European CIIP Newsletter

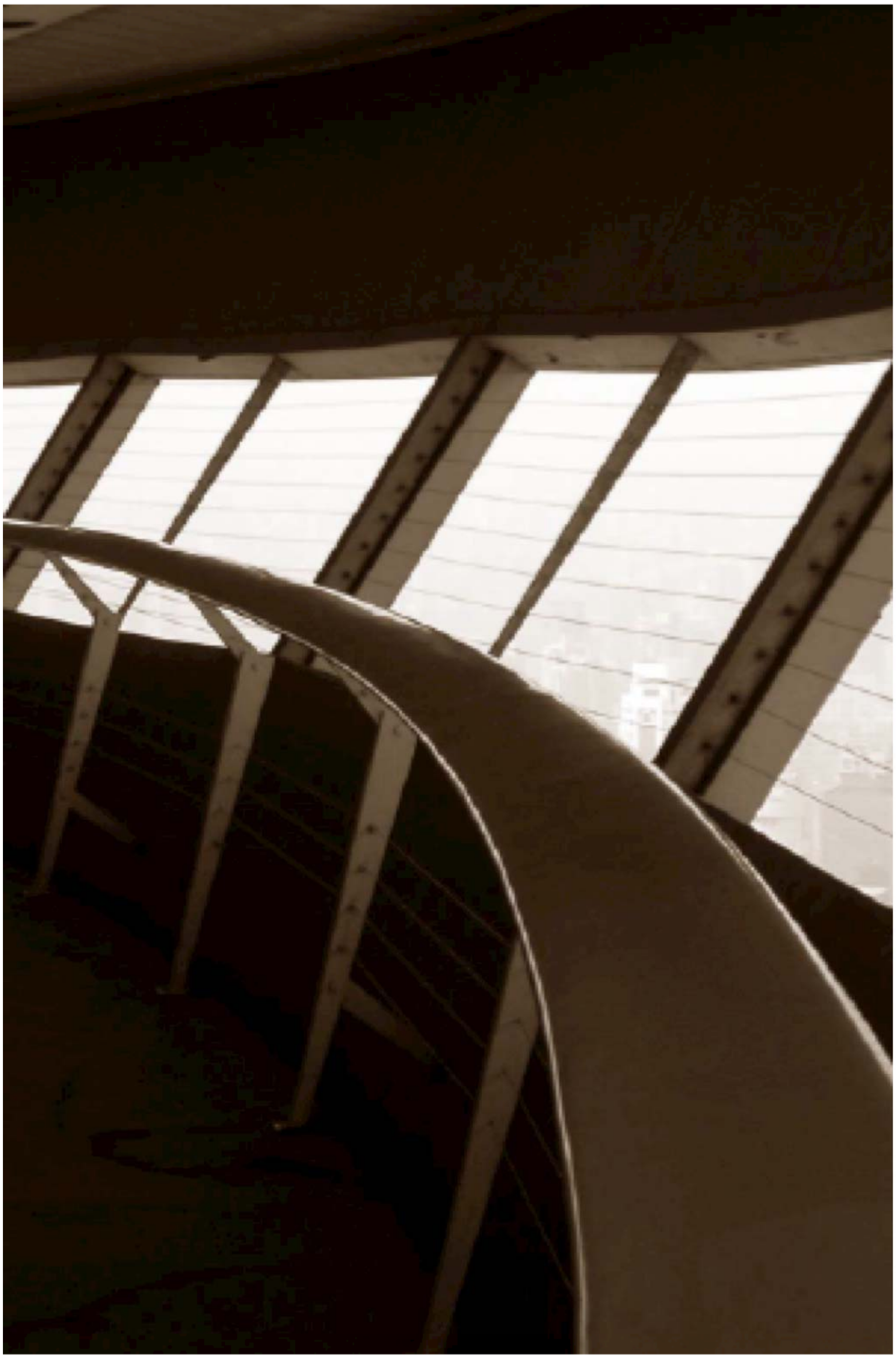
March 15 – June 15, Volume 9, Number 1

CRITIS 2015

Submission deadline
May 10, 2015

2nd Young CRITIS Award

Conference
Oct. 5-7, 2015 Berlin



ECN

Contents

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

>For ECN registration ECN registration & de-registration:
www.ciip-newsletter.org

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

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Editoral

European Activities

Country Specific Issues

Country Specific Issues

Method and Models

Conferences 2015

Links

Media on C(I)IP

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 **P**r**I**vacy and **T**echnology 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

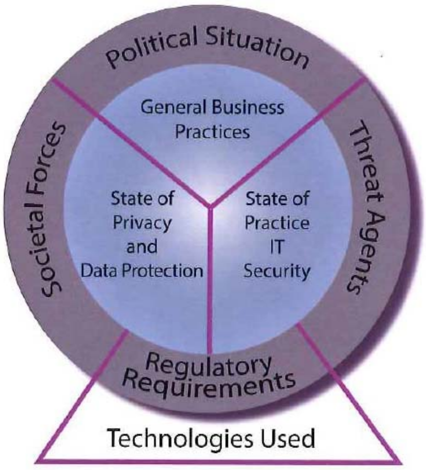
The security and privacy needs associated with an area of information technology are influenced by the business practices of the emerging area, the technology used and environmental forces. Market trends, the societal impact and the evolution of technology determine the future evolution of the emerging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


Political Situation
General Business Practices
Societal Forces
Threat Agents
State of Privacy and Data Protection
State of Practice IT Security
Regulatory Requirements
Technologies Used

