FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

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

D8.522 European CIIP Newsletter issues 23–26

Due date of deliverable: 28/02/2017
Actual submission date: 17/02/2017

Revision: Draft version 1

ACRIS GmbH (ACRIS)

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

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

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

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

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

TABLE OF CONTENTS

1 Introduction – Rationale of this document

This deliverable contains the bundled issues 23, 24, 25 and 26 of the European CIIP Newsletter (ECN). All issues so far have also been published on the CIPRNet website and distributed via the CIPRNet consortium's mailing lists.

2 References

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

Appendix: ECN issues 23 (Vol. 10, No. 1), 24 (Vol. 10, No. 2), 25 (Vol. 10, No. 3) and 26 (Vol. 11, No. 1)

European CIIP Newsletter

March 16 - June 16, Volume 10, Number 1

CRITIS 2016
Call for Papers

CYCA Young researcher Competition

ECN

Contents

CIPR Net

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

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

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

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Editorial

European and Global Activities

Country Specific Issues

Method and Models

Method and Models (continued)

Ads of upcoming Conferences, Workshops and more

Links

Media on C(I)IP

Editorial: About the importance of soft factors in C(I)IP

Increasing the resilience of European Critical Infrastructures through science requires closer collaboration of projects with similar scope, close communication with end users and links to EU policy.

Research on Critical Infrastructure (Information) Protection (C(I)IP) has tremendously developed over the last 25 years. The rapid expansion of engineering and computer sciences has led to an impressive progress on modelling, simulation and analysis in order to better respond to a variety of threats, either natural or man-made.

However, there is less knowledge nowadays about the human emotion, cognition and behaviour in crisis situations. Behavioural and social sciences as well as research on human factors have still much to offer in this applied area. This could be achieved in the future by fostering collaborative research in at least three directions: better preparing first responders, raising awareness among citizens and learning from survivors.

The professional responding bodies such as the staff working in fire brigade, police, medical emergency, civil protection, command and control centres etc. may face poor communication, lack of relevant information or inappropriate decisions that may impair their professional performance and interfere with rescue procedures. Human factor research can bring more in-depth knowledge on the needs and requirements of these professional categories, in order to optimise decision-making, resource allocation and ultimately improve their response actions. Research results can be used for developing better recommendations and training programs for the concerned professional categories.

Moreover, crisis research has shown that lay citizens react more effectively than we would intuitively expect, and often respond at least as effective as well-trained emergency personnel. While fear is the dominant emotion across different types of disasters, it appears that in most cases panic does not take over the rational behaviour. Yet, the ongoing challenge is to find solutions to raise citizen awareness and improve their preparedness. Current research shows that citizens will prepare for a specific event only if they believe that preparation is useful and the event is indeed likely to occur. Social science can shed more light on how people perceive and accept risk, and can reveal their needs in terms of well-being during a disaster management. Social studies can also show the citizen's role is mass crisis dissemination and information flows for example through social media.

Last but not the least, disaster survivors and witnesses may provide useful feedback and lessons learned from their experience with various threats. The little existing research based on interviews and focus-groups suggests that during a crisis situation people's responses may depend on one's ability to recognise and to make sense of cues to life-threatening stimuli. There have also been insights that people tend to underestimate such cues and there are still conflicting results about the post-traumatic stress and the amount of accurate information that survivors and witnesses are able to recall.

Further research is needed to clarify these unanswered questions and help complement the CI resilience with a better psychological preparedness and resilience.

Some of these challenging topics will be addressed during the **11th edition of the CRITIS conference** which is scheduled from 10–12 October 2016 in Paris: www.critis2016.org

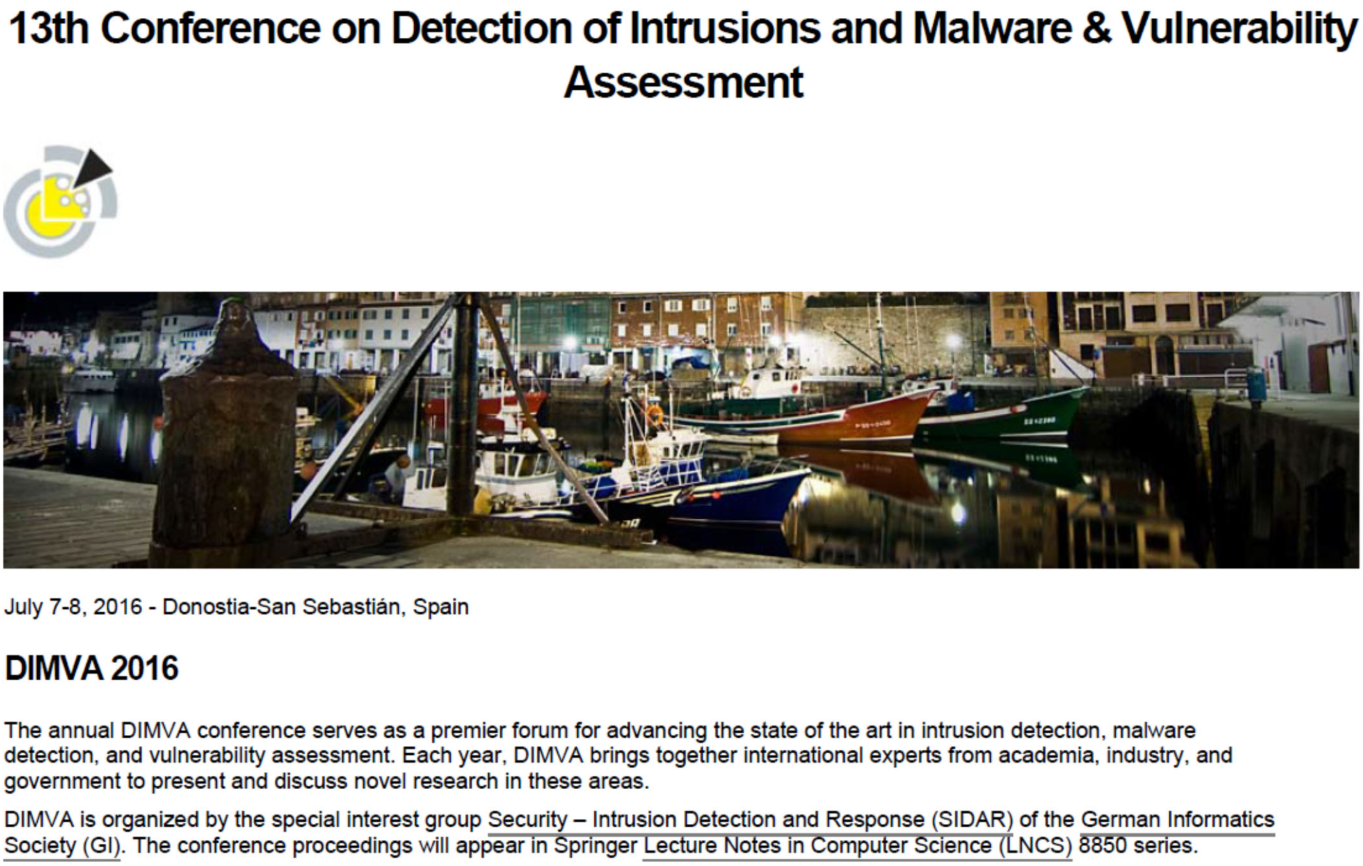
Enjoy reading this issue of ECN!

Grigore M. Havârneanu
is Traffic and Transport Psychologist with a PhD in Social Psychology. He is Research Advisor within the International Union of Railways' Security Division

e-mail: **havarneanu@uic.org**

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



13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment

July 7-8, 2016 - Donostia-San Sebastián, Spain

DIMVA 2016

The annual DIMVA conference serves as a premier forum for advancing the state of the art in intrusion detection, malware detection, and vulnerability assessment. Each year, DIMVA brings together international experts from academia, industry, and government to present and discuss novel research in these areas.

DIMVA is organized by the special interest group Security – Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI). The conference proceedings will appear in Springer Lecture Notes in Computer Science (LNCS) 8850 series.

Central topics of the conference

INTRUSION DETECTION
Novel approaches and domains
Insider detection
Prevention and response
Data leakage and exfiltration
Result correlation and cooperation
Evasion and other attacks
Potentials and limitations
Operational experiences

Privacy, legal and social aspects
Targeted attacks
MALWARE DETECTION
Automated analyses
Behavioural models
Prevention and containment
Classification
Lineage, Forensics and recovery
Underground economy

VULNERABILITY ASSESSMENT
Vulnerability detection
Vulnerability prevention
Vulnerability analysis
Exploitation prevention
Situational awareness
Active probing

Organising Committee

- General Chair: Urko Zurutuza, Mondragon University, Spain
- Program Chair: Juan Caballero, IMDEA Software Institute, Spain
- Publication Chair: Ricardo J. Rodríguez, Universidad de Zaragoza

Join DIMVA 2016

http://dimva2016.mondragon.edu/en

Towards a competitive European Digital Single Market

EOS represents the interest of European security suppliers including large companies, SMEs, research centres, universities, clusters and associations. Our work and purpose is to provide a platform of collaborative work, insightful exchange of ideas and best practices between the European Institutions, the Member States and our Members.

Europe has taken important commitments and concrete actions towards building a sustainable Digital Single Market. The European strategy developed in this regard comes at the right time as Europe is in danger of falling behind in the international digital economy.

EOS welcomes this strategy that aims at creating the right conditions and a level playing field for advanced digital networks and innovative services along with maximising the growth potential of the digital economy.

This important objective should, however, be supported by an effort to protect and develop the European Digital Single Market (DSM).

Against this background, EOS has produced, in collaboration with its Members, an extensive in-house study of the European cybersecurity market. In this unique study, EOS gives an overview of the current cybersecurity market and describes the challenges ahead providing recommendations and concrete actions to be taken in order to raise Europe to its full potential in the global cyber chessboard.

The European cybersecurity market

Following the revelations made by Mr. Snowden, the questions of privacy and data protection figure highly among societal concerns. Todays, and thanks to fruitful societal and high level political debates and actions, Europe is seen as a trusted stakeholder in the world when it comes to data security and privacy.

This status should be sustained and developed with the support of a strong and competitive European cybersecurity market in line with EU privacy and data protection requirements. Unfortunately, the European cybersecurity market has inherited some of the problems faced by the general European security market.

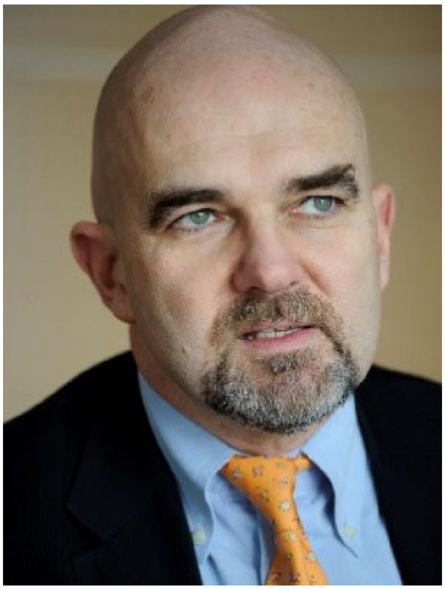
In a nutshell, the cybersecurity market, currently, suffers from a large fragmentation which is partly due to the fact that security in general and cybersecurity in particular (especially as a component of critical infrastructures and national assets protection) remains a national prerogative. The 28 EU Member States have different regulations and approaches towards cybersecurity as well as data privacy concerns which inevitably lead to the development of different specific solutions not necessarily competitive on a global scale.

At the same time, even though innovation is strong in Europe (coming from ICT labs, SMEs, research centres, and large companies) it often lacks the necessary funding based on a consistent transnational approach. Research and Development (R&D) and Research and Innovation (R&I) in cybersecurity, like in security in general, hardly reaches market deployment and is exacerbated by weak public procurement policies.

All in all, Europe is far from being at the right level of preparedness. The full implementation of an EU single digital market calls for more coordination at the EU level with a clearly identified industrial strategy and investment plan.

The main questions for Europe are:

- What is the level of strategic autonomy that Europe needs to achieve in the cybersecurity domain?
- In which cybersecurity areas can European industry make a breakthrough and become a global and competitive player?



Luigi Rebuffi

Luigi Rebuffi is the CEO of EOS. After having worked on the development of high power microwave systems for the next thermonuclear fusion reactor (ITER) he continued his career at Thomson CSF / Thales where he took on increasing responsibilities for European Affairs (R&D) in different sectors: telecom, industrial, medical, scientific. He became in 2003 Director for European Affairs for the civilian activities of the Group.
He is a Member of the European Commission's Protection and Security Advisory Group on EU Security Research and President of the Steering Board of the French ANR for security research.

e-mail: luigi.rebuffi@eos-eu.com

European Organisation for
Security (EOS), 10, rue Montoyer
1000 Brussels / Belgium

The need for technological autonomy

Networks do not know boundaries and the continuous interconnection between information systems make cybersecurity a transnational issue by nature. In addition, the globalisation of trade makes network interconnection and interoperability a necessary requirement between the various economic agents increasing cooperation at regional and international level. Cyber attackers / hackers use this feature to their advantage to bounce from one country to another to cover their tracks.

In this scenario, the weakest link in the supply chain endangers the activity of many stakeholders' especially critical infrastructure managers and operators.

Because of current highly fragmented cybersecurity market, European users depend largely on non-European solutions for their cyber-protection. The increasing demand for cybersecurity products and services are often met by non-EU originating companies due to a lack of European policies designed to strengthen the European offer.

These technologies might potentially include built-in backdoors and with time, increase our vulnerability to the risks posed by cyber threats especially towards vital and critical infrastructures.

The question we need to ask ourselves today is how Europe can overcome these challenges and control its data when it is not even controlling its own ICT infrastructure and services?

Some EU Member States like Germany, France, Finland and the UK have started a discussion on how to achieve a greater autonomy and authority over ICT services and equipment. Several solutions have been proposed at national level but no convergence has been reached for a common approach based on certified, trusted EU solutions.

It is however essential to define a common, standardisation procedure for EU products and services among the Member States to avoid further fragmentation and higher costs. It is also of paramount importance that all the players in the ICT value chain, operating or not from a European Member States, adhere to similar requirements concerning data protection and cybersecurity. All market operators of the Digital Economy should share the responsibility for a secure cyber space and all players involved must be committed to secure digital products, software and services.

Developing trusted EU solutions and securing the supply chain

To achieve this goal, and due to rapidly emerging threats, we must plan the coming years in a smart and strategic way.

Massive investment campaigns to build the entire supply chain for IT components and services in Europe would demand a too large effort.

Instead, Europe should find a good balance between the use of certified trusted non-EU technologies and the development of European solutions in vital areas (e.g. ICT infrastructure and public services), and in applications where Europe is a market leader (e.g. aeronautics, car manufacturing, finance services and all sectors falling under the Industry 4.0).

In parallel, areas of higher competence in Europe like Identification and Access Management (e.g. smart cards) as well as Data Security (e.g. encryption) should be continuously improved to maintain leadership, while competitiveness should be increased in strategic components for Network Security Systems and Management of Security Services.

In this respect, EOS has been actively supporting the creation of a European Public-Private Partnership (PPP) on cybersecurity which will be set up in 2016. This collaborative platform will be a major opportunity to build a stronger technology base, and outline a common European industrial strategy to effectively meet the interests of Europe.

EOS and its members are confident that the work stemming from this partnership will lay down the basis for a "European Cybersecurity Flagship" harmonising capacity building in Member States and allowing, by 2025, our industry to become a world leader in key strategic sectors, implementing trusted European cybersecurity solutions and ensuring a greater digital autonomy.

EOS' cybersecurity Flagship initiative

The Flagship initiative developed and advocated by EOS and its members is built upon two main objectives:

1. The creation of a Flagship initiative for an EU Cybersecurity Investment Programme supported by adequate funding (initial estimate of €13 billion over 10 years), which would be composed of:

- Research & Innovation Programme based upon a competitive growth strategy.
- Capacity deployment across Europe according to an agreed Roadmap, including short term focus on concrete strategic projects on capability and capacity building.

The Public-Private Partnership (PPP) foreseen in the DSM Strategy could well be the initial step of this Flagship.

2. The development of a European Cybersecurity Industrial Policy touching upon several dimensions including: standards, certification and EU labels, innovative funding initiatives, education / training / awareness, support to SMEs and clusters, etc. This Industrial Policy will support the implementation of the DSM Strategy and the EU Cybersecurity Strategy (as well as the Cybersecurity Flagship objectives) at EU and Member State level.

More information can be found on the EOS website: www.eos-eu.com

EOS is registered at the EU Transparency register: 32134385519-64

CI2C Critical Infrastructures and Cloud Computing: understanding cross-sectorial criticalities and security practices

The goal of the CI2C project is to investigate and is focused on enhancing the security and resiliency of Cloud Computing and Critical Information Infrastructures (CIIs).

The CI2C project is a new project co-funded by the European Commission under the under "The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS) programme. The project started on September 1st 2014 and runs until May 2016.

The coordinator of CI2C project is Maria Cristina Brugnoli, Coordinator of the ICT4People Research Unit (ict4people.cnit.it).

"CI2C Observatory "

In order to widespread the research activities realised the project will develop a web portal, the "CI2C Observatory", to support to provide all involved CI2C stakeholders with a practical way for identifying vulnerabilities and weaknesses of the CI2Cs and for consolidating best practices. The "Observatory" will also support the cooperation and results exploitation over the long term and to collect and disseminate recommendations, experiences, expectations, needs from CIIs stakeholders, Cloud providers, CII and Cloud specialists through an intense stock-taking study.

Background

In the last years EC has highlighted the relevance of introducing Cloud Computing (CC) in EU Member States (MS) and has unveiled its ambitious cloud strategy – which aims to boost the use of CC in the European Union area. In the next future, the diffusion of cloud services will then spread over many critical sectors, like for examples public sectors as well as strategic private sectors. An uncontrolled take-up of CC in CIIs would have unpredictable effects.

Focus

The CI2C project is focused on enhancing the security and resiliency of Cloud Computing and Critical Information Infrastructures (CIIs) by assessing and evaluating cross sectors criticalities that could amplify effects and impacts in case of failures.

The CI2C project will create the foundation for securing and protecting CIIs with intense use of CC (CI2C systems). It will execute in-depth analysis and map of the best practices and policies for CIIPs and research on CC and security's state of the art, to form a complete picture of the EU CI2C systems and of their protection and security practices. CI2C will perform cross sector criticalities analysis, and will identify patterns and provide metrics for the quantification and modelisation of interdependencies in CI2C systems.

Maria Cristina Brugnoli

Maria Cristina is the Coordinator of the "ICT4People" of CNIT (Consorzio Nazionale Interuniversitario per le Telecomunicazioni), a Research Unit that aims to promote a unique and challenging way of studying ICT innovation, bridging the gap between Technology and Human Society. Maria Cristina is a researcher specialised in the evaluation and validation of ICT service and applications with more than 10 years of experience in the EU RTD funded projects. In CNIT since 2010, her current research interest are focused on the investigation and evaluation of end users aspect of security of distributed systems, critical infrastructures, and cloud computing.

e-mail: mariacristina.brugnoli@cnit.it

ICT4people Research Unit Coordinator
www.cnit.it
ict4people.cnit.it
Department of Electronic Engineering
University of Roma, Tor Vergata

Objectives

The project main objectives are to enhance security and resiliency of CC and CIIs by assessing and evaluating cross sector criticalities, to increase security awareness on Clouds within CII operators and the larger community, and to provide relevant information in order to foster coordination on the topics at EU level.

1) Proposing recommendations and technical guidelines for the protection of CI2C systems and the enhancement of security of the critical cloud services

2) Enhancing the capabilities of the cloud community and the CIIs as users of the cloud services to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in CC and security of CIIs

3) Strengthening the protection of the CI2Cs with practical contributions for circumventing the main security concerns

4) Contributing to the EC's efforts and strategy for the enhancement of the awareness of the shared culture of security and protection of CIIs within EU MSs

5) Demonstrating models and metrics for quantifying cross sector criticalities in support of C2ICs risk assessment activities with realistic case studies

6) Developing a project observatory for C2ICs, extended at all the EU MSs, and will provide the stakeholders with practical way for identifying risks and vulnerabilities of the CI2Cs and for consolidating best practices. The cooperation portal will ensure transferability of project results (to MSs and critical sectors not covered in the project).

Cloud Computing and Critical Information Infrastructures: A survey of the CI2C project

CI2C Online survey

CI2C has launched a survey on how cloud computing (CC) services are used by critical infrastructures and organizations providing critical services. As a first step of our work we have launched an online survey: the final results of the CI2C will be published in the course of 2016 on our website (www.ci2c.eu). We would be very interested in having your opinion on these topics, so if you wish to have your say please go to: https://it.surveymonkey.com/s/ci2c_survey

CI2C methodologies

During the first phase of the project, the work will be conducted realising a stock taking of current CC and CIIs security practices (orientations, expectations, criticalities, concerns). This work will be based on a number of methodologies used to collect and analyse data gathered from multiple relevant stakeholders across Europe. In particular will be leveraged a wide range of investigation techniques (survey, interviews and questionnaires, panel assessment, workshops) as well as quali-quantitative methods of analysis to identify existing and innovative security practices for CI2Cs systems.

The second and final phase step will focus on the mapping cross-sector criticalities emerging in CI2C systems and to propose models and metrics for quantifying them. The analysis and quantification of cross-sector criticalities, widely known as interdependencies, is an activity core in critical infrastructures risk assessment. The methodology will be based on complex networks modelling and analysis methods and will be used for the quantification of interdependencies in CI2C systems and the evaluation of the cross sectors criticalities (and the criticality level) in real use cases identified during the project.

CI2C Consortium

The CI2C Consortium consists of 5 partners:

- CNIT Project Coordinator– ICT4People Research Unit (Coordinator), www.ict4people.cnit.it, ITALY
- Deloitte ERS – Enterprise Risk Services, – www.deloitte.it, ITALY
- LIMS London Centre for Mathematical Science, www.london-institute.org, --- UNITED KINGDOM
- Eurocloud Europe,
- www.eurocloud.com, LUXEMBOURG
- Associazione Italiana Infrastrutture Critiche ITALY, www.infrastrutturecritiche.it/aiic/

If you would like to know more about CI2C please visit the project website: www.ci2c.eu

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

WISER helps organisations implement effective cyber risk management

WISER is a European collaborative Innovation Action that puts cyber-risk management at the very heart of good business practice, benefitting multiple stakeholders in particular critical infrastructure operators and process owners, and ICT-intensive SMEs.

Cyber-attacks are becoming a clear obstacle for European economies to strive. It is decreasing trust of the users and slowing down the growth of the Digital Single Market. Damage is not only economical, but also has high societal impact, since attacking sensitive information and critical infrastructures that provide essential services for society that, in the most dramatic case, may lead to loss of human lives.

Cyber threats are evolving and becoming more sophisticated, what should compel organisations to be in a position of permanent surveillance, monitoring continuously each system. But in spite of the big risk, available solutions still keep weak.

The lack of cyber risk awareness is becoming a very serious problem. Enterprises and SMEs are not able to cope with the dynamicity and complexity of cyber risk which is putting them in a vulnerable position. Besides, they often lack tools or qualified teams to support the decision-making process regarding the mitigating measures.

Cyber risk detection and assessment is usually a manual process, mainly performed periodically at static points of time. In addition, current focus is on the ICT side, not considering business or societal impact. This perspective contrasts with the cyber risk dynamic nature that sometimes demands rapid ad-hoc mitigation measures.

Started in June 2015, WISER project will deliver, by 2017, a cyber-risk management framework able to dynamically assess cyber risk based on a continuous risk monitoring. It is also incorporating socio-economic impact assessment and is building on current state of the art methodologies and tools, leveraging best practices from multiple industries.

Risk management frameworks lack integrated agile methodology to analyse cyber risks. There is also demand for the continuous monitoring of related events and dynamic assessment of risk,

To give the best answer when cyberattack threatens valuable assets, a reliable support for decision-making is needed. WISER helps to adopt the correct measures while maximizing the ROI.

Objectives

WISER faces this changing risk landscape by focusing on areas that complement each other to make progresses beyond the state of the art:

1. Provide tools that enable continuous cyber risk monitoring solution, e.g. access to relevant freshly updated information, in order to feed module for continuous assessment of risks.

2. Multi-level risk assessment, focusing not only at ICT system (or combination of interdependent systems), but also considering the business processes or services that depend on it, and including also the implications of cyber disruptions at a wider level, considering all the societal impact (in public services, industrial capacity, resource availability for the functioning of societies and the economy, and in general well-being of the population).

3. Provide decision support tools to facilitate selection of optimal mitigation options based on integrated overall risk impact (IT, societal, business…).

Elena González

Elena González is Exploitation and Dissemination Manager at Atos.

She is involved in the WISER Project, in exploitation/ dissemination tasks.

email: elena.gonzalez@atos.net

Antonio Álvarez

Antonio Álvarez is Research and Innovation Consultant at Atos. He is involved in the WISER Project participating in technical, dissemination and management tasks.

Methodology and tools

To reach this new level in cyber security WISER will develop a methodology, based on best practices, with a set of taxonomies for cyber risk concepts, as well as a set of cyber risk checks and metrics.

The cyber risk framework will have to reflect the changes in cyber threat climate, not only at the level of information systems but also at the level of business processes and services that run on top of these processes, as well as societal services and support functions depending on the given ICT system.

It will provide decision support tools to facilitate selection of mitigation options based on dynamic and integrated risk impact assessment at different levels (qualitative and quantitative techniques for assessing the level of cyber risk exposure). Focus is on integrating technological advancements related to implementation of the continuous monitoring, assessment and mitigation mechanisms for cyber risk management in real time.

Focus on SMEs

WISER also has focus on SMEs needs that often do not have means to handle cyber risk with advances methodologies & tools. WISER will deliver a pre-packaged risk management solution for SMEs that combines sophistication of the solution with simplicity of use and adoption by the end-user. Among all the different goals defined in WISER, the most important one, having the highest priority, is to make cyber security affordable for SMEs.

WISER Pilots

From the very beginning of the project, WISER project will develop its activities in a market driven and market oriented manner. The goal is to make possible the early roll-out and application of WISER in different verticals. The project has started with the engagement of 10 different companies from a range of sectors. These companies will provide an overview of their business goals, their business processes and their current practice regarding cybersecurity in order to identify their emerging and future needs, and shape the product according to operational requirements.

Besides, the definition of the project has also considered three different full-scale pilots carried out with the consortium partners, playing the role of early adopters. By doing this, valuable feedback will be obtained early in the project and the likelihood of successful marketability of WISER will be notably increased.

WISER Consortium

WISER is executed by a consortium of technology providers, risk management experts, market experts and service providers for piloting:

- ATOS (Spain)
- Trust-IT (UK),
- SINTEF (Norway)
- XLAB (Slovenia)
- AON (Italy)
- REXEL (France)

If you would like to know more about WISER please visit our website:

www.cyberwiser.eu

WISER has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement no 653321

SECRET EU project: Security of Railways against Electromagnetic Attacks

This FP7 EU project ended in November 2015 and delivered a series of recommendations to better prevent and protect rail infrastructure from intentional electromagnetic interferences

Cyber threats are an increasing concern for every business. Barely a week goes by without new reports of sophisticated IT systems – even of the largest organisations or intelligence services – falling victim to cyber-attacks. It was therefore important to check what further precautions could be taken within the railway sector should the need arise.

In this context, the project SECRET was selected by the European Commission as part of its fourth call for 'transport' proposals, under the 7th Framework Programme for Research and Development.

The SECRET EU project addressed the issue of electro-magnetic (EM) attacks targeting rail infrastructure and contributed to reinforce the signalling systems. The EM attacks considered in SECRET were low power intentional interferences that could break the communication links and affect voice communication and the good transmission of signalling information.

The SECRET consortium came together to assess the risks and consequences of EM attacks, to identify preventive and recovery measures and to develop protection solutions to ensure the security of the rail network, subject to intentional EM interferences, which can disturb a large number of command-control, communication or signalling systems.

SECRET objectives

- identify the vulnerability points at different levels (from the electronic to the systemic vision)
- identify EM attack scenarios and risk assessment (service degradation, potential accidents, economic impacts…)
- identify public equipment which can be used to generate EM attacks
- develop protection rules to strengthen the infrastructure (at electronic, architecture and systemic levels)
- develop EM attack detection devices and processes
- develop resilient architecture able to adequately react in case of EM attack detection
- extract recommendations to ensure resiliency and contribute to standards

SECRET Approach

The project illustrated the risk by implementing some electromagnetic attacks and analysing their effects, thereby inciting the different railway actors to work together to strengthen the resilience of a system that must remain effective and safe for the serenity of our society.

Then, the project opened ways to resilience solutions regarding this type of attack. Preferring to avoid unconstructive and alarming rhetoric, which is unjustified as the European railway system is above all a very safe means of transport, the project identified and proposed strategies in which each actor would be able to inspire itself in order to act towards resilience.

The strategies developed mainly concern:

- The tests that can be performed to assess the susceptibility of individual network components dealing with intentional interferences and allowing each designer, integrator or operator to build, evaluate and compare the susceptibility of these products.

Virginie DENIAU
SECRET technical coordinator

Virginie Deniau holds a PhD in Electronic University of Science and Technology of Lille. She is researcher at IFSTTAR (French Institute of Science and Technology for Transport, Development and Networks) since July 2003. She conducts works in the field of electromagnetic compatibility (EMC), the characterization and modeling of EM transportation environments, and the immunity test methodologies for embedded systems. Since 3 years, she is involved in hardening the transport systems vis-à-vis the cyber attacks, such "electromagnetic attacks.". She is also chair of the URSI Committee E (Electromagnetic Interference) French section.

e-mail: virginie.deniau@ifsttar.fr

Marie-Hélène BONNEAU
Security Advisor at the UIC Security Division, leader for dissemination in the SECRET Project

e-mail: bonneau@uic.org

- The methods of detection of electromagnetic attacks that are essential for several reasons: Detecting means to be able to demonstrate that we have been a victim of an electromagnetic attack, detecting avoids confusing an electromagnetic attack with a technical failure which could unduly jeopardize the operator, who could initiate unnecessary diagnostic inquiries. And, finally a reliable detection can instigate a fast and appropriate reaction to the threat.

- The resilient architecture which is a compulsory issue when we consider a critical infrastructure which is a network. The resilient architecture has to ensure the maintenance of communication for the transmission of critical information, thus maintaining the control of the network. We worked on an adapted architecture permitting us to assess the impact of certain technological solutions on reliability and responsiveness.

SECRET results

About 40 recommendations at organisation, standardization and technical levels have been identified, classified and described. These recommendations are organised in three categories described below.

The first category called "**prevention from EM jamming effects**" groups the recommendations which can be adopted permanently and can permit to inhibit or reduce the impact of jamming signals (precautionary principle). In order to prevent from jamming attacks on the railway environment the first recommendation that can be done is the provision of risk assessments. The Bow-tie and TVRA were used in Secret to assess railway incidents and railway communication system incidents. Operational recommendations have also been identified like minimising train emergency brake impact. Finally a series of engineering recommendations focusing on the system architecture, the radio network features, rolling stock, train antenna and the BTS (Base Transceiver Station) antenna were defined.

The second recommendation category is dedicated to the **EM attack detection solutions**. It presents the different detection techniques which were studied in SECRET and gives their potential applications. The different detection techniques are based on the monitoring of different parameters like the Error Vector Magnitude (EVM), frequency spectrum occupation, excess of energy in the operated band and the Quality of Services (QoS). These techniques were studied for on board train, on the track side and in train station conditions.

The third category is "**Mitigation of EM jamming effect**". In this category, the recommendations are focused on solutions which can be activated temporally when EM jamming is detected. All recommendations in this category are classified as operational considering their activation will depend on the operational context. Some of the recommendations focus on temporarily improving the system radio coverage. These recommendations shall meet the EIRENE specifications to ensure a minimum received radio level for voice or ETCS applications. The recommendations are not necessarily linked and, most of the time, can be implemented separately. Such temporary recommendations require important guidelines to decide the conditions in which they can be used by taking into account the environmental criteria: jamming location, train location, level of communication degradation, railway lines category, and presence of alternative radio bearer. Their activation can be made automatically using the jammer detection system or manually from the train or control centres.

Conclusion

In the European railway sector, the homogenisation of network technologies and the increasing use of wireless communications have made the scenario of an EM attack very likely. The communications could potentially be jammed, with trains being delayed, blocked or even diverted.

The secret project has contributed to this problematic by assessing the real risks concerning EM attacks, identifying areas for strengthening the railway network and developing detection solution and to designing a resilient architecture. As a result the SECRET white paper gives an overview of the recommendations on preventive and recovery measures as well as the suitable methodology to evaluate and mitigate EM attacks in the railway context. Finally, the recommendations consider the possible evolutions of the system architecture following the introduction of next generation technologies.

The next step is to take into account these recommendations (especially regarding the system architecture permitting resilient reconfiguration) in the various existing standardisation bodies (especially ETSI) and to incorporate the results into International Railway Standards.

The project was coordinated by the French research centre IFSTTAR and the consortium was composed of 9 other members: Research centres (Fraunhofer Institute IAIS from Germany, Politecnico di Torino from Italy, University of Liege-Institut Montefiore from Belgium, University of the Basque Country-UPV/EHU, ZANASI & Partners from Italy, industries (ALSTOM TRANSPORT S.A. from Belgium, TRIALOG from France) and railways representatives (SNCF – French railways and UIC – International Union of Railways based in France).

If you would like to find out more about the project please visit our website at www.secret-project.eu

Foreign policy's role in improving critical infrastructure protection in cyberspace

Foreign policy and diplomacy are enablers of international cooperation, which is essential for countering global cyber risks to critical infrastructures. Switzerland is committed to promoting the three core components of international cooperation: a framework of rules, trust and capacity.

Three components of international cooperation

When it comes to improving Critical Infrastructure Protection (CIP) in cyberspace, foreign policy and diplomacy play an important role. Because of its global and almost ubiquitous nature, cyberspace creates significant interdependences between critical infrastructures located in different states.

No country alone can guarantee the security of its critical infrastructure in isolation. We therefore need close and efficient international cooperation to tackle the ever-growing risks emanating from the malicious use of Information and Communication Technologies (ICT). It is the role of foreign policy and diplomacy to enable this cooperation.

In Switzerland, the Federal Council recognised in its National Cyber Strategy (NCS) the importance of international cooperation to improve protection against cyber risks. Within the Swiss federal system, close-knit cooperation among different actors to ensure security takes place quite naturally. This also needs to be promoted at the international level.

A cooperative approach with three pillars is required for greater security in the cyber domain: a clear framework of rules, trust among the involved actors, and a minimum level of capacity to fight threats and cooperate effectively. These three elements are at the core of the Swiss cyber foreign policy and this article outlines how they are promoted.

Framework of rules

For a secure cyberspace, we need first and foremost a clear framework of rules that defines what is acceptable behaviour in cyberspace.

In Switzerland's view, the existing international legal order provides a strong foundation for the rules in cyberspace. International law is equally applicable online as it is offline. This view has also been confirmed by the UN Group of Governmental Experts (UNGGE).

A clear framework of rules is particularly important for the security of critical infrastructures, which are increasingly becoming the targets of cyber-attacks. In the case of critical infrastructure, these attacks can have particularly devastating effects.

International law is directly relevant for purposes of CIP. General principles of international law, such as the principle of non-intervention or the prohibition of the use of force, outlaw cyber-attacks on critical infrastructure that would reach a certain threshold of severity or intensity. Other bodies of international law also provide for specific legal protection. As an example, international humanitarian law forbids the parties of an armed conflict to attack certain critical infrastructures, namely dams, dykes and nuclear electrical generating stations. Such provisions also apply to cyber-attacks.

In addition to the legal framework, voluntary, legally non-binding norms of responsible state behaviour can further clarify the framework of rules in cyberspace. Because these are political and not legal in nature, they can often be negotiated in a more flexible and timely manner, which is a significant advantage in the quickly evolving cyber domain.

Ambassador Benno Laggner

Ambassador Benno Laggner is currently the Head of the Division for Security Policy and Ambassador for Nuclear Disarmament and Non-Proliferation in the Swiss Federal Department of Foreign Affairs.

Prior to this appointment, Benno Laggner was the Deputy Chef de Cabinet of the President of the 65th session of the United Nations General Assembly. Earlier postings included serving as Head of the UN Coordination Unit in the Federal Department of Foreign Affairs (2007-2010), as Head of the Political Section at the Swiss Embassy in Berlin (2004-2007) and as Head of the Political Section at the Permanent Mission of Switzerland to the United Nations in New York (2000-2004). Benno Laggner holds a Master's Degree in International Relations (University of St. Gallen, Switzerland) and also completed postgraduate studies in European Affairs at the College of Europe in Bruges, Belgium.

In its report of July 2015, the UNGGE recommended for consideration a first set of norms of responsible state behaviour for cyberspace. One of these norms provides specific protection for critical infrastructures (see box below). This constitutes an important recognition of the special protection that critical infrastructures should enjoy in the view of the international community.

Building upon this norm, we should now work towards clarifying its scope of application and explore mechanisms that would ensure compliance with it.

> *"A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."*
>
> UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (July 2015, A/70/174)

Trust

A second prerequisite for a more secure cyberspace is an adequate level of trust among the involved actors. Since the anonymous nature of cyberspace leaves much room for ambiguity, building confidence through transparency and cooperation is vital to reduce the danger of miscalculation, misperception and misunderstanding. Trust in a way is the glue holding the decentralised network that cyberspace constitutes together.

Switzerland is therefore engaged in efforts to apply the tool of Confidence-Building Measures (CBMs) to cyberspace. CBMs were invented by the Organisation for Security and Cooperation in Europe (OSCE) in the context of the East-West conflict four decades ago. It is therefore no coincidence that the OSCE in 2013 was the first regional security organisation to formally adopt CBMs in the realm of cybersecurity, too.

The initial set of OSCE CBMs aims at increasing transparency and confidence. To this end, the 57 participating States committed to exchange information on their cybersecurity policies, organisation and strategy. They also committed to defining national contact points in order to facilitate cooperation.

Because cybersecurity depends upon trust and cooperation between all relevant actors it is important to also include non-governmental actors in CBM activities. During the Swiss Chairmanship of the OSCE in 2014, Switzerland organised an event on cyber CBMs. For the first time, the private sector and critical infrastructure operators were also included in the confidence-building activities between states. It is important to further develop this multi-stakeholder cooperation.

Switzerland will continue to promote cyber CBMs, both within the OSCE context and beyond. At the OSCE, we push towards implementation of the initial set of CBMs, while also contributing to the adoption of additional measures, which would take the cooperation in this forum to the next level.

Given the global nature of cyberspace, it is also important to engage in confidence-building measures across regional boundaries and organisations. This is why we reach out to actors in different regions of the world, for example by supporting a regular dialogue between European countries and China, with participants from government but also the private sector and academia.

Capacity

The third element that is necessary for securing cyberspace is the capacity to do so. We understand capacity as a broad concept: It clearly includes technical skills and resources, but also a strategic and policy framework that guide states' efforts to tackle cyberrisks. Capacity further includes the ability to engage in international processes and cooperation, without which it is impossible to cooperate.

It is important to highlight that capacity-building in the cyber domain is in the interest of all states. In cyberspace, we are only as secure as the weakest link in the network – and that is particularly true for critical infrastructure.

Switzerland therefore contributes to the global effort to raise the level of capacity in cybersecurity. Last year, Switzerland became a founding member of the Global Forum on Cyber Expertise (GFCE) alongside more than 40 other states and actors from the private sector committed to boosting global capacity-building efforts.

One project that Switzerland supports in the GFCE is the "Meridian" initiative, which aims at making best practices and policy recommendations in the field of Critical Information Infrastructure Protection (CIIP) available to a wider range of actors, thereby promoting CIIP throughout the world.

Switzerland also launched the Geneva Internet Platform (GIP) which pursues the objective of empowering actors from all stakeholder-groups to actively participate in the relevant international processes. To this end, the GIP teaches online courses in the field of digital policy and provides an online policy observatory that allows all interested actors to follow the current policy debates and international processes (see http://digitalwatch.giplatform.org/). Finally, the GIP is also a neutral platform for debates and discussions.

Conclusion

Technical and defensive measures are not sufficient to improve the security of CIP in cyberspace. Geared towards the decentralised network that cyberspace constitutes, a truly collaborative approach to security is necessary. This means that we must closely cooperate across country borders and regional boundaries.

Switzerland is committed to advancing this approach by promoting a solid and globally shared framework of rules, fostering trust among the different actors and contributing to building capacity worldwide.

Understanding Systemic Interdependencies

The increasing complexification of our society is creating and tightening interdependencies among all its component systems; it is thus crucial to understand the consequences of such evolution. We will discuss how such interdependences can lead to systemic risk, i.e. to the emergence of unforeseen behavior that could have not been predicted from the understanding of the single systems. In this chapter we will pose some examples of systemic interdependencies and introduce some tools and models that allow to understand their possible consequences in socio-technical systems; we will then revise some reference literature with particular attention to complex networks approaches.

The structural organisation of the society in the countries of elevated development is experiencing a terrific enhancement of its complexity. Tools and devices employed in our ordinary life are becoming increasingly more technological and smart. Both the materials and the technology involved are constantly improved, whilst a cyber layer is becoming an essential component of smart devices. In general, we are immersed in a world consisting of interdependent systems, which functioning critically depend on each other (like the Internet depending on the electric power network and vice versa). Those different systems form actually a "System of Systems" (SyoSy). Single domain systems are strongly engineered infrastructures and, to some extent, we do understand their functioning and related risks; however the interaction among such systems lays ground for new emerging phenomena. In fact, the ability to reduce everything to simple fundamental laws does not imply the ability to start from those laws and reconstruct everything: such constructionist hypothesis breaks down when confronted with the twin difficulties of scale and complexity. At each level of complexity, entirely new properties appear and we are nowadays convinced that the whole becomes very different from the sum of its parts [1]. The former considerations do apply to all different sectors of modern society; however they become more stringent when applied to Critical Infrastructures (CI) [2]. The huge concentration of people in the metropoles and the general increase of the world population requires giant provisions of basic goods, such as both edible and sanitary water, food, electric energy, gas, fuels etc. To securely deliver and distribute such a variety of services represents one of the main issues in modern society. It is worth noting that the term infrastructure here is employed in the broad sense referring to the synergistic functioning of the allocated humans and devices. Human intervention can be "a priori" while defining and assessing "contingent plans" or "ex post" by real time management of the operational setting of the infrastructure. There are several reasons for which static rules are not sustainable to manage infrastructures in the long run; among them the following are worth mentioning: the advent of "Smart Society" including the Internet of Things (IoT); the improvements in the materials and devices; the rise of new types of attacks (new threats) both on physical and cyber side; the discovery of new vulnerabilities of the system; the reduction/increase in the allocated funds or humans; the increase in the demand; and even possible climate changes.

During last decades, the owners and handlers of infrastructures have reached a very high level of performance concerning the management, the protection and the defence. They are able to face most of the predictable and even unpredictable adversities, behaving according to predefined rules coded in the "contingency plans" and practiced during continuous exercises. However, most of the countermeasures foreseen to deal with contingencies do rely on the availability of other commodities or services. For instance, small fires can be doomed by autonomous systems, yet larger ones require the intervention of firemen rescue teams. Similarly, infrastructures providing communications can stand short electric power outages by resorting to their UPS (Uninterruptible Power Supplies) and their fuel reservoirs, yet long enough ones require either re-fuelling or recovery of the Electric Systems (ES).

Gregorio D'Agostino is Senior Scientist scientist at ENEA. He is visitor Scientist at London Institute of Mathemathical Studies. He is al so president of the Netonets Association.
e-amail:
gregorio.dagostino@enea.it

Antonio Scala is Staff Scientist at CNR, Professor at Institute of Advanced Studies IMT (Lucca) and Visitor Scientist at London Institute of Mathematical Studies

He will also chair Critis 2017 conference in Lucca.

Similarly, telecommunications can be reactivated after a main event (such as a earthquake or a flood) providing the transports (mainly highways and roads) are available to allow mobile bridges appropriate allocation and deployment "in situ".

Generally speaking an infrastructure is said to depend on one other when the second is required for normal functioning of the first or to enforce contingency plans upon undesired events. When two infrastructures do depend on one other they are said to be "mutually or reciprocally dependent". Sequential dependence is an asymmetrical chain of one way interactions. When different infrastructures do exhibit a series of dependencies in closed chains they are said to be interdependent. Interdependence represents a resource for efficient provision of services, since it allows savings and allocation "on demand", yet it may hid "systemic risks". "Systemic interdependence" is the term we employ to refer to indirect or hidden dependencies in a System O Systems. The Systemic Interdependence implies a "systemic risk", that is one not strictly related to a part of the system, but just arising globally, while the different parts function together.

The term "systemic risk" arose to the chronicles after 2008 crises in finance. No company was exhibiting any apparent problem, nevertheless a liquidity lack triggered the largest financial crisis after 1930. Generally speaking, "systemic risk" may be defined as a global risk not related to a vulnerability of a specific part of the system, but to its "global" behavior. The system may collapse as a whole entity while none of its components appears vulnerable. The reason is basically related to interdependency: banks as well as stocks depend on each other and a fall in the prices of one results in that for another, thus possibly leading to a domino effect. In general, the complexity of a system lays the grounds for the possibility of systemic risk, i.e. for system-wide failures that cannot be predicted from the analysis of the single components, but emerge from the interdependencies of the constituting system(s). Thus, systemic interdependencies are a central issue in our world.

Systemic interdependencies have been shown to be relevant even in the human body where Network Physiology reveals relations between network topology and physiological function [21]. In this case one does not observe specific symptoms but a complex global syndrome. Again, details on functioning of specific organs (and relative treatments) are not enough to deal with the general pathology.

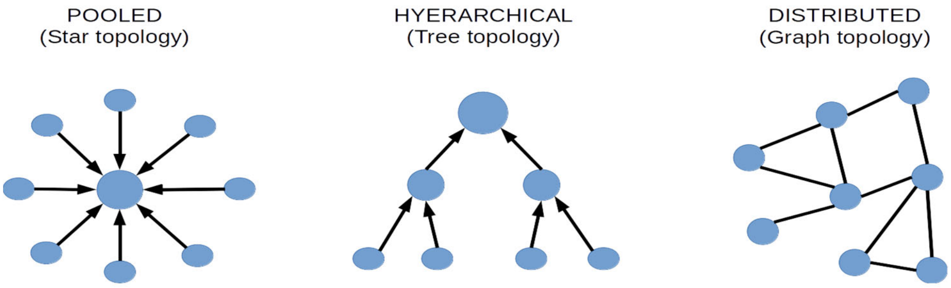


Figure 1 " The different basic topologies for systemic interdependences. Notice that the natural way to represent such topologies is in the form of graphs or networks, where nodes represents the systems, arcs represent mutual relations and oriented arcs (arrows) represent dependencies "

During last six years the authors have devoted a significant part of their efforts to understand systemic interdependence and to build up a community merging experts and scientists to deal with the problem from both the academic and the applied perspectives. This resulted in the Netonets organisation (www.netonets.org). In the following, we will explicit some models for systemic interdependencies that highlight the emerging properties of a SyoSy.

Models for interdependence

There are several organisational models to integrate different units into a coordinated system of systems. Pooled interdependence is the lowest form of interdependence resulting in the least amount of conflict. Departments (or single infrastructure in our case) do not directly depend or interact with one another; however they do draw resources from a shared source. This model is rarely representative of real systems where pairwise provision-demand agreements dominate. More complex organisations normally imply pair (and in some rare case multiple) interactions. In principle, there could be a thinking entity responsible to plan these interactions (and in the future there will possibly be); however, generally speaking the different owners of the infrastructure will establish agreements to receive and/or provide services or commodities. In other words the systems are self-assembled according to individual goals. It is worth noting that even if the pooled interdependence is a very simple one it may explain several phenomena, such as for instance a volatility crisis in a network of loans. Normally several bank and financial institutions have both credits and debits. The provide credits when the beneficial owns goods (real estates etc) or other valuable assets. When looking at the system locally (that is from any single unit perspective), no problem is seen. However it may happen that one (even a small one) o the entity needs some liquidity and hence claims its credits; this may induce a cascading effect on the whole system [3]. The effect is also predicted assuming that all entities take their money from a common source that experiences a deficiency. This represents a kind of "mean field approximation" to the real situation where credits are claimed on a specific network. The same applies to the electric system. When an extra power is injected it may produce a chain of faults; however, even homogeneous distribution of the extra power, that corresponds to both the mean field approach and to simplified pooling dependence, may induce cascading effects [4]. These are typical systemic risk problems: the system appears in perfect shape locally and yet it experiences collapse.

Generally speaking when modelling a system of systems one has to perform basically the following steps:

1. Turn all the information of the systems into a treatable representation.
2. Select the appropriate level of abstraction (including granularity) of possible representations, depending on the goal of the analysis
3. Analyse the system to outline the interdependencies of the different component systems.
4. Simulate the system or run the developed analytical tools.
5. Provide a means to outline the emergent behaviours of the system. This step is just to understand the systemic behaviour.

Models can be classified according to general types. Among several of them we will discuss the most diffused models with a focus on those employed to study systems of infrastructures.

A very neat application of such representation is represented by the "Design Structure Matrix" [5], a very useful tool for managing and coordinating projects. A DSM lists all the information exchange, interactions, and dependency patterns among the constituent element of a project (subsystems/activities). DSMs can be broadly distinguished in two main categories: static and time-based [6]. Static DSMs represent systems of systems where all of the elements exist simultaneously and are equivalent an adjacency matrix or a graph. The main analysis tool for static DSMs are usually clustering algorithms [7] that help separate the systems of the SyoSy in groups that are mostly related. On the other hand, time-based DSMs are directed graphs and can be thus analysed using sequencing algorithms [8].

Another approach originates from works of economists of the fifties of the last century: the Nobel laureate Leontief introduced a simple linear model for interaction of the different sectors in economy [9]. Moving from similar reasoning a simple approach, based on inoperability, has been developed to describe interdependent systems. In the Inoperability I/O Model (IIM) [10] each infrastructure is modelled by a node i in a network with a given "inoperability" Qi ∊ [0, 1] measuring to what extent the node i is performing the function it is devised for. These ideas were further developed leading to stochastic differential equations describing the phenomenon:

$$dQ_i = \sum_{j=1,N} h_{ij}\, Q_j \;\; + \gamma_i\, dD_A$$

For some further information one can see [25,26]. In the simple case of constant disturbance, the system, with initial inoperabilities Qi(0) tends to an equilibrium Qeq = H−1γ(0) □d(0) which depends (linearly in this case) on the impact of the external disturbance d (disturbance per unit time) on the inoperabilities of the different components. Figure (2) shows how starting from a disturbance localised on one infrastructure it may spread to the others. Again this surprising effect is due to systemic interdependence.

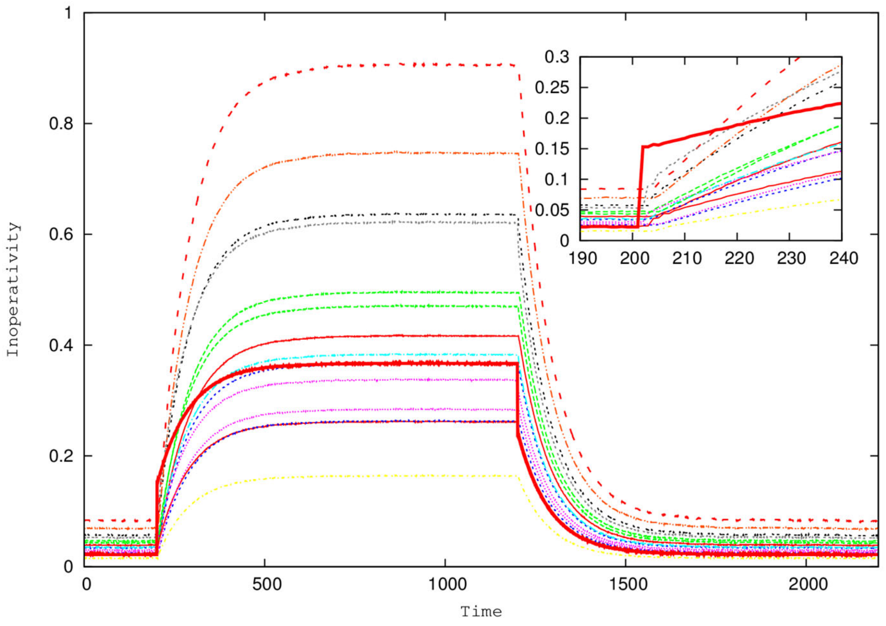


Figure 2 The typical evolution of inoperabilities upon a disturbance of one component only (red bold line). Inset: initial evolution of the system after the shock. Due to systemic interdependencies, the fault propagates and shortly after the failure the component suffering the maximum inoperability is not the one subject to the initial fault.

