and handfuls of crowd sourced entrepreneurs. With big data we have more open data. With open data we have more open source software, open applications, open frameworks, open standards and open communities all disrupting the "old ways" of doing business.

It isn't just the technology that will have changed, so will the leadership style of many businesses – from generation X to generation Y and maybe the first fruits of pressure from generation Z all impacting on business models, decision making, collaboration and approach to risk.

Economically will margins be wider? Unlikely as competition tends to drive margins lower. Will competition be less? Unlikely as the "new world" will enable more start-ups from any location with the best talent, the lowest taxes, and the greatest entrepreneurial culture to thrive.

Finally will technology security be any more effective? Will we be able to secure critical infrastructure, or any other infrastructure, more comprehensively than we can today? Unless we change our approach this will only be in our dreams, but why is this?

Imagine a world where we have moved from a position where there is an "app for that" to a position of "an API for that" – anyone can connect almost anything to anything.

The Security Challenge

When we look around today it is fair to say that almost everything we see has been shaped by the combination of Governments, regulators, vendors and consumers continuously improving the products and services that we use.

Your trip to your home or office today regardless of by car, bus, cycling, and yes even walking has sustained many years of functional and safety innovations and improvements.

John Suffolk

John Suffolk joined Huawei Technologies in 2011 and is the Global President of Cyber Security and Privacy based in China. His role is to work across the whole company, the supply chain, with customers, Governments and regulators to improve the inherent security design , development and operation of all Huawei's products and services in 170 countries.

Prior to this he was the Chief Information Officer in the UK for Her Majesty's Government supporting three Prime Ministers in the creation and execution of the technology and transformation strategies for the UK. He was the UK Government's Senior Information Risk Owner having accountability for the security and protection of a range of Government assets.

He has been a Chief Information Officer three times a Customer Services Director; an Operations Director and a Managing Director of a retail financial services organisation accountable for $US 30bn of assets

e-mail: **john.suffolk@huawei.com**
www.huawei.com

The room you are in has been shaped by health and safety considerations on maximum room size versus the size of the exits to allow a timely escape in the event of an incident.

The materials to build and furnish the room are tested for structural, wear, chemical and fire protection and performance. But what has not gone through the same improvements is the security in the technology you are using or connected to. Your mobile phone, your tablet, your computer - They have gone through enormous technical changes, enormous, functional changes, and enormous cost improvements but sadly security has not followed this same improvement curve.

Consider this when you purchased your phone or almost any technology nowhere did it state any warning about security of your personal details or protection of your identity. Nowhere would you have been able to find a commonly accepted certificate of security conformity or security testing. Electricity – yes, environmental waste disposal probably, security, absolutely not.

How did we get ourselves into this position?

We should stop and ask ourselves why technology security has followed a different improvement trajectory to almost everything else in life.

- First is the pace of change. It is sometimes hard to comprehend how technology has changed in such a short amount of time. The shelf life of products is short; the effects of Moore's law can be seen everywhere and because of this the cumulative impact of innovation built on innovation is breath-taking
- This cumulative innovation impact makes technology more usable, more comprehensive, more available and at the same time a lot more complicated – simplification for the end-user equals increased complication for the technology vendor – and increased complexity does lead to increased security risk
- Ubiquity has led to complacency. Today we take technology for granted. We do not really consider the power of what we are using, the interconnectedness of the device, the global supply chain that delivered the device and the experience and nor do we consider the amount of hands and prying eyes who have the ability to interact with our technology and the data we store in ways that pose threats to citizen, enterprises and countries.

All of this has led to a lack of comprehensive knowledge of the technology by policy makers, regulators, buyers and users of technology. This lack of knowledge on how technology has been built, or should be built and what good security looks like leaves the buyer, whether it is a consumer an enterprise or a government helpless in determining the good from the bad.

This is not a criticism of individuals but a statement of the inherent complexity of the end-to-end ICT ecosystem – there are few experts with end-to-end knowledge and experience

.

> What is missing in technology is the knowledge of policy makers, regulators and buyers of technology to make informed decisions about security

What is missing in technology is the knowledge of policy makers, regulators and buyers of technology to make informed decisions about security. This lack of knowledge manifests itself in the reality that few people are able to specify in any level of detail what security capability they want their vendors to have or build-in to the products and services they create. This in turn has not created the pressure on vendors to improve their security capability at a similar pace to that of functional, other quality and cost improvements – hence the divergence that has been created over many years.

In summary if no one asks vendors about detailed security requirements then generally no one gets any detailed security built into their products and services.

The problem with standards is that they are not standard

Let us not get too excited over standards and best practice of which our cup runneth over. There has been excellent work undertaken by NIST, ENISA, ISO, SANS and the Open Group to name but a few but in the face of increasing sophistication of cyber attacks of all sorts they haven't really stemmed the tide, and I just wonder if they have created a false sense of security in some areas.

As with every standard, policy, regulation or best practice just ticking the boxes is like "looking" both ways with your eyes shut before you cross a very busy road – you are carrying out the best practice to the letter but you kind of miss the point, and like in security, you pray you do not become a victim. For standards and best practice to be successful the inputs, outputs and outcomes need to be understood; there has to be attention to the detail every day and there has to be integration into the culture, risk philosophy and operational management of the business.

But, and it is a big but, many standards and best practice for security, if not the majority, focus on the uses and users of technology not on the design and build of the technology. You can end up with a fabulous set of integrated business processes to address security risk but the technology you are using can still be completely rubbish from a security perspective and you have little way of knowing.

Improving vendor end-to-end security focus and capability

Cyber security is not just about the bits and bytes of hardware and software development. If security is only a technical debate amongst the technical experts this is where the focus tends to be. Vendor cyber security has to be end-to-end, top-to-bottom and bottom-to-top.

Let me explain by exploring the supply chain security issue as an example. Most vendors, if not all, rely on a global supply chain for their product hardware and software components. Open up a Huawei box and 70% of what is inside comes from a global supply chain, i.e. not made or manufactured by Huawei – 30% comes from USA based organisations. Those suppliers have their own global supply chain so in essence we have layers built on layers – try protecting that from tainting and substitution.

For a vendor to "offer" its customers a secure product it must have process(es) to work with their suppliers to validate/verify the inherent security of the components they buy and build into their products. The vendor suppliers have to be able to protect against the insider threat; they must have mechanisms in place to protect against tampering and tainting as well as notification mechanisms to notify people of any vulnerabilities they find.

> Building cyber security into everything a vendor does ensures it becomes a part of the vendor's DNA and is not treated as some sort of programme or project with a defined start and end or even worse "it's their job, not mine" mentality

Imbedding third-party software whether open source or not is fraught with its own challenges. How will a vendor like Huawei know that the software does not contain vulnerabilities – think Heartbleed, think Poodle, think any zero-day exploit. How will a vendor like Huawei know that the third-party component will be maintained for the required duration? If the supplier stops supporting an important component to the vendor's product who will fix security of functional issues when the vendor may not have access to the source code? What will a vendor do if they are using open source software but find security vulnerabilities or design weaknesses that the community will not address?

So what approach should vendors take to building-in security to their products and services?

End-to-end vendor security is not just about product design and development it covers everything the organisation does. All vendors need to establish their own end-to-end transparent approach to enhancing the security capabilities of their organisation. There is not a set methodology for this, or a handbook, all vendors need to assess their own organisation design, values, culture and approach and establish its own approach.

At Huawei we cover twelve areas in our end-to-end approach:

1. Strategy, Governance and Control
2. Building the basics: Processes and standards
3. Laws and Regulations
4. People matter
5. Research and Development
6. Verification: Assume nothing, believe no one, check everything
7. Third-party supplier management
8. Manufacturing
9. Delivering services securely
10. When things go wrong: Issue, defect and vulnerability resolution
11. Traceability
12. Audit

Just like with any quality-Management system where quality cannot be bolted onto a product nor can cyber security be bolted on, it has to be built-in to everything you do.

This has ramifications for every part of the vendor's organisation. Whilst there may be a security office it is HR's responsibility to get the HR activities upgraded to cater for any security requirement just as it is the role of manufacturing to build-in any security requirements in their area and so on. This drives ownership, this drives accountability, this ensures it becomes a part of the vendor's DNA and is not treated as some sort of programme or project with a defined start and end or even worse "it's their job, not mine" mentality.

This also helps the buyer. Being able to go and inspect every part of your vendor's operation enables you to get a good feel and obtain empirical evidence of their commitment to end-end cyber security. When you speak to the Board Members are they clear on their role and their accountability? Can they articulate the governance, the loop back learning mechanisms and the pain/issues customers feel on security. When you speak to R&D engineers, the designers, coders and testers can they actually show you the design standards, their integrated tools, the coding standards etc. Can they show end-to-end traceability of who has touched code, or where every vendor supplier component has come from and gone to? What is their approach to independent testing? Are they open for audits, inspections and for your people to come and apply their own tests?

Working closely with our customers around the world we have documented the most frequent non-technical questions we are asked by our customers and other stakeholders when it comes to cyber security. In this context, "most frequent" also means the ones that generate the most conversation or review or follow-up questions. We have taken "poetic licence" to tweak the questions posed to us to make them generic. You can find a copy of the 100 questions you could ask your ICT vendors on the Huawei website.

What can critical infrastructure providers do?

Whilst the Top 100 is a start the EastWest Institute has agreed to take this initial Top 100 forward and, using its extensive knowledge and networks, shepherd the evolution of updated and more tailored versions.

Within the CIPRNet and academic communities there is immense knowledge and talent on threats, technology, standards, challenges and requirements. Using the Top 100 as a start a version could be generated for CNI operators collectively or by industry – get involved.

We fervently believe that the more demanding the buyer and the more consistent the buyers in asking for high quality security assurance the more likely the ICT vendors are to invest and raise their security standards.

Together we can augment the quality of security considerations in technology products and services, and from this we can collectively do more to enrich people's lives through the use of ICT.

You can play your role by being more demanding.

About Huawei

Huawei's products and solutions cover over 170 countries and regions and serve more than one-third of the world's population. We employ 150,000 people. The average age of our employees is 32 and 45% of our employees work on R&D. On average, 79% of our people are locally-employed in countries in which we operate. By 31st December, 2013, Huawei had filed 44,168 patent applications in China,

and 18,791 patent applications overseas, 14,555 under the Patent Cooperation Treaty (PCT). We have been awarded 36,511 patent licenses by accumulation

website at www.huawei.com

Critical infrastructures are at risk under electromagnetic attacks

EM threats should be included already in early planning of infrastructures

Background and scope

Electromagnetic terrorism, or Intentional Electromagnetic Interference, IEMI, is often defined as "the intentional malicious generation of electromagnetic energy introducing noise or signals into electrical and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes".

First, it should be mentioned that very severe incidents, with a large loss of life, money and property have already occurred due to unintentional electromagnetic interference. So it should from the start be clear that systems are vulnerable to electromagnetic energy, if these are not protected.

> Unexpected electromagnetic energy can interfere with electronic devices creating severe impacts on the normal operation modes. Protective measures have to be implemented to improve the resilience of the critical infrastructures

Due to the military heritage from the cold war and the research that grew out of the experience with electromagnetic effects on systems from nuclear explosions in the atmosphere (so called NEMP Nuclear Electromagnetic Pulse), much of the past research has focused on the effects of electromagnetic energy on military systems (such as aircrafts, ships, satellites, communication systems or munitions). However as of the late 1980's, the research focus has started shifting towards non-military systems. This shift in research is much in due to the huge increase in the amount of sensitive and sophisticated electronic devices (often commercial-off-the-shelf, COTS) being used in critical civil infrastructure components and everyday systems today. With the increased miniaturization and lowering operating voltages these systems become inherently more vulnerable to disturbances. This means that supervisory and control systems in complex distributed systems are today not especially hardened against electromagnetic interference, other than the regulated electromagnetic compatibility (EMC) demands, which however experimental experience has shown is not adequate to handle intentional or uncommon disturbances.

EMC regulations do not protect against IEMI threats

It is important to mention that for IEMI there exist no (and this is not expected either) restraints on the type of disturbances considered as a threat. The main difference between IEMI and traditional EMC research is the human intent behind the disturbance. Thus, any type of spectrum for interference, ranging from low (few KHz or even Hz) to very high frequencies (GHz) could appear. Also, due to the previous military heritage, much research has focused on the threat from an antenna radiating fields of high magnitude towards a system; however, this is barely half the side of the threat. Due to the openness of civil society (accessibility) an eventual attacker could come very close to the intended target carrying an electromagnetic system. The same attacker could also enter the before mentioned intended target to inject a conducted transient into this network. Research has shown that such transients would spread far into the power network of a facility, and interfere with all of the systems that are connected to this network (e.g., computers, servers, surveillance equipment etc.).

Dominique Sérafin

Dominique Sérafin is in charge of developing security research at CEA-centre de Gramat. He is also an expert in the field of infrastructure protection against electromagnetic attacks.

e-mail: **dominique.serafin@cea.fr**
CEA,DAM,GRAMAT,
F-46500 Gramat, France

It is well known that IEMI sources can be considerably reduced in size. Furthermore, the existing EMC regulation and testing has shown that the CE mark, supposedly showing a compliance with the EMC regulations, is not always valid. CE marked system could for some tested systems be interfered with at electric field levels far below the demands of the regulations. Thus, not only are non-hardened systems used for critical mission operation in infrastructures, the immunity of these are not as good as thought. The problem with IEMI, compared to traditional EMC is the human intent behind the interference ("is there a will there is a way"), the openness of the civil society (an attacker can come very close to the intended target) and that non-hardened systems and equipment (COTS) are being used for critical mission operations (of which much is known, e.g., working frequency). Also, today there are many possible electromagnetic systems or other malicious-intent wireless devices or systems available on the market (through commercial companies or through design schematics found on the internet) that requires no, or little, experience to be used.

Unfortunately, the vulnerabilities do not end there. In our societies today, the different infrastructures depend on each other. This interconnectedness between, for example, the electric power grid and the telecommunication, can create disturbances in systems and infrastructures not originally targeted.

If an attack disables the power grid for some extended period of time, backup systems running on, e.g., battery or diesel power will start to fail, and thus the communication infrastructures, such as internet servers or mobile communication (speech, text messages, etc.) will not be operational. The coordination of efforts to restart the operation of the systems will become increasingly difficult as time passes. After some time period, we will start to see second- and third-order effects, that is, the effect of the original disturbance has spread to other connected infrastructures and multiple effects have appeared. For instance, disruption in the power grid can lead to disturbances in the operation of petrol pumps (second order), which will lead to diminished transportation (third order) of goods (fuel, food, etc.).

> The use of standard EMC regulations does not protect enough against electromagnetic attacks.
>
> It is recommended to consider EM threats at the very early stage of the definition of critical infrastructures to apply the protection by design concept.

The anticipated consequences of an IEMI attack are severe delays to return to normal operation, loss of money or public relation, extortion of funds or any further dramatic consequences. One important characteristic of the IEMI attack is the lack of signature compared to the attack of an infrastructure using explosive devices where the cause is quite evident. It would be very difficult to rapidly prove the attack and to determine who is behind the attack.

The appropriate response to IEMI threats is to protect adequately critical infrastructures. The technical solutions are there (improvement of the shielding effectiveness of the buildings, protection devices on antennas, communication and power supply cables, redundancy of systems, installation of the vital parts at a safe distance from the public access...)

Several security research projects under the 7th framework programme of the EU are already addressing the impact of IEMI threats and the protection aspects of targeted infrastructures such as (air transportation, railways systems, ground segment of space assets, critical infrastructures etc....).

Conclusion

In conclusion, Electromagnetic attacks may result in serious disruptions of vital parts of the society's technical infrastructure and in some cases even in the loss of lives. Means for deployment of IEMI are readily available for a determined adversary.

The recommended strategy is to consider this potential electromagnetic threat at the very early stage of the design of any new critical infrastructure. In parallel, there is a need for new electromagnetic regulations to help designers and architects to apply the concept of protection by design. For existing infrastructures, basic and already available measures can be applied to improve their global resilience.

Cascading Failures: Dynamic Model for CIP purposes - case of random independent failures following Poisson Stochastic Process

About the importance to understand the background of simulation

Introduction

Modern systems are more and more complex, distributed and interconnected. Because of this ever-increasing complexity, a localised single failure may be propagated and amplified through many interconnected systems leading to a serious crisis. One will then talk about "cascade effect". A full description of cascading failures may include both structural and dynamical. An interesting review of cascade modelling is given in Boccaletti, [1].

The graph theory provides a powerful mathematical basis for modelling distributed systems, [2].

Dynamic **modelling** aims at introducing the time into the description of the failures occurrence, propagation and mitigation. Robust crisis management strategies require reliable capability of MS&A. A dynamics-based model is proposed in the paper assuming independent failures.

Overview of Cascading Models

One may identify four specific problems that appear to reoccur when CIs are challenged: 1) heterogeneity, 2) multiple and inconsistent boundaries, 3) resilience building and 4) knowledge transfer and sharing. This is called the "causal modelling methodology".

One may also focus on the modelling the chain effects of the cascading events. That led some researchers to propose the "database approach" in order to assess the potential damage that arise from various combinations of phenomena and locations. This method results in too many rules to model the complexity and the uncertainty of the problems.

Others have proposed a "simulation-Others have proposed a "simulation-based risk network model" for decision support in project risk management. This method accounts for the phenomena of chain reactions and loops, but neglects the detailed connections of information among the internal components of a cascading crisis event. It seems not yet feasible to combine the crisis chain reaction (macro-view) and the elements within the crisis event (micro-view) involved in the cascading event.

Tentative efforts are oriented towards a "generalized modelling framework" that may combine multilayer infra-structure networks (MIN) concept and a market-based economic approach using the computable general equilibrium (CGE) theory and its spatial extension (SCGE) to formulate a static equilibrium infra-structure interdependencies problem. However, the applicability is still to be demonstrated, specially, in engineering fields.

Ouyang, [3], has made an extensive review on modelling and simulation of interdependent critical infrastructure systems (CISs) and broadly grouped the existing modelling and simulation approaches in six types: 1) empirical approaches, 2) agent based approaches, 3) system dynamics based approaches, 4) economic theory based approaches, 5) network based approaches, and 6) others. The model proposed in our paper could accordingly be considered as a system dynamics based approach. It considers only the independent failure events

Mohamed Eid

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

email: **mohamed.eid@cea.fr**

Overview on Dynamic Modelling

The independent cascading failures may be described under the form of an integral of a differential equation, Equation (1). Fussell, [4], and Yunge, [5], use the same mathematical description (but with different forms) to model the sequential occurrence of events. Many other authors followed almost the same way of modelling and produced very interesting applications, see [6] for an interesting list of relevant references.

Other researchers could solve the same problem using numerical techniques such as Petri Nets or Dynamic Bayesian Net (DBN).

The Description of the Algorithm

Let T be a cascade of failures described by the occurrence of the independent events e_i in a given order, $[e_1, e_2, e_3, \ldots, e_n]$. The corresponding occurring instants are defined by $[t_1, t_2, t_3, \ldots, t_n]$. The first event is e_1 and the last one is e_n. Each of these instances has its own probability density function ρ_n. The probability $p_n(t)$ that the cascade T happens within the interval [0,t] is given by:

$$p_n(t) = \int_0^t \rho_1(\xi_1)d\xi_1 * \int_{\xi_1}^t \rho_2(\xi_2)d\xi_2 * \ldots * \int_{\xi_{n-1}}^t \rho_n(\xi_n)d\xi_n \quad (1)$$

Where:

$0 \le \xi_1 \le \xi_2 \le \xi_3 \le \ldots \le \xi_n \le t$ and ρ_i is the Poisson density function characterizing the event e_i [$\rho_i = \lambda_i * e^{-\lambda_i t}$] and λ_i is the occurrence rate of the event e_i. The number n refers to the number of the elementary failures involved in the cascade T . Many authors have previously developed analytical solutions to Equation (1) when the number of the events is relatively small. If the failures dependency is considered, the integral equation (1) will still be valid but not its analytical solution. If the dependencies are well-described, the integral equation (1) can, then, be numerically solved using Monte-Carlo Simulations or Petri-Net.

The analytical solution of Equation (1) and the corresponding quantities are given in details in [7].

$$p_n(t) = \sum_{j=1}^{n} C_j^n * (1 - e^{-(\sum_{l=n-j+1}^{n} \lambda_l)t}) \quad (2)$$

The coefficients C_i^n are described in details in, [7].

Conclusion

A cascade event Tn implies n well-defined successive random failures. Dynamic modelling is necessary if one should describe the temporal evolution of a cascading event. Dynamic modelling aims at introducing the time into the description of the failures occurrence, propagation and mitigation. Robust crisis management strategies require reliable capability of MS&A. A dynamics-based model is proposed in the paper assuming independent failures.

A cascading event is fully described by and integral equation that can be rewritten under a differential form, as well. If the elementary events involved in the cascading sequence are considered **independent**, the integral equation may have an analytical solution.

The cascading event may be characterized by: an occurrence probability, an occurrence probability density function and a mean occurrence time. These characterizing quantities can have analytical expressions if the n independent random failures follow a Stochastic Poisson process (SPP). Subsequently, the occurrence characteristics of the consequences and the related hazard can be determined as well.

If the failures dependency is considered, the integral equation (1) will still be valid but not the analytical solution. If the dependencies are well-described, the integral equation (1) can, then, be numerically solved using Monte-Carlo Simulation or Petri-Nets based algorithms.

Acknowledge

The current work has been partially realized and fully used in the frame of the EU collaborative project "PREDICT: PREparing for the Domino effect in Crisis siTuations", FP7-SEC-2013-1. It is, then, a synthesis of contributions from all PREDICT consortium's members.

References

1. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D.-U., 2006. Complex networks: Structure and dynamics. Physics Reports 424 (2006) 175□308.
2. Panayiotis Kotzanikolaou, Marianthi Theoharidou, Dimitris Gritzalis, "Assessing n-order dependencies between critical Infrastructures". Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2 (2013) 93-110. Copyright © 2013 Inderscience Enterprises Ltd.
3. Ouyang, M., 2014. Review on modelling and simulation of interdependent critical infrastructure systems. Reliability Engineering and System Safety 121(2014) 43–60.
4. J.B. Fussell, E.F. Aber, R.G. Rahl, "On the Quantitative Analysis of Priority-AND Failure Logic." IEEE Transactions on Reliability, vol. R-25, No. 5, December 1976.
5. T. Yuge, S. Yanagi, "Quantitative analysis of a fault tree with priority AND gates." Reliability Engineering & System Safety 93 (2008) 1577-1583.
6. Mohamed Eid et al., "Cascading Failures: Dynamic Model for CIP purposes - case of random independent failures following Poisson Stochastic Process". CRITIS 2014, 9th International Conference on Critical Information Infrastructures Security, October 13-15, 2014, Limassol, Cyprus
7. Mohamed Eid, "A General Analytical Solution for the Occurrence Probability of a Sequence of Ordered Events following Poison Stochastic Processes". Journal of Reliability Theory & Applications, vol.2/No. 2 (21-32) June, 2011

CRITIS 2015: 10th International Conference on Critical Information Infrastructures Security – Call for Papers

CRITIS' 10th anniversary takes place in Berlin, Germany, October 5–7, 2015.

In 2015, the International Conference on Critical Information Infrastructures Security faces its tenth anniversary. CRITIS 2015 continues the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP) and fostering the dialogue with stakeholders. CRITIS 2015 aims at bringing together researchers and professionals from academia, industry and governmental organisations working in the field of the security of critical (information) infrastructure systems.

As in previous years, invited keynote speakers and special events will complement a programme of original research and stakeholder contributions. The conference invites the different research communities and disciplines involved in the C(I)IP space, and encourages discussions and multi-disciplinary approaches to relevant C(I)IP problems.

Call for Papers

CRITIS 2015 has four foci. Topic category 1, Resilience and protection of cyber-physical systems, covers advances in the classical CIIP sectors telecommunication, cyber systems and electricity infrastructures. Topic category 2 focuses on advances in C(I)IP policies and best practices in C(I)IP specifically from stakeholders' perspectives. In topic category 3, general advances in C(I)IP, we are explicitly inviting contributions from additional infrastructure sectors like energy, transport, and smart built infrastructure) and cover also cross-sector CI(I)P aspects.

In 2013, the CRITIS series of conferences has started to foster contributions from young experts and researchers ("Young CRITIS"), and in 2014 this has been reinforced by the first edition of the CIPRNet Young CRITIS Award (CYCA). We will continue both activities at CRITIS 2015, since our demanding multi-disciplinary field of research requires open-minded talents.

Topic category 1: Resilience and protection of cyber-physical systems

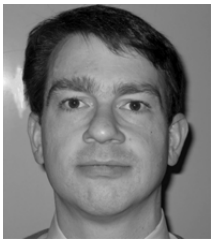
- Modelling and analysis of cyber-physical systems for monitoring and control
- Security, protection, resilience and survivability of complex cyber-physical systems
- Impact and consequence analysis of C(I)I loss or reduction of quality of service
- C(I)I dependency Modeling, Simulation, Analysis and Validation
- Cyber security in critical infrastructure systems
- Fault tolerant control for cyber-physical systems
- Security and protection of smart buildings

> CRITIS 2015 continues the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP) and fostering the dialogue with stakeholders.

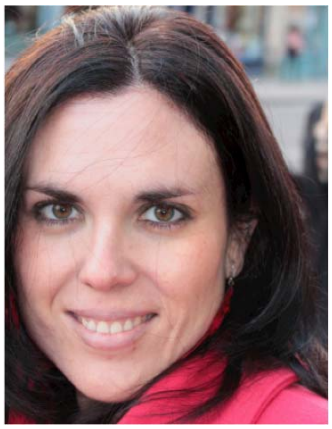
Topic category 2: C(I)IP policies and best practices in C(I)IP – stakeholders' perspective

- Risk management in C(I)IP
- The role of C(I)I in the implementation of the EU directive on European Critical Infrastructures in EU Member States
- C(I)I exercises & contingency plans
- Advances in C(I)IP policies at national and cross-border levels
- C(I)IP R&D agenda at national and international levels
- Trust models in normal situations and during escalation

Erich Rome, Fraunhofer IAIS, General Chair
e-mail: erich.rome@iais.fraunhofer.de



Marianthi Theocharidou, EU JRC, Stephen D. Wolthusen, Royal PC Co-Chairs
e-mails: stephen.wolthusen@rhul.ac.uk
marianthi.theocharidou@jrc.ec.europa.eu



Cristina Alcaraz, University of Malaga, Publicity Chair
e-mail: alcaraz@lcc.uma.es

- Public-private partnership for critical infrastructure resilience
- Economics, investments and incentives of critical infrastructure protection
- Defense of civilian C(I)I in conflicts with cyber elements
- Forensics and attribution in C(I)I

Topic category 3: Advances in C(I)IP

- Advanced decision support for mitigating C(I)I related emergencies
- C(I)IP for energy infrastructures (like oil and gas sector, renewable energies)
- C(I)IP for transport infrastructures (like railways, toll systems, tunnel control systems, logistics centers, airports)
- Advances in cross-sector CI(I)P approaches
- Recent trends in cyber economy (clouds, quasi-monopolies, new payment methods etc.) and implications for C(I)I and C(I)IP

Topic category 4: YOUNG CRITIS and CIPRNet Young CRITIS Award (CYCA)

- Topics of interest for category 4 include all topics mentioned under topic categories 1 and 3.

Paper submission

We encourage submissions containing original ideas that are relevant to the scope of CRITIS 2015. Researchers are solicited to contribute to the conference by submitting research papers, work-in-progress reports, R&D project results, surveying works and industrial experiences describing significant advances in C(I)IP. Stakeholders from governments, Critical Infrastructure operators, and industry are encouraged to submit papers that describe their current and future challenges to be engaged by researchers and multidisciplinary research teams.

It is required that papers are not submitted simultaneously to any other conferences or publications; and that accepted papers not be subsequently published elsewhere. Papers describing work that was previously published in a peer-reviewed workshop are allowed, if the authors clearly describe what significant new content has been included.

All papers need to be written in English. There will be full papers and short papers. Full papers should be no longer than 12 pages, including bibliography and well-marked appendices. Short papers should be 4 to 6 pages long. Any submission needs to be explicitly marked as “full paper” or “short paper”.

All paper submissions must contain a title, a short abstract, and a list of keywords. All submissions will be subjected to a thorough double blind review by at least three reviewers. The paper submissions should be anonymised and all author names, affiliations, acknowledgements, and obvious traceable references should be eliminated.

Papers must be submitted via the EasyChair conference system. The submitted paper (in PDF or PostScript format) must be formatted using the template offered by Springer LNCS and be compliant with Springer's guidelines for authors.

CRITIS 2015 continues the “Young CRITIS” community-building activities for fostering open-minded talents.

Acceptance policy and publications

For publication in the CRITIS 2015 proceedings, all accepted papers (full and short) must be presented at the conference; at least one author of each accepted paper must register to the conference by the early date indicated by the organizers.

Publication – Pre-proceedings

Pre-proceedings will appear at the time of the conference. All accepted papers would be included in full length in the pre-proceedings.

Publication – Post-proceedings

As in previous years, it is planned to publish post-proceedings at Springer in their Lecture Notes in Computer Science series. Accepted full papers will be included in full length in the post-proceedings. However, we recommend that the authors produce a revised version of the paper, based on feedback received at the CRITIS event.

For accepted short papers, a four page extended abstract will be included in the post-proceedings.

Any accepted paper (full paper and extended abstract) that shall be included in the post-proceedings requires that its authors sign Springer’s copyright agreement.

Important dates

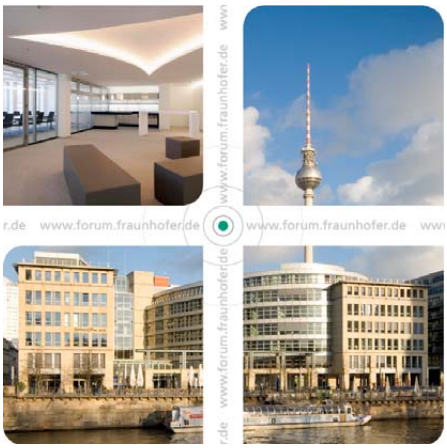
Submission of full papers:
May 10, 2015 (firm deadline)
Notification of acceptance:
July 8, 2015
Camera-ready papers:
September 10, 2015
CRITIS 2015 event:
October 5–7, 2015

Venue

CRITIS 2015 will take place at the Fraunhofer Forum, in the very heart of Berlin, vis-a-vis Museum Island and Berlin Cathedral. It has excellent reachability, just a three minutes’ walk from the S-train station "Hackescher Markt".

Street address:
Fraunhofer Forum
Anna-Louisa-Karsch-Str. 2
10178 Berlin

Website:
http://www.forum.fraunhofer.de/start_en.html



More information

If you would like to find out more about CRITIS 2015, the venue, and travel directions, then please visit our website at

www.critis2015.org

Links

ECN home page	www.ciprnet.eu
ECN registration page	www.ciip-newsletter.org The registration is free of charge
CIPedia© The upcoming and **new** CIP reference point	www.cipedia.eu

Forthcoming conferences and workshops

ISPEC 2015 11th Information	http://icsd.i2r.a-star.edu.sg/ispec2015	May 5-8 Bejing China Security Conference
1st TELERISE	www.iit.cnr.it/telerise2015	Technical and LEgal aspects of data pRIvacy and Security
1st WS Cyber Crime & Terror	www.ares-conference.eu	Aug. 24 – 28, 2015Toulouse, France: Add p. 16
10th CRITIS Conference	www.critis2015.org	Call f. Paper up to May 5, 15, Oct 5-7, 2015, Berlin
9th Conference IT Forensic	www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2015	May 18-20, 15, D- Magdeburg
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016
2nd EAIS, Sept 13-16, 2015	https://fedcsis.org/eais	WS on Emerging Aspects in Information Security
16th IEE EI.Tech Conference	http://melecon2016.org	Call for Papers: open until Sept. 15, 2015

Exhibitions

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

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu
Financial ISAC FS-ISAC	www.fsisac.com/

Project home pages

FP7 Astarte	www.astarte-project.eu
FP7 Capital	www.capital-agenda.eu
FP7 CIPRNet	www.ciprnet.eu
ERNCIP Project	https://erncip-project.jrc.ec.europa.eu
FP7 BESECURE	www.besecure-project.eu
FP7 Progress	www.progress-satellite.eu
FP7 INFRARISK	ww.infrarisk-fp7.eu
RAPID-N	http://rapidn.jrc.ec.europa
Democrite	www.agence-nationale-recherche.fr/?Project=ANR-13-SECU-0007

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on “Resilience of Networks and Services and Critical Information Infrastructure Protection” I this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
ENISA information pool on cyber strategy	www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss
Network Information Security Platform	https://resilience.enisa.europa.eu/nis-platform

Websites of Contributors

Joint Research Centre	http://ipsc.jrc.ec.europa.eu
Access Consulting	www.cercle-k2.fr/users/single/296/Alain-Coursaget
CEA	www.cea.fr
Crabbe Consulting	http://crabbe-consulting.com
Huawei	www.huawei.com
Delatres	www.deltares.nl/en
Pôle Risques	www.pole-risques.com
University of Trento	http://r.unitn.it/it/sdc

www.cipedia.eu

CIPedia© is here!

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

> CIPedia© aims to become a common reference point for CIP concepts & definitions.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

> The initial content was provided by the EC-JRC, Fraunhofer, TNO, and the CIPRNet consortium.

The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

Marianthi Theocharidou

Marianthi Theocharidou works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), for the CIPRNet and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes CIP **experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information

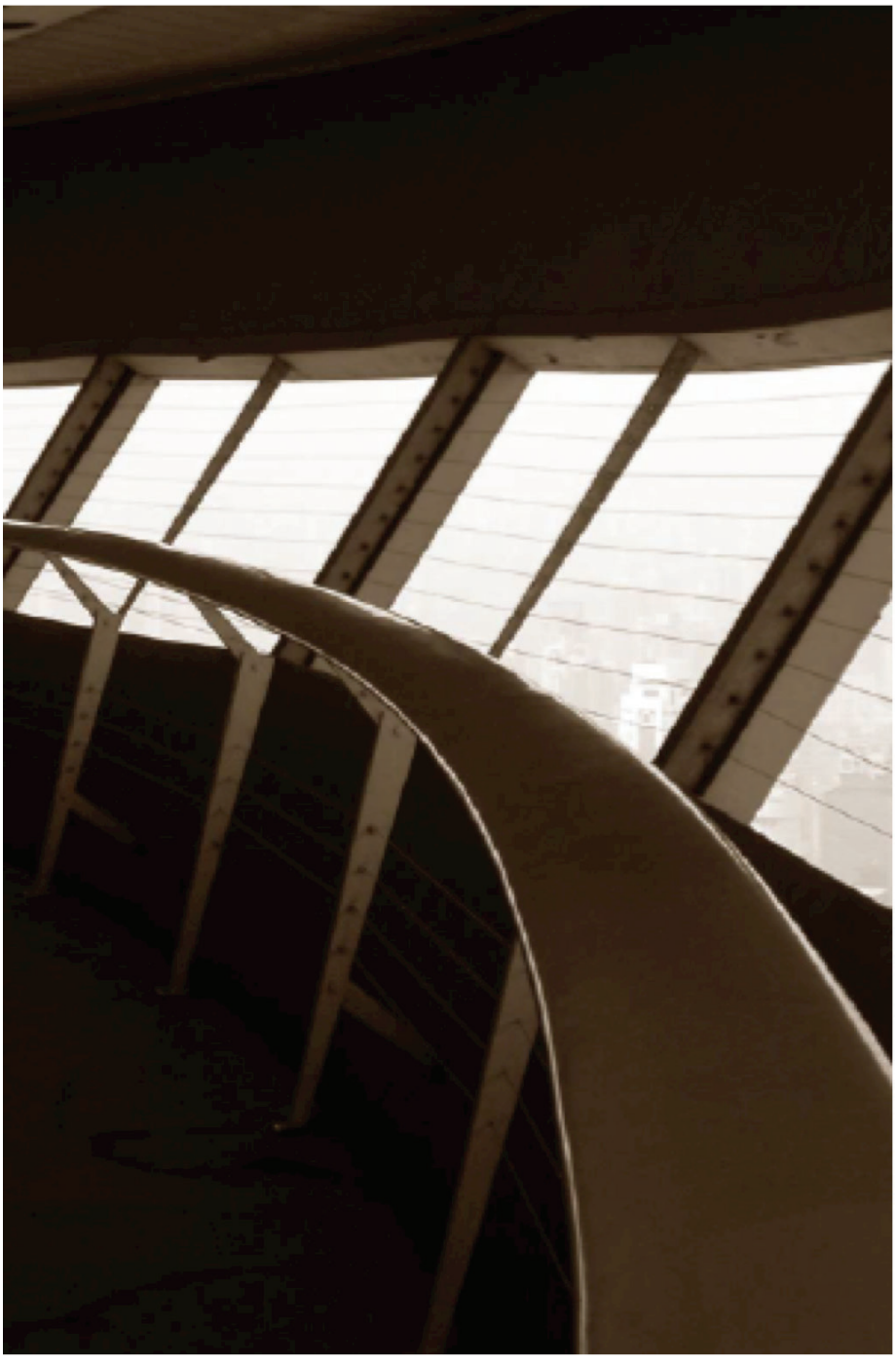
European CIIP Newsletter

July 15 – October 15, Volume 9, Number 2

CRITIS 2015

Call for Participation

Conference
Oct. 5-7, 2015 Berlin



ECN

Contents

CIPR Net

> 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) 312450

>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

> Spelling:
British English is used except for US contributions

Editorial: Critical Infrastructures Trust and Public Private Partnership (PPP)

In the frame of PPP information sharing is becoming popular and practice guides are available. NL EU Presidency will push this forward. Trust is the glue of our society, also in Cyberspace: But whom to trust.