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 Intergovernmental 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 **R**eduction 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 Southern 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

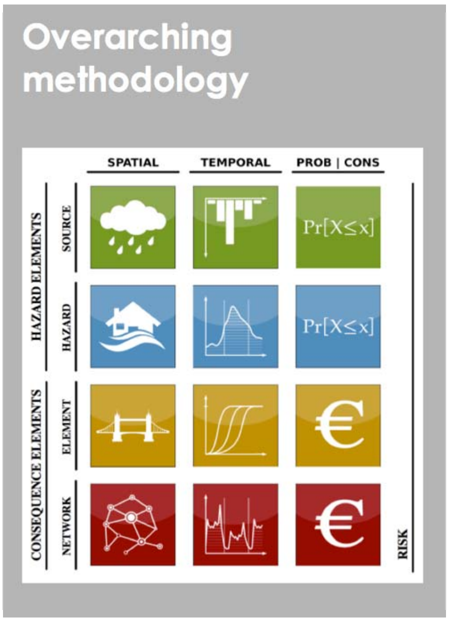
Dr. Maria-Jose Jimenez is physicist and senior research seismologist. She is staff scientist at the Spanish National Council for Scientific Research-CSIC (Consejo Superior de Investigaciones Científicas). She is currently involved in different EU projects and she is member of the Executive Committee 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.

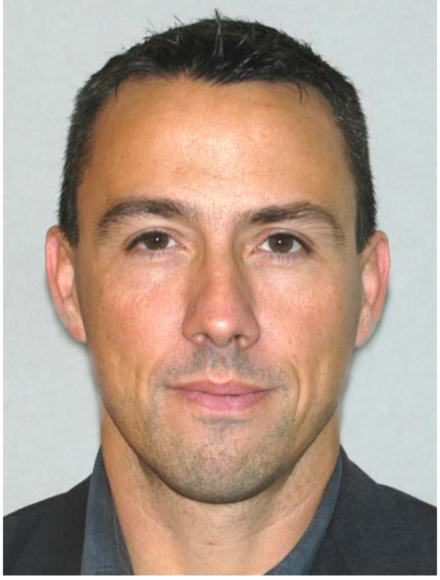
The SMS will be developed with full consideration of present methods and measures for the security and resilience of complex interconnected space control ground station networks by present operators.

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:

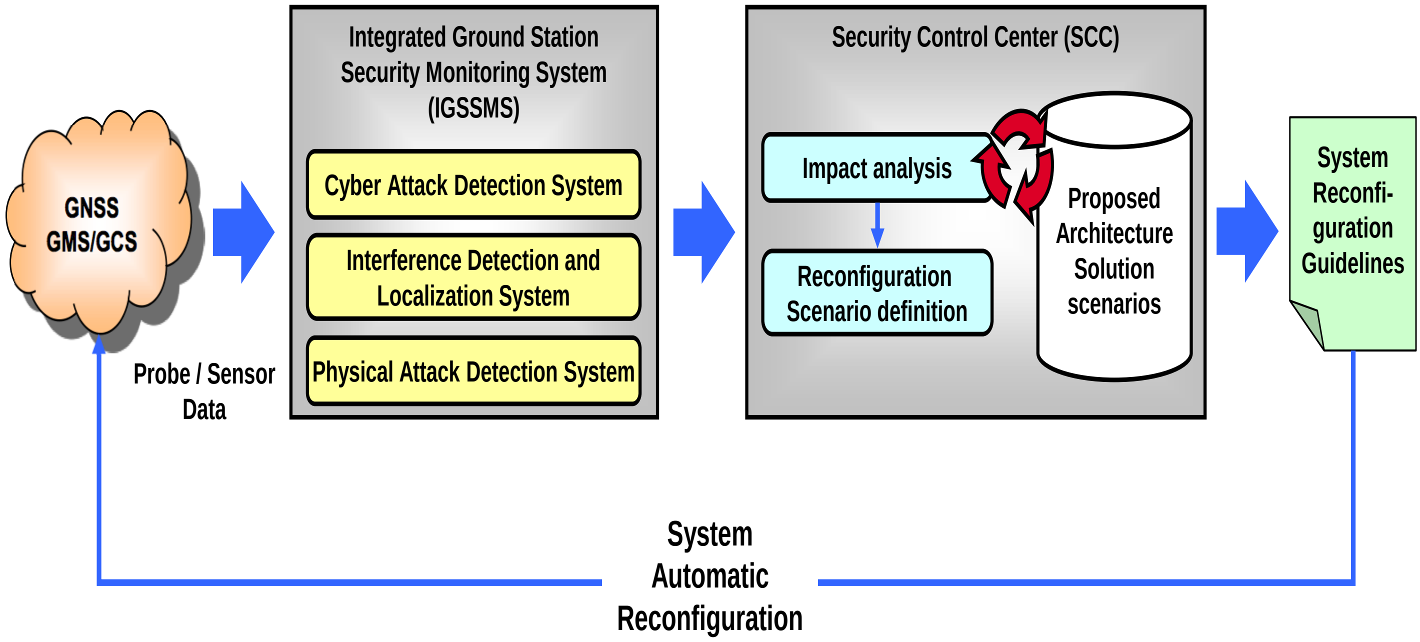
1. Development of risk assessment methodology and tools to assess threats on generic GNSS ground based infrastructure and assets operating space systems and their secure communication links to satellites and a prioritization of the threats for which detection, protection and mitigation solutions should 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


GNSS GMS/GCS
Probe / Sensor Data
Integrated Ground Station Security Monitoring System (IGSSMS)
Cyber Attack Detection System
Interference Detection and Localization System
Physical Attack Detection System
Security Control Center (SCC)
Impact analysis
Reconfiguration Scenario definition
Proposed Architecture Solution scenarios
System Reconfi-guration Guidelines
System Automatic Reconfiguration

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

"The information *appearing in this document has been prepared in good faith and represents the opinions of the authors. The authors are solely responsible for this publication* and *it does not represent the opinion of the European Commission. Neither the authors nor the European Commission are responsible or any use that might be made of data including opinions appearing herein.*

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.