There are several other examples of model where the systemic interdependence plays a crucial rule in the emergent behaviour. Possibly one of the most promising is the group of "Fault propagation models" inspired by epidemics. In this case each component is given a Boolean value representing its operability. Null operability is transmitted to those components that are directly connected. The typical example is given by local "fault propagation"; again each component can be in a operable or non operable state; there exists a probability rate of restoring normal behaviour and a probability rate that a fault induces an other one on a component that depends on it. We can name this model VIV (Vulnerable, Inoperable, and Vulnerable). From the mathematical point of view it would just correspond to the classical SIS (Susceptible, Infected, and Susceptible) model of epidemiology. If one further assumes that after the first fault the lesson is learned and a component cannot undergo the same type of fault, there exists a third state to be accounted corresponding to invulnerable nodes. Hereby, this simple model will be referred to as VIP (Vulnerable, Inoperable, and Patched): it corresponds to the classical SIR (Susceptible, Infected, Recovered) model in epidemics. Since several different independent faults may take place, one should deal with competitive multiple epidemics spreads.

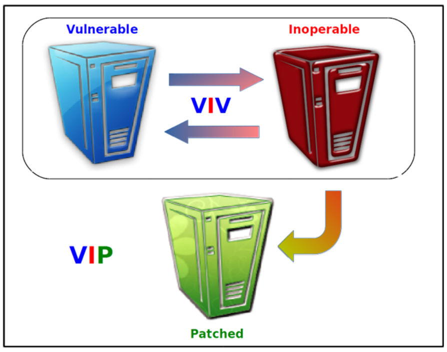


Figure 3 *V IP* Model: Each platform in a network can be in one of three states: Vulnerable (Susceptible), Inoperable (Infected) and Patched (Recovered).

The evolution is again stochastic and it is dominated by the healing rate roughly corresponding to the Mean Time to Repair, which is a common index of resilience capability of the infrastructure, and by the infection rate that corresponds to the mean time to fault that is also a common metric for infrastructural vulnerability.

According to the ratio between infection and healing rate, the initial fault may spread all over the network or extinguish. The critical value at which this phenomenon takes place is the epidemic threshold of the system and it depends on the **topology** of the network only. It has been demonstrated that the inverse of the maximum eigenvalue of the adjacency matrix is lower bound for the epidemics threshold, [12, 13]. The threshold can also be estimated by neglecting correlations [14].

Diffusion is the most fundamental dynamical mechanism allowing the propagation on a system [15]. It describes the propagation of any scalar quantity on the system through random exploration. Generally speaking the diffusion-like equations can be applied to different fields including synchronisation among different infrastructures. These models were also applied to interdependent infrastructure and it can be proven that for small couplings among the infrastructures, the SysoSys behaves as components were separate; while for large couplings the SysoSys behaves as a whole [16]. In general, synchronisation is the capability of the systems to function in unison and is often modelled with the non-linear Kuramoto model [17] (especially for electric systems); it is an example of a non-linear dynamics where special tools like the master stability function [18] must be applied. Ref. [19] provides a wide review of synchronisation on networks.

Conclusions

The interest in systemic interdependencies is witnessed by the blossoming of the related field of networks of networks: over the course of 2014, one book [22] and several reviews [23, 24] have been published and a major EU project (MULTIPLEX - Foundational Research on MULTIlevel comPLEX networks and systems www.multiplexproject.eu/) involving 23 research groups and producing more and resulting in almost two hundred publications has ended in 2015.

Beside the efforts in understanding the systemic behaviour, the research in the field is spreading along several directions. Dealing with real infrastructures requires models to assess operational parameters and the systemic approach cannot provide such information. To such an aim, agent based models can be introduced to simulate the behavior of the different infrastructures (or their components) and interdependence analysis provides information on how they interact. Since the systems are brought around some desired stable condition, the simulation are carried in the discrete event paradigm which consists in finding novel equilibria after undesired events. In some rare case one may employ accurate domain specific codes to simulate the different infrastructure in details while using the interdependencies as reciprocal boundary conditions. This type of approach is named "federated modelling and simulation". The fundamentals of all the previous approaches can be found in the references above [22, 23, 24]. However, at the present stage, models catching the emergent behaviors are not able to provide applicable recipes to manage real infrastructures and systems of systems; on the other hand, detailed models can mimic the accurate evolution of the systems often hiding the global picture.

Our society in experiencing a remarkable change due to the advent of the smart society, that is the introduction of computer aided networks to control any activity of our life from domotics and internet of things (IoT) to smart grids, buildings, cities and nations. The theory of complexity may enhance the awareness in the scientific community and hopefully in the whole society of the systemic risk that is not limited to finance or other known systems, but is a general mechanism related to the increasing amount of interactions among people, systems and devices needed to implement a smart society.

Acknowledgements

GD acknowledges interesting discussion with participants to the CIPRNET network of excellence. The authors acknowledge interactions within the MULTIPLEX project.

References

[1] P. W. Anderson. More is different. *Science*, 177(4047):393–396, 1972.

[2] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25, 2001.

[3] Xuqing Huang, Irena Vodenska, Shlomo Havlin, and H. Eugene Stanley. Cascading failures in bi-partite graphs: Model for systemic risk propagation. *Sci. Rep.*, 3:–, February 2013.

[4] Sakshi Pahwa, Caterina Scoglio, and Antonio Scala. Abruptness of cascade failures in power grids. *Sci. Rep.*, 4:–, January 2014.

[5] SD Eppinger. Innovation at the speed of information. *Harvard Business Review*, 79:149–158, 2001.

[6] T.R. Browning. Applying the design structure matrix to system decomposition and integration problems: a review and new directions. *Engineering Management, IEEE Transactions on*, 48(3):292–306, Aug 2001.

[7] Vladimir Estivill-Castro. Why so many clustering algorithms: A position paper. *SIGKDD Explor. Newsl.*, 4(1):65–75, June 2002.

[8] S.D. Eppinger and T.R. Browning. *Design Structure Matrix Methods and Applications*. MIT Press, Cambridge, 2012.

[9] Wassily W. Leontief. *Input-Output Economics*. Oxford University Press, 2nd edition, 1987.

[10] Kenneth G. Crowther and Yacov Y. Haimes. Application of the inoperability inputoutput model (iim) for systemic risk assessment and management of interdependent infrastructures. *Systems Engineering*, 8(4):323–341, 2005.

[11] Stefano Battiston, Michelangelo Puliga, Rahul Kaushik, Paolo Tasca, and Guido Caldarelli. Debtrank: Too central to fail? Financial networks, the fed and systemic risk. *Sci. Rep.*, 2:–, August 2012.

[12] Yang Wang, Deepayan Chakrabarti, Chenxi Wang, and Christos Faloutsos. Epidemic spreading in real networks: An eigenvalue viewpoint. In *22nd Symposium on Reliable Distributed Systems (SRDS 2003), 6-8 October 2003, Florence, Italy*, pages 25–34, 2003.

[13] Cong Li, Huijuan Wang, and Piet Van Mieghem. Epidemic threshold in directed networks. *Phys. Rev. E*, 88:062802, Dec 2013.

[14] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic spreading in scale-free networks. *Phys. Rev. Lett.*, 86:3200–3203, Apr 2001.

[15] G. D'Agostino, A. Scala, V. Zlatic, and G. Caldarelli. Robustness and assortativity for diffusion-like processes in scale-free networks. *EPL (Europhysics Letters)*, 97(6):68006, 2012.

[16] J. Martin-Hernandez, H. Wang, P. Van Mieghem, and G. D'Agostino. Algebraic connectivity of interdependent networks. *Physica A: Statistical Mechanics and its Applications*, 404(0):92 – 105, 2014.

[17] Yoshiki Kuramoto. Self-entrainment of a population of coupled non-linear oscillators. In Huzihiro Araki, editor, *International Symposium on Mathematical Problems in Theoretical Physics*, volume 39 of *Lecture Notes in Physics*, pages 420–422. Springer Berlin Heidelberg, 1975.

[18] Louis M. Pecora and Thomas L. Carroll. Master stability functions for synchronized coupled systems. *Phys. Rev. Lett.*, 80:2109–2112, Mar 1998.

[19] Alex Arenas, Albert Diaz-Guilera, Jurgen Kurths, Yamir Moreno, and Changsong Zhou. Synchronization in complex networks. *Physics Reports*, 469(3):93 – 153, 2008.

[20] Ludwig von Bertalanffy. *General System theory: Foundations, Development, Applications*. New York: George Braziller, revised edition 1976: isbn 0-8076-0453-4 edition, 1968.

[21] Amir Bashan, Ronny P. Bartsch, Jan. W. Kantelhardt, Shlomo Havlin, and Plamen Ch. Ivanov. Network physiology reveals relations between network topology and physiological function. *Nat Commun*, 3:702–, February 2012.

[22] Gregorio D'Agostino and Antonio Scala, editors. *Networks of Networks: The Last Frontier of Complexity*. Understanding Complex Systems. Springer International Publishing, 2014.

[23] S. Boccaletti, G. Bianconi, R. Criado, C.I. del Genio, J. Gómez-Gardeñes, M. Romance, I. Sendiña-Nadal, Z. Wang, and M. Zanin. The structure and dynamics of multilayer networks. *Physics Reports*, 544(1):1–122, 2014. The structure and dynamics of multilayer networks.

[24] Mikko Kivelä, Alex Arenas, Marc Barthelemy, James P. Gleeson, Yamir Moreno, and Mason A. Porter. Multilayer networks. *Journal of Complex Networks*, 2014.

[25] G. D'Agostino and A. Scala "Sistemic Interdependence" in "Handbook of Science and Technology Convergence" by W- S. Bainbridge, and M. C. Roco - Springer International Publishing 2015

[26] G. D'Agostino, R.Cannata, V. Rosato, "On modelling of inter-dependent network infrastructures by extended Leontief models" LNCS - Critical Information Infrastructures Security 1-13, 2009, Springer Berlin Heidelberg

Layer 2 Encryption: Securing Carrier Ethernet and MPLS Networks against Espionage and Attacks

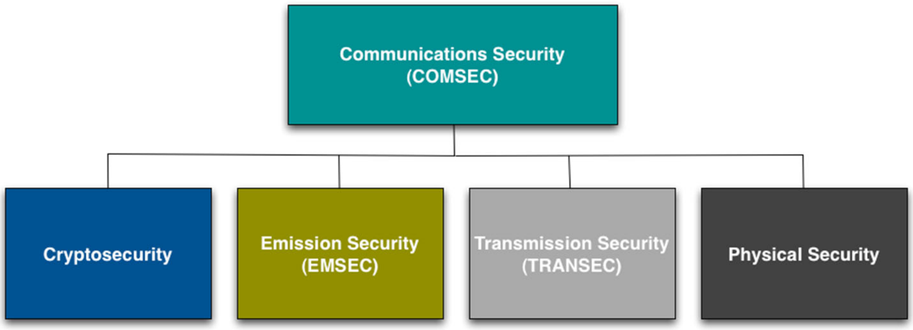
Advanced encryption solutions provide protection for mission-critical data networks at layer 2, 2.5 and 3 of the OSI network protocol stack.

Network Security

In today's world data networks are mission-critical. Metro (MAN) and Wide Area Networks (WAN) handle the data traffic between different sites. Due to their function and the data they carry, MANs and WANs are a prime target for espionage and attacks. Foreign governments, state-sponsored actors, criminals, terrorists and lone actors are increasingly targeting data networks. On their agenda: Espionage, infiltration and disruption. The tapping of network data is unpreventable. It is common practice and the difference in behaviour between state and criminal organizations in that respect is minimal. The goals are used to justify the means. Next to the simple "passive" tapping of networks there is a multitude of possibilities to actively attack networks. It is thus not a question if security measures are needed; it is only a question which security measures are the most efficient and the most secure. Fortunately there are adequate means to minimize the impact or even completely prevent the success of such attacks. It is the combination of crypto security, emission security, transmission security and physical security. The sum of it is known as Communications Security (COMSEC).

Today's network security architecture is based on the principle of network segmentation, also known as zoning. A zone demarcates a logical area within a networking environment with a defined level of network security. Zones are used to define the network boundaries and their associated perimeter defence requirements. Segmentation comes with security and cost benefits. It allows using the most efficient security approach for each zone as security challenges differ dependent on usage scenario and network layer. Metropolitan and Wide Area Networks can either be in separate groups or in a combined segment, as both are static mission-critical networks crossing public ground and often using a third-party network transport infrastructure.

For network security simple data encryption is insufficient. The requirements are substantially higher as the integrity of the transmitted data has to be ensured as well as the authenticity of the sender. On top of that any intrusion has to be detected and prevented. What makes network encryption particularly challenging is the fact that it must not limit network functionality and must cope with network-specific behaviour. This requires additional functionality such as variable encryption offsets and replay windows.


Communications Security (COMSEC)
Cryptosecurity
Emission Security (EMSEC)
Transmission Security (TRANSEC)
Physical Security

Christoph Jaggi

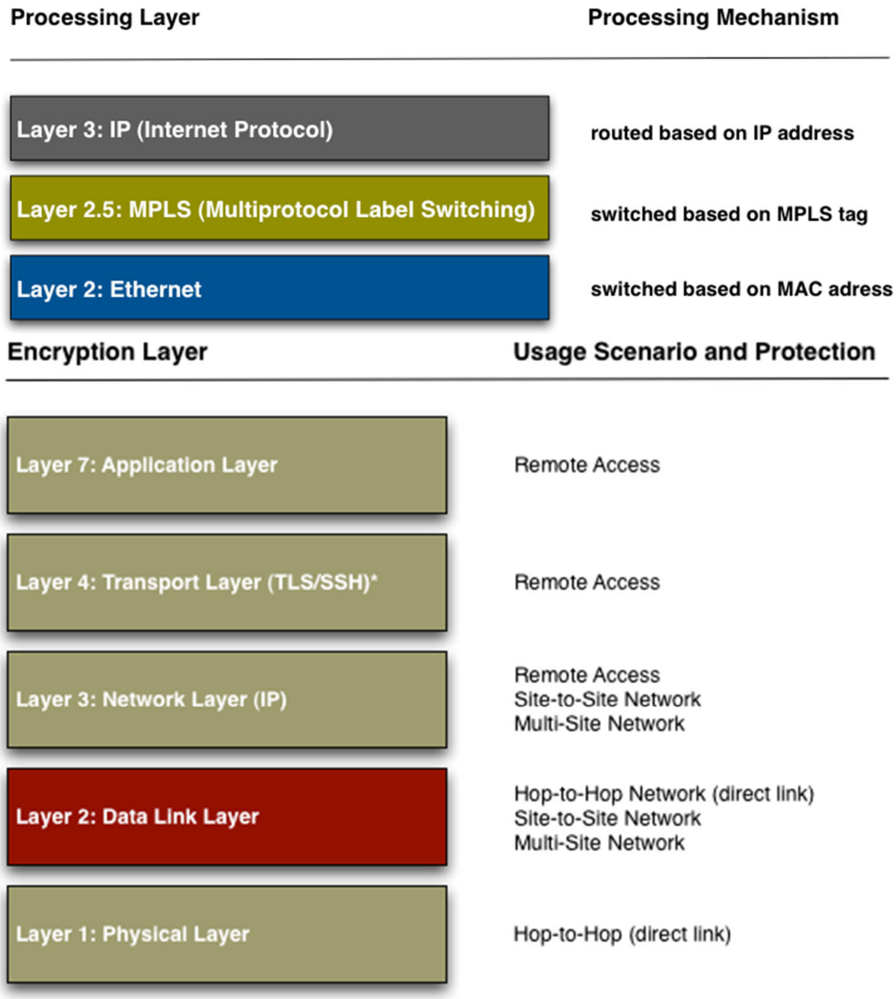
Christoph Jaggi works as technology, strategy and marketing consultant.

e-mail: cjaggi@uebermeister.com

http://www.uebermeisster.com

More detailed information is available on the author's website.

If attacks on an encrypted network fail to provide the desired results, the attacker will concentrate its efforts on the encryption devices. Therefore the security of the cryptographic module must be assured as well as the security of the encryption devices.


Processing Layer
Processing Mechanism
Layer 3: IP (Internet Protocol)
routed based on IP address
Layer 2.5: MPLS (Multiprotocol Label Switching)
switched based on MPLS tag
Layer 2: Ethernet
switched based on MAC adress
Encryption Layer
Usage Scenario and Protection
Layer 7: Application Layer
Remote Access
Layer 4: Transport Layer (TLS/SSH)*
Remote Access
Layer 3: Network Layer (IP)
Remote Access
Site-to-Site Network
Multi-Site Network
Layer 2: Data Link Layer
Hop-to-Hop Network (direct link)
Site-to-Site Network
Multi-Site Network
Layer 1: Physical Layer
Hop-to-Hop (direct link)

*Layer 4 establishes the foundation, but the actual encryption takes place on layer 7

Secure Encryption Device

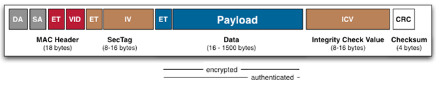
Network security starts with a secure encryption device. It is less complex to secure a dedicated device than a portion of a larger device. Although there are many less access possibilities to a dedicated device than to and within an integrated appliance or a virtual appliance, there is still the requirement to secure every single one of them. The encryption device must be fully secured against attacks from the inside and the outside. This is quite difficult by itself. The more access possibilities, the higher the complexity and the risk of vulnerabilities. Most dedicated appliances are optimised for security and meet the highest assurance requirements. The systems form a closed and tested environment that has been proved to be secure. They only provide the interfaces that are absolutely necessary. For integrated and virtual appliances it is between difficult and impossible to provide such a security level. There are simply too many gateways to be secured.

Secure Keys

Weak or accessible keys compromise any encryption. Key security starts with key generation and continues with key storage and key exchange. Hardware plays again an important role. For generating a secure key you need true random numbers. A properly engineered hardware-based true random-number generator will provide the needed randomness. Software-based random-number generators lack the needed entropy source and can only generate pseudo random numbers. It is often the lack of real and sufficient randomness that compromises key security from the beginning.
Most dedicated appliances provide hardware-based true random number generation, a fully secured key storage and a secured casing. The protection can include measures against emissions. Any attempt to tamper with the unit will result in the immediate emptying of the key storage and the notification that an attempt at tampering took place. The casings are tamper resistant.
One fact that often doesn't get the attention it deserves: Encryption uses the key in plaintext. The security of the environment in which key is used is thus a decisive factor.

Protecting Data in Transit

State-of-the-art encryption algorithms such as AES-GCM provide protection of the frames in transit by combining a set of different basic security measures.



1. Payload encryption provides confidentiality of the data.

2. The foundation for the detection of data manipulation is provided by an integrity check value (ICV).

3. The signing of the integrity check value by the sender ensures the authenticity of the frame.

4. A counter ensures that no frames can be inserted into the network without being detected.

For networks that are part of a critical infrastructure additional transport-specific security measures come into play:

1. Tunneling hides the internal network addresses and exposes only the network address of the encryptor.

2. Traffic Flow Security (TFS) fills unused network bandwidth with dummy traffic to prevent traffic analysis.

Securing Carrier Ethernet and MPLS Networks

Metro and Carrier Ethernet networks are layer 2 networks. It is thus obvious that the best approach to secure them is at layer 2. The lower the layer in the OSI network protocol stack, the more comprehensive are the protocols that can be encrypted and the more efficient the protection and the processing. Over 99% of attacks happen at layer 3 or above. Encryption at layer 2 or below locks down all network data and prevents successful attacks on layer 3 or above.

MPLS networks operate at layer 2.5 and can either run over layer 2 or layer 3 networks. By securing at layer 2 and tunnelling over IP, layer 2 encryptors can support different MPLS scenarios. Some of them also provide a secure alternative to GET VPN for securing high-bandwidth WAN connections.

Key System

Ethernet frames come in three different variants, depending on the number of recipients of a frame:

- Unicast for the communication of one MAC address with a single other MAC address
- Multicast for the communication of one single MAC address with multiple MAC addresses
- Broadcast for the communication of one single MAC address with all other MAC addresses

Ethernet frames can also carry a VLAN tag (IEEE 802.1q). A VLAN is a virtual network that is logically separated from the other frames on the network. The VLAN tag also provides facilities for class of service (CoS) through a 3-bit Priority Code Point (PCP).

There are two different approaches to ensure that next to unicast frames also multicast and broadcast frames are properly encrypted: Pairwise keys and group keys.

For pairwise key systems a network consists of a multitude of point-to-point connections. Each encryptor is connected with each other encryptor by a point-to-point connection. Traditional pairwise key systems use unidirectional keys for the connection between the encryptorn endpoints.

Group keys are based on the principle that for the communication within a defined group the same key is used to encrypt the communication. The membership in one group does not exclude a member from concurrent membership in other groups. For the communication within different groups different keys are used. Keys are unique to a group and separate the groups cryptographically. A group consists of two or more members. Group membership can be e.g. based on VLAN-ID, multiple VLAN-IDs, MAC addresses and multicast group membership. Group key systems normally use a redundant key server setup or are set up in a distributed way. The key server takes care of providing the right group keys to each encryptor, so that the group members can communicate across sites. Another task of the key server is to ensure that a new key is generated and put in use if there is any change in the membership of the group. With the new key the old data traffic cannot be decrypted and with the old key the new data traffic cannot be decrypted.

Key Exchange

There are two different approaches to key exchange: One is symmetrical and the other one is asymmetrical. The asymmetrical approach needs more computing power but is considered to be more secure. Some physicists, technologists and mathematicians are assuming that a quantum computer with the proper algorithms could solve the mathematical problems used as foundation for asymmetrical key exchange within minutes and that powerful quantum computers might become a reality within the next decade. A big jump in security that also prevents successful attacks by quantum computers is therefore provided by a combination of asymmetrical and symmetrical key exchange, such as the combination of Diffie-Hellman with symmetrical encryption of the partial keys. A 256 bit AES key is used as signature and makes the key exchange immune against attacks from quantum computers.

In a symmetrical approach, all keys are directly derived from each other. First, a shared secret is entered into the encryptor. Then the encryptor generates internally a master key and encrypts the master key with the shared secret. The session key is also generated by the encryptor and is encrypted with the master key. Master key and session key are transmitted to the other encryptor in encrypted form. The big issue with this approach is the shared secret. If that shared secret ever becomes known, then all previously recorded data communication can be decrypted.

In an asymmetric approach the partial keys are generated completely inside the encryptor, without any user having access to it. After exchanging the partial keys both sides calculate the same shared secret. Contrary to a symmetric approach, nobody knows the shared secret. Subsequently the encryptor generates internally the master key and encrypts it with the shared secret. The encryptor also generates the session key and uses the master key to encrypt it. The transmission of the master and session keys from one encryptor is always encrypted.

Common asymmetrical approaches are Diffie-Hellman and RSA. Diffie-Hellmann uses in its basic variant the discrete logarithm problem, which comes with the disadvantage of needing very long partial keys to be really secure. The same is true for RSA. A more state-of-the-art variant is the use of Diffie-Hellman with elliptic curve cryptography (ECC), which provides better security with shorter partial keys. The security of ECC is heavily dependent on the curves used. Among experts the security of the NIST curves is severely in doubt. Appropriate security requires the choice between NIST curves, Brainpool curves and custom curves.

Asymmetrical approaches sign the partial keys that are exchanged to ensure that the correct remote station sends them. There are different ways to accomplish this: Either by using a certificate (X.509) in combination with appropriate procedures (RSA, DSA or ECC) or by encrypting the partial keys with a pre-shared secret. Most systems use a hybrid approach. Session keys are always symmetric.

The more frequent the sessions keys in use are replaced, the lower the probability that the key will be compromised. The security of the key does not only depend on the secrecy of the key, but also depends on the process used and the parameters chosen. The length of the counter and the ICV play an important role. E.g. in counter mode the key has to be changed before the counter starts back at 0. With group key systems it is therefore required that the system automatically changes the session key after a given number of minutes.

The same is true for the key encryption key (master key), which is used to encrypt the session keys. The exchange frequency is lower as it is only used to encrypt the session key and thus is used less often and encrypts less data. The regular exchange of master keys should take place automatically after a certain period of time. Key exchanges using Elliptic Curve Diffie-Hellmann are compute-intensive. Sufficient processing power of the encryptor is a requirement for keeping the lifecycle of a master key low, especially in large, complex networks.

The initial secrets should be exchanged every 12-24 months. They are the only manual key exchanges.

Management

Device management is an often-overlooked issue. Not everybody needs to have access to all the different management functions, especially network and security management need to be separated. Such a separation is also a pre-condition for Managed Security Services and Managed Encryption Services. The authentication of the user is based on the user identity, while the access is granted according to the role of the user. Typical roles include crypto officer, network management, maintenance and user). Roles with hierarchy levels allow mirroring actual hierarchies and responsibilities. Such a setup is also commonly used in managed security settings in which the customer needs the final control over changes to the security settings.

While preferable, a strict internal separation of users is difficult to achieve, as it also requires a separate memory space for each user.

Performance and Scalability

Dedicated appliances are optimised for performance. There is no competition for the available resources between different functionalities.

Integrated appliances are optimised for specific performance features that hardly ever can be fully exploited in parallel. Often cost considerations favour the use of ASICs (Application Specific Integrated Circuits) over FPGAs. Those ASICs support only a limited set of functions. If functions are used that are not implemented in hardware, they are executed in software, which leads to a performance loss. If the entire processing is executed on a standard CPU, the performance is limited to low and medium bandwidths and latency and jitter are increased. If the CPU is dedicated to a dedicated encryption appliance, the performance characteristics can be properly predicted and remain constant. A CPU that has to serve a range of different applications – as is typically the case with integrated appliances and virtualised environments – has a performance characteristic that is dependent on the particular load generated by other applications at a given time and thus is variable and unpredictable.

While scalability is less of an issue with point-to-point networks, it becomes an issue with point-to-multipoint and multipoint-to-multipoint networks. Dedicated appliances can often handle everything from small to large networks. Some deployments serve networks with more than 500 peers and group sizes exceeding 150 members.

Upgradeability

Dedicated layer 2 encryptors tend to be specified and dimensioned in a way that al-lows the expansion of the functionality at a later point in time. This is an essential requirement to keep the device state-of-the-art for the years to come. Amply dimensioned FPGAs (Field Programmable Gate Array) fit the bill, but they increase the cost. Underpowered FPGAs are quickly saturated and draw a high amount of power, which leads to extensive heat development.

Upgradeability and expandability are cost drivers and thus not high on the priority list for developers of integrated appliances. They prefer to focus on initial cost containment rather than on mid- to long-term cost efficiency and high assurance security. The cheapest way in mass-production is the use of ASICs, The only way to upgrade an ASIC is to replace it.

Software-based real and virtual appliances running on standard CPUs can easily be upgraded, but are substantially less powerful. Extensions of the software functionality can accentuate this lack of performance.

Links to in-depth background:

www.uebermeister.com/files/inside-it/2014_Introduction_Encryption_Metro_and_Carrier_Ethernet.pdf
www.uebermeister.com/files/inside-it/2014_Evaluation_Guide_Encryptors_Carrier_and_Metro_Ethernet.pdf
www.uebermeister.com/files/inside-it/2015_market_overview_Ethernet_encryptors_for_Metro_and_Carrier_Ethernet.pdf

Evolving threats and vulnerability landscape: new challenges for the emergency management

The International Emergency Management Society Conference, Roma September 30- October 2, 2015

Nowadays, communities rely on services provided by technological infrastructures. These are modern "lifeline systems" physically tying together urban areas, communities, and neighbourhoods, and facilitating the growth of local, regional, and national economies. These (inter)dependent systems work together to provide essential services to modern societies which are thus strictly dependent on the capability of exploiting the capacities provided by such technological resources and assets. The use of infrastructures contributes furthermore to reshape and improve relationships between communities, government, private sectors, non-profit communities and citizens. For that reason, citizens are more and more directly involved in supporting public services and infrastructure systems (e.g. transportation, energy, education, health and care, etc.) for example through so-called open data, living labs and tech hubs. These future developments will further improve the sustainability of our societies.

On the other side, crises due to natural (or anthropic) related events might seriously endanger these infrastructures and weaken the fruitful feedbacks they supply. Disasters are thus dramatic events which, other than producing casualties, break the connections between citizens and between citizen and the community, thus producing relevant social damages.

The TIEMS Conference, organised by the TIEMS Chapter Italy and hosted by the Istituto Superiore Antincendio (i.e. Italian Firefight Academia) has been aimed at investigating what are the new challenges in the field of risk and disaster management (also in relation to infrastructure integrity and service continuity) to face old and new type of threats by bring together leading researchers, practitioners and industries from all areas of emergency management to take advantage of the presented methodologies and practical applications. In particular the Conference aimed at evaluating gaps and the constraints that need to be overcame to improve the response capacities of first responders and the resilience of communities exposed to several type of hazards and threats.

The Conference covered all aspects related to Emergency Management, Risk Analysis and Preparedness activities, either for predicting Critical and/or for managing hot phases.

Presentation included aspects like:

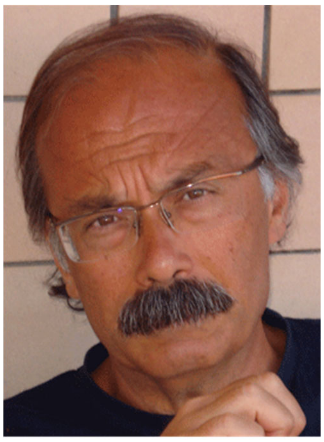
- risk reduction and mitigation techniques,
- cyber-physical threats and vulnerability analysis,
- model-based and experimental assessment of safety, reliability and security,
- human and social aspects in emergency managements, and
- management of complex emergency scenarios and epidemic spreading.

With more than 250 registered participants and 67 oral presentations, the organiser's expectations were overcome. The broad variety of topics is also reflected in the topics covered by keynote speeches and the related thematic sessions:

- Dr. Meen P. Chhetri (NCDM, Nepal) - "Nepal earthquake aftermaths";
- Ing. M Dolce (General Director of Italian Department of Civil Protection, Italy), "The Italian Dept. of Civil Protection (DPC) and its role in the Emergency Management";
- Dr. Kim, Jae-Kwon (Korean Society of Disaster & Security), "Sewol Ferry Disaster and Emergency Response Management in Korea";

Carmelo Di Mauro
Carmelo is an environmental Engineer with more than twenty years experience in the applied science, in particular in the field of risk-based decision-making processes.

e-mail: carmelo.di-mauro@jrc.it



Vittorio Rosato

Head of the Laboratory for the Analysis and Protection of Critical Infrastructures at ENEA Casaccia Research Centre in Roma.

e-mail: vittorio.rosato@enea.it

- Scenario prof. John Hamilton (Kestrel Group, New Zealand), “Emergency Management after the Christchurch earthquake” (video interview by dr. Sonia Giovinazzi, University of Canterbury in Christchurch, NZ);
- Prof. Dirk Helbing (ETH Zurich, Switzerland), “How to Increase Systemic Resilience in an Information Rich World”;
- Dr. Nicola Perra (University of London-Greenwich Business School), “Modelling and Forecast of epidemic events”
- Dr. Daniel Stevens, (Director of Emergency Management at City of Vancouver - Canada) “Emergency Management and Resilience in the metropolitan area of Vancouver”;
- Dr. David Bamaung, (Scottish Government, Scotland, UK), “Critical Infrastructure Resilience and Public Private Collaboration”;
- Dr. Ji Zhang, (Harmony Technologies Ltd, CHINA), “Ten years development in China Emergency Management 2006-2015”.

Besides many invited and contributed talks, the conference participants especially enjoyed a vivid roundtable discussion titled “Lesson Learnt from the Nepal Earthquake event: what still are the main challenges to improve the disaster management and the role of emerging technologies” with the main contribution of

- Prof. Dr. Meen B. Poudyal Chhetri – President, Nepal Centre for Disaster Management
- Dr. Guosheng Qu, Dep. General Team Leader of CISAR, China
- Dr. Kailash Gupta - Honorary Managing Trustee, TIEMS India Chapter
- Jaroslav Pejcoch, T-SOFT (Crisis management, Interoperability, Security), Czech Republic
- Prof. Carl W. Taylor, Fraser Institute for Health and Risks Analytics, Princeton
- Ing. Mauro Dolce, Italian Civil Protection, Italy

Due to the proximity of the Conference to the tremendous disaster hitting Nepal on April 25, 2015, the Conference has focused the first day around that event, by hosting a number of relations documenting the event (which produced over 8.000 casualties and more than 21.000 injured) and its aftermaths. An extensive report has been provided by prof. Meen Chhetri, President of the Nepal Center for Disaster Management through a clear exposition of the facts and the management actions of several international groups called to collaborate. A similar focus has been also provided on another recent disaster occurred in New Zealand in 2009 (Christchurch earthquake) provided by the keynote of prof. John Hamilton, former Director of New Zealand Civil Protection that, through a video interview recorded by dr. Sonia Giovinazzi of the University of Canterbury (NZ) has recalled the major problems arising in the Christchurch earthquake and the following lesson learnt incorporated into the NZ Disaster Management protocols.

The Conference also hosted a special workshop co-organized by Dennis Andersson (FOI), Josine van de Ven (TNO), Maciej Szulejewski (ITTI) on “Pan EU lesson sharing crisis management: DRIVER Project” which aimed to identify what types of methods and tools can support the lesson sharing process European Member states and how such lessons can be transferred to other organisations.

Large emphasis and interest has been triggered by prof. Helbing’s keynote on the revolutionary project of providing the planet of a “nervous system” made by open and shared data collected by mobile devices which could contribute to build a digital democracy, also providing invaluable support to Emergency Management.

The main outcome of the Conference was that many approaches in the disaster risk management area are still mainly sector-specific. The concept of resilience is becoming a key reference in disaster risk management, acknowledging that arising awareness of experts and as well as laypeople that all social assets can be protected. The conference discussions also identified the strengthening of infrastructures as an important field for disaster risk reduction. Although the respective research is valuable in order to learn more about the system characteristics and potential disaster risk reduction measures, it remains often vague how society is or could be affected by their failure. In order to reduce societal effects, a broader perspective needs to be carefully evaluated since the CIs impact on the functioning of many societies are not yet fully understood. This aspect will increase its importance in the future when communities will become more “Smart” i.e. they will heavily rely on ICT technologies and other advance infrastructure services. If from one side the future development will link networks supporting and positively feeding off each other, from the other one such inter-dependency may be prone to failures that can be propagate through a number of systems and that may results in a more severe impact for the communities. In other terms, future communities will count on more efficient services but at the same time may become more vulnerable due to complexity of interconnection of sophisticated infrastructure and services. This implies the need to develop new approaches and strategies to cope with hazards and disasters.

The all TIEMS Chapter Italy would like to thank again all participants and speakers that contributed to make this event a success.

ARIMA-Based Modeling and Validation of Consumption Readings in Power Grids

The goal of this project is to mitigate electricity theft due to attackers who hack smart meters and under-report electricity consumption. Such attacks have begun taking place in Europe and, if gone unchecked, pose a threat to the availability of power supply, a critical infrastructure resource.

In addition to the well-known benefits of smart meters, such as automated data collection and estimation of the state of the electric distribution grid, utilities such as BC Hydro believe that these meters would aid them in detecting electricity theft. This belief was challenged in 2010, when the Cyber Intelligence Section of the FBI reported that smart meters were hijacked in Puerto Rico, causing electricity theft amounting to annual losses for the utility estimated at $400 million. More recently, in October 2014, BBC News reported that smart meters in Spain were hacked to cut power bills. These reports indicate that there could be a growing number of thieves, referred to as attackers, in the power network, which could lead to electricity theft on a large scale.

Smart meters are increasingly being deployed to measure electricity consumption of residential as well as non-residential consumers. It has been recently reported that consumers were hacking their meters to under-report consumption. Compromising meter readings can cause operators, who rely on these readings, to misjudge true demand, and not schedule the required generation potentially leading to outages. The contribution of this work is to ensure that theft is drastically mitigated, so that theft cannot adversely impact power grid operation.

Objectives

The anomaly detection methods presented in this paper assume that an attacker has compromised the integrity of smart meter consumption readings, and aim to mitigate the impact of such an intrusion in the context of electricity theft. How the attacker can get into a position where he is capable of modifying communication signals is not a focus of this work and is discussed in related work. Our approach is to validate the data reported to the utility by modelling the normal consumption patterns of consumers and looking for deviations from this model. We use data-driven insights on consumption characteristics, similar to our award-winning work "PCA-Based Method for Detecting Integrity Attacks on Advanced Metering Infrastructure", which employs Principal Component Analysis and clustering. Also, our algorithms for intrusion detection are specific, as opposed to high-level security guidelines for network administrators.

Summary of contribution

The Auto-Regressive Moving Average (ARMA) and Auto-Regressive Integrated Moving Average (ARIMA) models are used to predict future data points in a time series. We show that the ARIMA model is a better model for capturing consumption behaviour and forecasting future behaviours. We evaluate the effectiveness of ARIMA forecasting in the context electricity theft. Finally, we propose additional checks that can mitigate the total amount of electricity that can be stolen by an attacker by 77.46%. Our evaluation is based on an open dataset of meter readings from a real deployment with 450 consumers.

Varun Badrinath Krishna

Varun is a graduate student in the Electrical and Computer Engineering department and a research assistant in the Information Trust Institute, University of Illinois at Urbana-Champaign, USA. With Prof. William H. Sanders, Varun is researching data-driven methods to secure communications in power grids, a critical infrastructure. He is Co-PI on that project, partially supported by the Siebel Energy Institute, and leveraging the Blue Waters supercomputer at National Center for Supercomputing Applications, USA. His papers won the best paper award at QEST 2015 and CYCA at CRITIS 2015. This work received contributions from Prof. Sanders and Prof. Ravishankar Iyer.

e-mail: varunbk@illinois.edu
University of Illinois at Urbana-Champaign,
1308 W. Main Street, Urbana,
Illinois, 61801

Dataset Used in the Study

The data we used was collected by Ireland's Commission for Energy Regulation (CER) as part of a trial that aimed at studying smart meter communication technologies. This is the largest, publicly available dataset that we know of. The fact that the dataset is public makes it possible for researchers to replicate and extend this paper's results. The data is accessed via the Irish Social Science Data Archive at www.ucd.ie/issda. The providers of the data, the CER, bear no responsibility for the further analysis or interpretation of it.

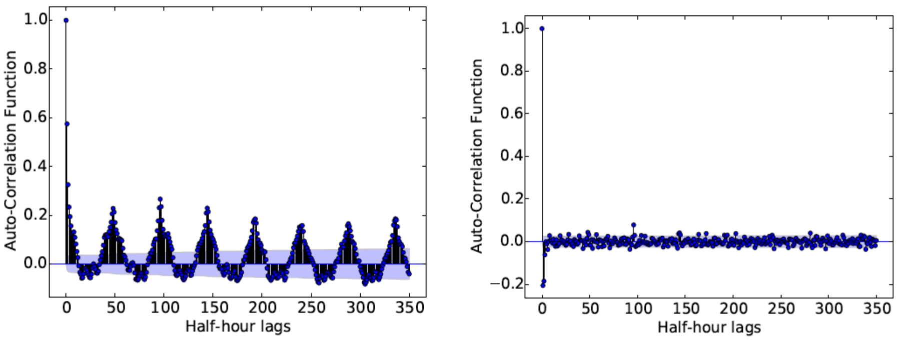
We evaluate our models and algorithms on 450 consumers from this dataset. For each of these consumers, the smart meter readings are collected at a half-hour time resolution, for a period of up to 74 weeks. The consumers include 377 residential consumers, 18 small and medium enterprises (SMEs), and 55 unclassified by CER.

We assume that this dataset is free from maliciously compromised measurements, and use the data to understand and model normal consumption behaviour.

Modelling Approach

The underlying assumption of the ARMA model is that the time series data is weakly stationary. Stationary data has three characteristics: (1) the mean is constant, (2) the variance is constant and (3) the covariance of the signal with itself at different time lags is constant. We define a weakly stationary signal as one that fails condition (1), but satisfies conditions (2) and (3). The moving average component of ARMA automatically adjusts for changing means, so condition (1) is not important for the suitability of ARMA for a given time series.

The ARMA model does not handle largely changing covariance in non-stationary signals. Fig.1 (a) illustrates the Auto-Correlation Function (ACF) for a single consumer. The ACF is the correlation of the time series with itself at a specified lag. We extract the time series for a single consumer and depict the ACFs for 350 half-hour lags. There are 336 half-hours in a week, so the figure captures a little over a week. As expected, high autocorrelation was observed for this consumer at multiples of 48 half-hour (or 1 day) time periods. These high correlations persist for all lags throughout the consumption history captured in the dataset.



(a) ACFs without differencing (b) ACFs with first-order differencing

Figure 4: Auto-Correlation Function (ACF) of the electricity consumption of a single consumer

Further, the plot demonstrates failure of the third requirement for stationarity since the ACFs change significantly over time. This lack of stationarity implies that the ARMA model would fail to provide a reliable prediction of the next point in the time series. The ACFs need to rapidly decrease to constant or insignificant values in order for the ARMA model to reliably work. The rate of ACF decrease will determine the model order.

We propose an alternative model, the ARIMA model, which has an additional differencing term. We find that first-order differencing causes rapidly decreasing ACFs for consumers who have non-stationary consumptions. Instead of predicting the next value in the time series, we predict the difference between the current and next value in the time series as a linear function of past differences. After applying first-order differencing, we observe Fig.1 (b). Clearly, the ACFs are close to zero beyond 3 time lags. Therefore, the order of the ARIMA model is finite. In addition, the order is small, which is important to ensure minimal computational costs.

We have applied first-order differencing and observed its benefits for one consumer, but visual inspection is impractical for our dataset of 450 consumers. Therefore, we employ the Hyndman-Khandakar algorithm to estimate the model order. This method combines cross-validation techniques, unit root tests, and maximum likelihood estimation. The results revealed that for 92% of consumers, first-order differencing is required, justifying our ARIMA model proposal.

Once the ARIMA model is estimated, the next consumption point in the time series is forecast. From this point forecast, a 95% confidence interval is constructed with the assumption of independent and identically distributed Gaussian errors in the Moving Average model.

Electricity Theft Attack

The ARIMA confidence interval provides a bound on the amount of electricity an attacker can steal. Without the ARIMA detection mechanism in place, the attacker can steal an arbitrary amount of electricity. He is only constrained by the physical limits of the electric distribution system. Specifically, electric distribution lines are rated based on the maximum current that they can carry. If the demand from the attacker increases (while the distribution voltage is kept approximately constant by reactive power compensation), the current in the distribution lines will increase. If the current increases beyond the rated threshold, the lines will exceed their thermal limits. The ensuing damage may lead to blackouts or other equipment failures. Although this is not an electricity theft attack, it highlights what can happen if operators rely on meter measurements that may be compromised.

We consider a specific attack model in which the attacker steals electricity from a neighbor for monetary gain. The attacker compromises his own smart meter and under-reports his consumption. In addition, to avoid detection by industry techniques, he also compromises his neighbour's smart meter and over-reports the neighbour's consumption. To further mitigate the amount of electricity that can be stolen by the attacker, we augmented the ARIMA confidence interval with checks on mean and variance of the attacker's consumption pattern. The mean and variance were compared against historic data in the dataset.

Evaluation

The evaluation of our anomaly detection method was performed using the CER dataset from Ireland. We injected well-crafted attacks, as described in the publication, that maximise the attacker's gain in electricity theft. For each of the 450 consumers, we evaluated the maximum amount of electricity that could be stolen.

Results

Although the ARIMA confidence intervals bounded the attack, an attacker could steal up to 285,914kWh from 450 neighbours in one week. However, with additional checks on mean and variance of the data reported by the attacker, the worst-case attack would lead to 64,447kWh being stolen.

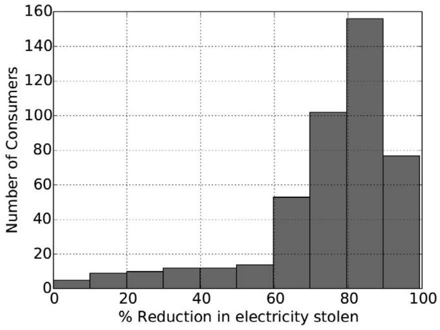


Figure 5: Savings obtained by additional checks on mean and variance of data reported by attacker per consumer.

The maximum amount of electricity that could be stolen from each neighbour was naturally reduced by additional checks on mean and variance, leading to the aforementioned reduction for the entire week. Fig. 2 captures this reduction. For most neighbours, a savings of over 70% was observed. In the best case, 99% of theft was reduced, which emphasises the benefit of the additional checks.

CYCA 2015

This work was presented as a research paper at the 10th International Conference on Critical Information Infrastructure Security (CRITIS 2015), and Varun was awarded the CIPRNet Young CRITIS Award (CYCA). As the authors of this work, we are truly honoured to have received this recognition from CIPRNet.

Collaborators

This work performed with guidance of Varun's PhD advisor, Prof. William H. Sanders, and Prof Ravishankar K. Iyer.

Prof. William H. Sanders is the Donald Biggar Willett Professor of Engineering and Head of the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign. He is a Fellow of the IEEE, the ACM and the AAAS, a past Chair of the IEEE Technical Committee on Fault-Tolerant Computing, and past Vice-Chair of the IFIP Working Group 10.4 on Dependable Computing. He was the founding Director of the Information Trust Institute at Illinois (2004-2011), and served as Director of the Coordinated Science Laboratory at Illinois from 2010 to 2014. His research interests include security and dependability metrics and evaluation, with a focus on critical infrastructures. He has published more than 250 technical papers in those areas. He was the Director and PI of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center, which is at the fore-front of national efforts to make the U.S. power grid smart and resilient.

Prof. Ravishankar Iyer is the George and Ann Fisher Distinguished Professor of Engineering at the University of Illinois at Urbana-Champaign. He holds joint appointments in the Department of Electrical and Computer Engineering, the Coordinated Science Laboratory (CSL), and the Department of Computer Science, and serves as Chief Scientist of the Information Trust Institute. Iyer has led several large successful projects funded by NASA, DARPA, NSF, and private industry. He currently co-leads the CompGen Center at Illinois. Funded by NSF and partnering with industry leaders, hospitals, and research labs, CompGen aims to build a new computational platform to address both accuracy and performance issues for a range of genomics applications. Professor Iyer is a Fellow of the AAAS, the IEEE, and the ACM. He has received several awards, including the American Institute for Aeronautics and Astronautics (AIAA) Information Systems Award, the IEEE Emanuel R. Piore Award, and the 2011 Outstanding Contributions award from the Association of Computing Machinery - Special Interest Group on Security for his fundamental contributions in secure and dependable computing. Professor Iyer is also the recipient of a degree of Doctor Honoris Causa from Toulouse Sabatier University in France.

If you would like to access this publication, and other related publications by Varun and Prof. Sanders, please visit Varun's University of Illinois profile:
http://www.ece.illinois.edu/directory/profile/varunbk

This project was supported by the U.S. Department of Energy under Award Number DE-OE0000097 and the Siebel Energy Institute.

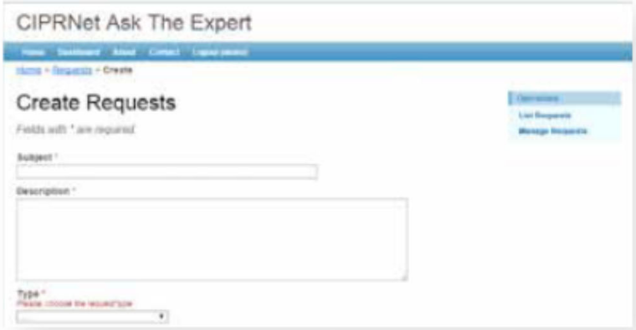
Ask the Expert service

Brought to you by CIPRNet –
the Critical Infrastructure Preparedness and
Resilience Research Network

A chance to reach a critical mass of experts in CIP

The Ask the Expert service is a platform of experts in various domains of crisis management and critical infrastructures protection created to answer questions and help solving problems in the areas such as:

> Technical challenges for CIP;
> CI management, crisis management for CI;
> CI-related documentation, e.g. national and EU regulations, policies, public reports and statistical data;
> Practical aspects of CI operation.



CIPRNet Ask The Expert

Create Requests

*Fields with * are required.*

Subject *

Description *

Type *
Please choose the request type

Who are the experts?

CIPRNet consortium partners and key representatives from CIP research communities and in area of:

> Modelling, simulation and analysis,
> Monitoring and control,
> Risk analysis, assessment and management,
> Telecommunication and cyber security,
> Transportation, and many others.

How can we help you?

By answering the questions, Ask the Expert service of the CIPRNet project and portal helps solving current and future problems and challenges of critical infrastructures. We can explain past cases, discuss emerging problems and direct you to relevant documents, regulations and strategies.

For Whom?

> Public administration,
> CI operators,
> CIP experts,
> Practitioners in the CIP area,
> Citizens and society.

Where and how?

1. Register to access the service: http://ciprnet.casaccia.enea.it/ate/
2. Check your e-mail to activate your account
3. Log in to the service
4. Once you are logged in, you can use your service dashboard to ask the question

Exemplary questions

> Where can I find reports about CI cascading effect after the L'Aquila earthquake in 2009?
> What are the cyber security challenges to be taken into account while designing smart grids?

CIPRNet

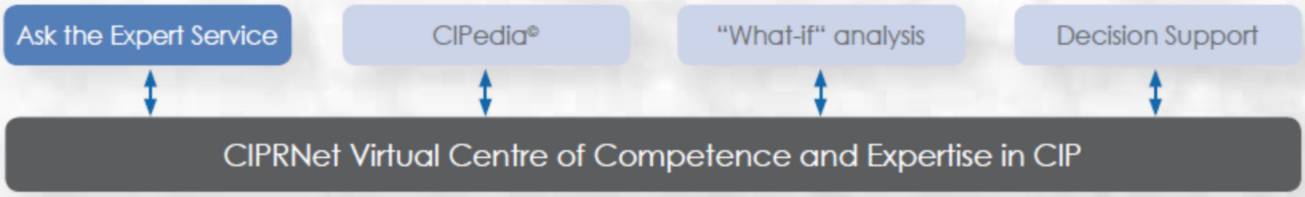
Critical Infrastructure Preparedness and Resilience Research Network – background information

CIPRNet establishes a Network of Excellence in Critical Infrastructure Protection (CIP). CIPRNet performs research and development that addresses a wide range of stakeholders including (multi)national emergency management, critical infrastructure operators, policy makers, and the society. By integrating resources of the CIPRNet partners acquired in more than 60 EU co-funded research projects, CIPRNet will create new advanced capabilities for its stakeholders. A key technology for the new capabilities will be modelling, simulation and analysis for CIP. CIPRNet builds a long-lasting virtual centre of shared and integrated knowledge and expertise in CIP.

Co-funded	EU FP7
Instrument	Network of Excellence (NoE)
Start date	March 1, 2013
Duration	48 months
Partners	12
Proposal number	312450

CIPRNet partners:

1. Fraunhofer IAIS
2. ENEA
3. TNO
4. UIC
5. CEA
6. Joint Research Centre
7. Deltares
8. University of Cyprus
9. UTP
10. UCBM
11. University of British Columbia
12. ACRIS GmbH



CIPRNet Virtual Centre of Competence and Expertise in CIP

CIPRNet will create the tangible VCCC already during the project term. The VCCC serves as the foundation of a long-lasting network of facilities providing enduring support from research to CI stakeholders in EU Member States. This network of facilities has the working title EISAC (European Infrastructures Simulation and Analysis Centre). A European headquarters shall foster standardisation of technology, organise cross-border collaboration, and provide support at EU level.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The European Commission's support is gratefully acknowledged.
The contents of this document and the view expressed in the publication are the sole responsibility of the author and under no circumstances can be regarded as reflecting the position of the European Union.

European CIIP Newsletter
Call for Papers

October 16 – February 17, Volume 10, Number 3

Special Issue on Cybersecurity:

Challenges Landscape and Solutions

Call for Papers ECN Special Issue:
Cyber security landscape, challenges, initiatives & solutions

Guest editors are calling for European and International contributions to reach best possible coverage for depicting state-of-the-art.

Nowadays, cyber security should be considered as a crucial aspect of critical infrastructure protection. Currently, the networked mission critical systems and national critical infrastructure might be vulnerable to cyber threats, cyber-crime and cyber terrorism. The same hazards apply to citizens and small scale ICT systems (e.g. used by SMEs).