The reaction on the big cut of trust in suppliers is becoming more and more evident: We have hardware, software, BIOS, middleware, applications, updates, crypto and other components of our ICT infrastructure which do serve the intended purposes, but support also other parties' interests. As a reaction to this tendency, nationalisation of ICT is a serious point of discussion. But do we really want this? Are there no other ways to balance leaking means and intended purpose, e.g. by behaviour

ICT infrastructure for CI should be bullet-proof and not manipulated to serve other purposes. In this context it is well understandable that weaponised infrastructures should be secured against any attack or malfunctioning.

Europe is reflecting how to react on this challenge, and how to bring the right knowledge together. The task is very challenging, but urgently needed for the sovereignty of nations and Europe in particular. A nation is defined by its sovereignty. We have to think about what this means in cyberspace in general and in the interconnected CI in particular. A huge challenge, but with preliminary discussions only: a need to be active!

The Netherlands are well known for taking care of flood protection, which stays a vital necessity. Next to that, earthquakes are happening more frequently in the northern part of the country. It is no surprise that next to the traditional CIP topics the connection between CI and emergency management is getting more attention. In the first half of 2016, The Netherlands have the EU presidency. It is the aim to use this opportunity to stimulate Information Exchange and Private-Public Partnerships in the area of CIP throughout Europe.

In addition, the Netherlands have contributed with the "Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach" https://www.gccs2015.com/documents/sharing-cyber-security-information of which the EU will publish soon chapter three "Voluntary Information Sharing" of the networking Information Security Platform NIPS.

Several articles in this volume give a broad overview on relevant projects and initiatives of the Dutch CI community: "CI cascading effects: from research into practice" by Marieke Klaver and Nico van Os, "Cyber security for critical infrastructures" by Eric Luiijf, "The influence of triggered earthquakes on critical lifelines in the North of the Netherlands" by Henk Kruse and Mandy Korff, "ROADAPT: Roads for today, adapted for tomorrow" by Thomas Bles and "System Robustness Analysis in Support of Flood and Drought Risk Management" by Marjolein Mens. In a couple of these projects described, the partnership between government, water boards, security regions and private companies are already taking form.

We would like also to remind you that the CIP community has a rendezvous in Berlin at the 10th edition of the CRITIS conference which is scheduled October 5-7. The programme will be enhanced with several distinguished keynote speakers and includes about 25 very carefully selected scientific contributions. The young scientific community is involved again and in the frame of CIPRNet Young CRITIS Award all participants are invited to follow the competing youngsters and contribute with their opinion to the election of the best contribution.

Enjoy reading this issue of the ECN!

PS: Please have a look at CIPedia©: http://www.cipedia.eu.. Please bring your knowledge in to contribute to a real CIP compendium!

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

Micheline W.A. Hounjet

Her background as an engineering geologist, she is not only active in the cross-over between technical disciplineshrough cascading effects.

e-mail: micheline.hounjet@deltares.nl

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

e-mail: **bmhaemmerli@acris.ch**
He is ECN Editor in Chief

CRITIS 2015

10th International Conference on
Critical Information Infrastructures Security

October 5–7, 2015, Fraunhofer Forum, Berlin, Germany

www.critis2015.org

With

2nd Young CRITIS Award Competition

Take your chance and be audience voting member
to promote the CIP youth

CI cascading effects: from research into practice

This article gives an introduction on the collaboration between R&D and emergency management organisations in the Netherlands. The collaboration is aimed to improve the assessment of CI cascading effects in emergency management.

Introduction

Critical Infrastructure Protection (CIP) has been a research topic in the Netherlands for quite some years. Until recently, most of the research was aimed at the national level, e.g. on identifying Critical Infrastructure (CI), performing risk assessment and analysing dependencies.

Recently, the relationship between CI and emergency management is increasingly getting attention.
The 25 Dutch safety regions ("Veiligheidsregio's") play an important role in Dutch emergency management structure and processses. These Safety regions increasingly include CI in their risk assessments and emergency plans.
This article describes how a close collaboration is developing between research organisations and the emergency management organisations regarding CI and their dependencies. In particular, we describe the collaboration between TNO and the Safety region South-Holland-South. This article will discuss how this collaboration builds on the results from earlier research and how these results are used in the development and assessment of a case study.

Earlier results on CI and emergency management

Empirical evidence from reports about emergencies and disasters in various regions in the world shows that CI disruptions may cause unwanted extensions of the duration, affected area and impact of emergencies with more casualties, more suffering, and more damage. It is therefore important to include the possible impact of CI disruptions in the risk assessment and preparation processes of emergency management organisations at the local level.
One of the main lessons learned from CI disruptions all over the world is that the set of CI dependencies changes with the mode of operation. When an organisation enters another mode of operations, e.g. due to the failure of a CI, its operational continuity depends on a different set of CI. For example, the availability of diesel, roads and oil trucks are of no importance to the operation of a hospital until it has to switch on its backup generators due to a power failure.

> Emergency plans should take into account non-normal mode of operation dependencies and common cause failures

Empirical evidence also shows that CI operators and emergency management planning mostly understand and plan for possible CI disruptions critical to normal operations. However, it is much harder to understand and prepare for CI dependencies which occur in the non-normal modes of operations and when multiple CI fail simultaneously (common cause failure), e.g. due to an extreme weather event. This crucial kind of dependency analysis is often some levels of analysis too deep for most public and private sectors to plan for.

In addition to the direct impact on CI, more damage may occur due to cascading effects, e.g. the loss of electricity may lead to loss of all information and communication technology (ICT) dependent services and by that cause an impact on hospitals and the transport system. The cascading effects may refer to the cascade of disruptions across multiple CI within an area covered by the emergency management organisation, but may also refer to cascading effects outside that area.

Marieke Klaver (TNO)

Dr. Marieke works as programme manager on research in Critical Infrastructure Protection (CIP) and Cyber Security.
Her research focusses on CI dependencies, risk analysis and cyber resilience.

Phone ++31 (0)88 866 38 68
e-mail: marieke.klaver@tno.nl

Nico van Os MPAN

Nico works as project manager for EU projects at the Safety Region South-Holland South.

e-mail: n.van.os@vrzhz.nl

For instance, due to the structure of the power grid, the loss of electricity will almost certainly not be limited to an inundated area.

A systematic approach to assess the dependencies

As part of the EU FP7 project PREDICT (PREparing for the Domino effect in Crisis siTuations), a methodology was developed to systematically assess the CI dependencies and the impact for emergency planning at the local level.

The methodology provides seven steps in order to systematically:

- assess the threats to be taken into account for the considered area;
- Identify the CI;
- Identify the key CI elements;
- characterise the vulnerability of the key CI elements to the threats;
- assess the first order impact of the threats on the CI elements;
- describe the dependencies between the CI elements;
- assess the CI cascading effects.

For each of these steps, supporting tools such as checklists or algorithms can be established based on results of earlier research.

A case study of large scale flooding

In order to test this methodology, a case study was developed. The case study describes a developing dike breach near Gorinchem, The Netherlands which directly leads to failure of the quays directly behind the dike. As a result, the influx of water will threaten the polder 'Alblasserwaard' lying directly behind these quays.

Such a large scale flooding will have impact on almost all CI within the affected area. The seriousness of the scenario is increased by the short timelines: the western area of the polder will flood in a period of approximately sixteen hours.

In order to assess the effects for all CI, the assessment is performed in a close dialogue with all stakeholders within the Safety region South Holland South, including operators of the main CI within the region, emergency management organisations and research organisations.

Figure 1: the location of the Alblasserwaard

Based on this close collaboration, the methodology is tested and the required level of detail can be established that is needed to support the decision making process. The case study is also used to assess the availability of the Information needed.

An initial result is that the assessment methodology does not require highly detailed CI information; understanding the main issues, decision points and time characteristics for the CI operators is often sufficient for proper emergency management planning and operations.

Next steps

The main results of the case study will be discussed in a workshop with the main stakeholders in South Holland South end of May 2015.

The EU project PREDICT will use the methodology and findings from this and other use cases to develop supporting tools.

Finally, in close collaboration between TNO and the Safety Region South Holland South an extensive scientific paper is being written that describes both the methodology and the results of the case study.

Acknowledgement

The PREDICT project has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement no 607697.

This article reflects only the authors' views. The European Union is not liable for any use that may be made of the information contained therein.

http://www.predict-project.eu/

PREDICT
PREparing for the Domino effect in Crisis siTuations.

Launch of CYSPA: the European Cyber Security Protection Alliance

The CYSPA Alliance is an initiative for EU stakeholders working together to articulate, embody, and deliver the concrete actions needed to reduce cyber disruption

CYSPA is a European-based Alliance that started as an FP7 EC-funded project (October 2012-March 2015) and which is now operating under the European Organisation for Security.

Managing cyber risks is not only a technical issue. Correctly managing cyber risks is a corporate level responsibility – it is not something that can be delegated, it is an issue that can bring down a company. This is the first pillar on which CYSPA built its approach from the start – the need for every organisation to protect their assets means that organisations need to be empowered to understand and be fully aware of which assets are at risk, which assets are more at risk than others, leading to a clearer view to investments and policy decisions.

The CYSPA Alliance aims to protect cyberspace, an environment characterised by its world-wide outreach and its speed – speed of propagation of information, unfortunately also matched by speed and ease of propagation of attacks. Over the last years, the key trends are driven by increasingly distributed operations, ranging from cloud-based platforms to mobile technologies, intelligent devices and bring your own devices. Of course, cyber-attacks take place on a global level, but over the last years, it has become evident that even analysing only at a European level, the cyber threat landscape has changed significantly. This, together with the fast paced nature of cyberspace, means that cyber security should be of paramount focus for every organisation in order to protect their assets.

Current evaluations of economic impact and costs are given at very high level (i.e. for a whole activity sector, or for a country) but the negative side of this macro-approach is that individual organisations cannot relate to such huge numbers – there is a strong need for more personalised evaluations of the impact of cyber-attacks.

Managing cyber risks is not only a technical issue. Correctly managing cyber risks is a corporate level responsibility – it is not something that can be delegated, it is an issue that can bring down a company. This is the first pillar on which CYSPA built its approach from the start – the need for every organisation to protect their assets means that organisations need to be empowered to understand and be fully aware of which assets are at risk, which assets are more at risk than others, leading to a clearer view to investments and policy decisions.

The European context

Since the start of CYSPA, another key evolution has taken place – the actions of the European Commission have been consolidated into a European cybersecurity strategy.

This is a key evolution in integrating the multiple dimensions of cyber-space because it is the first step towards implementation – implementation of new directives, of research opportunities, of procurement guidelines etc. It is key for each organisation to not only be aware of what is taking place at European level, but more importantly to understand how this can impact operations and to get involved in ensuring that the implementation path of the European strategy is aligned to one's needs.

Nina Olesen

Nina Olesen is a senior project manager at the European Organisation for Security. She is currently involved in different EU projects and is leading the operational management of CYSPA.
She was also the project coordinator for the CYSPA project.

e-mail: nina.olesen@eos-eu.com
European Organisation for Security
Rue Montoyer 10, BE-1000 Brussels
ww.eos-eu.com

CYSPA is therefore positioned across these two dimensions:

- The need to empower each organisation not only with awareness but also with the means to understand and prioritise how to protect its operations
- The need to be active at European level to contribute to the European cybersecurity strategy, to ensure that ultimately the various directives, policies and research activities are well aligned to the needs of each organisation's economic activity sector and operations.

Objectives

In order to reflect its vision statement of working together at European level and being active not only in defining but also in implementing actions, CYSPA has translated this approach into five core objectives.

The first objective of CYSPA focuses on specific campaigns, each campaign representing a concrete set of activities and outcomes. These campaigns aim to encapsulate the approach of getting members actively involved in CYSPA.

The second objective focuses on the need to identify and express the real impact of cyber threats at a level that is relevant to individual organisations. CYSPA is therefore focusing on a sector per sector approach – starting with the e-government, energy, finance and transport sectors. This approach delivers the right balance between organisations being able to access information that is relevant to their activities, while at the same time taking into account the sensitiveness of the information. CYSPA will add additional sectors (based on feedback from members) after the CYSPA model has been fully tested on the four current sectors of focus.

The third objective is to deliver concrete services to members – meaning that CYSPA is focused on supporting its members with approaches, tools and solutions to increase not only awareness but also their analysis capabilities of their own cyber risks.

The fourth objective is to promote an open culture of active participation. This means that for the different recommendations that CYSPA is working on in terms of identification of risks, methodologies to handle risks, solutions etc., members should not only elaborate them together but also take up these recommendations and implement them internally to then help evolve. By encouraging our members to implement in their own contexts and to then share feedback, the dynamic nature and complexity of the cyber security domain is better supported.

The fifth objective is the coordination and collaboration with other European-wide initiatives. For instance, CYSPA has consolidated results from its sector impact reports and the threat taxonomy coming from ENISA's threat landscape reports in order to feed into a risk self-assessment tool that is accessible to members via the CYSPA Community Portal.

Providing added value

Since CYSPA was created as a European project, numerous associations and alliances have emerged, focused on different aspects related to cyberspace. A valid question is therefore what CYSPA can bring of value – especially in a context where we want to avoid duplication.
First and foremost, CYSPA introduces a sector specific approach to cyber risks – moving to a level of granularity to make the impact of cyber risks relevant to individual organisations.

Secondly, CYSPA has developed a community approach, supported by an online portal for members, to ease interaction and access the value added services.

Thirdly, in creating a network between users, providers and public authorities not only as a meeting point, but also through concrete activities, an important contribution is being made to achieve the sharing philosophy without which cyber security will never become a reality.

Finally, CYSPA will be used as a gateway between needs and European policy makers, aiming to improve the alignment of policies to needs but also to speed up uptake.

CYSPA community

CYSPA is working with users, providers and public authorities in the context of cyber security.

Starting with the users, the benefits are clearly to move to numbers, approaches and solutions that are applicable to the specific sector in which a user operates.

For the providers, the benefits are to have faster, easier access to user needs – and as a consequence of increased user-provider collaboration decrease the time to market by earlier involvement of users and better alignment to already identified needs.

CYSPA involves public authorities in their role as policy providers, strategy promoters and awareness drivers – activities that require uptake by the actual industrial organisations.

Starting with the initial consortium partners comprising 16 organisations from industry and research, CYSPA has evolved its community to include national security clusters, SME's, national public administrations, and operators. CYSPA is also working on setting up national chapters, the first of which will be set up in Turkey.

CYSPA organisation

The CYSPA Alliance is a membership-based "de facto" association established under the European Organisation for Security (EOS). Organisations joining CYSPA need not be a member of EOS but EOS members are granted free access to CYSPA.

CYSPA is organised through a Board and operates through Sector Groups and Task Forces.

Sector Groups are used to create a focal point for stakeholders from each sector, a space of interaction for members operating in similar contexts, from transport to utilities, finance and e-government. Members can also propose new sectors of focus. Task Forces are used to implement focused activities with a defined duration and target result.

CYSPA is also supported by External Advisors.

How to join

CYSPA will be introducing membership fees as of July 2015. Until then, organisations can join free-of-charge via the Community Portal (https://cyspa.eng.it/).
The CYSPA Community Portal provides members of the Alliance with a comprehensive **online collaboration** platform designed specifically to enable and ease interactions between the CYSPA members.

The sector approach of CYSPA provides you with a unique opportunity to get a more precise view of the different needs of customers operating in your domain. In the dynamic context of cyberspace, no single company, no single organisation, no single country can work ALONE in tackling the challenge of cyber threats.

CYSPA focuses on defining action lines that require a community to deliver value and on encapsulating the results of these activities as services to deliver value back to its members.
CYSPA builds these action lines across three pillars:

1. By actively contributing to policy at European and national level
2. By building the capacity of CYSPA members to assess the vulnerabilities, prioritise how critical those vulnerabilities are to their own operations and identifying solutions
3. By creating cyber knowledge

By joining CYSPA, you choose to participate to one or more of these action lines – turning your effort and involvement to those activities that are the closest to your needs.

If you would like to know more about CYSPA please visit our website and Community Portal:

www.cyspa.eu
https://cyspa.eng.it/

Watch our video: "CYSPA Launch Alliance":
https://www.youtube.com/watch?v=YdJq0_Hb_wg

For more information on membership (fee structure, statutes, etc.), please contact nina.olesen@eos-eu.com)

CYSPA
EUROPEAN CYBER SECURITY PROTECTION ALLIANCE

TIEMS 2015 Annual Conference

TIEMS 2015 Annual Conference in Rome
30th September - 2nd October 2015

http://tiems.info/tiems-2015-annual-conference.html

TIEMS 2015 Annual Conference which takes place in Rome.

TIEMS Italy Chapter is conference host, see:

Italy Chapter WEB-site

Registration coming soon:

http://tiems.info/tiems-2015-annual-conference.html

Cyber security for critical infrastructures

A vision for action and two good practice booklets were launched at the fourth Global Conference on CyberSpace (GCCS 2015): Sharing Cyber Security Information and Cyber Security of Industrial Control Systems.

The fourth Global Conference on CyberSpace (GCCS 2015) took place in The Hague, The Netherlands on April 16-17 2015. More than 1600 governmental, private sector and civil society representatives from 100+ nations gathered together to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behaviour in cyberspace.

Cyberspace is a domain that no single party or entity governs on its own. The internet houses multiple actors that are becoming increasingly interconnected and interdependent, in an enormous, complex environment where a balance must be struck between security, freedom and social and economic growth.

The Cyber Security track included a session on Building Public Private Cooperation in Cyber Security. In support of that topic, a number of documents were developed and handed over to the international community.
The Netherlands Organisation for Applied Scientific Research TNO was responsible for developing three of the deliverables which will be described below.

Towards Action

The first deliverable **From Awareness to action: bridging the gaps in 10 steps** is an interactive webpage. It is the result of the cyber security debates which take place at both the Board Level and the government policy levels at the earlier The Grand conferences (Amsterdam 2013, Rotterdam 2014), MERIDIAN and World Economic Forum (WEF) conferences. This deliverable is a stepping stone for the 2016 cyber security activities by the Dutch EU Presidency.

Information Sharing

The second deliverable is a booklet on **Sharing Cyber Security Information** which reflects the good practice stemming from the Dutch public-private participation approach. Moreover, knowledge collected about international good and bad experiences made its way into the booklet. Contributions by the Meridian CIIP community were included.

As the threat landscape is continuously changing, the sharing of cyber security related information between organisations – in a critical sector, cross-sector, nationally and internationally – is widely perceived as an effective measure in support of managing the security challenges. Information sharing, however, is not an easy topic as it comes with many facets.

> "Information Sharing is a mindset"

The booklet aims to support the cyber security and resilience governance. Its aim is to assist public and private policy-makers, middle management, researchers, and cyber security practitioners, and to steer you away from pitfalls.

Industrial Control Systems

The third deliverable is a booklet on **Cyber Security of Industrial Control Systems** (ICS). It was developed with support by the Meridian community and several associations and private organisations.

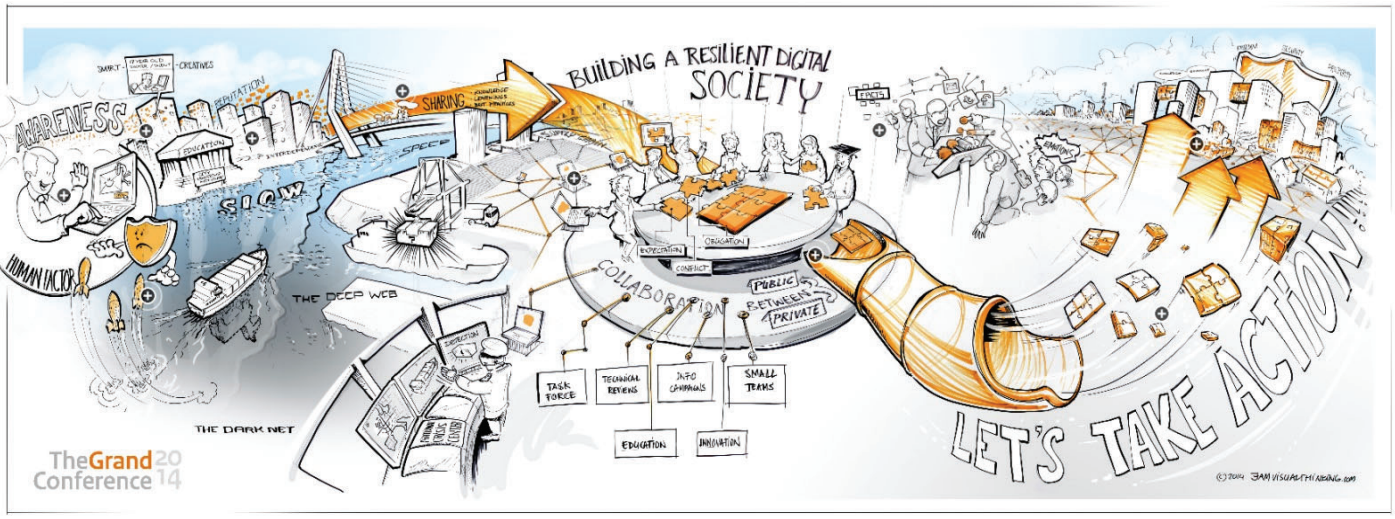
Crucial processes in most critical infrastructures, and in many other organisations, rely on the correct and undisturbed functioning of Industrial Control Systems (ICS)[1].

[1] ICS are also known under a wide variety of other names, such as SCADA, DCS, IACS, PLC, and PCS.

Eric Luiijf

Eric Luiijf is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. Since 2000 he contributed to many national and EU projects in the field of Critical (Information) Infrastructure Protection, both at the technical and policy levels. Eric has published many popular articles, reports, and peer-reviewed publications about cyber terrorism and warfare, C(I)IP, process control security, and cyber security. He has been interviewed many times by press, radio and TV on these topics.

e-mail: eric.luiijif@tno.nl



A failure of ICS may both cause critical services to fail and may result in safety risk to people and or the environment. Therefore, the cyber security and resilience of ICS is of utmost importance to society as a whole, to utilities and other critical infrastructure operators, and to organisations which use ICS.

> **"Good Morning with ICS"**
>
> Unconsciously you may have already met and used many ICS before taking the first sip of coffee."

Executive level

The good practice document first and foremost, provides private and public sector executives with an Executive Summary outlining the ICS risk and challenges. The document appeals to the executive leadership of organisations to address the clear and present cyber security danger to their organisations and our societies as a whole.

… and all others involved

Underpinning the Executive Summary, the good practice document provides governmental policy-makers, technical managers, ICS suppliers and others involved in the ICS domain with background and security awareness information about the cyber security challenges for ICS. Moreover, the document provides a perspective for action and pointers to seventy relevant resources.

References

From Awareness to action: bridging the gaps in 10 steps:
https://zoom.frontwise.com/public/4/towardsgccs2015#

Sharing Cyber Security Information:
https://www.gccs2015.com/sites/default/files/documents/Sharing%20Cyber%20Security%20Information%20GCCS%202015.pdf
or: www.tno.nl/infosharing

Cyber Security of Industrial Control Systems:
https://www.gccs2015.com/sites/default/files/documents/Cyber%20Security%20of%20Industrial%20Control%20Systems%20GCCS2015.pdf

or: www.tno.nl/ICS-security

email eric.luiijf@tno.nl

Securing National Critical Infrastructure

The Role of Public-Private Security Collaboration

Introduction: The State of CIP in Switzerland

Historically, Switzerland has been the home to longstanding and successful public-private partnerships: the militia system that is a key feature of the post-1848 modern Republic of Switzerland has placed seasoned professionals into all tiers of government at the community, cantonal and (con-) federal levels and harnessed professional skillsets in the service of the state with considerable success. However, in terms of close cooperation between private corporate entities and government authorities for the protection of national critical infrastructure from a security angle, Switzerland is relatively new to the task. Most of the attention regarding CIP has been paid to its utility and safety aspects, based on a post-Cold War and quasi-isolationist assumption that infrastructure and services reliability primarily is a maintenance task. This observation stands in stark contrast with pioneering endeavours of other countries, or, for that matter, national public-private cyber security projects, i.e. MELANI[2] and in a manner is ironic in that the arguably intuitive integral security approach practiced with vigour during the Cold War in Switzerland has lagged behind the strides taken by dedicated government agencies to protect the computer systems of private critical infrastructure owners and operators.

Nevertheless, once awareness for the evolving threat scape – from physical, logical and personnel threats with all their attendant attack vectors – had reached critical mass with both public and private decision makers[3], it proved a compelling incentive to pose a fundamental query: how much can a private corporate entity achieve in pursuit of protecting the infrastructure it owns and, at least to some extent, is both responsible and liable for? The answer may prove more elusive than assumed, yet its pursuit usually leads to a corollary query: not if, but to what extent ought the state and its institutions be involved in protecting highly critical assets, the functioning of which not only ensure business continuity for the corporate owner and operator, but effectively constitute vitally important processes to the operation of that self-same state?[4]

Vulnerability and Impact

Particularly piquant in the context of this discussion eventually leading to an integral approach to public-private partnerships and even to an explorative form of collaborative governance of such joint ventures, are the implications of both the above queries with special reference to impact and consequence of a failure of national critical infrastructure.

[2] Cf. Critical Infrastructure Partnership Advisory Council, Annual Update, Department of Homeland Security, at http://www.dhs.gov/sites/default/files/publications/nppd/cipac-2012-final-508-compliant-versionv2.pdf ; also view http://www.melani.admin.ch/ for the Swiss federal cyber security organisation.

[3] Cf. the Swiss minister of defence's recent deliberations on the changing face of national security policy of 16 March 2013 in the context of which CIP mentioned as a priority at http://www.news.admin.ch/message/index.html?lang=de&msg-id=48186

[4] The Swedes have defined the roles, responsibilities and financial burden sharing between their regulator-cum-inspectorate Svenska Kraftnät (SVK) and privately held TSO and DSO infrastructure owners and operators. Thus, SVK bears the cost for securing highly critical substations that connect into the bulk electricity transport network (400KV) and those elements of the electricity distribution network that assumes TSO functions (130KV). Private communications on the occasion of a security cooperation visit, Swissgrid-Vattenfall, 19-21 March, 2013. Also cf. http://www.svk.se/Start/English/About-us/

Doron Zimmermann

Doron Zimmermann PhD read for his doctorate at Cambridge University. Over the past fourteen years, he has been a Senior Researcher at the Swiss Federal Institute of Technology (ETH) with Center for Security Studies and subsequently took up the position of head of political risk analysis for a special lines insurance company. He was an Assistant Professor for International Security Affairs at National Defense University in Washington and practiced what he had taught as Head of Interagency Intelligence Integration on the Swiss government cabinet's Security Committee staff. From 2012, he has worked as Senior Manager for Security Affairs at Swissgrid. From 2012-2014, he has worked as Senior Manager for Security Affairs at Swissgrid. At present, Doron is a Senior Risk & Security Consultant with ISPIN, a leading company in the field of information and data security located in Switzerland.

e-mail:
doron.zimmermann@cantab.net

The more advanced a country's critical infrastructures are, the higher is the likelihood of such assets' interdependency and, hence, their vulnerability to multiple, distributed points of failure, up to and including vulnerability risk concentrations in the shape of single points of failure. For obvious reasons, Western countries are particularly affected.

Arguably, the acuity in regard to an infrastructure's criticality is highest at the sequential beginning of any given national economic value chain; with no energy to supply communications, guidance systems and fuel for transportation, water and food supply, delivery of vital medical services, to name but a few interdependencies, not only economic, but also socio-political functioning of a state will within the space of a few days grind to a jarring halt. Imagine, quite literally, a domino effect: the interdependence in this instance is an effective "if/then" proposition. Within a week, if one scenario is to be lent credence[5], the affected state is not only facing crippling damage to its national economy, but is likely witnessing the first signs of a crumbling national cohesion, beginning with plundering and riots due to supply problems and the shortage of essential goods and services. In the case of Switzerland, the economic losses incurred on a per diem basis are estimated to be in the range of between 12 and 42 billion CHF.[6]

The exceptional criticality of the energy sector is, indeed, vested in its position within the sequence of a national economy's value chain. Therefore, the cascading effects its potential failure would have on any other "subsequent" sector of a national economy, with attendant spill-over consequences across borders of adjacent countries, even affecting countries with no shared borders, would almost certainly be catastrophic. In the case of the bulk electric transmission system operation, its criticality is even more pronounced vis-à-vis energy producers and distribution system operators: hydro- and nuclear energy production is the subject of considerable security investment, while decentralized ownership of distribution system operations mitigate the problem of single points of failure. To use an analogy from the energy sector, even pipelines tend to be better protected and less vulnerable than the bulk transmission system grid. Though both energy transport systems are usually built above ground, there is potentially fewer, geographically dispersed pipeline-miles to protect, than the spread out, highly complex bulk transmission grid has to offer. Or, in other words, the streamlined backbone of national and international oil transport may offer fewer vulnerabilities in structural terms than its equivalent in the power energy sector, albeit without taking into account either exposure to dynamic man-made risk or absolute dimensions.

The Swiss CIP Endeavour

The implications of criticality and vulnerability of key infrastructure dawned on the Swiss federal government at a comparatively late point in time: while in America the President's Commission on Critical Infrastructure Protection produced a seminal report published in October 1993, which acted as a harbinger of two Presidential Decision Directives, (PDD-62 & 63) addressing CIP in May 1998[7], no such equivalent was forthcoming in Switzerland until the early 21st Century. With what is today commonly known as the "SKI-Programme" (SKI stands for the German "Schutz kritischer Infrastrukturen")[8], the Swiss federal government launched a comprehensive yet pragmatic undertaking in the area of CIP that in its comprehensiveness is reminiscent of Switzerland's total defence approach cultivated after the Second World War: in this the SKI programme does not fall short of other national federal programmes' traditional emphasis on thoroughness. Accordingly, an all-hazards approach sets the stage with respect to the SKI related threat-analysis in accordance with the principle of comprehensiveness. To the keen observer, an "anthropologically" induced overreliance on impact analysis commonplace in a country dominated by its financial industry may mar the otherwise flawless execution of this sterling government initiative. All sectors of the economy have, since the inception of the programme, been mapped and their respective designated critical infrastructures are being inventoried in a continuous drive to keep this repository up-to-date. The programme, which in organisational terms is a part of the Federal Office of Civil Protection in the Swiss Ministry of Defence, had its major breakthrough with the adoption of the CIP basic strategy of July 2009 by the Federal Council; on 27 June 2012, the Swiss executive passed the CIP Strategy, which irrevocably established CIP as a priority subject on the national security agenda.

An offshoot of the SKI-programme, or rather, the key derivative of the 2012 CIP Strategy is the Guide to Critical Infrastructure Protection.[9] The Guide has been peer reviewed within the relevant departments of the federal administration in Berne, but remains an internal document and is as yet not published. In spite of the executive character of its parent document, the CIP Strategy,

[5] Cf. Marc Elsberg, „Blackout" (Blanvalet, 2012); http://www.blackout-das-buch.de/ ; the seminal study on the effects of a blackout used in Elsberg's dramatization "Blackout" was conducted by the Berlin School for Economics and Law and can be found at http://www.tanknotstrom.de/assets/content/images/pdfs/Szenario%20Berlin_2012.04.23.pdf, accessed 22 March 2013.

[6] http://www.stromzukunft.ch/versorgung/stromnetz/, accessed on 8 March 2013.

[7] Myriam Dunn Cavelty, Manuel Suter, „Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, *International Journal of Critical Infrastructure Protection*, (August 2009), pp. 2-3.

[8] A recap of the SKI Programme can be found at http://cgd.swissre.com/global_dialogue/topics_info/risk_management_insurance/RDS_IRM_Fostering_Infrastructure_Resilience_Article.html, "Critical infrastructures in Switzerland and the provision of essential goods and services" by Willi Scholl, Stefan Brem and Ruedi Rytz in *Integrative Risk Management: Fostering Infrastructure Resilience*, pp. 72-83 (Rüschlikon, Swiss Re Centre for Global Dialogue, 2012); for further information cf. SKI website at www.infraprotection.ch

[9] „Leitfaden zum Schutz kritischer Infrastrukturen," internal draft document, Swiss Office of Civil Protection, 23 July 2012.

the Guide itself is currently not intended to represent a regulatory framework binding upon the owners and operators of national Critical Infrastructure, although these are its primary target group. Its significance, however, goes beyond an attendant optional or advisory DIY to the aforementioned national CIP Strategy and is borne out by the fact that its utility lies in its potential to close a gap in minimum security standards. To date, there is no applicable or binding minimum security standard for private owners and operators of national Critical Infrastructure in the energy sector, with the exception of energy producers using nuclear power technology.[10]

Standards in Energy Security and the Need for PPP Collaborative Governance

On 3 January 2013, the mandated national transmission system operator of Switzerland, Swissgrid, assumed control and, hence, responsibility for all the bulk transmission system infrastructures – from command and control systems, e.g. supervisory control and data acquisition (SCADA) systems, substations to approximately 15,000 pylons and 7000 kilometres of power grid. Previously spread across 18 corporate entities according to one account,[11] the consolidation had a variety of economic synergetic advantages, such as reducing the cost of bulk power transport, primarily by the reduction of disparate investments and duplications of maintenance and operations costs of previously multiple owners and operators. This change went hand in hand with the concomitant increase in national and international competitiveness; over time, we will likely see a decrease in absolute costs.

However, there is also a drawback from a security vantage in that the concentration of the assets also created a closer fusing of previously dispersed command and control nodes. The security dimension was either to be defined at a later stage at the time the decision was taken to incorporate a national transmission system operator, i.e. Swissgrid, or, considering Switzerland's record of neutrality and political stability, it was simply not considered relevant. Complicating the security situation is the historic circumstance that since Switzerland's transmission system grid had been an achievement of the post-World War II era, today stretches of it are older than 60 years and require not only maintenance, but replacement. Moreover, with transport capacity in the existing grid having reached its limit [12] , Switzerland's transmission system grid is in dire need of expansion. Expansion of the grid, in turn, will likely spark opposition and it is safe to assume that not all critics and sceptics will chose due process of law to vent their spleen. Consideration of legislations to shorten permit periods for the construction of additional pylons which are to mark the future landscape, as well as measures for the compulsory nationalization of assets and real estate towards the expanded grid are not likely to improve opponents' willingness to compromise and, in fact, will likely serve to harden attitudes in the future.

In spite of the undeniable relationship of energy security as a prerequisite for energy reliability, which in general cannot be said to constitute its ineluctable product, the former was never given its due consideration. As of this writing, though belatedly, the understanding that there simply cannot be energy reliability without first securing the energy infrastructure is making headway, albeit at a crawl. Arguably, the consequent cumulative security risk created with Swissgrid's incorporation coupled with the above explained structurally immanent vulnerabilities to the infrastructure have perforce created a potentially higher exposure to security risks from a multiplicity of attack vectors, including, but not restricted to, the logical, physical, organisational spheres. Moreover, in assuming responsibility for the bulk transmission system of Switzerland, Swissgrid as a legal corporate entity also assumed liability for the assets it had taken over. Would the implications of a future attack on the energy power hub represented by Swissgrid go well beyond the corporation's financial and security saturation capacity; and would it then almost certainly damage the national economy, impinge upon the capacity of Switzerland's neighbours to export or import energy transported through Switzerland's bulk transmission system grid and may such a scenario of a prolonged and regional or national blackout even lead to an aggravated security situation within Switzerland? If so, would the risk to Swissgrid have to be assumed to be at a sovereign level? These speculative questions do not yet have definitive answers. Yet the Swiss Office of Civil Protection's assessment in this regard puts paid to this claim.[13] The problem is that other than a threat passing the threshold to traditional interstate war, nobody really knows with whom and "where" the responsibility and liability of the corporation to protect the national critical energy infrastructure in its care begins or ends. It is as per the writing of this paper not clear at which point of an unfolding security-relevant event any given security related incident or crisis is to be considered as within the remit of the designated cantonal or federal government security agencies: the division of roles and responsibilities between private corporations and government agencies in matters security and critical infrastructure protection is anything but clear.