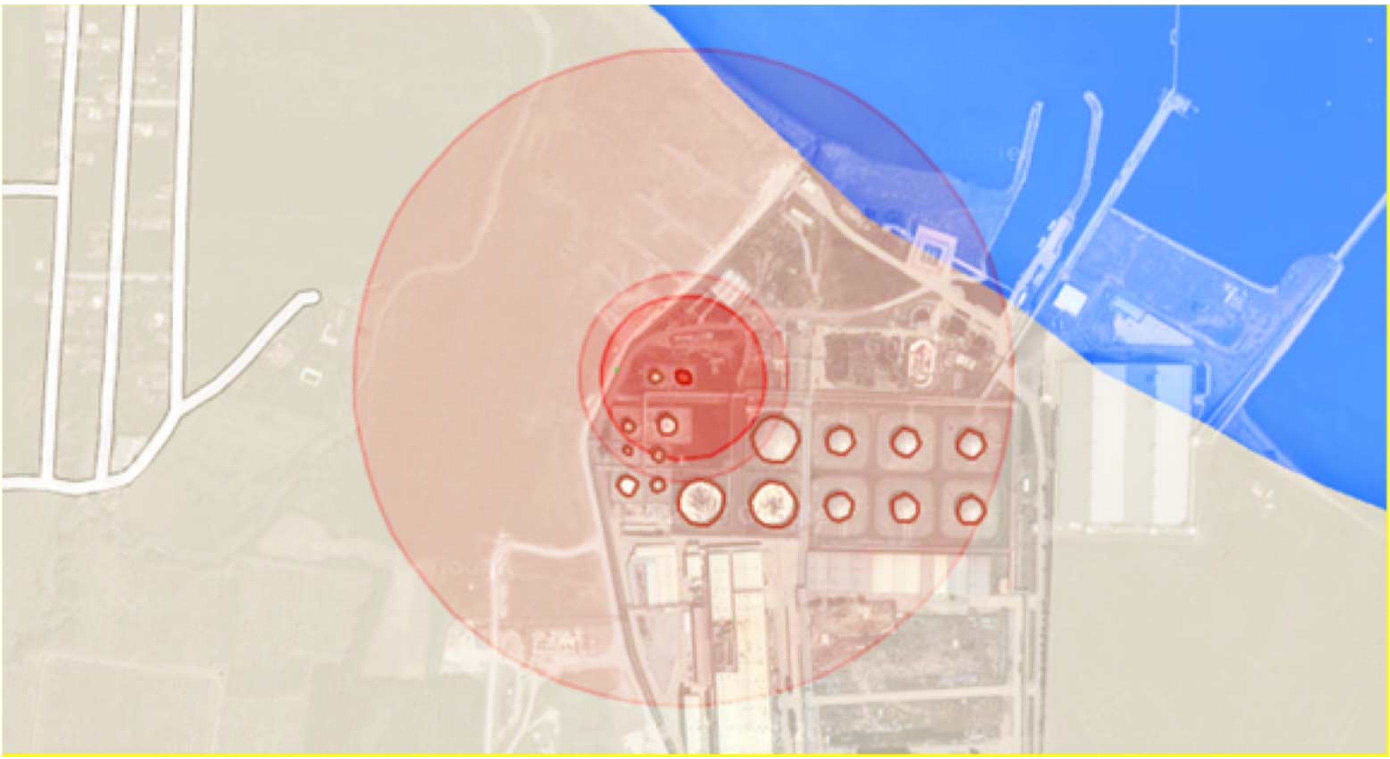


Figure 1: RAPID-N output for the release of a flammable substance from a storage tank upon earthquake impact.

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.

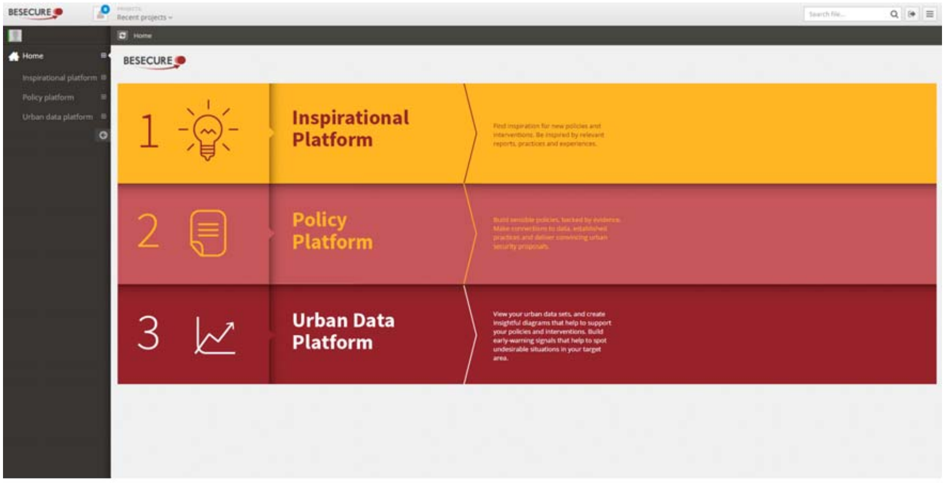
e-mail: **stephen.crabbe@crabbe-consulting.com**

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.