Therefore, we cordially invite prospective authors to submit ECN-like papers (https://www.ciprnet.eu/ecn.html) on the following topics (list is not exhaustive, and my be prolonged by your contribution):

- Information and presentation about past and ongoing cyber security research projects
- Research lines, directions, results and ideas
- Information on current initiatives (groups, strategies, formal and informal bodies) in the area of cyber security
- Presentation of cyber security strategies
- Emerging research areas and techniques in cyber security
- Presentation of cyber security labs
- Cyber security case studies
- End-users views, needs and opinions

Guest Editors:

Prof. Michal Choras and Dr Rafal Kozik

University of Science and Technology, Bydgoszcz, Poland

Contact:
chorasm@utp.edu.pl

Paper submission deadline: 15.06.2016

Please send your submission to:

chorasm@utp.edu.pl

Smart grid networks: models & communities

Overview on standards, communities and advancement

Introduction

In this paper we address the Next Generation Infrastructures and smart grids in particular. Those new networked approaches and technologies bring new opportunities, but also new challenges and threats.
Next Generation Infrastructures operation and secure design are also a part of the analysis performed in the FP7 project CIPRNet.
Hereby, we focus on smart grids, and present the smart grids models, architectures as well as the communities involved in smart grid technology.

Smart grid models

There is not a one definition of a smart grid and no one-fit-all model. There are different models of implementing smart grids and they have to be based on and adjusted to the potential of existing grids and specific local requirements.

A smart grid is a highly complex system where ICT play a crucial role, ensuring communication between different smart grid system components. These different components have to be interoperable and thus there is a need for standardisation as regards the technical solutions used in the smart grid, interfaces, communication protocols and also processes. There exist a number of standards related to introducing smart grids developed by the International Electrotechnical Commission (IEC) and the National Institute of Standards and Technology (NIST). There are initiatives that aim at giving guidance on how to introduce the standards and to provide the models describing smart grid functions and technology. A group of institutions in Europe, the European Commission's Mandate 490 (M/490) for Smart Grid, the European Telecommunications Standards Institute (ETSI), European Committee for Standardization (Comité Européen Normalisation – CEN), and the European Committee for Electrotechnical Standardization (CENELEC), created the CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture. NIST developed a Framework and Roadmap for Smart Grid Interoperability Standards. The experts behind those initiatives in Europe and in the United States have started a cooperation with the aim to align their work results.

The European Reference Architecture was proposed in November 2012 but the work continues and the update is to be expected soon. The NIST Framework was proposed in September 2014 (3rd release).

Smart Grid Reference Architecture
The European Commission's Smart Grid Reference Architecture is a widely accepted model in Europe. The mandate presents a consistent architecture composed of a set of standards, digital computing and communication technologies and electrical architectures, the processes and services. Its aim is to foster an easier adoption of smart grids in Europe. The mandate does not cover business models. The Smart Grid Architecture Model (SGAM) has been proposed in the mandate, which is based on different approaches and methodologies of building a smart grid infrastructure. The SGAM is composed of five core viewpoint layers: Business, Function, Information, Communication, and Component, taken from the Gridwise Alliance Architecture Council (GWAC). The Business layer focuses on business strategic goals, processes and services and it also concerns regulations. The Functional layer contains the description of use cases including logical functions or services independent from physical implementation. The third, Information layer, provides the information objects and data models that are being used and exchanged between functions, services and components and that ensures interoperability in information exchange by providing the common semantics for

Prof. Michał Choraś

Prof. Michał Choraś holds the professor position at University of Science and Technology (UTP) where he is the Head of ZST Division. He also works as the consultant in security and coordinates projects (e.g. FP7 CAMINO on cyber crime and cyber terrorism). He is the author of over 150 publications.
e-mail: **chorasm@utp.edu.pl**

Patrycja Młynarek
Consultant at ITTI Sp. z o. o., Poznan, Poland. Manages and contributes to EU and commercial projects. Work areas: IT@telecom market and services, ICT, security, technology transfer, evaluations and market research, regulations, funds acquisition (e.g. FP6, FP7, H2020, structural funds).
patrycja.mlynarek@itti.com.pl

functions and services. The Communication layer contains protocols and mechanisms for the exchange of information between components. The last, Component layer, describes physical components which host functions, information and communication means.

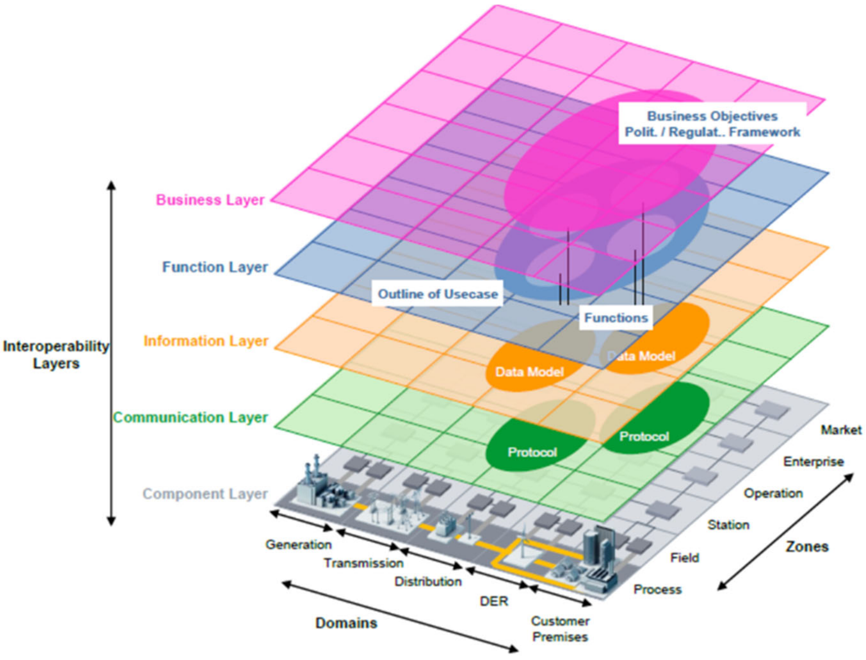


Figure 6: SGAM Framework (source: CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture 2012)

The SGAM layers are divided each into five domains and subdivided in six zones. The domains are Generation, Transmission, Distribution, DER, and Customer Premises. The zones are Market, Enterprise, Station, Operation, Field, and Process. The SGAM framework (called SGAM cube) is presented in Figure 1.

The presented model may be used to make a description of the current infrastructure, the possible data flows, the comparison of the current situation to the future, planned one. It will help identify standards that should be applied in the individual layer, domains and zones and to verify whether there is no overlap between standards. A crucial advantage of SGAM is that it provides a good visualisation of an overall smart grid infrastructure, which is a highly complex system of systems, and of the interactions of the stakeholders concerned. The SGAM is flexible and will be updated in order to address new technical deployments.

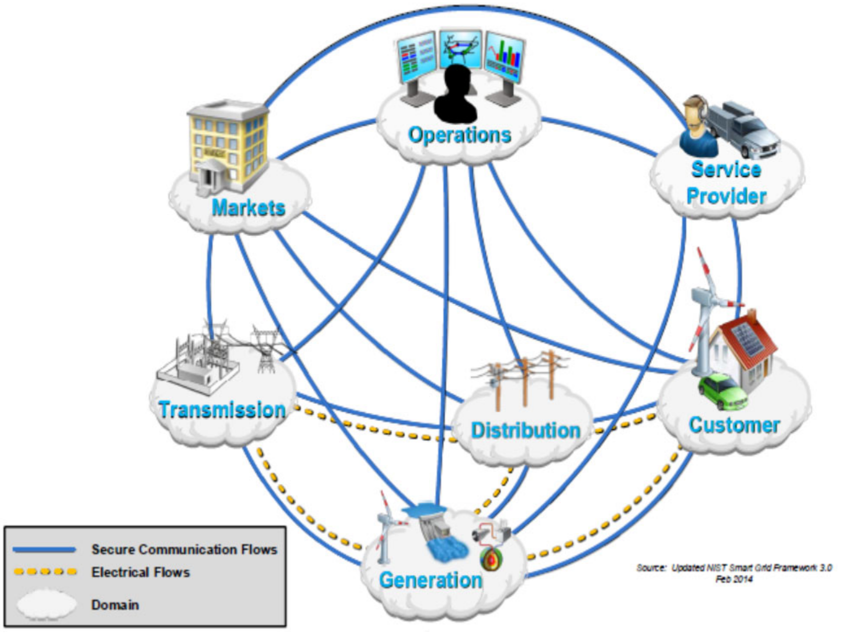


Figure 7: Original NIST Conceptual Domain Model (source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, 2014)

Framework and Roadmap for Smart Grid Interoperability Standards

The NIST Framework and Roadmap for Smart Grid Interoperability Standards is a reference architecture model for Smart Grids developed in the USA. In its latest release, 3.0, the model has been harmonised with the European Smart Grid Reference Architecture. NIST was made responsible to undertake such work under the U.S.' Energy Independence and Security Act (EISA) of 2007.

The NIST framework provides a holistic vision for the smart grids for the United States, based on relevant policies regarding the energy market in the U.S. NIST has been working on the subsequent versions of the framework with Smart Grid Interoperability Panel (SGIP), the smart grid community that it established in order to accelerate the development of standards and protocols for the interoperability of the smart grid. The status of SGIP has changed over the years and is now an industry-led non-profit organisation. An important feature of the NIST framework is that it provides a list of protocols and standards that support interoperability of smart grid devices and systems and that are the building blocks for the smart grid. The framework now contains over 65 standards or families of standards that ensure the smart grid system elements are interoperable and work seamlessly, be it wind turbines, solar panels, conventional generators, batteries, smart meters, transmission and distribution sensors etc.

The NIST architectural framework provides a general view of smart grid architecture, the processes and methodology of introducing the smart grid, with diagrams and descriptions that help identify the characteristics of the grid. Based on this high-level model different standard organisations may propose more detailed propositions.

The cybersecurity framework describes standards, guidelines and strategies for the electric sector to ensure the security of the IT systems in smart grids, their confidentiality, integrity and availability. The issue of cybersecurity has been deepened in NIST Guidelines for Smart Grid Cybersecurity (NISTIR 7628), the most recent version of which dates from November 2014.

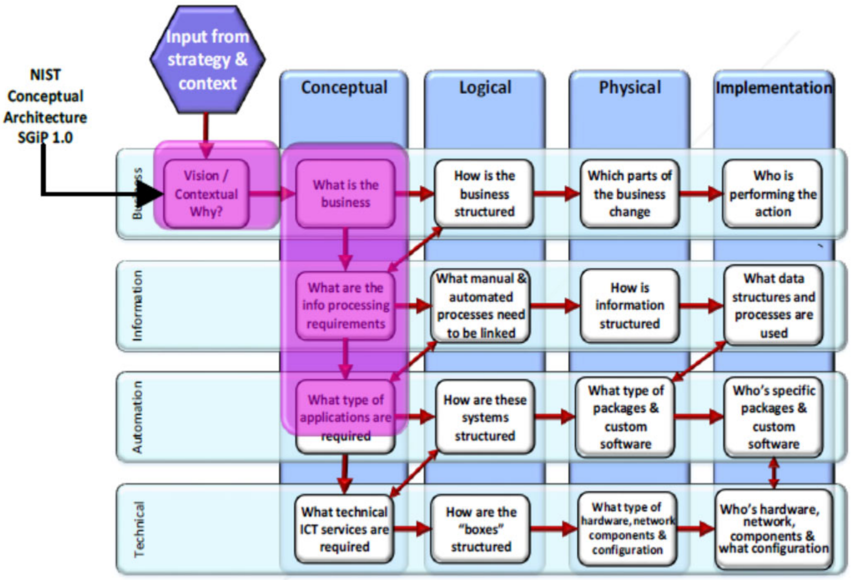

NIST Conceptual Architecture SGiP 1.0
Input from strategy & context
Conceptual
Logical
Physical
Implementation
Business
Information
Automation
Technical
Vision / Contextual Why?
What is the business
How is the business structured
Which parts of the business change
Who is performing the action
What are the info processing requirements
What manual & automated processes need to be linked
How is information structured
What data structures and processes are used
What type of applications are required
How are these systems structured
What type of packages & custom software
Who's specific packages & custom software
What technical ICT services are required
How are the "boxes" structured
What type of hardware, network components & configuration
Who's hardware, network, components & what configuration

Figure 8: NIST Conceptual Architecture mapped onto the Architecture Matrix Service Orientation and Ontology (source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, 2014)

The framework is technology neutral and it enables all electric resources to contribute to the smart grid. NIST originally created a conceptual domain model useful in activities such as planning, requirements development, documentation, and organisation of the diverse, expanding collection of interconnected networks and equipment composing the smart grid. The smart grid was divided into seven domains: Customer, Markets, Service Provider, Operations, Generation, Transmission, Distribution. The model is shown in Figure 2.

Each domain is assigned conceptual "roles" and "services" describing types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing identified goals, such as: customer management, distributed generation aggregation, and outage management.

NIST in its further work and in cooperation with different stakeholders modified the Conceptual Domain Model and proposed an architecture matrix, presented in Figure 3.

NIST proposed the conceptual architecture in order to provide smart grid stakeholders building blocks they could use to easily and rapidly build the architectures of their own systems. This architecture contains abstract roles and services necessary to support smart grid requirements and does not present details concerning application or interface specifications.

Smart Grid Maturity Model

There are several models that are very helpful for an electric power utility to assess itself and see where it is now in its way towards a smart grid and to get inspiration for the actions that are still needed. The first such model was the Smart Grid Maturity Model (SGMM) maintained by the Carnegie Mellon Software Engineering Institute (SEI) and it is addressed to electric power utilities that want to introduce the smart grid innovations. SGMM is a tool that will help utilities manage all aspects related to passing to smart grids. Using SGMM utilities will be able to tell in which areas they already made progress and to measure the progress, to prioritise the actions planned and to ensure all areas are covered.

SGMM covers eight domains and has overall 175 characteristics of a mature utility using smart grids. The eight domains are as follows:

- Strategy, Management, and Regulatory,
- Organisation and Structure,
- Grid Operations,
- Work and Asset Management,
- Technology,
- Customer,
- Value Chain Integration,
- Societal and Environmental.

A utility may make a self-assessment by analysing its own characteristics against the ones in the model.

The Electricity Subsector Cybersecurity Capability Maturity Model

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) covers the area of the electrical grid security. It has been created by the initiative of the USA government. This model has been created based on the Cybersecurity Capability Maturity Model (C2M2) that was designed to be used by any organisation to enhance its own cybersecurity capabilities (regardless of size, type, or industry) but it contains in addition some part that specifically concern the electricity subsector. Basing on this model it is also possible for an entity to make an assessment of its own maturity in the area of cybersecurity. Ten domains have been specified.

Smart grid communities

Smart Grids are an important concept that yet has a long way ahead before it is fully implemented and becomes an everyday reality. Research in Smart Grids is on-going and there are different initiatives that are pushing it forward.

There are thousands of grid operators worldwide that operate in different environments and many solutions emerge to meet their local needs and this fragmentation of research and of existing solutions is a big challenge. There does not exist a one organisation or initiative at a global or a European level that would coordinate the progress in Smart Grids, in research and in technology implementation but there are some initiatives that are important in this context and should be mentioned.

At the global level there exists the IEEE & Smart Grid organisation that aims at facilitating and guiding the evolution toward the Smart Grid. It gathers key stakeholders at different events, it fosters publications and standards and host a Smart Grid-related website. It has 395,000 members being research institutions, governments and companies and thus has the critical mass to take the leading role. IEEE runs the Xplore digital library with scientific articles on latest research in the Smart Grids area. Nearly 2,500 papers relevant to smart grid have been published in over 40 IEEE journals. The events organised by IEEE are e.g. "IEEE Innovative Smart Grid Technologies 2010" and the new "IEEE Smart Grid World Forum". IEEE has approximately 100 standards and standards in development focused on smart grid.

At the European level, there are a number of initiatives in the fields of Smart Grids. There are approximately 200 research, development and demonstration projects focused on Smart Grids. But the coordination between different activities is lacking, which constitutes a very big challenge, as without it the resources are not used as efficiently as they could be. Separate activities, even very good ones, do not have a chance to have a real impact on the whole or even on the majority of the Smart Grids community.

The European Strategic Energy Technology Plan (the SET-Plan) is an initiative aiming at accelerating the development and deployment of low-carbon technologies. It coordinates research and innovation and co-finances projects focusing on technologies enhancement and on ensuring their cost-effectiveness. The SET-Plan was adopted by the European Union in 2008 and it is the main tool supporting decision makers in the area of the European energy policy. The first major timeline for the SET-Plan is 2020, for a 20% reduction of CO2 emissions, a 20% share of energy from low-carbon energy sources and 20% reduction in the use of primary energy by improving energy efficiency. The second major timeline is 2050, for the worldwide transition to a low carbon economy (limiting climate change to a global temperature rise of no more than 2°C, in particular by considerably reducing greenhouse gas emissions). The SET-Plan's budget is approximately of €71.5 billion.

The SET-Plan encompasses several implementation mechanisms, such as the SET-Plan Steering Group, European Industrial Initiatives (EII), the European Energy Research Alliance (EERA), and the SET-Plan Information System (SETIS). One of the European Industrial Initiatives is focused on the Smart Grids sector: the European Electricity Grid Initiative (EE-GI). EEGI is a 9-year programme (until 2018) for research, development and demonstration to foster innovation of the electricity networks. EEGI brings together all stakeholders in the Smart Grids sector, such as researchers, industry, EU Member States and the European Commission and its focus is on system innovation and on integration of new technologies in real life conditions.

An important initiative that considerably contributes to the SET-Plan is ERA-Net Smart Grids Plus. Its ambition is to expand the EEGI initiative. ERA-Net Smart Grids Plus gathers 21 European countries and regions with the aim to achieve the Smart Grids vision and goals of Europe. The initiative fosters new technologies and market designs, as well as prepares customers to the adoption of new solutions. The members of ERA-Net Smart Grids Plus are entities responsible for national and regional programmes funding research in the fields of Smart Grids and the initiative is building a structure for cooperation between those entities and with external initiatives at the European level. The initiative promotes the electric power system that integrates renewable energies and is more flexible, efficient and secure, with low greenhouse gas emissions and with an affordable price. It promotes open markets for energy products and services. The initiative also seeks Europe's leading role at the world arena in low-carbon energy technologies. All this requires the research to be both cross-sectoral and interdisciplinary. ERA-Net Smart Grids Plus has the ambition to be the most important platform in the fields of all smart grid-related research in Europe. A number of leading European distribution system operators (DSOs) have created EDSO for SmartGrids, with the aim to coordinate research on smart grids and influence regulations at the national and European level. It considers itself the main interface between DSOs and the European institutions. EDSO for SmartGrids focuses e.g. on development of new models for smart grids and on testing the models on a large scale.

One other initiative is KIC InnoEnergy, i.e. a Knowledge and Innovation Community (KIC) focused on sustainable energy, fostered by the European Institute of Innovation and Technology (EIT). It is a European network, a commercial company with the shareholders being top ranking industries, research centres and universities, key players in the energy field. Its goal is to reduce costs in the energy value chain, increase security and reduce CO2 and other greenhouse gas emissions. Smart Electric Grid is one of the technology areas (out of eight) KIC InnoEnergy focuses on.

One of the FP7 projects that contribute to creating Smart Grid communities is e.g. ETP SmartGrids (Thee European Technology Platform for Electricity Networks of the Future), which is the basic forum in Europe for the crystallisation of policy and technology research and development pathways for the smart grids sector, as well as the link between EU-level related initiatives. One other is GRID+, a Coordination and Support Action with the aim to support the development of EEGI.

Some other initiatives worth mentioning are the International Energy Agency (IEA), an autonomous organisation promoting reliable, clean and affordable energy for its 28 member countries and beyond, International Smart Grids Action Network (ISGAN), promoting an international cooperation on smart grids adoption in the world and Global Smart Grid Federation (GSGF) aiming at development of smarter, cleaner electricity systems around the world.

CRITIS 2016: 11th International Conference on Critical Information Infrastructures Security – Call for Papers

CRITIS
2016

The 11th edition of CRITIS takes place in Paris, France, October 10–12, 2016

In 2016, the International Conference on Critical Information Infrastructures Security faces its 11th anniversary. CRITIS 2016 aims at bringing together researchers and professionals from academia, industry and govern-mental organisations working in the field of the security of critical (information) infrastructure systems.

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

> CRITIS 2016 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.

Call for Papers

CRITIS 2016 covers five thematic foci. Topic category 1 focuses on technologies and innovative responses for the protection of cyber-physical systems; topic category 2 covers the procedures and organisational aspects in C(I)IP including policies, best practices and lessons learned; topic category 3 includes advances in Human Factors, decision support, and cross-sector CI(I)P approaches; additionally topic category 4 is dedicated to railway stakeholders. Last but not least, CRITIS 2016 aims to encourage and inspire early stage researchers demonstrating outstanding research performance through topic category 5: Young CRITIS and CIPRNet Young CRITIS Award (CYCA).

Topic 1: Technologies: Innovative responses for the protection of cyber-physical systems

- C(I)IP – Critical Information Infrastructure Protection
- Cyber security in critical infrastructure systems
- Fault tolerant control for cyber-physical systems
- Security and protection of smart buildings
- Self-healing, self-protection, and self-management architectures
- Modelling and analysis of cyber-physical systems for monitoring and control
- Modelling, Simulation, Analysis and Validation Approaches
- C(I)IP applications in transportation, energy, communication, finance, health and water infrastructures
- CI in modern Warfare and cyber-warfare

Programme Co-Chairs:
Roberto SETOLA, Campus Bio-Medico University of Rome
e-mail: **r.setola@unicampus.it**

Hypatia NASSOPOULOS, Ecole des Ingénieurs de la Ville de Paris (EIVP)
e-mail: hypatia.nassopoulos@eivp-paris.fr

General Chair:
Jean-Pierre LOUBINOUX, General Director of UIC, represented by UIC Security Division
e-mail: loubinoux@uic.org

uic
INTERNATIONAL UNION OF RAILWAYS

Local Chair:
Jacques COLLIARD, Head of UIC Security Division
e-mail: colliard@uic.org

Programme Organizing Chair:
Grigore HAVARNEANU, Research Advisor, UIC Security Division
e-mail: havarneanu@uic.org

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

Publicity Co-Chair:
UIC Communications Department

Topic 2: Procedures and organisational aspects in C(I)IP: Policies, best practices and lessons learned

- Preparedness, prevention, mitigation and planning
- Risk management in C(I)IP
- Security, protection, resilience and survivability of complex cyber-physical systems
- CI Preparedness and Emergency Management
- C(I)I exercises and contingency plans
- Crisis Management and CI
- CI Resilience Assessment
- Impact and consequence analysis of C(I)I loss or reduction of quality of service
- Public-private partnership for critical infrastructure resilience
- C(I)IP policies at national and cross-border levels
- The role of C(I)I in the implementation of the EU directive on European Critical Infrastructures in EU Member States
- C(I)IP R&D agenda at national and international levels
- Economics, investments and incentives of critical infrastructure protection
- Defence of civilian C(I)I in conflicts with cyber elements
- Forensics and attribution in C(I)I

Topic 3: Advances in Human Factors, decision support, and cross-sector CI(I)P approaches – focus on end-users

- Analysis of Human Factor and Security Awareness in C(I)IP
- Advanced decision support for mitigating C(I)I related emergencies
- Social aspects and public communication in C(I)IP
- Psycho-social dimensions of crisis management and intervention
- Training for C(I)IP and effective intervention
- Coping with Social Media in C(I)I-related Crisis Management
- Recent trends in cyber economy (clouds, quasi-monopolies, new payment methods etc.) and implications for C(I)I and C(I)IP

Topic 4: Special private stakeholder session

- C(I)IP specificities in the railway sector
- Constraints, challenges and opportunities for railway infrastructure
- Tunnel protection and tunnel control systems
- Protection of depots and marshalling yards
- Power stations
- Railway bridges
- Railway construction

Topic 5: Young CRITIS and CIPRNet Young CRITIS Award (CYCA)

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

Paper submission

We encourage submissions containing original ideas that are relevant to the scope of CRITIS 2016. 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 which 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.

Paper submission will be done 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 2016 continues the “Young CRITIS” community-building activities for fostering open-minded talents.

Acceptance policy

For publication in the CRITIS 2016 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 organisers.

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

As in previous years, it is planned that **post-proceedings** are published by Springer-Verlag in their Lecture Notes in Computer Science (LNCS) 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.

10-12 October 2016
UIC HQ Paris, France
CRITIS
2016
11th International Conference on Critical Information Infrastructures Security

Call for Sponsors and Exhibitions

A limited number of opportunities are available for organisations and companies that wish to exhibit at this conference.

As a Sponsor or Exhibitor you will be able to present your products and services in the Exhibition Area, which will be located in the heart of CRITIS 2016 event. Conference attendees will have full and frequent access to the Exhibition Area, which will be open continuously during all three days of the conference, so that the Sponsors and Exhibitors will get most of the attention value.

There are three Sponsoring Packages and two Exhibition Packages to choose from (please check conditions and details on the website):

Platinum Sponsor (only one)

- one stand 6 m^2 (with table, 2 chairs, electricity, internet connection)
- one presentation included in the Conference programme (not included into the post-conference proceedings)
- one flyer/brochure in conference bag
- logo on conference bag
- logo on CRITIS 2016 website
- free access for 2 persons (3 days conference and full social programme)

Gold Sponsor

- one stand 6 m^2 (with table, 2 chairs, electricity, internet connection)
- one flyer/brochure in conference bag
- logo on conference bag
- logo on CRITIS 2016 website
- free access for 1 person (3 days conference and full social programme)

Silver Sponsor

- space for one poster/roll-up
- one flyer/brochure in conference bag
- logo on conference bag
- logo on CRITIS 2016 website
- free access for 1 person (3 days conference and full social programme)

Exhibition & Demo Desk (3 days)

- one stand 6 m^2 (with table, 2 chairs, electricity, internet connection, including space for one roll-up)
- logo on CRITIS 2016 website

Poster area (3 days)

- space for one poster / roll-up

Venue

CRITIS 2016 will take place at the International Union of Railways (UIC) Headquarters, in the very heart of Paris, between the banks of the Seine and Champs de Mars, only a foot away from the Eiffel Tower.

Street address:
16 rue Jean Rey, F-75015 Paris, France

More information

If you would like to find out more about CRITIS 2016, travel directions, preliminary programme, etc, then please visit the website at

www.critis2016.org

Photo credit: UIC / P. Fraysseix

Key dates

Submission of full papers:
10 May 2016

Registration open:
1 July 2016

Notification of acceptance:
15 July 2016

Camera-ready papers:
1 September 2016

CRITIS event:
10-12 October 2016

CRITIS 2016

11th International Conference on
Critical Information Infrastructures Security
October 10–12, 2016, Paris, France

Call for Papers open until May 10, 2016, see

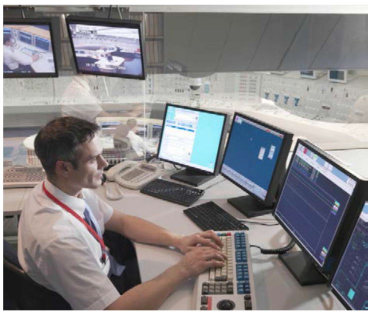
www.critis2016.org

With

3rd CIPRNet Young CRITIS Award

www.critis2016.org/ciprnet-young-critis-award

If you are less than 32 years and you contribute,
You may win extra money: Please apply!



Links

ECN home page	www.ciprnet.eu	
ECN registration page	www.ciip-newsletter.org	Please register free of charge
CIPedia©	www.cipedia.eu	the new CIP reference point

Forthcoming conferences and workshops

ACM CPSS'16	http://icsd.i2r.a-star.edu.sg/cpss16	Call for Paper, Xi'an, China – May 30, 2016
DIMVA 2016	www.dimva2016.org	July 7&8 San Sebastian ES. Call for participation
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016, Davos Switzerland
TIEMS 2016 Annual Conference	http://tiems.info/About-TIEMS/tiems-2016-annual-conference.html	13 – 15 September 2016, San Diego, USA
11th CRITIS Conference	www.critis2016.org	Call for Paper, open to May 10, 2016 Conference Oct,10-12, 2016 in Paris
Cyber Storm	www.swisscyberstorm.com	Oct. 19, 2016 in Lucerne Switzerland

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu
European Organisation for Security	
Netonets organisation	www.netonets.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu
Effective cyber risk management for organisations	www.cyberwiser.eu
Critical Infrastructures and cloud computing	www.ci2c.eu
Security of Railways against Electromagnetic Attacks	www.secret-project.eu
MULTIPLEX - Foundational Research on MULTIlevel comPLEX networks and systems	www.multiplexproject.eu/

Interesting Downloads

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

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security	https://resilience.enisa.europa.eu/nis-platform
Platform Current policy debates	http://digitalwatch.giplatform.org

Cloud Computing and Critical Infrastructure
www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

Websites of Contributors

Acris	www.acris.ch
Campus Bio-Medico di Roma	www.unicampus.it
CINIT National Inter-University Consortium for Telecommunications	www.cnit.it/node/103
EC Joint Research Centre	https://ec.europa.eu/jrc
EOS European Organisation for Security	www.eos-eu.com
H2020	http://ec.europa.eu/programmes/horizon2020
Italian National Agency for new Technology	www.enea.it/en
French Institute of Science and Technology for …	www.ifsttar.fr/en
ITTI Sp. z o.o. e-technology and business	www.itti.com.pl
Übermeister	http://uebermeister.com/homepage.html
Union International Chemin de Fer	www.uic.org
University of Illinois	http://illinois.edu/
University of Malaga	www.uma.es
University of Science and Technology	www.utp.edu.pl/en/start
School for advanced Studies Lucca Italy	www.imtlucca.it

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

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

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

CIPedia© has more than 250.000 qualified clicks and is still growing. Join and look!

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

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

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

Your contribution is essential for putting even more value in the CIPedia© effort.

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

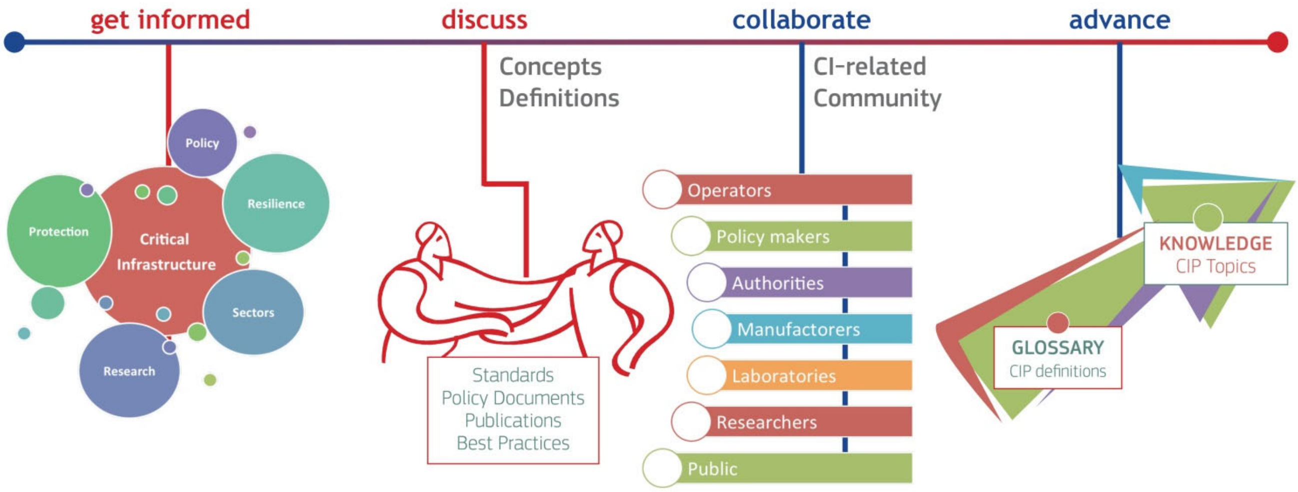
marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.



European CIIP Newsletter

July 16 - October 16, Volume 10, Number 2

CRITIS 2016

Call for

Participation

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

> Spelling:
British English is used except for US contributions

North American and European Views of CIP: What we can learn from each other

"Next stages: the role of human factors in CIP modelling, management, training, and response."

Research on Critical Infrastructure Protection (CIP), including Critical Infrastructure Information Protection (CIIP), has developed tremendously over the last 25 years. The rapid expansion of engineering and computer sciences has led to an impressive progress on modelling, simulation, and analysis that allow us to better respond to a variety of threats, both natural and man-made.

The CIPRNet International Symposium, held in Vancouver, Canada, June 14-15, brought together disaster response practitioners and researchers from Canada, the U.S., and Europe in a two-day forum to exchange ideas and experiences on CIP. The symposium was hosted by the University of British Columbia (UBC), external international partner of the European Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet).

Presentations from North American and European speakers showed similarities in their scientific approaches toward monitoring natural disasters and developing sophisticated preparation and response plans. One notable difference is in information sharing, which is influenced heavily by the vast territory and isolation of jurisdictions in Canada and the U.S. as compared to the geographical proximity among European nations. In Europe, multinational political issues require prearrangements of common actions, whereas in North America greater collaboration is needed to cover extensive territories. As a result, sharing of information in Europe is more regulated, while in NA it is more on an ad hoc basis and is dependent on establishing trust among individuals of different organizations.

A theme that emerged in the symposium, particularly from Canadian presenters, is the need to incorporate human factors in disaster response plans. In this context, researchers at UBC currently are advancing modelling and simulation that incorporate human factors as part of the complex system of systems model, and, as an integral objective in the optimization of resilience and response actions.

Human aspects, such as human emotion, cognition, and behaviour in crisis situations still need to be better understood. Behavioural and social sciences as well as research on human factors have much to offer in this applied area. This could be achieved in the future by fostering collaborative research in at least four directions: better preparation of first responders, raising awareness among citizens, learning from survivors, and better understanding the factors that determine human response and human well-being.

The professional responding bodies, such as the staff working in fire brigades, police, medical emergencies, civil protection, command and control centres, etc. often face poor communication, lack of relevant information, or inappropriate decisions that impair their professional performance.

Moreover, crisis research has shown that lay citizens often respond at least as effectively as well-trained emergency personnel. While fear is the dominant emotion across different types of disasters, it appears that in most cases panic does not take over rational behaviour. The social media effect emphasizes the citizen's role in mass crisis dissemination and information flows.

Last but not the least, disaster survivors and witnesses may provide useful feedback and lessons learned from their experience with various threats.

Some of these challenging topics will be addressed during the **11th edition of the CRITIS conference** which is scheduled from 10–12 October 2016 in Paris: www.critis2016.org

Enjoy reading this issue of ECN!

José R. Martí

Professor of Electrical and Computer Engineering at the University of British Columbia in Canada, Fellow IEEE and of the Canadian Academy of Engineering.
e-mail: **jrms@ece.ubc.ca**

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

European Safety, Reliability and Data Association

Clermont-Ferrand, France

October 20th – 21st, 2016

51st ESReDA Seminar on

Maintenance and Life Cycle Assessment of Structures and Industrial Systems

www.esreda.org/events

The Life Cycle Analysis of structures and infrastructures is a challenging topic, where reliability, durability, robustness and resilience have mandatory roles, in addition to economic and political considerations. The life cycle involves all events and operations occurring during the structural lifetime, such as design, construction, testing, use, degradation, inspection, monitoring, maintenance, repair, failure, and recycling. The life cycle management implies not only optimal design of structures and systems, but mainly the degradation handling through monitoring, inspections and maintenance interventions. The random environment and operating conditions that structure can meet during its lifetime make the deterministic predictive models insufficient to fit the safety and reliability requirements. Therefore, the life cycle management should take into account the uncertainties and variability all over the life span and for the whole system, including electronics associated to mechanics or hydraulics. There are therefore real needs to balance conflicting requirements, such as cost, performance, safety, reliability, etc., taking into account non-technical issues such as organisational or financial parameters related to design, use and operation. The above aspects are targeted by the ESReDA project group ROLCCOST: "*Reliability-based Life Cycle Cost Optimization of Structures and Infrastructures*".

CIRAS: Critical Infrastructure Risk Assessment Support

The CIRAS project is a research project co-funded by the DG HOME CIPS Programme. The CIRAS Decision Support System provides a comparison of different Security Measures Alternatives by performing several assessments.

Introduction

From some time past ensuring the security of critical infrastructures has become a serious concern and priority.

As a result policies are being adopted and defined at national and international level. For instance one of the targets of the Sendai Framework for Disaster Risk Reduction is " *Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030.* " This is so important a framework that the United Nations Office for Disaster Risk Reduction (UNISDR) has been tasked to support the implementation, follow-up and review it. At European level there are several dedicated research programmes focusing on critical infrastructures.

Nowadays decision-makers are facing more and more threats in a challenging and evolving situation where they may follow different approaches and alternatives.

Thus, adopting the best possible decision to achieve the required protection for infrastructures, as well as the people around them, has become a real need. The staff in charge must assess thoroughly the available information to reach the highest accomplishment.

The CIRAS project is devoted to the advancement of protection of critical infrastructures in Europe. It is a two-year project which was launched in September 2014 by the European Commission's Directorate-General for Home Affairs from a call for proposals on Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks (CIPS).

CIRAS aims at supporting decision-makers by providing a methodology and toolset to compare several alternatives. The project promotes a new approach to risk assessment in critical infrastructure protection (CIP). It is focused on advanced risk assessment which compares security measures alternatives and takes into account the typical critical infrastructure (CI) effects of interdependencies of systems, and of cascading and escalation of incident consequences.

The CIRAS project exploits and extends methods of the already completed FP7 ValueSec project by adapting them to the specific needs of critical Infrastructures. (www.valuesec.eu)

Project Outcomes

The CIRAS project provides a methodology and decision support system (DSS) for public and private CI/CIP managers, which allow a holistic assessment of how to reduce risks in critical infrastructures at a cost-efficient way, and at the same time considering social and political needs and restrictions.

The CIRAS Decision Support System offers a comparison of different security measures alternatives that may comprise several security measures by performing several assessments as follows:

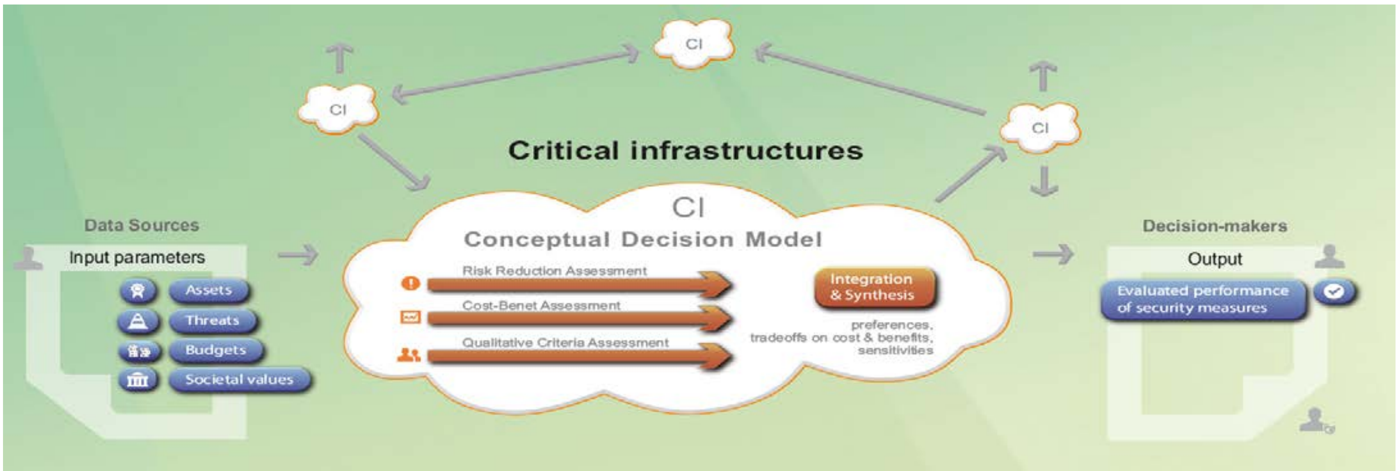
- **Risk Reduction Assessment (RRA):** for measuring the risk reduction capability of the different Security Measures and the Alternatives that include them. It implies two steps: first of all, an Asset oriented Business Impact Analysis is done to evaluate the consequences and impact levels in case of an incident. Secondly, an Asset Oriented Risk Analysis is carried

Jaime Martín Pérez

is Deputy Head of the Homeland Security and Defence Sector of the Research and Innovation group of Atos. Jaime is the coordinator of CIRAS project, which belongs to the aforementioned sector.
He has strong managerial and technical skills which he has proven in European research projects in the scope of security. His expertise covers critical infrastructures, decision support systems, crisis management, society resilience, risk analysis, eID and privacy.

He has experience managing consortia teams across different countries and as speaker in international symposia and conferences and as chairman in international research workshops.

e-mail: jaime.martinp@atos.net


CI
CI
CI
Critical infrastructures
CI
Conceptual Decision Model
Data Sources
Input parameters
Assets
Threats
Budgets
Societal values
Risk Reduction Assessment
Cost-Benet Assessment
Qualitative Criteria Assessment
Integration & Synthesis
preferences, tradeoffs on cost & benefits, sensitivities
Decision-makers
Output
Evaluated performance of security measures

out to calculate the risks levels that would be achieved after the implementation of security measures alternatives.

- **(CBA)**: for assessing the different alternatives based on the cost (immediate and operational) and future benefits of the Security Measures considered during a certain period of years. These costs are evaluated according to different financial categories and the results comprise key indicators values such as: total investment costs, total future benefits and current value of costs. These indicators allow to rank the alternatives and to select the most financially reasonable. The results provide graphs for each financial category and the calculation of time-profile trade-offs and break-even points.

- **Qualitative Criteria Assessment (QCA)**: for the assessment of "social" and other non-tangible criteria related to the Security Measures, thus putting into numbers these criteria that are, otherwise, difficult to measure objectively.

  CIRAS offers two ways of performing this kind of assessment. On the one hand, QCA could be performed via a Utility Function based method (UFBA). It allows to associate verbal subjective descriptions with numerical graphs to quantify the extent of the possible values. On the other hand, CIRAS introduces an innovative method developed within the project called MAHP. It is a modification of the AHP concept introduced by Thomas Saaty in the 1990s

- Finally, **Aggregated Results** are provided to compare all the alternatives individually and together considering the assessments performed. A report is generated displaying in tables and graphs how security measures alternatives are ranked according to RRA, CBA, QCA. If both ways of QCA have been carried out it means a specific rank for UFBA and another one for MAHP.

Conceptual Decision Model

The picture above depicts the CIRAS Conceptual Decision Model. Initial input parameters are needed to properly define the scenario where decision-makers are required to select the most suitable alternative among several available options. This information comprises the assets to be protected, the threats that may harm these assets, the budget to buy or maintain security measures and societal criteria to be taken into account for acceptance

Then several assessments are performed in parallel:

- Risk Reduction Assessment
- Cost-Benefit Assessment
- Qualitative Criteria Assessment: it may be done by means of UFBA and/or MAHP.

The same set of security measures alternatives are compared in all the assessments and specific results are achieved by each kind of assessment. Finally, a set of reports are generated providing a summary of the key results which were concluded in the previous analysis, in a simple or more thorough way according to the end-user´s preference.

The shortest version of the summary report is just one-page long and it makes it possible to have at a glance a comparison of the security measure alternatives considering all assessments carried out. It displays the results in tables where alternatives are ranked and makes it possible to have a quick idea at a glance with bar charts showing the values got. An alternative could be the best according to an assessment but the worst according to another one. It will be up to the decision-maker to balance the ranks and choose wisely. For instance, if there is a clear threat the RRA results should be prioritized no matter the costs.

Engagement of stakeholders

End-users and stakeholders are key to research projects in order to prepare sound and meaningful use cases, and to provide their know-how of daily business. In order to gather their useful input a big group of stakeholders were invited to two public workshops which were organized.

A large spectrum of needs and requirements were identified in the first workshop that took place in Katowice, Poland, on March, 5th, 2015. User related requirements mainly refer to functional properties of the toolset, e.g. concerning quantitative analyses of costs and benefits of security measures, qualitative criteria (like societal, political, legal etc.) to assess the positive and negative impacts of security measures, calculation and presentation of risk reductions etc.

The second workshop was organized in Aschaffenburg, Germany, on November 26th, 2015 to show the methodology and to gather valuable information to identify use cases that

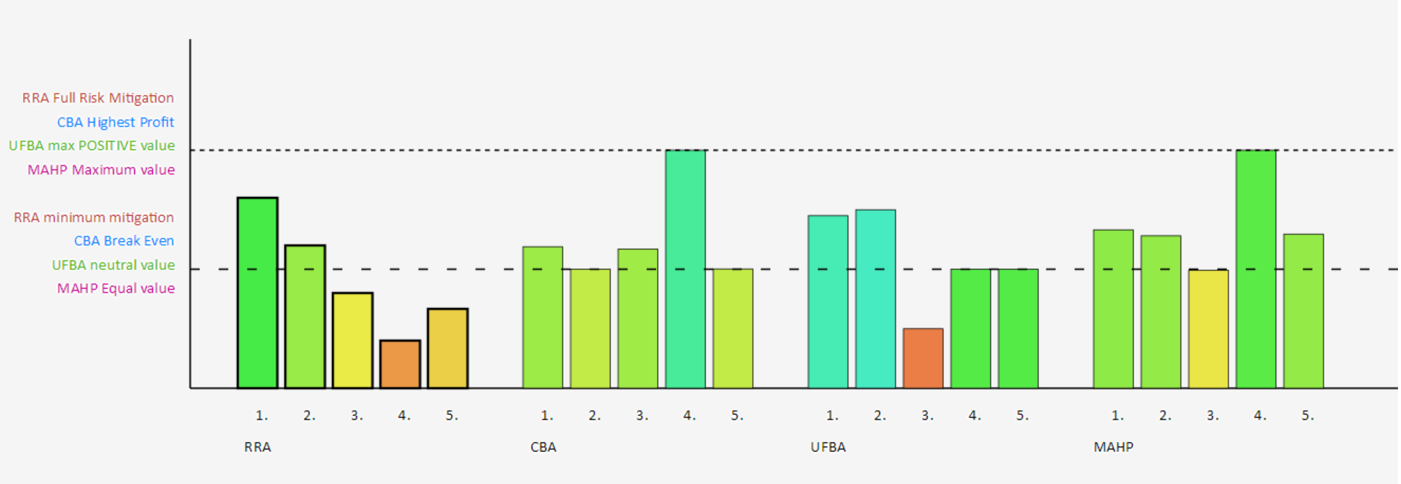


Figure 2: Example of aggregated result

could be suitable to test the framework that CIRAS will provide in the last stage of the project.

As a result of these workshops some stakeholders started to cooperate closely with the consortium for the preparation and validation of use cases

A final conference was organized on June, 8th, 2016 in Katowice where the main outcomes were presented. On top of that a demo of the prototype was done for the audience.

Validation: Use cases

Six use cases were carried out with the following goals:

- To validate CIRAS usability for real challenges
- To validate the final users' requisites by using real scenarios and simulation data
- To obtain feedback of real users for further improvement

The use cases were grouped according to the Critical Infrastructure they were related to: Transportation and Energy.

Transportation use cases

Transit systems offer an easy target for high order violence. Transit systems combine high visibility with a design created for openness and easy access. The high number of people using public transportation means in predictable routes at fixed times make control and security a demanding challenge. Metro offers a big target for any kind of criminal threats, especially those related with the low intensity crime. It has many potential targets concentrated in a small area that leave the platforms and trains very fast, not to return in many hours. At the same time, metro systems are created to be open and easy to enter and leave fast, making controls very difficult.

Three use cases were prepared regarding Transportation CIs. Stakeholders involved were Transports Metropolitans de Barcelona (TMB) as main subject and Mossos d'Esquadra (Catalonian Police) in its Metropolitan Transport Security Area. Several bilateral meetings were arranged with them to define the use cases detailing the relevant assets, potential threats and a list potential security measures which could be assigned to deal with one or more threats. Also in the meetings the progress of the prototype were shown.

Use cases had as common location the facilities of the metro network of the city of Barcelone, Spain.

The use cases were the following:

- Bomb at metro maintenance facilities during the night: it implies the trespassing of the metro depot and workshop facilities (jumping fences, breaking access doors and so on) and placing a bomb there during the night (while trains are in maintenance and being cleaned).
- Stabbing during rush hour: This scenario covers the act of stabbing at random in a metro platform during rush hour. It means the use of concealed knives, machetes or other sharp weapons like screwdrivers or even broken glass.

Energy use cases

Power plants are mostly very large and complex facilities and of high national or international relevance. Therefore, they need extended protection especially against terrorist attacks.

Three use cases were prepared as far as Energy CIs are concerned. They were carried out in cooperation with one of the biggest energy operators in Poland which provides energy to several million of private and business customers.

The use cases were the following:

- Bomb brought to a power plant and to a substation: simulating that a person has succeeded to pass the entrance control or overcome fences or walls around the plant carrying a bomb.
- Sabotage in a power plant to disturb the energy production or decrease it to zero: Sabotage performed by employees with a criminal or terrorist motivation is an ongoing threat which needs special protection measures (not necessarily technically oriented).
- Cyberattack in a power plant to disturb the energy production or decrease it to zero: Cyberattack to the control system of a power plant and the power network to decrease the power distribution

CIRAS tool has proven a real success in the described use cases for both Transportation and Energy CIs. The tool's flexibility in the combination of different Security Measures and the possibility of recovering previous recorded scenarios make the tool ideal for the objective of the evaluation of different Security Measures alternatives.

CIRAS has been validated and tested in transportation and energy Critical Infrastructures. A total of six use cases were carried out to compare security measure alternatives.

The Decision Support System (DSS) has proven a real success in the use cases for both kinds of CIs. The tool's flexibility in the combination of different Security Measures and the possibility of recovering previous recorded scenarios make the tool ideal for comparing several options.

The aggregated results make it possible to have at a glance a comparison of the security measure alternatives considering all assessments performed.

The consortium

The CIRAS Consortium comprises three partners:

- **Atos** Spain: Atos SE (Societas Europaea) is a leader in digital services with 100,000 employees in 72 countries. The Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation. Atos Research & Innovation (ARI), whose headquarters are in Spain is the research, development and innovation hub of Atos and it is a key reference for the whole Atos group, delivering technology innovation to our customers.

- **CESS**, Germany: CESS provides strategic, operational and technical security and risk management expertise. It has competences in security and defense consulting, decisions support systems, analytical methods and tools, scenario development and modelling and simulation.

- **EMAG**, Poland: EMAG's R&D include competences in information society issues, especially in ICT security and safety and ontology-based information systems including development of computer-aided tools to support information security Management.

Would you like to find out more about CIRAS please visit our website at www.cirasproject.eu/
or contact us via the form at www.cirasproject.eu/contact

Air Traffic Management: moving towards Cloud Computing?

Air traffic management (ATM) is undergoing a major modernisation programme in Europe, the US and other parts of the World. Ancillary closed analogue ATM systems are in the process of being replaced by digital, network enabled communication, navigation and surveillance technologies, which will exponentially increase connectivity and data sharing.

The Air Traffic Management System, in Europe, today, represents a total revenue of about B€9/year, related to air navigation charges. EUROCONTROL, the European Organisation for the Safety of Air Navigation, is the EU network manager and looks after flows totalling approximately 30,000 flights per day. www.eurocontrol.int

Air traffic management in Europe employs around 58,000 people, of whom approximately 17,000 are air traffic controllers.