As if this inconclusive state of affairs in the face of a new cumulative risk to the energy transmission system operation of Switzerland were not enough, no responsible authority in the country presumably is in a position to either issue or regulate

[10] Cf. Swiss nuclear energy law and directives at http://www.admin.ch/ch/d/sr/7/732.1.de.pdf and http://www.admin.ch/ch/d/sr/7/732.11.de.pdf , respectively.

[11] Communication from Swissgrid's CEO, Mr P.-A. Graf, 14 March 2013.

[12] According to one account, the Swiss transmission system grid is at overcapacity during 1500 hours p.a.

[13] The Swiss MoD considers the energy sector to constitute one of the few „deep red" elements of the 31 listed critical sectors of the national economy. Cf. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/kritische_infrastrukturen.parsys.77606.downloadList.90979.DownloadFile.tmp/28teilsektorene.pdf

minimum security standards for energy security, not to speak of inspecting their implementation by owners and operators of national critical infrastructures. In the absence of robust, national security minimum standards, confronted with mounting attacks on the critical information infrastructure of Swissgrid or corporate entities in the country [14] and in the face of increasingly urgent queries by senior management regarding the state of security, the Corporate Security branch was compelled to "borrow" appropriate standards. The challenge of finding relevant standards is that generic standards, e.g. the 2700x series of standards by the International Standards Organisation[15], are too broad or too shallow due to their non-industry specific nature and thus rarely provide feasible and pragmatic application opportunities in the context-sensitive security TSO environment, especially its pronounced vulnerability problem with respect to the exposed grid cable and multitude of potentially neuralgic pylons. It is for this reason that Swissgrid Corporate Security eventually elected to benchmark its logical security measures against the CIP standards issued by the North American Electricity Reliability Corporation. Known as the NERC-CIP standards, and divided into nine segments (NERC-CIP 001-009) [16], Swissgrid since their adoption has concentrated on the implementation of standards 002-009, which for the most part address cyber security measures. NERC-CIP 001[17], the standard which addresses security challenges of a more integral nature, notably sabotage and insider threats, was for the time being set on the backburner and hence opened yet another kink in the armour in the sense that all the focus on highly sophisticated cyber-warfare and its equally complex body of countermeasures left, figuratively speaking, the door ajar to low-tech, but no less perilous, attack vectors, such as conventional terrorist operations, sabotage and traditional industrial and economic espionage.

Based on the all-hazards risk analysis approach and a continually groomed inventory of infrastructures, as well an understanding of their relative interdependencies, the SKI-programme's Guide emerges as the compendium of best practice for national CIP. Albeit not industry-specific and therefore potentially imbued with a "weakness" similar to that of the corresponding ISO security standards, the SKI Guide has the advantage of addressing the subject of CIP-specific integral security with the 28 Swiss economic sectors in mind, whose risk analytic properties, i.e. the threats to them and their respective weaknesses, shaped its outlook. The Guide at a minimum partially bridges the gap between the depth of the NERC-CIP's industry specificity and the horizontal breadth of ISO security standards, while being a "native" product designed to meet national challenges.

The SKI-Pilot Project

With the passage of the SKI Strategy through the Swiss Federal Council in July 2012, the eponymous Guide, though still in a mature drafting stage, was upgraded in the sense that post-ratification it was considered part and parcel of a CIP programme underwritten by the government's executive branch. Though not having the force of law once finalized and ratified, to some it has become clear that the SKI-Guide will at the very least constitute the foundation or a capstone of any future regulatory framework – and for lack of viable alternatives, some would say it does so today. With this understanding in mind, Corporate Security at Swissgrid was well placed to promote the case for proposing to the relevant government entities, starting with the originator of the SKI-programme at the Office of Civil Protection, and including the federal agencies for national supply (BWL), energy (BFE) and two federal security organizations, that Swissgrid offer itself as a "pilot project" for the application of the SKI-Guide. Additionally, the regulatory authority, the Electricity Commission's (Elcom) participation is designed into the project-plan as an indispensable partner in this venture. Thus, following months of preparatory "shuttle diplomacy" between Berne and Swissgrid's offices, the SKI Pilot Project was launched in the autumn of 2012; it held its initial meetings, during which the project scope and time-table were agreed upon by the participants, in early 2013. The project's governance is collaborative: though it is a public private partnership, the driving interest behind the project may not only be a mutually beneficial arrangement, but instead may well be impelled by a maturing and more thorough understanding of the shifting threat-scape; and the forbearance thus engendered in the parties involved. The background to this observation is a nascent collective understanding among the participants of not only the high interdependency between the state with its sovereign responsibilities of national supply on the one hand, and the owners and operators of national critical infrastructure with special reference to TSOs on the other. The mutual dependency between the two parties is both fundamental and in terms of the complexity of modern societal infrastructural interlacing, near absolute. The first workshop addressing the identification of critical processes at Swissgrid was scheduled for late March 2013; several other gatherings focussed on themes such as threat- and vulnerability-scapes [18], which eventually are to coalesce into a comprehensive risk analysis; it, in turn, is the basis for a gap analysis, from which recommendations are to be derived from both the corporate and CIP perspectives. The SKI Pilot Project was slated to run for approximately two years and move through the currently undisclosed risk analytic and management steps of the SKI Guide in order to produce a short final report featuring, inter alia, the previously mentioned recommendations regarding security measures. This final report is intended to be submitted to the

[14] Regarding the most recent cyberattacks, purportedly carried out by, or with the connivance of, Chinese government organisations cf. http://intelreport.mandiant.com/mwg-internal/de5fs23hu73ds/progress?id=ZCJjbRfMGl

[15] Cf. http://www.27001-online.com/

[16] NERC's CIP standards are listed on the standards site at http://www.nerc.com/page.php?cid=2%7C20

[17] Op. cit. http://www.nerc.com/files/CIP-001-2a.pdf

[18] No final decision has as yet been taken on whether to address exposure to risk as a set part of the SKI Pilot Project.

office of the head of the Swiss Federal Department of the Environment, Transport, Energy and Communications (UVEK/DETEC) with the ultimate goal of pinpointing need for action in the sphere of energy security and the protection of critical energy infrastructure protection.

Conclusion: Challenges to Collaborative Governance in Public Private CIP Partnerships

The SKI Pilot Project is a pioneering undertaking in the area of public private security cooperation in Switzerland and stands out due to its genuinely collaborative governance framework underpinned by its participants' common understanding. It is, as explained above, well underway to produce a key gap analysis of the extent to which corporate entities can (afford to) secure assets within their remit as private organisations and the requirements as set by the federal and cantonal authorities with a view to national security and especially with regard to protecting highly critical infrastructures. Yet there are more elusive challenges to meet beyond articulating the divergences between private and public stakeholders potentially disruptive to any joint CIP project. A key obstacle to be surmounted is the application of the need-to-share principle between providers of early warning intelligence – especially of government provenance – and owners and operators of key critical infrastructures, up to and including the introduction of a clearance process [19] . But the information requirement, too, it should go without saying, is bidirectional. (Which is not necessarily the case, as corporate CIP owners and operators have in the past withheld information about being successfully targeted, e.g. by hackers or corporate or government spies. The reason is obviously to sustain good investor relations and avoid reputational impact). As Donahue and Zeckhauser put it:

The most consistently valid argument for a collaborative approach to infrastructure security turns on information. The government itself almost certainly lacks the fine-grained understanding of particular infrastructure assets..., necessary to mount the most robust and least costly defences. Yet the public sector likewise can have privileged or exclusive access to information and procedural options – intelligence data, negotiations with foreign governments, the right to detain a suspect or tap a phone line – that could, in principle, be extended to the private sector but generally are not.[20]

Alas, the latter issue still constitutes an impediment to effective public private security collaboration – at least formally. Discussions are underway to amend (others would argue to overhaul) the intelligence service law (NDB) to the effect of introducing dedicated security personnel of owners and operators of highly critical infrastructures into an expanded intelligence fusion platform operated by the Federal Intelligence Service [21] ; Swissgrid would, in all likelihood, qualify for membership.

As seen by the present writer, the key structural challenge that the SKI Pilot Project had to meet was the successful streamlining and management of the potential, even likely, fluid public-private divergence of priorities. For this reason, Donahue and Zeckhauser state:

Before designing a collaborative infrastructure security effort, government must first appraise the threat-reduction goal. It must map, as precisely as data permit, both the public and the private risks embodied in the status quo – the nature and dimensions of the threat, the degree to which public and private vulnerabilities overlap or diverge, and the major uncertainties surrounding this appraisal. This first step, in short, involves figuring out what success looks like.[22]

It is therefore imperative that public private governance in CIP formulate a clear, common goal based on a common understanding of mutual necessity.

In light of the responsibility for the national bulk power energy supply; an absence of binding regulatory security standards and the self-evident vulnerability of the arguably single most critical infrastructure with an immediate, palpable economic and public security impact across the length and breadth of the country, Swissgrid is well advised to encourage a collaborative governance CIP framework with the relevant federal government agencies. This set of circumstances applies with some urgency to the questions of roles, responsibilities and, from a corporate point of view in particular, to liabilities of privately organized owners and operators of highly critical national infrastructures. The reasons are not all self-evident, yet for that no less compelling: not only does the currently manifest endeavour at public private CIP collaborative governance, the SKI Pilot Project, come equipped with a government-cleared methodology of determining critical processes and, hence, protection targets, thus creating the foundation for defining a division of labour and clarifying responsibilities; it also gives Swissgrid the opportunity to provide direct input into what might well be tomorrow's regulatory capstones. Thus, the federal government benefits directly from the know-how and skills of the CI owner and operator; and the private entity, as a quid pro quo, can help shape the future regulatory environment. Ultimately, where there are real stakes for the involved parties, a mutual effort arguably has the best chance of succeeding.

[19] A proposal from the Swiss Ministry of Defence to provide clearances for key personnel employed by highly critical infrastructure owners and operators is under way concurrently with the Swissgrid CIP project.

[20] J.P. Donahue and R.J. Zeckhauser, „Public-Private Collaboration for Infrastructure Security," in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (Cambridge University Press, New York, 2006), pp. 429-456, p. 437.

[21] Also cf. fn. 17.

[22] Donahue and R.J. Zeckhauser, 453.

ARES Conference
The International Dependability Conference

Call for Participation

The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism (FCCT 2015)

August 24–28, 2015

Université Paul Sabatier Toulouse, France

The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism

to be held in conjunction with ARES EU Projects Symposium 2015, held at the 10th International Conference on Availability, Reliability and Security (ARES 2015 –. www.ares-conference.eu) and organized by the FP7 project CyberRoad www.cyberroad-project.eu.

With the constant rise of bandwidth available and with more and more services shifting into the connected world, criminals as well as political organizations are increasingly active in the virtual world. While Spam and Phishing, as well as Botnets are of concern on the cyber-crime side, recruiting, as well as destructive attacks against critical infrastructures are becoming an increasing threat to our modern societies. Although reactive strategies are useful to mitigate the intensity of cyber-criminal activities, the benefits of proactive strategies aimed to anticipate emerging threats, future crimes, and to devise the corresponding countermeasures are evident.

The aim of the **First International Workshop on Future Scenarios for CyberCrime and CyberTerrorism** is to anticipate the future of cyber-criminal activities, enabling governments, businesses and citizens to prepare themselves for the risks and challenges of the coming years. The first step towards the creation of a strategic roadmap for future research on cyber-crime and cyber-terrorism is the building of scenarios on the future transformations of the society, business activities, production of goods, commodities, etc. The aim of FCCT 2015 is to create a forum on scenario building and creation of research roadmaps for cyber-crime and cyber-terrorism. The building of future scenarios should allow the identification of the main driving forces and factors that will shape the evolution of cybercrime and cyberterrorism. A principled analysis of the differences between the current state of play and the future scenarios should allow drawing roadmaps and priorities of future research on cybercrime and cyberterrorism.

The influence of triggered earthquakes on critical lifelines in the North of the Netherlands

Introduction

The production of the gas fields in the North of the Netherlands leads to changing rock stresses in and around the reservoir. The change in stress on existing fault planes can lead to a sudden small slip of the plane with a release of seismic energy as a consequence. Since 1986, a low intensity seismic activity is present in the Groningen gas-field area (Netherlands), due to the tremors following the compaction of the gas reservoir due to stress decrease. An extensive study performed by the Dutch Meteorological Institute (KNMI), see Dorst et al. (2013), shows that in the last decades (2003-2013), the seismic activity changed from low intensity activity with a constant events rate per year to a higher rate with slightly increasing magnitude. The depth of the earthquakes is at 2.5 - 3 km, being the depth of the gas reservoir. The reservoir consists of Rothliegendes sandstone with a thickness of 150- 200 m. and is overlain by Zechstein salt . On 16 August 2012 an earthquake with a local magnitude of M = 3.6 occurred near Huizinge in the neighbourhood of Loppersum in the Northern part of the Province of Groningen. This earthquake is the largest earthquake so far.

In the North of the Netherlands and the rest of the world the energy and water pipelines and the electricity connections can be considered as the lifelines of our society. Damage to pipelines may lead to environmental disasters or can in worse case lead to casualties, in case of toxic or flammable substances transported in pipelines. The damage or the disruption of the electricity lines also will cause a major economic impact, especially for industrial areas, The Groningen gas field serves the rest of Netherlands and is also used for export. Furthermore imported Norwegian and Russian gas passes through the area affected by earthquakes. A large portion of the electricity production is located in the Eemshaven area and high voltage lines cross the earthquake affected area. Also, electricity power stations are present in the earthquake area. Furthermore production as well as gas transmission for a large portion depend on the availability of high voltage power.

Studies on the vulnerability of pipelines are available in literature (O'Rourke (1998) or Pitilakis et al (2010)) based on observational analysis of the performance of lifelines subjected to earthquakes of large magnitude. However in the north of the Netherlands the triggered seismic activity is not of tectonically nature and is characterised by short duration of the signal and triggering a local seismic response. Therefore recently several studies have been carried out to investigate the lifelines in the North of the Netherlands.

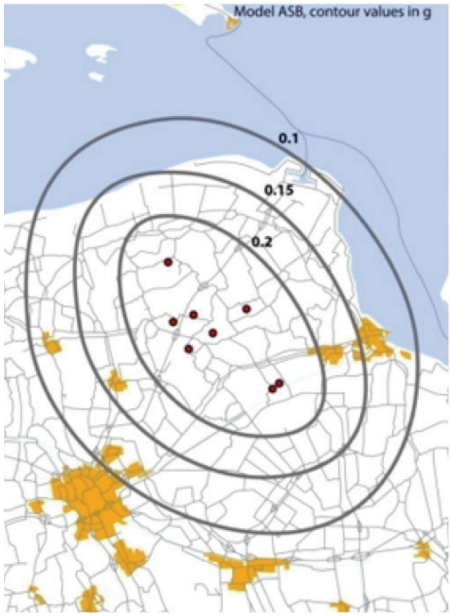


Figure 1: Contours for the highest median PGA due to a Mw=5 event in the area spanned by historical M≥3 events. Seismic sources are indicated as red circles, contours as grey lines. Median values are shown in g (Dost et al. 2013).

Henk Kruse
senior researcher at Deltares.

e-mail: henk.kruse@deltares.nl

Mandy Korff MSc
Business Development and Senior Advisor at Deltares.

e-mail: mandy.korff@deltares.nl

Jan Spiekhout Executie Senior Consultant at DNV-GL has contributed as well.

Earthquakes

The magnitude of an earthquake is often expressed using Richter's scale or by means of the peak ground acceleration (PGA). An earthquake leads to two types of soil deformations near the surface:

1) **Temporary soil movement** due to the soil vibration due to the passing of the waves. When the waves are near to the surface an increase of the wave amplitude is possible, where the soil properties and layering influences the amplitude of the vibrations.

2) **Permanent soil movement** can also be induced by the earthquakes. The following permanent movements can be distinguished:

- Liquefaction of loose packed granular soils.
- Densification of granular soils.
- Mass movements along natural or artificial slopes.
- (Tektonic) movement along faults.

The term "liquefaction" indicates a phenomenon for which a saturated, cohesion less soil loses its shear resistance due to the accumulation of plastic deformations caused by transient and cyclic force actions in un-drained conditions. Liquefaction can lead to large permanent soil deformations and is therefore an important mechanism in the evaluation of the effects of earthquakes. The Eurocode 8 (2005) is the guideline for the assessment of all types of structures such as pipelines and electricity pylons, but also the installations such as power stations and pressure units.

Figure 2: An example of liquefaction due to a tectonic earthquake (Roermond 1992)

Lifelines

Lifelines are often grouped into six principal types of systems (in alphabetical order): electric power, gas and liquid fuels, telecommunications, transportation, 3 wastewater facilities, and water supply. These systems share three common characteristics: geographical dispersion, interconnectivity, and diversity (O Rourke, 1998). Lifelines are geographically dispersed over broad areas, and are exposed to a wide range of seismic and geotechnical hazards. They are interconnected and interdependent. Each lifeline system is composed of many interconnected facilities and is influenced by the performance of other lifeline systems.

In this paper the vulnerability of the following groups of lifelines with respect to triggered earthquakes in the Netherlands are considered:

- Gas transportation network
- Electricity transportation network

The local distribution networks are not considered.

The subsequent figures show the two lifeline networks schematically.

Evaluation fragility of lifelines

In order to evaluate the impact of a triggered earthquake on the electricity and gas network in the North of the Netherlands, a global analysis was carried out. In this analysis the strength of the different elements of the network was considered. The strength of the element was defined as the maximum peak ground acceleration at which

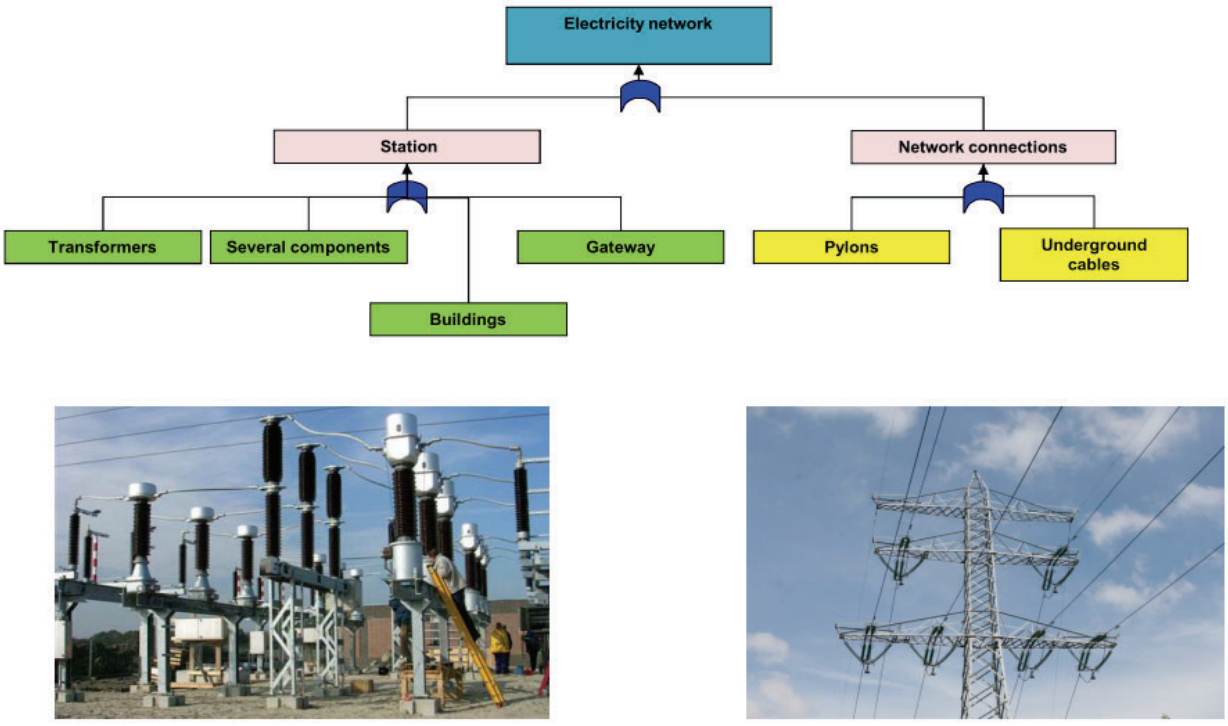


Figure 3: The Electricity transportation network

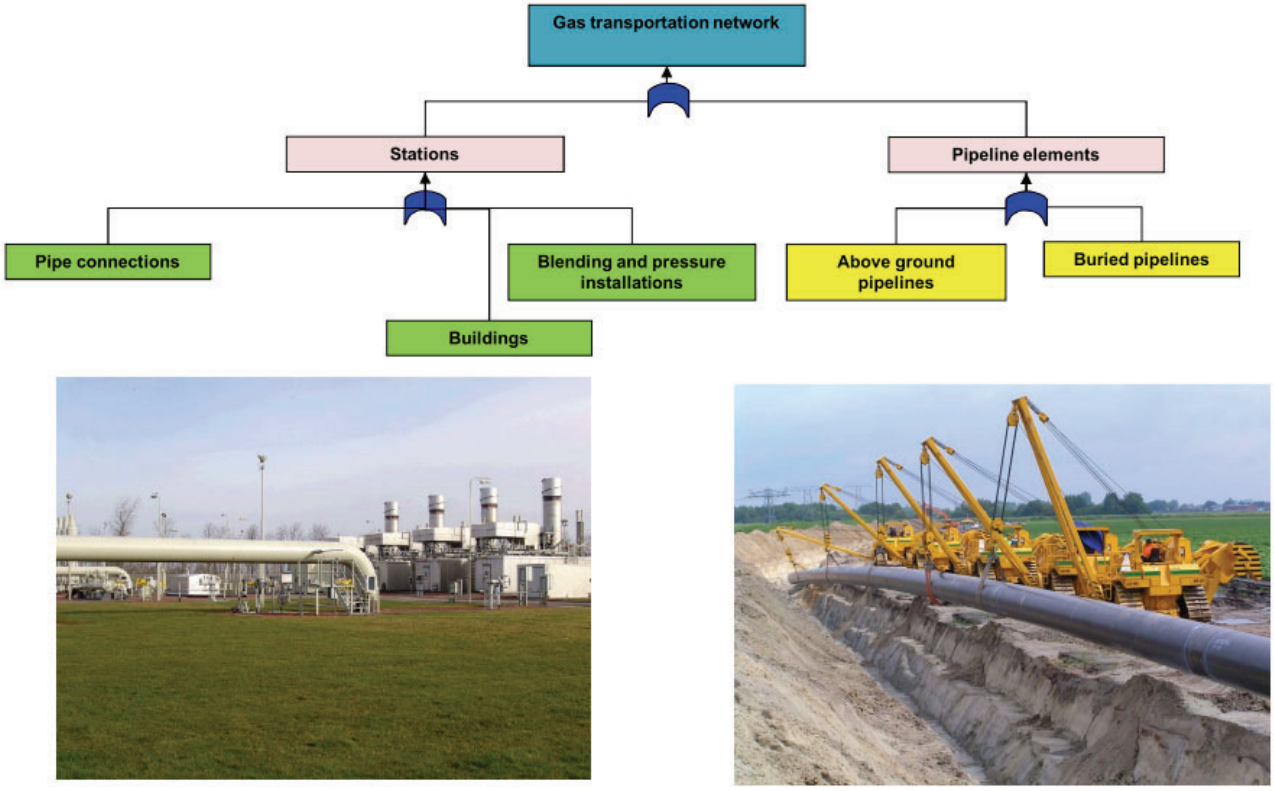


Figure 4: The Gas transportation network

damage could be expected. This maximum value was deduced by calculations or by specifications available for certain installations and components.

The gas transportation pipelines in the north of the Netherlands are buried and the soil cover is more than 1 meter. The predominantly steel pipes are able to withstand an earthquake of significantly more than 0,5 g. Some sections with curves or sections where the pipelines cross other infrastructure such as railways, river dikes and canals or rivers are less robust than the straight sections, but if the condition of the pipeline is good (some poorly welded pipeline sections can be expected to withstand a significantly lower earthquake level), these pipeline sections are also able to withstand an earthquake of about 0,5 g. The connections of the above ground pipelines at the blending and pressure stations are not yet all considered in detail, but it appears that the increase in stress level of the above ground pipelines is not extremely high. During the analysis (Korf et al 2013) was recognised that the configuration of the above ground pipelines and the presence of supports significantly influence the resonance effect.

The above corresponds to findings in international literature (ASCE 2011), about experiences with earthquakes:

Figure 5: Example of a designed bearing support that is not designed for earthquakes ("one foot support")

- Steel pipelines continuously welded and with good weld quality, are able to withstand the shaking effect induced by an earthquake.
- Piping on stations with simple piping configurations in general possess no problem with regard to the shaking effect from earthquakes.
- Machinery, if bolted to the floor, generally anchor bolts are oversized, possess no major problems with regard to the shaking effect from earthquake. Because of vibration there is a probability of a trip, but after the earthquake machinery can often be restarted.

Besides the evaluation of the so called piping systems, secondary mechanisms were also evaluated. Although a first consideration does not emphasize many risks, a further analysis showed the importance of the following mechanisms:

- Collapse of masonry buildings at the gas reception locations on operation equipment.
- Collapse of not well-designed bearing supports.
- Collapse of raised computer floors on which the operation system is situated.

Secondary mechanism both for the electricity network and the gas network can be important. Problems can be expected with the raised floors and control and computer cabinets in control rooms. Unreinforced raised floors with cabinets placed on the floor or cabinets which are not fixed, may cause significant damage to the control room. The consequence could be an out of service period with a duration of several months.

Figure 6: Raised floors and cabinets in control room on a raised floor.

Disruption of electricity lines is internationally rather common in case of earthquakes. Until now, no damage has been reported in the North of the Netherlands resulting from the gas extraction induced vibrations. The Netherlands is known to have a high level of supply security for high voltage. Although the stations with the transformers are not located in the area where the epicentres of the future highest magnitude earthquakes are expected, there is a possible malfunctioning of the different components of the transformer station. Most of the components belong to vibration class AF 3 (a maximum acceleration of 0,3 g), but some of them start mal functioning at 0.2 g. The transformers themselves are designed to withstand accelerations of 0.5 g and can be considered as robust, however because of wave effects (oil filled transformer) from the earthquake there will be a trip that can easily be restored after the earthquake. The different types of pylons can with stand an earthquake of 0,25 g without damage. It should be noticed that especially the new types of pylons can withstand an earthquake with a higher PGA. Besides the evaluation of the different components and the pylons, the secondary equipment such as operation devices need to be evaluated because it is expected that some devices can start malfunctioning at PGA levels of 0,1 or 0,2 g.

The above mentioned evaluation results are general results achieved by a global analysis. It should be mentioned that the effect of permanent ground deformation must be studied on a more detailed level for a final conclusion about the networks. The permanent soil deformations depend on the local soil conditions and are therefore site specific. Especially the effects of liquefaction require further investigation.

Conclusions

Recent developments in the analysis of seismic activity of the Groningen gas field showed that the estimated maximum magnitude for induced events in the region can be higher than previously thought. Due to the increase of the expected peak ground acceleration, the most important lifelines of the Northern Netherlands were evaluated with respects to earthquakes. The electricity network and the main gas transportation network were evaluated.

In the analysis carried out for the evaluation, the strength of the different elements of the networks was considered. The strength of the element was defined as the maximum peak ground acceleration at which damage could be expected. The results of the evaluation show which elements require attention and can be used for the definition of further research.

The permanent soil deformations depend on the local soil conditions and can be of major importance for a network. Especially the effects of liquefaction may yield large permanent ground deformations and require attention in further investigations

Literature

Dost B., Caccavale M., van Eck T., Kraaijpoel D. (2013). "Report on the expected PGV and PGA values for induced earthquakes in the Groningen area" Report KNMI (Koninklijk Nederlands Meteorologisch Instituut),Utrecht, The Netherlands.

Eurocode 8 (2005) Design of structures for earthquake resistance. General rules, seismic action, design rules for buildings, foundations and retaining structures. Tomas Telford books, first published in 2005

O'Rourke, T. D. (1998) An Overview of Geotechnical and Lifeline Earthquake Engineering, ASCE Geotechnical Special Publication No. 75, Pakoulis, P., M. Yegian, and D. Holtz, Eds., Reston, VA, Vol. II, 1998, 1392-1426.

Pitilakis K., Crowley H., Kaynia A.(2014) " SYNER-G: Typology Definition and Fragility Functions for Physical Elements at Seismic Risk" ISBN 978-94-007-7872-6. Spinger

Korff M., H.M.G. Kruse,. T.P. Stoutjesdijk, J. Breedeveld, G.A. van den Ham, P. Holscher, G. de Lange, P. Meijers, E. Vastenburg, Vermaas. And M.A.T. Visschedijk (2013) Effecten geïnduceerde aardbevingen op kritische infrastructuur Groningen Quick Scan naar de sterkte van de infrastructuur, Deltares report Delft

ASCE (2011) Guidelines for Seismic Evaluation and Design of Petrochemical Facilities, second edition, ASCE, ISBN 13: 978-0-7844-1140-7, Reston VA, 2011

ROADAPT:

Roads for today, adapted for tomorrow

The goal of CEDR project ROADAPT is to provide risk based methods and tools for assessing climate change risks for roads, towards an action plan for adaptation

Infrastructures are the backbone of our society. Citizens, companies and governments have come to rely on and expect uninterrupted availability of the road network. In the same time it is generally understood that the world's climate is changing and that this will have significant effects on the road infrastructure. Since road infrastructure is vital to society, climate change calls for timely adaptation.

However there are great uncertainties involved in both the projections of future climate change plus their effects on the road infrastructure and related socio-economic developments. In the meantime, there is a constant need for decisions and development of the road transport system.

The ROADAPT project is part of the CEDR Call 2012 'Road owners adapting to climate change' in which is stated that one of the most important tasks of the road owners is the prioritisation of measures in order to maximise availability with reasonable costs. This includes a risk based approach addressing causes, effects and consequences of weather related events to identify the top risk that need to be taken action on with mitigating measures. In this respect the RIMAROCC framework (Risk Management for Roads in a Changing Climate) has been developed within ERA NET ROAD in 2011.

Objectives

ROADAPT aims at a further development of this framework into practical and useful methods for road owners and road operators. Output of the ROADAPT project is one ROADAPT-RIMAROCC integrating guideline containing different parts (Figure 1):

A. Guidelines on the use of climate change projections.
B. Guidelines on the application of a QuickScan on climate change risks for roads.
C. Guidelines on how to perform a detailed vulnerability assessment.
D. Guidelines on how to perform a socio economic impact assessment.
E. Guidelines on how to come to an adaptation strategy.

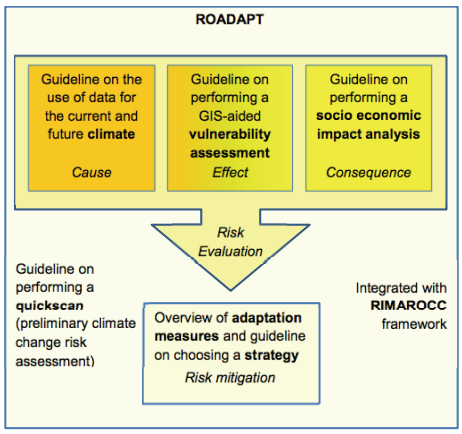


Figure 1: The ROADAPT guidelines

Output

Climate change

Part A provides background information and guidelines for tailored and consistent climate data and information for studies on the impact of the current and future climate for transnational road networks in Europe, suitable for National Road Authorities (NRA's). The document can be used by NRA's to judge the climate information that they receive from e.g. (impact) research institutes, consultancies, and to find answers to their questions. It can also be used by impact researchers and consultancies to select the most appropriate datasets and methods for a certain application. Also requirements related to climate data are included.

Thomas Bles

senior consultant at Deltares.

Thomas worked on the ERA NET ROAD project RIMAROCC (risk management for roads in a changing climate). The results of this research project have been applied on the Dutch national highway network, aiming at gaining insight in the risks for flooding plus an action perspective for keeping in control in the future.

Since 2012 he is the coordinator of the CEDR ROADAPT project that aims at developing hands on methods as an extension to the RIMAROCC framework. The gained experiences are now used for the FP7 INTACT case study that focuses on extreme weather impacts on the functioning of the Rotterdam harbor with its hinterland connections.

e-mail: thomas.bles@deltares.nl

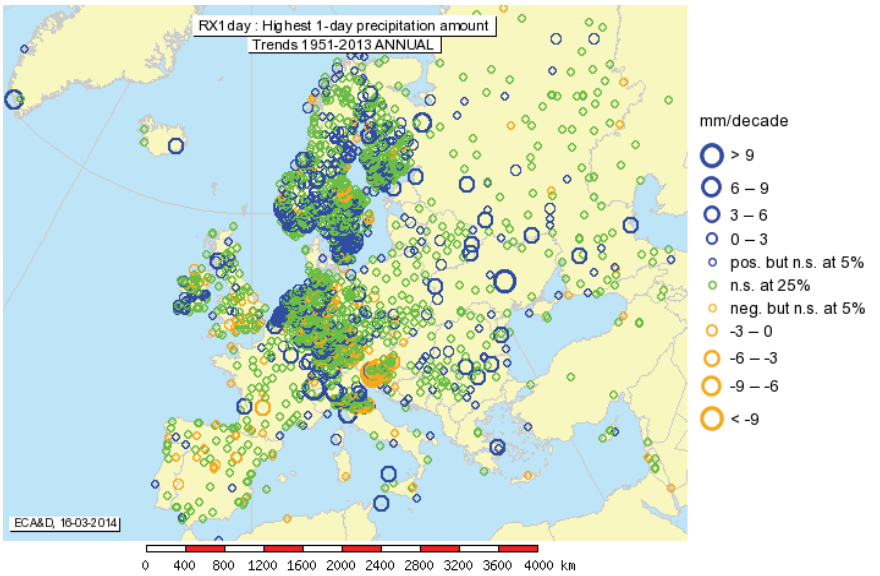


Figure 2: Trend in highest 1-day precipitation amount per year over the period 1951-2013 (ECA&D)

QuickScan

Part B provides a QuickScan method that preliminary estimates the major risks that can be associated with weather conditions both in the current climate and in the future, together with an action plan for adaptation. The identification and light-assessment of top risks allows a road authority and/or road operator to consciously and effectively focus on specific areas in their network and/ or on specific threats.
A founded first impression of climate (change) risks plus an action plan for adaptation is assessed in the QuickScan, by bringing all available knowledge, information and especially experiences of stakeholders together in three workshops. During implementation of the QuickScan method in the case studies it was learned that the brainstorming process in the QuickScan method showed to be important in terms of team building. The approach develops awareness on climate change issues, and climate related risks in general. This helps developing adaptation strategies.

Vulnerability assessment

Part C provides efficient tools for assessing vulnerabilities within the TEN-T road network. A new vulnerability assessment method, *ROADAPT VA*, has been developed. Vulnerability is assessed in a GIS using geographically distributed vulnerability factors describing the infrastructure and the area surrounding the road. The output is a GIS layer with areas with prerequisites for the analysed risk, and vulnerability scores. ROADAPT VA can be used for all climate-induced risks.

Socio Economic Impact Assessment

Part D of the ROADAPT guideline deals with the socio-economic impact assessment of road traffic event. It is based on three levels of analysis:

- Network level: considering potential impact on traffic; delays, risk of accident, GHG emissions, etc.
- Local territory level: the territories that are served by the road network with impact on economic activity.
- Economic system as a whole: at wider scale the potential impact at corridor or inter-regional, national or cross-border level (including potentially very long distance re-routings on the TERN, passing through different countries).