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).



Find inspiration for new policies and interventions. Be inspired by relevant reports, practices and experiences.

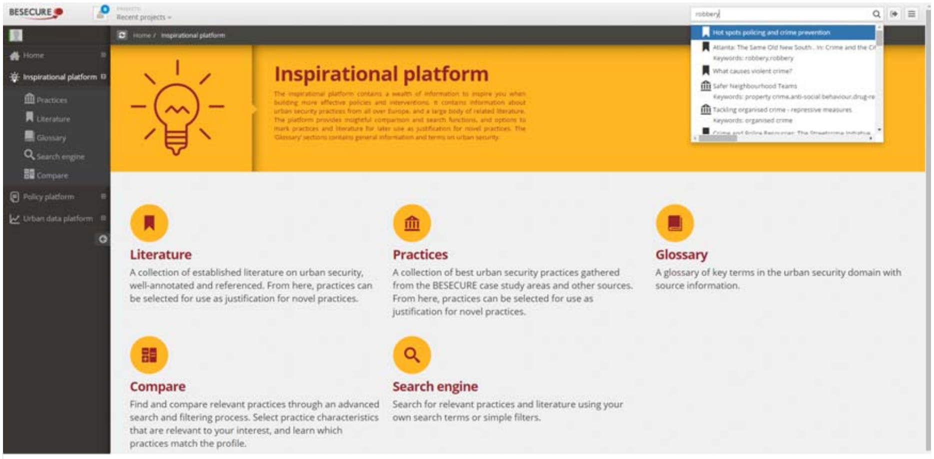
Build sensible policies, backed by evidence. Make connections to data, established practices and deliver convincing urban security proposals.

View your urban data sets, and create insightful diagrams that help to support your policies and interventions. Build early-warning signals that help to spot undesirable situations in your target area.

Figure 1: Screenshot of BESECURE Platform Interface

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.



Hot spots policing and crime prevention
Atlanta: The Same Old New South... In: Crime and the Ci
Keywords: robbery,robbery
What causes violent crime?
Safer Neighbourhood Teams
Keywords: property crime,anti-social behaviour,drug-re
Tackling organised crime - repressive measures
Keywords: organised crime

Inspirational platform

The inspirational platform contains a wealth of information to inspire you when building more effective policies and interventions. It contains information about urban security practices from all over Europe, and a large body of related literature. The platform provides insightful comparison and search functions, and options to mark practices and literature for later use as justification for novel practices. The 'Glossary' sections contains general information and terms on urban security.

Literature
A collection of established literature on urban security, well-annotated and referenced. From here, practices can be selected for use as justification for novel practices.

Practices
A collection of best urban security practices gathered from the BESECURE case study areas and other sources. From here, practices can be selected for use as justification for novel practices.

Glossary
A glossary of key terms in the urban security domain with source information.

Compare
Find and compare relevant practices through an advanced search and filtering process. Select practice characteristics that are relevant to your interest, and learn which practices match the profile.

Search engine
Search for relevant practices and literature using your own search terms or simple filters.

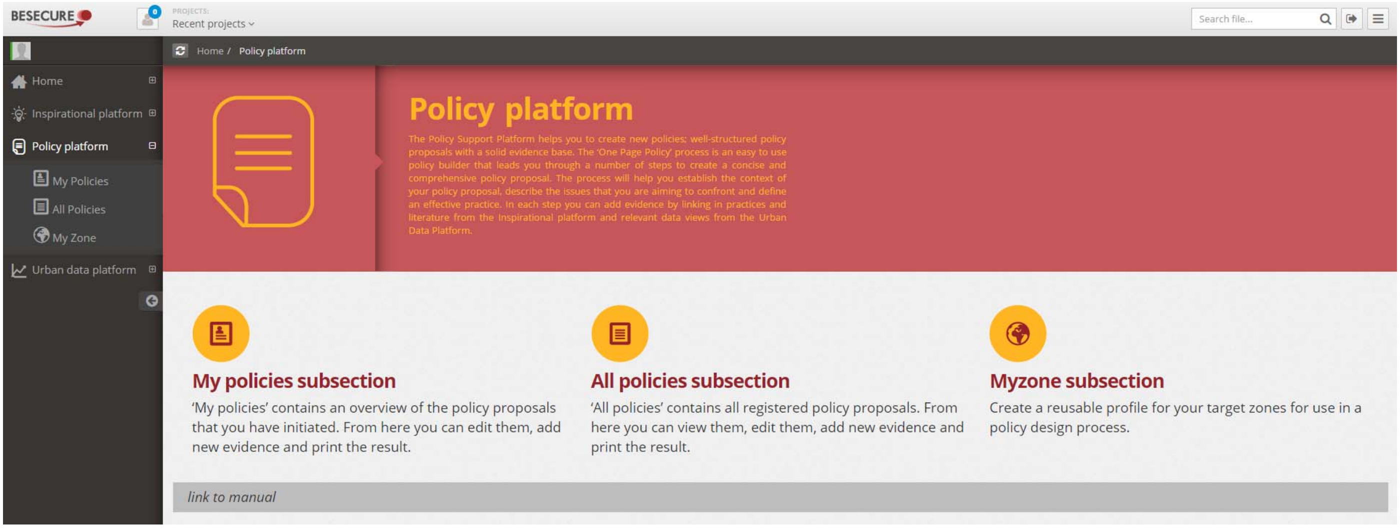
Figure 2: Screenshot of the Inspirational Platform

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.