ATM Security

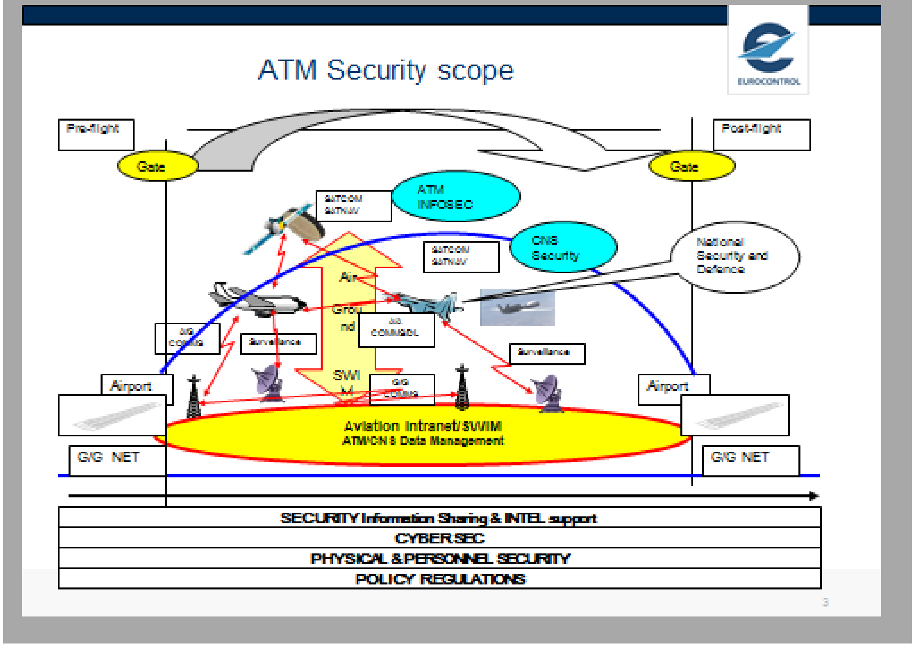
The protection of the ATM infrastructure follows a layered approach and is a combination of:

1. Legal framework: regulations, policies and standards.2. Personnel and physical security measures.
3. Cyber security, which in ATM includes information and communication security.
4. Security information sharing.
5. Intelligence support.

ATM Security focuses on the protection of ATM infrastructure, personnel and data. This infrastructure consists of ground, airborne and space based facilities and assets (e.g. aircraft, civil and military, including RPAS (remotely piloted aircraft systems) communication, navigation and surveillance (CNS) infrastructures, information systems and networks and the associated data and data flows).

ATM security refers not only to the tactical phase of aircraft movements but also to the pre-flight and post-flight phases.

ATM has an obligation to support the overall aviation security, national security and defence and law enforcement.



ATM Security scope

SECURITY Information Sharing & INTEL support
CYBER SEC
PHYSICAL & PERSONNEL SECURITY
POLICY REGULATIONS

Antonio Nogueras

Antonio Nogueras is the Head of the Air Traffic Management Security Unit at EUROCONTROL (the European Organisation for the Safety of Air Navigation). The Unit’s work programme focusses on enhancing current levels of Air Traffic Management security through international collaboration and implementation support to Member States and stakeholders.

e-mail:
antonio.nogueras@eurocontrol.int

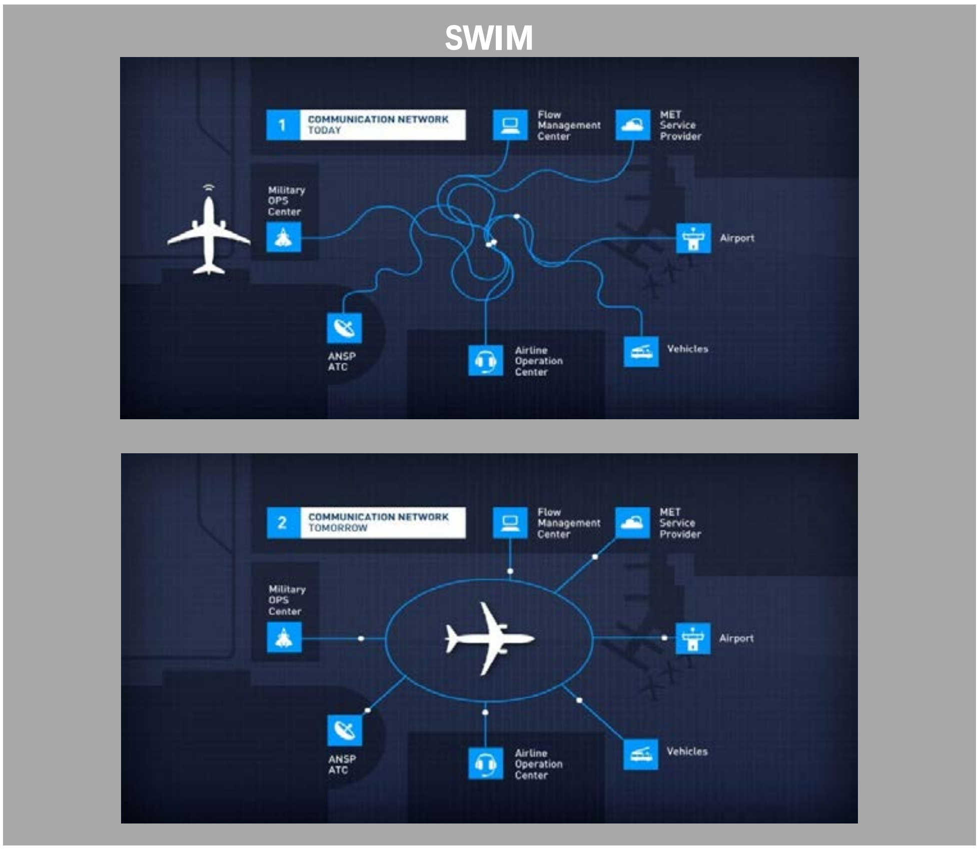
EUROCONTROL
96 Rue de la Fusée, 1130
Brussels, Belgium

SWIM
future aviation intranet

Ongoing ATM modernisation programmes will rely on the concept of System Wide Information Management (SWIM), which is expected to be a global aviation intranet able to safely manage a huge amount of ATM and CNS (communications, navigation, surveillance) data.

SWIM consists of “standards, infrastructure and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services.” This is expected to bring enormous benefits in terms of airspace capacity, cost-efficiency and safety.

Indeed, SWIM means a massive migration from ancillary closed ATM systems to new technologies facilitated by digital and cyber space. As a consequence, for the first time, ATM will have to face (is already facing) the impact of ‘Malspace’. http://www.eurocontrol.int/swim

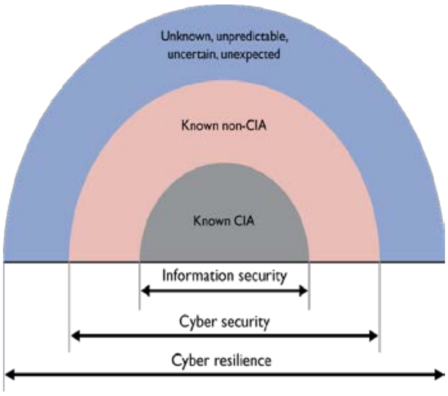


The goal: cyber resilience

There’s no doubt that the future ATM system, operating in a net centric SWIM enabled environment, will be subject to cyber-attacks. Nevertheless, ATM should achieve acceptable levels of resilience, ensuring safety and service continuity for air operations.

Cyber resilience means a defence in depth or a layered approach to security:

- Information security provides the first layer to tackle ‘known CIA’ (confidentiality, integrity and availability) requirement. Its aim is to achieve information assurance, and it includes personnel and physical security requirements, governance, policy making (e.g. for SWIM), liability and audits. In the aviation environment, information security should be tackled at the level of the national Civil Aviation Security Committee, which is the governance level for aviation security in the Member States.
  Information security includes ICT security, which is a technical layer, at the level of the entities responsible for implementation of the security requirements derived from the Aviation Security Committee.



- Cyber security provides the second layer, to tackle ‘known non-CIA’ threats, e.g. APT (advanced persistent threat). Cyber security is a transversal cross domain issue where interdependencies need to be considered, e.g. for incident management and information sharing regarding critical information infrastructures protection (CIIP). Cyber security also requires civil military cooperation and public private partnership.
- Finally, cyber resilience provides the umbrella to deal with the unknown/unpredictable/uncertain/unexpected threat.

Cyber security is a term used generically but may well become meaningless unless it is framed in the proper context.

The EU provides for such a context within its Cyber Security Strategy and its associated Network and Information Security Directive, and Directive 2008/114/EC on the ‘Identification and Designation of European Critical Infrastructures (ECI)’.

It requires the putting in place of robust crisis management capabilities; incident management will not be sufficient since incidents might often escalate to actual crises. Cyber resilience cannot be achieved without international collaboration at political and strategic level, which includes intelligence support. For ATM, this would mean that, even when under attack, safety is maintained as well as an acceptable level of air navigation service provision.

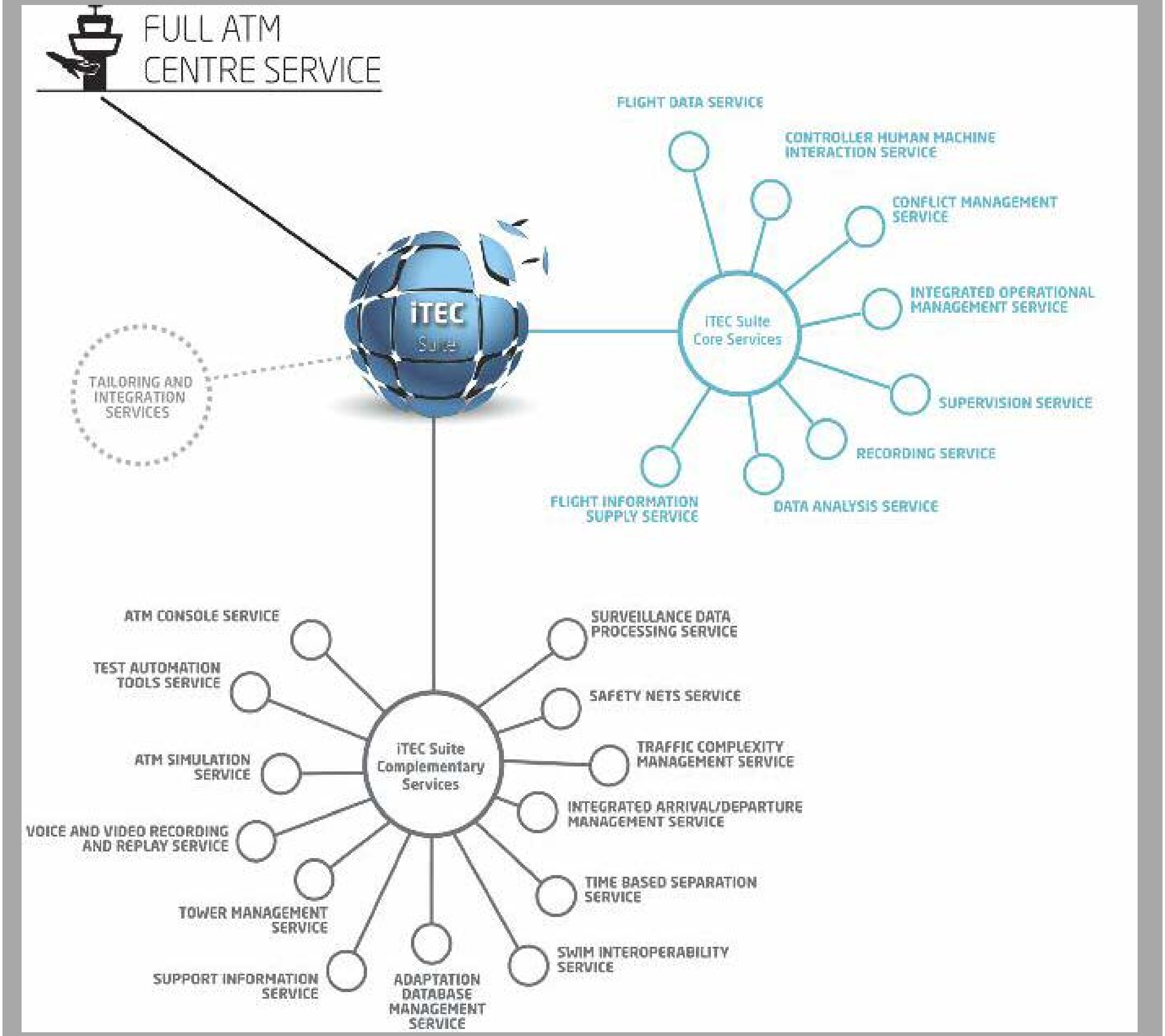
ATM on the move

A number of initiatives at global and regional level show the way in which ATM is moving:

- ICAO is embarked on the implementation of the Global Air Navigation Plan (GANP), which depends on a number of 'Performance Improvement Areas'. One of these areas is 'Globally Interoperable Systems and Data – through Globally Interoperable System Wide Information Management (SWIM)'.
- As part of the GANPG, and also facilitated by SWIM, air traffic flow management (ATFM) is going global. It envisages the exchange of standardised data across all relevant ATM partners at global level. This will facilitate Collaborative Decision Making and greater coordination of the ATM community.
- EUROCONTROL is developing Centralised Services (CS) for ATM. The aim of the CS is to provide air navigation support services run at network level, rather than at regional or national level, thus improving overall performance. These CS include ATM Information Management; a European Traker Service (to provide a consistent picture of the air situation for air traffic controllers); and a ground to ground Pan-European Network, to be the sole infrastructure supporting ATM operations in Europe, etc. www.eurocontrol.int/centralised-services

It should be noted that the Military ATM community, as part of their 'Initial Military Security Requirements for Centralised Services' have stated that: *'Military sensitive data shall not be stored on laptops, Portable Storage Devices, External / cloud storage,*

iTEC Cloud


FULL ATM
CENTRE SERVICE
iTEC
Suite
TAILORING AND INTEGRATION SERVICES
iTEC Suite Core Services
FLIGHT DATA SERVICE
CONTROLLER HUMAN MACHINE INTERACTION SERVICE
CONFLICT MANAGEMENT SERVICE
INTEGRATED OPERATIONAL MANAGEMENT SERVICE
SUPERVISION SERVICE
RECORDING SERVICE
DATA ANALYSIS SERVICE
FLIGHT INFORMATION SUPPLY SERVICE
iTEC Suite Complementary Services
ATM CONSOLE SERVICE
TEST AUTOMATION TOOLS SERVICE
ATM SIMULATION SERVICE
VOICE AND VIDEO RECORDING AND REPLAY SERVICE
TOWER MANAGEMENT SERVICE
SUPPORT INFORMATION SERVICE
ADAPTATION DATABASE MANAGEMENT SERVICE
SWIM INTEROPERABILITY SERVICE
TIME BASED SEPARATION SERVICE
INTEGRATED ARRIVAL/DEPARTURE MANAGEMENT SERVICE
TRAFFIC COMPLEXITY MANAGEMENT SERVICE
SAFETY NETS SERVICE
SURVEILLANCE DATA PROCESSING SERVICE

© EUROCONTROL- Skyway Autumn/Winter 2015

Bring your own device (BYOD), etc.' However, it might be possible for them to accept a 'private cloud'.

Industry paving the way

The air navigation service providers (ANSPs) of Spain, the UK, Germany and the Netherlands, and the company INDRA as the technological partner, together launched in March 2015, at the Madrid World ATM Congress, the iTEC Cloud concept.

This concept opens up new business opportunities in the ATM market, e.g.:

- To provide infrastructure solutions to ANSPs willing to deploy and use an 'internal Cloud', supporting various IT services.
- To develop an 'iTEC Cloud' to provide ITec software-based services to consortia, e.g. applying to EUROCONTROL Centralised Services.
- To be able to provide services based on iTEC software to ANSPs, airports, airlines, and all other entities requiring such solutions. www.eurocontrol.int/download/publication/node-field_download-9852-0

ATM as critical infrastructure

Many countries have already included ATM infrastructures in the list of national critical infrastructures.

At European level, Council Directive 2008/114/EC, on *'the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection'*, was followed in 2013 by a Commission Staff Working Document, on *'a new approach to the European Programme for Critical Infrastructure Protection'.* The document identifies the following four critical infrastructures with a European dimension: EUROCONTROL, Galileo, the electricity transmission grid and the gas transmission network. Discussions with competent national authorities are ongoing regarding EUROCONTROL.

Additionally, the EU Directive concerning measures for a high common level of security of network and information systems across the Union (the so called NIS Directive), identifies ATM as an *'essential service for the maintenance of critical societal and/or economic activities'*.

Final thoughts

Going back to the title of this article; is Air Traffic Management moving towards Cloud Computing (?). The answer is YES (ATM is already partly moving towards Internet based infrastructures so in principle there's no reason why it should exclude the iCloud); BUT it won't be a 'Big Bang'.

ATM is a 'conservative' environment, which tends to move slowly (only aircraft move fast!). And there is a good reason for this, 'Safety First'. Any change in ATM requires the implementation of a very demanding safety case, to ensure that the same or even higher levels of air safety are maintained.

Additionally, Cost and Operational Benefit Analyses must support any evolutions in ATM.

Finally, the study of security considerations is becoming more relevant than ever before new concepts or technologies are introduced (e.g. Military requirements in civil-military ATM).

Therefore, safety critical and security sensitive data is unlikely to move to the iCloud, at least in the short term.

With all the caveats expressed above, we could envisage a partial migration of ATM to cloud services via 'Cloud service providers for ATM', as the iTEC Cloud experience, which could provide services to individual stakeholders, consortia, a country or group of countries, or even at regional and global ATM Network level.

CIPRTrainer – simulation-based »what if« analysis for exploring different courses of action in crisis management

The EU FP7 project CIPRNet developed an application that provides a new capability for training crisis managers. Computer simulation of complex crisis scenarios allows 'going back in time' and trying different options. Different outcomes can be assessed by means of Consequence Analysis.

The EU FP7 Network of Excellence CIPRNet has developed CIPRTrainer, an application that provides a new capability for training crisis management (CM) staff. It enables exploring different courses of action and comparing their consequences (»what if« analysis) in complex simulated crisis and emergency scenarios. The simulation employs threat, impact, and damage models and is based on federated modelling, simulation and analysis (fMS&A) of Critical Infrastructures (CI).

The management of a disaster or crisis typically consists of cycles of situation update, decision taking, planning, and execution of response actions, sometimes under severe time pressure. At decision points, crisis managers often do not have just one option for action, but several. The challenge is to take a well-informed and most effective decision. Insufficient awareness of the role of Critical Infrastructures [2] and incomplete information on consequences of crisis or disaster evolution [4] contribute to that challenge. In most cases, it is not possible to revert a decision or an action already taken – in reality. However, in *simulation* it is possible to do exactly this: 'go back in time' and explore a different course of action. This constitutes an unprecedented training opportunity that complements standard command post, table-top, or physical exercises.

The expected benefits would be increased awareness of crisis managers of the role and behaviour of interconnected Critical Infrastructures in disasters, emergencies, and crisis situations, and a better understanding of possible consequences of scenario evolution and the influence of own actions.

CIPRTrainer system

CIPRTrainer is the software system that enables crisis managers to train decision-making in crises involving cascading effects of Critical Infrastructures. At the front end, the prototypical training system presents itself to the user as a single-page web application. Its back end includes a federated simulation of three Critical Infrastructure simulators, a scenario database, a consequence analysis module, a complex event processor, and a threat simulation (flooding) [1].

> The combination of federated CI simulators for simulating cascading effects, the »what if« analysis for exploring different courses of action, and the consequence analysis for assessing overall consequences constitute the added-value of CIPRTrainer.

Scenarios for training

One design goal of CIPRTrainer was a wide applicability of the system, including crisis situations with cross-border effects. We picked a region spanning both sides of the border of two countries represented in the CIPRNet consortium: Germany and The Netherlands. The geographical location is restricted to the Kleve district in Germany and the city region of Arnhem-Nijmegen in the Netherlands. The area is prone to flooding by high water levels of the river Rhine. Also, it contains a number of infrastructures, like the railway line connecting Rotterdam harbour with the European hinterland. In this setting we designed two storylines in a complex scenario with cross-border effects [3].

Erich Rome, Fraunhofer IAIS
Coordinator of CIPRNet
e-mail: erich.rome@iais.fraunhofer.de

Jingquan Xie, Fraunhofer IAIS
Manager CIPRTrainer development
e-mail: jingquan.xie@iais.fraunhofer.de

Betim Sojeva, Fraunhofer IAIS
CIPRTrainer UI designer
e-mail: betim.sojeva@iais.fraunhofer.de

For the development of the scenario, we started with own research on information on and data from the considered region. Data are the basis for modelling the scenario on the computer. Some of the modelled CI networks are fictive for two reasons: first, we did not have data on some of these networks and second, for security reasons, since we did not want to disclose sensitive information. We employed the domain expertise of the consortium, including electrical and telecommunications engineers, security professionals, and experts in railway security, cyber security, crisis management, and the water domain. External expertise was provided by the head of the fire fighters in a large city, and experts from CIPRNet's international advisory board.

Federated CI simulation

For achieving a plausible simulation of the behaviour of CI under perturbations, including failures and cascading effects that propagate failures to other dependent CI, CIPRTrainer employs two commercial simulators (SIEMENS PSS© SINCAL for electricity networks and OpenTrack for railway networks) and one free simulator (ns-3 for telecommunication networks). Information on dependencies between interconnected infrastructures, like which electricity CI element supplies which telecommunication CI element with power, are stored in a database. A failure of the former element triggers a stressed state or failure of the latter element.

Such state changes are represented by software 'events'. Each of the simulators is connected to the rest of the CIPRTrainer system by a special 'connector' that translates 'events' into a format that the simulator can understand. The 'connectors' are also employed for synchronising the simulators and for enabling the rollback, that is, the 'going back in time'.

»What if« analysis

The new »what if« analysis capability enables trainees to explore different courses of CM actions in computer-based simulation (Figure 1). CIPRTrainer displays information on events that happen in the simulation, like a derailment of a cargo train. The system has an inventory of actions available for reacting on the occurring events. Rules within CIPRTrainer provide some additional flexibility. For instance, if a certain response action is being performed by the trainee within a given time window, then it would prevent some disastrous event from happening.

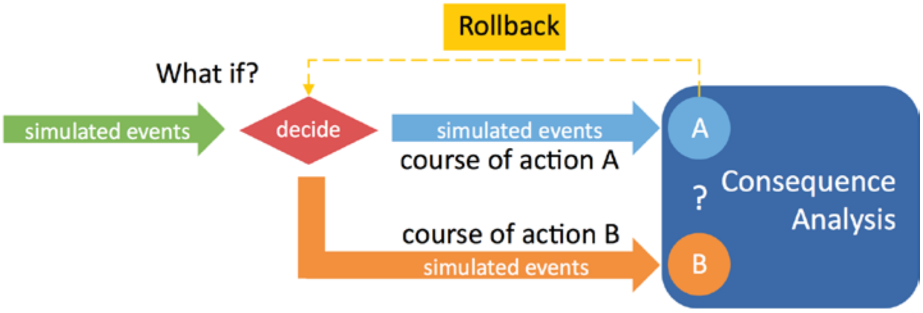
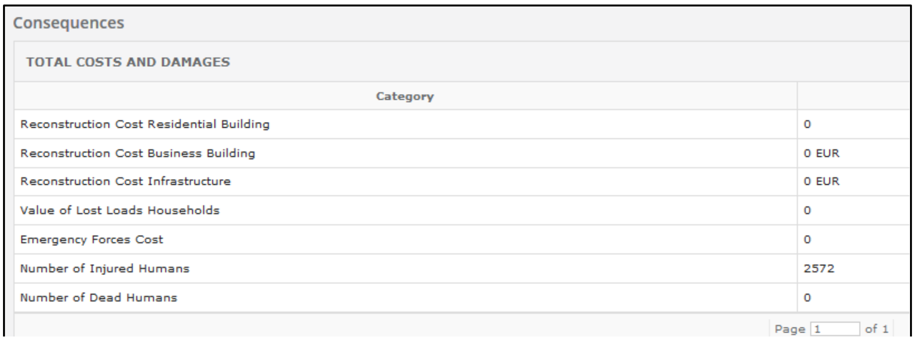


Figure 1: »What if« analysis: After taking course of action A, roll back to decision point, and take different course of action B. Use consequence analysis to compare the overall consequences of both scenario evolutions.

At any time after the simulation started, the trainee may choose to perform a rollback and explore a different course of action. In order to do this, the trainee must select one of the previously performed actions, and then perform the rollback. CIPRTrainer then resets all components (simulators, database, GUI, consequence analysis module) into the state that they had before the selected past action. By following a different course of action, the trainee creates another version of the simulated 'world'.

Such rollbacks can be performed multiple times. Since the history of all performed actions is recorded, the generated courses of actions form a tree-like structure. CIPRTrainer can display this structure for providing an overview of the training activities.



Consequences

TOTAL COSTS AND DAMAGES

Category	
Reconstruction Cost Residential Building	0
Reconstruction Cost Business Building	0 EUR
Reconstruction Cost Infrastructure	0 EUR
Value of Lost Loads Households	0
Emergency Forces Cost	0
Number of Injured Humans	2572
Number of Dead Humans	0

Figure 2: Tabular presentation of consequence analysis results

A core element of the training is evaluating the training session and the performed courses of action. The trainee shall be enabled to find out how the chosen courses of action influenced the overall outcome or consequences of the simulated crisis or disaster. For doing this, the tree-like visual representation of the courses of action serves as starting point for performing Consequence Analysis.

Consequence analysis

CIPRTrainer contains a Consequence Analysis Module (CAM), which enables the user to understand the consequences (in terms of human, service and monetary losses) of the simulated impacts and of the chosen actions (or inactions). The CAM utilises data from the CIPRTrainer database, and an array of methods implemented for calculating the consequences for the population, and the critical and non-critical infrastructure in the affected region.

There are three types of such methods: a) for direct consequences of specific (natural) hazards, like building damage caused by floods or storms; b) more general methods for loss of life [5]; and damage to property; and c) methods for indirect economic damage through the possible inoperability of (critical) infrastructure and economic sectors (input-output-model).

The results are sent to the CIPRTrainer GUI to be displayed for the user. The user can request consequence analysis results for all courses of action explored in the current training session. The GUI can display the consequences in three different ways: a) a tabular / textual representation (Figure 2); b) a presentation as column charts; and c) a geographically mapped and color-coded presentation.

The side-by-side display of the consequences for all courses of action allows also direct comparison of consequences, like in which course of actions occur the least fatalities. Please note that a potential ethical issue could be that a user may weigh human losses against economical damage. It remains the utmost responsibility of the human end-user to comply with ethical standards.

Graphical User Interface

The essential means of CIPRTrainer for displaying information on the crisis situation are maps. That is, CIPRTrainer uses known functions form geographical information systems (GIS), like basic map layers and additional information layers for displaying regional maps, infrastructure networks, positions of hospitals, police stations, and more (Figure 3).

CIPRTrainer has been equipped with a localised graphical user interface (GUI), providing menus in several languages, and also with two sets of tactical CM icons (German and Dutch) for the cross-border scenario. Since In the CM icons are not internationally standardised, it is difficult for CM staff to recognise foreign icons. In the Dutch CIPRTrainer localisation, it is possible to see the Dutch icons on both sides of the border, since CIPRTrainer has an icon translation table. This table is an idea of the EU project FORTRESS and has been extended and updated as a result of cooperation between FORTRESS and CIPRNet. It facilitates identifying which forces or resources from the other country could be used in the local crisis or disaster.

The GUI also supports training a small CM team. For this purpose, there are three different roles for trainees in CIPRTrainer: Situational awareness, operations coordinator, and administrative coordinator. For each of the roles, a specific set of actions can be performed in simulation. CIPRNet has chosen this approach for supporting the wide applicability of CIPRTrainer. A study of the EU project PREDICT showed that although the CM governance structures in different countries vary to a great extent, there are some common roles of CM staff. CIPRTrainer supports the most essential of these roles.

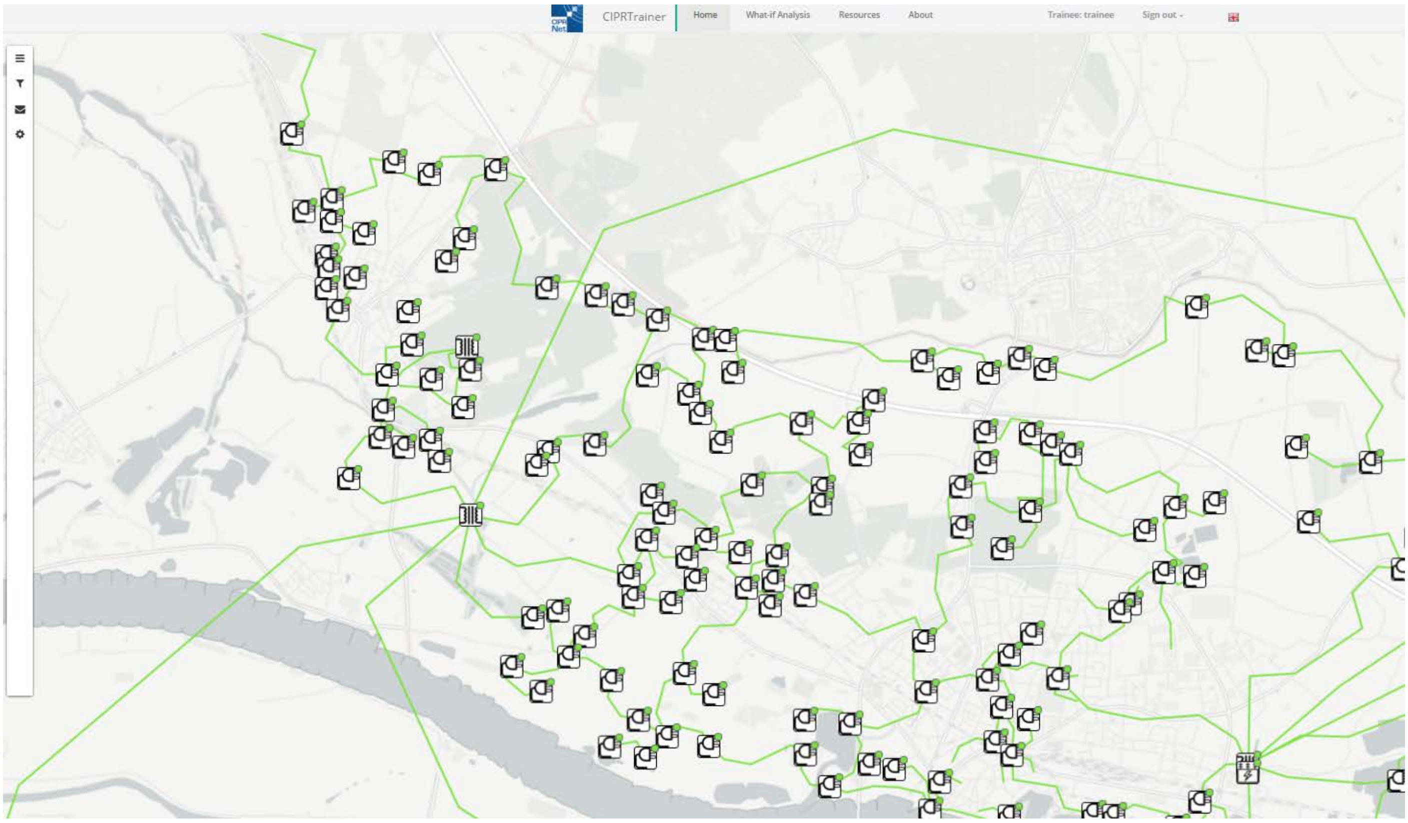


Figure 3: GIS functionality of CIPRTrainer: Information layer showing artificial telecommunication network. Green lines and green ‘LED’s at router icons indicate that the network is fully functioning

Conclusion and Outlook

CIPRTrainer provides a new capability for training crisis management staff. It enables exploring different courses of action in complex simulated crisis scenarios involving CI. For comparing the consequences of the scenario evolution and assessing the outcomes of the chosen courses of action, CIPRTrainer uses Consequence Analysis methods. Federated simulation of CI provides information on disaster impacts like CI outages and resulting cascading effects.

Domain experts like electrical engineers, telecommunication and railway experts, and fire-fighters have supported the modelling activities required for creating realistic scenarios and user roles in CIPRTrainer [3]. CIPRTrainer has been demonstrated at the second CIPRNet review, at a meeting of the VRGeo consortium for stakeholders in the oil and gas industry, and for young professionals studying for the Master in Homeland Security at Università Campus Bio-Medico di Roma. More demonstrations and training events are planned. Systematic acquisition and evaluation of end user feedback will help improving the system further.

Disclaimer and Acknowledgement

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

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

The authors gratefully acknowledge the contributions of the CIPRNet project team! A special acknowledgement goes to Thomas Doll, Stefan Rilling, and Norman Voß of Fraunhofer IAIS.

More information

If you would like to find out more about CIPRNet, then please visit the project website at

www.ciprnet.eu

Check out CIPedia©, CIPRNet's popular online glossary of CIP related terms at

www.cipedia.eu

Forthcoming training event: CIPRNet Master Class in Sankt Augustin, end of November 2016. Watch the CIPRNet website for announcement.

References

[1] EU FP7 CIPRNet, Fraunhofer, Deliverable D6.4 – Implementation and integration of the federated and distributed cross-sector and threat simulator, Fraunhofer IAIS, Sankt Augustin, April 2016

[2] Luiijf, E., Klaver, M. "Insufficient Situational Awareness about Critical Infrastructures by Emergency Management", in: Proceedings Symposium on "C3I for crisis, emergency and consequence management", Bucharest 11-12 May 2009, NATO RTA: Paris, France. RTO-MP-IST-086

[3] Xie, J., Theocharidou, M., Barbarin, Y., Rome, E.: Knowledge-driven scenario development for critical infrastructure protection. In: Rome, E., Theocharidou, M., Wolthusen, S.D. (Eds.), Critical Information Infrastructures Security, 10th International Workshop, CRITIS 2015, Berlin, Lecture Notes in Computer Science, Vol. 9578, Springer, Heidelberg, 2016, pp. 91-102

[4] Klaver, M.H.A., Luiijf, H.A.M., Nieuwenhuijs, A.N., Van Os, N., Oskam, V., Critical Infrastructure Assessment by Emergency Management, in: Rome, E., Theocharidou, M., Wolthusen, S.D. (Eds.), Critical Information Infrastructures Security, 10th International Workshop, CRITIS 2015, Berlin, Lecture Notes in Computer Science, Vol. 9578, Springer, Heidelberg, 2016, pp 79-90

[5] Jonkman, S. N.; Lentz, A.; Vrijling, J. K. (2010): A general approach for the estimation of loss of life due to natural and technological disasters. In: Reliability Engineering & System Safety 95 (11), p. 1123–1133.

Smart Mature Resilience project: European Resilience Management Guideline

Resisting, absorbing, accommodating and recovering from the effects of man-made and natural hazards

The 21st Century has been termed "the century of disasters" (Jan Egeland, former United Nations Undersecretary-General for Humanitarian Affairs and Emergency Relief Coordinator, February 2011). Worldwide there were twice as many disasters and catastrophes in the first decade of this century as in the last decade of the 20th Century. Europe is no exception: our continent is affected directly and indirectly. And the trend continues, fueled by climate change and social dynamics.

The need for resilience is emphasized. But how to best deal with known risks and prepare for the unexpected is enormously complex and still nascent. The much needed operationalization of resilience – the breaking down of the resilience concept into a holistic framework of measurable interventions – must be seen as a directed dynamic process: a process that unfolds over time.

How the SMR project meets the challenge

Smart Mature Resilience (SMR) is developing and validating the European Resilience Management Guideline, using three pilot projects. SMR's Resilience Management Guideline will provide a robust shield against man-made and natural hazards, enabling society to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner. The Guideline is constituted by five crucial interdependent supporting tools: a Resilience Maturity Model defining the trajectory of a city through measurable resilience levels; a Systemic Risk Assessment Questionnaire that, beyond assessing the city's risk, determines its resilience maturity level; a portfolio of Resilience Building Policies that enable the city's progression towards higher maturity levels; a System Dynamics Model (computer simulation model) that embodies the Resilience Maturity Model, allowing to diagnose, monitor and explore the entity's resilience trajectory as determined by resilience building policies, and a Resilience Engagement and Communication Tool to integrate the wider public in community resilience, including public-private cooperation.

Beyond delivering the validated Resilience Management Guideline and the five supporting tools the SMR project establishes as a project result an emergent European Resilience Backbone consisting of adopters, from fully committed through direct project participation to alerted potential adopters.

> "SMR's Resilience Management Guideline will provide a robust shield against man-made and natural hazards, enabling society to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner"

The adopters are vertebrae in the European Resilience Backbone. The SMR project's powerful impact maximizing measures will assist the implementation of the European Resilience Management Guideline by consolidating the resilience vertebrae as mutually supporting functional units of a growing and fortified European Resilience Backbone.

The Resilience Management Guideline including the five tools will be developed based on the requirements gathered from CITIES in workshops; which gives the Smart Mature Resilience project a unique advantage concerning project impacts.

Jose Mari Sarriegi

Industrial Engineer (1994, PhD 1999) is a professor of Information Systems, Knowledge Management and Modelling and Simulation at TECNUN. His research interests include security management, knowledge management and complex systems modelling. He has led several research projects in all these topics. He has been coordinator of the FP7 ELITE project.

He has published in journals such as IEEE Software, International Journal of Computer Integrated Manufacturing, IEEE Internet, Journal of Homeland Security and Emergency Management, Journal of Technological Forecast and Social Change, International Journal of Critical Infrastructures, as well as in conference proceedings such as in the Lecture Notes in Computer Science.

email: jmsarriegi@tecnun.es

The SMR Approach

Our units of analysis are entities that we denominate by CITIES (with upper case characters). Each CITY (Bristol, Donostia/San Sebastian, Glasgow, Kristiansand, Riga, Rome and Vejle) is analyzed in the perspective of serving their citizens and their metropolitan area, with the Critical Infrastructures (CIs) residing in or affecting such area, in their functional role as part of Europe in a multi-level governance perspective, and linked with other CITIES by shared interests and responsibilities through formal and informal networks so as to yield a resilience backbone.

We have engaged seven cities as partners in our proposal. In our project they appear as entities where critical infrastructure is situated, where human dynamics plays out, where the threats in question (man-made/natural) most likely will unfold, where rescuers, volunteers and the media are found and have their strengths and where a public-private cooperation has its strongest playground.

We also recognize and address the fact that resilience requires community engagement and public-private cooperation in our choice of stakeholders and in the paths of dissemination and training. Further, the concept of resilience backbone consisting of mutually supporting and networking CITIES enables the feasibility of substitution processes in a crisis or disaster, to deal with a lack of material, technical or human resources or capacities.

Each CITY has been performing specific actions towards resilience in different ways. Some of them have been working for several years on the concept of resilience while others have just started. Therefore, the requirements each of the CITIES have are not the same. In fact, a CITY that has been developing resilience building activities for several years will require different activities than a CITY that has just started the path of developing this concept.

Although the CITIES taking part in the project vary significantly, they have accepted as valuable the definition of every stage of the SMART Maturity Model. They have also contributed to the definition of a set of policies for every maturity state. These policies act as an operational guide for the development of Resilience within CITIES.

SMR project has implemented four workshops to analyze potential crises caused by dependencies from Critical Infrastructures, Climate Change and Social dynamics.

The SMR Circle of Learning and Sharing

A Circle of Sharing and Learning will be used in a four-tier process to reach and engage more CITIES so as to form a growing resilience backbone.

The SMR project has seven partner cities. Three of them (Tier-1 – the earliest adopters) will implement the Resilience Management Guideline, the other four (Tier-2) will be engaged in the pilot implementations as peer reviewers. By their participation in project workshops and their peer reviewing activity, the Tier-2 cities will feel ownership of the tools and the Resilience Management Guideline and become early adopters.

The SMR project will reach out to more cities, first to Tier-3 CITIES, those that form part of established networks (such as UNISDR, European members in 100 Resilient Cities of the World), and then to other CITIES (Tier-4 CITIES).

Scenario planning is a central part of our approach. We will conduct workshops operationalizing resilience in a holistic risk management approach with pilot implementations. Three scenario threads run in parallel, as a whole covering major European natural and man-made disasters with human dynamics and considering cascading effects. The scenarios describe archetypical resilience challenges with European dimension for three different stages of resilience maturity, so as to, in the aggregate, demonstrate and validate pilot implementations of resilience guidelines for the full spectrum of resilience maturity.

Expected impacts

The development of the European Resilience Management Guideline and demonstration through pilot implementation in our network of CITIES will be a direct result of the SMR project. In the last phase of the project we shall vigorously reach out to other potential vertebrae of Europe's resilience backbone (mainly with CITIES as vertebrae) using the 'Circle of Sharing and Learning' described before.

The action is expected to proactively target the needs and requirements of users, such as civil protection units, first responders and Critical Infrastructure providers.

The SMR Consortium

The SMR consortium was selected for the optimal coverage and complementarity of expertise, and consists of 13 partners: The project coordinator TECNUN University of Navarra (Spain), CIEM University of Agder (Norway), University of Strathclyde (UK), Linköping University (Sweden), ICLEI European Secretariat (Germany), City of Kristiansand (Norway), City of Donostia (Spain), City of Glasgow (UK), City of Vejle (Denmark), City of Bristol (UK), City of Rome (Italy), City of Riga (Latvia) and DIN (Germany). This represents an ideal mix of commercial, academic and public collaboration team.

The key strength of the consortium is the experience and mutual trust gained from successful collaborations related to harmonization, standardization and bringing added value to data through networks and project activities.

If you would like to find out more about SMR project, please visit our website at
http://smr-project.eu/home
or email SMRProject@tecnun.es

FS-ISAC: The Financial Services Information Analysis Centre

FS-ISAC is the financial industry's go to resource for cyber and physical threat intelligence analysis and sharing.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was formed in 1999 with a simple mission: help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly functioning of the global economy. Over the years, FS-ISAC has aimed to do just that through the sharing of relevant and actionable information and analysis among participants. This mission has propelled FS-ISAC into the position of a trusted and global leader in the dissemination of threat, vulnerability and incident information.

The scope, complexity and magnitude of information security threats is constantly growing. No single organization - no matter how well funded and experienced – can prepare against every attack. Cooperation between companies allows efficient use of scarce resources to respond to threats. In this way the collective strength of entire industries can be used to deal with the evolving cyber menace.

The Financial Services Information Sharing and Analysis Center is a not-for-profit information sharing community supporting the global financial sector. FS-ISAC is the world's largest threat intelligence sharing and collaboration organization with over 7,000 members globally.

A not for profit funded by its membership fees, FS-ISAC has grown rapidly in recent years. In 2004, there were only 68 members, most of which were large financial services firms. Today, we have close to 7,000 member organizations, including commercial banks and community lenders of all sizes; investment companies including broker-dealers, asset management and hedge funds, insurance companies; payments processors; and trade associations representing all of the financial services sector. Because today's cybercriminal activities transcend country borders, FS-ISAC has expanded globally and has active members in 38 countries and staff in 9 countries.

Threat Environment

The current cyber threat environment continues to evolve and intensify. Each day, cyber risk grows as attacks increase in number, pace, and complexity. Our members constantly adapt to this changing threat environment. We are no longer in the days wherein the threat was confined to individual hacktivists and fraudsters. We are now in an era of attacks by not only organized crime syndicates, but also nation-states and entities affiliated with terrorist operations. Correspondingly, the attacks have grown beyond webpage vandalism and fraud into large-scale, prolonged campaigns that threaten the availability of services to citizens and threaten the privacy and accuracy of their information.

Malicious cyber actors with increasing sophistication and persistence continue to target the financial services sector. These actors vary considerably in terms of motivation and capability: nation-states conducting corporate

Ray Irving

Ray Irving is the FS-ISAC Regional Director for EMEA. With over 20 years experience in IT Ray is a CISSP and a certified Project & Program Manager. He has managed information security programs covering cyber threats, data protection, security monitoring, identity management & vulnerability management.

Highlights include the first financial services implementation of FireEye, a global ArcSight implementation and deploying Data Leakage Prevention to over 100,000 workstations 50 different countries.

For 3 years prior to joining FS-ISAC Ray was Head of Security Programs at a major bank, delivering a portfolio of dozens of IT Security projects.

e-mail: rirving@fsisac.eu

espionage, advanced cyber criminals seeking to steal money and hacktivists intent on making political statements. Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems.

Key Activities

FS-ISAC’s operations and culture of trusted collaboration has evolved into a successful model for how other industry sectors are organizing themselves around this security imperative. In addition to defending the financial sector, FS-ISAC is also helping other sectors develop their information sharing and analysis capabilities.

FS-ISAC core activities include:

- Enable anonymous submission and sharing of member threats and incidents.
- Delivery of timely, relevant and actionable cyber and physical alerts from other members and trusted sources.
- Regular threat information sharing calls for members and invited security and risk experts to discuss the latest threats, vulnerabilities, and incidents.
- Rapid response briefings to members when a broad-scale threat or attack is imminent or underway.
- Development of cyber exercises and active participation in cyber exercises organised by other organisations.
- Engagement with other critical sectors, government agencies, law enforcement and other industry bodies to facilitate information sharing.
- Organise member meetings, workshops and conferences to facilitate sharing of threats, incidents, experiences, best practices and training opportunities.

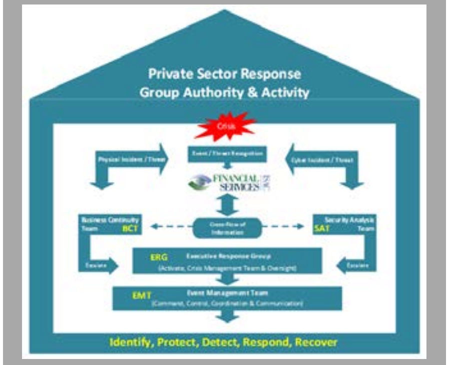
Circles of Trust

FS-ISAC divides its membership into circles of trust based on a member organization’s primary function within the financial sector. These smaller groups have the ability to share amongst one another in email distribution lists, creating sharing on a more relevant level. Examples include councils dedicated to various sectors within the financial services sector such as payments processors, insurance companies, and broker-dealers. Other councils and committees deal with more narrowly focused issues such as business resiliency and threat intelligence. FS-ISAC provides these groups with email distribution lists so that they may actively share ideas and information in real time.

Incident response exercises and plans

Members of the FS-ISAC collaborate to write resilience exercises to test and improve incident response preparedness. One example is the Cyber Attack Against Payment Systems (CAPS). Written by members of the payments council this simulated table top exercise takes place annually and involves responding to a cyber-attack scenario related to same-day wholesale payment systems.

Overarching methodology


Private Sector Response
Group Authority & Activity
Crisis
Physical Incident / Threat
Event / Threat Recognition
Cyber Incident / Threat
FINANCIAL SERVICES
Business Continuity Team BCT
Cross-Flow of Information
Security Analysis SAT Team
Escalate
ERG Executive Response Group
(Activate, Crisis Management Team & Oversight)
Escalate
EMT Event Management Team
(Command, Control, Coordination & Communication)
Identify, Protect, Detect, Respond, Recover

The financial services sector not only faces cyber threats, but also physical and environmental threats as well. For this reason, in the US the FS-ISAC and critical infrastructure partners have worked together to develop the FS-ISAC All-Hazards Crisis Response Playbook. The Playbook guides how the financial sector identifies and responds to a crisis event, how it will coordinate partnerships activities, and how it will share information to achieve resiliency goals.

Over the past year, the Playbook has undergone extensive revision, reducing the size from over 70 pages to just 10 pages. This smaller playbook has been aligned with the NIST Cybersecurity Framework and gives crisis response teams a playbook they can have in hand during an event. A series of resource guides have been included in appendices to provide further guidance depending on the type of hazard facing the sector.

Next Steps

If you would like to know more about FS-ISAC please visit our website: www.infrarisk-fp7.eu

The GDW Index: An Extension of the GDP Index to Include Human Well-being

The Gross Domestic Wealth (GDW) index expands the conventional GDP index to include human well-being as part of the system production dynamics.

Leontief's Production Model

Leontief's seminal work of 1973 [1] relates the interdependencies among a country's economic sectors in terms of a production matrix. This model is used to estimate the prosperity of a country in terms of the Gross Domestic Product (GDP). Leontief's equation is given by

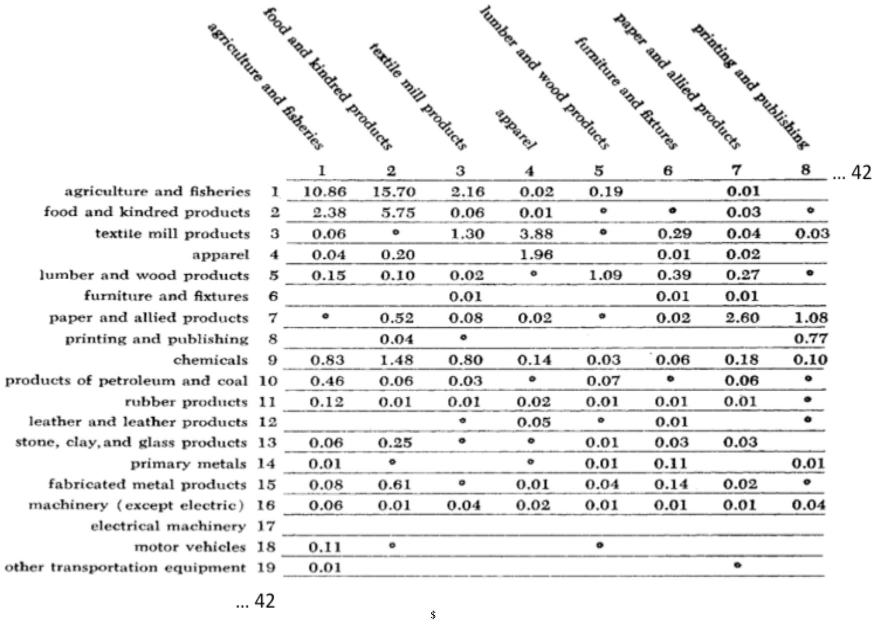
$$\overline{x}_L = A\overline{x}_L + \overline{f} \qquad (1)$$

Subscript *L* is used to indicate Leontief. With reference to Fig. 1 *[1], a country's* economy is divided into *N* sectors. Vector x_L represents the collection of all sectors (rows and columns in Fig.1); matrix *A* is Leontief's production matrix and vector *f* is the surplus of the production process. Vector *f* includes human consumption, government expenditures, maintenance and expansion of production infrastructure, and export-import. The product Ax_L gives the contributions of each sector to the production of the other sectors (including itself). For example, sector 'lumber and wood products' is element 5 in the x_L vector, and sector 'agriculture and fisheries' is element 1. In the table of Fig. 1, 0.19 units of lumber and wood products are needed for the total production of the agriculture and fisheries sector. Thus, in matrix *A* of (1), element A_{15} will be 0.19. The total production of sector 1 is therefore given by the sum of all elements in row 1 of *A* plus the surplus f_1. In total, Ax_L gives the contribution of all sectors to the production process, while *f* gives the net production output. In terms of systems theory, we can write

$$f = (I - A)^{-1} x_L \qquad (2)$$

Matrix $(I\text{-}A)^{-1}$ is the effectiveness of production of a given country's economy and is (to a high degree) under the control of the given country. The smaller the amount of resources needed x_L for a given output *f*, the more efficient the production processes are. The net production output *f* is used for components considered "outside" the production process: final goods and services consumed (including government as a service), physical infrastructure up keeping, and export-import trade.

In the particular case where $x_L = Ax_L$ in (1), all production is used for the production itself. In such a system, the *f* vector is zero and there is nothing left for consumption by the citizens. Such a system would not be able to support human life since humans would not be able to eat, dress, or attain other goods or services.



		agriculture and fisheries	food and kindred products	textile mill products	apparel	lumber and wood products	furniture and fixtures	paper and allied products	printing and publishing	
		1	2	3	4	5	6	7	8	... 42
agriculture and fisheries	1	10.86	15.70	2.16	0.02	0.19		0.01		
food and kindred products	2	2.38	5.75	0.06	0.01	•	•	0.03	•	
textile mill products	3	0.06	•	1.30	3.88	•	0.29	0.04	0.03	
apparel	4	0.04	0.20		1.96		0.01	0.02		
lumber and wood products	5	0.15	0.10	0.02	•	1.09	0.39	0.27	•	
furniture and fixtures	6			0.01			0.01	0.01		
paper and allied products	7	•	0.52	0.08	0.02	•	0.02	2.60	1.08	
printing and publishing	8		0.04	•					0.77	
chemicals	9	0.83	1.48	0.80	0.14	0.03	0.06	0.18	0.10	
products of petroleum and coal	10	0.46	0.06	0.03	•	0.07	•	0.06	•	
rubber products	11	0.12	0.01	0.01	0.02	0.01	0.01	0.01	•	
leather and leather products	12			•	0.05	•	0.01		•	
stone, clay, and glass products	13	0.06	0.25	•	•	0.01	0.03	0.03		
primary metals	14	0.01	•		•	0.01	0.11		0.01	
fabricated metal products	15	0.08	0.61	•	0.01	0.04	0.14	0.02	•	
machinery (except electric)	16	0.06	0.01	0.04	0.02	0.01	0.01	0.01	0.04	
electrical machinery	17									
motor vehicles	18	0.11	•			•				
other transportation equipment	19	0.01						•		
	... 42									

Figure 4: Leontief's production matrix.