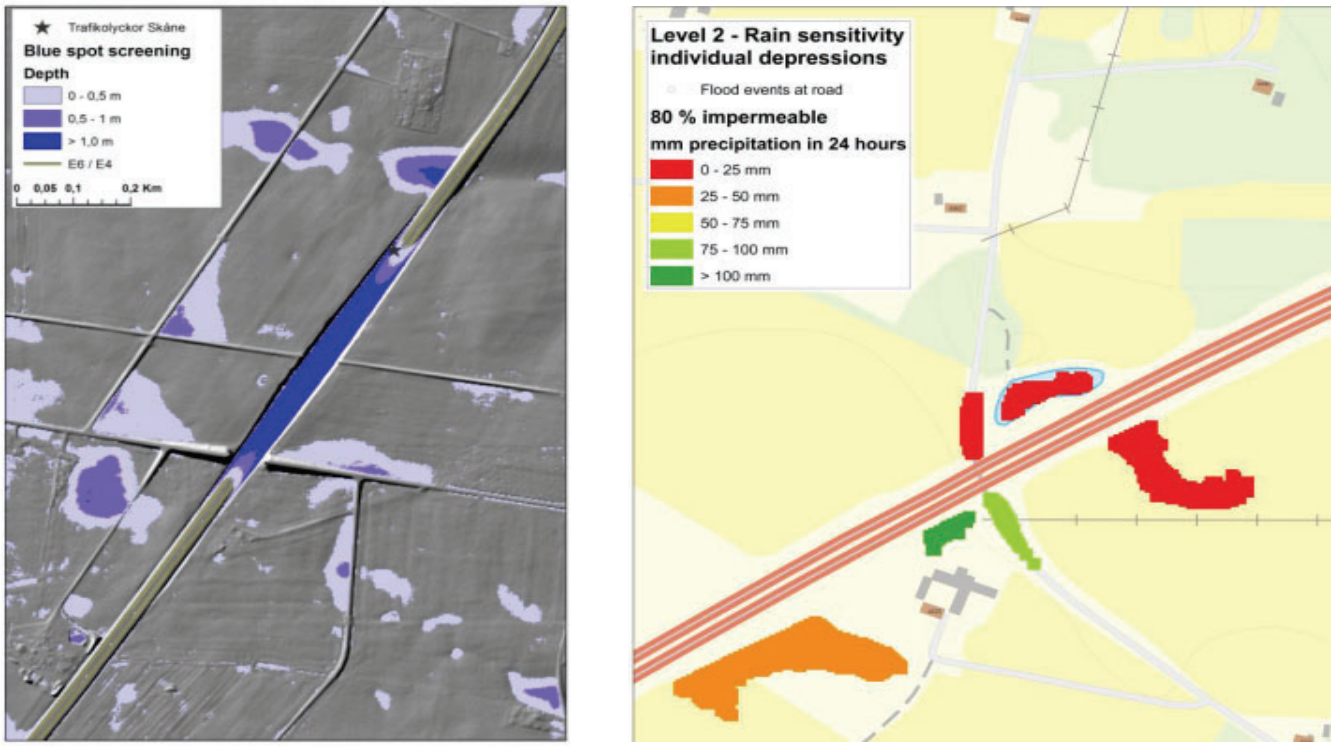


Figure 3: Vulnerability assessment of a road

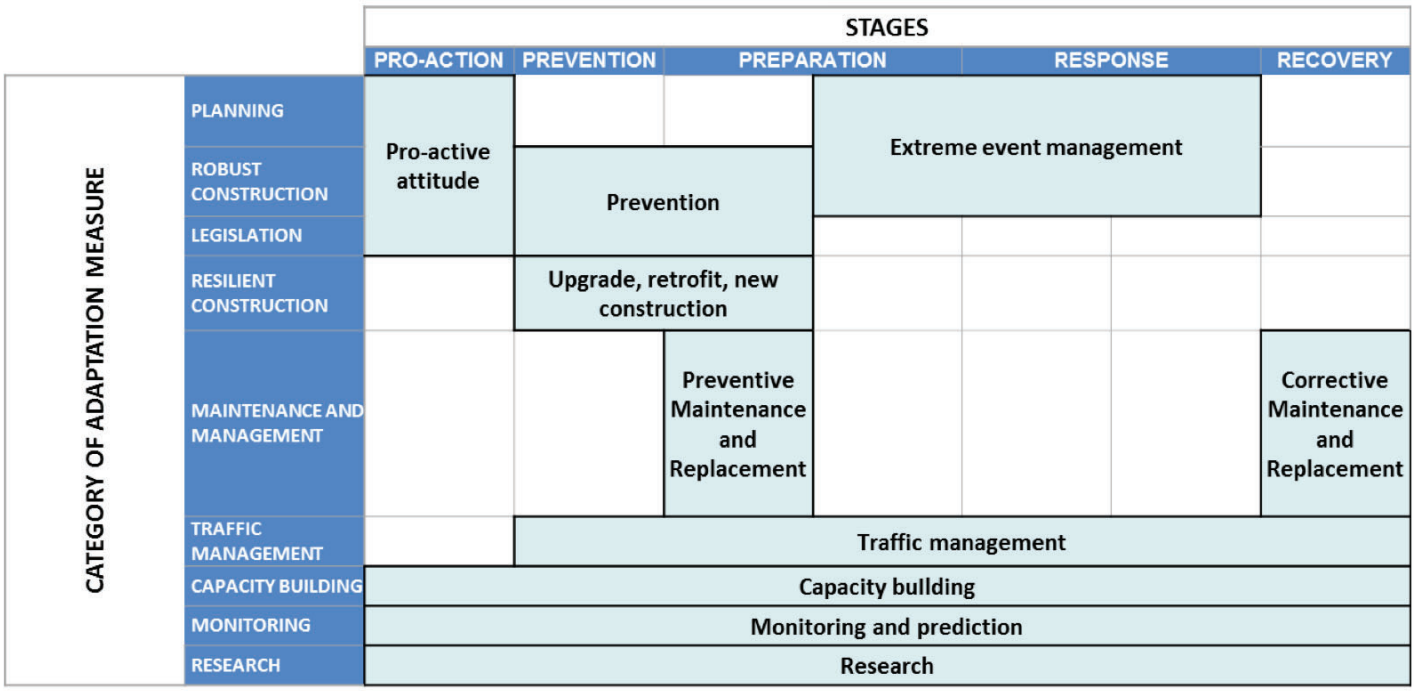


Figure 4: Policy matrix

For each of these three levels, the guideline describes methodologies that enable to evaluate the risk consequences of events linked to climate change, and in a broader manner, provides necessary information to identify the strategies to adapt to climate change.

Adaptation measures and strategies

Part E of the ROADAPT guideline presents an overview of adaptation measures and helps in selecting an adaptation strategy. This part of the guideline provides practical support in RIMAROCC step 5: Risk Mitigation. The selection of the adaptation strategies follows a 10 step approach that is applied to ten specific climate change related threats. Starting from the specific road owner's needs, the 10 step approach helps her/him to identify relevant damage mechanisms, design models, climate parameters for assessing the resilience of the asset in the current and future situation. Next, the approach identifies adaptation measures and strategies, assesses consequences of selecting measures and strategies, and identifies stakeholders to be involved. Knowledge gaps in climate change projections, adaptation technologies and essential construction and site specific data are identified. The time to market of innovative adaptation technologies is estimated to help in the development of technology roadmaps. The guideline is supported with the ROADAPT database with over 500 adaptation measures for geotechnical and drainage assets, pavements and traffic management.

Case studies

Three case studies have been carried out for validation and demonstration purposes. These are the A24 in Portugal, the Rotterdam-Ruhr corridor and the Öresund region. The latter one includes all ROADAPT outputs, where the other only focus on the QuickScan method. The case study report will become available together with the ROADAPT guideline.

More information

The ROADAPT guideline will be available in spring 2015. For more information about the project you may contact Thomas.Bles@deltares.nl (coordinator ROADAPT project) or Kees.van.Muiswinkel@rws.nl (project manager CEDR).

The research being done within the ROADAPT project is carried out as part of the CEDR Transnational Road research Programme Call 2012. The funding for the research is provided by the national road administrations of the Netherlands, Denmark, Germany and Norway. The ROADAPT consortium consists of the following partners: Deltares (the Netherlands, coordinator), SGI (Sweden), Egis (France) and KNMI (the Netherlands).

SGI

egis

Koninklijk Nederlands Meteorologisch Instituut
Ministerie van Infrastructuur en Milieu

Deltares
Enabling Delta Life

This page intentionally left blank.

Criticality of High-Voltage Direct-Current Power Transmission Systems

The complexity of modern Power Systems requires supplementary resilience to prevent undesired consequences not only of the Power System itself but also of other Critical Infrastructures. HVDC technology has the capability to reach this goal.

The continuous increase in electrical power demand and the environmental needs for adopting more Renewable Energy Sources (RES) to the generation blend alter the pattern of the state-of-the-art power systems. The large-scale power generation plants (both fossil fuel and RES generation) are often located far away from the consumers requiring transmission infrastructure to deliver the power to the residential and industrial areas. Whereas the small-scale RES offers advantages to the distribution system only when the stability of the grid can be maintained, the high Voltage Direct Current (HVDC) systems enable low loss transmission and also add stability to the grids making the power system more resilient to unexpected contingencies. HVDC technology can contribute toward future electrical power system grids in many ways:

- **Resilience:** the flexibility of HVDC system is well suited for quick responses to both operational changes and customer needs;
- **Preparedness:** HVDC network reliability assures both quality of supply and immunity/isolation between uncertainties/hazards healthy consumers'/producers' networks;
- **Economy:** HVDC technology provides efficient operation and energy management, and the flexibility to adapt to new regulations;
- **Awareness and sustainability:**the feasibility of development options given environmental constraints.

Resilience

The word resilience is specified by several definitions which, more or less, have a common meaning [CIPedia/Resilience]; "the recovery after physical stress." In Power Systems it is assumed that the resilience can be achieved by decreasing the possibility of failure, along with the reduction of the recovery time and also the limitation of the consequences from such failures.

The resilience index can be measured in the three following indicators:

- Social Indicators such as human life behaviour and blackout consequences;
- Environment Indicator;
- Economic indicator such as electricity and investment costs.

The resilience which is achieved by the HVDC technology is significant not only for the Electrical Power System but also for the other Critical Infrastructures (CIs) which are interconnected to the Power System. The so called "Cascade Effect" of generic interdependencies among CI sectors is analysed in the literature [Zimmerman, "Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction"]. The Cascade Effect by Electrical Power System disruption on some CIs is summarised as follows:

- Oil and gas: electricity for extraction and transport;
- Transportation: power for overhead transit lines;
- Water: electric power to operate pumps and treatment;
- Communication: energy to run cell towers and other transmission equipment.

Preparedness

The preparedness of the HVDC system is characterised by the robustness of the transmission, redundancy and rapidity.

Robustness of HVDC transmission: most of the HVDC systems transmit power through high-power HVDC transmission cables (a pair of cables

Nikolas Flourentzou)

Nikolas Flourentzou (PhD) is a research fellow at KIOS Research Center for Intelligent Systems and Networks of the University of Cyprus. He received the BEng degree in Electronics and Communications Engineering from the University of Birmingham, in 2002, the joint MSc degree in Power Electronics and Drives from the University of Birmingham and the University of Nottingham, in 2003, and the PhD degree in Power Systems from the University of Sydney, in 2010.
He has received the first prize of ElectricaAwards 2010 international innovation contest for the future of electricity networks by AREVA T&D (now known as ALSTOM Grid). His fields of interests are Critical Infrastructure Protection, HVDC power transmission systems, converter topologies and integration of renewable energy systems.

e-mail: flourentzou.nikolas@ucy.ac.cy

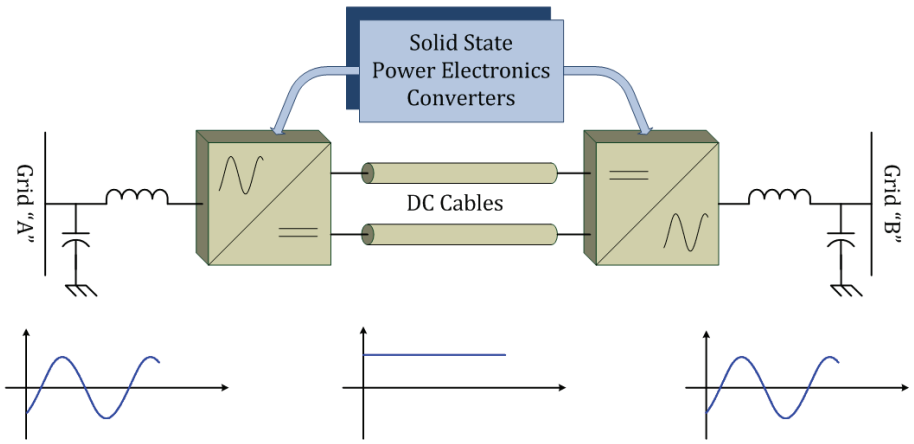


Figure 4: HVDC connection of two AC grids

instead of at least six overhead lines for equivalent power rating – High Voltage Alternating Current (HVAC) transmission through cables is extremely and unreasonably expensive over long distances and producing reactive power). The cables are much more robust than the vulnerable to extreme weather conditions overhead lines. The HVDC does not require additional vulnerable apparatuses such as high-voltage transformers which as necessary for the long distance HVAC transmission.

Redundancy: there are several methods for power redundancy on HVDC systems over faults. The simplest method for redundancy is to construct more than one HVDC systems with a pair of transmission cables each; this however would be a costly option. Since most of the recent HVDC systems are constructed in bipolar configuration, the midpoint can set to ground to allow the bipolar system operating as two monopolar systems, and therefore even during damage of one of the poles (either converter fault or cable fault) the HVDC can operate in more than half of the power-rating; the power-rating of the monopolar with the over-voltage capabilities. The midpoints of the converter stations must be capable to transfer electrical current; either by electrodes (earth return) or by conductor. A number of ground electrodes and sea electrodes are available for ground power transmission and offshore transmission, respectively. However, due to recent environmental concerns, the new HVDC systems have limitations on the continuous allowed time of operation through electrodes. Therefore, the midpoint current return through an additional conductor seems an attractive solution when the construction budget allows. The three options of midpoint current return are the neutral metallic wire, the medium-voltage DC cable and the third HVDC cable.

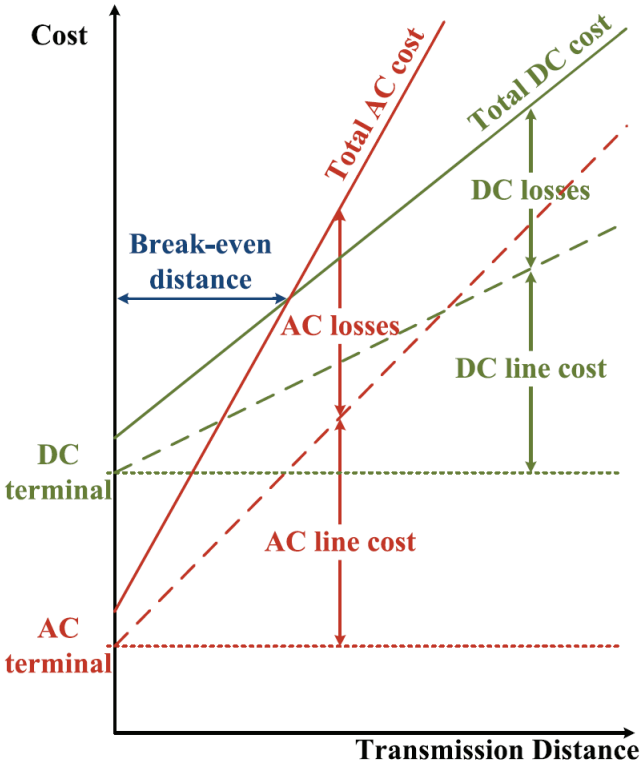


Figure 5: High-voltage transmission cost

- During a pole fault (converter fault or cable fault), when the bipolar HVDC system has midpoint current return through a neutral metallic wire, the HVDC system can operate in half power but the transmission losses are increased; this setup can operate until the fault is repaired.
- During a pole fault (converter fault or cable fault), when the bipolar HVDC system has midpoint current return through a medium-voltage cable, the HVDC system can operate in half power and has the overpower capability as well; this setup can operate until the fault is repaired.
- During a pole fault, when the bipolar HVDC system has midpoint current return through a third HVDC cable (identical to the cables of the two poles), the HVDC system can instantly operate in half power with overpower capability; if the fault is a converter error this setup can operate until the fault is repaired but if the fault is cable error the faulty cable can be replaced by the third HVDC cable within hours and the HVDC system can operate at full power.

Rapidity: HVDC does not suffer from power inertia like HVAC does. Since synchronisation is not required between the stations of the DC grid, it is easy to synchronise each station with the AC network (if required). Therefore, the HVDC system provides immunity between two or more AC sides, while offering simplicity in the transmission system and prevention of synchronisation errors. Recent HVDC technologies have advanced control capabilities to overcome some AC faults such as unbalanced of the three phases, frequency errors, and voltage dips. Recent HVDC technologies allow "low-voltage ride through" capabilities to support the network during a voltage dip without any power interruption.

Economy

Investment on resilience and preparedness over the threads of critical infrastructures is an important dynamic element of CIP. Studies demonstrate the economic benefits of increasing electric grid resilience to weather outages.

- HVDC systems are the widely known economical solution for bulk power transmission over long distances. The investment cost is

lower after the break-even distance (Figure 5);
- The number of transmission lines for HVDC transmission is much less which reduces the material required and hence the cost;
- The HVDC system requires simple power transformers instead of phase-shifting transformers. Therefore, they are simpler to design and manufacture, do not require additional material and hence the cost is reduced.

Awareness & Sustainability

For the sustainability and awareness of the HVDC systems is explained by its resourcefulness. Studies on the total amount of material required for bulk power transmission over long distances determines the economic, environmental and life-time benefits of HVDC over HVAC transmission.

- HVDC systems are the widely known for the power sea-crossing and off-shore connections capabilities;
- The transmission corridor required for HVDC system is significantly narrower than the corridor required for HVAC system (Figure 67) – using HVDC cables instead of overhead lines the area required is much less and by considering sufficient laying depth agricultural activities are safe above the cables (Figure 78);
- The number of transmission lines or cables for the HVDC system is much less, which, from the environmental point of view, means less material is required per Watt;
- The DC transmission does not require phase-shifting transformers to control the power flow through specific lines in a complex power transmission network. The phase-shifting transformers are vulnerable and involve additional material, cost and special designed according to individual factors (such as voltage, power, climate, system topography, sound level and many more);
- The latest HVDC technologies are capable to provide the amount of reactive power required for the load regardless of the reactive power produced by the generation, thus, the effort of maintaining the stability of the power system is prevented;
- Supports reliable connection and interconnection of very weak AC systems.

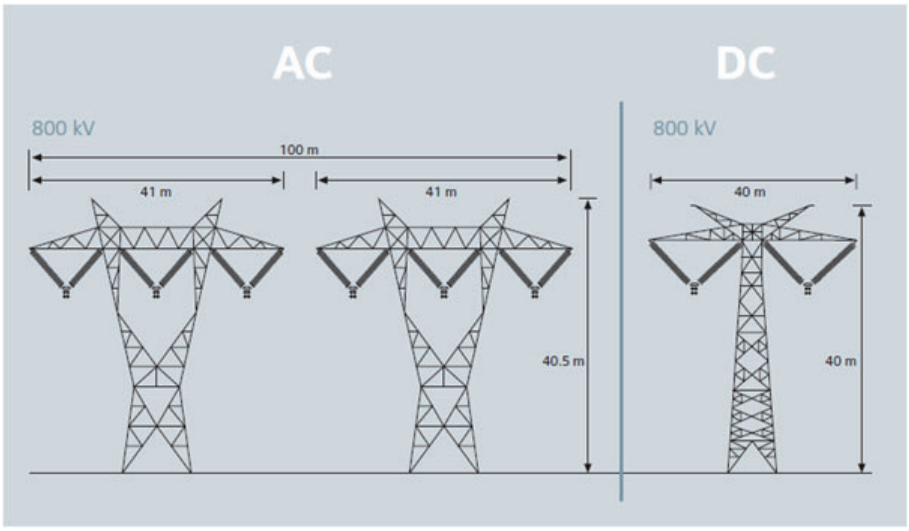


Figure 6: Transmission corridor width of HVAC vs. HVDC [SIEMENS.com]

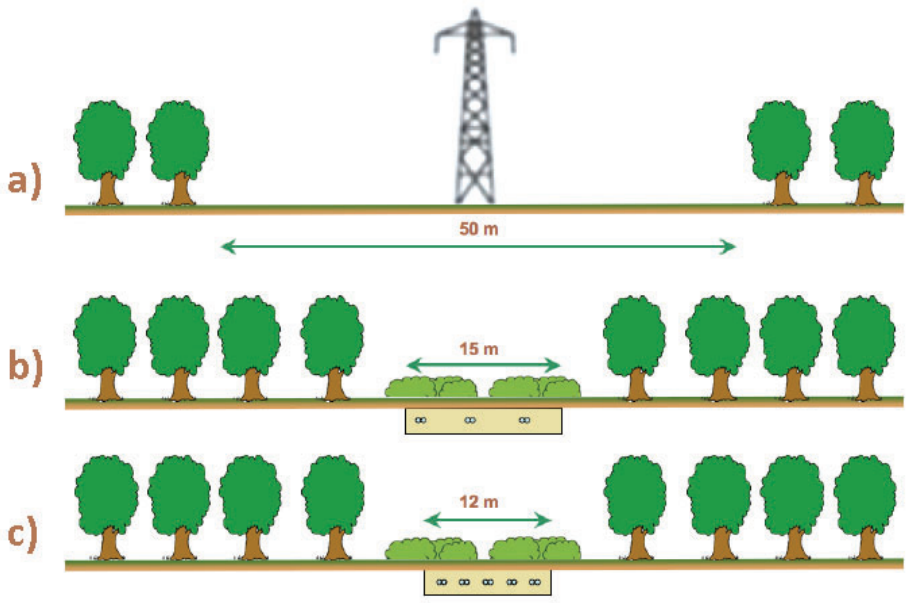


Figure 7: Transmission layouts for 5 GW HVDC systems; a) 800 kV overhead lines, b) 3 pairs of 500 kV MI cables, c) 5 pairs of 320 kV XLPE cables [europacable.com]

These are the characteristics that have been inspiring the engineers of more than half century to design a more sustainable, more efficient and less polluted power system.

Threats to CIs

The numerous disastrous events of the last decades proved us that modern societies depend on CIs. The vulnerability of the CIs is reminded not only by the natural hazards but also from events caused by humans.

The "anthropogenic threats", such as the terrorist attacks of 9/11 (2001), Madrid (2004) and London (2005) but also the system failures of Eschede train disaster (1998) and Vasilikos Power Station explosion (2011) specify the need for substantial CI resilience and preparedness.

Infrastructures are also at risk from natural disasters such as hurricane "Kyrill" (2007), the heat waves of recent years (for example 2003), the drought in Africa (2011), or the great floods in China (1998) and Pakistan (2010) and the tsunami in Fukushima (2011).

The hazards which pose the highest threat to Critical Infrastructures can be categorised as follows:

Natural threats:
- storms, tornadoes

- extreme rainfall, flood
- droughts
- earthquakes
- epidemics / pandemics

Anthropogenic threats:
- accidents
- system failures
- sabotage, malicious programs
- terrorism
- war

The HVDC power transmission systems are more resilient during storms, tornadoes, extreme rainfall, droughts and earthquakes compared to AC power transmission. Since the sensitive apparatuses are enclosed into a solid building the risks from the above threats are not as high as if they would be on a power yard. Furthermore, in most systems built with the latest HVDC technology, the power is transferred through underground and/or submarine cables which are less vulnerable on weather conditions than transmission lines.

Although, the HVDC systems do not offer any significant advantages over anthropogenic threats, special design considerations are usually applied over cyber-attack, physical-attack, hybrid-attack (combined cyber and physical) and several accidents.

Further Information

Energy saving, emission reduction and low carbon economy seems to be major global targets of our era. Long term projects (such as DESERTEC Foundation, Mediterranean Solar Plan and Medgrid among others) aim to accomplish the above targets by energy utilisation and integration of the optimum mixture of RES to the Electrical Power Grid. Such goal can be achieved by introducing several HVDC systems to connect/interconnect large areas, islands, countries and even continents. Therefore, a vast area (i.e., entire Europe) can be connected by an enormous DC Grid, having different weather conditions at each end of the grid (i.e., from Ireland to Greece), allowing reduction of conventional power generation and hence reduction of fossil/nuclear fuel consumption and reduction of CO_2 gas emission.

A lot of investments are devoted in research to find ways to increase the power-rating and efficiency of the HVDC systems, while keeping the controllability and reliability at the high standards of the recent HVDC technologies. The recent trends involve the development of the high-temperature superconducting DC power cables, high-power gas-insulated transmission lines, hybrid DC circuit breakers and super-conducting switching valves, along with the invention of several high-voltage apparatuses such as vacuumed-channel transistors, new materials etc.

One of the major drawbacks of creating a multi-terminal HVDC grid is the lack of DC circuit breakers. Latest invention of hybrid circuit breakers which combine mechanical and semiconductor technologies seem promising to reach the voltage-ratings required for the grid of the near future. Therefore, further control and security will be added to the DC transmission grids.

Existing overhead AC lines can be converted to overhead HVDC lines. Such a conversion can increase the AC power level by a factor of more than 2.5 for the same current density [ABB review]. The specific transmission losses are reduced by more than half. Converting existing AC power lines to HVDC not only to increases the power transmission capacity and efficiency but also to increase the resilience of the long distance interconnected areas.

System Robustness Analysis in Support of Flood and Drought Risk Management

Summary of a PhD Study

Flood and drought impacts are increasing

Floods and droughts cause increasingly large impacts on societies worldwide. The probability of these extreme events is also expected to increase due to climate change. Water management primarily tries to protect against floods and droughts, for example by building flood protection infrastructure and reservoirs. Despite structural measures to prevent flooding and water shortage, 100% protection can never be provided.

Therefore, over the past decades, water management has shifted to a risk-based approach. This means that policies do not only aim at reducing the probability of occurrence of floods and droughts, but also include actions to limit the consequences of potential flooding or water shortage. Both types of measures may aid to reduce flood and drought risk to an acceptable level.

Limitations of a risk approach

Even if the risk is reduced to an acceptable level, extremely large impacts are not avoided, as demonstrated by recent floods and droughts events with devastating impact. A risk approach considers ten casualties per year in 100 years equal to 1000 casualties at once during the same period. However, the latter have a much larger societal impact. Large impacts occurring at once are considered unacceptable when it is difficult to recover from them. Hence, not only the risk but also the potential impacts should be reduced to an acceptable level. There is a need for decision support methods that help avoiding unacceptably large impacts from floods and droughts.

Another reason why risk may not suffice as decision-criterion is that it is uncertain, under both current and future conditions. Estimating current risk requires assumptions on return periods of events that do not occur in measured data. Furthermore, it is uncertain how risks develop into the future, because of uncertain future climate (and climate variability) and socio-economic developments. It is therefore difficult to decide on the most cost-effective strategy in terms of the effect on risk. This further underpins the need for additional decision criteria that take uncertainty into account.

Robustness: a new perspective on dealing with extreme events

The concept of robustness seems useful for dealing with extreme events. Robustness is known from other areas such as engineering and biology, where networks or systems have to maintain their functionality even when some components fail. Areas prone to floods or droughts can be understood as systems. When these systems can remain functioning during flood and drought events, it is likely that unmanageable impacts (i.e. disasters) are avoided. In this thesis, the concept of robustness is made operational by proposing quantifiable criteria. These criteria were tested in two flood cases and two drought cases. The cases have demonstrated the applicability of the framework and have provided insight into the characteristics that influence system robustness.

Furthermore, the case studies demonstrated that assessing system robustness may change the preference ordering of management strategies.

Robustness = resistance + resilience

In the thesis, system robustness is defined as the ability of a system to remain functioning under a large range of disturbance magnitudes. Disturbances in this thesis are flood waves in river valleys that may cause flooding, and droughts (resulting from precipitation deficit or streamflow deficit) that may cause water shortage.

Marjolein Mens

Dr. Mens graduated in January 2006 at the department of Water Resources of Wageningen Univ. Since March 2006 she has been working at WL | Delft Hydraulics and later Deltares, where Ms. Mens now works as a researcher in the field of flood risk management. She has been involved in consultancy projects for the National Gov. to calculate flood risks and to advise on the national safety policy. Also, she has been working on decision support systems for a broad range of end-users. Because of her experience in flood risk management, Ms. Mens is frequently involved in climate change adaptation projects. For example, the European research project RIMAROCC and an advise about climate-proofing of the Netherlands. In 2015 ms. Mens finished her PhD-research on the use of robustness in decision-making for long-term water management.

e-mail: marjolein.mens@deltares.nl

To remain functioning' means either no impact from the disturbance or limited impact and quick recovery. System robustness is a function of two other characteristics: resistance and resilience. Disturbances that cause no impact are in the resistance range; larger disturbances that cause limited impact from which the area can recover are in the resilience range. Robustness analysis aims to identify these ranges for a specific system.

Three criteria to quantify robustness

To obtain insight into robustness, the thesis proposes three criteria to describe a system's response to disturbances:

1. The resistance threshold is the point where the impact becomes greater than zero;
2. The proportionality refers to the graduality of the response increases with increasing disturbance magnitudes;
3. The manageability is the ability to keep the response below a level from which recovery is difficult or impossible.

The **first criterion** refers to the smallest disturbance magnitude causing significant impacts and is strongly related to the system's design standard (e.g., protection against floods or reservoir capacity to prevent water shortage).
The **second criterion** originates from the flood risk literature; sudden floods are considered undesirable because people have too little time to prepare, leading to large impacts. Sudden events should thus be avoided in a robust system.
The **third criterion** compares the impact with a critical recovery threshold. This threshold represents the physical and socio-economic capacity to recover from the impacts of floods and droughts. When impacts exceed the critical threshold, it is assumed that the recovery time is long and that long-term impacts will be unacceptably high.

A robustness perspective may change decisions

In flood risk management, measures are often prioritized based on risk (a metric that combines flood probabilities and corresponding impact), in comparison to the investment costs. Both flood cases showed that a variety of measures may reduce the risk, but not all of those measures enhance system robustness. This means that different measures may be preferred when their effect on system robustness is also taken into account.

Three criteria to quantify robustness:

- Resistance threshold
- Proportionality
- Manageability

In drought risk management, measures are often assessed on the resulting water supply reliability (i.e., the probability of meeting water demand). The drought cases have demonstrated that not all measures that increase the supply reliability also reduce the drought impacts over the full range of plausible drought events. Thus, different measures may be preferred when their effect on system robustness is also taken into account.

What characterizes a robust flood risk system?

Systems with high protection levels for the entire river valley have high resistance against flood waves. However, when protection's levels are equal everywhere, sudden floods can still occur and affect a large and/or vulnerable area. Such a system is not considered robust to flood waves. Robustness of a system with a high resistance threshold can be increased by differentiating protection levels, so that least-vulnerable areas will flood first and more-vulnerable areas are relieved. Another option is to build virtually unbreachable embankments. This prevents sudden flooding and limits the inundation and thus the impact. A combination of unbreachable embankments that are also differentiated in height will further increase robustness to extreme floods. Finally, measures aimed at impact reduction increase robustness when they reduce the impacts below the recovery threshold.

What characterizes a robust drought risk system?

Drought risk systems have a high resistance threshold when their storage capacity is large compared to the demand, for example systems with large reservoirs. The resistance threshold is related to the supply reliability. A variety of supply sources will increase the supply reliability and the resistance threshold. When the objective is to reduce impacts from extreme drought events, demand reduction and temporary measures are more effective than increasing supply on a structural basis. In agricultural drought risk systems, crop diversity and having alternative sources of supply will enhance robustness to drought (see for example Figure 1).

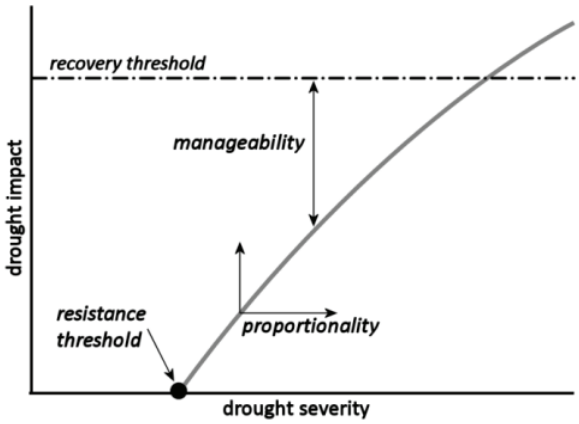


Figure 1: Example response curve: relationship between drought severity and drought impact and robustness criteria

Conclusion

In conclusion, this thesis contributed to decision making in flood and drought risk management, by developing and testing an additional decision criterion. A robustness analysis method supports the assessment of impacts from extreme events, and is applicable on flood and drought risk systems. A robustness perspective supports decision makers in exploring low-probability/high-impact events and considering whether these impacts are societally acceptable. Quantifying robustness inspires the development of strategies that reduce flood and drought risk in a way that disasters are avoided.

Evolving threats and vulnerability landscape: new challenges for the emergency management

The International Emergency Management Society Conference, Roma September 30- October 2, 2015

Communities rely on the use of advanced technologies and infrastructures. The term infrastructure has been used many different ways to include a variety of components. They are the "lifeline systems" that physically tie together urban areas, communities, and neighbourhoods, and facilitate the growth of local, regional, and national economies. These (inter)dependent systems work together to provide essential services of a modern society which rely on the exploitation of their capacities. ICT, energy and transport networks are enabling a change in the paradigm of citizen's interactions and reshaping relationships between communities, government, private sectors, non-profit communities and citizens.

Infrastructures play a crucial role to increase the capacity and efficiency of risk and disaster management and emergency response by providing advanced solutions and accurate information. People will be more and more involved to support public services and infrastructure systems (e.g. transportation, energy, education, health and care, etc.) for example through so-called open data, living labs and tech hubs. If from one side the future development will link networks supporting and positively feeding off each other, from the other one such (inter)dependency may be prone to failures that can propagate through a number of systems and that may results in a more severe impact for the communities. In other terms, future communities will count on more efficient services but, at the same time, can be more vulnerable due to complexity of interconnection of sophisticated infrastructure and services. This implies the need to develop new approaches and strategies to protect them, enhancing resilience and their capacity to survive to hazards and critical situations. In the recent years, **resilience** has become a key term in disaster risk management and the strengthening of infrastructures has been identified as an important field for disaster risk reduction.

With the aim of focusing on new technological and organizational trends in Emergency Management, the 2015 TIEMS Conference that will be held in Roma on September 30-October 2, 2015 at the ISA (Istituto Superiore Anticendi) will bring scientists, stakeholders and Public Authorities committed in Disaster response, emergency management and risk analysis to share their experiences and views, to present new technological tools coming from R&D projects, usually resulting from Public-Private-Partnerships.

This year is foreseen a special emphasis on Nepal Disaster after-maths. The Conference will host, among the other distinguished Keynote Lecturers, the President of the Nepal Center for Disaster Management and a Round Table Discussion (September 30, afternoon) on lessons learnt from this recent dramatic event.

Register for TIEMS now!

The TIEMS 2015 conference will be held in Rome on September 30th to October 2nd in Rome. Further information can found at the TIEMS Italian Chapter website: http://tiems.info/tiems-2015-annual-conference.html

Carmelo Di Mauro

Carmelo is an environmental Engineer with more than twenty years experience in the applied science, in particular in the field of risk-based decision-making processes.

e-mail: carmelo.di-mauro@jrc.it; carmelo.dimauro@riskgovernancesolutions.eu

Vittorio Rosato

Vittorio is the Head of the Computing and Technological Infrastructures Lab at ENEA Casaccia Research Centre

e-mail: vittorio.rosato@enea.it

CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (Edition 2)

Rome, 11th – 13th November 2015

Organised by University Campus Bio-Medico of Rome in coordination with ENEA (Italian National Agency for New Technologies, Energy and Sustainable Economic Development)

Scheme: 1 + 1 + 0.5 days lectures and training (3 optional modules)

Language: English

Description:

The second edition of the Master Class on Modelling, Simulation and Analysis of Critical Infrastructures will be delivered following a "module" approach. In each day an optional module will be delivered:

- Module 1 (11th November 2015): notions and theories regarding Critical Infrastructure modelling, simulation and analysis will be described in details. This module is particularly indicated for researchers and any professional needing a general approach to the topic;
- Module 2 (12th November 2015): Decision Support System and consequence analysis, description of the DSS tool developed by ENEA within the CIPRNet project. This module is particularly indicated for any type of audience, including CI operators;
- Module 3 (13th November 2015, morning): Hands-on exercises on DSS. This module is particularly indicated for technicians and researchers needing to practice with DSS.

Audiences:

- CIP Researchers and experts from different research communities (European and non-European);
- Public/governmental authorities in charge of Critical Infrastructure Protection or Civil Protection matters;
- Stakeholders from Critical Infrastructures' operators.

More information regarding the second edition of the CIPRNet Master Class and the registration form will be published soon at https://www.ciprnet.eu/endusertraining.html.

CRITIS 2015: 10th Int'l Conference on Critical Information Infrastructures Security
Call for Participation

CRITIS' 10th anniversary takes place in Berlin, Germany, October 5–7, 2015.

In 2015, the International Conference on Critical Information Infrastructures Security faces its tenth anniversary. CRITIS 2015 continues the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP) and fostering the dialogue with stakeholders. CRITIS 2015 aims at bringing together researchers and professionals from academia, industry and governmental organisations working in the field of the security of critical (information) infrastructure systems.

As in previous years, invited keynote speakers and special events will complement a programme of original research and stakeholder contributions. The conference invites the different research communities and disciplines involved in the C(I)IP space, and encourages discussions and multi-disciplinary approaches to relevant C(I)IP problems.

CRITIS 2015 continues the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP) and fostering the dialogue with stakeholders.

In 2013, the CRITIS series of conferences has started to foster contributions from young experts and researchers ("Young CRITIS"), and in 2014 this has been reinforced by the first edition of the CIPRNet Young CRITIS Award (CYCA). We will continue both activities at CRITIS 2015, since our demanding multi-disciplinary field of research requires open-minded talents.