Policy platform

The Policy Support Platform helps you to create new policies: well-structured policy proposals with a solid evidence base. The 'One Page Policy' process is an easy to use policy builder that leads you through a number of steps to create a concise and comprehensive policy proposal. The process will help you establish the context of your policy proposal, describe the issues that you are aiming to confront and define an effective practice. In each step you can add evidence by linking in practices and literature from the Inspirational platform and relevant data views from the Urban Data Platform.

My policies subsection

'My policies' contains an overview of the policy proposals that you have initiated. From here you can edit them, add new evidence and print the result.

All policies subsection

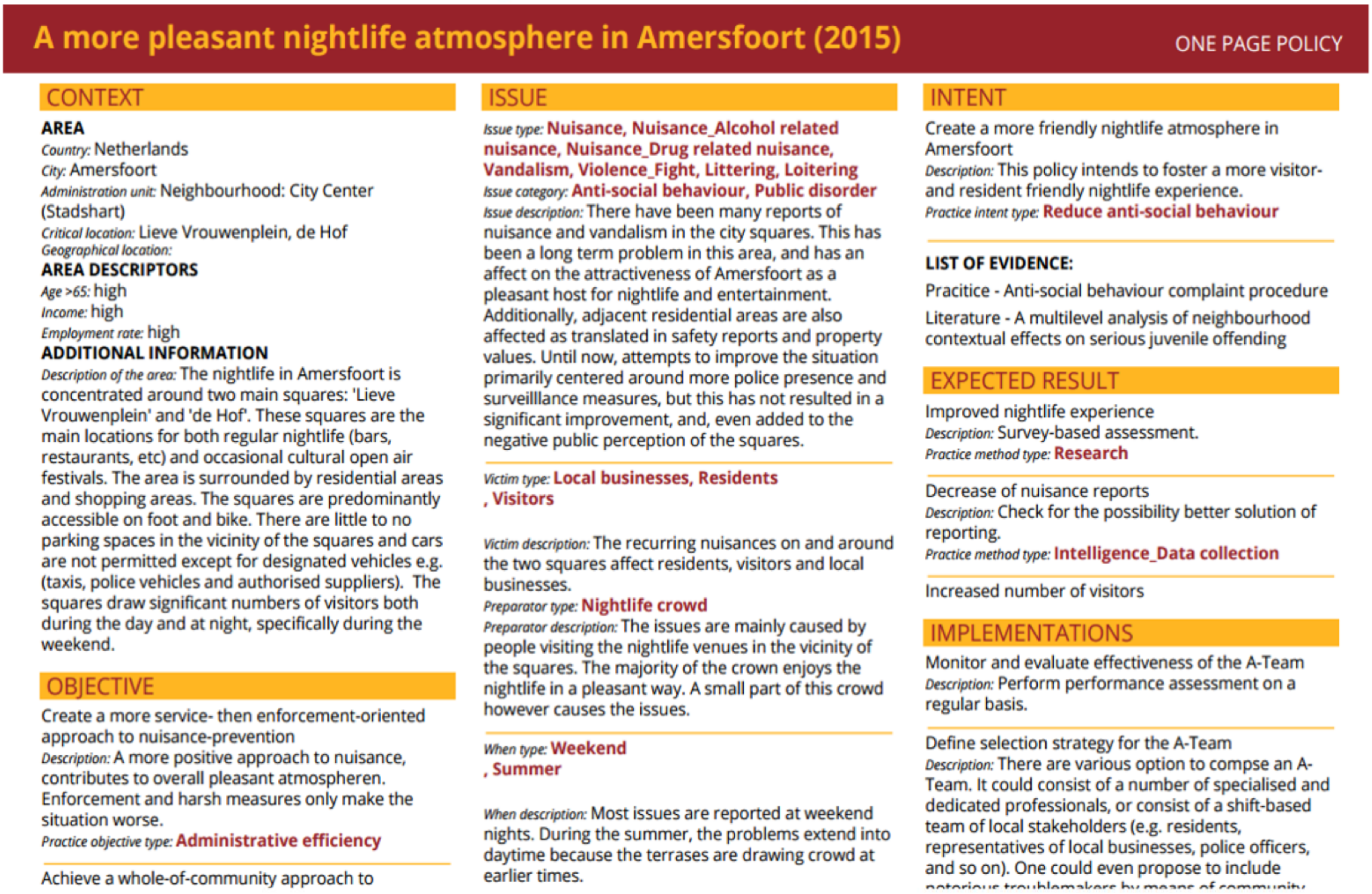
'All policies' contains all registered policy proposals. From here you can view them, edit them, add new evidence and print the result.