José R. Martí

Dr. José R. Martí is a Professor of Electrical and Computer Engineering at the University of British Columbia in Canada. He is a Life Fellow of the Institute of Electrical and Electronic Engineers (IEEE) and a Fellow of the Canadian Academy of Engineering. He has made a number of contributions to modelling and simulation of large power system networks and integrated multi-sector critical infrastructure systems. He is the main architect of the i2Sim simulation environment that can incorporate physical laws and human factors into a common analytical solution environment.

e-mail: jrms@ece.ubc.ca

In the normal case when *f* is not zero, the value of *f* minus the net export-import balance is what is available for internal use. To simplify the discussion, we can loosely group direct consumption, government, and infrastructure costs as simply “consumption”.

For example, in Fig.1, the surplus from the food and kindred products sector is the food available for the country’s people to eat. If the people cannot consume all of this food, what is leftover will be available for export. But if the surplus of food is insufficient to meet the people’s needs, food will have to be imported. In order to be able to import food, however, a different sector must have a surplus beyond internal consumption that can be exported. For example, if vehicles had a surplus beyond internal consumption, the surplus of vehicles can be exported to procure the monetary resources needed to import food. A system in which individual elements of vector *f* cannot satisfy the country’s internal needs will depend on this export-import balance to satisfy these needs. This is of great concern, as the export-import balance is not directly controllable by the country but depends on external factors.

Human Wellness in the Production Model

The Gross Domestic Product (GDP) index that is normally used to measure the economic health of a country is calculated by adding up all the elements of the surplus vector *f*. Tacit in this assumption is that the excess goods available for export will be equal in monetary value to the goods that will need to be imported.

> “The proposed Production-Consumption (PC) model includes human well-being in the system dynamics.”

In equations (1)(2), the individual components of vector *f* are not mathematically constrained and there might be a number of combinations of some large elements and some small elements whose sum gives the same GDP. The problem with Leontief’s model, and the associated GDP definition, is that only the production matrix *A* is controllable internally as part of the system’s dynamics. The export-import part of *f* depends on dynamics of the global markets, which are beyond the control of the particular country.

The available goods and services for consumption, which in the classical Leontief model depend on the export-import external dynamics, determine the well-being of the citizens of a country. In the system proposed in our work, we remove the export-import uncertainty by moving the internal part of vector *f* (consumption of goods and services, government, and infrastructure costs) to the inside of the economic process of production:

$$\bar{x}_L = A\bar{x}_L + \bar{f} = A\bar{x} + (\bar{d} + \bar{e})$$

which results in the equation

$$\bar{x}_h = B\bar{x}_h + \bar{e} \qquad (3)$$

Subscript *h* is used to indicate that human consumption variables are included in *x*. We call matrix *B* in (3) the production-consumption (PC) matrix and it replaces Leontief’s production matrix *A* in (1).

The proposed production-consumption (PC) model includes human well-being in the system dynamics. In this model, surplus vector *e* is the excess production after satisfying the needs of the population and the system of infrastructures. Excess *e* can be used for export, which, in turn, can be used for import of extra goods that can be used to increase the population’s well-being beyond the originally targeted level and to improve the system of infrastructures.

We recognize that it may not be possible (or efficient) for every country to produce every good needed to satisfy its citizens’ needs. For example, one country might be unable to produce bananas whereas another might find it inefficient to manufacture automobiles. However, by incorporating consumption as part of the production dynamics, suboptimum solutions can still be found that will be closer to satisfying first the internal needs than when these internal needs are left unconstrained.

Mathematically, in order to incorporate human consumption into the production process, we need to develop a mathematical model that can be made part of matrix B in (3). This can be achieved by solving equation (3) within the simulation environment of the i2Sim simulator [2] developed at the University of British Columbia.

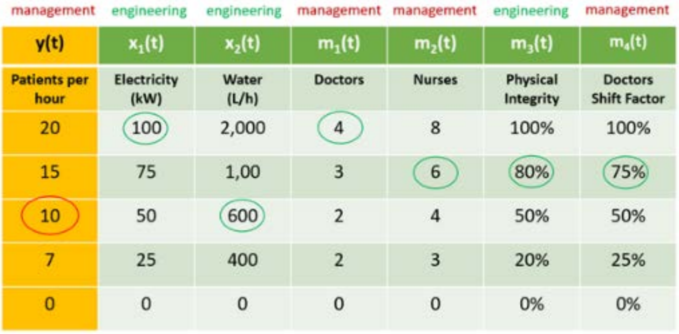
I2Sim Simulator to Integrate Physical and Human Systems

The i2Sim simulation framework of [2] was developed to optimize the allocation of resources during emergencies, such as natural disasters. The production units in i2Sim are called “cells” and the points where decisions are made to allocate the output from the cells are called “distributors”.

> i2Sim’s Human Readable Table (HRT) can take nonlinear human factors as inputs to define input-output transfer functions.

i2Sim introduces the concept of a Human Readable Table (HRT) to relate the inputs to a production cell to its output. The Human Readable Table (HRT) can take nonlinear human factors as inputs to define input-output transfer functions. After the HRT is defined, it can now be synthesized analytically by a continuous nonlinear function. A system of equations can then be formed that includes these cell equations and the distributor equations. The distributors are decision points that determine how the output from a production cell is split and distributed to the other production cells.

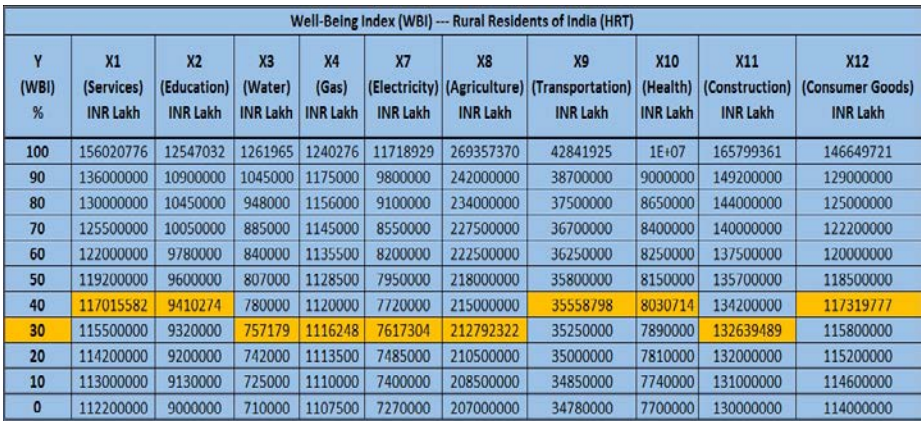
We can explain the functionality of i2Sim’s HRT using, for example, the case of an ER unit in a hospital (Fig. 2). Suppose that due to an earthquake, some damage has occurred in the system of critical infrastructures and the availability of input resources is as shown by the circled values. There is



management	engineering	engineering	management	management	engineering	management
y(t)	$x_1(t)$	$x_2(t)$	$m_1(t)$	$m_2(t)$	$m_3(t)$	$m_4(t)$
Patients per hour	Electricity (kW)	Water (L/h)	Doctors	Nurses	Physical Integrity	Doctors Shift Factor
20	100	2,000	4	8	100%	100%
15	75	1,00	3	6	80%	75%
10	50	600	2	4	50%	50%
7	25	400	2	3	20%	25%
0	0	0	0	0	0%	0%

Figure 5: HRT for a hospital ER unit.

no lack of electricity or doctors, but there are limited resources in terms of nurses, physical integrity, some tiredness of the doctors, and lack of water. The least available input, in this case the water supply, limits the entire operability of the hospital to 10 treated patients per hour. This row in the table is called the operating row and determines the amount of each input needed to provide the operating output. Inputs in excess of the values in the HRT's operating row represent resources that are not needed. For this scenario, there is no need to have more than 2 doctors because the output is limited by the water resource.



Well-Being Index (WBI) --- Rural Residents of India (HRT)										
Y (WBI) %	X1 (Services) INR Lakh	X2 (Education) INR Lakh	X3 (Water) INR Lakh	X4 (Gas) INR Lakh	X7 (Electricity) INR Lakh	X8 (Agriculture) INR Lakh	X9 (Transportation) INR Lakh	X10 (Health) INR Lakh	X11 (Construction) INR Lakh	X12 (Consumer Goods) INR Lakh
100	156020776	12547032	1261965	1240276	11718929	269357370	42841925	1E+07	165799361	146649721
90	136000000	10900000	1045000	1175000	9800000	242000000	38700000	9000000	149200000	129000000
80	130000000	10450000	948000	1156000	9100000	234000000	37500000	8650000	144000000	125000000
70	125500000	10050000	885000	1145000	8550000	227500000	36700000	8400000	140000000	122200000
60	122000000	9780000	840000	1135500	8200000	222500000	36250000	8250000	137500000	120000000
50	119200000	9600000	807000	1128500	7950000	218000000	35800000	8150000	135700000	118500000
40	117015582	9410274	780000	1120000	7720000	215000000	35558798	8030714	134200000	117319777
30	115500000	9320000	757179	1116248	7617304	212792322	35250000	7890000	132639489	115800000
20	114200000	9200000	742000	1113500	7485000	210500000	35000000	7810000	132000000	115200000
10	113000000	9130000	725000	1110000	7400000	208500000	34850000	7740000	131000000	114600000
0	112200000	9000000	710000	1107500	7270000	207000000	34780000	7700000	130000000	114000000

Figure 6: Human Wellness Table (HWT)

Because the HRT concept can relate variables that can be physical or human, it allows the extension of Leontief's production unit concept to incorporate human factors in the PC system matrix *B* (3). These factors are not considered in Leontief's system matrix *A* (1). In addition, while Leontief's requires a linear (or linearized) relationship between inputs and output, i2Sim's analytical synthesis of the HRT does not have this restriction and can model nonlinear relationships over the whole range of the functions. This nonlinearity is characteristic of human needs (e.g., we cannot continue eating after we have eaten enough). Both, Leontief and i2Sim share the concept that the production output is limited by the least available input.

Human Wellness Table (HWT)

The Human Wellness Table (HWT) relates the level of well-being to the availability of consumption goods and services. A very simple example of an HWT is shown in Figure 5 (next page). This figure shows the degradation of services in a city due to a natural disaster or a system failure.

Figure 3 shows an HWT that is being used in an economic development project to deploy distributed clean energy resources in rural regions of India. The level of human wellness is the table's output.

The table's inputs, which are supplied by the region's infrastructure sectors, are needed to satisfy the human needs for food, shelter, electricity, water, ICT, education, services, etc. The HWT follows the same rules as the other i2Sim's HRTs: the least available input determines the output, in this case, the wellness level.

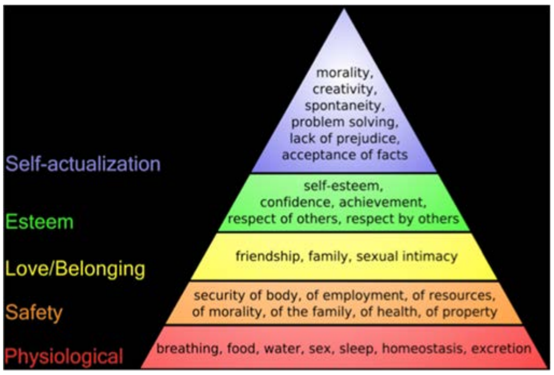

morality, creativity, spontaneity, problem solving, lack of prejudice, acceptance of facts
Self-actualization
self-esteem, confidence, achievement, respect of others, respect by others
Esteem
friendship, family, sexual intimacy
Love/Belonging
security of body, of employment, of resources, of morality, of the family, of health, of property
Safety
breathing, food, water, sex, sleep, homeostasis, excretion
Physiological

Figure 7: Maslow's pyramid of human needs.

> "To achieve a coordinated growth of the sectors such that the next wellness level is achieved efficiently, a system optimization problem has to be solved."

The table of human needs depends on the particular community or country and depends on a number of personal and social factors. An example of such needs is provided by Maslow's pyramid in Figure 4 [3]. The lower rows in the HWT correspond to Maslow's bottom layers and the higher rows to Maslow's higher layers. The bottom layers are common to most societies, while the higher layers will show more pronounced differences among communities, and among countries. With respect to the HWT of Fig. 3, to increase the wellness of this population the resources that must first be increased are those with the lowest value. Once these resources are increased to match the level of the next lacking resources, the next higher wellness level will be achieved.

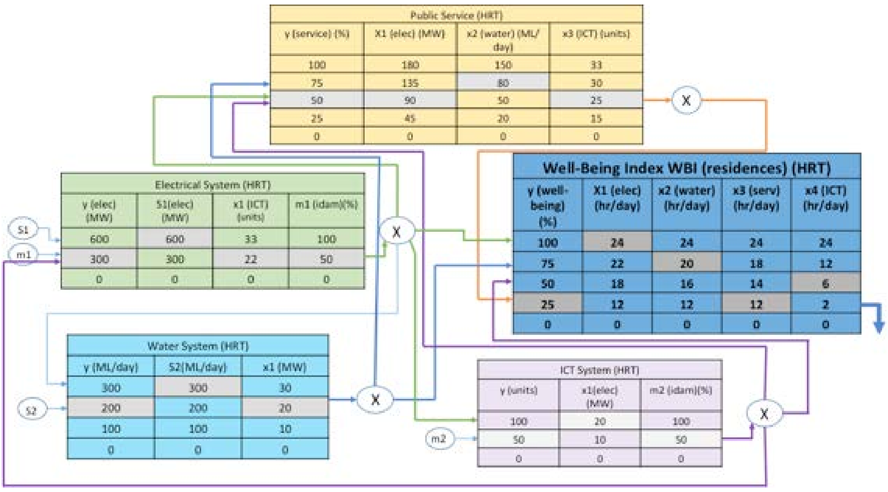
To achieve a coordinated growth of the sectors such that the next wellness level is achieved efficiently, a system optimization problem has to be solved. This solution needs to consider the interdependencies among production sectors and the geographical locality of the consumption. Since i2Sim can consider the full range of nonlinear interdependencies among sectors, a global optimum solution can be formulated. Figure 5 shows a simplified example of interdependencies among infrastructure systems in a city resiliency study.

The Gross Domestic Wealth (GDW) Index

The gross domestic product (GDP) is the most commonly used index to rate the degree of development of a country. As discussed earlier, in terms of Leontief's production equation (1), the GDP is calculated by adding all elements of surplus vector *f* measured in terms of the monetary value of each element. In this definition, vector *f* includes both internal consumption and exports and is not constrained in terms of satisfying internal demand needs.

> "We can define the Gross Domestic Wealth (GDW) index of a country as the sum of the inputs to the operating row of the HWT."

In fact, it is generally assumed that when the GDP is large the internal needs are satisfied. However, this may not be true in many cases. Not including consumption in the system dynamics can result in production distortions, such as the overproduction of some basic items and the underproduction, or reliance on imports, for the supply of others.



Public Service (HRT)			
y (service) (%)	X1 (elec) (MW)	x2 (water) (ML/day)	x3 (ICT) (units)
100	180	150	33
75	135	80	30
50	90	50	25
25	45	20	15
0	0	0	0

Electrical System (HRT)			
y (elec) (MW)	S1(elec) (MW)	x1 (ICT) (units)	m1 (idam)(%)
600	600	33	100
300	300	22	50
0	0	0	0

Well-Being Index WBI (residences) (HRT)				
y (well-being) (%)	X1 (elec) (hr/day)	x2 (water) (hr/day)	x3 (serv) (hr/day)	x4 (ICT) (hr/day)
100	24	24	24	24
75	22	20	18	12
50	18	16	14	6
25	12	12	12	2
0	0	0	0	0

Water System (HRT)		
y (ML/day)	S2(ML/day)	x1 (MW)
300	300	30
200	200	20
100	100	10
0	0	0

ICT System (HRT)		
y (units)	x1(elec) (MW)	m2 (idam)(%)
100	20	100
50	10	50
0	0	0

Figure 5: Interdependencies among city services providing human needs.

A better index can be derived from the formulation of (3). Using the i2Sim simulator, we can choose as the objective function to attaining a given row in the HWT. The solution of the optimization problem will give the right amount of production needed from each sector. Production of a given sector beyond this point does not contribute directly to satisfy the objective.

Based on the HWT operating row concept, we can define the Gross Domestic Wealth (GDW) index of a country as the sum of the inputs to the operating row of the HWT.

In a well-balanced economy, the GDP, after subtracting the value of the exports, will be equal to the GDW. However, in an unbalanced economy the GDW will be less than the GDP minus exports because the well-being row in the HWT is determined by the least satisfied need. Production of resources above this row will not contribute to the GDW. This difference between the GDW and the GDP more accurately reflects the fact that countries with large GDP may not necessarily have a high level of population well-being.

Notice that in a well-balanced production system, after the internal needs are satisfied by the inputs to the HWT table, surplus vector *e* in (2) will be available for exports. These exports will generate extra revenue, which can now be used to raise the well-being operating row with imports, or can be used for capital investment in additional infrastructure, which in future production cycles will raise the level of well-being to a higher operating row.

As a corollary to the HWT concept, we can extend the concept to the wealth of a nation as a whole by defining the Gross National Wealth (GNW) index. This index is obtained by adding the elements of surplus vector *e* to the corresponding inputs of the operating row of the HWT. The GNW will consider the total useful production of the country, which beyond satisfying its citizens' well-being needs, will also produce exports to increase this well-being.

Conclusion

The Gross Domestic Wealth (GDW) index described in this article is part of the work in progress at the University of British Columbia (UBC) in developing the i2Sim simulation environment. I2Sim is a multisystem, multilayer simulation environment that can capture the interdependencies among multiple infrastructure sectors and their cascading effects across physical, financial, economic, and human layers. I2Sim has been successfully deployed to optimize the response after natural and man-made disasters, and after equipment failures, such as earthquakes, cyber-attacks, and in smart city resiliency.

The concepts introduced in this article are the result of the application of i2Sim to economic development projects to optimize the production of resources to improve human well-being of a region or a country. In this context, the Gross Domestic Wealth (GDW) index is proposed as an alternative to the traditional Gross Domestic Product (GDP) index to better capture the effect of economic development on satisfying basic human needs.

Leontief's traditional production equations have been modified into production-consumption (PC) equations to include human well-being in the economic optimization. This is possible by defining the Human Wellness Table (HWT) and converting this table into an analytical transfer function in the i2Sim simulation environment. I2Sim can then optimize the production-consumption system so as to satisfy the internal well-being needs and minimize the dependencies on non-controllable export-import dynamics.

References

[1] *Wassily Leontief*, Input-Output Economics, 2nd ed., Oxford, 1986

[2] *José R Martí, (Chapter) Multisystem Simulation: Analysis of Critical Infrastructures for Disaster Response, D'Agostino, Gregorio, Scala, Antonio, Networks of Networks: The Last Frontier of Complexity: 255-277. Springer International Publishing.*

[3] *J. Finkelstein, Diagram of Maslow's hierarchy of needs, Available from: http://commons.wikimedia.org/wiki/File:Maslow's_hierarchy_of_needs.png [Accessed 21/06/16].*

Authors' Contributions

Prof. José R. Martí is the main architect of the i2Sim simulator and its extension to economic systems, which includes the concepts of the HRT and the HWT.

Ehssan Ghahremani

Ehssan is a Masters of Applied Science student at the University of British Columbia in Canada. He is currently implementing the economic model of i2Sim for the development of rural regions in India based on renewable energy sources.

Andrea T.J. Martí

Andrea is a Masters of Applied Science student at the University of British Columbia in Canada. She is developing the i2Sim algorithm code and its extensions for economic development systems.

Open-source Network Defense: Protecting Critical Infrastructures with Bro

The widely deployed open-source network monitor has evolved from a research platform to an operational capability securing large scientific environments, corporations, government agencies, and non-profit organizations.

For more than two decades now the open-source network security monitor Bro[1] has been protecting some of the most powerful networks in the world from attacks on their cyberinfrastructure. While historically deployed primarily at large scientific environments, Bro has continuously expanded its reach more broadly. Increasingly, its user base now also includes providers of critical infrastructure seeking effective defense against today's sophisticated online attackers. While these organizations already benefit from Bro's standard, powerful out-of-the-box capabilities, some of our recent research efforts aim to further exploit the unique setting that critical infrastructure environments offer by taking their domain-specific semantics into account for tailoring detection and response.

History

Bro was originally created in 1995 by Vern Paxson at Lawrence Berkeley National Laboratory (LBNL). Over time, a growing Bro team has extended the system's functionality with a range of innovative mechanisms and detection approaches that by far exceed the capabilities of other network monitoring software—open-source and commercial alike. While much of the early work took place in the context of research projects, Bro has always been able to bridge the traditional gap between academia and operations—leading to numerous scientific publications at prestigious academic venues while facilitating a tremendous number of real-world deployments that now include many major universities, research labs, supercomputing centers, open-science communities, government institutions, and Fortune 50 companies. Even the 2012 Obama campaign used Bro to protect their Chicago headquarters.

Bro enjoys a very active user and development community. More than a 100 people have contributed to the system over time, and Bro's GitHub mirror has garnered more than 1100 stars and close to 400 forks. GitHub also features Bro as one of their security showcases, and InfoWorld awarded Bro a 2014 *Bossie Award* in the category *Best Open-source Networking and Security Software*. Bro is maintained today by a core team of researchers and engineers working out of the International Computer Science Institute (ICSI) in Berkeley, California, and the National Center for Supercomputing Applications (NCSA) in Urbana-Champaign, Illinois. The team is currently funded primarily through the U.S. National Science Foundation (NSF), which in 2009 began to invest substantially into Bro as a means to protect U.S. research & education cyberinfrastructure.

Capabilities

As the most immediate benefit from installing Bro, network operators gain deep visibility into their network. Bro exports detailed streams of real-time metadata that provide high-level representations of the network's complete activity—including, e.g., all connection attempts, all HTTP requests with responses, all DNS lookups with replies, and all file transfers. Archiving this data provides an invaluable record for later forensic analyses if critical assets become compromised. Many sites also forward Bro's output into analytics systems, such as Splunk, for correlation and interactive analysis.

Beyond providing visibility, Bro differs more fundamentally from traditional intrusion detection and prevention systems (IDS/IPS) in its inherent flexibility: whereas standard IDS tend to remain limited to a particular detection strategy—most commonly to basic signature matching scanning the raw traffic for simple byte patterns indicating attacks—Bro is not tied to any specific approach, but able to

Robin Sommer

is a Senior Researcher at the International Computer Science Institute, Berkeley, where he leads the open-source Bro project. He is a co-founder, and the CTO, of Broala, a recent startup by Bro's creators offering professional Bro solutions to corporations and government. He is also an affiliated researcher at Lawrence Berkeley National Laboratory where he works with the Lab's cybersecurity team. Robin Sommer holds a doctoral degree from TU München, Germany.

e-mail: robin@icsi.berkeley.edu

act like a signature-based, behavioral-based, or specification-based detection system all at the same time. Much of this flexibility comes from Bro's modular design, split across two main layers: First, an event engine reduces the stream of incoming network pakkets to a series of higher-level events. The event engine provides both generic transport analysis and application-specific analysis (e.g., understanding the particular workings of HTTP, DNS, SMB, and many other protocols). Second, a script interpreter executes scripts written in a specialized, high-level language that can express both a site's security policy and general forms of high-level analysis (e.g., blacklist checks, scan detection) in terms of the event stream. The scripting language is strongly typed and geared for managing large quantities of state.

The key to understanding Bro is realizing that even though the system comes with powerful functionality preconfigured, fundamentally it represents a platform for traffic analysis that remains fully customizable and extensible—a capability that proves crucial for protecting critical infrastructure environments. Indeed, Bro's flexibility is well appreciated even beyond the security domain: networking researchers frequently use Bro for measurement studies and prototyping.

Critical Infrastructure

Inside the critical infrastructure sector, networked control systems provide a particularly promising opportunity for Bro to leverage the power of its flexible approach for effective, domain-specific security monitoring. As these environments differ substantially from traditional IT systems, they also face unique security challenges that render protection more challenging. Off-the-shelf IDS prove a particularly ill fit here: classic signature matching requires precise patterns of anticipated intrusions—an unrealistic assumption in a setting where attacks remain rare overall, yet may carefully target their victims—and existing behavioral approaches fail to incorporate the domain-specific context of operating in these specialized environments.

Continuing the Bro team's tradition of conducting basic research efforts to prototype new functionality, we recently undertook several projects aiming to develop novel approaches for monitoring critical infrastructure. In one study aiming at industrial control systems, we used Bro to analyze network traffic that we recorded from programmable logic controllers (PLCs) at two operational water treatment plants.[2] We used Bro to extract, from the raw traffic, all process operations carried out over the network, and then constructed a corresponding time series for each process variable to characterize its expected activity. We derived variable-specific forecasting models and showed that they can reliably detect attacks that manifest as changes to variables that would normally remain stable during operation. We also explored extending this approach to more indirect process control attacks that reflect only as deviations in field measurements, for example because of tampering with sensors. While our analysis there remained preliminary, investigating a series of specific cases illuminated several routes towards novel, powerful attack detectors that Bro could implement in the future.

> There's no other software available that does what Bro does. We regularly see people replace expensive commercial products with Bro.

In a second study our team turned to protecting smart grid environments.[3] We proposed a semantic analysis framework on top of Bro that can detect attacks modifying control fields from the network traffic exchanged between SCADA and power substations. Instead of focusing on complete outages of power system components, as previous work had, we considered attacks causing system perturbations remaining within a normal range of legitimate operations. Such control-related attacks pose a serious threat to power grids and can result in catastrophic consequences, such as overloaded transmission lines or generators. Exploiting knowledge of the grid's cyber and physical infrastructure, we built a prototype of the framework that extracted control commands from the network through a corresponding DNP3 protocol parser that we developed for Bro. At runtime, it then invoked external power flow analysis software to predict the physical consequences that executing the issued control commands would incur. We found that such high-level semantic analysis could complete attack detection in about 200ms even for a large-scale test system, making it feasible to stop an intruder in time by triggering an active response.

In our most recent study we leveraged Bro to prototype a specification-based intrusion detection system monitoring building automation systems.[4] Generally, specification-based monitoring employs a comprehensive functional model of a system's permitted behavior to create a reference for identifying non-conforming activity. However, while conceptually powerful, in practice the approach often remains infeasible to undertake, as it not only requires an explicit and unambiguous description of the system's functionality, but also substantial human effort in crafting comprehensive specification rules. Our work addressed these challenges by automating the process to a high degree through mining specification rules automatically from device documentation that was readily available. We then encoded these rules as logic in Bro's scripting language so that the system could monitor the network for any deviations from the reference. We evaluated our approach with real-world network traffic from two operational building automation infrastructures—a university and a large research lab—each encompassing hundreds of devices. In both settings Bro correctly identified deviations from the derived specifications. While no actual attack took place during our experiments, every alert that Bro reported did indeed reveal either an actual mismatch between device documentation and implementation, or an operator mistake.

In critical infrastructure environments a standard challenge for Bro concerns their use of less common, domain-specific protocols. As Bro's rich analysis requires access to low-level communication semantics, it needs corresponding protocol parsers that closely follow what endpoints are exchanging. Unfortunately, implementing such parsers remains a daunting task today. It not only regularly proves time-consuming and cumbersome, but also poses fundamental security challenges on its own due to the need to process untrusted input that may—inadvertently or maliciously—fail to follow standards and RFCs. To lower the barrier to supporting new protocols, in another research project we developed a novel, comprehensive framework for developing parsers for wire format data, integrating and unifying capabilities, approaches, and lessons-learned from existing efforts.[5] The framework consists of a novel type-based specification language that integrates syntax and semantics into a unified processing model expressing a protocol's structure; a just-in-time compiler toolchain that, from these specifications, creates robust and efficient native code for parsing wire format; and an extensive API for applications to drive the process and integrate its output.

> Bro has successfully bridged the traditional gap between academia and operations for more than two decades now.

Once detected, an ongoing attack must be stopped as quickly as possible. While Bro itself operates out-of-band, organizations can provide it with a control channel back to their network for taking actions. LBNL for example blocks thousands of external IP addresses every day using Bro. To better support such setups, we recently added a novel *Network Control Framework* to Bro that provides users with a flexible, unified interface for active response, hiding the complexity of heterogeneous network equipment behind a simple task-oriented API.[6] The framework comes with several backends, including an interface to OpenFlow hardware. Furthermore, exploiting a new generation of programmable network cards and switches that have recently emerged at affordable price points, we are planning to extend this line of work by moving low-level computational tasks that remain challenging to perform in software into the network fabric.

Enterprise Solutions

As Bro has been gaining traction outside of its traditional community of open-science networks, a need for enterprise-level solutions has emerged that the grant-funded open-source team behind the system proves ill-positioned to address satisfactorily. Consequently, in 2013 the three primary architects of Bro founded a startup, Broala[7], that caters specifically to corporate customers. The company provides support services for open-source Bro installations, and it also offers a commercial Bro-based hardware appliance, *BroBox One*, that facilitates in-depth visibility into a network's activity. Aggressively tuned for performance, *BroBox One* provides a carefully tailored subset of Bro functionality that focuses on feeding Bro's real-time analysis streams into Big-Data enterprise analytics pipelines. It runs a minimalist, custom OS based on the Linux kernel, and it features a specialized NIC that provides the performance that high-volume deployments require.

With its offerings, Broala pursues a two-fold corporate mission: it strives to develop a viable business model for transitioning to practice unique security technology resulting from many years of academic research; while embracing and sustaining the technology's immensely successful open-source model that has facilitated operational deployment at a scale quite rare for basic research efforts. With its unique team—which includes Bro's inventors as well as a broad range of relevant skills and expertise among its staff—the company is also in an excellent position to adapt Bro to the needs of large-scale critical infrastructure environments.

Conclusion

Bro is a widely-used open-source software that offers deep visibility into a network's operation, analyzing its activity at a high semantic level suitable for identifying sophisticated cyberattack strategies. Bridging the traditional gap between academic research and large-scale operational deployment, Bro has helped reveal countless attacks on corporations, government agencies, universities, and nonprofit organizations. For providers of critical infrastructure, Bro offers powerful detection and response capabilities that they can tailor to their settings. In recent research efforts, our team has developed prototypes of several domain-specific monitoring approaches that exploit the specific nature of critical infrastructure environments.

If you are interested in learning more about Bro and its highly engaged community, we invite you to come join us at the annual BroCon conference, which this year will take place in September in Austin, Texas. [8]

---

[1] https://bro.org

[2] D. Hadžiosmanović, R. Sommer, E. Zambon, P. Hartel: Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes. Proc. Annual Computer Security Applications Conference, 2014.

[3] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer: Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids. IEEE Transactions on Smart Grid, 2015.

[4] M. Caselli, E. Zambon, J. Amann, R. Sommer, F. Kargl: Specification Mining for Intrusion Detection in Networked Control Systems. Proc. USENIX Security Symposium, 2016.

[5] R. Sommer, J. Amann, and S. Hall: Spicy: A Unified Deep Packet Inspection Framework Dissecting All Your Data. Technical Report TR-15-004, International Computer Science Institute, 2015.

[6] J. Amann, R. Sommer: Providing Dynamic Control to Passive Network Security Monitoring. Proc. Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2015.

[7] https://www.broala.com

Organizational Barriers to Cloud Adoption in CI

Cloud computing offers economic benefits, but CI organisations are slow adopters, citing security concerns. Are these concerns genuine – due to technical constraints - or do they result from organizational and cultural factors?

Cloud computing offers economic benefits and organisational efficiencies. Cost savings of up to 40% can result from moving into the cloud. Organisations can also make efficiency gains as the ability to create new platforms on demand allows them to spin up applications rapidly.

But critical infrastructure organisations are slow to adopt the cloud computing model. Security concerns are often cited as a factor.

These concerns may arise from real technical constraints, but often they are rooted in irrational thinking at individual and group level. This article addresses how to cut through these "emotional" barriers and to ensure appropriate decision making when adopting the cloud.

> Organizational response to technology is difficult to predict because each organization consists of individuals and groups with different values, identities, power relations and histories. Their culture and language also differ as do their attitudes to discipline and supervision. Hence the way in which a technology is taken up by an organization will certainly differ from the way in which its designers considered it would be taken up and also differs between organizations. Failure to account for social aspects during risk analysis and decision making can lead to unexpected failures.

Decision-making in Groups

Individually, human beings exhibit bounded rationality. In groups, they demonstrate emergent behaviour, typical of agent environments – the key difference from software agents being that humans are self-aware. In fact, we communicate by gestures (including words) and responses and the meaning is found in the interaction, not necessarily the intent, of gesture and response. Hence, in our interactions with each other, strong emotions can be set off and unexpected themes may arise. This complex, responsive process contributes further to apparently erratic decision-making. It is only partially possible to stand apart from this and plan for probable (mis-) interpretations as they arise. This article seeks to aid this process with regard to decision-making for CI adopters of cloud services.

5 Factors

A number of factors could be considered in the context of human relating and decision-making. Normally, researchers focus on aspects such as decision support, leadership, organisational vision and strategic planning.

But I suggest that other factors play as much if not more of a role:

- Emergent markets
- The use of language
- Power relations
- Surveillance
- Values and Identity

Thomas Richard McEvoy

Dr. Thomas Richard McEvoy is a senior consultant with Hewlett Packard Enterprise and a Research Fellow at NTNU, Norway. His research interests include the application of formal methods to information security and information security management and consultancy practice as a science.

Email: richard.mcevoy@hpe.com

HP Enterprise Ltd
Microfocus House
2 East Bridge Street
Belfast BT1 3NQ

Emergent Markets

Self-help management textbooks often give the impression that great leaders have a vision for what they want to accomplish, translate that vision into a strategy and ultimately implement that strategy to achieve their goals.

In fact, a great deal of good business leadership comes from the ability to improvise in the face of changing circumstances. Markets are not designed, they emerge. Examples include the success of Honda scooters in the USA, Facebook, and, indeed, the idea of cloud computing.

But because business markets are emergent in nature, the circumstances which gave birth to cloud computing in its original form are not the same circumstances which will allow CI organisations to adopt the cloud.

For business leaders, this might suggest a “wait and see” strategy, but I would suggest the real strategy is “wait and act”. There is no advantage in being first, but there are a lot of disadvantages in being late. You have to move at the right time for your firm. This means continually probing for opportunities, asking supplier firms to demonstrate technical and service capabilities, running pilots and mini-projects to understand what can and cannot be accomplished.

Language Issues

For all the large body of literature produced on decision making methodologies and planning too, it has been clear from more than half a century that management talk their way to decisions.

Using language in a disciplined fashion is therefore key to invoking appropriate management responses.

However, the use of language about cloud and CI both is often far from disciplined.

CI refers to many different industries – finance, transport, certain govt. sectors, certain sectors of the pharmaceutical industry, multiple energy sectors, food, water and sanitation.

Cloud, strictly speaking, refers to computing on demand with ubiquitous network access, but is often associated with other characteristics, none of which need be present, e.g., multi-tenancy, transnational geo-location of data stores, large scale data centres.

Relating back to the need to test the market to see if your organisation is ready for cloud, there is also a strong need to properly define what kind of cloud you want and where you expect a specific CI organisation to benefit from its adoption.

In addition, it is important to ensure that the language used, not only describes the opportunity correctly in technical terms, but also connects to the values of managers in the organisation. If managers don’t see how the move is valuable to them and to their business and understand how they can relate to it, they are less likely to adopt it.

A simple example of the difference between technical and value statements can be found in buying a car. Describing a car’s ABS specifics may be technically accurate, but this is not the same as saying the car is “safer”. In the same way, it is not enough to describe technical or procedural security measures for the cloud, you have to convey the business and security values they promote.

The discipline of combining technical accuracy with value statements is known as “socio-technical scripting”.

Power Relations

Power is not a possession or a state, but an ongoing interaction – a relationship. Something which perhaps parents bringing up children experience the most directly on a daily basis.

The power balance between clients and supplier’s changes as well. One of the factors in these changing relationships is the way in which technology is provided and procured. Traditional outsourcing arrangements involve the client effectively dictating how the service will be delivered in considerable detail. But in the cloud many of the services are standardised and automated (which explains much of the cost savings) and the degree of standardisation increases depending on the type of cloud provided (IaaS, PaaS, SaaS) as well as whether the cloud is managed private cloud, virtual private cloud or public cloud.

One of the paradoxes which arises from this is that customers tend to identify security with control and control with private (i.e. dedicated) services, but, in fact, suppliers are ablest to cheaply supply high level security when they can leverage security resources across multiple customers. A multi-tenanted virtual private cloud offering is therefore able to more cost-effective security solutions, while security is often sacrificed at the altar of cost savings in managed private clouds.

Another issue, which also arises in traditional outsourcing arrangements is a transfer of power, which is not infrequently associated by the transfer of resources, including staff. Where this is likely to lead to job losses, it will be resisted and this can lead to duplication of labour as both the supplier and the client end up with teams effectively assigned the same task.

Having a clear view of power relations in a company and being prepared to engage in organisational politics to positively influence outcomes is key.

Surveillance

Here surveillance is used to refer to the monitoring and supervision of business tasks, not snooping by companies or governments. Surveillance is therefore a necessary part of enabling business transformation, but this does not mean that is accepted by those supervised – or properly implemented by those responsible for supervision.

Examples of both resistant behaviours and failures in supervision can be found in the banking industry and education. It would be more surprising rather than less if it didn’t it also appear in the computing industry.

The need for supervisory arises from the number of layers of interdependency in that system. If I do some work myself, I don’t need to supervise my work, but I may recognise and value another pair of eyes on it. However, where someone else is working for me or indeed there is a long chain of command, the number of eyes which are needed to check the work rises exponentially. The same can be said for a value-chain or workflow between different parts of an organisation or different organisations.

Of course, supervision techniques can be made more efficient e.g. reporting summary information rather than individual events, or automated using sensors and software tools. But it takes time to understand what the best measures to use are and how best to process and analyse them.

In addition, there are both legitimate and illegitimate attempts to resist surveillance. For example, cloud suppliers rightly resist a detailed examination of security controls where the security of other customers as well as the requesting client are at threat. On the other hand, the same tactics might be used to cover up incompetence.

What is needed is a trusted (by both sides) auditing capability whose power and integrity are not in doubt. Whether the appetite exists in a particular sector for such a capability is a different question. In the financial sector, it arguably already exists. In the oil industry, it would be hard to see how it could get off the ground, due to the ad hoc nature of oil industry contracting arrangements.

What is true is that the means of supervising cloud operations should be carefully considered as part of the contract and elements which may be unsatisfactory will have to be treated as risks.

Values and Identity

Values relate to both group norms and individual ideals. They influence what potential individuals and groups see in technology and hence how they exploit that technology.

Since organisations which design technology are not necessarily the same as the ones which supply or support solutions based on it, and, almost certainly, not the same as the organisations which use it, this creates the potential for unexpected usage of technology. It also means that possible, beneficial uses can be missed.

Both unexpected use and potential, but untapped, capability opens the door to "hacking" the system, i.e. – exploiting unrealised capabilities – and, in turn, this can lead to unexpected security vulnerabilities.

An interaction of the values of different groups can further complicate the picture. For example, a build-up of methane gas in a water tunnel was partly caused by the system operators and local anglers agreeing that water flows should be minimal for lowering water levels in the tunnel.

In CI, the role of group identity in this process should not be underestimated. Process engineers see themselves as distinct from IT staff and hence do not readily comprehend why IT staff should be interested in their systems, never mind its security. This, in turn, could make them resistant to advantageous technical changes.

On the other hand, we can see that the cloud opens up new potentials for using technology (e.g., "big data") but that companies may not be positioned to understand or utilise these and hence determine the risk from their misuse. However, it could potentially be used against them, e.g., using distributed information sources within the same cloud to calculate information of commercial value such as the state of oil fields.

It is key therefore to try and analyse the values and assumptions behind the creation and adoption of a system to understand potential gaps in adoption or vulnerabilities which may arise from misuse.

Conclusions

There is a tendency in information security, both in research and in commerce and industry, to spend the majority of time considering technical issues, rather than organisational and human factors. The latter, if they are addressed, are often reduced to considering procedural matters or addressing education and awareness.

But properly understanding patterns of human behaviour in relation to technology and associated decision making, not just at management level but also on the "factory floor" is important to understand errors in judgement at individual and group level which can cause new technologies such as cloud services not to be used, to be used poorly or, worse, to be misused.

Consideration of organisational culture and history analysed within a well-defined sociological framework can give a perspective on the potential barriers to good decision-making.

I have tried to give a flavour of this process in this article, although, of course, a complete analysis would consider a much wider range of behaviours. The end goal of any such analysis is to improve how we approach the decisions we make by seeking to minimise the influence of irrational forces.

CRITIS 2016: Call for Participation

11th International Conference on Critical Information Infrastructures Security
10–12 October 2016 Paris, UIC Headquarters

CRITIS Unites Experts from Governments, Regulators, Science, Academia, Service Providers and other Stakeholders in one Conference to Secure Infrastructure

The registration for the 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016) is open. To register, please go to the dedicated website page which will guide you through the process:
http://critis2016.org/registration

Registration discounts

There is a discounted fee for confirmed speakers, attending students, as well as for members of the external associated event (the IMPROVER workshop). In addition, there is an early bird fare before 31 August 2016. Registration will close five working days before the event.

> CRITIS 2016 is a global forum for researchers and practitioners to present and discuss the most recent innovations, trends, results, experiences and concerns in selected perspectives of Critical Information Infrastructure Security and Critical Infrastructure Protection at large.

Peer reviewed papers

The submitted papers cover one of the following topics: (1) Technologies: Innovative responses for the protection of cyber-physical systems; (2) Procedures and organisational aspects in C(I)IP: Policies, best practices and lessons learned; (3) Advances in Human Factors, decision support, and cross-sector C(I)IP approaches; (4) Special private stakeholder session; (5) Young CRITIS and CIPRNet Young CRITIS Award (CYCA).

The peer-review process is currently concluding. All accepted papers will be included in full length in the conference pre-proceedings. The selected post-proceedings will be included in a special volume published by Springer-Verlag.

Keynote speakers

As in previous years, invited keynote speakers and special events will complement a programme of original research and stakeholder contributions. Three keynote speakers have already confirmed their attendance with presentations on hot topics of the moment (http://critis2016.org/keynote-speakers).

Dr Artūras PETKUS (NATO Energy Security Centre of Excellence, Lithuania) will give a CIPRNet Lecture entitled: “CEIP and Energy Security in Perspective of NATO Energy Security Center of Excellence”.

Dr Paul THERON (Thales Communications & Security, France) will present “A way towards a fully bridged European certification of IACS cybersecurity”, related to the work of DG JRC’s ERNCIP Thematic Group on IACS cybersecurity certification.

Mr Kris CHRISTMANN (University of Huddersfield, Applied Criminology Centre, UK) will give an overview of the “Findings from the PRE-EMPT Project: Establishing Best Practice for Reducing Serious Crime and Terrorism at Multi-Modal Passenger Terminals (MMPT)”.

Commander Cyril STYLIANIDIS (Ministry of Interior, General Directorate for Civil Protection and Crisis Management, France) will provide on overview of “The Crisis Interministerial Cell (CIC), the French tool for interministerial level crisis management”, illustrated with recent examples from France.

Local Chair:
Jacques COLLIARD, Head of UIC Security Division
e-mail: **colliard@uic.org**

Programme Organizing Chair:
Grigore HAVARNEANU, Research Advisor, UIC Security Division
e-mail: **havarneanu@uic.org**

Programme Co-Chairs:
Roberto SETOLA, Campus Bio-Medico University of Rome
e-mail: **r.setola@unicampus.it**

Hypatia NASSOPOULOS, Ecole des Ingénieurs de la Ville de Paris (EIVP)
e-mail: **hypatia.nassopoulos@eivp-paris.fr**

CRITIS 2016

uic INTERNATIONAL UNION OF RAILWAYS

Associated events

In addition, several C(I)IP-related events will be organised at UIC during the next days after CRITIS. Most of these associated events (http://critis2016.org/associated-events) will be organised in parallel and will be open to registered CRITIS participants, but the number of places is limited. Registration is therefore made on a "first come first served" basis.

The IMPROVER Workshop: Meeting public expectations in response to crises – aims to discuss how infrastructure operators meet these requirements today and how this can be improved. The program will begin with a short introduction to the project and then detail the findings from the project with regards to the tolerance of the public to service disruption. Then some scenarios will be presented before discussing with the operators about public expectations and crisis management.

> CRITIS 2016 continues the "Young CRITIS" community-building activities for fostering open-minded talents.

Call for Sponsors and Exhibitions

Given its wide scope and interesting topics, but also due to its scientific quality and impact in the worldwide Critical (Information) Infrastructure (C(I)IP Security) community, CRITIS 2016 can also be the perfect opportunity for sponsors and exhibitors. A limited number of opportunities are available for organisations and companies that wish to exhibit at this conference: http://critis2016.org/sponsors-and-exhibition

Venue

CRITIS 2016 will take place at the International Union of Railways (UIC) Headquarters, in the very heart of Paris, between the banks of the Seine and Champs de Mars, only a foot away from the Eiffel Tower. **Address:** 16 rue Jean Rey, F-75015 Paris, France

Key dates

CRITIS event:
10-12 October 2016

Associated events:
13-14 October 2016

Additionally, to find out more information about CRITIS 2016, travel directions, etc. please visit the website at www.critis2016.org

Previous conferences

LNCS CRITIS 2014 and 2015 proceedings have been recently published:

- http://www.springer.com/us/book/9783319316635
- http://www.springer.com/us/book/9783319333304

Programme and additional information

The full CRITIS 2016 programme will be published on the conference website shortly after this ECN issue.

Preliminary programme

10th October
12:00 - Registration
14:00 -14:30 Conference Opening
14:30 -16:00 Session 1
16:30 -17:50 Session 2
18:00 - Networking Cocktail at UIC

11th October
09:00 - 10:30 Session 3
11:00 - 12:20 Session 4
12:30 - 14:00 Lunch at UIC
14:00 - 15:50 Session 5
16:20 - 17:20 Session 6
19:30 - Dinner at Paris Wine Museum

12th October
09:00 - 10:30 Session7
11:00 - 12:20 Session 8
12:30 - 14:00 Lunch at UIC
14:00 - 14:40 Session 9
14:40 – 15:30 Closing Session

13th October
10:00 - 17:00 IMPROVER Workshop
9:30 - 17:00 CIPRNet Plenary Meeting

14th October
9:30 - 14:00 CIPRNet Plenary Meeting

Links

ECN home page	www.ciprnet.eu	
ECN registration page	www.ciip-newsletter.org	Please register free of charge
CIPedia©	www.cipedia.eu	the new CIP reference point

Forthcoming conferences and workshops

6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016, Davos Switzerland
TIEMS 2016 Annual Conference	http://tiems.info/About-TIEMS/tiems-2016-annual-conference.html	13 – 15 September 2016, San Diego, USA
11th CRITIS Conference	www.critis2016.org	Conference Oct,10-12, 2016 in Paris
Cyber Storm	www.swisscyberstorm.com	Oct 19, 2016 in Lucerne, Switzerland
51ST ESReDA Seminar	www.esreda.org/events	Oct 20-21, Clermont-Ferrand, France

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu
European Organisation for Security	www.eos.ecom
Netonets organisation	www.netonets.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu
DG HOME CIPS CIRAS	www.cirasproject.eu
Eurocontrol Service	www.eurocontrol.int/centralised-services www.eurocontrol.int/download/publication/node-field_download-9852-0
Novel indicators for identifying critical **INFRA**structure at **RISK** from Natural Hazards	www.infrarisk-fp7.eu
Smart Mature Resilience project	http://smr-project.eu/home

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" In this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security	https://resilience.enisa.europa.eu/nis-platform
Platform Current policy debates	http://digitalwatch.giplatform.org

Websites of Contributors

Acris	www.acris.ch
Atos	www.atos.net
The Bro Network Security Monitor	https://bro.org
Broala - Understand your network	https://www.broala.com
Campus Bio-Medico di Roma	www.unicampus.it
CINIT National Inter-University Consortium for Telecommunications	www.cnit.it/node/103
EC Joint Research Centre	https://ec.europa.eu/jrc
EOS European Organisation for Security	www.eos-eu.com
Eurocontrol – Air Traffic Management	www.eurocontrol.int
Financial Services Information Analysis Center	www.fsisac.com
Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS	www.iais.fraunhofer.de
H2020	http://ec.europa.eu/programmes/horizon2020
Hewlet Packard Enterprise	www.hpe.com
International Computer Science Institute	www.icsi.berkeley.edu/icsi
TECNUN – School of Engineering	www.tecnun.es
Union International Chemin de Fer	www.uic.org
University of British Columbia	www.ubc.ca

www.cipedia.eu

Let’s grow CIPedia©

An online community service by the CIPRNet Project.

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

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

> CIPedia© has more than 200.000 qualified clicks and is still growing. Join and look!

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

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.
The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

> Your contribution is essential for putting value in the CIPedia© effort.

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

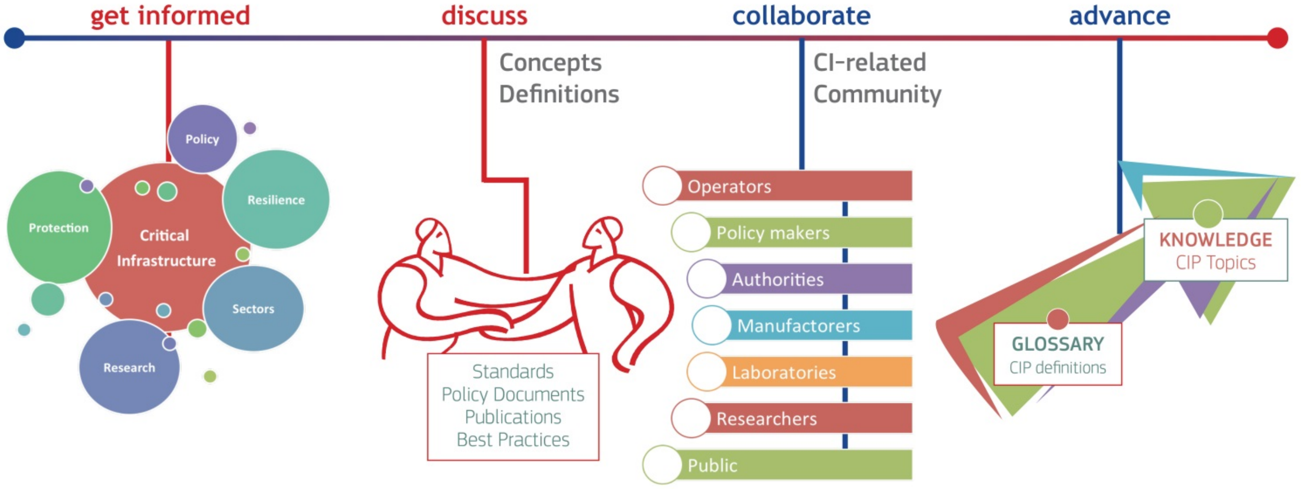
marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.



European CIIP Newsletter

November 16 - February 17, Volume 10, Number 3

Industrial Control System (ICS) Security Focus

ECN

Contents

CIPR Net

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

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Method and Models

Ads of upcoming Conferences and Workshops

Links

Media on C(I)IP

Cyber security landscape, challenges, initiatives and solutions

Approaching next level of security by securing against APT and introducing new concepts for securing Industrial Control System

Nowadays, cyber security should be considered as a crucial aspect of critical infrastructure protection. Networked mission critical systems and national critical infrastructure may be vulnerable to cyber threats, cybercrime and cyber terrorism. The same hazards apply to citizens and small-scale ICT systems (e.g. used by SMEs).

Currently, there are many initiatives and projects working on critical infrastructure protection and cyber security. In this issue of ECN, several European and national research initiatives focused on increasing resilience and cyber protection of CI are described. A special focus is on state-of-the art research in Industrial Control Systems (ICS), because of little computing resources and real time availability the hardest IT infrastructure to protect and to detect malware.

The EU CIPS project FACIES targets to illustrate the feasibility of a distributed approach to detect in an early stage failures and malicious adverse events of different nature in CIs.

The idea of the SAWSOC is to bring a significant step forward in the convergence of cyber and physical security technologies. SAWSOC platform is validated and demonstrated using three CI-related use-cases: air-traffic control system, energy production and distribution system, and security of mass-crowded events (at the stadium).

The EU project SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks, by determining gaps in current technologies and standards through a risk management approach.

European project SECURED funded by the FP7 Programme of the European Commission, focuses on the development of a complex security framework designed to manage all user security controls at the network edge.