Call for Participation

The CRITIS 2015 programme will be published on the conference web site http://www.critis2015.org shortly after publication of this ECN issue. Simultaneously, the registration will be opened.
The 2.5 days programme will consist of five keynotes, eighteen full paper and seven short paper presentations, demonstrations, the awarding of the second CYCA, a permanent poster exhibition, and more.

Venue

The venue is located in the heart of Berlin, vis-à-vis the Museum Island and close to railway station Hackescher Markt:

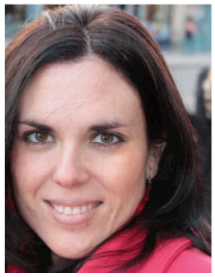
Fraunhofer Forum
Anna Louisa Karsch Street 2

Programme & Registration

To be published shortly on http://www.critis2015.org

Erich Rome, Fraunhofer IAIS, General Chair
e-mail: erich.rome@iais.fraunhofer.de

Marianthi Theocharidou, EU JRC, Stephen D. Wolthusen, Royal PC Co-Chairs
e-mails: stephen.wolthusen@rhul.ac.uk
marianthi.theocharidou@jrc.ec.europa.eu



Cristina Alcaraz, University of Malaga, Publicity Chair
e-mail: alcaraz@lcc.uma.es

Links

ECN home page	www.ciprnet.eu
ECN registration page	www.ciip-newsletter.org Please register free of charge
CIPedia©	www.cipedia.eu The upcoming and new CIP reference point

Forthcoming conferences and workshops

1st TELERISE	www.iit.cnr.it/telerise2015	Technical and LEgal aspects of data pRIvacy and Security
1st WS Cyber Crime & Terror	www.ares-conference.eu	Aug. 24 – 28, 2015, Toulouse, France
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016
TIEMS 2015 Annual Conference	http://tiems.info/tiems-2015-annual-conference.html	Sept. 20 - Oct. 2, 2015, Rome.
10th CRITIS Conference	www.critis2015.org	Call for Participation, Oct 5-7, 2015, Berlin
CIPRNet Master Class	www.ciprnet.eu/endusertraining.html	Rome, 11th – 13th November 2015
16th IEE El.Tech Conference	http://melecon2016.org	Call for Papers: open until Sept. 15, 2015
49th ESReDA Seminar	http://www.esreda.org/	Brussels, October 29-30, 2015

Institutions

National and European Information Sharing & Exchange	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange

Project home pages

FP7 CIPRNet	www.ciprnet.eu
FP7 CyberRoad	www.cyberroad-project.eu
FP7 CYSPA	www.cyspa.eu
ERNCIP Project	https://erncip-project.jrc.ec.europa.eu
FP7 INTACT FP7	http://www.intact-project.eu
PREDICT	www.predict-project.eu
ROADAPT	www.swedgeo.se/templates/SGIStandardPage____3218.aspx?epslanguage=EN

and Deltares Brochure:
https://www.deltares.nl/en/projects/climate-change-risk-assessments-and-adaptation-for-roads-the-roadapt-project/

Global Conference on CyberSpace www.gccs2015.com e.g.:
https://www.gccs2015.com/sites/default/files/documents/Cyber%20Security%20of%20Industrial%20Control%20Systems%20GCCS2015.pdf

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection" I this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Global Conference on CyberSpace	www.gccs2015.com e. g. on ICS: https://www.gccs2015.com/sites/default/files/documents/Cyber%20Security%20of%20Industrial%20Control%20Systems%20GCCS2015.pdf
From Awareness to action: bridging the gaps in 10 steps:	https://zoom.frontwise.com/public/4/towardsgccs2015#
Network Information Security Platform	https://resilience.enisa.europa.eu/nis-platform

Websites of Contributors

Acris	www.acris.ch
CEA	www.cea.fr
Deltares	www.deltares.nl/en
EU Organisation for Security	ww.eos-eu.com
Joint Research Centre	http://ipsc.jrc.ec.europa.eu
University of Cyprus	www.ucy.ac.cy/el/
TNO	www.tno.nl
University of Trento	http://r.unitn.it/it/sdc
Veiligheidsregio Zuid-Holland Zuid	www.vrzhz.nl/

www.cipedia.eu

CIPedia© is here!

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

> CIPedia© aims to become a common reference point for CIP concepts & definitions.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

> The initial content was provided by the EC-JRC, Fraunhofer, TNO, and the CIPRNet consortium.

The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

Marianthi Theocharidou

Marianthi Theocharidou works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), for the CIPRNet and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes CIP **experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

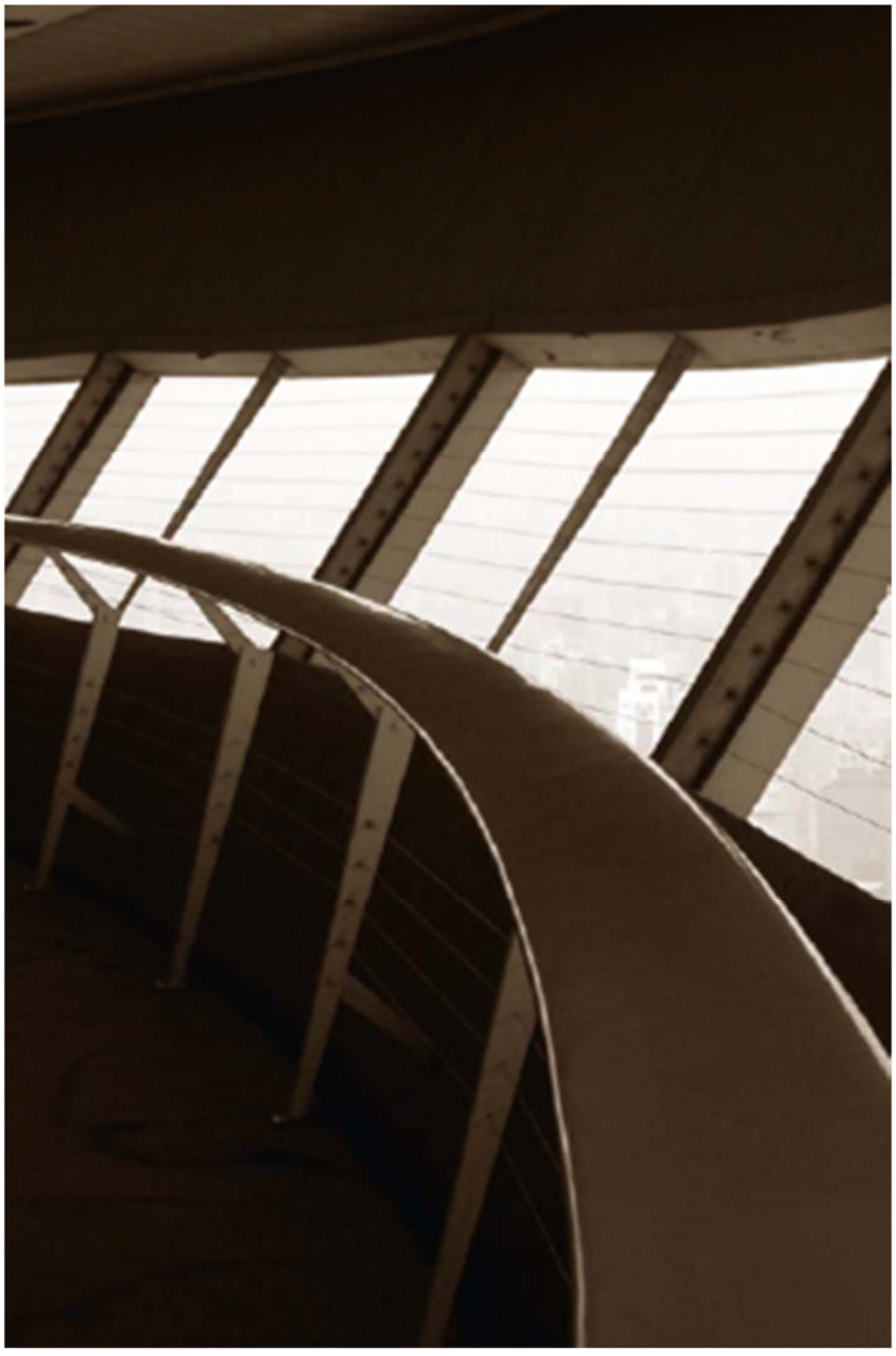
If you are interested to become an active contributor, please contact Dr. Theocharidou for information

European CIIP Newsletter

Special Issue

CRITIS 2015

October 15 - February 16, Volume 9, Number 3



ECN

Contents

CIPR Net

> 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

> Spelling:
British English is used except for US contributions

Editorial: Strengthening collaboration among research projects within the EU

Increasing the resilience of European Critical Infrastructures through science requires closer collaboration of projects with similar scope, close communication with end users and links to EU policy.

The protection and resilience of Critical Infrastructures (CI) remains a priority for Europe, as reflected by the funded security projects under the 7th Framework programme and the on-going ones under the Secure Societies H2020 programme. As Dr. Martínez-Garcia explains in the first article of this issue, upcoming **H2020 calls for innovation projects** (2016-2017) will focus on physical and cyber protection for critical infrastructures, building on the research work been performed and strengthening the link with end users, the industry and standardisation bodies.

EU-funded projects should interact in order to benefit from past results, to avoid duplication of effort and to increase exploitation by end users within the EU market. For this reason, the EC has initiated the development of a **Community of Users in Disaster Risk and Crisis Management**. This issue of the ECN series continues to contribute towards this direction, as its past issues. It aims to act as a forum of dissemination but most importantly of synergy among projects, both EC funded ones and national research ones on CIP topics.

To this end, the issue welcomes articles by two recently funded H2020 projects **IMPROVER** and **RESIN**, which focus on **resilience**. IMPROVER aims towards a risk-based approach combining different dimensions of resilience to four living labs. RESIN develops standardised approaches to help city administrators, the operators of urban infrastructure networks, and related stakeholders to develop their adaptation strategies and ensure that their decisions strengthen the resilience of a city. The Geospatial Risk and Resilience Assessment Platform (**GRRASP**) –a JRC project- is also presented. It is a collaboration and analysis tool that can be used by authorities and operators for risk and resilience assessment at local, regional, national and international scale.

The issue continues with **national approaches and initiatives**. The novel national approach for CIP and resilience in the **Netherlands** is presented. Other national initiatives include the Center for Cyber and Information Security, in collaboration with the long-standing Network Information Security Lab in **Norway**, and the launch of the Research Centre on Resilient Information and Control Systems in **Sweden**. On the cyberspace front, alternative **Cyber Defence** national strategies are presented and analysed.

The issue concludes with insights on **cybersecurity**, as well as **CI research** and **training**. To start, new advances in **identity and access management** are presented. The article discusses how these could affect the security market. Two seemingly different research topics are compared, i.e. **asset management and critical infrastructures**. The article identifies similarities and potential areas for collaborative research. On the **training** side, two courses on **Homeland Security** in Italy and USA are compared to guide readers to useful conclusions when planning and conducting such courses.

We would like to remind you that the CIP community has a rendezvous in Berlin at the **10th edition of the CRITIS conference** (October 5-7). We also announce that the 2nd student award is presented at this year's CRITIS conference. As this tradition will continue to upcoming conferences, young researchers are encouraged to apply for the 2016 award.

Enjoy reading this issue of the ECN!

PS: Please have a look at CIPedia©: http://www.cipedia.eu. Please bring your knowledge in to contribute to a real CIP compendium!

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

Marianthi Theocharidou

Marianthi Theocharidou works as a research fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

e-mail: **bmhaemmerli@acris.ch**
He is ECN Editor in Chief

ACM CPSS'16 CALL FOR PAPERS

2nd ACM Cyber-Physical System Security Workshop

Xi'an, China – May 30, 2016 (in conjunction with ACM AsiaCCS'16)

http://icsd.i2r.a-star.edu.sg/cpss16/

Important Dates

Submission due: Dec 5, 2015 Notification: Feb 15, 2016 Camera-ready due: March 15, 2016

Cyber-Physical Systems (CPS) consist of large-scale interconnected systems of heterogeneous components interacting with their physical environments. There are a multitude of CPS devices and applications being deployed to serve critical functions in our lives. The security of CPS becomes extremely important. This workshop will provide a platform for professionals from academia, government, and industry to discuss how to address the increasing security challenges facing CPS. Besides invited talks, we also seek novel submissions describing theoretical and practical security solutions to CPS. Papers that are pertinent to the security of embedded systems, SCADA, smart grid, and critical infrastructure networks are all welcome, especially in the domains of energy and transportation. Topics of interest include, but are not limited to:

- Adaptive attack mitigation for CPS
- Authentication and access control for CPS
- Availability, recovery and auditing for CPS
- Data security and privacy for CPS
- Embedded systems security
- EV charging system security
- Intrusion detection for CPS
- IoT security
- Key management in CPS
- Legacy CPS system protection
- Lightwight crypto and security
- SCADA Security
- Security of industrial control systems
- Smart Grid Security
- Threat modeling for CPS
- Urban transportation system security
- Vulnerability analysis of CPS
- Wireless sensor network security

Steering Committee

Dieter Gollmann (Hamburg Uni of Tech, Germany)
Ravishankar Iyer (UIUC, USA)
Douglas Jones (ADSC, Singapore)
Javier Lopez (University of Malaga, Spain)
Jianying Zhou (I2R, Singapore) – Chair

Programm Chairs

Jianying Zhou (I2R, Singapore)
Javier Lopez (University of Malaga, Spain)

Publicity Chair

Cristina Alcaraz (University of Malaga, Spain)

Publication Chair

Ying Qiu (I2R, Singapore)

Submission Instructions

Submitted papers must not substantially overlap papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. All submissions should be appropriately anonymised (i.e., papers should not contain author names or affiliations, or obvious citations). Submissions must be in double-column ACM SIG Proceedings format, and should not exceed 12 pages. Position papers and short papers of 5 pages describing the work in progress are also welcome. Only pdf files will be accepted. Authors of accepted papers must guarantee that their papers will be presented at the workshop. At least one author of the paper must be registered at the appropriate conference rate. Accepted papers will be published in the ACM Digital Library**. There will also be a best paper award.**

Paper submission site: https://easychair.org/conferences/?conf=cpss2016.

Contact

Email: cpss2016@easychair.org
CPSS Home: http://icsd.i2r.a-star.edu.sg/staff/jianying/cpss/

Horizon 2020 CIP Programme: 40 Million Available for Competition

Soon new opportunities for CIP researchers and operators are coming up. "What are the topics" and "how to build successful a consortia" in this industrial, research and innovation partnership is disclosed from first hand.

The Secure Societies Societal Challenge of the European research programme Horizon-2020 has recently approved by the Member States (MMSS) and the European Commission (EC) a new focus area entirely devoted to physical and cyber-protection for critical infrastructures (CI). Two calls for innovation action projects will be opened both in Spring 2016 and in Spring 2017. In total, the programme will grant up to 20 million Euros each year for selected actions that should include in the consortia, as mandatory, the participation of at least two operators of CI from two different member states and associated countries and, at least, one innovative technological small and medium enterprise (SMEs).

This initiative is in line with the aim of the EC for reducing the vulnerabilities of Europe's CI and for increasing its resilience across all the MMSS and in all relevant sectors of economic activity. The Secure Societies H2020 programme contributes to support the EU's 2008 Directive on European Critical Infrastructures and to build common approaches and tools for the protection, resilience and better understanding and management of their interdependencies. The focus area on CIP within this H2020 Societal Challenge results from the collaboration of both the General Directorate for Migration and Home Affairs (DG-Home) and the General Directorate for Communications Networks, Content and Technologies (DG-Connect), while the overall management and monitoring of the selected projects as well the organisation of the calls and the evaluations will be performed by the Research Executive Agency (REA) of the EC.

Research on physical and cyber CIP is built-up on the experience already tackled in the Security Research domain of the 7th Framework Programme. More than 50 projects were been awarded between 2008 and 2013 in the areas of energy, transport and communication grids, designing and planning of buildings and urban areas, supply chain and cyber-security for CIP (see catalogue of the projects funded under the Security Research Programme in FP7).

Efficient and effective CIP, a European and global challenge

In the last years we have observed how the disruptions in the operation of our national, regional and local CI may put at risk the efficient functioning of our societies and our economies. Some of these disruptions result from natural, man-made hazards or unexpected accidents but, in other occasions, they are the effect of physical and/or cyber-attacks on installations and systems. Furthermore, the increased interconnection among different installations, the scope of the attack (or hazard), and the need of the operators for having to combine cyber and physical security solutions to protect their CI, have arisen the urgency for deploying comprehensive and holistic approaches.

The final aim would be to ensure an effective and efficient protection of our public and private, connected and interdependent installations. On top of that, and because the current global financial crisis, unprecedented budgetary restrictions have been imposed everywhere. So, innovative security solutions must be more efficient and cost-effective than the ones available up to the moment.

Marina Martínez Garcia

Dr. Martínez-Garcia is in H2020 responsible for the Secure Societies Challenge. She is physicist and H2020 Programme Officer at SOST (Spanish Office for Science and Technology) in Brussels. SOST is the EU branch of CDTI (Centro para el Desarrollo Tecnológico e Industrial), which is the Spanish Funding Agency for Industrial R&I belonging to the Ministry of Economy and Competitiveness.

Dr Martinez is also responsible for the collaboration of SOST with the Spanish regions in Brussels and follows the opportunities for SMEs on European R&D and Innovation programmes. She is the coordinator of the capacity building and strategic positioning programme of CDTI in Brussels.

e-mail: marina.cdti@sost.be
Horizon-2020 Programme Officer at the Spanish Office for Science and Technology (SOST-CDTI)
Spanish Ministry of Economy and Competitiveness

What is funded under the Secure Societies CIP focus area?

Both at the end of March 2016 and 2017, the call on CIP at the Secure Societies H2020 programme will open a call for proposals addressed to fund innovation actions that would cover: Prevention, detection, response, and in case of failure, mitigation of effects and consequences (including novel installation designs) over the life span of the infrastructure. The project would also have the aim for achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

It is necessary to address not only all the aspects of both physical (e.g. bombing, plane or drone overflights and crashes, spreading of fires, floods, seismic activity, space radiations, etc.) and cyber threats and incidents, but also systemic security management issues and the combinations of physical and cyber threats and incidents, but also systemic security management issues and the combinations of physical and cyber threats and incidents, their inter-connections, and their cascading effects. Innovative methods should be proposed for sharing information with the public in the vicinity of the installations, and the protection of rescue teams, security teams and monitoring teams as well.

The proposals are expected to lead to developments up to Technology Readiness Level 7 (TRL 7), that is, to have as outcome a system prototype demonstration in operational environment. The installations not covered in the awarded projects within the call-2016 will remain eligible in 2017. Thus, the list of CI and sectors eligible for the call-2017 will be accordingly updated once the results of the evaluations of the first call will be communicated (Winter 2016).

In line with the EU's strategy for international cooperation in research and innovation, international partners and international cooperation is encouraged, as the topic aims a global dimension. In any case, international organisations will be eligible for funding only when the EC considers the participation of those entities as essential for carrying out the action.

The **size of the projects is expected to be up to 8 million Euros of EC contribution, which means an overall budget of the project about 11 and 12 million Euros (approximately),** as innovation actions are 70% funded (except for non-profit public or private legal organisations, which are always funded up to 100%). **About 3 innovation action projects per year** are expected to be funded both in the 2016 and in the 2017 CIP calls.

Projects should focus in the following CI, paying special attention in tackling their interdependencies. Each project should, at least, involve minimum of two CI operators from two different Member States or Associated Countries and, at least, one innovative technological SME within the consortium.

The CI considered are: Utilities such as Water Systems and Energy Infrastructures (i.e., power plants and distribution of electricity, gas, oil, etc.), Transport Infrastructures as well any mean of Transport and mobility at urban, regional, national, cross-border and international level, terrestrial and satellite Communications Infrastructure, Health Services (i.e., hospitals, first aid services) and, finally, Financial Services (banking system, stock exchange, etc.).

Funding rate for the projects is 70% (innovation actions,) with a ceiling of 8 M€ of EC requested.

What is expected of the CIP projects?

At short term, it is expected that projects will make a state-of-the-art analysis of physical and cyber detection technologies and risk scenarios, in the context of a specific CI.
Also, an analysis of both physical and cyber vulnerabilities of a specific CI, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure are expected to be delivered.

In the medium term, the selected projects should:
- Present innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific CI.
- Develop innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the CI.
- Perform in situ demonstrations of efficient and cost-effective solutions.
- Provide security risk management plans integrating systemic and both physical and cyber aspects.
- Deploy tools, concepts, and technologies for combatting both physical and cyber threats to a specific CI.
- Where relevant, the project should carry out test beds for industrial automation and control system for CI in Europe, to measure the performance of CI systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines.
- Also, the project should test the results and validation of models of a specific CI against physical and cyber threats.

As in all H2020 projects and initiatives, efficient and continuous dissemination activities at European level have to be planned in order to target the relevant user communities. Special attention has to be given by showing specific models of information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.

Also the policy side has to be considered by shaping recommend-dations and contributions to relevant sectorial frameworks and European regulatory initiatives on CI.

The innovation actions granted are expected to contribute, as long term impact, to the safety and security standards, and to the pre-establish-ment of enhanced certification mechanisms in the CI domain.

Some hints about a well-balanced consortium

In addition of the compulsory conditions of the action (at least 2 operators from 2 different countries and at least 1 SME), a good consortium should involve key players at industrial level (i.e., operators and industrial security service providers) but also the most advanced and innovative actors in applied research (i.e., private companies, SMEs, technology and research centres of proven close collaboration, dialogue and transfer with the private sector).

As the standardisation dimension has to be present, the project may include the advice (or, if possible, the participation) of entities, well at national or at European level, which have a specific role in the standardisation and certification process.

The consortium has to take attention to the social side so, local, regional or national authorities and first responder bodies should take part in close cooperation with, for instance, citizenship associations of volunteers which are mobilised in case of large scale incidents of such a kind of installations. A complete and realistic environmental impact should be provided by expert private or public entities.

Finally, given the practical aim of the action, test trials and validation exercises involving not only the internal personnel but also all the actors concerned, should be envisioned within the life-time of the project.

Communication is crucial in these projects so, a complete consortium should involve professional expert communication partners which understand the needs for information of all the chain (from citizens to decision makers, inside workers, etc.) and who would be knowledgeable in information management and information tools.

If you would like to know more about the Secure Societies Challenge in H2020 as well to be updated on the latest news and networking and information events about the calls 2016 and 2017 please visit the EC Participant portal where main information is regularly posted.

What is an "innovation action" in H2020?

An Innovation Action (IA) consist in a collaborative project aiming at producing plans and arrangements or designs for new, altered or improved products, services or processes.
For this purpose the project should consider prototyping, testing, large-scale product validations, demonstration activities, piloting and market replications.
In a "demonstration or pilot" it is expected to validate the technical and economic viability of a new or improved technology, product, process, service or solution in an operational (or near to operational) environment, whether industrial or otherwise, involving, if appropriate, a larger scale prototype or demonstrator.
On the other hand, a "market replication" aims to support the first application or deployment in the market of an innovation that has already been demonstrated but not yet applied/deployed in the market due to market failures/barriers to uptake.
Finally, "Market replication" does not cover multiple applications in the market of an innovation that has already been applied successfully once in the market.
In any case, an "Innovation Action" may include limited research and development activities and it is always funded at 70% except for non-profit legal entities, where a rate of 100% applies).

CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (Edition 2)

Rome, 11th – 13th November 2015

Organised by University Campus Bio-Medico of Rome in coordination with ENEA (Italian National Agency for New Technologies, Energy and Sustainable Economic Development)

Scheme: 1 + 1 + 0.5 days lectures and training (3 optional modules)
Language: English

Description:
The second edition of the Master Class on Modelling, Simulation and Analysis of Critical Infrastructures will be delivered following a "module" approach. In each day an optional module will be delivered:

- Module 1 (11th November 2015): notions and theories regarding Critical Infrastructure modelling, simulation and analysis will be described in details. This module is particularly indicated for researchers and any professional needing a general approach to the topic;
- Module 2 (12th November 2015): Decision Support System and consequence analysis, description of the DSS tool developed by ENEA within the CIPRNet project. This module is particularly indicated for any type of audience, including CI operators;
- Module 3 (13th November 2015, morning): Hands-on exercises on DSS. This module is particularly indicated for technicians and researchers needing to practice with DSS.

Audiences:

- CIP Researchers and experts from different research communities (European and non-European);
- Public/governmental authorities in charge of Critical Infrastructure Protection or Civil Protection matters;
- Stakeholders from Critical Infrastructures' operators.

Please find the registration form and more information regarding the second edition of the CIPRNet Master Class at https://www.ciprnet.eu/endusertraining.html.

IMPROVER: Improved risk evaluation and application of resilience concepts to critical infrastructure

The IMPROVER project is a research and innovation action funded under Horizon 2020. Tasked with operationalising resilience concepts applied to critical infrastructure, the project is aiming for a risk-based approach combining different dimensions of resilience in four living labs.

The exposure of critical infrastructure to different emerging and evolving threats, as well as increasing interdependencies between infrastructures, means that large scale crises are occurring with a growing frequency and having an increasingly significant impact on infrastructure.

To respond to these evolving risks, protection is not always an option, largely because of prohibitive costs and difficulties in implementing technological or other solutions to ensure that critical infrastructure assets or systems are fully protected against a range of threats. There is therefore a paradigm shift taking place not only in technological analysis and system design but also on the political level both here in Europe and abroad - from a focus on the protection of critical infrastructure to the resilience of critical infrastructure.

Despite this change and increasing interdependencies between infrastructures, there is no common European methodology for measuring or implementing resilience, and different countries and sectors employ their own practices. Neither is there a shared, well-developed system-of-systems approach, which would be able to test the effects of dependencies and interdependencies between individual critical infrastructures and sectors. This increases the risk as a result of reliance on critical infrastructures, as well as affects the ability for sharing resources for incident planning due to no common terminology or means of expressing risk.

The IMPROVER project, which started on the 1st of June 2015 and runs for three years, aims at contributing to improving infrastructure resilience through the implementation of resilience concepts to real life examples of pan-European significance, including cross-border examples.

Background

The definition of resilience is a contested one, with different definitions for ecological and engineering resilience and some researchers even extending the definition of resilience so that it encompasses protection as well. In IMPROVER, at least at the initial stage, we have been focusing on the engineering definition of resilience, which closely resembles the UNISDR definition of resilience: "[Resilience is] the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of essential basic structures and functions".

Naturally, because there are many definitions of resilience from different communities and different sectors, there are many frameworks detailed in research literature and applied in practice focusing on its assessment and implementation. These focus either on communities or the infrastructure, but in any case they rely on combinations of different factors to contribute to the overall resilience of a system or a system-of-systems.

Within IMPROVER, we look at these factors as a kind of a resilience tool-kit which is implemented to manage and to increase the resilience of infrastructure, and the society which is dependent upon it. Resilience is therefore a complex construct which relies upon the interaction between the different tools in the toolkit, and the interaction between the tools and the infrastructure in question.

David Lange

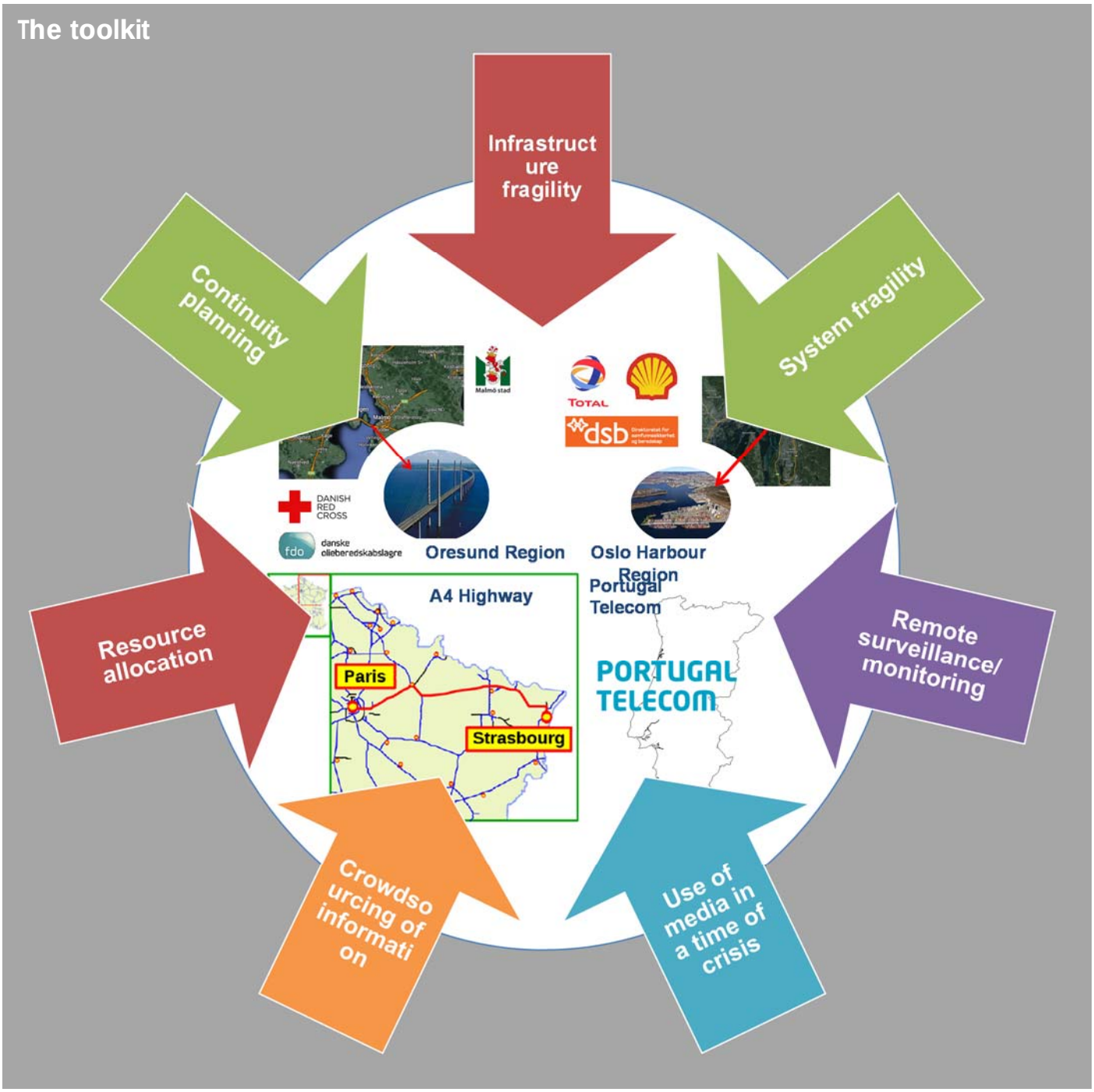
Dr. David Lange is a researcher at SP Fire Research in Borås, Sweden.

e-mail: david.lange@sp.se
SP Technical Research Institute of Sweden, Box 857, 501 15
Sweden

Fanny Guay

Fanny Guay is a project manager at the Danish Institute of Fire and Security.

e-mail: fgu@dbi-net.dk
DBI - Dansk Brand- og sikringsteknisk Institut, Jernholmen 12, 2650 Hvidovre
Denmark



Understanding and operationalising resilience requires a thorough understanding of how these different tools contribute to the fundamental attributes of resilience, such as robustness or recovery of the system in question.

The IMPROVER approach

The project is divided into three stages, which are needed in order to achieve the projects objectives. The first stage is a survey of available approaches for the definition, implementation and evaluation of resilience concepts to critical infrastructure. This will include an extensive literature review, a set of workshops as well as review of ongoing and previous projects both within Europe and globally. The second phase of the project is an evaluation of the available methodologies and the further development of a promising approach to improve its effectiveness, taking account also of existing EU risk assessment guidelines. The final stage is a demonstration of the developed methodology in operation.

In order to properly understand the interaction between resilience concepts which make up the tool-kit and the infrastructure itself we are focussing on 4 'living labs' which represent either clustered infrastructure assets, cross border assets or assets with wide spread geographical dependencies.

In IMPROVER, we will focus on the resilience concepts applied to the infrastructure in these living labs, principally the technological and organisational resilience. In order to assess resilience, it is necessary not only to evaluate the overall resilience of critical infrastructure to threats but also to evaluate the performance and impact of the individual resilience concepts. Working within and across the living labs, the partners in IMPROVER will be able to study resilience concepts acting in isolation and together on the critical infrastructure in order to better

understand the mechanism in which they contribute to resilience. The use of these living labs will also enable us to evaluate and adapt potential existing methodologies for their implementation in critical infrastructure.

This approach using living labs has the advantage of allowing the dependencies, and importantly, the differences between infrastructures to be taken into account when evaluating the different implementations at various stages of the project. This is important when considering that the impact of disasters and crises in Europe is characterised by a highly interconnected society which is increasingly reliant on critical infrastructures providing services which are centralised, if not territorially then contextually. Due to cascading failures through dependencies between critical infrastructure systems, the indirect consequences of natural and man-made disasters may be more severe than expected.

In addition to this focus on resilience of the infrastructure, we will also consider in our overall approach the community resilience, i.e. the combination of societal and economic resilience concepts, through the use of social media and population engagement. The baseline criteria for performance of the infrastructure in times of crises should be based on the response of society to the crisis.

Throughout this work, we will be relying on fields such as resilience, risk assessment, structural engineering (including response of structures to extreme loading), systems analysis, media and communication, crisis management, emergency response, business continuity planning as well as a number of novel and exciting techniques including for example paired comparison, expert elicitation, and crowdsourcing, resulting in improved population engagement.

Next steps

At the time of writing this article, it is just over two months into the projects' three year period. We have been organising our first workshop with different stakeholders and participants in our living labs for the end of September and expect to have a very good attendance from outside of Europe. We have also started our work to evaluate and compare existing approaches for operationalising resilience using the living labs as test cases.

The consortium

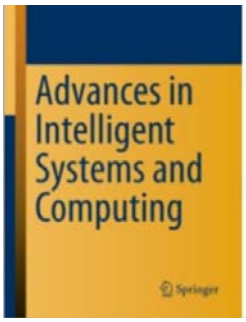
The consortium partners have specific expertise in the different tools which will form our approach. It also includes researchers who are involved in both ERNCIP and the EPCIP programme. The project is coordinated by SP Technical Research Institute of Sweden. The consortium includes 9 additional beneficiaries from throughout Europe including: DBI - Danish Institute of Fire and Security Technology in Denmark, INERIS and the Euro-Mediterranean Seismological Centre in France, the University of Leicester and University College London in the UK, SP Fire Research and the Arctic University in Tromsø in Norway, INOV in Portugal, and the JRC's Institute for the Protection and the Security of the Citizen in Italy.

Acknowledgements

The IMPROVER project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 653390

www.improverproject.eu

For updates of the project, follow us on twitter @improverproject and on LinkedIn: IMPROVER – EU Project.



Springer

the language of science

Call for Papers: Advances in Networking Systems: Architectures, Security, and Applications

Aims and Scope:

Modern network systems encompass a wide range of solutions and technologies, including wireless and wired networks, network systems, services and applications. This appears in numerous active research areas with particular attention paid to the architecture and security of network systems. In parallel, novel applications are developed, in some cases strongly linked to rapidly developing network-based data acquisition and processing frameworks. Information security works as a backbone for protecting both user data and electronic transactions in network systems. Protecting the communication and data infrastructure of an increasingly inter-connected world has become vital nowadays. Security has emerged as an important scientific discipline whose many multifaceted complexities deserve the attention and synergy of the computer science, engineering, and information systems communities. This book volume covers a wide range of topics related to networking systems, security, and network applications. The volume will provide comprehensive reviews of cutting–edge state-of-the-art algorithms, technologies, and applications, providing new insights into a range of fundamentally important topics in networking infrastructures and applications. The edited book volume serves as a reference for engineers and scientists by ensemble up-to-date research contributions. Topics of interest include, but are not limited to:

Network Architecture and Systems

- Architecture, scalability and security of network systems
- Service delivery platforms - architecture and applications
- Resource allocation, QoS, and fault tolerance in networks
- Architecture, data allocation and information processing in sensor networks
- The applications of intelligent techniques in network systems
- Software, applications and programming of network systems
- Management, energy and control of Sensor Networks
- Network protocols, algorithms and standards
- Network traffic engineering
- Traffic classification algorithms and techniques
- Wireless communications
- Innovative network applications
- Network-based computing systems
- Network-based data storage systems
- Open data acquisition and exposure systems
- Crowdsourcing systems
- Network systems for large scale data acquisition and processing
- Web services – standards and applications

Security

- Social, organizational and other aspects of information security
- Information security and business continuity management
- Decision support systems for information security
- Digital right management and data protection
- Cyber and physical security infrastructures
- Security and monitoring of sensor networks
- Computer forensic and network security
- Security systems and Surveillance
- Network, cloud and data security
- Misuse and intrusion detection
- Military

Applications

- Social applications
- Environment monitoring
- Transportation & Infrastructure
- Precision agriculture
- Industrial applications
- Home automation
  Entertainment Health-care

Publication Schedule:

The tentative schedule of publication is as follows:

- Deadline for paper submission: **Dec. 01, 2015**
- Author notification: **Feb. 2, 2016**
- Camera-ready submission: **Feb. 15, 2016**
- Publication date: **Q3 / 2016**

More see: http://staff.www.ltu.se/~ismawa/ansasa

RESIN: Resilient Cities and Infrastructures

A new Horizon 2020 project aimed at standardising approaches and delivering decision support tools for cities to support the development of climate change adaptation strategies linking critical infrastructures with other elements of cities.