Myzone subsection

Create a reusable profile for your target zones for use in a policy design process.

link to manual

Figure 3: Screenshot of Policy Platform



A more pleasant nightlife atmosphere in Amersfoort (2015)

ONE PAGE POLICY

CONTEXT

AREA

Country: Netherlands
City: Amersfoort
Administration unit: Neighbourhood: City Center (Stadshart)
Critical location: Lieve Vrouwenplein, de Hof
Geographical location:

AREA DESCRIPTORS

Age >65: high
Income: high
Employment rate: high

ADDITIONAL INFORMATION

Description of the area: The nightlife in Amersfoort is concentrated around two main squares: 'Lieve Vrouwenplein' and 'de Hof'. These squares are the main locations for both regular nightlife (bars, restaurants, etc) and occasional cultural open air festivals. The area is surrounded by residential areas and shopping areas. The squares are predominantly accessible on foot and bike. There are little to no parking spaces in the vicinity of the squares and cars are not permitted except for designated vehicles e.g. (taxis, police vehicles and authorised suppliers). The squares draw significant numbers of visitors both during the day and at night, specifically during the weekend.

OBJECTIVE

Create a more service- then enforcement-oriented approach to nuisance-prevention
Description: A more positive approach to nuisance, contributes to overall pleasant atmospheren. Enforcement and harsh measures only make the situation worse.
Practice objective type: **Administrative efficiency**

Achieve a whole-of-community approach to

ISSUE

Issue type: **Nuisance, Nuisance_Alcohol related nuisance, Nuisance_Drug related nuisance, Vandalism, Violence_Fight, Littering, Loitering**
Issue category: **Anti-social behaviour, Public disorder**
Issue description: There have been many reports of nuisance and vandalism in the city squares. This has been a long term problem in this area, and has an affect on the attractiveness of Amersfoort as a pleasant host for nightlife and entertainment. Additionally, adjacent residential areas are also affected as translated in safety reports and property values. Until now, attempts to improve the situation primarily centered around more police presence and surveilllance measures, but this has not resulted in a significant improvement, and, even added to the negative public perception of the squares.

Victim type: **Local businesses, Residents , Visitors**

Victim description: The recurring nuisances on and around the two squares affect residents, visitors and local businesses.
Preparator type: **Nightlife crowd**
Preparator description: The issues are mainly caused by people visiting the nightlife venues in the vicinity of the squares. The majority of the crown enjoys the nightlife in a pleasant way. A small part of this crowd however causes the issues.

When type: **Weekend , Summer**

When description: Most issues are reported at weekend nights. During the summer, the problems extend into daytime because the terrases are drawing crowd at earlier times.

INTENT

Create a more friendly nightlife atmosphere in Amersfoort
Description: This policy intends to foster a more visitor- and resident friendly nightlife experience.
Practice intent type: **Reduce anti-social behaviour**

LIST OF EVIDENCE:

Practice - Anti-social behaviour complaint procedure

Literature - A multilevel analysis of neighbourhood contextual effects on serious juvenile offending

EXPECTED RESULT

Improved nightlife experience
Description: Survey-based assessment.
Practice method type: **Research**

Decrease of nuisance reports
Description: Check for the possibility better solution of reporting.
Practice method type: **Intelligence_Data collection**

Increased number of visitors

IMPLEMENTATIONS

Monitor and evaluate effectiveness of the A-Team
Description: Perform performance assessment on a regular basis.

Define selection strategy for the A-Team
Description: There are various option to compse an A-Team. It could consist of a number of specialised and dedicated professionals, or consist of a shift-based team of local stakeholders (e.g. residents, representatives of local businesses, police officers, and so on). One could even propose to include notorious troublemakers by means of community

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.