The increased severity and variability in extreme weather events create effects of climate change: INTACT provides methods to re-assess climate-related risk for critical infrastructure owners and operators.

VITEX 2016 is an international table-top exercise with an innovative design for CIP within the EU.

The human factor is often neglected when planning and assessing critical infrastructure preparedness and resilience. A truthful consideration.

The Criminal Use of Information Hiding Initiative launched in cooperation with Europol's *European Cybercrime Centre* (EC3) combines expertise and experience from academia, industry, law enforcement agencies and institutions to tackle the increased utilisation of information hiding techniques and prevent its wider diffusion.

The goal of the SEZBC project is to create a Cyberspace Security Threats Evaluation System (SEZBC) for national security management in Poland. With its unique and novel approach, SEZBC integrates information from monitoring of cyberspace in a country.

The Polish national project BIPSE proposed and developed CI Security System that able to ensure secure IP-communications within the power grid management network in order to response current threats to SCADA systems.

Selected projects and experiences of the NASK/Polish CERT related to threat intelligence and actionable information sharing to fight Internet threats are described.

CIPRNet Trainer is designed as an al hazard tool to exercise crises management. A report of the first industry-research training.

Some of these challenging topics were addressed during the **11th edition of the CRITIS conference** in October in Paris. see: www.critis2016.org.

Enjoy reading this issue of ECN!

Michał Choraś [1]

he holds the professor position at University of Science and Technology (UTP) where he is the Head of ZST Division. He also works as the consultant in security and coordinates projects (e.g. FP7 CAMINO on cyber crime and cyber terrorism). He is the author of over 160 publications.
e-mail: **chorasm@utp.edu.pl**

Rafał Kozik

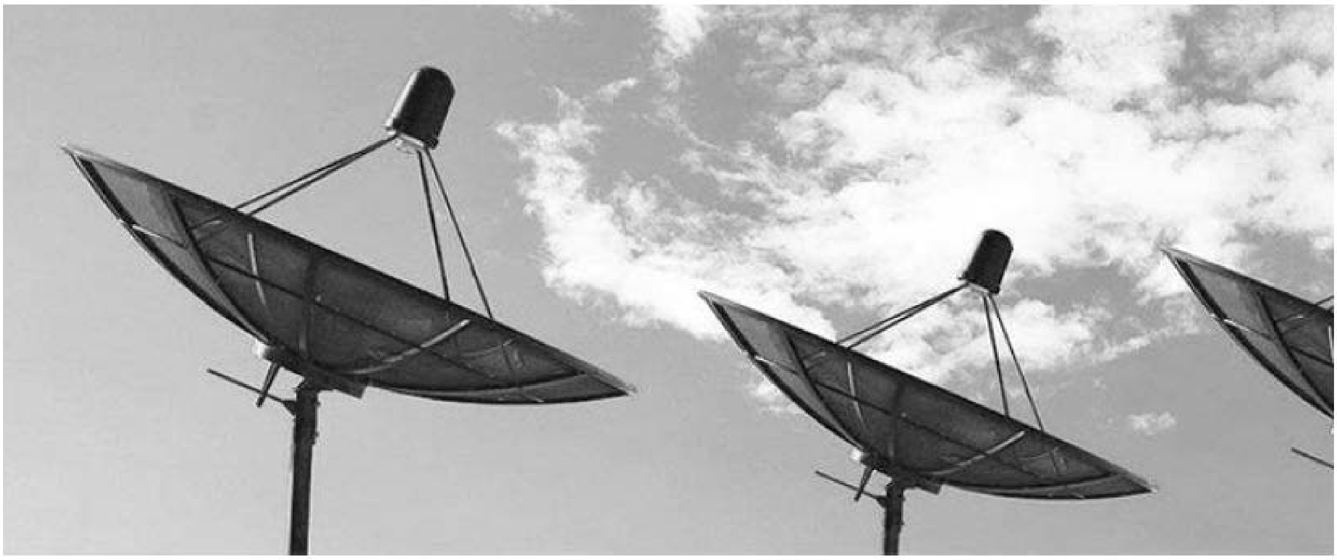
He is an assistant professor University of Science and Technology (UTP). In 2013 he received his Ph.D. in telecommunications. Since 2009 he has been involved in number of international and national research projects related to cyber security, critical infrastructure protection and data privacy
e-mail: **rkozik@utp.edu.pl**

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



IFIP 2017 - International Conference on Critical Infrastructure Protection

The Eleventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will take place in **Arlington (Virginia, USA) on March 13th-15th, 2017**.

The conference will provide a forum for presenting original unpublished research results and innovative ideas in the field of critical infrastructure protection.

Papers are solicited in the following areas of the critical infrastructure protection domain:

- Infrastructure vulnerabilities, threats and risks
- Security challenges, solutions and implementation issues
- Infrastructure sector interdependencies and security implications
- Risk analysis, risk assessment and impact assessment methodologies
- Modeling and simulation of critical infrastructure
- Legal, economic and policy issues related to critical infrastructure protection
- Secure information sharing
- Infrastructure protection case studies
- Distributed control systems/SCADA security
- Telecommunications network security

The deadline for paper submissions is **January 10th, 2016**; notification of acceptance will be communicated by February 3rd 2016. A selection of papers from the conference will be published in an edited volume – the eleventh in the series entitled ***Critical Infrastructure Protection*** (Springer) – in the fall of 2017.

For further information on the event please proceed to the following link

www.ifip1110.org/Conferences

Cyber-Physical attack analysis against Industrial Control Systems

A cyber-physical testbed, developed within the EU Project FACIES, has been exploited to study the interactions between the cyber and physical domains that arise due to physical faults and cyber-attacks against different components of an Industrial Control System.

Industrial Control Systems' (ICS) security has become a harder challenge since the fusion of ICS with Information Technology (IT) networks, as new and often unpredictable vulnerabilities and attack vectors typical from the cyber domain have emerged.

Several studies have demonstrated that the implementation of well-known cyber solutions and protection schemes is not enough, not even suitable most of the times, for ICS. In addition, as ICS generally constitute the core of Critical Infrastructures (CI), their correct, reliable, secure and safe operation is paramount. Consequently, tests can be hardly performed on real infrastructures.

With this premise, it becomes essential to develop realistic emulated environments where the analysis of the effects of cyber events on the operative conditions of the physical system can be properly addressed.

> Although similar to and enhanced by standard Information Technology systems, Industrial Control Systems present unique security challenges, especially in safety-critical contexts, and generally constitute a susceptible target for malicious attacks.
>
> The physical and cyber domains are to be studied as an overall system, considering their interactions and interdependencies, which are too often neglected.

The EU Project FACIES

In 2011, the CIPS European Project FACIES (online identification of Failure and Attack on interdependent Critical InfrastructurES) was born with the objective of illustrating the feasibility of a distributed approach able to detect in an early stage failures and malicious adverse events of different nature, taking place against CI.

Within this framework, a cyber-physical testbed has been created, where a wide number of experiments have been carried out to demonstrate and analyse the impact of cyber-attacks on the various elements of the system. These experiments include amongst others the control system, the SCADA (Supervisory Control And Data Acquisition) system, and the Fault Detection module.

The FACIES Testbed

The cyber-physical testbed consists in an emulator of a water supply and distribution system of a small city, a scaled down version reproducing a typical daily operation. For its realisation, all the main components of a real water system have been considered, from the plant (pumps, valves, tanks, pipes...) to the SCADA and control systems (Programmable Logic Controllers (PLCs), switches, Human-Machine Interfaces (HMIs)...) and (communication) networks.

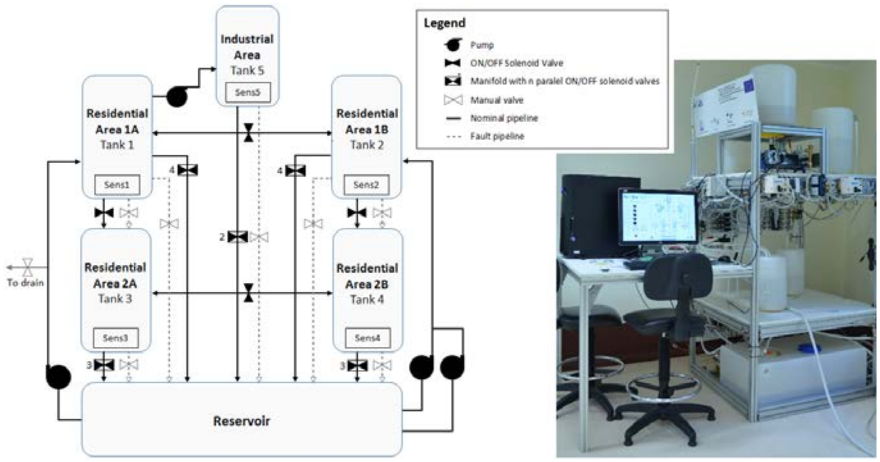
Three different areas have been considered, characterised by different water demand patterns from the customers, evolving in a six minutes scenario. The whole physical system is composed by six water tanks of different capacity, four centrifugal pumps, 20 solenoid valves, and a system of pipes.

Estefanía Etchevés Miciolino

Dr. Estefanía Etchevés Miciolino received the PhD in Engineering from University Campus Bio-Medico of Rome in 2016, where is member of the Complex Systems & Security (COSERITY) Lab since 2011. She has been involved in several EU Projects for Critical Infrastructure Protection, and received the 2014 CIPRNet Young CRITIS Award for the best conference paper.

e-mail: **e.etcheves@unicampus.it**

Eight manual valves have been included to reproduce water leaks from the tanks or along the pipes.
The system configuration allows its deployment in a large number of different configurations (serial, parallel, crossed-connections, and their combinations). Thereby, different scenarios can be studied with high flexibility, varying from 14 nominal configurations, discretely modulating the water output flow of the tanks, and exploiting 39 different physical faults that can be induced in the testbed.


Legend
Pump
ON/OFF Solenoid Valve
Manifold with n paralel ON/OFF solenoid valves
Manual valve
Nominal pipeline
Fault pipeline
Industrial Area Tank 5
Sens5
Residential Area 1A Tank 1
Sens1
Residential Area 1B Tank 2
Sens2
Residential Area 2A Tank 3
Sens3
Residential Area 2B Tank 4
Sens4
To drain
Reservoir
4
4
2
3
3

On the control side, a commercial framework has been employed, a centralised architecture consisting of two PLCs collecting the sensors measurements and controlling the actuators, deploying the Modbus/TCP for communication. Through a local TCP network, the PLCs, SCADA, HMIs and monitoring systems have been connected.

The Fault Detection System

The Fault Detection (FD) module monitors the operation of the physical system, comparing the sensors' near real-time measurements obtained from the SCADA system with the relative expected values calculated from a nonlinear model of the system, and triggers an alarm where a considerable deviation is observed, revealing the occurrence of a fault.

A graphical interface allows the operator to monitor the evolution of both the water level in the tanks and the error signal. The detected faults trigger the proper alarms on the SCADA HMI.

A wide number of experiments tested the FD's validity and effectiveness, considering both single and multiple physical faults on the system.

Testbed's Cyber Domain

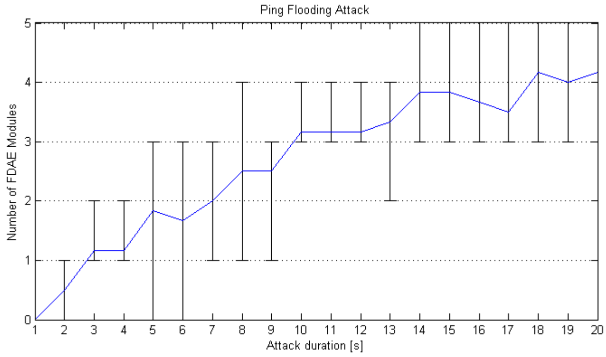
Significant differences can be enumerated between ICS/SCADA systems and traditional IT networks. For the former, among others, the principal concerns and challenges are represented by the unavailability of critical data or assets, and the violation of their integrity.

Atypical and unexpected situations could be induced on the system through targeted and well-designed cyber-attacks. Assuming an attacker has already gained access to the control network, several attacks against the availability (Denial of Service (DoS)) and the integrity (Man-In-The-Middle (MITM)) of the system have been carried out. These attacks differed on the pursued goal, depending on the target component (PLCs, FD system, SCADA/HMI...), and varying from single to concurrent and/or coordinated attacks.

Cyber and Physical Domains Interaction

The experimental results have shown not only the FD system's validity against induced physical faults and the effectiveness of the cyber-attacks targeting the control and/or SCADA system. It was also demonstrated in *Etcheves et. al*[1] that, if the attacker gains sufficient knowledge about the system and its operation, it would be possible to cover the effects of the attacks by designing the proper combination of events and relative duration, making it hard for the operator to distinguish whether the system is undergoing a cyber or a physical anomaly.
Indeed, a complex behaviour could be obtained by combining attacks. Fake healthy information could be sent to the HMIs, while actually corrupting the system's component in a way to move it to an unstable state. The hazard is made undetectable to the operator, who is therefore not able to perform required recovery actions. Conversely, the malicious agent would be prone to emulate an attack taking place on the target system. In such a case, the operator would face the anomalous behaviour, performing recovery operations which are not actually required or, in the worst case, halting the system, moving it to an unexpected or unstable state.

If you would like to know more about FACIES please visit our website: http://facies.dia.uniroma3.it/



[1] Etcheves M. E., Bernieri G., Pascucci F., Setola R. *Communications Network Analysis in a SCADA System Testbed Under Cyber-Attacks*. 23rd Telecommunications forum TELFOR 2015, 24-25th November 2015, Serbia (Belgrade). (2015)

The FACIES Project was supported by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission – Directorate – General Home Affairs (HOME/2011/CIPS/AG/4000002115).

SAWSOC: An integrated platform for achieving the convergence of physical and cyber security technologies

The FP7-SECURITY Programme project SAWSOC provides an advanced security solution for enhancing Critical Infrastructure protection guaranteeing the protection of citizens and assets.

Despite logical and physical security depend on each other, it is surprising that until now many companies still treat them as separate entities. Today, technologies for implementing security in the aforementioned domains are both stable and mature, but they have been developed independently of each other. over time some advancements have been achieved – e.g. Security Event Management (SEM) and Security Information Management (SIM) have merged into Security Information and Event Management (SIEM), and Logical Access Control Systems (LACS) and Physical Access Control Systems (PACS) have merged into Identity Management (IM) – but the real convergence is still a faraway target.

The main goal of **S**ituation **AW**are **S**ecurity **O**perations **C**enter SAWSOC project is bringing a significant step forward in the convergence of cyber and physical security technologies. By "convergence" we mean an effective cooperation (i.e. coordinated and results-oriented effort to work together) among previously disjointed functions. The project provides a security platform which is experimentally evaluated in the domains of three use cases that deal with: the protection of a Critical Infrastructure for Air Traffic Management, the protection of a Critical Infrastructure for Energy Production and Distribution, and the protection of a public place, specifically a stadium, during a public event. These use cases are characterised by very different requirements and directly involve people, and thus provide concrete evidence of the improved security on the citizens.

SAWSOC idea

The basic idea behind SAWSOC is shown in Figure 1 where the most relevant security technologies are grouped in two partially overlapping categories, namely Physical and Logical. The figure emphasizes that, especially in the recent years, some solutions have been combined (i.e. SEM and SIM have merged into SIEM) but much is yet to be done.

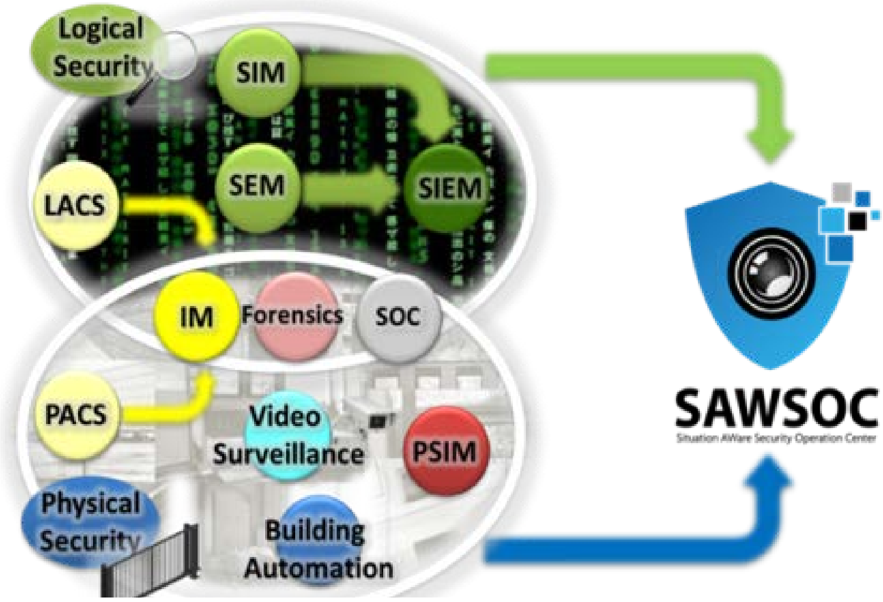


Figure 1– SAWSOC: A leap forward in convergence direction

Gaetano Papale [1]

Gaetano Papale is a PhD Student at University of Naples "Parthenope". His research activities are focused on intrusion detection, fraud detection and big data analytics. Currently, he is involved in the FP7 LeanBigData project.

gaetano.papale@uniparthenope.it

Gianfranco Cerullo
Gianfranco Cerullo is a PhD student at University of Naples "Parthenope". His field of interest is the cyber-physical security through the use of the Data Fusion techniques.

Bruno Ragucci
Bruno Ragucci has received from University of Naples "Federico II" a master degree in Computer Engineering. His thesis work was focused on Critical Infrastructure protection.

Also, Security Operations Center (SOC) technology has improved significantly, but SOC solutions have typically designed using custom specific needs. Others key security systems like Video Surveillance, Forensic support and Building automation are still a limited capability of performing complex correlations on security relevant data. SAWSOC holistic approach and enhanced awareness technology allow dependable detection and diagnosis of attacks. By "dependable" we mean:

Accurate
The detection and false positives rate must be an improvement of current State of the Art products. Accuracy is achieved by performing sophisticated correlations on multiple streams of diverse events which are collected in the logical and physical domains. It is important remarking that in contexts as Critical Infrastructures or crowded places, false alarms can be as harmful as false negatives.

Timely
It represents a challenging task, since the large amount of heterogeneous data that the system has to process in near real-time. To this end, SAWSOC platform implements the best solutions available in the field of Complex Event Processing, distributed real-time computation, and message brokering.

Trustworthy
SAWSOC is designed and implemented using fault-and intrusion-tolerant techniques. It is resilient to faults and attacks and is able to perform its tasks even in the presence of attacks or/and if itself is under attack.

SAWSOC features

The main features of SAWSOC platform are the following:

1. Enhanced situation awareness
2. Real-time monitoring facilities, implemented as dependable functions
3. Distributed platform, designed as a resilient system
4. Ability to handle data heterogeneity
5. Ability to interoperate with existing technologies
6. Ability of escalating from fault/intrusion symptoms to the adjudged cause of the fault/intrusion, and of estimating the damage to individual system components

SAWSOC use cases

SAWSOC is designed and validated considering the following use cases:

1. Maintenance Impacts and Attack Recognition on Critical Infrastructure (MIARCI)
2. Energy Production and Distribution Critical Infrastructure (EPDCI)
3. Crowded Events Safety & Security (CES&S)

The MIARCI use case is provided by ENAV S.p.A. ENAV is responsible of the Air Traffic Control (ATC) service in the Italian sky area and national airports. ENAV Security Operation Center monitors and manages several types of security events collected by a plethora of physical and logical devices including SIEM, Network and Service Monitoring Systems and Physical Access Control Systems with real-time data processing features. In this use case, the SAWSOC platform is used to protect the ATC infrastructure from malicious internal attacks (i.e. those perpetrated by company employees). SAWSOC enhanced data integration and data correlation capabilities will allow a timelier and accurate detection and diagnosis of attacks. Also, the SAWSOC awareness technology will consent to understand whether an outage is due to a legitimate maintenance operation or is the effect of a malicious attack.

The EPDCI use case is provided by the Israel Electric Corporation (IEC). IEC generates and distributes the electricity to the whole country. IEC ensures a continuous supply of electricity (only two hours per year of outage is allowed) leveraging capability to remotely control the electric grid through a SCADA system. This system includes operation centre functions, communication infrastructure and field equipment, such as: SIEM, IP cameras, biometric fingerprint readers and Intrusion Detection Systems (IDs). Under normal operating conditions, the use of this SCADA system provides continuous service guaranteeing the compliance with the Service Level Agreement (SLA). However, a cyber-attack or improper actions on the SCADA system may result in severe interruptions in the supply of the electric service. A cyber-attack can violate both security and electrical equipment by causing the sensors to show wrong information and producing damage and/or prolonged interruptions. The SAWSOC solution provides an effective coordination of the security systems and allows to backtrack he origin of the attack, the identification of the suspected person performing the attack and re-enabling of compromised sensors.

The CES&S use case is provided by Comarch S.A. and deals with the protection of a public place during an event. Comarch is the majority shareholder of Cracovia sports club, the oldest football club in Poland. Specifically, Comarch is the owner of the Krakow Stadium and must provide the citizens protection during the crowded football matches. The system used to guarantee the security of supporters is composed of CCTV cameras and biometric systems like face recognition and fan card (i.e. a magnetic card which contains all the details to identify the supporter). SAWSOC platform demonstrates the benefits of converged physical and logical security to the large public and it guarantees/supervises:

- the recognition of unusual activity taking place inside the stadium (movement of large crowd, gathering of a large number of people or people suddenly running away)
- the recognition of persons involved in some unethical or criminal activity inside the stadium
- the access to the stadium only to the authorised people

SAWSOC architecture

SAWSOC is the integrated technology platform that allows for accurate, timely and trustworthy detection and diagnosis of security attacks, combining information from physical and logical event sources. The overall architecture of SAWSOC platform is been designed through a collaborative process, during which both general and use case specific requirements have been taken into account. In Figure 2 the overall SAWSOC architecture is shown. SAWSOC platform has the ability to combine event information from multiple event sources to make sophisticated diagnosis based on the received events. It is made up of the following components:

- Video Content Analysis
- Correlation Engine
- Rule Engine
- Forensic Module
- Identity & Credential Management System
- Visualisation Module

The VCA (Video Content Analysis) receives the inputs from Video Surveillance system and focus them into high-level concepts and events. Computer vision algorithms are applied to the video streams to perform person detection, position and movement direction of the detected person, and specific action.

The Correlation Engine is the component in charge of the event diagnosis process. The attack diagnosis process is driven by correlation rules that aggregates the parameters of attack symptoms, such as the attack type, the target component and the temporal proximity. The Correlation Engine operates by correlating a huge amount of security relevant information (coming from logical and physical sources and VCA) in real-time, and implements Complex Event Processing (CEP) techniques and stream processing computing technologies.

The Rule Engine provides the logical rules followed by the Correlation Engine. It includes two main components: Signature Based Support and Anomaly Based Support. The basic concept is that the rule defined in the Signature Based Support are not enough to detect all the attempts aimed to mine overall security. The Anomaly Based Support cooperates and complements the Signature Based Support in order to detect all possible breaches to system. The Anomaly Based module operates the following two steps:

- Get events to create behaviour model
- Process incoming events passing them to the behaviour model

The output produced by Anomaly Based Support (i.e. the timestamp of involved events and their anomaly level parameters) are provided to the Correlation Engine for the decision task.

The Forensic Module provides a set of services that enable the SOC operator to trace from an event to the log data that identify it. The module ensures that the events and their associated logs are stored in a relational database, namely the Forensic Storage, for further processing and investigations.

The Identity & Credential Management System provides credentials for user authentication, device authentication, and event signing in the SAWSOC platform. This information is used, for example, to allow a trusted employee to enter in a secure location or access to a secure IT system, or to allow a trusted device the connection to a secure network.

The Visualisation Module is a powerful Human Machine Interface able to present to the user the alerts received from the Correlation Engine. It has been developed in such a way that the user has an immediate understanding of the situation in order to take proper and quick actions. This component provides also functionality for forensic evidence, such as browsing logs of original events and generating reports.

SAWSOC Demonstration

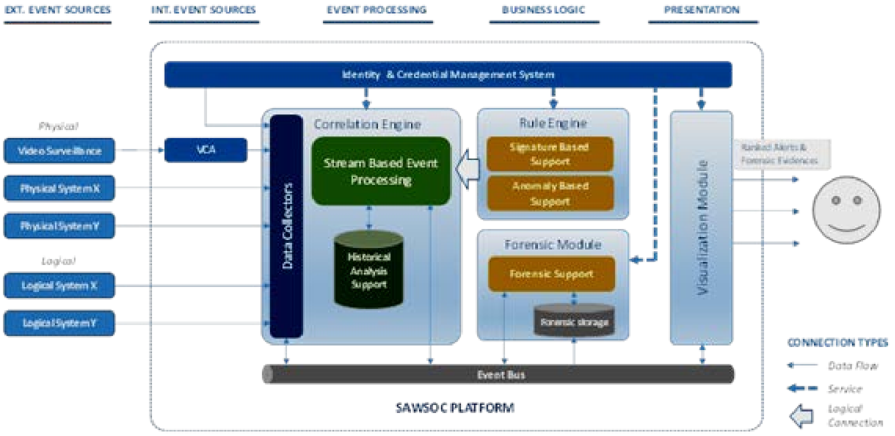


Figure 2 – SAWSOC Platform: Overall Architecture

In the following the features of SAWSOC platform are demonstrated.

In order to present misuse-based detection, effectiveness of Visualisation module, event correlation and data fusion features, the CES&S use case has been considered as a reference scenario. This demonstration consists of a detection of a guard during his/her patrol path.

Each sector of the Krakow Stadium is controlled by means of a camera (whose output is analysed by the VCA module) and by using Bluetooth beacons. VCA and Beacons are used to identify the guard during its patrolling. Three situations may occur: In the first case both VCA and Beacon recognise the guard. This case is a no alarm situation and the Visualisation module lights the corresponding sector of the stadium green.

The second case occurs when the guard is detected only by either the VCA or a Beacon (the order is irrelevant). This case is a warning situation and the sector turns orange.

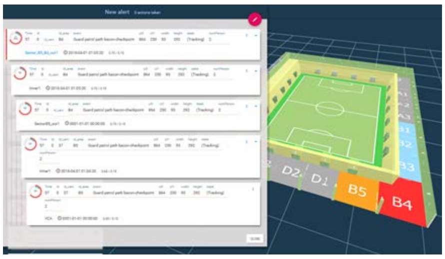


Figure 3 – An alarm showed by Visualisation module

The last scenario occurs when the guard is not detected both by VCA and Beacon. This is the alarm situation and the colour of the sector turns red (sector B4 in Figure 3).

In addition to these situations, the SAWSOC platform is able to detect many other events and it is customizable according to the user needs. For example, SAWSOC detects an alert also if the guard takes too much time to pass a sector or to complete the entire patrolling path.

The SAWSOC cyber-physical security provisioning features are demonstrating in the EPDCI use case. Suppose that the network administrator of a Power Grid company is corrupt or he/she has been bribed to install a proxy machine implementing a Man-in-the-Middle attack. The goal of the attack is to disrupt supplying power to a big number of customers and hide from operators the real state of the system. The attack sequence consists of the following steps:

1. A person enters the secured room using his personal badge and is then detected by the camera. This event does not generate an alarm situation

2. If the person unplugs one of the Ethernet cords from the rack and connects a new device, these events are detected as a warning (Figure 4)
3. The attacker connects his device and performs the attack (taking the control of one or more Remote Terminal Unit and blind the control to the entire SCADA system). This event is detected as a warning.

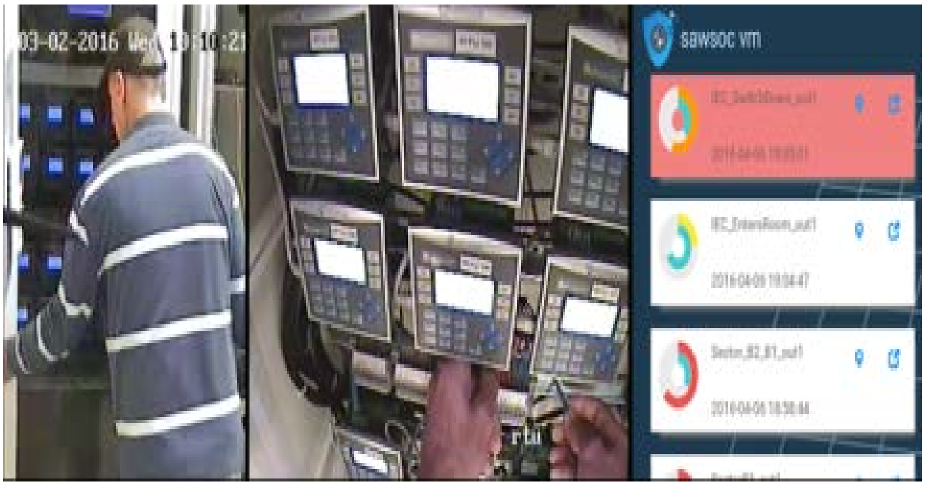


Figure 4 -Detection of router state change – Warning situation

Now, the SAWSOC Correlation Engine correlates all these events, detects the malicious pattern and generates the alarm. In Figure 5 is depicted the visualization of an alert situation in case of Man in the Middle attack detection. The Visualization module shows the equipment that has generated the alarm and its location within the infrastructure.

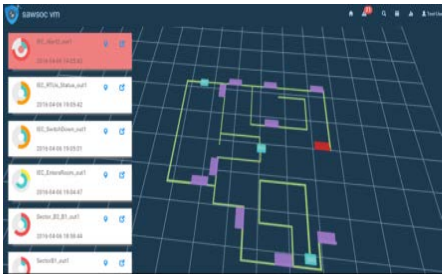


Figure 5 – Man in the Middle attack detection

The SAWSOC platform anomaly based capability is demonstrated considering the MIARCI use case. ENAV security policies provide that within the ATC (Air Traffic Control) room two operators must be simultaneously present at every desk. In case of one operator is not present, the post should not be activated. Each operator has at his position: a headset, a monitor that shows radar information and an authentication pad to log in. We consider an internal attack in which an operator has stolen the credentials of his colleague. Now, he can access to ATC room, sits to his position and logs in to it. After a while the attacker can move to his twin post and logs in with the stolen credentials of the unaware colleague. In this way, a single operator can take control of ATC position and perpetrates malicious actions. The SAWSOC platform detects the insider attack thanks to the inconsistency between the Physical Access Control system of the room and Logical Access Control at the post, specifically:

- One person enters the room, whereas two operators are logged in
- The legitimate owner of stolen credentials is not in the room, but is logged at the post
- VCA counts one person at the desk, but two employees are operating

SAWSOC platform focused all these events and triggers an alert (Figure 6).

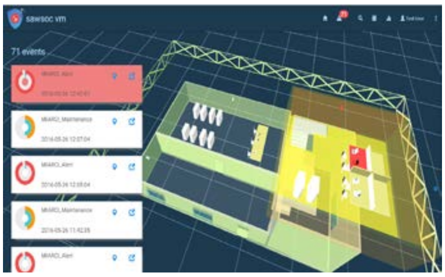


Figure 6 – Insider attack detection

The SAWSOC Consortium

The SAWSOC Consortium consists of 11 partners: Selex ES S.p.A. (Italy), CINI - Consorzio Interuniversitario Nazionale Per L'Informatica (Italy), Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.v. (Germany), The Israel Electric Corporation Ltd (Israel), ENAV S.p.A. (Italy), Intercede Ltd (United Kingdom), Espion Ltd (Ireland), Lonix OY (Finland), Bergische Universitaet Wuppertal (Germany), Esaproject SP Z OO (Poland) and Comarch S.A. (Poland).

Security for Smart Electricity GRIDs

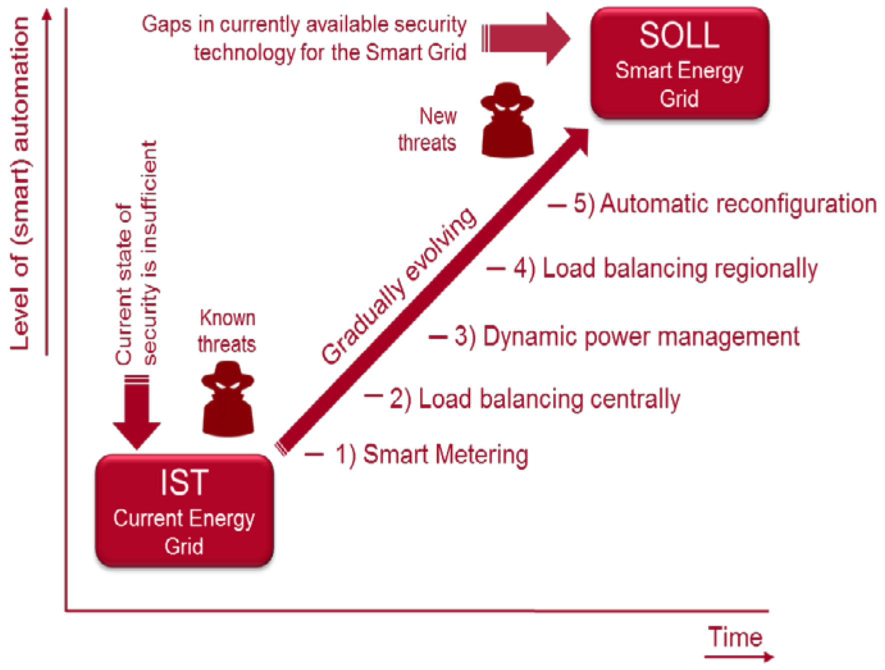
SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks, by determining gaps in current technologies and standards through a risk management approach, and by developing and testing novel security measures for smart grids.

The SEGRID project, funded by the EU under the FP7 program is a three-year (2014-2017) collaborative project coordinated by TNO.

SEGRID use cases

A smart grid can be considered as a utility-wide system (-of-systems) that will of course not come into being overnight, so it will be composed of a mix of old and new components. This is why SEGRID introduced the concept of a gradually evolving system in which new functionality is added to accommodate new use cases. We have deduced five use cases (The SEGRID use cases) that clearly demonstrate this gradual evolving systems concept (figure 1).

Figure 1 : The SEGRID storyline and use cases


Level of (smart) automation
Gaps in currently available security technology for the Smart Grid
SOLL
Smart Energy Grid
New threats
Current state of security is insufficient
Known threats
Gradually evolving
5) Automatic reconfiguration
4) Load balancing regionally
3) Dynamic power management
2) Load balancing centrally
1) Smart Metering
IST
Current Energy Grid
Time

The SEGRID use cases have been selected based on the work already done by ENISA along with the working parties involved in the mandates 441 and 490, as well as based on the work and competence of the project partners. The rationale for the SEGRID use cases is based on:

- Relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power;
- Addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

The SEGRID use cases cover the most relevant security issues that will arise from the increasing complexity of smart grids, which is confirmed by the strategic plans of the SEGRID Distributed System Operator partners Alliander and EDP.

Reinder Wolthuis

Reinder Wolthuis, M. Sc. is senior project manager and consultant cyber security at TNO (since 2006). He has almost 20 years of experience in innovation in information- and cyber-security. He participated in and led many security projects, involving innovations in (cyber)security, conducting security benchmarks & assessments, and security consulting
Reinder is the coordinator of the SEGRID project, leads WP6 (dissemination), and is involved in the risk assessment work of WP2.

e-mail: **reinder.wolthuis@tno.nl**
TNO
Eemsgolaan 3
9727 DW Groningen
The Netherlands

SEGRID objectives

The objectives of the SEGRID project are:

1. Establish security goals and determine threats of the SEGRID use cases.
2. Define the gap between available and needed security for smart grids, and develop new security methods, designs and tools to fill the identified gap.
3. Evaluate and enhance existing security risk and vulnerability assessment methodologies in order to encompass the increasing complexity of smart grid.
4. Evaluate and test new developed security methods and tools for smart grids (in realistic testbed environments), and assess their cost versus the consequences of failure.
5. Ensure that the SEGRID results are fed into the appropriate industrial partners, standardisation groups, governmental bodies, research community and regulators and to raise awareness

> The supervision and automation of power infrastructures is extending from the SCADA (Supervisory, Control, And Data Acquisition) control rooms to the high- and medium voltage network operations, and even low voltage networks, through monitoring and control of household appliances and renewable energy sources. This concept is generally referred to as the 'smart grid'. A smart grid essentially encompasses the smart automation of the complete transmission and distribution infrastructure that is needed for electric power transport; it covers the complete energy conversion chain from (distributed) generation to consumer.

First project results

SEGRID currently is in its third year and the first results are ready. We have detailed our SEGRID use cases, where each use case was split into several scenarios. We have selected a suitable risk assessment (RA) approach from several industry standard RA approaches and conducted a detailed RA on a number of the scenarios. These provide, combined with the smart grid security and privacy goals that were drawn up, valuable input for the development of new security measures. We also are working on enhancement of the risk assessment methodology, which includes aspects such as threat actor capability and motivation, societal impact, and dependencies between systems and stakeholders.

We are also working on enhancing and automating vulnerability assessment, where we use KTH's Cyber Security Modelling Language (CySeMoL) as a basis.

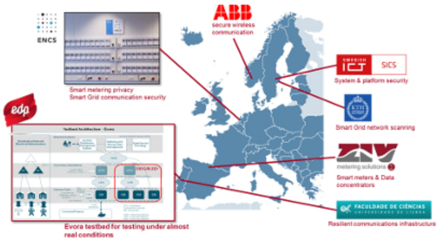

ENCS
Smart metering privacy
Smart Grid communication security
ABB
secure wireless communication
SICS
System & platform security
Smart Grid network scanning
edp
SEGRID
metering solutions
Smart meters & Data concentrators
Evora testbed for testing under almost real conditions
FACULDADE DE CIÊNCIAS
Resilient communications infrastructure

Figure 2: SEGRID Integrated Test Environment (SITE)

We have designed the SEGRID Security & privacy architecture (SPADE), a general design process to define security and privacy architectures specific for single use cases. Some of the concrete new security measures that SEGRID is working on are:

- Trusted platform, improvements to platform security solutions for devices in the smart grid.
- Resilient SCADA systems, to make the SCADA system tolerant not only to accidental failures but also intrusions.
- Enhancing IDS in mesh networks, by network traffic analysis and through authentication.
- resilient communication infrastructure for the core WAN network of a smart grid, by applying Software Defined Network (SDN) principles.
- Robust and scalable (D)TLS-based communication by improving its robustness and tolerance to Denial of Service attacks and key material provisioning during the (D)TLS handshake process
- Key management for group software distribution to distribute, revoke and redistribute (i.e. rekeying) the security material currently used within the group,
- Privacy-by-design solutions for the SEGRID Use Cases, by collecting and creating new privacy design patterns and Privacy Enhancing Technologies

To test these solutions, we have implemented the SEGRID Integrated Test Environment (SITE, see figure 2), which is a distributed test environment.

SEGRID Consortium

The SEGRID Consortium consists of ten members from five different countries. The consortium represents a well-balanced and strong partnership among DSOs, manufacturers, universities and research institutions,

The ten partners in SEGRID are:

- Organisatie voor toegepast natuurwetenschappelijk onderzoek TNO (NL)
- Swedish Institute of Computer Science (SE)
- Kungliga Tekniska högskolan (SE)
- Instituto Consultivo para el Desarrollo (ES)
- European Network for Cyber Security (NL)
- Liander NV (NL)
- ABB AS corporate research (NO)
- Foundation of the Faculty of Sciences of Lisbon University (PT)
- Energias de Portugal (PT)
- ZIV Metering Solutions S.L. (ES)

If you would like to know more about SEGRID please visit our website: www.segrid.eu

SEGRID has received funding from the European Union's Seventh Programme for research, technological development and demonstration under grant agreement No. 607109.

Promoting user-centric security in cyberspace: SECURED - SECURity at the network Edge

The growth of the Internet in recent years has transformed the way in which we manage business operations, engage in day to day activities, and communicate both personally and professionally, making it an indispensable pillar of modern society. With the advent of smart technologies, particularly within the framework of the Internet of Things (IoT), individuals have come to rely on a range of connected devices in the home and office environments. Depending on their role, individuals may not only be responsible for the security of their gadgets, but also those of their children or employees. At the same time, threats in cyberspace, such as malware, are on the rise, and even the most vigilant users are susceptible to a range of cyberattacks.

Managing the security of multiple devices through the configuration of various security applications rarely, if ever, provides a level of uniform security capable of protecting data and personal information. Moreover, many of today's smart devices, especially those used in the home, are not capable of independently running security software, despite the fact that they are connected to the Internet in some capacity and are therefore vulnerable to attack. This new environment requires that users be effective in managing their cybersecurity needs by employing both a proactive and streamlined approach.

SECURED, a project funded by the FP7 Programme of the European Commission, focuses on the development of a complex security framework designed to manage all of a user's security controls at the network edge[1]. In simpler terms, SECURED can be perceived by end users as a portal or initial entry point allowing them access to an individualised profile through which they can manage all aspects related to the cybersecurity of their devices before connecting to the Internet. Profiles are protected in a user repository that can be accessed through the cloud or a network edge device, such as a router, and are only accessible via a secured, verified connection that is remotely attested and can be made available through a trusted third party host, for example a user's telecom provider.

Within this trusted virtual domain, users can configure their security controls. All of a user's security settings previously defined through SECURED will also become operational during this stage. Basic and expert users will have the option to manage their security requirements (policies) as they see fit, with expert users able to customise security controls through medium-level security requirements, while basic users can express their preferences via the use of checkboxes referring to easy-to-read security statements and high-level security requirements. Depending on the requirements selected, SECURED will be able to determine which personal security applications (PSAs) to automatically assign to the user, such as those developed for anti-phishing, content filtering, network monitoring, etc. User requirements are enforced at the level of a network edge device (NED), ensuring that all traffic to the user's device is checked in accordance with security requirements, and that user preferences are transportable, providing uniform protection across all devices and Internet access points. In addition, user security requirements are part of a hierarchical structure, or policy stack, that can be beneficial to employers and parents aimed at keeping their networks and dependents safe, as will be highlighted below when discussing the practical applications of SECURED.

Francesca Bosco

Unicri (United Nations Interregional Crime and Justice Research Institute)

Francesca Bosco is UNICRI Programme Officer. She is responsible for cybercrime and cybersecurity related projects and member of the Advisory Groups on Internet Security Expert Group of the EC3.
Email: **bosco@unicri.it**

Arthur Brocato

Unicri (United Nations Interregional Crime and Justice Research Institute)

Arthur Brocato is a Fellow at UNICRI, working within the Emerging Crimes Unit on issues related to cyber-security, terrorist organizations' use of the Internet, and other security-related projects.
Email: **brocato@unicri.it**

[1] Further information on SECURED can be found by visiting the project's website, available at: https://www.secured-fp7.eu/

The PSAs that have already been developed by the SECURED consortium include those designed for packet filtering, application filtering, content filtering, re-encryption, anti-phishing, network monitoring, anonymisation, bandwidth control, and a corporate VPN. As more PSAs are developed and refined, users will be able to uniformly protect all of their devices with applications that are able to adapt to mitigate the risks posed by emerging cyber threats. The protection of communication channels and certain traffic stipulated by users provides a robust form of data protection.

Real World Applications

The possible applications of the SECURED technology in the real world are manifold; however, within this context, the positive effects for child online protection, businesses employing bring-your-own-device (BYOD) policies, and individual management of devices within the IoT should be highlighted.

The protection of children and minors online has continuously been an issue of critical importance for parents and policymakers alike. Offering parental controls has become fundamental for Internet service providers since the age of dial-up connections; however, with the proliferation of mobile devices, laptops, and other gadgets, parents can have a harder time enforcing security policies across a range of their children's devices, while also being assured that these policies are uniform in nature when referring to devices that utilise differing telecommunications services. By using SECURED, policies for all devices can be implemented through a single control centre, allowing parents to comprehensively restrict access to certain websites; categorically themed areas of the web, including gambling, pornography, and extremist websites; applications; and chat rooms, all of which can serve as areas of illicit activity.

As mentioned above, the hierarchical policy stack of SECURED represents a positive feature for parents, in particular, as well as for employers. In the event that policies higher up in the stack are active, users of SECURED, in this case children, would be notified of these overarching policies before accessing the Internet.

With respect to the workplace, aside from headline-catching cyberattacks against large corporations, small and medium enterprises (SMEs) are increasingly becoming targets of cybercrime. These entities represent weak links in the cybersecurity chain, having few or no IT experts employed within their organisations, while also potentially serving as backdoors for cybercriminals to enter the systems of large corporations with whom the SMEs have a business relationship. Start-ups, small family run businesses, or even larger entities may rely on employees to use their own laptops and other devices for carrying out their work, risking sensitive payment data being exposed via a single employee carrying out an unencrypted transaction.

BYOD policies may be more cost effective for employers, but the ramifications of a data breach can significantly damage the reputation and financial standing of any company. Through SECURED, businesses and other organisations can mandate that all employees accessing the Internet via their networks maintain a certain level of security on their personal devices. This ensures that anyone accessing the NED has a secure connection and uniform policies in place, before surfing the Internet.

Finally, with the expansion of the IoT, laptops, desktop computers, and smart phones will come to represent only a fraction of the devices connected to cyberspace. The refrigerator that is capable of notifying its owner via the Internet when it is low on milk, or the ability of homeowners to control their thermostats remotely are only a few examples of IoT technology currently in existence.

The IoT exists beyond the home environment, extending to the workplace and capable of connecting heavy machinery, monitoring accessories in hospitals, tracking mechanisms for transport, and other sensitive equipment across an array of different sectors. SECURED technology acts as a focal point for security management and can therefore significantly assist actors from a variety of sectors in the administration of their respective security architectures in the IoT. The system addresses the needs of devices that are more at risk: devices having limited computational power (and therefore unable to locally execute security controls) and devices that run on custom platforms, which may not be designed with security in mind. In short, administrators controlling the NED of their respective IoT networks have the ability to protect all of their connected devices of varying sophistication as they see fit, customising security controls to meet their personal or business needs, while incorporating devices that may not be able to execute cybersecurity measures via their own accord.

Conclusion

In conclusion, establishing a uniform level of cybersecurity across all user devices to defend against emerging threats has become paramount for ensuring adequate protection in cyberspace. Moreover, SECURED's use of trusted virtual domains at the network edge for setting up individualised security controls adds a much needed level of trust and verification to the configuration process and overall cyber ecosystem. Easy specification of security policies simplifies configuration and hence encourages users to take direct control of their protection. As stakeholders in the tech and international community strive to promote a global culture of cybersecurity, SECURED's user-centric architecture and approach to device security serve as valuable components for achieving this aim.

Risk management support on critical infrastructure protection against extreme weather events

The increased severity and variability in extreme weather events resulting from effects of climate change, requires critical infrastructure owners and operators to re-assess their risks: the INTACT project supports this process.

INTACT is an EU FP7 project which aims

to offer **Decision Support**

to **CI operators and policy makers**

regarding **Critical Infrastructure Protection** (CIP)

against changing **Extreme Weather Event** (EWE) risks

caused by **Climate Change**.

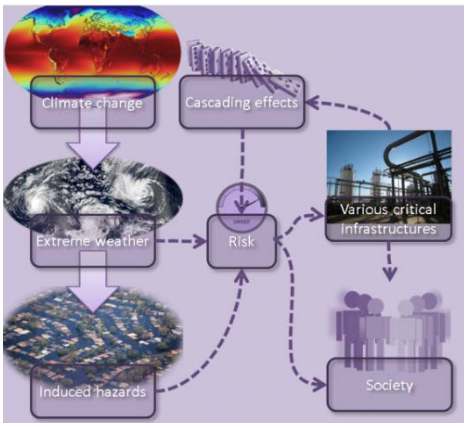
We have five case studies in which we have developed and tested our concepts with a variety of true local end-users:

- Landslides, in the Campagnia region, Italy;
- Flash floods, in the Southern region of Spain;
- Flooding the Cork area, Ireland;
- Winter storms, in the Pirkanmaa region, Finland;
- Flooding, in the Rotterdam Harbour, Netherlands;

We now have entered the final stage of the project in which we will validate our concepts with the end-users in each of the case studies.

INTACT Wiki

The main concept of the INTACT project, depicted in the figure below, is how we connect the various domains/ expertise, with risk (management) as key-point.



This concept is also depicted on the home page of the INTACT Wiki:

www.intact-wiki.eu

The INTACT Wiki is the platform in which the knowledge, tools and methods, developed in INTACT are shared with the world. On it, you can find information, references, guidance, and experiences on how to ensure continued resilience of critical infrastructures in the context of changing climate and related extreme weather events. This information is primarily directed at operators of critical infrastructures and policy makers involved with these critical infrastructures and can be used in various ways.

The Wiki contains a large amount of interconnected information that attempts to cover the needs of a wide range of potential users. In order to support users looking for a specific type of information, we provide several entry points that direct them to the various sections of the Wiki that would be of most interest to them.

In this way, the Wiki serves as a user friendly and intuitive online repository on valuable background information and knowledge about climate change, EWE, and CI, with examples, illustrations and references. Amongst other, it contains data on:

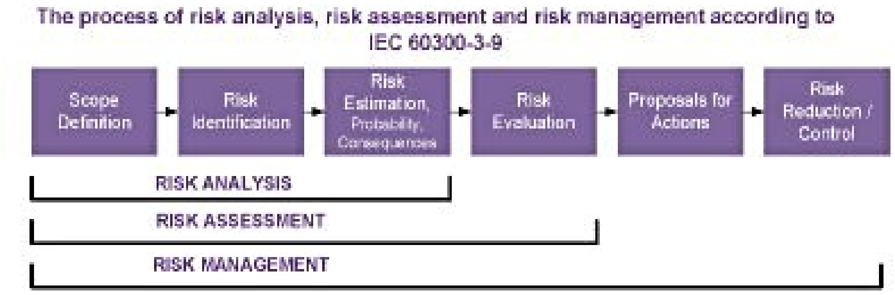
- Climate change for the medium-term & long-term period;
- Changes in frequency and strength of EWEs;
- Changes in induced hazards;
- State-of-the-Art tools and methods used in risk assessment;
- Specific vulnerabilities for EWE for specific CI;
- Assessed best practices on mitigation measures;

Peter Petiet

Peter Petiet is a senior project manager at the Netherlands Organisation for Applied Scientific Research TNO. Amongst current other activities, he is the project coordinator of the EU FP7 INTACT project.

Since 2010 he has led many projects on technical and organisational innovations within safety and crisis management domains,
and on carbon capture innovations and business-to-business projects within the oil and gas domain.
His main interest is on connecting worlds, organisations and people for the sake of business continuity, increased efficiency and effectiveness and increased safety and security.

e-mail: **peter.petiet@tno.nl**



Step-by-step method

In order to use this data to determine the future EWE risks to your CI, and to guide the user through this large information source (depending on the type of CI and EWE that are of interest to the user) we have developed a step-by-step method using the risk management process presented in BSI (2010).

The risk management process identifies the main steps comprising 'good practice' in decision-making. It recognises the circular nature of risk management, which may require the review of the risk analysis and assessment after implementation of risk reduction control measures. The steps of the process are:

- **Scope definition**

  Determines the scope of the risk assessment in terms of the CI, the information needed and the type of approach, timeframes and scales to be considered;
- **Risk identification**

  Explores and classifies the main hazards and vulnerabilities taking into account cascading effects;
- **Risk estimation:**

  Assesses the risk magnitude using available models and taking into account uncertainties;
- **Risk evaluation:**

  Assesses the magnitude of risk considering the particular context of the CI;
- **Proposals for action:**

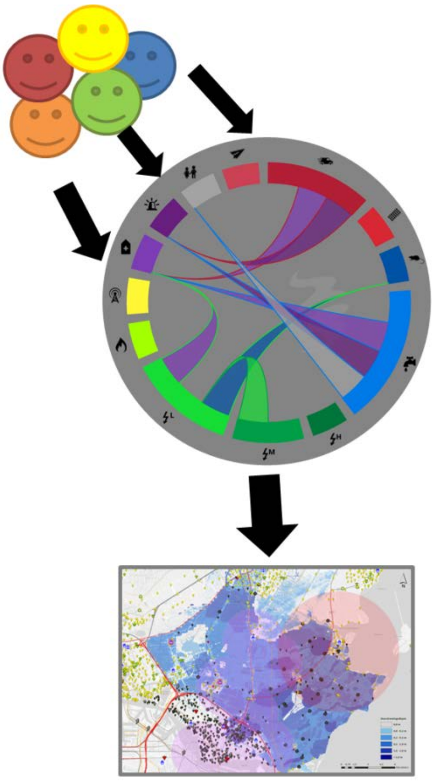
  Provides guidance on the possible mitigation measures to reduce the estimated risk;
- **Risk reduction control**

In each of these steps, it is described why which tools/methods are applicable, and how you should use them. One example tool, used in the each of the five case studies, and found very valuable for CI operators/ owners to get a notion of potential cascading effects, is the C!RCLE tool.