Background

With most of its population and capital goods concentrated in urban areas, cities are central to a well-functioning European economy and society. However, the concentration of people and assets in cities also renders them extremely vulnerable to the effects of extreme weather events and climate change. When disasters occur in urban areas, they threaten the lives of large numbers of people, critical infrastructure systems, and interregional and global value chains. The combination of increased urbanisation and the increasing consequences of global climate change place an imperative on cities to be proactive in strengthening their resilience to disasters in order to secure their economic competitiveness and to enhance the quality of life for their residents.

City adaptation strategies

Despite this imperative, the development of urban climate change adaptation strategies has been slow. The majority of EU cities are still lagging, and there is a significant north-south divide with cities in southern Europe showing less progress in this regard.

Even where urban adaptation strategies exist, there is a poor integration of different domains, and between critical infrastructures and other city systems. The absence of a standardised approach with regard to the methods for undertaking key tasks such as assessing climate risks and vulnerability, and prioritising between adaptation responses, limits urban adaptation planning. Limited comparability between cities and adaptation options is also a barrier to the provision of national and EU funding for adaptation projects.

And here RESIN comes in:

The RESIN project will develop standardised approaches to help city administrators, the operators of urban infrastructure networks, and related stakeholders to develop their adaptation strategies and ensure that their decisions strengthen the resilience of the whole city. These will be comprehensive by dealing with all elements of the urban system: critical infrastructures, built-up spaces and public spaces, and will cover impact-and-vulnerability assessment and selection of adaptation options. A decision support system will be developed to support decision makers in following a standardised path towards the choice of appropriate and effective adaptation measures into strategies tailored to the particular circumstances of a specific city. RESIN will explore the possibilities and prepare the materials to include adaptation in European standardisation processes.

Project deliverables

To this end, RESIN aims to create a common unifying framework that allows comparing strategies, results and identification of best practices by:

- Creating an urban typology that characterises European cities based on different socio-economic and biophysical variables;
- Delivering standardised methods for assessing climate change impacts, vulnerabilities, and risks;
- Providing an inventory of adaptation measures for critical infrastructures and other urban elements, and developing standardised methods to assess the performance of such adaptation measures;

Peter Bosch

Peter Bosch (MSc) is coordinator of the RESIN project. He works at as senior research scientist at TNO in the Netherlands. In the past years he was involved in the coordination of a large national research project on the adaptation of Dutch cities to Climate change ("Climate Proof Cities"), and other projects supporting cities and the Dutch government in climate change adaptation. He was educated as physical geographer and worked previously for the IPCC and the European Environment Agency.

e-mail: RESIN@tno.nl
TNO
PO box 80015
3508 TA Utrecht
The Netherlands

- Developing an overview of decision support tools in the areas of stakeholder analysis, risk and vulnerability assessment, prioritising between adaptation options and risk reduction strategies, and monitoring and evaluation.
- Collaborating closely with 4 'case cities' for practical applicability and reproducibility;
- Creating a circle of sharing and learning consisting of the core cities together with "Tier 2" cities around them for sharing knowledge and expertise.
- Interacting with European Standardisation organisations to ensure a systematic (standardised) implementation;
- Integrating findings in a coherent framework for the decision making process, with associated methods, tools and datasets.

The consortium consists of researchers with a background in urban climate adaptation (such as the University of Manchester, TNO, Tecnalia) and in risk assessment of critical infrastructures (Fraunhofer, TNO, Siemens). The team includes a large (ARCADIS) and a small (BC3) consultancy experienced in delivering this knowledge to the cities and other customers. Siemens and ITTI are a large and a small business that deliver technical support for managing cities. Four cities from various parts of Europe are a key part of the team. These cities (Bilbao, Manchester, Bratislava, Paris) will serve as a testing ground and are part of the co-creation process to ensure the practical applicability of the research findings. ICLEI, as networking partner, has the capacity to disseminate all outcomes to other cities in Europe. NEN, as member of CEN, the European standardisation body, will take the work forward towards formal standardisation.

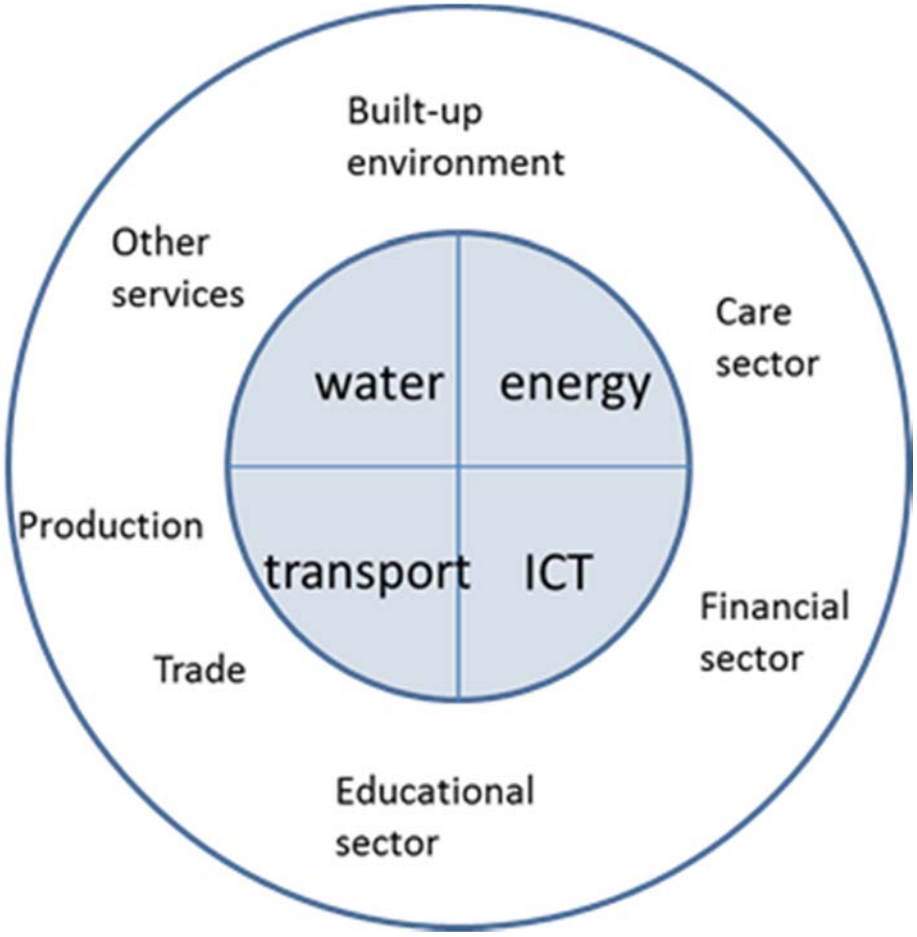


Figure: The cities living and working environment depends on well-functioning infrastructures

RESIN as a project

The RESIN project started in May 2015 and will run for 3.5 years.

UNIRESEARCH will bring project coordination capacities to ensure a successful delivery.

Cooperation will be established with existing European projects dealing with (urban) critical infrastructures and climate change such as INTACT, RAMSES, STREST and PREDICT.

More information

More information about the project can be found already now (and certainly in the near future) on our website: www.resin-cities.eu

Contacts: resin@tno.nl

RESIN has received funding from the European Union's Horizon 2020 programme under grant agreement No. 653522.

RESIN
CLIMATE RESILIENT CITIES AND INFRASTRUCTURES

Poor integration between critical infrastructures and other parts of cities in existing urban climate adaptation strategies formed the starting point of the RESIN project. RESIN will link the existing approaches for climate change adaptation of cities with disaster risk management of critical infrastructures to develop an overall approach for all sectors and elements of the urban system.

Developing a "unifying framework" for the adaptation and disaster risk management process is one of the first steps to be taken in the project.

In developing the subsequent assessment methods and support, we will standardise what can and needs to be standardised.

GRRASP: Geospatial Risk and Resilience Assessment Platform

The development of GRRASP addresses the issue of developing tools for performing analysis of complex networked infrastructure systems.

Critical Infrastructure Protection is getting increased attention as a result of the number of man-made threats (terrorism, malicious attacks, cyber events) and natural disasters. In addition to that, critical infrastructure systems are becoming more and more interconnected with the introduction of ICT technologies and thus isolated events may lead to large-scale or even continent wide disruptions. Interdependencies between critical systems are a key factor that needs to be considered when it comes to the analysis and simulation of critical systems in terms of their resilience. In the US, the NISAC (National Infrastructure Simulation and Analysis Centre) has developed a number of tools for the analysis of CI systems, supply chains, etc. that are tailored for the US reality.

In the aftermath of the terrorist attacks in US and EU the European Commission proposed A European Programme for Critical Infrastructure Protection (EPCIP). The EPCIP was adopted in 2006 and in 2008 the EPCIP Directive was put in force. In 2013 a revised EPCIP was published, clearly mentioning the importance of resilience, interdependencies and impact of CI disruption. JRC responds to this request by developing tools and methodologies. One of them is GRRASP (Geospatial Risk and Resilience Assessment Platform), which aims to bridge the gap of lack of tools for the analysis and simulation of CI at European level. GRRASP is available to be used by CI stakeholders. Furthermore it can be also used for training professionals in the domain of tools for prevention, preparedness and response.

In Europe, most tools are developed responding to national efforts and focus on the specific issues that need to be addressed at national scale. Obviously this approach shows its limitations when it comes to large-scale CI that expand across borders and jurisdictions.

Data sharing is a major issue in the field of CI analysis and this is a parameter that actually hinders development of tools and methodologies for the analysis and simulation of CI.

Collaboration among CI stakeholders is an open issue that is strongly associated with CI analysis and simulation. In order to foster collaborative analysis it is important to make sure that all stakeholders agree on a common terminology and to provide tools enable collaboration while ensuring data security and privacy through the whole analysis cycle.

CI owners and operators have agreed on several occasions the importance of developing tools and methodologies for modelling and simulation in CIP. It is true that in the recent years, an important number of tools have been developed and these can be used for the assessment of a wide number of disruptive scenarios. It seems though that most of such tools lack the features to be used throughout Europe and therefore fail to become standards. In principle, they represent ad-hoc efforts tailored to the needs of a particular region, state or sector. Consequently, often they lack the capability to scale up to international level.

In response to the above-mentioned issues we have developed in JRC the Geospatial Risk and Resilience Assessment Platform - GRRASP.

Georgios Giannopoulos

Dr Georgios Giannopoulos MS Mechanical and Aeronautical Engineering / PhD in Engineering from Vrije Universiteit Brussel / MS Solvay School (Economics & Management).

e-mail:
georgios.giannopoulos@jrc.ec.europa.eu

Luca Galbusera

Luca Galbusera, MSc degree in systems and control engineering / PhD Information Engineering from Politecnico di Milano.

e-mail: luca.galbusera@jrc.ec.europa.eu

Both authors are with:
European Commission
DG Joint Research Centre (JRC / IPSC)
Institute for the protection and security of the citizen
Security Technology Assessment Unit

The main objective is to provide an analysis tool that can be used by MS authorities and operators in order to improve risk and resilience assessment at local, regional, national and international scale. In addition to that we aimed at developing a tool that can be also useful for developing and testing new models as well as for training.

GRRASP tiers and applications

GRRASP can be considered as a hybrid tool that combines the power of GIS systems with mathematical models in order to provide a complete analysis environment with strong visualisation and simulation capabilities. The GIS layer is implemented for data entry (where applicable) and for data/analysis results visualisation as well as for taking advantage of the large amount of available libraries for performing analyses on geospatial data. However, in order to expand GRRASP's capabilities, the computational engine is based on Matlab® developed modules that have been compiled and can be used in stand-alone mode using the Matlab Runtime Compiler (available for download for free). This approach facilitates the interoperability between mathematical models and web based technologies (Apache, Tomcat, etc.).

GRRASP is based on a modular open architecture in order to render the system expandable and scalable to cope with future technology developments (e.g. cloud services). A server-client architecture is implemented in order to facilitate collaboration among users on common projects. Apart from the computational engine, GRRASP is based on a Postgres database where information relevant to models is stored and can be retrieved upon request by the end user. Geoserver, Tomcat, Apache and Drupal technologies (see Figure 1) are used in order to enable to remote users to introduce data, run models and visualise results through their web browser.

As already mentioned GRRASP is developed having in mind the need for a collaborative environment, however, data security is a prerequisite. The architecture implemented in GRRASP strongly considers this element. In addition to that, GRRASP allows (for certain modules) uploading proprietary data, invoking the necessary module, visualising the results and then cancelling all uploaded data. This is an additional level of data security that has been implemented in order to cope with the requirements of the CIP analysis community.

When it comes to the structure of the scientific modules, GRRASP follows a tiered approach (see Figure 2) that facilitates the engagement of actors from various fields and with different expertise.

Tier 1 (sectoral analysis) constitutes the basis of most simulation software for critical infrastructure analysis and obviously there is a reason for this. Research institutes and scientists are often specialised in a particular domain and for this reason there is the tendency to develop detailed engineering models. Typically, such approaches require a high amount of specialised data. On the other hand, these models can provide very detailed descriptions of critical infrastructures and exhibit limited uncertainty, while they often require considerable development time. Further, typically they can only be used by experts in the respective field and the developers have certainly the

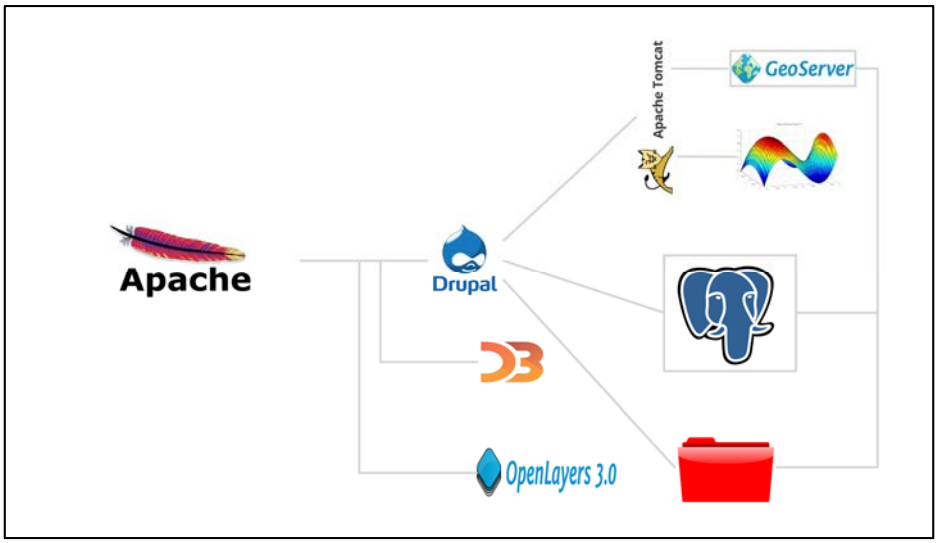


Figure 1: GRRASP architecture

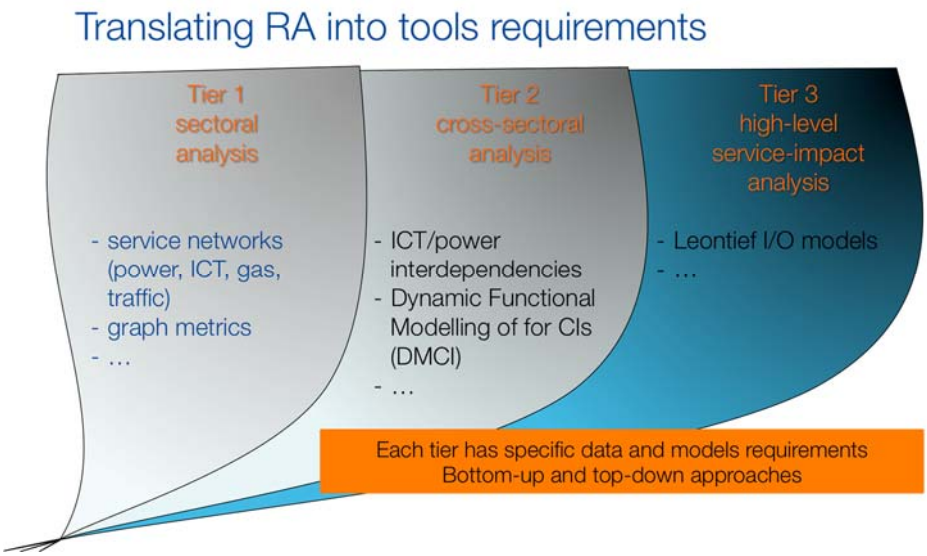


Figure 2: GRRASP tiered approach

primary ownership due to the inherent complexity of such systems. In principle the maturity in this area is high and the vast majority of actors in the field are focused on this particular Tier. In this Tier one may find models that are applicable at all levels (local, regional, national, international), however, their complexity and difficulty rather increases as we scale-up towards national/international level. An example of a model in GRRASP belonging to this tier is the Geomagnetically Induced Current module that evaluates the development of geomagnetically induced currents on power grids due to the variation of earth's magnetic field that follows severe space weather events. Another example is the one of structural analysis of networks (see Figure 3).

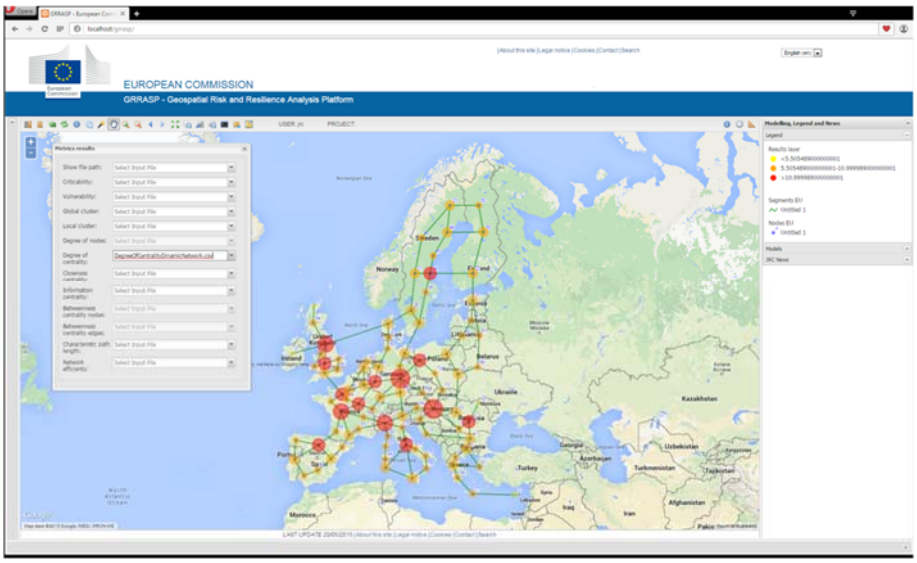


Figure 3: Interface for network metrics in GRRASP

By definition, **Tier 2** (cross-sectoral analysis) includes models that require more knowledge on the interactions between sectors and less specific knowledge on the particular dynamics of a sector. Piecing together models belonging to the first tier while addressing different sectors might lead one to think to obtain an analysis of interdependent systems however, this is not the case. Although this may seem reasonable as a claim, in reality it is strenuous due to the tremendous complexity that this approach would generate and also imply a request for a huge amount of data. So it is necessary to adopt a different approach that focuses on higher-level variables such as demand and delivery of services and in that way interdependent infrastructures can be modelled with less data and also reduced complexity. Here we have much fewer models, although their complexity can be even lower with respect to Tier 1 models. It is important to mention here that Tier 2 models are applicable at all levels but certainly their real strength is shown when it comes to regional and national level. At an international level it is very important to represent large parts of infrastructures with a limited amount of information otherwise there is the risk to go towards first tier models.

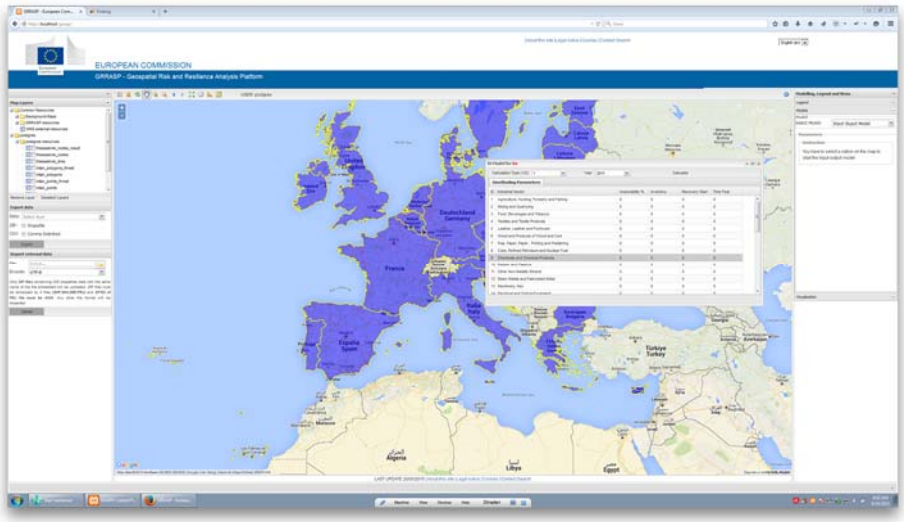


Figure 4: Input-Output model interface

Tier 2 modules are related to the assessment of interdependencies between sectors of critical infrastructures. Interdependencies can be classified as functional, logical, cyber and geographical and certainly a robust interdependencies analysis module should be able to take into account all these types of interdependencies. In order to address this issue we have jointly developed with Polytechnic School of Milan an interdependencies analysis module, the DMCI (Dynamic Functional Modelling of vulnerability and interoperability of CIs)[1] that takes into account the above mentioned types of interdependencies while its modularity enables the end user to define nodes of critical infrastructures on a map and establish cross-sectoral interdependencies among these assets. Among other advantages, this type of tool enables the collaboration of multiple actors in the field thus it facilitates a bottom up approach towards improving the understanding of interdependencies among sectors. Relevant application examples include the impact assessment of power grid disruptions on telecommunications or the effects of a disruption in the rail transports on the road transport network due to the transfer of service demand by the end users.

Tier 3 (high-level service impact analysis) focuses on the assessment of high level impact at regional, national and international level taking input from the modules of Tier 1 and Tier 2, where relevant (see Figure 4). At JRC we have developed an economic impact module that has been introduced in GRRASP and it is based on an inoperability Input/Output

model[3]. This module includes enhanced features in order to describe the dynamics of the recovery process, while taking into account the existence of inventory within certain economic sectors. However, more modules are needed that can address important issues such as regionalisation of the effects of critical events. Although some of these issues this can be addressed, at a first stage, with a Tier 1 module, in that case the output would not be as accurate since high order effects (interdependencies) could be omitted. GRRASP's open architecture allows third party users to enrich the modules portfolio to complement existing capabilities of GRRASP across tiers. Currently the integration of the various modules belonging to different tiers is under development. This will lead to a seamless risk and resilience assessment framework, starting from the assessment of threats at sectoral level leading to estimate interdependencies between sectors and finally reaching the assessment of the total economic impact. The inclusion of further types of impact analysis at Tier 3 is also under development.

In addition to these functionalities, we have equipped GRRASP with the capability to fetch data from remote servers and use them for visualization purposes or for initiating a Risk/Resilience analysis. This functionality enables GRRASP users to set up dynamic and interactive processes for information exchange and sharing of risk maps as well as other geospatially related data. Currently such services are deployed only in a few cases. As an example we provide the case of Italy (see Figure 5) that has set up a portal for this purpose and shares information on risks concerning earthquakes at the level of NUTS 3 areas.

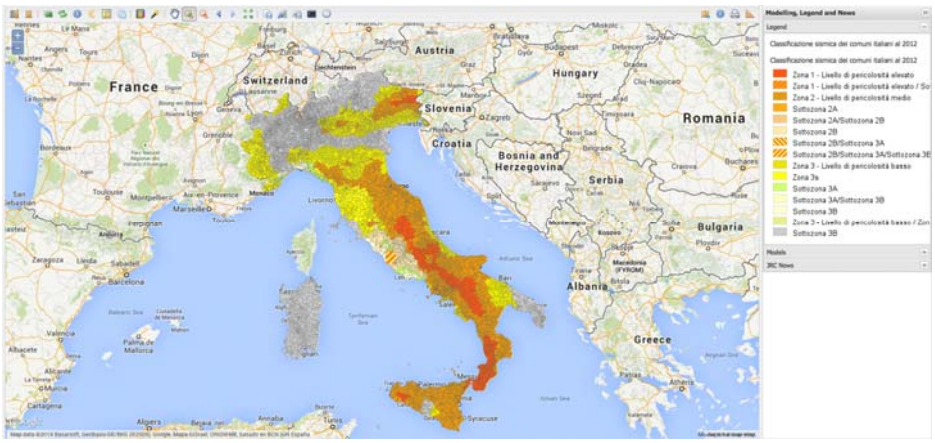


Figure 5: Visualisation of risk maps in the GRRASP environment

Future Work

GRRASP addresses several issues expressed by MS and operators mainly in the domain of tools and methodologies for assessing risks and resilience for CIs. We foresee a further development of GRRASP by introducing more modules, additional applications and a standardised interface in order to include modules by the end users. This will enable the CIP community to expand GRRASP in various directions and render it into a powerful tool for running a series of risk and resilience scenarios for CIs at local, regional, national and international level leveraging the scalability of the system.

In addition to purely Critical Infrastructure related applications, GRRASP enables the analysis also in other domains where the geospatial component is important and where strong modelling capabilities are required coupled with the necessity of a collaborative approach among various stakeholders.

Acknowledgements

GRRASP development has been supported by the "The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS)" Annual Work Programme 2011, 2012 through Administrative Arrangements with JRC. This support is highly appreciated.

References

1. Dynamic functional modeling of vulnerability and interoperability of critical infrastructures, P. Trucco, E. Cagno and M. De Ambroggi, 2012, Reliability Engineering and System Safety, vol. 105, pp. 51-63

2. Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms, E. Zio, L.R. Golea and C.M.S. Rocco, 2012, Reliability Engineering and System Safety, vol. 99, pp. 172-177.

3. Analysing Critical Infrastructure Failure With a Resilience Inoperability Input-Output Model, Olaf Jonkeren and Georgios Giannopoulos, 2014, Economic Systems Research, vol. 26, no. 1, pp. 39-59.

If you would like to know more about GRRASP please visit our website: https://ec.europa.eu/jrc/en/grrasp

Critical Infrastructure Protection: from protection to resilience

A review of critical infrastructure based on uniform criteria and limit values for social disruption that apply to all public, private and semi-private partners in the Netherland

An incident on 27 March 2015 illustrated the dependency of our society on electricity. A power failure left one million households without electricity. Traffic lights stopped working. Trains, metros and trams were out of service and aircraft could no longer land at Schiphol Airport. In the affected area, mobile telephone communications and electronic payment systems were disrupted as well and parts of the businesses came to a standstill.

Guaranteeing the continuity of critical infrastructure is of common interest to both critical (usually private) organisations and to society. Critical infrastructure includes products, services and underlying processes which, should they fail, could cause large-scale social disruption. That is why the government and critical organisations in the Netherlands cooperate in protecting this infrastructure.

Integrated approach

An integrated approach is required, due to the number of parties involved. This is a dynamic and complex domain due to technological developments and interconnectedness of critical processes.

Society has become more dependent on critical infrastructure while the failure of such infrastructure has become less accepted in society. Infrastructure has become more dependent, for example, on IT systems and electricity and has become more vulnerable to (deliberate) cyber incidents.

Moreover, the interconnectedness of critical processes makes it difficult to predict cascade effects. Due to cascading effects the impact can be larger if single processes fail. Critical organisations and the National Government recognise this also on the basis of chain analyses of critical organisations.

Change to a sectorial approach

On behalf of the Dutch Government, the Minister of Security and Justice informed the House of Representatives in 2013 that the policy on the protection of critical infrastructure was to be reviewed. That review has resulted in a new prioritised list of what is considered critical infrastructure in the Netherlands with more focus than before. Instead of a sectorial approach, the relevant processes underlying the products and services are identified. As such, as of 2015, critical infrastructure in the Netherlands is defined in critical processes.

The review has also provided insight into the most important risks, threats, vulnerabilities and the degree of resilience of this infrastructure. Moreover, (more) attention is paid to the implementation of resilience enhancing measures (e.g., security measures). On the national and regional level, businesses, government and scientific institutes work together towards strengthening the identified critical infrastructure processes.

Sven Hamelink

Sven Hamelink (MSc) is program manager at the Dutch Ministry of Security and Justice. He has been working on a variety of topics in the fields of counterterrorism, security and crisis management. He is currently in charge of the national approach for CI resilience.

e-mail: vitaal@nctv.minvenj.nl

Jeroen Mutsaers

Jeroen Mutsaers is a policy officer at the Dutch Ministry of Security and Justice working on (inter)-national security and resilience and climate change adaptation. He is currently involved in the novel national approach for CI and resilience.

Definition of critical infrastructure

A clear definition and identification of critical infrastructure for the Netherlands in 2015 and a suitable policy that ensures and enhances resilience are essential for the national security. For this purpose, the degree of criticality was assessed on the basis of criteria and limit values for social disruption which apply to all public, private and semi-private partners.

Criteria

Criteria were developed based on the National Risk Assessment methodology as used in the National Security Strategy. An integrated impact assessment of the consequences of a failure of the previously identified critical sectors was conducted based on economic, physical and social impact.

Cooperation with partners - Tools and Instruments

In 2015-2018 further action is taken to identify possible new critical processes. Moreover, the aim is to improve accessibility to security tools and, where necessary, develop new instruments for the critical infrastructure. Strategic alliances will be established between businesses, scientific institutes and government.

The review will result in a (more) targeted use of resilience enhancing instruments. For instance, critical infrastructure will be incorporated into the crisis management decision making structures and will be given special attention in the trainings of the National Academy for Crisis Management (NAC). In addition, the National Cyber Security Centre provides its services to businesses in critical processes.

The review has, due to the joint efforts by the relevant public and private partners, resulted in an up-to-date and clear insight into what is critical to our society. The review focusses on the impact on society which resulted into one complete list of critical infrastructure. In future policy and projects, the degree of criticality is used as the guiding principle for programmes and policies.

Categories A & B

A distinction is made between category A and category B in order to reflect the diversity within critical infrastructure, in order to set priorities in case of incidents for example, and in order to allow for individual arrangements if measures are taken that enhance resilience.

New list of Critical Infrastructure

The table on the following page shows the new list of critical infrastructure.

Category A

This includes infrastructure whose disruption, damage or failure will have the type of impact described in at least one of four impact criteria below:

- Economic impact:
  > approx. €50 billion in damage or an approx. 5.0% drop in real income
- Physical consequences:
  more than 10,000 dead, seriously injured or chronically ill
- Societal impact:
  more than 1 million people afflicted by emotional problems or serious problems with basic survival.
- Domino effect:
  failure results in the breakdown of at least two other sectors.

Category B

This category includes infrastructure whose disruption, damage or failure will have the type of impact described at least one of three impact criteria below:

- Economic impact:
  > approx. €5 billion in damage or an approx. 1.0 % drop in real income
- Physical impact:
  more than 1,000 dead, seriously injured or chronically ill
- Societal impact:
  more than 100,000 people afflicted by emotional problems or serious problems with basic survival

NCTV

The National Coordinator for Security and Counterterrorism (NCTV) protects the Netherlands from threats that could disrupt Dutch society. Together with the partners within the government, the research community and the private sector, the NCTV ensures that the Netherlands' critical infrastructure is safe and remains that way.

For any further questions about the protection of critical infrastructure, you can contact the Critical Programme via vitaal@nctv.minvenj.nl .

See next page:
Table on Processes, categories, services, sector and responsible ministry.

Processes	Cat.	Product, service or location	Sector	Ministry
National transport and distribution of electricity	A	Electricity	Energy	Economic Affairs
Regional distribution of electricity	B			
Gas production National transport and distribution of gas	A	Natural gas		
Regional distribution of gas	B			
Oil supply	A	Oil		
Internet access and data traffic	TBD		IT/ Telecom	Economic Affairs
Speech-communication services (mobiles and landlines)				
Satellite				
Time and location services (satellite)				
Drinking water supply	A	Drinking water	Drinking water	Infrastructure and the Environment
Flood defences and water management	A	- primary flood defences - regional flood defences	Water	Infrastructure and the Environment
Air traffic control	B	Schiphol Airport	Transport	Infrastructure and the Environment
Vessel traffic service	B	Port of Rotterdam		
Large-scale production/processing and/or storage of chemicals and petrochemicals	B	Chemical and petrochemical industry	Chemistry	Infrastructure and the Environment
Storage, production and processing of nuclear materials	A	Nuclear Industry	Nuclear	Infrastructure and the Environment
Retail transactions	B	Financial transactions	Financial	Finance
Consumer financial transactions	B			
High-value transactions between banks	B			
Securities trading	B			
Communication with and between emergency services through the 112 emergency number and C2000	B	Maintaining public order and safety	Public Order and Safety	Security and Justice
Police deployment	B			
E-government: the availability of reliable personal and corporate data about individuals and organisations, the ability to share such data, and the availability of data systems which multiple government agencies require in order to function	B	Digital government	Public Administration	The Interior and Kingdom Relations

Swiss Cyber Storm 2015

International IT Security Conference

21st of October 2015
KKL Lucerne, Switzerland

Meet international experts talking about the latest findings, techniques, visions, opinions and lessons learned. With coffee breaks, lunch and apéro riche, the conference provides a lot of room for networking. Thanks to the co-location with the European Cyber Security Challenge, the conference offers an unique opportunity to network with young talents from Austria, Germany, Romania, Spain, Switzerland, and the United Kingdom. All of these countries send a team formed by the winners of their national cyber competition to foster collaboration and to find out who has the best young cyber talents in Europe.

EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!

Featured Talks:

- **Keynote: Why organizations keep getting breached....Still, in 2015**
  Kevin Beaver, Security Consultant, Writer and Professional Speaker, Principle Logic, LLC
- **Flushing Away Preconceptions of Risk**
  Thom Langford, CISO, Publicis Group
- **Threat Intelligence Sharing – Lessons from the Front Lines**
  Patrick Miller, President Emeritus, EnergySec
- **Visibility in the ENISA Threat Landscape**
  Louis Marinos, Senior Expert Risk Management, ENISA

... please check out the full program on our website!

http://www.swisscyberstorm.com

Partners

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Eidgenössisches Finanzdepartement EFD

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Center for Cyber and Information Security and Norwegian Information Security Laboratory

Nations need research support to defend their Cyber Space. Norway reacted early and took coordinated effort.

NISlab

The Norwegian Information Security Laboratory (NISlab) was founded in 2002 and is situated at Gjøvik University College becoming in January 2016 part of NTNU – the Norwegian University of Science and Technology. The group conducts international competitive research in several areas of information and cyber security, supervises Ph.D. research projects in this field and operates study programs in information security at the Ph.D., M.Sc. and B.Sc. level. NISlab leads the national COINS Research School of Computer and Information Security, presenting round about half of Norway's PhD students in the field.

With around 50 affiliated persons, NISlab constitutes one of the larger academic information and cyber security groups in Europe, and has a broad approach to information and cyber security. However, through our focus laboratories, NISlab has a particular focus on biometrics, forensics and information security management.

In Norway, key national cyber security stakeholders have initiated a partnership to establish the Center for Cyber and Information Security (CCIS), a national center for research, training, and education in cyber and information security.

NISlab has in the past five years had more than 80 research publications published in internationally renowned research papers and worked together with around 100 partners worldwide. NISlab hosts and is a member of the Center for Cyber- and Information Security in Gjøvik.

Contact: Dr. Laura Georg
E-Mail: laura.georg@hig.no
www.nislab.no

CCIS

A number of organisations, including the National Police, Industry and Academia, have partnered to create CCIS. CCIS's partners will strengthen the centre's expertise and skills to prevent, detect, respond to, and investigate undesirable and criminal computer based activities. CCIS establishes competence transfer across agencies, companies and sectors. It facilitates research projects that connect industry and government agencies with international research networks, thus helping to build the essential, critical infrastructure to strengthen Europe's cyber and information security. The centre is important because there is a need for extensive international cooperation and long-term research to prepare for tomorrow's challenges.

The CCIS Security of Critical Infrastructures (SCI) group was formed around a long-standing research group at NISlab studying selected aspects of the security and dependability of critical infrastructures at different abstraction levels ranging from national level and supranational dependency and interdependency models to protocols, sensor, and actuator security in process control systems. The SCI group seeks to address these core challenges in close collaboration with national and international partners.