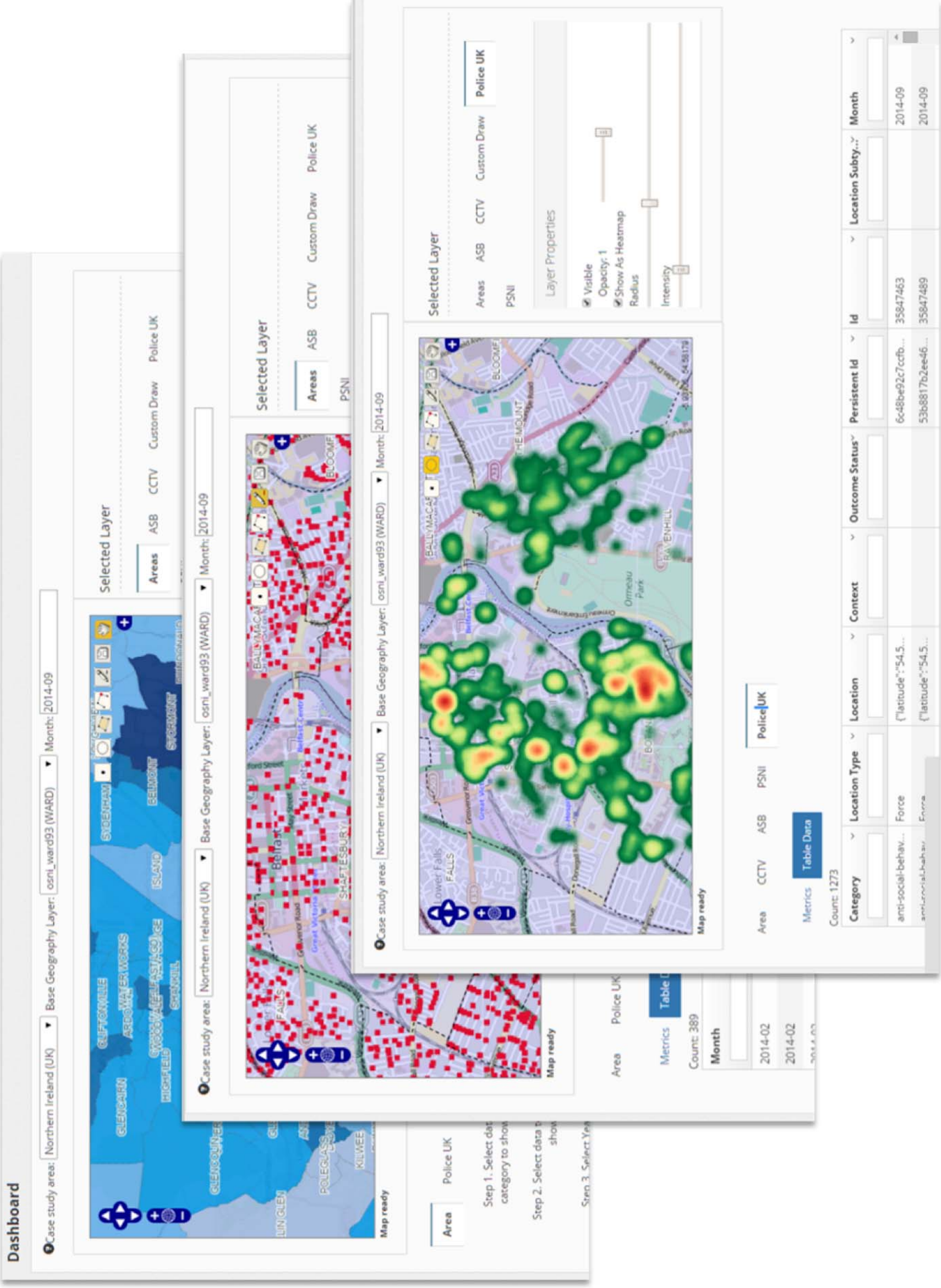
The Partners

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.



Dashboard

Case study area: Northern Ireland (UK)

Base Geography Layer: osni_ward93 (WARD)

Month: 2014-09

Count: 1273

Category	Location Type	Location	Context	Outcome Status	Persistent Id	Id	Location Subty...	Month
anti-social-behav...	Force	{"latitude":"54.5...			6c48be92c7ccfb...	35847463		2014-09
anti-social-behav...	Force	{"latitude":"54.5...			53b8817b2ee46...	35847489		2014-09

Count: 389

Month
2014-02
2014-02

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.

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

[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/

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 interdependencies 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.

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] 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

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. 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

[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

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 km^2) 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

In 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.
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.