C!RCLE is a support tool for different network owners, stakeholders and authorities or governments to find out and discuss cascading effects together in a workshop setting. During the discussion, dependencies between the networks or objects are drawn and the causal relationships between them are collected in a database (example figure shows results from the Irish case study, Cork).

What we found is that many CI owners and policy makers already have their own risk assessment/ management methods in place. With our approach, we do not just develop another method, but we tend to support them with all mentioned valuable information.

They should still use their own familiar current tools and methods, and possibly including our data on (future) EWE, and on subsequent induced hazards.



INTACT project and consortium

The INTACT project has been launched on May 01, 2014 and will deliver its final results in 2017. TNO is coordinator of the project consortium with eleven partners from eight countries: CMCC (IT), DELTARES (NL), FAC (IRE), DRAGADOS (SP), HR Wallingford (UK), PANTEIA (NL), NGI (NO), CSIC (SP), Un Stuttgart (GE), Un Ulster (UK), VTT (FI).

In case you would like more information on the INTACT project and its outcomes, please visit our websites:

http://www.intact-project.eu

http://www.intact-wiki.eu

or mail us at info@intact-project.eu.

References & acknowledgment

BSI (2010), "Risk management. Risk assessment techniques", BS EN31010:2010

Hounjet, M.W.A., Kieftenburg, A.T.M.M., and Altamirano, M. (2015), "Learning from flood events on Critical Infrastructure: relations and consequences for life and environment (CIrcle)",
Available at:
https://www.deltares.nl/app/uploads/2015/04/Learning-on-flood-events-on-CIrcle.pdf
[Accessed August 2016]

INTACT (2016), "Draft prototype IRG". [Online]
Available at:
http://www.intact-wiki.eu/
[Accessed August 2016]

Räikkönen, M., Mäki, K., Murtonen, M., Forssén, K., Tagg, A., Petiet, P.J., Nieuwenhuijs, A.H. and McCord, M. (2016), "A holistic approach for assessing impact of extreme weather on critical infrastructure", in International Journal of Safety and Security Engineering, Volume 6, Issue 2, pp 171-180

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 606799. The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion.

VITEX 2016 international table-top exercise

An innovative exercise design in the context of critical infrastructure protection within the EU.

Scenario

VITEX 2016 provided an intensive and innovative learning experience for participants from various disciplines and 22 Member States. The target group consisted of government specialists in the field of civil protection and electricity, and representatives of national (power) grids - internationally known as the Transport System Operators (TSOs). The table-top was based on scenario-based policy discussions, which means that the participants made use of situation descriptions to discuss the possible implications within a particular context. The main storyline was that the EU Critical Infrastructure Energy was affected. The shortage of power in Europe was a result of an extremely dry winter and a hot summer, which caused low water levels in rivers. Cooling water became scarce, ships loaded with coal could not reach the coal plants, an explosion of jellyfish clogged the pipes of cooling water and the electricity demand to power refrigerators, air conditioners and other cooling systems increased tremendously.

Security, economic stability and the general well-being of EU citizens largely depend on critical infrastructures and the services they provide. The make-up of a single country's critical infrastructure is complex, not least because of the dependencies and linkages with other countries.

All the more reason to strengthen the ties between EU Member states on this subject by facing challenges together during an exercise on different levels: international, national and public-private.

Therefore, the NCTV organised the international exercise VITEX 2016 in Amersfoort on 11 and 12 May 2016. The exercise was financed from the Internal Security Fund (ISF) of the European Commission.

Objectives

1. Bringing relevant existing networks together both at a national level, and a cross border level.

2. Strengthening the awareness of the need for cooperation for protecting Critical Infrastructure (CI).

3. Strengthening the awareness of the need for joint CI exercises (public and private).

4. Enhancing insight in the impact of the disruption or failure of CI on society, including the cascading and cross border effects.

5. Gaining insight in how cooperation can mitigate the impact of potential disruptions of CI and society.

6. Further establishing guidelines or lessons learned in a concise way.

Jeroen Mutsaers

Jeroen Mutsaers (MSc) is a policy officer at the Dutch Ministry of Security and Justice working on (inter)national security and resilience and climate change adaptation. He is the Netherlands CIP contact point and is currently involved in the novel national approach for CI and resilience.

Alyssa Brinkhof

Alyssa Brinkhof works as a project leader in the resilience department at the Dutch Ministry of Justice. Among other things, she was involved in the development, co-ordination and delivery of the VITEX 2016 Tabletop. Alyssa has a background in International Relations.

Innovative Exercise Design

The focus of the VITEX innovative exercise design is on interaction between the participants. To support this, the VITEX exercise design consists of scenario-based group discussions that are interlinked with several supporting elements:
1. blind spot identification;
2. lexicon development;
3. knowledge market;
4. expert feedback.

Scenario Based Group Discussions

VITEX 2016 consisted of four rounds, with each round having a different thematic focus. This served to facilitate insight in the differences and similarities in approach for the various cooperation levels that can be distinguished during a crisis of this type. The focus in the first round was national; what does this scenario mean for your own country and how are things organised? This first round was played within the setting of the national team. The focus in the second round was also national, but now countries had the opportunity to discuss differences between countries on a national level. The third round focused on cross border cooperation, while the last one focused on EU-wide cooperation.

Blind Spots

There are two different types of blind spots.

1. When collaborating cross-sector or cross-border, participants may come across things they do not know, e.g. ways of working, procedures or contact points. Beforehand, they may not have been aware that they did not know this but during discussions it became clear more knowledge was needed.

2. It is also possible that participants are aware they need more information but do not know where to find it. The focus on the collection of blind spots creates a 'safe' learning environment, in which it is alright for participants to share that they do not know something. In addition, participants can actually help others by sharing their blind spots.

Lexicon

International communication is complicated by the fact that terms and definitions may differ per country. The VITEX exercise design increases insight in terms and definitions by acknowledging this and by building a lexicon together. The Critical Infrastructure-Pedia (CIPedia) was used as a support tool. In CIPedia terms and definitions in the field of Critical Infrastructure Protection are collected and shared (www.CIPedia.eu).

Knowledge Market

The VITEX exercise design allows relevant EU projects and organisations in the field of Critical Infrastructure to present themselves at a 'knowledge market'. These EU organisations and projects are not that well known by the participants. By giving them the opportunity to meet the EU organisations, and speak to them about their tasks and possibilities the participants will understand better how they could benefit from these organisations and how they can collaborate during an incident or crisis.

Expert Feedback

The experts appreciated the elements of the innovative exercise design and participated in the discussions actively by correcting false assumptions, and giving feedback at the end of each part. Their feedback focused on elements that were missing in the discussion, specifically relating to cooperation.

Conclusions and follow up

VITEX 2016 has led to a greater awareness of the interdependencies and has both the potential and the problems of cooperation highlighted at national level and between Member States. The exercise contributes to knowledge and awareness on the European crisis management structures and reinforces the cooperation between EU Member States in protecting critical infrastructure.

Within the realm of CIP there are many networks, but a platform where public and private actors interact and explore the whole of national and international cooperation is a place that is largely unexplored. That is why the VITEX exercise was developed with a focus on building cross-sector and cross-border cooperation. The evaluation made clear that the participants appreciated the VITEX exercise and that they would like to use exercises like VITEX 2016 to explore the various levels of cooperation more often. In various cases the exercise organisation was told that even the simple fact of having to compose a national team with the required field of expertise involved, had in itself been very valuable.

Exercise Guide

Besides the evaluation of the exercise, an exercise guide with the exercise design is available, which describes step-by-step how such a meeting can be organised. This guide is available for everyone to encourage possible follow up exercises in the future.

Please contact:
vitex@nctv.minvenj.nl if you are interested in the exercise guide.

Critical Infrastructure Preparedness and Resilience – The Human Factor

We all view the world with our own lens, a factor of our experiences and perceived opportunities. Immersed in our formulae and offices it is easy to forget who benefits and who loses based on the decisions we make.

Most communities today, are dependent upon critical infrastructure (CI): without power, water, sewage treatment, gas pipelines, road and communication networks, daily life would come to a standstill. On a day-to-day basis, thousands of people are working to ensure that these systems remain operational and that society benefits from the advances in technology.

If you are one of those thousands of people, I would like to challenge some of your perceptions and improve the quality of decision-making.

What do you see?

Figure 1: Transmission line

If you answered "a high tension power transmission line system" you would technically be correct. But, there is another consideration: it is Judy's lifeline. Judy is 75 years old and is dependent upon her oxygen machine 24 hours a day, seven days a week. Without power, her oxygen machine will not function. Without oxygen, she will die.

There are millions of "Judys" in the world; people dependent on machines to keep them alive; life-saving medications that need to be refrigerated; homes that need to be kept warm; and communication channels that are need to respond to medical emergencies and crimes in progress. Millions more are dependent on CI to earn a living and support their families. Your work to enhance and protect critical infrastructure is important.

Your work doesn't just support an industry; what you do saves lives. CI can reduce suffering; save jobs and reduce financial losses; and protect the environment.

Not only does consideration need to be given on a day-to-day basis to ensure that often aging CI is functioning and able to meet the growing needs of the community, but increasingly, CI is threatened by disasters. Disasters can be caused by natural hazards (such as earthquakes or floods), diseases and epidemics (such as Avian flu or H1N1) or human-caused hazards. Human-caused hazards can be result from acts of omission (the dam wasn't built properly and collapsed) or by acts of commission (a terrorist planted a bomb in an urban centre).

> "Your work to enhance and protect critical infra-structure is important. Your work doesn't just help to support an industry; what you do saves lives."

Regardless of the cause, disasters are increasing. "There were 353 disaster events in 2015, of which 198 were natural catastrophes, the highest ever recorded in one year. There were 155 [human-caused] events."[2] There is no question that with the results of climate change becoming more visible, as we see natural hazards occurring in places where we never have seen disasters before, CI will increasingly be compromised.

Laurie D. R. Pearce

Dr. Laurie Pearce is an Associate Faculty member at Royal Roads University in Victoria and a Research Associate at the Justice Institute of British Columbia in New Westminster, both in British Columbia, Canada.

She sits on Canada's National Platform for Disaster Risk Reduction Advisory Committee and Chairs the Resilient Communities Working Group. One of her primary research interests lies in promoting investing in disaster mitigation strategies at the local community level and in increasing community disaster resilience. A current research project, the Aboriginal Disaster Resilience Project, can be accessed at https://adrp.jibc.ca

Laurie.Pearce@royalroads.ca

[2] Swiss Re Sigma. (2016). *Natural catastrophes and man-made disasters in 2015: Asia suffers substantial losses*. Retrieved from http://media.swissre.com/documents/sigma1_2016_en.pdf

The Sendai Framework

In 2015, 185 countries adopted the Sendai Framework for Disaster Risk Reduction 2015 -2030[3] at the United Nations World Conference in Sendai, Japan. The Sendai Framework is a successor to the Hyogo Framework for Action (HFA) 2005-2015: Building the Resilience of Nations and Communities to Disasters. These frameworks assisted in shifting the emphasis from one of responding to disasters to taking an approach that focus on reducing future and existing disaster risk, and strengthening disaster resilience.

The Sendai Framework provides a welcome focus on CI with an emphasis to "promote the resilience of new and existing *critical infrastructure*, including water, transportation and telecommunications infrastructure, educational facilities, hospitals and other health facilities, to ensure that they remain safe, effective and operational during and after disasters in order to provide live-saving and essential services (p.21).

The United National International Strategy for Disaster Risk Reduction (UNISDR) further stresses the importance of CI through its "Making Cities Resilient: My City is Getting Ready" campaign."[4] Around the world over 3,000 communities have pledged to adopt strategies to increase their disaster resiliency, including adopting:

Essential Four: Pursue, Resilient, Urban Development, and Design – Invest in a maintain critical infrastructure that reduces risk, such as flood drainage, adjusted where needed to cope with climate change; and

Essential Eight: Increase Infrastructure Resilience – Protect ecosystems and natural buffers to mitigate floods, storm surges and other hazards to which your city may be vulnerable. Adapt to climate change by building on good risk reduction practices.

Critical Infrastructure in Canada

Public Safety Canada designates key partners and stakeholders in CI as fitting into ten sectors:

1. Health
2. Food
3. Finance
4. Water
5. Information & Communication Technology
6. Safety
7. Energy & Utilities
8. Manufacturing
9. Government
10. Transportation[5]

The importance of these stakeholders can be recognised in recent disasters in Canada.

The 2016 Fort McMurray Fire ultimately destroyed 2,400 out of a total of approximately 19,000 homes. Once all of the residents were safely evacuated, the efforts on the second day were focused on fighting the fire but also a prime consideration was to protect CI[6]. There was recognition that without CI in place, no-one would be able to return to the city of approximately 61,000 residents.

The 2014 Lac Mégantic train derailment resulted in 47 deaths, and about 2,000 people were evacuated. Specialised hydrocarbon recovery operations were required to deal with the 6.7 million litres of petroleum crude oil which spilled into the community's storm and sewer system affecting the ability of evacuees to returning to their homes.[7]

The 2013 Calgary flood resulted in major damage to the city's CI.[8] The Bonnybrook rail bridge was undermined and resulted in a train derailment and all other 20 bridges were closed. Calgary's downtown, the business heart of the city, was essentially closed; all routes into the core were flooded and transit service was suspended. Power was shut off to all evacuated areas, including the downtown. Power was not completely restored to the core until for eight days. The transit system took a hit as the waters damaged C-Train tracks in the Erlton area, flooded tunnels and undermined roads. The flooding resulted in costs estimated at $1.7 CA billion.

As can clearly be demonstrated, there is a great need to consider how CI can be designed to be disaster resilient and to minimise post-disaster recovery and rebuilding costs.

How can CI Experts be Helpful to Local Communities?

Let me start off by stating what is *not* helpful. Keep in mind that most disaster and emergency management (DEM) personnel do not have any university education or research skills in CI. Presenting information to local DEM personnel as if you were speaking before a graduate class, or as if writing for a peer-review journal, is not helpful. Complicated formulae are certainly important to your peers to identify the validity and robustness of your data and findings; but they are not understood, and thus not helpful to local DEM managers.

What is helpful? First of all, consider your work in a local or regional disaster context. Is what you are working on relevant to the planning for, responding to, or recovery from a disaster? If so, then you have to step out of your research lab, university or college office and reach out to those involved in DEM. You may need to start by increasing your own under-standing of the DEM planning process.

[3] UNISDR. (2015). *Sendai Framework for Disaster Risk Reduction 2015 -2030*. Geneva, Switzerland: UNISDR.

[4] UNISDR. (2016). *Making cities resilient: My city is getting ready*. Retrieved from http://www.unisdr.org/campaign/resilientcities/

[5] Public Safety Canada. (2015). *Critical infrastructure*. Retrieved from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

[6] CBC News. (2016, *May wildfire rages in Fort McMurray as evacuees settle in Edmonton.* Retrieved from http://www.cbc.ca/news/canada/edmonton/wildfire-rages-in-fort-mcmurray-as-evacuees-settle-in-edmonton-1.3565573

[7] Transportation Safety Board. (2015). *Railway Investigation Report R13D0054*. Retrieved from http://www.tsb.gc.ca/eng/rapports-reports/rail/2013/r13d0054/r13d0054.asp

[8] City of Calgary. (2014). *Calgary's most damaging flood*. Retrieved from http://floodstory.com/floods/2013-flood

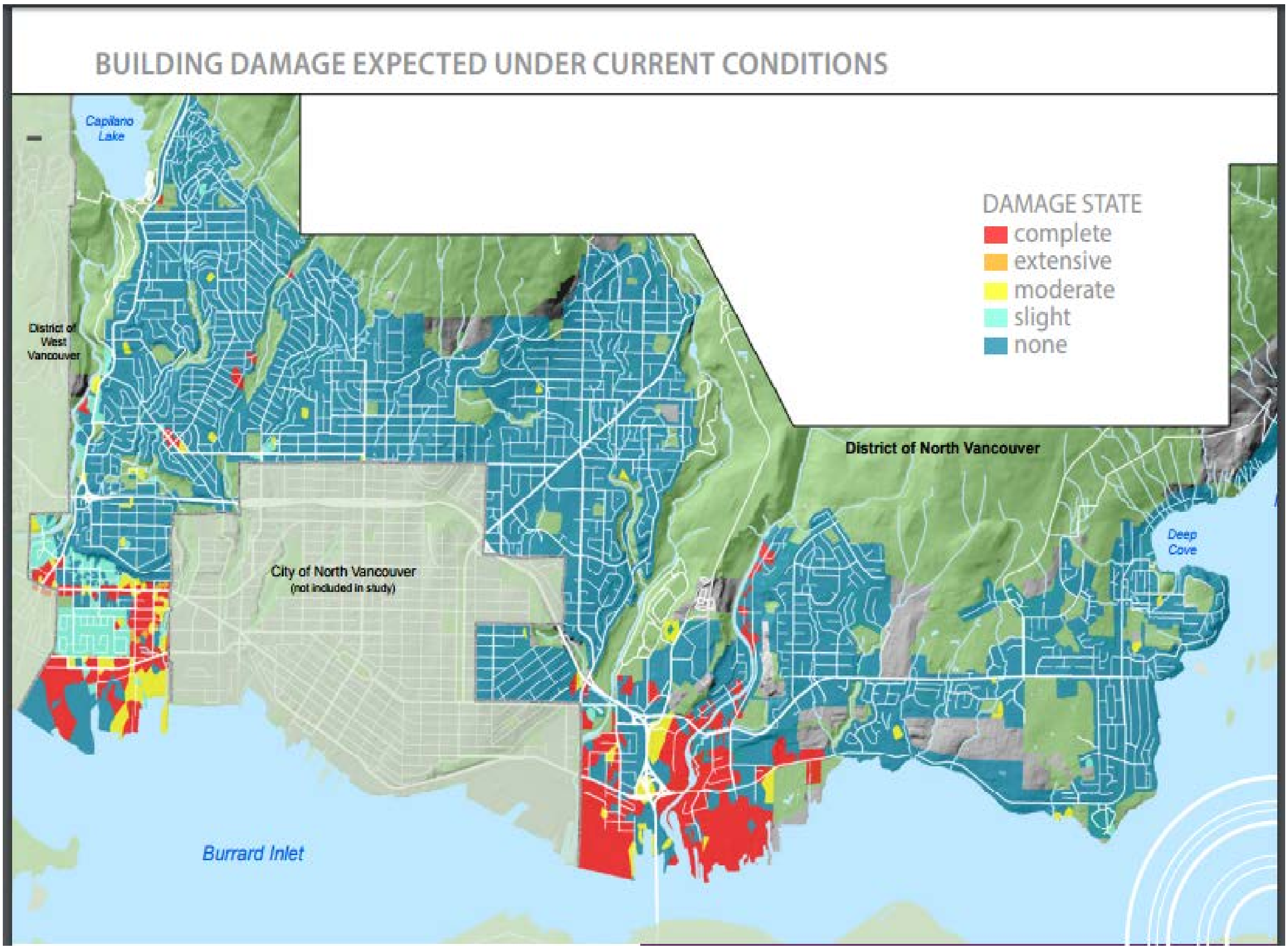

BUILDING DAMAGE EXPECTED UNDER CURRENT CONDITIONS
DAMAGE STATE
🟥 complete
🟧 extensive
🟨 moderate
slight
🟦 none
Capilano Lake
District of West Vancouver
City of North Vancouver (not included in study)
District of North Vancouver
Deep Cove
Burrard Inlet

Figure 2: Building Damage Expected Under Current Conditions

1. What are the potential hazards that could affect the community? Don't just focus on the typical hazards such as floods, wildfires or earthquakes. Think about the full range of potential hazards.

2. How would these hazards affect the CI that you are interested in? What is the exposure of the CI? Is the CI located in soil that would liquefy following a major earthquake? Would the CI withstand a snow-melt flood? What would be the demands on CI if the community was affected by a heat wave or period of severe cold weather? What would happen if 50% of the maintenance staff were not able to come to work as a result of a pandemic?

3. Once you have a good understanding of how the CI would be impacted by the hazard, you then need to consider how businesses, residents and industry would be impacted. What are the short- and long-term consequences?

4. Given the various hazards, are the risks acceptable, tolerable or unacceptable? If they are unacceptable, then what mitigative strategies would increase the CI disaster resilience? If they are only just tolerable, how can the CI be strengthened?

5. If there are no known mitigation strategies and the risk is unacceptable, this should be identified as a research priority.

6. When mitigative strategies are identified, who is responsible for implementing the strategy? What is involved in implementing the strategy in terms of costs and length of time?

7. Now take the results of your analysis and write them out in non-technical language so they can be understood by DEM professionals. Use simple graphics to illustrate the problems. Describe the impacts as stories.

   For example, consider the recent effort by the District of North Vancouver [9] to illustrate the potential impacts of a major earthquake on CI (see Figure 1) and how it would affect various community residents:

[9] District of North Vancouver. (2016). *When the ground shakes. Earthquake risk in the District of North Vancouver and what we can do about it.* Retrieved from https://www.dnv.org/sites/default/files/edocs/when-the-ground-shakes.pdf

Henry is driving to his first customer of the day when his van starts to bounce. He looks in the rear-view mirror for potholes in the road, but his attention quickly returns to the road ahead as the cars in front of him screech to a halt. They don't all stop in time and some are rear-ended, while a few others jump the sidewalk and another crosses the centre line into oncoming traffic. Henry watches as a powerline leans slowly into the street and the power cable suddenly snaps, spraying sparks….

Henry's van is hemmed in on all sides with other vehicles. … He can see almost every driver and passenger with a cell phone in their hand, but few have made a connection. He's not sure if he should try to help or walk back to Emma's daycare….

The stories are supported by complex analyses and GIS maps, but the report is written so that the impacts are clear to the average citizen.

8. Now you are ready to reach out to local DEM personnel and key stakeholders. Help them to understand what the issues are, and what you are concerned about. Advise them on ways to move forward; don't just leave them with the problem without some potential solutions.

   Consider how meeting the community's CI needs could be built into class project or would make an excellent graduate thesis. The next time you consider applying for a research grant, consider how the findings could be directly applied to help the community.

Perhaps this short article will stimulate your thinking and lead you to consider how you can:

1. Promote CI disaster resiliency.
2. Inquire as to what are the potential hazards.
3. Analyse your findings with a broad perspective – what does this mean to the citizens who live in the community?
4. Consult with peers to gain an appreciation of potential issues and solutions.
5. Encourage applied research to increase community disaster resiliency.
6. Reach out and share your findings and concerns with the local community.

No one knows when the next disaster will strike and who will be impacted it could be you and your family. The work that you do can contribute to your community's

1. sense of safety and calming,
2. self- and community efficacy,
3. social connectedness, and
4. hope.

SEZBC: Towards Situational Awareness in National Cyberspace

The goal of the project is to create a Cyberspace Security Threats Evaluation System (SEZBC) for national security management in Poland.

Cyber incidents pose a serious threat to governments, economies, businesses and individuals. Each country faces the problem of a growing number of serious attacks on essential computer networks. The first step to protect the national cyberspace is to improve situational awareness by continuous monitoring of critical infrastructure systems.

SEZBC project has been sponsored by National Centre for Research and Development and is carried out by the consortium of 3 entities: Military Communication Institute (leader), Enamor International Ltd. and PBP Enamor Ltd. Potential beneficiaries are Ministry of Digital Affairs, Internal Security Agency, Government Centre for Security and National Security Bureau.

EU has responded to this threat with policy and legislation proposals in the form of directives, plans and strategies [1][2][3]. Based on UE recommendations, national directives, acts, and programs have been incorporated (in Poland [4][5]). They emphasize that:

- Governments have a significant role in assuring a safe cyberspace, but since major parts of cyberspace are owned and operated by the private sector, cooperation between both sides is necessary.
- Each country should improve readiness and engagement of the private sector in cyberspace risk management in cooperation with the national authority for network and information security (NIS) (e.g. CERTs).
- There is a need for continuous monitoring of the national cyberspace that may be subject of cyber-attacks. The key cyberspace players like banking, energy supply, transport, Internet services as well as public administration should report incidents (identify, assess and manage the risks) to the national NIS competent authorities to enable common cyber situational awareness for decision makers.

National CIIP

Polish National Critical Information Infrastructure Protection assumes shared responsibility for the risk management across all levels of government and critical infrastructure owners and operators. In Poland a set of 11 systems, which have fundamental importance for the national security and comprehensive operation of the country has been identified. The full list includes:

- Energy, fuel and energy supply system,
- Communication system,
- Tele-information network system,
- Financial system,
- Food supply system,
- Water supply system,
- Health protection system,
- Transportation system,
- Rescue system,
- System ensuring the continuity of public administration activities,
- System of production, storing and use of chemical and radioactive substances, including pipelines.

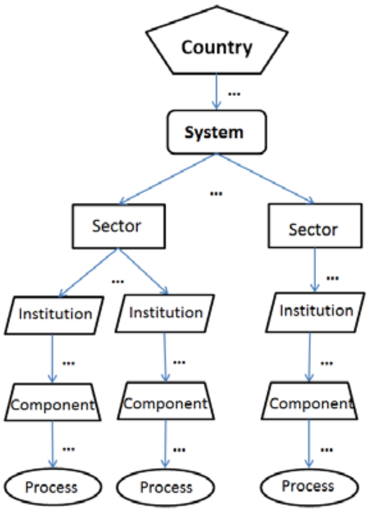


Figure 1

Each system may be composed of Sectors, Institutions, Components and Processes (Figure 1). The list of critical infrastructure elements is not available to the public.

J.Śliwa

Dr. J.Śliwa is a head of C4I Systems department in MCI. She has been responsible for SEZBC concept and architecture design .
e-mail: **j.sliwa @wil.waw.pl**

R.Piotrowski

Dr. R.Piotrowski is a researcher in MCI and as a Project Manager of SEZBC he has been involved in all phases of the project.
e-mail: **r.piotrowski @wil.waw.pl**

P.Berezinski

Dr. P.Berezinski is a researcher in MCI. He has been involved in implementation phase of SEZBC.
e-mail: **p.berezinski@wil.waw.pl**

SEZBC

SEZBC is a country-level cyber security evaluation system with decision support. It incorporates risk assessment and risk management functions together with situational assessment. In particular, SEZBC supports decision making process in evaluation of the state of emergency in case of large-scale cyber-attack/incident or high risk of cyber threats' materialization. This system supports what-if analysis for simulating potential threat escalation as well as testing the results of different mitigation options. Incidents' acquisition in SEZBC is supported by cyber-threat catalogue based on CAPEC [7].

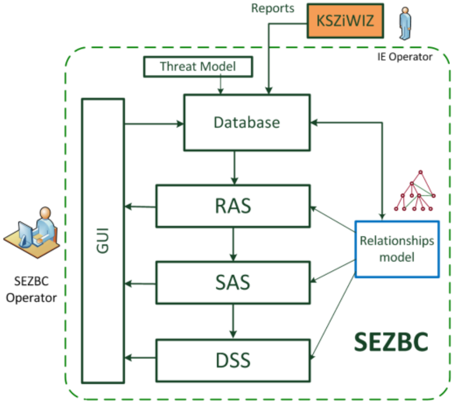


Figure 2

Analysis performed by SEZBC is done bottom-up based on relationships Model, a weighted graph where relations between nodes (Systems, Sectors, Institutions, Components, Processes) are modeled (according to National CIIP) and which maps the importance of particular entity to the operation of the whole country.

The heart of SEZBC is Risk Assessment Subsystem (RAS), see Figure 2. It employs an algorithm which takes into account system vulnerabilities (potential threats, possible effects resulting from threat materialization and security mechanisms used for attack counteraction) measured periodically by critical infrastructure elements' administrators, and incidents identified by security controls. Constituent parts of aggregated risk metric are propagated according to the predefined Relationships Model (Figure 3).

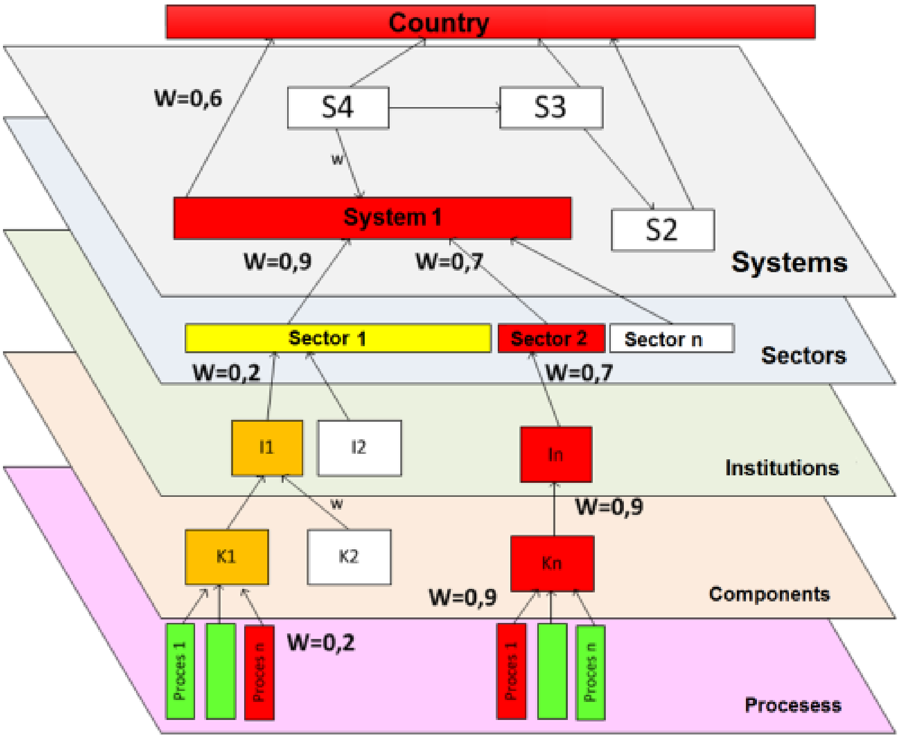
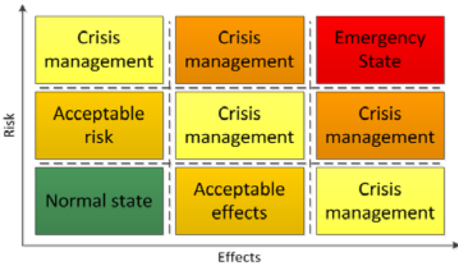


Figure 3

The results of Risk Assessment augmented with additional information on the effects of potential and actual attacks on the life of people and operation of the country are the input to Situation Assessment Subsystem (SAS). It evaluates the situation in terms of the impact of events on the life of the citizens and is able to recommend special organizational measures if necessary (e.g. crisis management, declaration of state of emergency or martial law). The effects of cyber-attack in real life are evaluated by a person responsible for attack/ incident reporting. The value of SAS recommendation is strongly dependent on the quality of input information (reliability of the Relationships Model and its parameters, precision of the systems' vulnerability level assessment and potential threats identification, assessment of the effects on a real life). Based on the national law, alarm states are grouped into 3 categories: emergency, natural disaster and martial law.



Crisis management	Crisis management	Emergency State
Acceptable risk	Crisis management	Crisis management
Normal state	Acceptable effects	Crisis management

Figure 4

Decision Support Subsystem (DSS) provides visualization and reporting of RAS and SAS results and enables to recommend possible reactions on the actual situation (on the country level) as well as simulate different decision scenarios. It is designed to support top-level decision makers yet allows to drill down into technical details in order to deeply investigate each threat (Figure 5).

SEZBC operates mainly on external data entered by the operators of the infrastructure. A proxy between SEZBC and other data source elements was called KSZiWIZ (Figure 2). In the current implementation it offers an application to be used by public administration (all levels), critical infrastructure operators, and business sector. However in the future it has been proposed to develop a specially tailored system for exchange of information between key cyberspace players, giving them the possibility to access cyberspace situational awareness on their level of responsibility and provide value-added early warning.

Conclusions

Figure 5

SEZBC integrates information from cyberspace monitoring on the country level and, in this terms our approach, is quite new and unique. The goal of the project was to prepare the pilot deployment enabling evaluation of cybersecurity threats of the Republic of Poland cyberspace. Successful deployment will enable improvement of cyber situational awareness and decision support for administrative units responsible for the national security.

Deployment of such a system demands a lot of effort and up to now it still leaves open issues, problems and challenges. Firstly, how to acquire all information to build and maintain (keep it up-to-date) comprehensive Relationships Model. Secondly, how to attract private sector to share data about risks and incidents which they observe in their systems and networks they are responsible for. This information is usually very sensitive and may be used against the company, resulting in the loss of reputation. In this aspect the institutions collecting such sensitive data must be in a position of an unlimited trust.

Thirdly, how to ensure that only reliable and up-to-date information from data source elements feed the system. This is the key requirement for the proper SEZBC operation and its ability to present actual situation.

References

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL Brussels, 7.2.2013 JOIN(2013) 1 final

[2] EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive

[3] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, {http://ec.europa.eu/maritimeaffairs/policy/maritime_spatial_planning/documents/swd_2013_65_en.pdf}

[4] Cyberspace Protection Policy of the Republic of Poland, Warsaw, 25 June 2013,

[5] National Critical Infrastructure Protection Programme, http://rcb.gov.pl/eng/?p=79

[6] Description of Project "Cyberspace Security Threats Evaluation System of the Republic of Poland for national security management", project No DOBR-BIO4/011/13221/2013,

[7] Common Attack Pattern Enumeration and Classification (CAPEC), Mitre Corporation, https://capec.mitre.org/ .

The 52nd ESReDA Seminar On Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity

52nd ESReDA seminar will be held on May 29-31, 2017 in Lithuania

Announcement and Call for papers

Critical Infrastructures Preparedness and Resilience (CIP&R) is a major societal security issue in modern society. Critical Infrastructures (CIs) provide vital services to modern societies. Some CIs' disruptions may endanger the security of the citizen, the safety of the strategic assets and even the governance continuity.

The critical role that CIs play in the security of modern societies is a direct effect of the ever-increasing spread out of the information technology (IT) in every smallest task in man's daily-life. The continuous progress in the IT fields pushes modern systems and infrastructures to be more and more: intelligent, distributed and proactive. That increases the productivity, the prosperity and the living standards of the modern societies. But, it increases the complexity of the systems and the infrastructures, as well. The more complex a system is, the more vulnerable it will be and the more numerous the threats that can impact on its operability. The loss of operability of critical infrastructures may result in major crises in modern societies.

To counterbalance the increasing vulnerability of the systems, engineers, designers and operators should enhance the system preparedness and resilience facing different threats. Much interest is currently paid to the Modelling, Simulation & Analysis (SM&A) of the CI in order to enhance the CIs' preparedness & resilience.

The European Safety, Reliability and Data Association (ESReDA) as one of the most active EU networks in the field has initiated a project group (CI-PR/MS&A-Data) on the "Critical Infrastructure/Modelling, Simulation and Analysis – Data". The main focus of the project group is to report on the state of progress in MS&A of the CIs preparedness & resilience with a specific focus on the corresponding data availability and relevance.

In order to report on the most recent developments in the field of the CIs preparedness & resilience MS&A and the availability of the relevant data, ESReDA will hold its 52nd Seminar on the following thematic: "***Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity***".

Topics

Threats identifications & specifications
CIs disruptions MS&A
CI's vulnerability MS&A
CIs' dependencies and interdependency MS&A
Data and Databases
Emergency and crises management models & tools
IT inferences on CIs preparedness & resilience
Standards & Ontology in the domain of CI protection (CIP)

Critical Infrastructures Sectors

Air-transport & airports
Electrical power generation & supply
Gas & Oil production, storage & transport
ICT networks
Massive data storage & servers
Maritime transport & ports
Medical & health care
Process industry
Railway transportation
Supply chain process
Water supply and water works

Threats

Extreme weather conditions
Natural threats
Earthquake
Flood
Forest fire
Landslide
Torrential rain
Tsunami
Volcanic eruptions
Industrial & technological accidents
Financial & stock market perturbation
Wastes disposal

www.esreda.org/event/52nd-esreda-seminar/?instance_id=39

BIPSE: Cyber security in Industrial Control Systems

BIPSE system offers a complex and effective protection of the Industrial Control Systems' (ICSs) information infrastructure from cyber threats

The Critical Infrastructure (CI) of a country is usually defined as the one providing essential services for the society, serving as a backbone on the nations' economy, security and health. According to National Critical Information Infrastructure Protection Program [1] in Poland it includes several systems, among which there are: power and fuel supply, communications, financial, food supply, water supply, health protection and transportation. CI plays a key role in the state operation and influences the lives of the citizens. Serious systems' disruptions or damages caused by natural forces or as a consequence of human activities can generate significant losses for the citizens and the economy.

SCADA

Power supply processes are realised hierarchically, from the level of the power plant, through the energy transfer grid, controlled by the Central Control System (CCS), to the distribution systems. They are controlled by the Supervisory Control And Data Acquisition (SCADA) systems. In the past, SCADA systems ran over dedicated analogue lines and networks with vendor specific protocols, hardware and software. The network for power generation control was isolated from the public network.
Today's SCADA systems take advantage of open transmission protocols, broadly used in communications networks together with computers running common operating systems that work as the base for Intelligent Electronic Devices (IEDs). This significantly improves automation efficiency and decreases costs spent on control systems, but certainly it also increases the risk of system vulnerabilities' exploitation and influences its security level.

Nowadays SCADA control commands and responses flow across IP-networks and over IP-stack. As a result, control systems such as SCADA, power transmission management system, centralised Load Frequency Control (LFC) System, intelligent field devices (e.g. Remote Terminal Unit located in the Control and Supervisory Substation (CSS)) or IEDs, create new concerns for the cyber security.

BIPSE System

In response to these threats, we have proposed and developed a CI Security System that is to ensure secure IP-communications within the power grid management network [2]. BIPSE cybersecurity system prototype provides:

- analysis of the network traffic, searching for threats and anomalies;
- detection of malicious actions using specially designed IED-emulating probes;
- correlation of events flowing from the sensors;
- automated detection and tracking of threats, giving appropriate response measures;
- management of the ICT infrastructure security (stations and technological communication);
- cyber situational awareness of the whole monitored CI (SIEM – like).

BIPSE system was developed by the consortium of four entities: Military University of Technology (leader), Research and Academic Computer Network, Military Communication Institute and Asseco Poland S.A. within the research project sponsored by the National Centre for Research and Development.

In particular, the security measures used in the BIPSE system are:

- authentication;
- advanced access control, e.g. with the use of ABAC model and security policies;
- anomaly detection and filtering of management and control IP traffic transferring IEC protocols;
- encryption of BIPSE management messages;
- monitoring of the status of the protected infrastructure and secure storage of information;
- honeypots and SCADA hardware emulation;

Marek Amanowicz [1]

Professor and Project Manager responsible for coordination of the entire work and cooperation with the customers.

marek.amanowicz@wat.edu.pl

Jacek Jarmakiewicz

Dr. Jarmakiewicz responsible for BIPSE system architecture design, framework tests, system verification and validation.

jacek.jarmakiewicz @wat.edu.pl

Adam Kozakiewicz [1]

Dr. Kozakiewicz, the Architect of the project, responsible for BIPSE reference architecture.
e-mail: **adam.kozakiewicz@nask.pl**

Joanna Śliwa

Dr. Śliwa, responsible for validation of the IEC 104 probe and engineering access control.
e-mail: **joanna.sliwa@wil.waw.pl**

- secure communications with the central SIEM and GUI;
- audit and traceability of management operations, and detection of potential unauthorised operations.

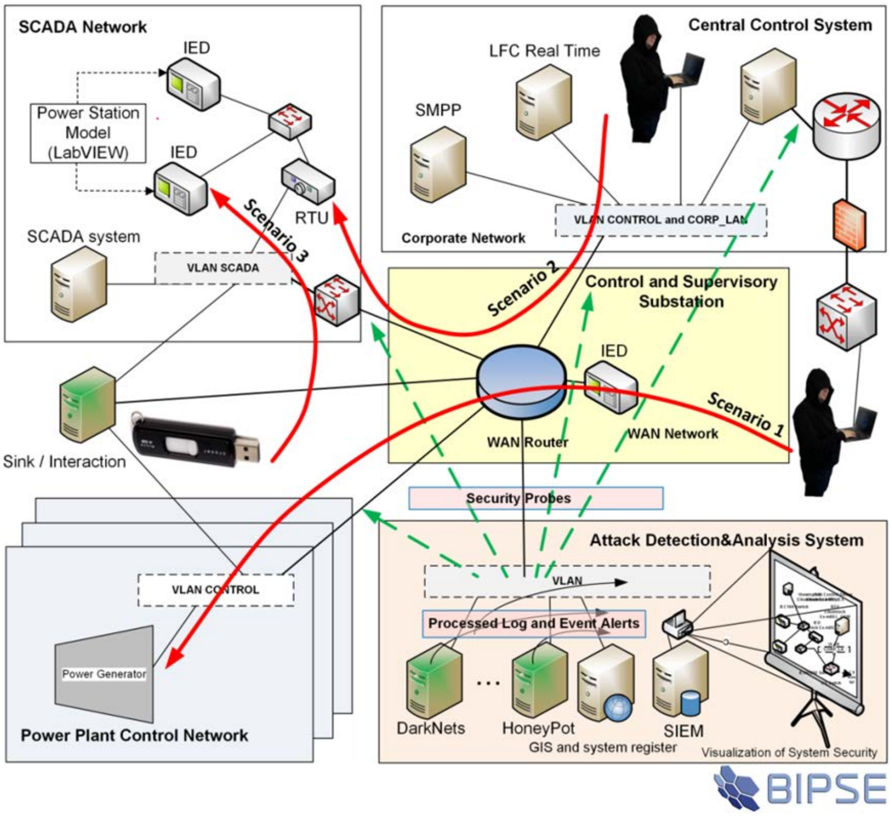


Figure 2. BIPSE test scenarios

BIPSE system evaluation

Functional tests of the system have been performed both in the consortium-owned laboratory environments [3] resembling the architecture of power stations as well as in the Laboratory of Distributed Generation at the Lodz University of Technology [4].

The experiments were designed to verify the ability of the system to detect cyber-attacks and to protect against them, as well as to adjust the sensitivity of probes and decoys developed in the project.

We intended to verify the efficiency of threat detection by tools developed by us, i.e.:

- probes based on Snort and Bro software that are adapted for analysis of the SCADA protocols (e.g. IEC 60870-5-104) in order to detect anomalies in the power control and management systems;
- commercial IDS/IPS probes that were previously purchased and are currently used in the power control and management network;
- HoneyPots, SCADA HoneyNets and DarkNets for monitoring and logging of all of the suspicious activities in ICS network;
- Mediation Device developed to normalise the messages obtained from the other security systems and elements;
- SIEM System gathering, analysing and aggregating information received from abovementioned elements;
- databases gathering the history of power control and management conditions;
- Cyber security Visualisation and Management System processing data produced in SIEM in real-time;
- engineering access control system for monitoring and control of all technical service activities – including video registration.

Test scenarios (see Figure 1) defined the following directions of attacks:

- from the Internet and over WAN with the use of unauthenticated and unauthorised measures by intruders;
- from the enterprise network, the attacks coming from authorised users of this network who, due to various reasons, attack the power control system;
- from the control network by persons who know the effects of the attacks and due to personal and/or external reasons conduct attacks on the infrastructure;
- from the control network by users who are not aware of the threats, authorised to resources (e.g. during a software update a malware is installed and transferred along with the useful software).

Conclusions

The positive results of the BIPSE validation allowed for its installation in the power station of the Polish Transmission System Operator PSE S.A. Exhaustive tests performed in real operating environment confirmed that BIPSE system meets all functional requirements. Its specific features like modular and scalable architecture, closed-loop reaction to detected threats, expanded engineering access control subsystem, and lack of negative impact on security and reliability of the protected object allows the system adaptation both to small and large-scale implementations. BIPSE system can be also adapted to other critical infrastructure environments, such as fuel or water supply systems.

The advanced concept of BIPSE system covers a trusted multi-domain cooperation when the domains share the identified threat information building a cybersecurity situational awareness picture of the power supply process.

References

[1] National Critical Infrastructure Protection Programme,

[2] Description of Project “Cyber security provision system for critical infrastructure”, project No. DOBR/0074/R/ID1/2012/03

[3] J. Jarmakiewicz, Development of Cyber Security Testbed for Critical Infrastructure, 2015 ICMCIS, IEEE Explore DOI:10.1109/ICMCIS.2015.7158686

[4] Laboratory of Distributed Generation – Institute of Electrical Power Engineering, Lodz University of Technology http://www.i15.p.lodz.pl/pl/pliki_htm/LGR.htm

CUIng: Criminal Use of Information Hiding Initiative

The goal of the Criminal Use of Information Hiding Initiative is to combine expertise and experience from academia, industry, law enforcement agencies and institutions to tackle the increased utilisation of information hiding techniques and prevent its wider diffusion.

Current malware is increasingly using various types of information hiding techniques (like steganography) to avoid detection and hide communication and (confidential) data exfiltration. This new trend is confirmed by the latest examples of malicious software with information hiding capabilities, e.g., *Hammertoss*, *Stegoloader*, *Regin* or *Duqu*. Information hiding has been utilised by cybercriminals but also other actors such as spies (e.g., the Russian spy ring discovered in the US in 2010) and terrorists (e.g., members of al Qaeda arrested in Berlin in 2012 were in possession of video files containing hidden information). Information hiding techniques have also been used by insiders to exfiltrate sensitive data.

„The creation of new narrow-focused initiatives like Criminal Use of Information Hiding (CUIng) allows to investigate and share threat intelligence on various cybersecurity aspects and to develop more effective solutions"

Considering the sophistication of the techniques found in the wild, the authors believe that there is an urgent need to act at EU-level. To this end, the **Criminal Use of Information Hiding (CUIng)** initiative was launched in cooperation with Europol's *European Cybercrime Centre* (EC3). Working jointly and combining expertise and experience from academia, industry, law enforcement agencies and institutions, the initiative aims to tackle the threat posed by the criminal use of information hiding techniques while it is still characterised by a limited adoption.

Main Objectives

The five main objectives of the proposed initiative are:

Raise Awareness: inform about the threat that information hiding techniques can pose. Especially: increase the sensitivity to cybercriminals' potential for information hiding exploitation (e.g., in companies) and emphasize how forensic investigations could become significantly more challenging in the presence of such techniques.

Track Progress: monitor sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists and other actor groups.

Share Threat Intelligence: bring together security professionals from government institutions, academia, law enforcement and industry to distribute information and share experience and expertise from different viewpoints

Work Jointly: cooperate and benefit from joint potentials to develop effective countermeasures and integrate them on a global scale (or at least EU level).

Educate & Train: ensure that law enforcement agencies, companies, institutions, individuals, etc., will be ready and fully prepared to react against potential cybercriminals' information hiding exploitation.

Benefits

Depending on the type of the partner involved in CUIng, various benefits can be identified:

For academia, the main benefits include more chances to support other partners in better understanding

Wojciech Mazurczyk [1]

is an Associate Professor at Warsaw University of Technology, Poland. He is a coordinator of CUIng.

wmazurczyk@tele.pw.edu.pl

Philipp Amann

is the Senior Strategic Analyst of the European Cybercrime Centre (EC3) and Head of the Strategy and Development team.

Philipp.Amann@europol.europa.eu

Luca Caviglione [1]

is a Researcher at the National Research Council of Italy.

luca.caviglione@ge.issia.cnr.it

Steffen Wendzel

is head of a research team at Fraunhofer FKIE, Bonn, Germany, and author of five books.

steffen.wendzel@fkie.fraunhofer.de

information hiding-based threats as well as taking part in the development of more effective countermeasures.

It also improves awareness of professionals and researchers. In addition, CUIng fosters the competetiveness of European researchers in this domain, for instance through media coverage, participation in significant events and relevant publications (books, special issues for journals, papers, etc.)

For industry, the main benefits are a better evaluation of related threats and risks, and the facilitation of new markets focusing on data leakage protection and anti-malware information-hiding-aware solutions. Eventually, this will lead to an improved protection of the sensitive business data.

Law enforcement agencies can take advantage by consulting and informing the public and other partners about the potential risks related to information hiding threats. They can become more aware on the evolution of such techniques and adjust their subject-matter specific knowledge for investigations and the work of digital forensic analysts.

For institutional partners, the key gain will be a better understanding of the threats and risks involved. This improved awareness should impact on product and tool selection, IT configuration and training activities. In addition, the improved know-how on protection against hidden data leakage will help to secure critical assets, including intellectual property.

CUIng Structure

The initiative welcomes all interested members from different backgrounds to participate in CUIng.

The structure of the initiative consists of the Steering Committee and regular members. The Steering Committee is responsible for setting the strategic direction of the initiative and proposing, approving and coordinating all its activities. The Steering Committee is a mix of members from academia, industry, LEAs and institutions. Currently, it is composed of seven members from Canada, Germany, Italy, Poland, The Netherlands, and the United Kingdom.

Current Activities

The initiative uses the Europol Platform for Experts' EC3 - SPACE as a place for collaboration, networking, planning future activities and sharing information. It will provide a common environment to express views and to discuss pertinent trends. It also provides an up-to-date repository of relevant reports, publications and documents on criminal use of information hiding techniques.

The initiative gathers and shares the following information:

- **General background on information hiding**: provide a general overview on the topic,
- **Scientific publications**: relevant papers (mostly surveys), which present the state-of-the-art in academic research in information hiding,
- **Information hiding-capable malware**: analyses of real-life malware that utilises information hiding techniques. Reports are mostly delivered by security professionals from anti-malware companies and share specific details on the modus operandi.

Members have been co-organising and taking part in various events (conferences and workshops) to promote the initiative and to attract potential new members. Recently, CUIng has been a program partner and will be presented at the 2016 eCRIME conference in Toronto, Canada, and at the 2016 DeepIntel conference in Schladming, Austria. Some past events that provided an opportunity to promote the initiative was mentioned include: “Emerging and Current Challenges in Cybercrime and Cyberterrorism" (March 2016, The Hague, Netherlands) and “Secure Europe without borders” (February 2016, Lodz, Poland).

CUIng also helped Europol's EC3 to create a CyberBit, a brief backgrounder for the Trends Series entitled “Steganography for increased malware stealth”. CyberBits are intelligence notifications on cyber-related topics that aim to bring important facts and findings to the attention of the cyber community in a timely manner to raise awareness and to trigger discussions or further actions.

The CUIng Community

The members of the initiative firmly believe that working together allows building a robust community taking advantage of expert knowledge and expertise from academia, industry, law enforcement and institutions. This network approach, leveraging different communities, should alleviate the problem of the criminal use of information hiding techniques before it becomes a widespread phenomenon.

If you would like to find out more about CUIng or become a member of the initiative, please visit our website at: **cuing.org** or email us at: **info@cuing.org**.

NASK's experiences with actionable information and threat intelligence

CERT Polska is a division of NASK that secures the .pl domain and Polish networks. Dealing with actionable information is our bread and butter, as we handle incidents reported by users of Polish Internet and threat intelligence from our contacts from all over the world. Utilising threat data feeds in our daily operations and projects gives us unique insight on usability of threat intelligence information available in the security community.

What is actionable information?

For an incident response team (CERT / CSIRT) actionable information is information on all aspects of network security incident that are relevant to the incident and its possible handling. It can be a list of IP-addresses, a dump of traffic captured between malware installed on an infected computer and its C&C server, a hash of a malware sample or the sample itself. In the modern world of network threats, the possibilities are endless. For the information to be actionable, though, it has to meet the following criteria: **relevance**, **timeliness**, **accuracy**, **completeness** and **digestibility**. Let us take a closer look at these attributes:

Relevance means that the information must be related to the attack and relevant for the receiving party (for example, response team's constituency). Information that is not a description of an incident is not considered as actionable. Description of an attack affecting someone on the other side of the globe is not actionable for a team tasked to protect a single organization (or any other well-defined constituency).

Timeliness affects relevance of the information. With the attacks being carried out in real time, most of their characteristics can change rapidly, making the old information irrelevant. For example, it is quite common for malware to switch C&C domains in quick succession.

Accuracy of the information is crucial (as we will show in the "Lessons learned" section). Errors in the data can lead to false positive detections when the data is used to detect threats, or can hinder the investigation of an incident.