Contact: Sofie Nystom
E-Mail: sofie.nystrom@ccis
https://ccis.no

Laura Georg

Laura is Head of NISlab (PhD in information security, Geneva University) and worked eight years in consulting across various industries. For Deutsche Telekom's consulting unit, she acted as Global Head for IT Risk & Security, before becoming Managing Partner at BaXian AG.
e-mail: laura.georg@hig.no

Sofie Nyrstøm

Sofie is Director of CCIS and a member of the Government new Digital Vulnerability Committee. Previously, she served as Head of Group Security, Telenor Group and Chief information security officer at DNB Bank. Nystrom led the establishment of NorCERT within the National Security Authority.
E-mail: sofie.nystrom@ccis.no

The System Security Lab

Teaching practical security classes requires the existence of lab environments, where students can experience with methods and tools that they learn in theory. This includes attacking techniques that exploit weaknesses and vulnerabilities in computer systems, but also methods and techniques to defend against these attacks.

The goal of the System Security Lab is the creation of a dedicated hybrid network testbed that can be used for educational and research purposes. Hybrid means that the testbed contains both virtualised as well as real hardware components. This lab enables students to conduct cyber security exercises to get hands-on experience and skills in various practical information security topics, e.g., defence and offence mechanisms, incident response processes and security monitoring methods.

The development of the systems Security Lab started in June 2015, and the design of this lab provides:

(1) a high level testing language and a pre-defined catalogue of a wide range of exploits and defence techniques, which ease the design and deployment of the testing topology and infrastructure;
(2) customisable scoring engine that can be used for different types of experiments; and
(3) security monitoring infrastructure that enables the deployment of a wide range of agent sensors that corresponds to the conducted experiment and its associated vulnerabilities.

Besides the educational role of the lab, it provides the underpinning infrastructure for conducting research experiments in different areas of research, e.g., in software security, security testing, security monitoring, and software defined networks.

Contact: Assoc. Prof. Basel Katt
E-Mail: basel.katt@hig.no

The Forensics Group

The CCIS Testimon Forensics Group evolved from an academic research group established in September 2010 to a partnership and close cooperation with Norwegian law enforcement agencies (LEA), including the Norwegian Police Directorate, Norway's National Criminal Investigation Service (KRIPOS), the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM), the Norwegian Police University College (Politihøgskolen), and regional LEAs for instance the Oslo and Vestoppland police disctricts.

CCIS Testimon is an education and research environment, in particular for Digital and Computational Forensics. It is in charge of a Master of Science (MSc) specialisation track on Digital Forensics within the MSc Information Security (i.e. MSc Information Security / Digital Forensics) offered by Gjøvik University College. In addition, CCIS Testimon offers an Experienced-based Master in Digital Forensics and Cybercrime Investigation in cooperation with Politihøgskolen.

CCIS Testimon conducts fundamental research and applied research on behalf of LEAs. Members of the group contribute to forensic casework, expert witnesses, and advisory services in cooperation with partners, e.g. EC3 - Europol Cyber Crime Centre - AG Internet Security, and NRGD - Nederlands Register Gerechtelijk Deskundigen - Ministry of Security and Justice, The Netherlands.

In addition, Testimon members are involved in networking and community-building activities in the computing and digital forensic sciences, e.g., conferences, workshops, tutorials, and invited lectures such as the International Workshop on Computational Forensics (IWCF), and the Technical Committee (TC6) on Computational Forensics under the auspice of the IAPR – International Association of Pattern Recognition.

The current Testimon-research agenda is focusing on three main topics:

- Big-data Forensics and Forensic as a Service using secure computing infrastructure,
- Cloud Forensics and Cybercrime Investigation, and
- Mobile & Embedded Device Forensics (IoT, IoE).

This research agenda is in line with major strategies by the Norwegian police and European cyber-security strategy.

An example of on-going research projects is *ArsForensica*: Computational Forensics for Large-Scale Fraud Detection, Crime Investigation and Prevention. Funded by the IKTPLUSS programme of the Norwegian Research Council. The four-year project involves excellent research environments from Norway and abroad, such as the United Nations Interregional Crime and Justice Research Institute, the University California Santa Cruz, USA, the Kyushu Institute of Technology, Japan, the Netherlands Forensics Institute, the University of Groningen, Netherlands, and the Norwegian Computing Centre.

Contact: Prof. Dr. Katrin Franke
E-Mail: katrin.franke@ccis.no

The Biometrics Lab

Since its inauguration in 2011, the Norwegian Biometrics Laboratory (NBL) has evolved significantly in terms of the number of PhD students and its research activities. It is a fruitful lab to brainstorm and to generate new ideas for projects. NBL is an essential part of NISlab / CCIS and represents an active focus point with currently four ongoing EU research projects under the FP7 framework program. The projects namely *FIDELITY, INGRESS, ORIGINS* and *PIDaaS* deal with biometrics and identity management. Two additional project proposals are under evaluation at this moment. Moreover NBL is serving industry on bilateral research activities and has also established a project relationship with the Nasjonalt ID-senter (NID) and supports with its research and

testing future decisions that are taken. Also on the national level NBL was awarded recently with the *SWAN* project, which will be funded by the Research Council of Norway under the IKTPLUSS program.

NBL's biometric research is covering various physiological and behavioural biometrics including 2D- and 3D-face recognition, iris recognition, fingerprint recognition, finger vein recognition, dental biometrics, ear recognition, signature recognition, gait recognition, keystroke recognition, gesture recognition and mouse dynamics.

Furthermore, the lab focuses on privacy enhancing technologies such as biometric template protection and integration in physical and logical access control.

The Biometrics lab is an active member in the European Association for Biometrics (EAB), and organiser of several international conferences on Biometrics such as the IEEE BIOSIG conference and the EAB-RPC conference.

NBL is also representing Norway in the COST ACTION IC 1106 and was in this role organising the 3rd International Workshop on Biometrics and Forensics (IWBF'15), which took place in Gjøvik on 3-4 March 2015.

It is the intention of NBL to increase the awareness of biometrics in Norway via the Norwegian Biometric Forum (NBF) that is meeting twice a year. The lab also contributes to the international standardisation in the field and have organised the international standardisation conference ISO/IEC JTC1 SC37 in June 2015.

Contact: Prof. Dr. Christoph Busch
E-Mail: christoph.busch@hig.no

The Information Security Management Group

The adage "manage or be managed" when applied to security management can be expanded to read to continually learn to manage yourself and your organisation efficient and effectively with the right incentives or you will end up being managed by your enemies. The Information Security Management Group conducts theoretical, empirical and applied/ clinical research to modelling, measuring and managing information security management problems. The group leverages its academic research into the national arena by collaborating with the Norwegian Center for Information Security (NorSIS) to help organise and arrange the Norwegian Security Roundtable three times an year and participate in the annual national cyber security awareness month. Below is a picture from the 2013 kick-off of the Norwegian Cyber Security Awareness Month where one of the founding members of the ISMG gave a speech to explain "manage or be managed adage of the group. The speech was entitled "Edward Snowden: The Revenge of the Nerd" and outline how the Snowden affair was mainly a problem of poor security management rather than weak or inadequate security technologies.

Professor Kowalski (centre) NORSIS previous Directory Tore Larsen Orderløkken (right) and Nils Kalstad Svendsen (left) the previous leader of NISlab.

The group also has a special responsibility for the information's security management track of the MSc at University College Gjøvik. Consequently its research based teaching methods bring together a broad spectrum of socio-technical systems security research results that cover the social, organisational, psychological, legal, ethical, cultural, political, rhetorical educational and technical aspect of cyber- and information security management.

Contact: Prof. Dr. Stewat Kowalski
E-Mail: stewart.kowalski@hig.no

Critical Infrastructures Lab

The Critical Infrastructure Lab serves to co-ordinate research across the wide spectrum of security and resilience questions in national and supranational critical infrastructures particularly from the tighter integration of infrastructures using information and telecommunication systems, but also the embedding of computational and communication capabilities within the infrastructure elements themselves.

Research hence includes work at higher abstraction levels such as the analysis of dependencies and interdependencies among infrastructures and their dynamic changes, which was initiated by members of the lab in the late 1990s and continuing to evolve along with the infrastructure itself.

Many critical infrastructures also rely on control systems; this has attracted considerable attention in recent years. Research in the lab has focused on novel attacks and resilience mechanisms against the observability and controllability of control systems, particularly in areas where stability and timeliness is of importance such as in electrical power networks including smart grid environments, and continues to investigate attacks specific to such cyber-physical systems where in-depth modelling yields important insights. Whilst also applicable to general industrial control systems, the main emphasis is on the energy sector as the application domain, however, with a number of European and national projects providing support.

Given the complexity of the problem space, understanding risks and vulnerabilities cannot be achieved exhaustively, nor can all possible contingencies be considered; both the construction of scenarios and systematic attack models, as well as incident response mechanisms also have their place within the confines of the laboratory; given the frequent need to co-ordinate among entities and dependencies among not just the information technology but also the physical infrastructure, these

challenges are distinct from those encountered in a purely ICT-based environment; it is also at the same time more difficult to clearly identify the threat sources and actors as these are known to have a wide range of capabilities ranging from individuals to nation state actors.

Collaboration with partners from government including national security authorities and emergency services, but also the defence sector is important in understanding the scope of challenges and contributing not only to advancing the scientific and mathematical knowledge but also to contribute to the resilience of society to faults and attacks; similarly, close collaboration with industry is crucial in understanding present and future challenges in infrastructure security as well as providing the ability to collaboratively approach such challenges. Cooperation with national critical infrastructure operators such as Telenor, Statnett, and Statkraft as well as other infrastructure providers ensures timely and relevant research.

Contact:
Prof. Sokratis Katsikas
E-Mail: sokratis.katsikas@ccis.no /
Prof. Stephen Wolthusen
E-Mail: stephen.wolthusen@hig.no

European Projects

The areas of research that occupy NISlab's focus groups have already been mentioned with some details above. NISlab and CCIS comprise a large number of researchers in the various topics of cyber security; it is a dynamic and motivated group of young but seasoned academics and researcher with ample research background and with a strong international network. The researchers continuously engage in identifying project opportunities and developing high quality national and international consortia. For years, NISlab has been at the very top of the list of institutions in Norway with the largest EU-funding per researcher. For several years now researchers at NISlab have been well acquainted with responding to EU calls for proposals and with obtaining research funding from the various schemes and EU programmes.

NISlab's research interests are well aligned with the focus areas and themes in the European Commission's Horizon 2020 programme under the so-called pillars on Excellent Sciences, Societal Challenges and Industrial Leadership. NISlab has taken on various roles, including as participating partner, as coordinator, or as individual researcher through the MSCA programme.

The Research Council of Norway has played a key role in providing support to the research strategy and activities at NISlab by financing research through their funding schemes --most recently three important projects have been granted funded under its ICT-Pluss programme. But also RCN has contributed importantly with NISLab by making funds available to support the proposal development stage in responding to major EU calls.

Florissa Abreu
E-Mail: florissa.abreu@ccis.no

National Cyber Defence: Preparedness handling attacks on all level

Cyber act of war, Espionage, sabotage subversion: How to organise and prepare against it? See Norwegian approach below.

Thomas Rid states that there will be no war only in cyber, and he divide the threat into espionage, sabotage and subversion (Rid, 2011). This grouping of the threat is partly supported by Director of National Intelligence (DNI). But he only has two groupings, espionage and cyberattack (Clapper, 2013, p. 1). By studying the past, what kind of hostile activities have we seen so far, and would any of these activities lead to war. In the end how to organise to face this challenges.

Cyber act of war

The threshold of a cyberattack being an act of war is hard to find. NATO states in the latest strategic concept that cyberattacks may reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability (NATO, 2010). This is in line with Article 4 of NATO's founding treaty regulating consultation among the parties. USA has made an International Strategy for Cyberspace (The White House Office, 2011). This one states the right of self-defence, and it also states that cyberattacks may be faced with all necessary means. In Norway a cyberattack is linked to serious injury or death for personnel or material damage (Forsvarets høgskole/Forsvarets stabsskole, 2013, p. 190). This could lead to war. Stating war is a though a political decision, but linked to the criteria. These three examples show there is a possibility of a cyber act of war. But the aggression of the act is not defined.

Then a closer looks upon the three different groups of cyberattacks, and the severity which they may inflict to a nation.

Espionage

First we have espionage. Espionage in cyber is common to espionage in real life. Most of the states have an intelligence service trying to get as much information as possible on potential advisories. If a spy is cough in his activities on foreign ground, the case would be as a criminal act and handled by the police or the security services. In cyber it is hard to discover the person or organisation behind while the activity is underway. Cyberspace is borderless and the digital activity takes place on a different physical place than the location of the person or organisation behind. Even though there is an attribution problem there may be possible to point at someone doing espionage. USA has accused Russia on spying on the White House mail system[1]. In the early stages of the Sony hacking case in 2014 there had to be an espionage activity in order to find and exploit the data in the servers. Espionage is a large threat both to a nation or a company. Both the Director of the National Security Agency (NSA) and Richard Clarke have raised the issue. And they name the flow of vital information as "death by a thousand cuts"[2] (Rosenbaum, 2012). By this they state that the information stolen by espionage may threaten a nation's political or economic future. A company may lose their patents or business strategies, and thereby weaken their marked position in the years to come. In the end these activities are only criminal activities, which have to be faced by taking those behind to court or by inflicting sanctions on those supporting the activity.

Nils Gaute Prestmo

LtCol Nils Gaute Prestmo is a Army Signals officer and has more than 25 years of service. He currently serves in the staff of the Norwegian Cyber Defence in the operations branch. Last year he was a student at the Norwegian Defence Command and Staff College. This spring he delivered a master thesis on Cyber Security.

e-mail : nprestmo@cyfor.mil.no
Norwegian Cyber Defence
N-2617 Lillehammer
Norway

[1] Source http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/, 10th. August 2015

[2] "Alexander referred to the growing number of hacking incidents targeting US technology and corporate trade secrets as 'death by a thousand cuts." Source http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/us-facing-death-by-a-

Sabotage

Secondly there is sabotage. Sabotage in cyberspace is inflicting something through the digital world (Von Solms & Van Niekerk, 2013). Known sabotage actions are the STUXNET attack on Iranian nuclear facility and operation Orchard [3] on Syrian air defence system. The first one is against a governmental research facility and was executed by introducing malicious malware on offline systems (Rid, 2011, p. 17). The second one was targeting Syrian air defence systems making it possible for Israeli fighters to enter Syrian airspace undetected (Rid, 2011, p. 16) . Both were targeting the nation's ability to build nuclear weapons. Only the last caused effects outside the systems. The fighters targeted facilities and thereby probably both inflicted personal death and material destruction. Critical infrastructure is vulnerable to cyberattacks. In most of the nations around the world they are owned by private companies. The energy sector is often mentioned. In Brasil in 2007 there was a large blackout which was initially blamed on cyberattack [4]. It was later revealed that poor and lacking maintenance was the cause. In 2014 there was a large national outage in Turkey. Some media speculated on a large cyber-attack, but this was not confirmed (Senel, Hirsti, & Bruland, 2015). The indirect consequences of a power outage may be serious, and may lead to deaths among the population. The director of NSA, Admiral Mike Rogers, has stated that the energy sector is Americas Achilles heel [5]. To modern armed forces sabotage in cyberspace may hamper military operations, or even stopping them. Operation Orchard demonstrating what could be done to sensors. The Sony hacking case demonstrates the possibility to delete servers and making information unavailable.

Subversion

In the end there is subversion. Subversion is about changing the perception on subjects. It ranges from both defacing webpages and false twitter messages to large scale information operations. A false twitter message from Fox stating the death of president Obama, made the values on the stock exchange to drop [6]. Today we see large subversion attacks as a part of information operations in Ukraine. The pro-Russian fighters are controlling the electronic communication (ECOM) infrastructure in eastern Ukraine (Franke, 2015). By controlling the ECOM infrastructure there are multiple ways to perform hostile acts. Physical access to the net is vital for performing various cyberattacks. Controlling the network gives the possibility to deny access for certain users. All this together adds up to a favourable position to effectuate information operations. Few or none news agencies have formalised a cooperation regarding cyber security. In Norway the former national radio and Television Company, Norsk Rikskringkasting (NRK), has a formalised cooperation with NorCERT. During the process the journalists raised their voice and opposed the cooperation. They didn't want to lose their independence [7]. On the other side NRK didn't want to get in such a position where advanced cyberattacks could misuse their servers for hostile acts.

Sabotage is so far the only act in cyber which may lead to war. And the seriousness is judged on physical effects by the politicians. Espionage is influencing the power balance in advance and during war. Finally subversion are inflicting political decisions prior to and during war. Even though it's hard to find and prove quantitative effects caused by cyberattacks, there are some examples where a nation has responded by offensive means. According to the media USA blocked North-Korean internet access as a response to the Sony hacking case (Fackler, 2014). There are also articles on USA starting offensive actions as a response to several attributed cases over the last years [8].

How to organise

As describes in the previous text ownership of critical infrastructure (CI) is mostly private companies. They are exposed to sabotage, but the nations will be those who face the consequences. When looking into how to organise for handling the threat from cyberattacks there may be preferable to discuss two approaches. One approach is only focusing on the public part of the nation, while the other approach focuses on both the public and the private dimension of the nation.

Common to both approaches are the various Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT). These are related to the various sectors such as finance, energy, health etc. They are linked together both nationally and international, and they share information on threats and handling of these. Nationally there is often a national CERT on top level coordinating the information flow and reporting the government. Internationally there are organisations like European Union Agency for Network and Information Security (ENISA), Forum of Incident Response Teams (FIRST) and Fi-ISAC. They all share a function of sharing information and best practice. In case of cyberattacks the various national sectorial CERT and CSIRT are the entities to handle it on tactical level. There are no other response structures or incident handling organisations in cyberspace ready to respond and support. This is neither nationally or internationally. The only exception is NATO rapid reaction team [9]. The team is a part of the NATO Computer Incident Response Capability (NCIRC).

---

thousand-cuts-in-cyberspace/4ac6f26957f17cafb8611b6fa5899622.html , 7th. May 2015

[3] Source http://en.wikipedia.org/wiki/Operation_Orchard, 8th. May 2015

[4] Source www.wired.com, "Brazilian blaxckout Traced to Sooty Insulators, not hachers", 9th August 2015

[5] Source https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf, 5th May 2015

[6] Source http://www.theguardian.com/news/blog/2011/jul/04/fox-news-hacked-twitter-obama-dead , 5th May 2015

[7] Source http://www.klassekampen.no/article/20150113/ARTICLE/150119981, 5th. Mai 2015

[8] Source http://www.reuters.com/article/2015/09/01/us-usa-cybersecurity-russia-exclusive-idUSKCN0R12FE20150901 ,20th September 2015

[9] Source http://www.nato.int/cps/en/natolive/news_85161.htm

The first approach has focus on governmental structures and public systems. On one side the formalised command relations between decision makers and execute level is positive for prioritisation. In case of crisis or war the resources may be stretched, and the need for prioritisation is urgent. When focusing on public systems and having a large cyber capacity it's possible to focus on hostile states and state sponsored actors. On the other side this may narrow the focus area. The USA has several public organisations dealing with cyber security. The American model is criticized by Ricard Clarke (Clarke, 2009). He states that there is too much focus on offensive capacities. And the defensive capability is only focusing on governmental and public systems. In his article he is not discussing whatever the large offensive capability would deter potential adversaries. As the threat to public services is mostly espionage, there has to be a system of collaborating with private actors on handling sabotage and subversion. CERT and CSIRT, even in private sector, are mostly reporting incidents and handling incidents. They are not prioritising among each other. Laws and regulations on private ownership in Critical Infrastructure may not be enough to engage these actors in a cooperative venture to increase national cyber security.

The second approach and another way to organise are to have a stronger focus on public private cooperation. On one side this approach tries to establish a common interest in national cyber security. In the Dutch Cybersecurity strategy they describe cooperation between public and private entities (National Coordinator for Security and Counterterrorism, 2013, p. 24). In the first version of the strategy they described a process of coordination. This showing there is a development in making preparations to handle the threat in cyberspace. Thereby shifting wording from coordinate to cooperate. On the other side this approach challenges some areas of historical and sectorial responsibility. In many nations there are constitutional responsibilities linked to the different sectors. The energy sector is run by the Department of Energy, the telecom may be run by the Department of Transportation and so on. When responding to large crisis or war this "stow pipe organized" sectors need to cooperate in order to face the intra sectorial threats such as the cyber threat. A model of colocation could provide better information sharing in such a system. Instead of the information following organisational structures to the government, a colocation of assets on operational level may better the information sharing and the building of a common situational awareness. The link down to the different CERT and CSIRT could also benefit from such collaboration. Colocation of the assets does not remove the constitutional responsibility given to the sectors, but it may shorten the time for making the proper counter measures when facing cyberattacks of various kinds.

Preparedness

In the end declaring war is a political decision even in cyberspace. But the politicians need the facts and figures from the various national entities. Even though nations face harassing cyberattacks they may not be on the level of starting a war. These attacks may call for other counter actions than offensive military operations. In order to face the threat in cyberspace there need to be a good public private cooperation. Sabotage by cyberattacks against private owned systems such as energy critical infrastructure or electronic communications critical infrastructure may have severe consequences on a nation. These attacks could inflict death and material damage making it an act of war due to the consequences. Subversion as part of information operations in cyberspace may shift public opinion and hamper political decisions. The cooperation between public and private actors need to be formalised and organised in a way to speed up the response of various types of cyberattacks, and thereby gathering the nation's resources in a joint venture to counter the attacks. Colocation of resources on operational level could be a way of creating a common ground for cooperation.

Bibliography

Clapper, J. R. (2013). US Intelligence Community Worldwide Threat Assessment. US Senate Select Committee on Intelligence.

Clarke, R. (2009). War From cyberspace. National Interest.

Fackler, M. (2014, Dec 28). North Korea Accuses U.S. of Staging Internet Failure, New York Times. Hentet fra http://search.proquest.com/docview/1640597714?accountid=8017

Forsvarets høgskole/Forsvarets stabsskole. (2013). Manual i krigens folkerett. Oslo: Forsvarssjefen.

Franke, U. (2015). War by non-military means.

National Coordinator for Security and Counterterrorism. (2013). National Cyber Security Strategy 2 - From awareness to capability. NCSC Hentet fra https://http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf.

NATO. (2010). Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. Lisbon.

Rid, T. (2011). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.

Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack. Smithsonian Magazine.

Senel, E., Hirsti, K., & Bruland, R. S. (2015). Strømmen tilbake i Istanbul, NRK.no.

The White House Office. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: White House.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

The 49th ESReDA Seminar on:

Innovation through Human Factors in Risk Assessment and Maintenance

October 29-30, 2015, Clos Chapelle-aux-Champs, B-1200, Brussels, Belgium

www.esreda.org

Several research projects and programs on system safety engineering and Quantitative Risk Analysis in the last 40 years offered very strong evidence of the crucial role that human and organizational factors (HOFs) play in major accidents. According to this increasing concern toward the relevance of HOFs in limiting safety performance of complex socio-technical systems, considerable research effort has been spent worldwide in the last couple of decades. Rich literature covering areas from theoretical bases, to accident investigation methods and application to major disasters, to very sophisticated modelling approaches and techniques of HOFs in Quantitative Risk Analysis.

Contributions of the senior researchers involved in the Marie Curie Project InnHF **www.innhf.eu** address for instance the challenges described above. Addressing these challenges is carried on through the formalization of theoretical and applied approaches able to integrate the current and to develop advanced assessment methods. The integrating approaches should comply with the recommendations and requirements expressed by recognized industrial standards and methodologies. Required approaches should be easy to use but and completely integrating human factors and comprehensive system health management approaches.

The aim of the seminar is thus to share within a wider scientific and technical community, to discuss and to compare the results of the proposed approaches, demonstrating how they can be translated into a factual design improvement initiatives for new or existing plants, machinery and critical infrastructures. Seminar's conclusions should be able to provide leverages to achieve competitive and safe performances of complex systems (maximum availability, minimum unscheduled shutdowns of production incident and accident, economic maintenance and increased resilience etc.

Topics include (but are not limited to):

- Risk assessment and management techniques
- Human and organisational factors assessments
- Resilience Modelling and Simulation
- Decision Support Systems (DSS)
- Data collection, expertise & treatment
- Reliability and maintenance
- Prognostic, health monitoring & management
- Maintenance modelling and planning
- Maintenance effectiveness: indicators and measures
- Maintenance & incidents/accidents occurrence
- Maintenance: standards and specifications

Contact:

Michala Demichela micaela.demichela@polito.it
Politecnico di Torino (Italy)

Mohamed Eid mohamed.eid@cea.fr
CEA (France)

Seminar Place:

https://www.uclouvain.be/66833.html

RICS: Research Centre on Resilient Information and Control Systems

The Swedish approach to secure Critical Infrastructures' IT

Introduction

In September 2015 a Swedish research centre on Resilient Information and Control Systems (RICS) was launched to address societal critical functions in several critical infrastructure domains. RICS will be financed by the Swedish Civil Contingencies agency (MSB) over a period of five years totalling 20 MSEK (roughly 2.1 M€). The project leader Professor Simin Nadjm-Tehrani at Linköping University is happy to find this important topic on the agenda for Swedish research and development and presents the goals and motivations for the centre as follows.

Parallel with the growing role of information technology (IT) in business and society we see an alarming wave of computer-based failures leading to breaches of availability and integrity. Industrial control systems (ICS) are among applications with the highest availability and performance requirements. In this project we address the security threats against those ICS on which the critical infrastructures (CI) in society depend, among them power distribution networks, water and heat management systems, and other applications for which we find actively interested stakeholders during five years of the project. One of the main challenges in this sector is the blurring of the borders of the technical system, so far run as an isolated application with proprietary components and protocols, and the business IT, potentially connected with every day communication platforms. Another challenge is the complex nature of these systems which makes understanding of the functional and security related operational modes difficult, even for the most experienced operators. The absence of investments in research and competence building in the area of security-safety in ICS in Sweden has resulted in shortage of competence in terms of young workforce and researchers trained with the right mind set. Our project proposes to strengthen the security of ICS in CI (ICS-CI) using three connected pillars of research:

A) Data generation

Through collaboration with the defence research establishment, FOI, and relevant stakeholders in society we develop methods for creation of realistic datasets based on operational data or meaningful emulations of systems. The generated data using these methods will be a foundation for experimental research through the capability to replay on the current NCS3 test bed at FOI, and encompasses both normal and abnormal (subject to attack or benign failure) modes of operation.

B) Attack modelling and risk analysis

We develop techniques to create reusable models of attacks and malfunctions, and through exposing the simulated or emulated test networks (with extended capability compared to NCS3) characterise the vulnerabilities and concretise the risks to a CI, including the ensuing safety risks.

C) Real-time detection

We develop methods and tools to perform real-time monitoring of systems of comparable complexity to today's ICS-CI, based on adaptations of the concept of anomaly detection. This will include identifying the specific characteristics of the domains under study so that false positive rates are at acceptable levels, and mapping the verdict of the monitoring system to meaningful messages understandable for the operators, thereby enhancing their reaction and mitigation capability.

The first ingredient (A) above is in itself a valuable contribution to international research, provided that open data sets based on the collected or generated data can be created (this

Simin Nadjm-Tehrani

Prof. Nadjm-Tehrani is the coordinator of RICS, and leads the Real-time Systems Laboratory at Dept. of Computer and Information Science at Linköping University, Sweden. She has recently led a national project as a pre-study in the area of Internet of Things and security within the area of critical infrastructures, and for the past four years acted as a member of the scientific advisory board at the Swedish Civil Contingencies Agency.

e-mail: simin.nadjm-tehrani@liu.se

will obviously be subject to clearance by stakeholders). We plan to participate in exercises run by FOI together with a range of relevant stakeholders. Among the main stakeholders we expect the Swedish national grid (Svenska Kraftnät). The data thus collected will be used as an input when designing the platform that can be used for repeatable replay of (insensitive, cleaned) data streams. This improves the ability to develop relevant tools that can be adopted by industry, and increases the understanding about these systems among stakeholders. The data emulation layer thus created as an interface to the underlying test bed will be of a generic nature, so the applicability of the method in new sectors within ICS-CI is also a major contribution.

The second ingredient (B) above is a means to strengthening the societal functions in terms of preventative measures. Today's CI operators have several functions outsourced to external cloud services and their understanding of the risks and potential attack vectors is dependent on proactive analysis built within the operational environments. Given adequate inputs from stakeholders, from (A) above, RICS demonstrations of the methods for identifying weaknesses and vulnerabilities will be built on case studies recognisable by the stakeholders. Extending attack models in RICS will thereby include dealing with issues of scale and complexity that arises in networks with heterogeneous (and cloud-provided) services. Efficiency of the methods will be based on reusability, and their relevance based on combined safety and security analysis.

The third ingredient (C) brings an improvement on today's ability to react to and deal with adverse events by more precise and timely detection of these in the context of ICS-CI. A main part of detecting adverse events in real-time consists of identifying the features of the systems to be monitored. To monitor the vital IT processes in a SCADA environment, irrespective of which borders the data transgresses and where certain services are delivered, is a challenge in today's networked environments and RICS will address it as follows. The characterisation of the network structure, vulnerabilities, and potential attack vectors in part (B) above will create the relevant inputs to selection of features to be monitored. The created data sets in collaboration with our stakeholders in part (A) above, form a base for validation of our real-time anomaly detection algorithms in realistic scenarios. The attack models obtained based on work in (B) above will be used to test and verify the real-time adverse event detection in part (C) and used in demonstrative case studies in presentations to stakeholders.

RICS will operate as a national research centre with contributions from three strong research teams. The two teams that collaborate with the Real-time Systems Laboratory at Dept. of Computer and Information Science at Linköping University are the groups led by Dr. Magnus Almgren at Dept. of Computer Science and Engineering at Chalmers, and Professor Mathias Ekstedt at Industrial Information and Control Systems at the Royal Institute of Technology (KTH).

LINKÖPING UNIVERSITY

CHALMERS UNIVERSITY OF TECHNOLOGY

KTH VETENSKAP OCH KONST

Collaborating partner:

Swedish Defence Research Establishment (FOI)

Active Stakeholder: Swedish National Grid

Funded by: Swedish Civil Contingencies agency (MSB)

MSB Myndigheten för samhällsskydd och beredskap

Watch this space: www.rics.se

Elevating identity and access management to the digital era

Identity and access management is no exception to the digitisation of everything. The use of biometric features, behavioral aspects and physiological technologies is just around the corner, bringing new authentication and authorisation methods to the market.
Another wave of technology disruption or an actual business need?

Era of digitalisation and disruptive technology

The unprecedented explosion of technology disruption and innovation, the velocity of change and the tremendous impact on businesses are ultimately forcing a large number of industries to increase the pace at which they do business and transform technology.

At the same time, the need for increased data and information protection cannot be overstated.

> "The new digital ecosystem of connected entities, people and data requires an integral identity and access management, beyond the purpose of regulatory and security compliance."

The recent Ashley Madison hack (stolen personal information from a website dedicated to matching up people who want to engage in extramarital affairs) is prime evidence that the management of identities and accesses goes beyond the purpose of regulatory and security compliance.

It impacts the society as a whole and plays an important role in today's cyber ecosystem.

Cyber threats

Identity and access management must be re-aligned with today's digital and cyber ecosystem.

With the digitisation of everything, the classical perimeter of an organisation is disappearing, leading to an increased and complex exposure to potential cyber threats.

The range of the perimeter now includes the authentication and authorisation to and from the corporate organisation or the multiple types of users (e.g., employees, customers, business partners, third parties and suppliers) through multiple channels.

Customer-centric and resilient to cyber identity fraud

Traditionally, organisations have managed their identities and accesses primarily by focusing on the internal employees accessing corporate-wide internal applications. For many organisations, this remains an actual challenge, which requires continuous funding and available skills to maintain a sustainable state.

It is therefore not surprising that identity and access management continues to be a key priority on the agenda of information security.[10]

With the new reality of a digital and cyber ecosystem, organisations have no other choice but to extend the scope of identity and access management with the additional two aspects

1) customer-centric (especially for the external types of users who are accessing their trusted organisations) and

2) resilient to cyber identity fraud.

Maurice Bollag

Maurice works as a Senior Manager at EY (former Ernst & Young AG) in EMEIA Financial Services Advisory, IT Risk and Assurance & IT Advisory. He is a FINTECH advisor specialised in Cyber, IT and Information Security, IT Risk and IT Service Management.

e-mail:
maurice.bollag@ch.ey.com

[10] EY Global Information Security Survey 2014 "Get ahead of cybercrime", October 2014.

1. Customer-centric

Customer behaviour is changing in many ways. The following two examples highlight the reasons why a customer-centric identity and access management is key to building and retaining customer trust in the organisation they are working with:

a) End user acceptance and usability of usernames and passwords

In the digital ecosystem, customers have to manage multiple intercommnected identities.

This makes it very challenging to use the traditional management of usernames and passwords.

Customers are getting tired of and increasingly frustrated with the tedious and inconvenient processes involved in managing those identities.
The Millennial Generation (also known as Gen Y) might have been used to it, but the subsequent Generation Z will certainly not accept it.

Can we image how Gen Z would feel about accepting the use of indefinite usernames and passwords to enable their access to a web service? Will Gen Z accept having to prove who they are instead of being recognised automatically (authentication based on who they are, not what they remember)?

b) Increased customer awareness of security reliability

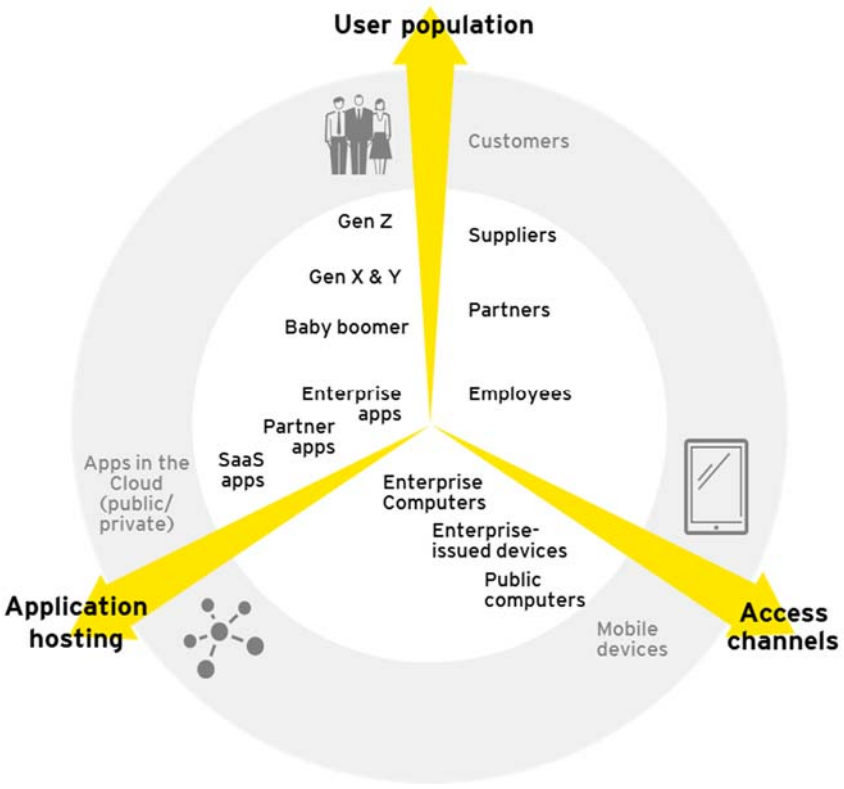
Society has become more aware of the risks related to information security. Customers are feeling less secure about the reliability of usernames and passwords to protect their personal data.

Even good habits and best practices of password management (e.g., different and strong passwords for each used service) are no longer secure and effective enough to protect from identity fraud and theft. Analysis of root cause for identity fraud and theft incidents often includes a flawed authentication method.

Therefore, providing customer-centric identity and access management will become a key factor in ensuring customer satisfaction and trust.

2. Resilient to cyber identity fraud

Indeed, breaches have been occurring for a long time, but their impacts have never been so severe. Incidents which are directly or indirectly related to weak management of identities and accesses are becoming a persistent business operational risk (e.g., damage to reputation, intellectual property, ability to serve customers, financial impact).



Regulations around the world are imposing rules, enforcing mandatory public disclosure of any breach (and even attempted breaches) that compromised personal or financial information and notification of affected consumers within a pre-defined timeline. Non-compliance will be subject to increased fines.

The recent Ashley Madison hack could not have been a better wake-up call. It impacts the society and can have consequences far worse than any financial impact.

Customers will no longer accept and trust companies who cannot demonstrate their ability to protect personal data and privacy.