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

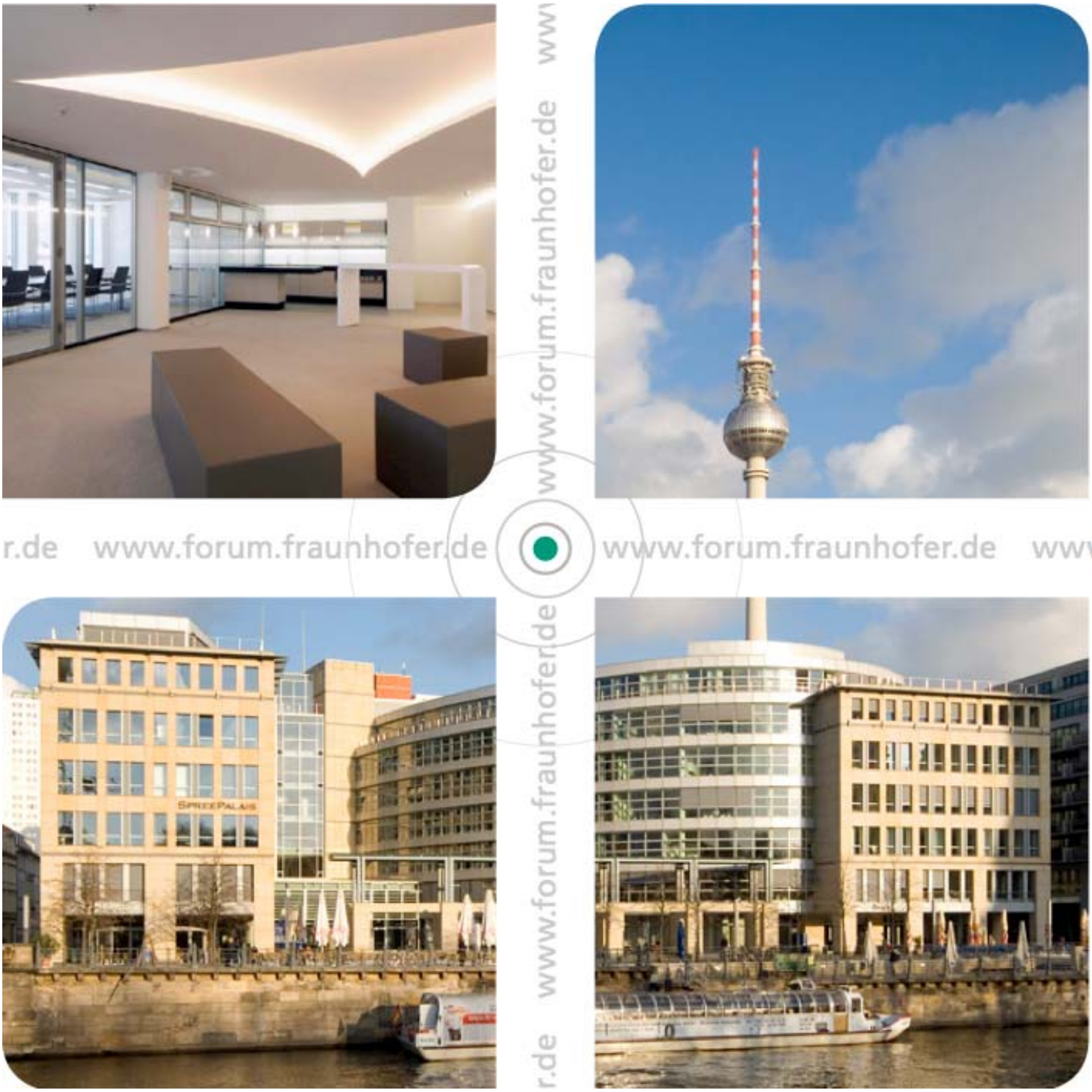
Oreste S. Bursi

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].

Dynami**c 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, $\left[e_1, e_2, e_3, \ldots, e_n\right]$. The corresponding occurring instants are defined by $\left[t_1, t_2, t_3, \ldots, t_n\right]$. 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:

$$p_n(t) =$$

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

Where:

$0 \leq \xi_1 \leq \xi_2 \leq \xi_3 \leq \ldots \leq \xi_n \leq t$ and ρ_i is the Poisson density function characterizing the event e_i [ρ_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].

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

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.

Acknowledgement

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

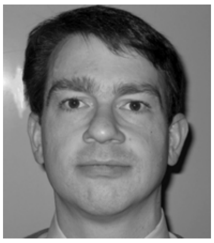
- Modelling and analysis of cyber-physical systems for monitoring and control
- Security, protection, resilience and survivability of complex cyber-physical systems
- Impact and consequence analysis of C(I)I loss or reduction of quality of service
- C(I)I dependency Modeling, Simulation, Analysis and 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

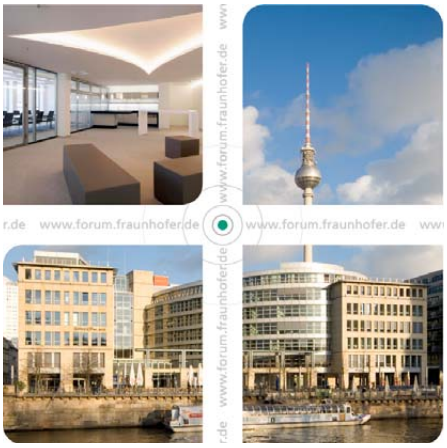
Submission of full papers:
May 10, 2015 (firm deadline)
Notification of acceptance:
July 8, 2015
Camera-ready papers:
September 10, 2015
CRITIS 2015 event:
October 5–7, 2015

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 El.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.

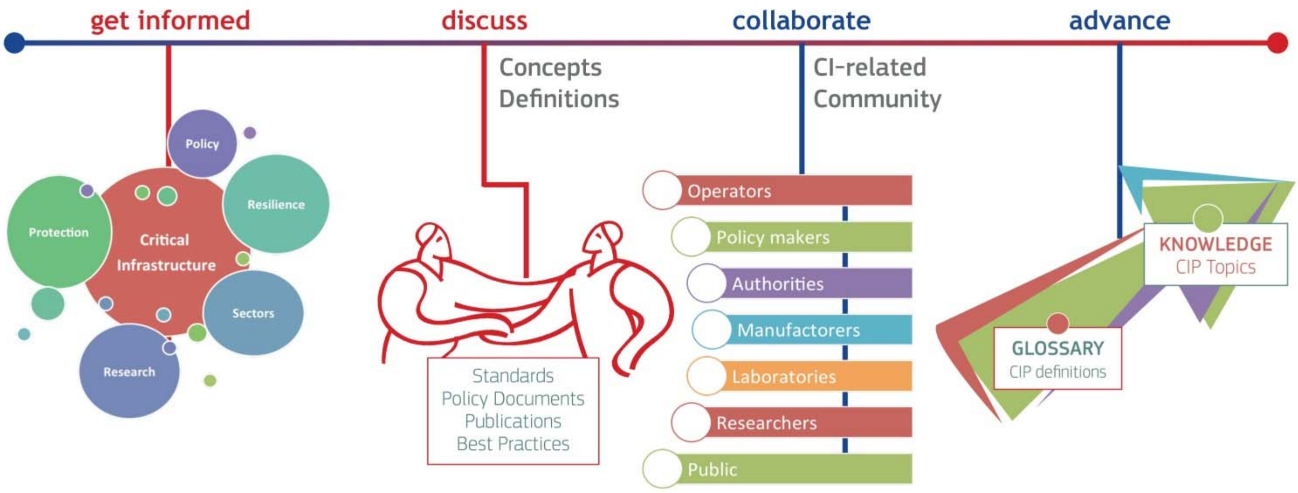
marianthi.theocharidou@jrc.ec.europa.eu

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


get informed
discuss
collaborate
advance
Concepts
Definitions
CI-related
Community
Policy
Resilience
Protection
Critical
Infrastructure
Sectors
Research
Standards
Policy Documents
Publications
Best Practices
Operators
Policy makers
Authorities
Manufactorers
Laboratories
Researchers
Public
KNOWLEDGE
CIP Topics
GLOSSARY
CIP definitions