Innovative solutions for authentication and authorisation methods are emerging to disrupt current practice, but their success will depend on whether they arrive on the market with a pre-installed system for protecting data privacy. (see figure next page Identity and Access Management)

Technology trends

A possible way to address this challenge is to deploy innovative authentication and authorisation methods.

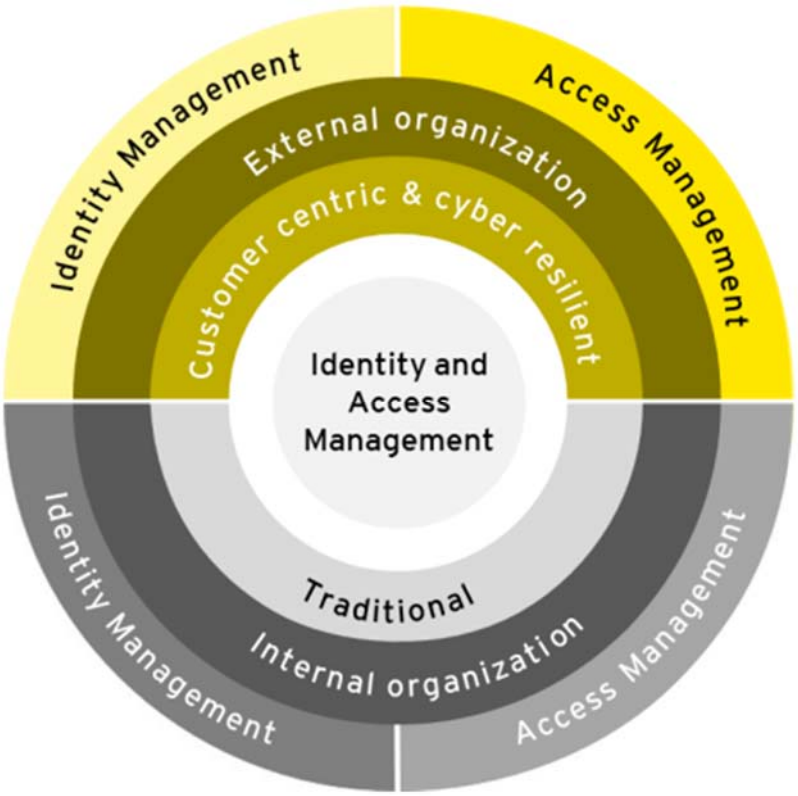
Research has been conducted to predict the key developments and roadmap of current and future identity and access management technologies.

At the end of the day, consumer perception of confidence and trust will play a key role in the success of each technology.

The following list is an overview of the new methods:

Context-based

Authentication and authorisation are driven by a risk context, taking into account criteria such as geographical location, physical device, time and duration of a user's request to access a service. The measures of authentication and level of authorisation dynamically change according to the actual contextual information and risk level.



Biometrics

Authentication and authorisation are based on digitalised biometrics from a human being such as fingerprint, facial or voice recognition – methods that have actually been in place for many years. The latest biometric frequency, vein, palm, iris, DNA, handwriting and even tattoos. technologies include other physical human elements such as heartbeat.

Behavioral

Authentication and authorisation are based on personalised gestures such as hand-eye coordination, keystroke dynamics or cursor movements. Algorithms and patterns of interaction might be combined to set the behavioural criteria.

Which technology will ultimately succeed is difficult to predict. A combination of different technologies might become the future best practice. The new technologies will have to prove their advantages before passwords become obsolete in the near future and assert themselves against emerging and future trends in password security (Password 2.0). However, what certainly can be predicted is that the cultural, geographical and industrial differences are going to play a key role. Offering choices of authentication methods for different locations and user populations might lead to a greater appeal and acceptance.

Cultural and geographical tendency

A global organisation will have to consider the cultural differences in the region they operate in and its online customer base. We have seen countries which have emerged and directly embraced new technologies. Others, however, have adapted their technology, but face challenges due to a lack of user acceptance.

Industry tendency

The question is "how" rather than "which" specific industry will be impacted. The following examples from three industries highlight the differences relating to the "how": the banking industry, which has been dealing with identity and access management for a while, the automobile industry and the smart home industry. The last two are becoming increasingly relevant to our private lives.

Banking

The strongly regulated financial industry has improved its capabilities of managing its identities and accesses over the last couple of years. Nonetheless, a digital banking business model requires massive adaption to its identity and access management methods to support upcoming digital banking services. Mobile and peer-to-peer payments, crowd funding as well as trading and lending functions need to be customer-centric and resilient to cyber identity fraud.

Automobile

Connected cars have to offer simple and secured authentication and authorisation methods. For example, access to the car could be provided based on biometric data such as fingerprints. Car owners might need to think about authentication and authorisation in the future, but car producers definitely must start to integrate secure and easy to use security functions.

The question is "how" rather than "which" specific industry will be impacted.

Smart home

Last but not least, society will have to start thinking about authentication and authorisation of their digitised home rooms, devices and furniture.

Three actions to be taken today

The industries and organisations need to start extending the scope of their current identity and access management model and elevating it to the digital era by:

- Assessing the current state and evaluating its current digital transformation journey to include adapted identity and access management methods.

- Assessing their ability to detect identity fraud and threats and readiness to respond to potential incidents.
- Reviewing the current technology, operating model and governance to effectively and efficiently include integral identity and access management beyond the purpose of regulatory and security compliance.

Conclusion

The new authentication and authorisation technologies have tremendous potential.

It is a business and a customer need. A business need for a robust resilience against identity fraud and cyber threats.

A customer need for a more convenient and trusted method of authentication and authorisation.

With the speed at which the digitalisation process is taking place, it will not be long until we find out which emerging technology will assert itself.

However, the challenge remains to introduce these new technologies with a watertight protection of data privacy.

Asset Management and Critical Infrastructures: Differences and synergies

Micheline W.A. Hounjet,

Micheline is a creative and strong connector between various fields of delta technology. With her background as an engineering geologist, she is not only active in the cross-over between technical disciplines, but also focuses on the link between technology and people. She is keen to find innovative solutions to help people manage flood risks, increase stakeholder participation for urban development and gain insight in integral critical infrastructure impacts in Delta regions. Serious gaming, information tools and visualisation techniques for crisis management are her main interests.

e-mail: micheline.hounjet@deltares.nl

J.M. IJmker - van Gent

Janneke is a communicative team player who translates her work into impacts for the natural system and stakeholders. As a physical geographer she has an eye for the "will" of the natural system itself, which results in more effective measures. To stakeholders, she expresses the results of her work into recognisable units, for example the task for dike enforcement in The Netherlands in euros and the uncertainty in hydraulic heads in 2050 in a bandwidth of costs. Her main interest is to accommodate decision-making with clear, unambiguous, fit-for-purpose information. Combined with her organisational skills, this has led to her present role in implementation of asset management in civil engineering.

e-mail: janneke.ijmker@deltares.nl

At Deltares there is a team of researchers on Asset Management and a team of researchers on Critical Infrastructures. Both focus on infrastructure networks, however their approaches seem to be different. What do these teams have in common and what are the differences between both research subjects? Janneke IJmker van Gent from the Asset Management team and Micheline Hounjet from the Critical Infrastructures team met to discuss these points (see figure 1).

Propositions

For this discussion several propositions and questions were raised:

- In many research calls, the Critical Infrastructures topic is linked to natural and man-made hazards. Has the Asset Management topic the same approach to hazards?
- Asset Management has its stakeholders at the maintenance and risk management departments of asset owners. Critical Infrastructures has its stakeholders at the risk management and crisis management departments of these asset owners. Is there overlap?
- For Critical Infrastructures interdependencies are very important. Does Asset Management take interdependencies into account?
- What types of data do both groups use?
- How do the different teams communicate with the end-product users and their stakeholders?

Hazards

Critical infrastructures research usually takes severe disruptions into account. These disruptions can be caused due to natural hazards or human errors. Sometimes Critical infrastructures are mentioned in combination with climate change, but usually heavy rainfall, storm surges, etc. are meant. For Asset Management long-term maintenance planning is important and climate change is certainly a topic that is mentioned. For instance in the Netherlands most assets are aging and efficient asset management has high priority. But it is not only the aging effects that need to be considered. Climate change effects are added threats for these assets.

In general Critical Infrastructures handles "what happens after a disruption, what are the impacts" while Asset Management handles "how to optimise performance and minimise failure and nuisance in the future". For each network the focus is a bit different: A dike system built to retain water is designed to perform during rare, extreme occasions, but some other networks are built for optimal performance in daily life situations under less extreme conditions.

Stakeholders

The Critical Infrastructures Team is mostly in contact with crisis managers from network owners, industries, governmental bodies and crisis organisations. It is quite easy to talk to crisis managers about extreme events. For example, when the team talked to risk managers from the same organisations, discussion quickly turned to chances of occurrence. However, it was difficult to get them interested in events that have an occurrence of less than 1 every 100 years.

The Asset Management Team approaches risk managers, network owners and governmental bodies. Risk assessments are a substantial part of the work related to Asset Management. These risk managers are involved in decision-making when daily performance is concerned. Their approach is much more detailed as they monitor performance constantly and they are trained to solve issues and outages as quickly as possible.

Deltares recently set up a new national research group with different Asset Management stakeholders. It is called ROBAMCI. The goal of this research initiative is to initiate projects where industry and research partners team-up. Until now, three projects on water management related assets have been launched.

These projects help Deltares to understand the needs of different organisation levels: Strategic, Operational and Tactical. They need different levels of detail and deal with different time intervals for disruptions and consequently handle decision making for future measures differently. It is essential that the outcome of this research exactly match to the needs of the end-users.

Figure 2: Different organisational levels within asset owners

(Inter)dependencies

Currently, the most important research questions for Critical Infrastructures at Deltares evolve around cascading effects between networks and the simulation and visualisation of them. The challenge is to look at a region or a city as a system of systems.

In contrast, the focus of Asset Management is on single networks and long-term adaptation strategies for climate change effects.

Both teams are now exploring whether knowledge on interdependdencies could be beneficial for Asset Management and how detailed Asset Management knowledge could be used for cascading effects simulations and impact models.

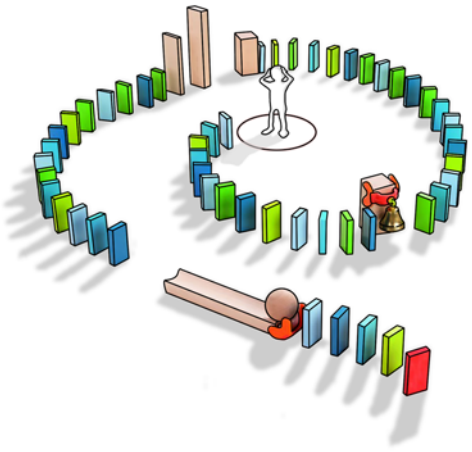


Figure 3: Stakeholder participation workshop for Critical Infrastructures

Data

As mentioned above, for Asset Management detailed risk management is necessary and sometimes available as well. But still there is a need to include knowledge and experiences from the different stakeholders as well (see table 1). It is therefore vital that these different parties work together.

	Data	Experience	Knowledge	
Government				
Industry				
Knowledge Institutes				

Table 1: Overview of parties with data, knowledge and experience for Asset Management.

For Critical Infrastructures it is difficult to receive detailed network data from stakeholders as it is classified. Deltares developed a method that is based on the use of open data combined with expert knowledge and experiences. The idea is that when different network owners discuss consequences with each other and share the knowledge of their own network, there is enough knowledge to evaluate cascading effects after a disruption. This method is called CIrcle and uses an interactive

Figure 1: Janneke IJmker-van Gent (l) of the Asset Management Team and Micheline Hounjet (r)of the Critical Infrastructures Team discuss research and overlap of these topics.

tool for data-mining during the discussion and visualisation techniques to simulate the results of this discussion.

Communication

For Asset management it is vital to communicate research results exactly on the right level of their end-users. ROBAMCI also pays attention to this aspect in their case studies and research projects. The third year of the program is especially designed for communication of results.
For Critical Infrastructures and cascading effects it was difficult to get stakeholders thinking about interdependencies. It seemed too complicated and many assumed everything would just fail at once. Deltares noticed that when the issues were visualised in a simple and understandable way, stakeholders were eager to think about it and

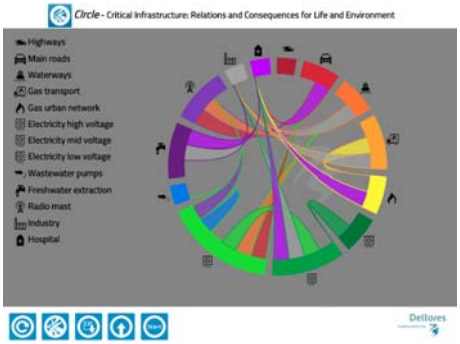


Figure 3: CIrcle tool.

share their knowledge. The level of detail that can be reached with open data can be enough to raise awareness and discuss these issues together. With the discussion results and sometimes more detailed data that is donated after a workshop session, cascading effects evaluations are carried out.
One of the workshops that were organised was for a Water Board. For the celebration of a flood that occurred in 1916 within their area, they wanted to have a visualisation that would show the difference in effects when the same flood would occur in 2016, as civilisation is now more dependent on networks as it was 100 years ago. This simulation will be used by the Water Board to raise awareness on cascading effects.

Example research projects

The research goal for Critical infrastructures focusses on cascading effects at the moment and interactive ways to visualise them and to discuss protective measures. The city of Jakarta is used as a case study. Open data was gathered and a workshop was organised with CIrcle to collect more local information.
For this case study Deltares is now developing a 3D, interactive environment in which cascading effects are visible and will change for different flood scenarios or when for instance the level of a vulnerable object is modified. The accuracy level of this project is at the moment lower than it is required for an Asset management projects.

For the ROBAMCI project in the Beemster polder, performance of important assets of the local water board, such as roads, dikes and pumps, has to be optimised for future situations, under climate change effects, increasing need for transparency and reducing funds. To identify every asset's contribution to risk reduction, a failure mode and effect analysis (FMEA) was carried out. The study is used to identify to what function it is best spending one Euro, so where one Euro creates the largest risk reduction. The method was shown for the Beemster polder, but to achieve reliable results, highly detailed data is required.

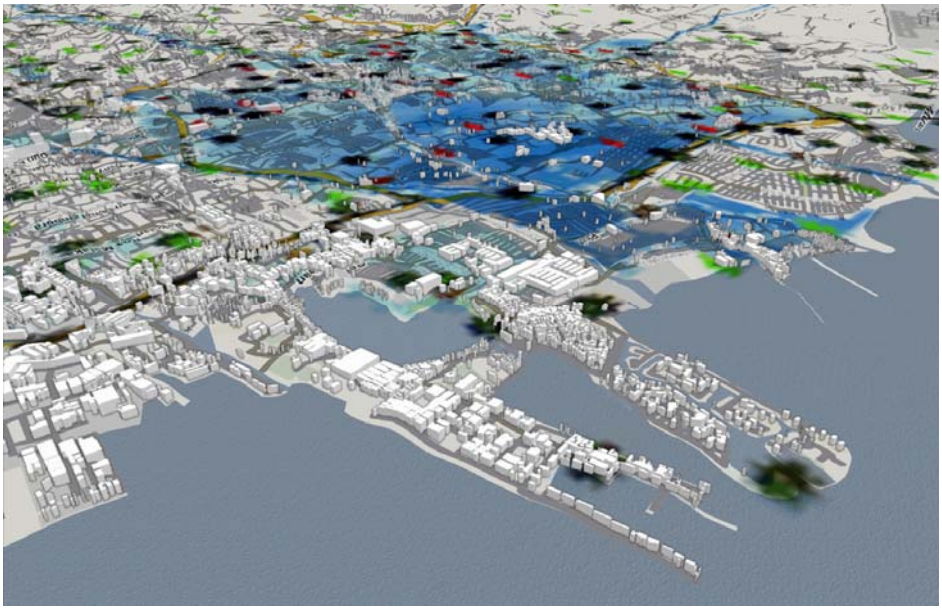


Figure 4: 3D, interactive environment for Jakarta

Furthermore, it should not be forgotten that decisions are often based on subjective arguments rather than objective ones, such as acceptability of risk in different sectors.

Both teams are now cooperating to realise a research project within ROBAMCI that benefits both research lines.

This page is intentionally left blank.

Teaching Homeland Security

Teaching Homeland Security is a hard challenge and a great opportunity to develop innovative curricula. The comparison between two training courses, in Italy and USA, shows a variegated scenario reflecting different HLS approaches.

Although a universal consensus does not exist for the definition of both domestic and international Homeland Security (HLS), it is still feasible to reach an agreement on its key features; one of the most established definitions, for instance, is that provided by the National Research Council (U.S.A.): "Any area of inquiry whose improved understanding could make U.S. (and International) people safer from extreme, unanticipated threats" [1].

According to the Quadrennial Homeland Security Review Report of the DHS, Homeland Security can be defined as: "intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defence, emergency response, law enforcement, customs, border patrol, and immigration" [7].

The key word in this particular definition is evolving. Hence the scope of HLS has graduated from National Security to Emergency Personnel to Critical Infrastructure Protection, to Private Security (both cyber and physical aspects) and subsequently setting a tone of blind acceptance for nearly all threats to be categorised under the wide umbrella of HLS. Another element that emerges from the above definitions is that the cornerstone is the safety of people (and goods) in spite of the source of the threats. In other words, actual HLS is adopting, especially after hurricane Katrina, an All Hazards approach.

The lack of a universally adopted definition of HLS is reflected by the operative choices of the different National and International governments and Institutions.

For example, although the United States continues to focus on a wholesale approach to domestic security and border protection issues, European countries have largely preferred to work within their existing institutional architectures to combat terrorism and respond to other security challenges and disasters, both natural and man-made [3].

Such a diversity has indubitably a deep echo in the way Homeland Security is taught across different countries and institutions; at least in terms of intended audience, contents, occupation of trainees, etc.

To date, quite a bit of research has been conducted on how to teach Homeland Security. In [6] the need for the coexistence of HLS and Emergency Management (EM) in the same program is stressed. In [16] a comparison of the US and EU approaches to homeland security teaching is carried out, pointing out that, while US has continued to focus on centralising and unifying HLS efforts, EU governments tend to maintain the existing institutional settings, and (unlike the US) do not have a dedicated Department of HLS in many European countries; thus, the responsibilities are often delegated to several ministries, law enforcement and intelligence agencies.

In Europe, a myriad of threats have led to the dilution of a singular definition (of particular note is the prioritisation of elements compared to the U.S.). For example, while 'terrorism' is a top priority for the United States, the European Union might be more focused on immigration and Critical Infrastructure Protection (CIP); these differing approaches obviously impact a HLS curriculum.

This work aims at assigning a core curriculum for a HLS program, following three main strategies: comparative analysis, prioritisation of threats and an understanding of the ethical playground one is attempting to navigate.

Further, we compare the experience acquired in managing HLS training program by the University Campus Bio-Medico of Rome, Italy (UCBM, www.MasterHomelandSecurity.eu) and the Naval Postgraduate School, USA (NPS, www.nps.edu/). These institutions have, through independent strategic approaches, constructed working HLS graduate programs. Ultimately, we aim to provide a loose framework (predicated upon the "lessons learned" from our two case studies) for building a strong HLS program.

Roberto Setola

Roberto Setola is professor at University Bio-Medico, Rome and head COSERITY Lab (Complex Systems & Security Lab) and director of the Post Graduate program in Homeland Security.
Email: r.setola@unicampus.it

Maria Carla De Maggio

She belongs to the Complex Systems and Security Laboratory of the University Campus Bio-Medico of Rome since 2009. She holds a Master Degree in Biomedical Engineering (2007) and a PGP in Homeland Security (2011).
Email: m.demaggio@unicampus.it

Teaching Homeland Security: the recipe for success

Teaching Homeland Security is, simultaneously, a hard challenge and a great opportunity to develop innovative curricula capable of quickly responding to the needs of a specific country [8]. In fact, unlike other disciplines (e.g. Medicine, Accounting), no standard baseline for academia exists for the Homeland Security arena; subsequently, "Homeland Security Experts" graduate into the field with no oversight or guarantee that the appropriate knowledge base was explored.

No matter how one interprets the skills of a Homeland Security graduate, one variable is certain: there is no recipe to follow, and thus no accurate prediction in the outcome of a HLS graduate. Indeed, the academic context of homeland security could be stretched to include almost every discipline and topic area imaginable (e.g. public health, military history, international diplomacy, the psychological-sociological examinations of other cultures, comparative government systems, etc.), with "homeland security" serving more as a target for the application of such studies, rather than as a descriptor of the studies themselves [1].

Consequently, constructing a boundary-spanning interdisciplinary educational strategy remains a utopia, and has arguably become the victim of benign neglect [2].

While no two programs are identical, every HLS program contains particular "planks" which ensure that the most vulnerable "gaps" are covered; at least in theory. When starting to analyse particular HLS building blocks, one quickly deduces that the area of focus is not molded by the needs of the international community per se; rather, it is shaped through personal opinion and local or domestic trends. This desire to stay within the "box" of HLS, albeit a large and ever-expanding box, can potentially limit the student's exposure to areas of interest. According to the Federal Emergency Management Association (FEMA), there are currently 25 Universities offering Graduate level Homeland Security programs within the United States (2013) [10]. However, it is important to keep in mind that this number is skewed by the language; there are many other programs operating in the United States that could be categorised under the HLS umbrella but do not contain the specific label "Homeland Security" in their respective course. Further, when one applies the "Homeland Security Graduate Degree" search parameters into the NPS Center for Defense and Security website, the results yield seventy-nine Universities currently offering Homeland Security Graduate programs (2013) [11]. This is a classic example of why it has become so difficult to understand the exact role of homeland security experts. The inability to obtain a consensus (even within the confines of DHS- of which both FEMA and the NPS are members) has propelled many within the community to incessantly expand their HLS definition; hence, the Homeland Security "bubble" becomes ever more inflated and complex.

"Neither the U.S. Department of Homeland Security, the Federal Emergency Management Agency (DHS and FEMA), nor the several professional associations have agreed upon and articulated a common benchmark standard for collegiate education in these related fields" [3]. In addition to the differing external (between universities and agencies) Homeland Security program paradigms, many of the classes internally (within a university or institution) continue to be controversial. So, even within their respective institutions, it remains a point of contention amongst instructors on which classes to expose their students to in order gain an appropriate scope of relevant topics. The discontent between colleagues is also fuelled by physical location: even though globalisation continues to interconnect every facet of our lives, physical locality can still steer the curriculum.

And this physical location is not limited to mere approaches; along with a certain environment comes a specific type of lexicon.

ELEMENTS OF A HLS PROGRAM – USA	***ELEMENTS OF A HLS PROGRAM – ITALY***
Protection of critical infrastructure	Protection of critical information
Cyber security (crime and political attacks)	Cyber security
Border security and global threats	Risk analysis
Intelligence and strategic analysis	Strategy and intelligence
Disaster management and all hazard approach	Security legislation and standards
Mass transportation safety and security (ground, air, and maritime transportation)	Crisis management and disaster recovery
Interagency cooperation (including information sharing and safeguarding)	Security management
Political violence and terrorism	System engineering
Technology applied to security	Technology applied to security
Ethical dilemmas and civil rights	Ethics and privacy

All of these contrasted approaches inherently drive respective syllabi. However, it should be noted that the United States and Europe, of late, are applying a much wider purview in their HLS teachings (as deduced from the inclusion of globalisation and diplomacy courses). Several areas are generally addressed in an upper-level Homeland Security program for the United States. Such areas are summarised in the Table.

Comparative analysis

The NPS Master of Arts in Homeland Security program and the UCBM post-graduated level Homeland Security program were chosen for comparative analysis because they present differing styles in their respective teaching approach to HLS. The biggest difference is their intended audience.

The NPS program is geared towards personnel already vested in U.S. government service; this prerequisite for government experience provides a unique classroom atmosphere and is critical to highlight because, as with any upper-level education, the professor serves more as a facilitator than a direct educationalist. Subsequently, it behoves the program to have an experienced cadre of students who, in addition to analysing the static curriculum, provide personal experience and

opinions. During the last three cohorts of the NPS HLS program, ninety students have graduated with an average age of 45 and a career level of mid to senior; thus, they encompassed the capability to implement change within their respective agencies [9].

According to the Director of Academic Programs at the NPS Center for Homeland Defense and Security: "The students are oriented more to practice than to theory, to applied knowledge rather than analysis…Our approach is to assume the students are participants in the course rather than an audience for what we have to deliver" [5]. However, limiting the applicant pool can inadvertently impact a program.

Uninfluenced by their respective government agency, a "fresh" and open-minded student may prove just as valuable as their professionally developed counterpart. In this respect, the University Campus Bio-Medico has the ability to produce students that are directly shaped through their studies, not their potential biases commonplace amongst differing government agencies. The subsequent graphs (Figures 1 & 2) illustrate the relative experience of the UCBM student cadre for the past three sessions editions.

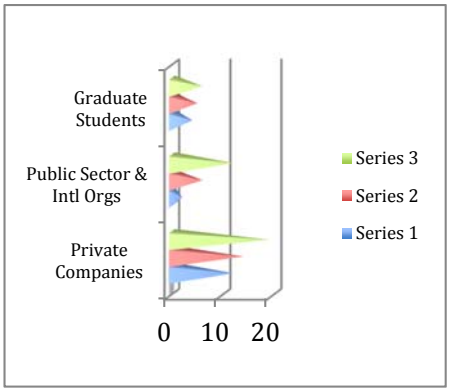


Figure 1 UCBM breakdown of student history for the past three editions.

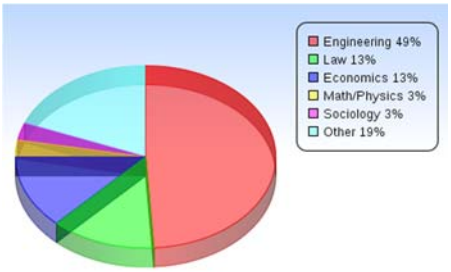


Figure 2 More background information regarding UCBM students for the past three editions.

Notice the high level of private company participants; although these companies irrefutably impact the HS community, there interests are most likely specified. Subsequently, the lessons learned in the program may not be applied on a global level. Although this is speculative, it is worth noting due to the known global impact of the NPS graduates. However, it is also worth mentioning that the lack of a target audience affords the student an ability to focus on their respective area of expertise. Additionally, the majority of participants in the UCBM HS program are 38-45 years old (see Figure 3); this statistic is extremely relevant because it highlights the fact that most participants in upper level programs are already entrenched within their career, thus we can assume that their respective opinions have already been influenced and subsequently formed.

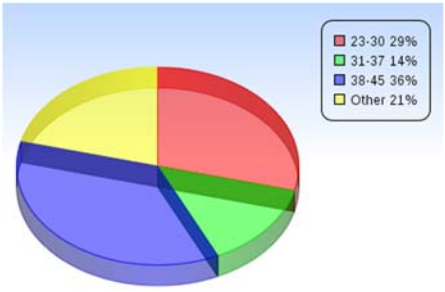


Figure 3 Age level of UCBM students for the past three editions.

Along with age, experience and background, the amount of time invested into each program is a critical element to examine. The NPS program is 18 months in duration while the UCBM is 12 months long (thus, the overall number of in-class hours invested by each student annually is more for those participating in the UCBM program). In this framework the NPS program incorporates also web-based coursework is a fundamental difference. While the online forum provides an extra level of interaction with the students, it is arguably an insufficient substitute for in-class instruction.

Yet another differing element is the inclusion of a thesis or capstone project. NPS requires a standard thesis project, while UCBM requires their students to complete an internship (minimum 2 months) within one of their sponsoring companies or a pre-approved public agency.

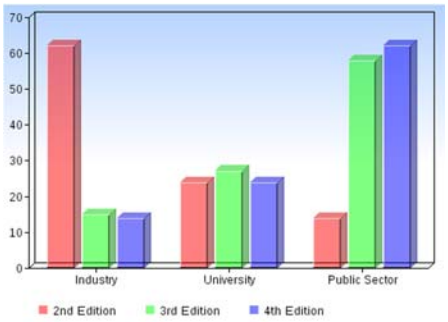


Figure 4 Background of the faculty for the past three editions for UCBM.

Because the NPS students are already entrenched within their government careers, students are required to construct a thesis within the confines of their relative agency. Thus, they develop their HLS skills within the very domain they impact; this practical approach behoves the U.S. government as much as the student. However, this also limits the student's ability to address issues outside of their immediate realm.

The graph of Figure 4 illustrates the teacher origins for UCBM; in the last 3 editions there was an evident inversion of tendency from a situation where the majority of teachers were from the Industry sector, to a situation where most of the instructors stemmed from the Public sector (including international organisations). The UCBM cadre of professors provides the students with a unique blend of Industry, Academia and Homeland Security experts.

Like the UCBM approach, the NPS program also incorporates a multidisciplinary cadre of professors whose wide ranging background provide the students with differing perspectives and subsequent teaching techniques.

In regards to outside the classroom experiences, both universities understand the value of gathering data first-hand and offer opportunities as such. For example, the UCBM program encompasses several field trips to some of the most relevant military, public and private homeland security agencies. These included: the Italian flight agency control room, the Italian civil protection control room, the virtual shooting polygon at Selex Elsag Spa, a power plant control room in Civitavecchia (near Rome) and the crisis unit of the Italian foreign office (U.S. State Department equivalent). When queried about field trips at NPS, Heather Issvoran (the Director of Strategic Communications at NPS) stated "as opportunities arise, we take advantage of them" [9].

Lessons Learned

How does one prioritise threats? Is it truly rational to place emphasis on one disaster over another? Should we focus more on the domestic or international front? Should an HLS program be tailored to counter a specific threat (i.e. cyber-security, industrial, private, transportation, emergency planning, natural disasters, etc.) or should it be a more all-encompassing approach? All of these questions present realistic challenges in molding an appropriate curriculum. And, once again, we believe that oversight is the answer. The real challenge lies in balancing probability, vulnerability and, most importantly, consequence. A curriculum focused on these elements, with the heaviest emphasis on consequence, is a sound recipe for success. This is based upon the mind-set of "when, not if". Operating under this umbrella of brutal realism, we can better prepare ourselves. Consider this: if the majority of resources are pumped into probability and vulnerability protection, then we can assume that the smallest amount of resources are allocated towards consequences. Further, is it possible to plan for EVERY threat? Ultimately, a new threat of a different variation will appear: this is fact. Therefore, it behooves the security mindset to accept a realistic outlook and form curriculum accordingly (i.e. providing a consequence-heavy focused syllabus).

Beyond student surveys, oversight of a program is necessary. With the Homeland Security field being such a fluid concept, wouldn't it make sense to overhaul program curriculum on an annual basis? For example, the Department of Defense promoted yhe presence of a Board of Visitors (BoV), comprised of Congressional members and civilians, into their program which role is to visit, examine and, ultimately, provide their findings to the Secretary of Defense and Congress. Although the power of the BoV is limited to an advisory capacity, the input provided has proven to be a valuable tool for the school. "In practicality, it has had impact on curriculum in two ways: 1) The Congressional members see specific needs or changes that can be made by legislation, and get those done and, 2) the knowledge and expertise of the civilians who have served (many lawyers, professors, former ambassadors) allow them to make practical suggestions that can be implemented right here" [4].

Understanding the ethical playground is another element which must be considered. As former U.S. Attorney General John Ashcroft wisely commented following September 11, 2001: "We always have to be careful that the rights which America stands for are protected, but we also have to understand that in order for those rights to be enjoyed, they have to be protected" [13].

At what point are civil liberties willingly sacrificed under the authority of 'homeland security'? In this regard, it is critical that a HLS program incorporate ethics and law into their respective syllabi. Nowhere is the moral playground murkier than in the field of technology. Simultaneously, the HLS field has been tasked with extending their technological capabilities and developing guidelines for their use. For example, "if precision weaponry is assumed to be inherently ethical, it may grant policymakers and strategists the chance to conflate the description of tactics with the prescription of normative judgments" [12]. Constrained only by the human element, technology itself neither answers nor ignores ethical questions; it is only the particular use of these technologies by practitioners that will either distract us from, or make us well attuned to, particular ethical questions concerning the rights and safety of citizenry [12].

Acknowledgement

Authors would to thank Gregory Fink for his support and to provide valuable information about US and NPS initiatives.

References

[1] Frameworks for Higher Education in Homeland Security Committee on Educational Paradigms for Homeland Security, National Research Council ISBN: 0-309-54511-0, 78 pages, 6x9, (2005)

[2] Journal of Homeland Security and Emergency Management; Volume 6, Issue 1 2009; Article 34, Educational Challenges in Homeland Security and Emergency Management. Robert McCreight; George Washington University, Copyright 2009, The Berkeley Electronic Press

[3] European Approaches to Homeland Security and Counterterrorism. Congressional Research Service: Report For Congress; July 24, 2006, Kristin Archick, Coordinator; Carl Ek, Paul Gallis, Francis T. Miko, and Steven Woehrel Foreign Affairs, Defense, and Trade Division

[4] Rials, Lee A. (lee.a.rials.civ@mail.mil). (2012, April 16). Interview results. Email to authors.

[5] Bellavita, Christopher; Gordon, Ellen M. "Homeland Security Affairs"; Volume II, Issue I, Article I (2006); Changing Homeland Security: Teaching the Core.

[6] Kiltz, L. The benefits and challenges of integrating emergency management and homeland security into a new program. Journal of Homeland Security Education, 1(2), 6-28. (2012). Retrieved from www.journalhse.org/vli2-kiltz.html

[7] U.S. Department of Homeland Security. (February, 2010). Quadrennial homeland security review: A strategic framework for a secure homeland. Retrieved from http://www.dhs.gov

[8] Pelfrey, W., Sr. & Pelfry, W., Jr. (2009). Curriculum evaluation and revision in a nascent field: The utility of the retrospective pretest-posttest model in a homeland security program of study. Evaluation Review, 33(1), 54-82.

[9] Issvoran, Heather. (hissvora@nps.edu) (2013, February 6). Interview results. Email to authors.

[10] FEMA homepage, retrieved from www.fema.gov

[11] NPS Center for Defense and Security website; retrieved from www.chds.us

[12] Another Question Concerning Technology: The Ethical Implications of Homeland Defence and Security Technologies John Jacob Kaag

[13] Cited in CSIS Briefing, "Strengthening Law Enforcement Capabilities to Combat Terrorism", October 2003.

[14] M. C. De Maggio, M. Mastrapasqua and R. Setola, "The professional figure of the Security Liaison Officer in the Council Directive 2008/114/EC", 10th International Conference on Critical Information Infrastructures Security (CRITIS 2015), Berlin, 2015

Links

ECN home page	www.ciprnet.eu
ECN registration page	www.ciip-newsletter.org: Please register free of charge
CIPedia©	www.cipedia.eu the new CIP reference point

Forthcoming conferences and workshops

TIEMS 2015 Annual Conference	http://tiems.info/tiems-2015-annual-conference.html	Sept. 30 - Oct. 2, 2015, Rome.
10th CRITIS Conference	www.critis2015.org	Call for Participation, Oct 5-7, 2015, Berlin
Cyber Storm	www.swisscyberstorm.com	Oct. 21, 2015
49th ESReDA Seminar	www.esreda.org	Clos Chapelle-aux-Champs, Belgium 29/30 Oct. 2015
CIPRNet Master Class	www.ciprnet.eu/endusertraining.html	Rome, 11th – 13th November 2015
16th IEE El.Tech Conference	http://melecon2016.org	Call for Participation
ACM CPSS'16	http://icsd.i2r.a-star.edu.sg/cpss16	Call for Paper, Xi'an, China – May 30, 2016
New book	http://staff.www.ltu.se/~ismawa/ansasa	Call for Paper
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu

Project home pages

FP7 CIPRNet	www.ciprnet.eu
H2020 IMPROVER	www.improverproject.eu
H2020 RESIN	www.resin-cities.eu
JRC GRRASP	https://ec.europa.eu/jrc/en/grrasp
Ernest & Young	http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014

and Deltares Brochure:
https://www.deltares.nl/en/projects/climate-change-risk-assessments-and-adaptation-for-roads-the-roadapt-project/

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection" I this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security Platform	https://resilience.enisa.europa.eu/nis-platform

Websites of Contributors

Acris	www.acris.ch
Center for Cyber & Information Security NO	https://ccis.no
Cyfor	https://www.dfs.no/Skytterlagssider/opplandskretsen/gudbrandsdal/cyberforsvaretcistg
Deltares	www.deltares.nl/en
EC Joint Research Centre	https://ec.europa.eu/jrc
EY	www.ey.com/CH/de/Home
Fire and Security DK	www.dbi-net.dk/
H2020	http://ec.europa.eu/programmes/horizon2020
Linköping University	www.liu.se/?l=en
Network Security Lab NO	www.nislab.no
RISC SE	www.rics.se
SP research Sweden	www.sp.se/sv/Sidor/default.aspx
Campus Bio-Medico di Roma	www.unicampus.it

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

CIPedia© needs you in order to become a common reference of CIP concepts.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

Your contribution is essential for putting value in the CIPedia© effort.

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.