Completeness of the information must be considered in the wider context of the data exchange. Leaving out something can make the information unusable, but it may be due to confidentiality rules, laws or agreements which can limit scope of the information to be shared. There is no rule of thumb of information completeness.

Digestibility means that the information needs to be in a form allowing it to be easily imported into organisation's information management systems, and then transformed, shared and/or used.

Our projects

Our experience comes from dealing with actionable information and threat intelligence in the course of following projects:

n6 platform

The n6 platform is the core of our operations. Its name is a wordplay on the Network Security Incidents Exchange acronym. The system is a threat intelligence and actionable information sharing platform developed by NASK. In 2015 it handled a record number of more than 200 million notifications of threats in Polish address space. The platform shares the data through an application programming interface (API) based on HTTPS and RESTful architecture. There is also a supplementary interface using STOMP protocol for streaming the data, minimising the delays that often occur when other methods of data exchange are employed.

Janusz A. Urbanowicz

Janusz A. Urbanowicz is a senior security projects specialist at NASK. Before that he built a commercial CERT, designed security featured in cloud
products and managed incident handling for a major Polish university.

He lately co authored a paper on cyber-attacks attribution:
"The Never-Ending Game of Cyberattack Attribution" with Piotr Kijewski, Przemek Jaroszewski and Jart Armin, and he is working on malware defense systems for the financial industry.

email: **Janusz.Urbanowicz@cert.pl**

Additionally, we have provided the users an ability of receiving periodic notifications when new information about their networks is available. The threat intelligence data stored in n6 platform comes from our research, from open data sources available on the Internet and from other organisations working with threat intelligence and actionable information.

ILLBuster

ILLBuster[10] is an another project based on utilising actionable information. The purpose of the project was to develop an automated system for detection and analysis of harmful websites. The project was developed by consortium led by Università degli studi di Cagliari and Università degli studi di Milano-Bicocca and thus the system operations are focused on the Italian Internet. The developed system detects suspicious domains using fast-flux detection technology and an automated crawler analyses the websites. The crawler detects advertisements of: sales of illegal goods, child pornography, phishing and malware. The ILLBuster system is both a producer and consumer of actionable information. It consumes n6 data about Italian networks and produces information as report of the analyses and detected suspicious domains which are reported back to the n6 platform.

FlowSense

FlowSense is a network threats detection software, operating on metadata only. FlowSense uses open source Argus[11] engine to analyse network traffic to extract flow information, then correlates it with threat intelligence from the n6 platform. The FlowSense solution gave us most experience with using threat intelligence in the real world.

Lessons learned

In our work with threat intelligence feeds we utilise them from various sources of information from all over the world. These sources are usually feeds of data coming from automatic analysis of malware or spam, by registered connections to sinkhole systems and found by other means that are sometimes not publicly disclosed. While the data from sinkhole systems are reliable, other means of creating feeds often could be not reliable enough.

As an example, we have received reports of phishing pages, that indicated real bank websites. We do not know how it was determined that the page hosts a phishing website. We may hypothesise that this is a false positive from an automated system that determined falsely that the actual bank page is a phishing page targeted at the bank.

Such cases stress out that there is a strong need to verify that the incident report is accurate. The verification method should be automatic, since it allows for processing the massive amounts of automatic threat reports. It is, however, the fallibility of automatic reporting and verification that is the reason for the need for verification, creating a chicken and egg problem.

Another danger comes from interaction of data enrichment process with social network design patterns. Social networking platforms commonly use URL shorteners to keep track of users clicking URL addresses shared as social content. As malicious URL-s are also shared through social media, and as a result of this processing often reported in shortened form, it associates the domain name of URL shortening service with malicious content. This leads us to assumption, that data enrichment procedures often do not follow the reported links to establish the real malicious URL.

Another pitfall lies in the data enrichment process. Our n6 platform routinely adds metadata to reported URL-s and IP addresses. For example, if the URL redirector or shortener is operated by a social network, its domain name resolves to its operator IP address range, usually serving the whole infrastructure, and not only the shortener. If this IP-address is then stored along the URL and used in malicious IP-addresses blacklist, chance is, any connection to a social network infrastructure will be marked as suspicious or blocked. Real life example is that supplanting a goo.gl shortened URL with the domain name IP-address will lead to marking at least some connections to Google services as connections to a malicious IP-address. This kind of false positive is created by automatic data enrichment without taking account of nature of the data item.

Another trouble lies in threat intelligence concerning malicious pages. Our research especially during the ILLBuster and earlier HSN/HSN2 projects shows that it is practically impossible to automatically and reliably determine if a URL is used to infect visitors with malware. While HSN/HSN2 is able to detect some common web exploits, most available automatic detection tools require a knowledgeable human operator to guide the analysis and interpret the results, especially as modern exploit kits employ various strategies in order to defeat automatic analysis. One such technique employed by exploit kit operators is to set DNS records for a domain which was used for nefarious purposes so it resolves to an invalid IP-address when no longer needed, for example to 0.0.0.0, or to an address within a private address space, making analysis of the malicious content previously hosted on that domain impossible and sabotaging the workings of automatic analysis tools.

Other exploit kit tricks include leading the victim’s browser through a maze of ever-changing redirections, setting cookies and blacklisting importunate IP-addresses that are used by the analysts to crack the workings of an exploit kit. In practice, it takes a sizable amount of an analyst’s work (measured in days) to trigger the exploit kit to take a malware shot at the analyst’s browser.

Those experiences led to implementation of “confidence” metrics in our n6 platform. Users of the platform can select confidence level of the source when querying the platform for data, to avoid false positives and low-quality automatic feeds data. The confidence score is (high, low or medium) is assigned due to observed quality of data coming from a given source.

Standards are great, there are so many of them to choose from

An apex of our work with actionable information was development, on commission from European Network Security Agency, a set of guides for utilizing actionable information in

[10] For more information about ILLBuster project visit http://illbuster-project.eu/

[11] http://qosient.com/argus/

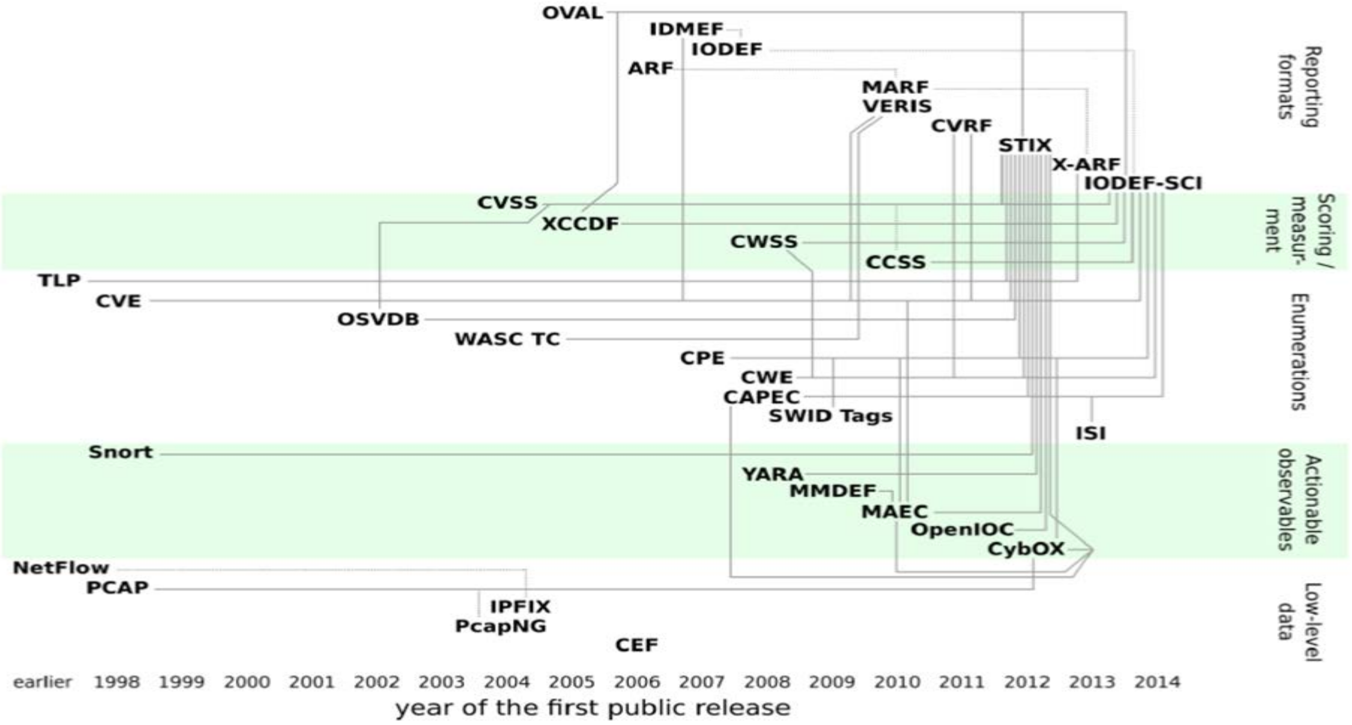


Figure 1 - Relationship and development tree of actionable information standards. Source: "Standards and tools for exchange and processing of actionable information", ENISA, 2014

CSIRT operations. We have catalogued 36 formats and standards for dealing with various aspects of actionable information. This abundance makes it quite complex to determine which formats and standards should be used [12] . The complexity we discovered while researching the formats and standards is presented as Figure 1, and new formats were introduced only after we finished the research.

Conclusion

Threat intelligence and actionable information sharing are one of the most important aspects of fighting Internet threats, as no single actor can secure the whole Internet. At NASK we developed significant capability in dealing with actionable information – our n6 platform distributes relevant actionable information to Polish network operators, and is free to access if you are one. Yet is not trivial both to create and consume actionable information and from our experiences it is a dangerous thing to rely on received actionable information only to detect and block internet threats. Further research on ensuring its quality and validity is needed.

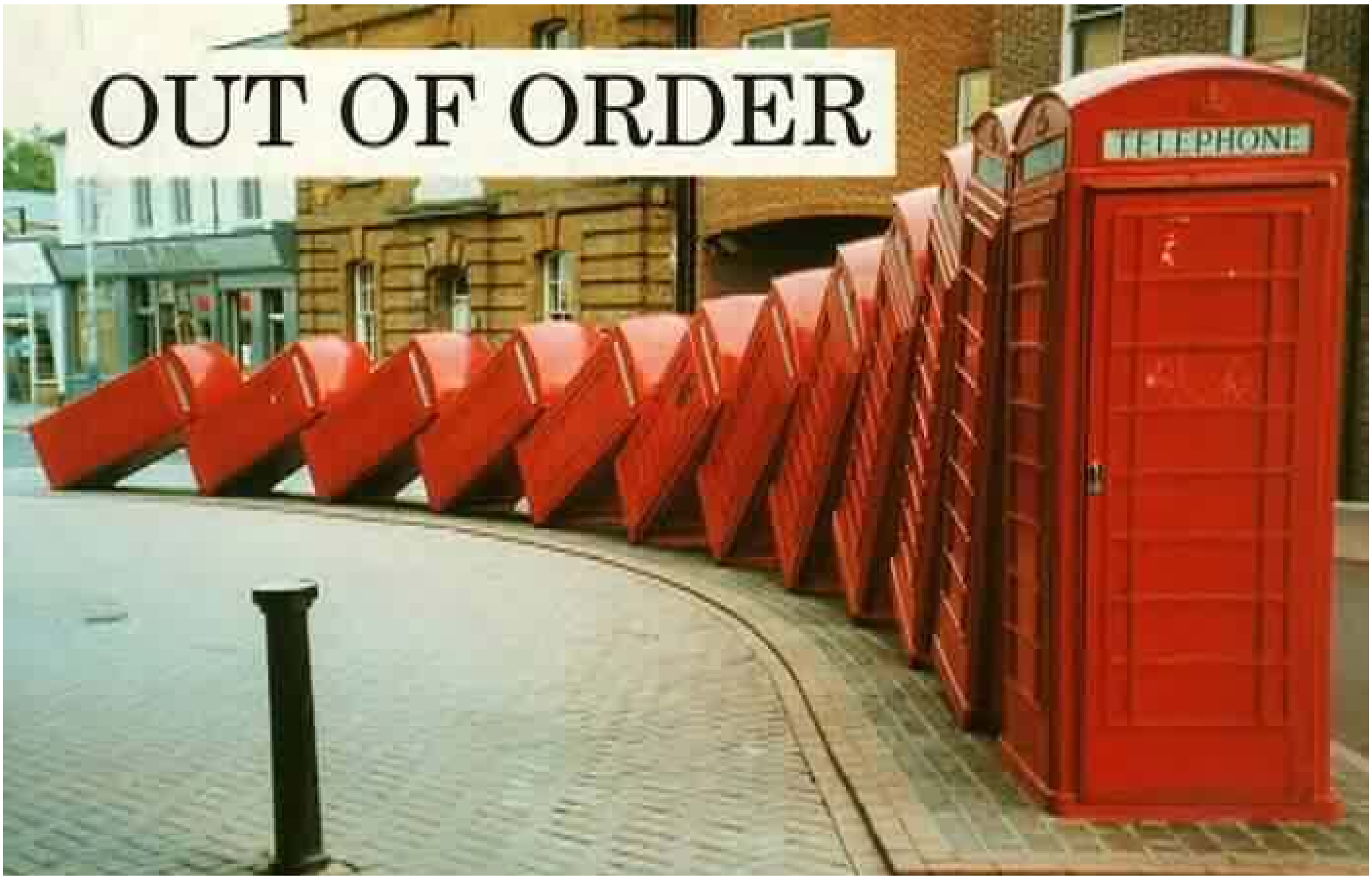
[12] For the full set of ENISA actionable information guides, see https://www.enisa.europa.eu/news/enisa-news/new-guide-by-enisa-actionable-information-for-security-incident-response

Joint final conference of projects on cascading CI Effects

CASCEFF, CIPRNet, FORTRESS, PREDICT, SNOWBALL

March 16 and 17, 2017

save the date



The **joint final conference** place t.b.d on the **16th of March** 2017 (full day) and in the morning of **17th of March** 2017 (1,5 days)

In the **afternoon of the 17th of March** a kind of **joint wrap-up session** is held together with **Joint Research Centre's (JRC) Disaster Risk Management Knowledge Centre (DRMKC)** event. This will be a summary session where main conclusions of both events will be presented to Policy DG representatives and inviting them to react from a policy viewpoint.

Follow on

www.ciprnet.eu

All-Hazard Training

How to exploit sophisticated simulation environment to improve the training to manage complex crisis situation: the experience of the students of the Master in Homeland Security (Italy) using the 'what-if' analysis tool of EU project CIPRNet

There is no doubt that the security of a country is measured also by its capacity to prevent, counter and recover from a catastrophic event. Natural disasters, social tensions and the upsurge of criminality and terrorism constitute threats that can seriously undermine the social, political and economic development of a country. Such threats must be analysed recognising that their targets, CI especially, are part of a system that is itself intertwined with other systems. This is why it is crucial for security experts from both private and public sectors to approach security in a holistic manner, as this will in fact preserve the country's overall development and prosperity.

Today, citizens demand and are rightfully entitled to higher security standards. It is therefore in the interest of every nation to ensure that governmental institutions and private companies, whose services are deemed essential to citizens, acquire all the necessary tools to win these new fights.

Throughout the world, in recent years, we have witnessed criminal or terrorist attacks that have had a high impact on the media and the population. People's perception of safety and security have been badly shaken. However, even though such events have had the capacity to frighten the population and feed a strong sense of mistrust towards the institutions that are responsible for its protection, a whole new type of threats, much more insidious and damaging, has recently emerged. In fact, we are facing new phenomena such as cyber-attacks to state institutions and infrastructures (e.g. the cyber-attacks to Estonia in 2007), disclosure of strategic military or diplomatic information (e.g. The Snowden case in 2013), personal identity and personal data thefts, industrial espionage and technology theft.

International concern is growing. This led some international organisations to take concrete action. NATO, at the recent Wales Summit, decided to strengthen its cyber defences and further engage with Industry; the NATO Communications and Information Agency was assigned this responsibility. Similarly, in July 2016 the EU adopted the first EU-wide legislation on cyber-security in the form of the Directive on Security of Network and Information Systems.

The Master's Degree in "Homeland Security – Systems, Methods and Tools for Security and Crisis Management" of Campus Biomedico University in Rome, is the programme of choice to learn about a country's major security threats, vulnerabilities and risks to CI and to identify and implement adequate safeguards and countermeasures. The programme, which combines theory and real-life cases including in international environments, also illustrates a number of

How does a company or a state actually meet citizens' high expectations for safety, security and business continuity? How can CI be duly protected in order to prevent any damaging incidents, mitigate the consequences when they do happen and allow business to resume as soon as possible? What does "security" mean for a country's CI.

To understand how to manage a crisis before, during and after a so-called

Carlotta Maraschi

is actually Assistant Security Manager at Ferrovie dello Stato Italiane

Anthony Testa

Anthony works at NATO Communications and Information Agency located in Mons, Belgium. He is Head of the Staff Management Office and Chief of the Front Office of his Service Line

A moment of the exercise

“catastrophic event”, particularly when it is caused by malicious behaviour, it is necessary to reduce the risks to an acceptable level.

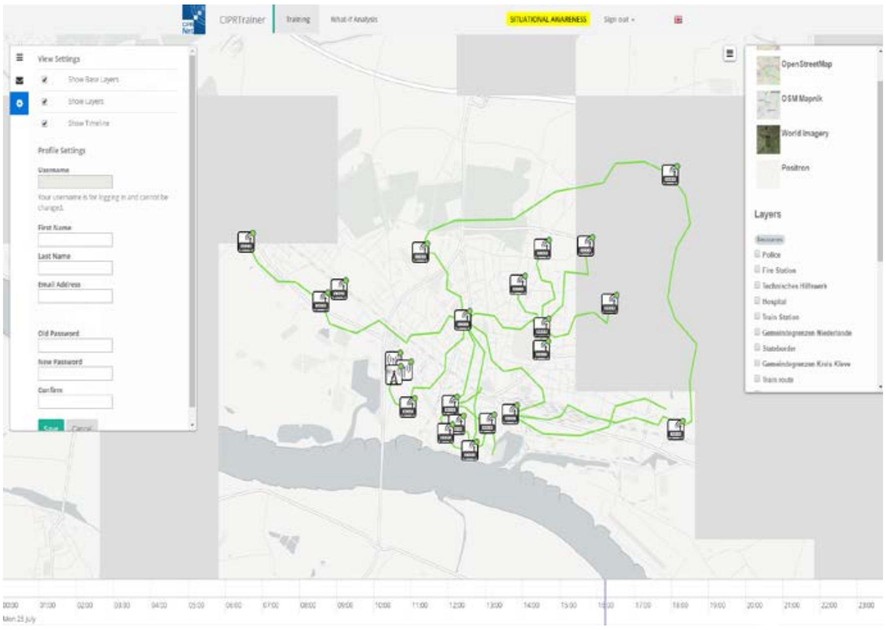
The US federal government has implemented “The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard” which states that "Risk is a function of the values of threat, consequence, and vulnerability. The objective of risk management is to create a level of protection that mitigates vulnerabilities to threats and the potential consequences, thereby reducing risk to an acceptable level”.

The CIPRNet what-if analysis tool

One of the highlights of the programme was the two-day seminar organised by the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) on how to plan for and manage catastrophic events affecting CI.

It is worth noting that a catastrophic event affecting critical infrastructure (i.e. assets such as energy, transport, telecommunications, health and financial services) together with the management of its consequences may provoke a phenomenon called domino effect, whereby the damages of the attacked infrastructure cause the malfunction of other critical infrastructure, thus negatively affectting other systems and possibly the whole country.

During the CIPRNet seminar we had the chance to experience exactly this: what could be the consequences of poor management following a catastrophic event. The Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS presented a disaster simulator prototype. Through this simulator we were able to analyse the case study regarding an industrial accident in Germany, and a flooding scenario in the Netherlands. We were able to observe the “domino effect” of the decisions taken during the crisis. It was a real eye opener! We could witness how a series of events, poor judgement and ineffective countermeasures could bring the whole operating system of a country to its knees, causing an incredible cascade of costly and damaging delays and inefficiencies.



CIPRNet What-if Analysis tools interface

The relevance of the Human Factor

The availability and efficiency of a country’s critical infrastructure is very much dependent on the competence of security experts. In fact, as natural disasters or catastrophic events caused by men can happen any time, it is essential that such security experts maintain high situation awareness, adopt creative and effective solutions and, last but not least, train and exercise regularly. The Master of Homeland Security, Campus Biomedico University in Rome, promotes this approach, provides an excellent way to keep abreast of modern methodologies and tools in the area of protection of CI and combines academic perspectives with pragmatic, real-life experience. It also provides an in-depth assessment of the importance of business continuity planning while defending the reputation of the firm, preserving the morale of the population and strengthening the resilience and resolve of the country.

For more info

See: www.ciprnet.eu

Master in Homeland Security
January-December 2017 – Rome (Italy)
www.MasterHomelandSecurity.eu

Links

ECN home page	www.ciprnet.eu	
ECN registration page	www.ciip-newsletter.org	Please register free of charge
CIPedia©	www.cipedia.eu	the new CIP reference point

Forthcoming conferences and workshops

Master in Homeland Security	www.MasterHomelandSecurity.eu	January 2017

Institutions

Cert of Poland	https://www.cert.pl/en
National and European Information Sharing & Alerting System	www.neisas.eu
European Organisation for Security	www.eos.ecom
Netonets organisation	www.netonets.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu
Criminal use of information Hiding	http://cuing.org
EU DG Home: Cyber-Physical attacks analysis against ICS (FACIES)	http://facies.dia.uniroma3.it
ILLBuster project	http://illbuster-project.eu
International crises exercise in NL	https://english.nctv.nl/current_topics/news/2016/SuccessfulinternationalexerciseVITEX.aspx
Poland Telco Security	https://pl.asseco.com/en/sectors/public-institutions/bipse-security-of-the-teleinformatic-system-374
FP 7 Smart Mature Resilience for Cities (SMR) EU Project	http://smr-project.eu/home
FP 7 SECURity at the network Edge (SECURED)	www.secured-fp7.eu
FP 7 Secures the smart grid of tomorrow	www.segrid.eu
Smart Mature Resilience project	http://smr-project.eu/home
Situation Aware Security Operation Centre (SAWSOC)	http://www.sawsoc.eu
FP 7 Weather CIP risk management and protection	www.intact-project.eu

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" In this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security	https://resilience.enisa.europa.eu/nis-platform
Polish National CIP Programme	http://rcb.gov.pl/en/critical-infrastructure/
Platform Current policy debates	http://digitalwatch.giplatform.org
GFCE-MERIDIAN Good Practice Guide on CIIP	https://www.tno.nl/gpciip/

Websites of Contributors

Acris	www.acris.ch
NASK Research Institute of Poland's Ministry of Digitisation	https://www.nask.pl
Campus Bio-Medico di Roma	www.unicampus.it
EC Joint Research Centre	https://ec.europa.eu/jrc
Europol	https://epe.europol.europa.eu
Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS	www.iais.fraunhofer.de
Wydział Elektroniki i Technik Informacyjnych PW	https://secure.tele.pw.edu.pl
Ministry of Justice Netherland	www.rijksoverheid.nl/ministeries/ministerie-van-veiligheid-en-justitie
TNO	www.tno.nl/en/
Royal Roads Canada	www.royalroads.ca/
United Nations Interregional Crime and Justice Research Institute (UNICRI)	www.unicri.it
Università degli Studi di Napoli Federico II	www.international.unina.it
UNIVERSITA' DEGLI STUDI ROMA TRE	http://uniroma3.it
Uniwersytet Technologiczno – Przyrodniczy	http://utp.edu.pl/en
H2020	http://ec.europa.eu/programmes/horizon2020

www.cipedia.eu

Let’s grow CIPedia©

An online community service by the CIPRNet Project.

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

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

> Within two years, CIPedia© reached 440,000 total views, at a current average of 450 views per day.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardisation, 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**.

> Your contribution is essential for putting value in the CIPedia© effort.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

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

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

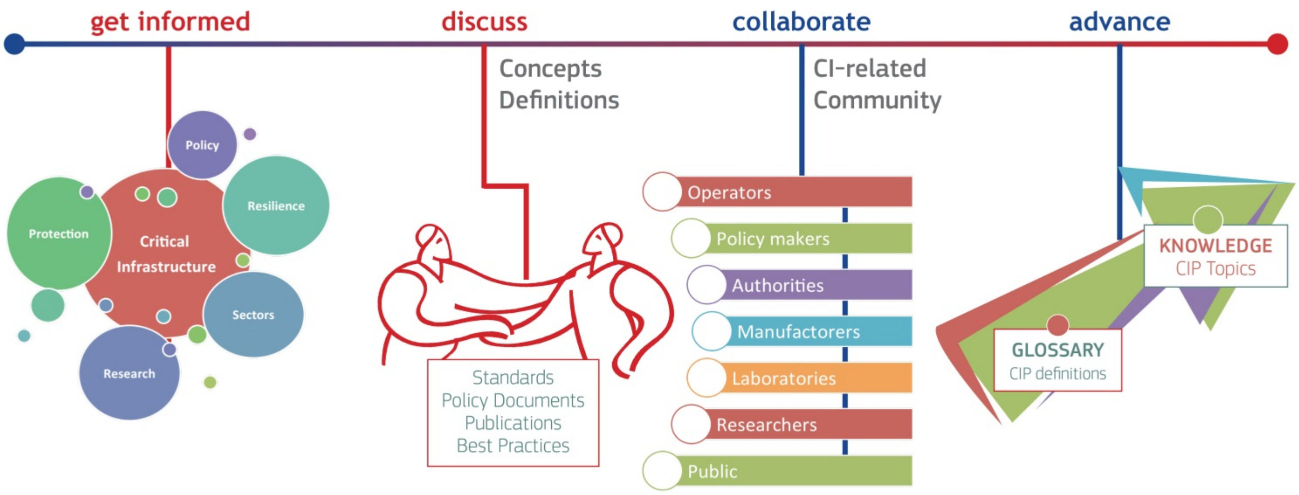
marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

✓ Add definitions and references!
✓ Create a new topic!
✓ Start a discussion!
✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.



European CIIP Newsletter

March - June 2017, Volume 11, Number 1

Industrial Control System (ICS) Security Focus

ECN

Contents

CIPR Net

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

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Editorial

European and Global Activities

Country Specific Issues

Method and Models

Method and Models

Ads of upcoming Conferences and Workshops

Links

Media on C(I)IP

Towards a European Infrastructure Simulation and Analysis Centre (2E!SAC), CIPRNet Completed

Looking back to our mission with CIPRNet and inspiring with some thoughts for the future

CIPRNet project ends February 28, 2017, a good opportunity to look back at how it started: In 2010 at the Centre for European Policy studies, I chaired the taskforce “Critical Infrastructure Protection in the EU”. CIPRNet coordinator Erich Rome, whom I knew from being a part of the EU project “Integrated Risk Reduction of Information-based Infrastructure Systems” www.irriis.org, was invited to a session for postulating a European Infrastructure Simulation and Analysis Centre in analogy to the NISAC in the USA. This vision still connects us with many other friends, which would like to see Europe taking more responsibility in this direction.

Erich Rome guided our CIPRNet team with superior seniority and reached significant advances by implementing the vision of the network of excellence CIPRNet: new capabilities for CIP stakeholders, dissemination and training activities that made CIPRNet highly visible in the communities, and a high degree of integration amongst partners. The team is now an interlinked network of friends pushing the resilience of vital infrastructure resilience in the EU. The recently founded association for fostering vital infrastructure resilience in Europe (2E!SAC) shall sustain the promotion of EISAC and we hope for further advances. Each one of us feels, that times are changing and we need more in-depth knowledge of our infrastructure and prediction how the CI behaviour and disaster consequences would be assuming different scenarios. CIPRNet could deliver two new applications built on top of earlier proofs of concept: advanced decision support and ‘what if’ analysis for exploring different courses of crisis management actions.

The consequent promotion of the CRITIS topic in the young scientist community, including them also in the boards of the conference developed its fruits. The last competition of the CIPRNet Young CRITIS Award (CYCA) in Paris had 17 registration of researchers below 32 years. This promotion will continue as Young CRITIS Award (YCA) at the 12th CRITIS Conference in Lucca, Italy. Somewhat less obvious was the work we did with respect to gender balance. Although our community is still dominated by men, a considerable number of women from different European countries were invited to contribute to the success of CIPRNet: not only as researches but also as keynote speakers, chairs to CRITIS conferences and members of CIPRNet’s International Advisory Board. The CYCA competition had two male and two female winners, the ideal balance. And finally, the ECN contributions came out gender balanced in a natural way. We consider such balancing strategies an important element of capacity building, which will make our community richer and more powerful in the long run.

Looking into the future our challenge for resilient infrastructure will most likely grow: The upcoming digitization using the Internet of Things and connecting SCADA and ICS to the Net are pending issues with a lot of research needs. We are proud that CYCA co-winner TingTing Li shares her work in this issue. Also in this issue is a large share of articles developing the SCADA / ICS challenge: society’s most essential systems are vulnerable and protection is not completely feasible. This means that we have to develop resilience, which fine-tunes the three domains protection, detection and reaction in a balanced way. Raising reaction, crisis management is a central part of reaction, and we are proud on Amélie Grangeat the CYCA co-winner 2016 presenting results for this domain.

In general, all Member States are somehow short on money and have limited political will to invest a lot into infrastructure. More security would mean higher costs, which turns into higher infrastructure usage fees: a message, which is difficult to sell, and impossible to win elections. As professors we know that motivations for learning are simplistic: avoiding pain, gaining advantage and very seldom intrinsic joy. But mostly we learn through pain. In case of CRITICAL

Continued next page ...

Javier Lopez

Prof. Javier Lopez is Full Professor in the Computer Science Department at the University of Malaga, and Head of the NICS Lab. He is Co-Editor in Chief of IJIS journal and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.

e-mail: jlm@lcc.uma.es

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

Infrastructure this means painful outages and failures that produces sufficient power to change the conditions towards more resilience. In between we focus on little incremental steps and work on a readiness with experts, ideas, concepts to be ready, when more engagement is wanted.
Please look at six focus topics of **12th edition of the CRITIS conference** in October 2017 in Lucca, Italy. Please prepare your submissions no later than June 5 for submission. see: www.critis2017.org.

We thank Javier Lopez, co-editor for his brilliant support for this issue and for all his engagement within CRITIS Conference Series.

We thank all contributors of the newsletter, of projects related to CIP and Crises Management for their work and their contributions, especially those who wrote in the ECN.

Enjoy reading this issue of ECN!

Bernhard M. Hämmerli on behalf of CIPRNet work package ECN

CRITIS 2017

12th International Conference on
Critical Information Infrastructures Security
October 9–13, 2016, Lucca, Italy

Call for Paper open until June 2nd, 2017, see

www.critis2017.org

Young CRITIS Award

www.critis2017.org/young-critis-award

If you are less than 32 years and you contribute,
You may win extra money: Please apply!

CIP/CIR Community Services offered by CIPRNet's Virtual Centre of Competence & Expertise in CIP

The CIPRNet project has established a Virtual Centre of Competence & Expertise in Critical Infrastructure Protection, offering a variety of services to the multi-community of stakeholders and researchers in Critical Infrastructure Protection and Resilience (CIP/CIR).

The EU FP7 Network of Excellence project CIPRNet has bundled its services to the CIP/CIR community in a Virtual Centre of Competence & Expertise in CIP (VCCC). The VCCC services include CIP/CIR knowledge sharing, demonstrations of new technical capabilities, an e-Learning platform, and access to CIPedia©, a very popular online glossary of CIP/CIR terms. The VCCC services can be accessed via CIPRNet's website. Moreover, most of the VCCC services will be kept active beyond the end of CIPRNet.

One of the major objectives of CIPRNet was to lay the foundation for a long-lasting centre of competence and expertise in Critical Infrastructure Protection (CIP), the ***European Infrastructures Simulation & Analysis Centre*** (**EISAC**). The CIPRNet consortium knew that implementing EISAC is a process that would take longer than the project's lifetime. Therefore, CIPRNet planned starting this process by creating the VCCC during the project term.

Many of CIPRNet's activities in research and technological development (RTD), training, and dissemination resulted in service offerings. These offerings are tailored to CIPRNet's audience: CI operators, CIP/-CIR policy-makers, and R&D community [1]. In this article, we describe which services are provided by the VCCC.

Service groups

CIPRNet uses a service framework consisting of a set of service groups for describing the VCCC's offerings to the CIP/CIR community. VCCC services include training and dissemination activities, web-based repositories (like a database of CIP related research projects), facilities like CIPedia©, and demonstration services of CIPRNet's new capabilities.

Service group Advanced Decision Support

This service group refers to the two new technological capabilities that CIPRNet has produced:

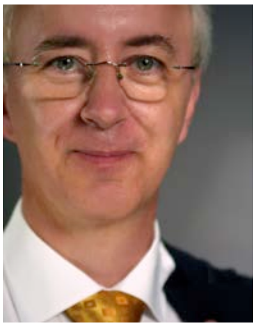
- **CIPCast**, a **Decision Support System**, aimed at supporting CI operators and civil protection agencies [2][5][9].
- **CIPRTrainer**, a training system that enables performing **'what if' analysis** in complex simulated crisis scenarios for exploring different courses of action and using consequence analysis [6][7]. Its target audience are crisis managers at the operational-tactical level of civil protection.

> Aiming at a sustained operation of the VCCC, CIPRNet members will keep most of the services active beyond the end of the project.

Capability related services that remain active beyond CIPRNet are the web demonstration services of CIPRTrainer (Figure 1) and CIPCast (Figure 3), both accessible via the VCCC web portal: http://www.ciprnet.eu/315.html

Service group Training

This group of services comprised training events such as CIPRNet courses, Master Classes, and lectures offered during the term of CIPRNet.
CIPRNet has issued a textbook [4] on the training material developed for the training events.



Erich Rome

...is a senior researcher at Fraunhofer IAIS and the coordinator of CIPRNet.

e-mail: erich.rome@iais.fraunhofer.de

Eric Luiijf

...is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO and an expert in C(I)IP. He leads the VCCC activities.

e-mail: eric.luiijf@tno.nl

Vittorio Rosato

...is head of the Analysis and Protection of Critical Infrastructures Lab at the ENEA Casaccia Research Centre. ENEA provides several VCCC services.

e-mail: vittorio.rosato@enea.it

A web service that remains active beyond CIPRNet is its MOOC (Massive Open Online Courses) CIP/CIR e-learning courseware. It contains parts of the CIPRNet training material, video recorded lectures, and sets of multiple-choice questions. The MOOC platform is directly accessible via this URL:
http://www.security-learning.eu

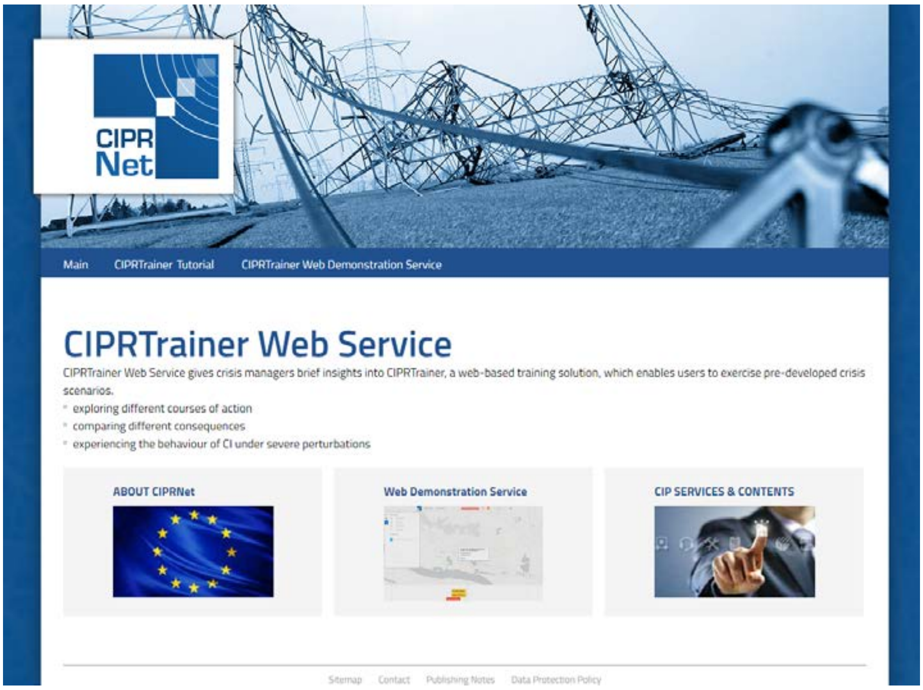
Service group Information Brokerage on CIP/CIR

This service group refers to glossaries, repositories, and databases related to CIP/CIR that are offered as CIP/CIR community services. Accessible services are:

- "Ask the Expert"
- CIPedia©.

"Ask the Expert" [8] is a knowledge brokering service. Users may use the web-based service for asking CIP related questions. Registered (CIPRNet) experts whose area of expertise matches the question are automatically asked to answer the question.

CIPedia© is probably one of the two most successful outcomes of CIPRNet. This Wikipedia-like online glossary of CIP/CIR related terms and definitions has received about half a million views with a daily average of about 475 views. CIPRNet partners made a massive effort for making CIPedia© address the international dimension of CIP/CIR by adding definitions from almost 100 different nations and in more than 40 different languages. This community service will sustain, kept alive by a multi-disciplinary community. Besides CIPRNet, the EU H2020 project RESIN (resin-cities.eu) has made contributions to CIPedia©.
The link to CIPedia© is also included in the VCCC web portal services page. CIPedia© is directly accessible via:
http://www.cipedia.eu



CIPRTrainer Web Service

CIPRTrainer Web Service gives crisis managers brief insights into CIPRTrainer, a web-based training solution, which enables users to exercise pre-developed crisis scenarios.

- exploring different courses of action
- comparing different consequences
- experiencing the behaviour of CI under severe perturbations

Figure 1: CIPRTrainer web demonstration services.

Service group Research Platform for CIP/CIR Collaboration

This service group bundles CIPRNet repositories and activities related to research and technological development (RTD). **Repositories** accessible via the VCCC web portal Research Platform include:

- a CIP EU **research project list**,
- a CIP/CIR **bibliography**, and
- an initial CIP MS&A **benchmark reference set**.

The latter contains a full scenario containing artificial CI data and threat models, including dependencies and cascading relationships. It is meant as a benchmark reference set for CIP Modelling, Simulation & Analysis (MS&A).
The elements of this service group are directly accessible via the VCCC web portal:
http://www.ciprnet.eu/315.html

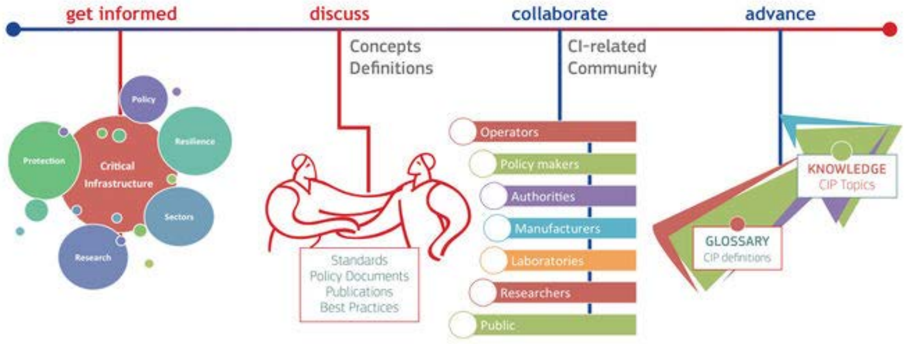


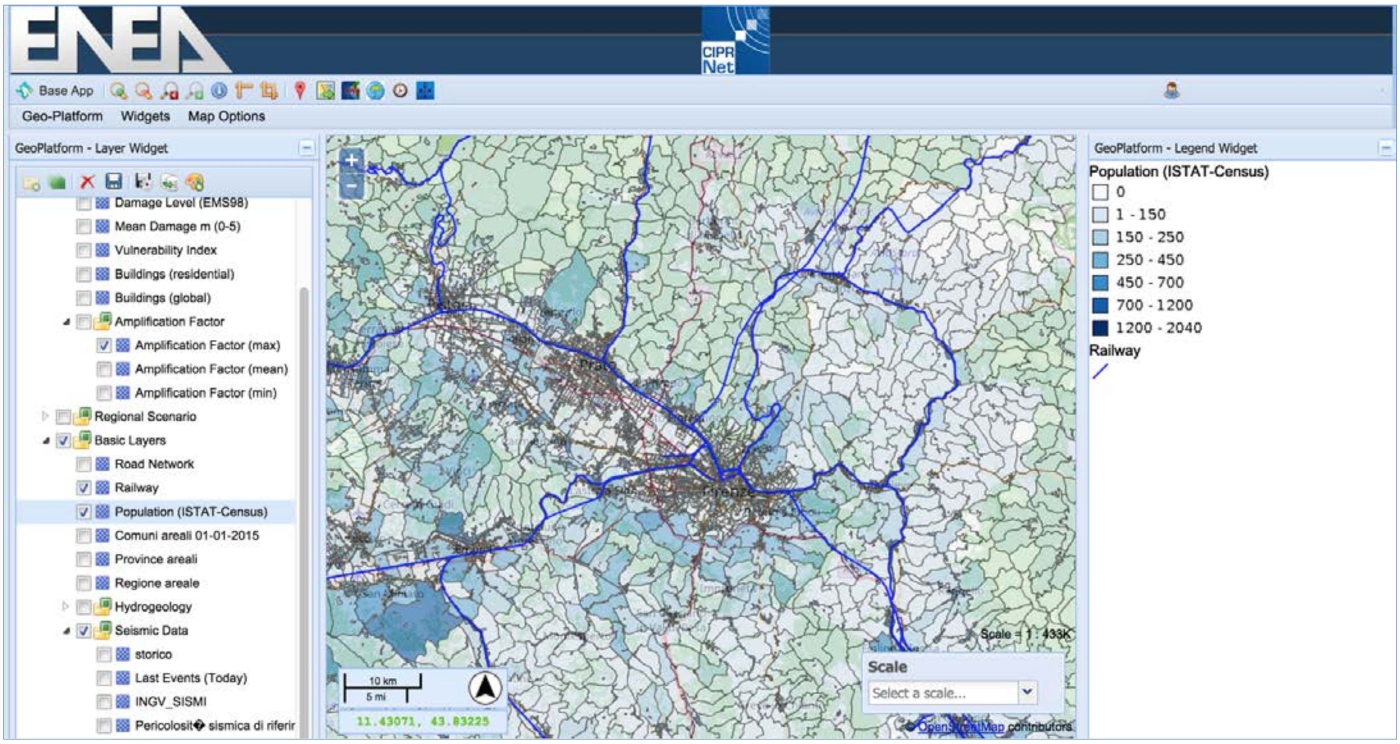
Figure 2: CIPedia© as a community service

Service group Dissemination

This group of services comprises the support of CIP/CIR related **conferences** like CRITIS, netonets, TIEMS, and the ESReDA seminars (see "More Information" at the end of this article), the **European CIIP Newsletter ECN**, the CIPRNet **publications**, the CIPRNet **deliverables**, and a **list of CIP/CIR conferences** on CIPedia©.
After the end of CIPRNet, CIPRNet's public pages on publications and deliverables will go into archival status. The links to these pages are:
https://www.ciprnet.eu/refereed-publications.html
https://www.ciprnet.eu/deliverables.html
CIPRNet partners will remain active in supporting CIP/CIR related conferences. The continuation of the ECN depends on the availability of continued funding (sponsors are welcome!). Visit the ECN (European CIIP Newsletter) home page, which includes an archive of all previous issues:
http://ciprnet.eu/ecn.html

Conclusion and Outlook

The VCCC is the end-result of CIPRNet in terms of services. Some of the established CIPRNet services, hosted by different partners, will be maintained and continued after the end of the CIPRNet project. Other advancements will not be maintained lacking time and funding; these will be made



□ Damage Level (EMS98)
□ Mean Damage m (0-5)
□ Vulnerability Index
□ Buildings (residential)
□ Buildings (global)
□ Amplification Factor
☑ Amplification Factor (max)
□ Amplification Factor (mean)
□ Amplification Factor (min)
□ Regional Scenario
☑ Basic Layers
□ Road Network
☑ Railway
☑ Population (ISTAT-Census)
□ Comuni areali 01-01-2015
□ Province areali
□ Regione areale
□ Hydrogeology
☑ Seismic Data
□ storico
□ Last Events (Today)
□ INGV_SISMI
□ Pericolosit� sismica di riferir

Population (ISTAT-Census)
□ 0
□ 1 - 150
□ 150 - 250
□ 250 - 450
□ 450 - 700
□ 700 - 1200
□ 1200 - 2040
Railway

Figure 3: Screenshot of CIPCast-IT, a web service demonstrating the new capability of advanced decision support for coping with CI related emergencies and disasters

visible in the VCCC's CIPRNet archive section. Several CIPRNet members and one external partner founded the German association 2E!SAC ("Verein" – association with international members by German law) to have a formal frame for continuing the CIP/CIR activities and services towards establishing and sustaining CIP/CIR competence centres in several European nations and at the EU level. Enquiries regarding this association could be sent to the authors of this article. Check out the VCCC services, contribute to CIPedia©, and let us know your ideas.

References

[1] Kozik R., Choras M., Flizikowski A., Theocharidou M., Rosato V., Rome E., "Advanced services for critical infrastructures protection". Journal of Ambient Intelligence and Humanized Computing, Springer Berlin Heidelberg, ISSN 1868-5137, December 2015, Volume 6, Issue 6, p. 783-795, http://dx.doi.org/10.1007/s12652-015-0283-x.

[2] Di Pietro A., La Porta L., Pollino M., Rosato V., Tofani A., Martí J.R., Romani C., "A Decision Support System for Emergency Management of Critical Infrastructures subjected to Natural Hazards," in conference proceedings Critical Information Infrastructures Security,

[3] 9th International Workshop (CRITIS2014), Berlin, LNCS vol. 8985, Springer, Heidelberg, 2016, pp. 362-367.

[4] Setola R., Rosato V., Kyriakides E., Rome E. (Eds.), "Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach", Series: Studies in Systems, Decision and Control, Vol. 90, Springer, ISBN 978-3-319-51042-2, 2017.

[5] Di Pietro A., Lavalle L., La Porta L., Pollino M., Tofani A., Rosato, V., "Design of DSS for Supporting Preparedness to and Management of Anomalous Situations in Complex Scenarios". In: [4]

[6] Rome E., Doll Th., Rilling S., Sojeva B., Voß N., Xie J., "The Use of What-If Analysis to Improve the Management of Crisis Situations". In: **Fehler! Verweisquelle konnte nicht gefunden werden.**

[7] Rome E., Xie J., Sojeva, B.: "CIPR-Trainer – simulation-based »what if« analysis for exploring different courses of action in crisis management." ECN 24 (vol 10, no 2), 2016.

[8] The CIPRNet Team: "ATE: A virtual Competence Centre in Critical Infrastructure Preparedness and Resilience." ECN 23 (vol 10, no 1), 2016.

[9] Tofani A., De Nicola A., Di Pietro A., Pollino M., La Porta L.: "Data management and Information sharing in CIPRNet DSS." ECN 19 (vol 8, no 2), 2014.

Disclaimer and Acknowledgement

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

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

The authors gratefully acknowledge the contributions of the entire CIPRNet project team!

More information

If you would like to find out more about the CIPRNet project, then please visit the project's website at

http://www.ciprnet.eu

and check the "Services" page.

Check out CIPedia©, CIPRNet's popular online glossary of CIP related terms at

http://www.cipedia.eu

Visit the ECN (European CIIP Newsletter) home page, which includes an archive of all previous issues: http://ciprnet.eu/ecn.html

Links to conference and seminars supported by CIPRNet

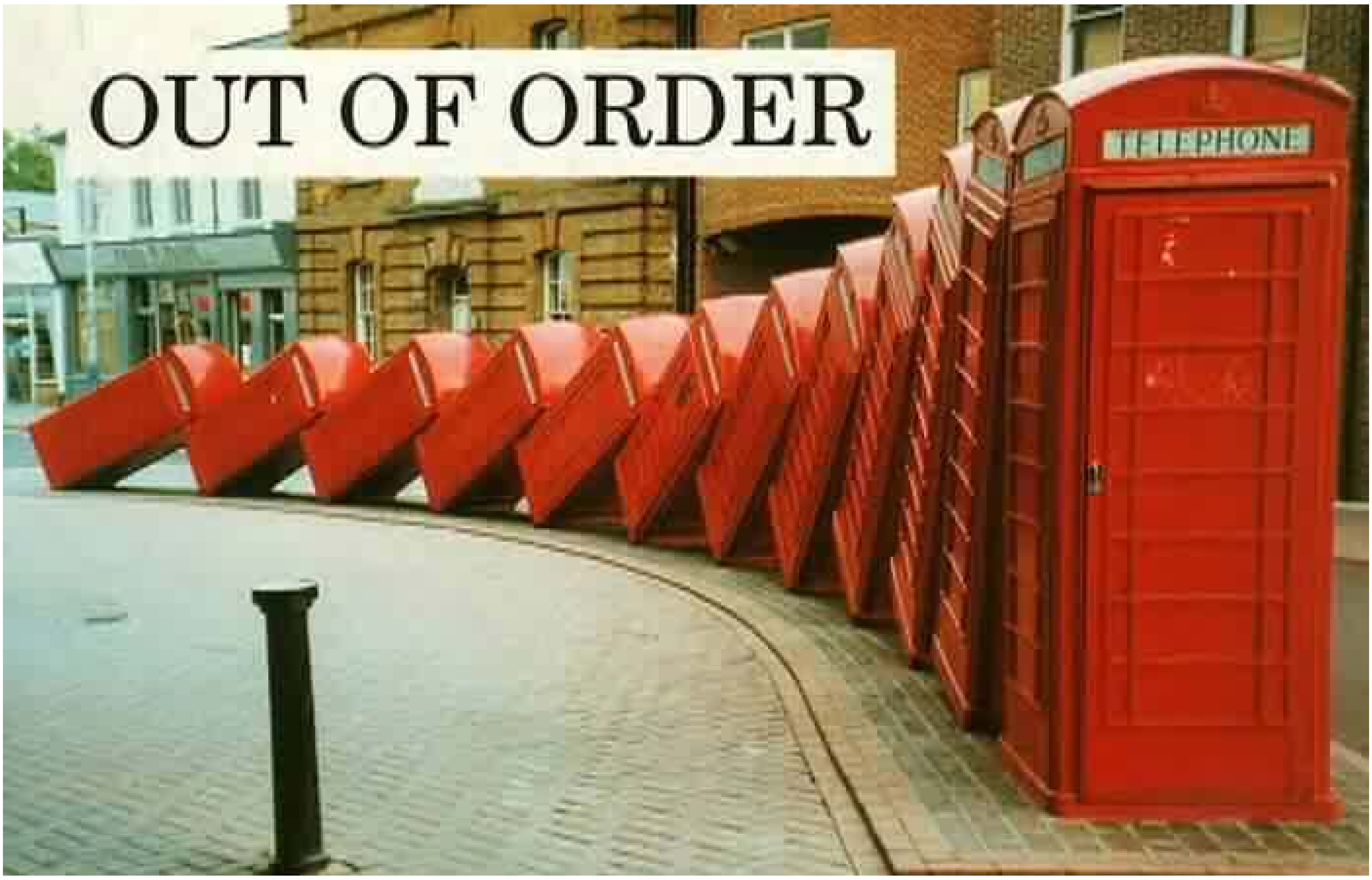
CRITIS	http://www.critis2016.org
netonets	http://www.netonets.org
TIEMS	http://tiems.info

Joint final conference of projects on cascading CI Effects

CASCEFF, CIPRNet, FORTRESS, PREDICT, SNOWBALL

March 16, from 13:30h and March 17, 2017

Brussels, BAO, le Bouche à oreille, Rue Félix Hap, 11, 1040 Brussels



The **joint final conference** will place on the **16th of March** 2017 (afternoon) and in all day **17th of March** 2017 (1,5 days).

see

www.cascadingeffects.eu

Energy sector and incident response

As the attack surface increases and attackers are becoming increasingly aware of the possibilities in attacking the energy sector, the sector must prepare to respond to cyber incidents and to share not only data on incidents, but also knowledge.

Introduction

Most of the critical infrastructure is going through a digital revolution, as automation is opening new doors to safer and more efficient infrastructure, as well as doors to new possibilities and effects in old industries. The industrial control systems (ICS), enables the operators in for instance the energy sector to ensure the frequency and balance are at the right levels at all times, and controlling this centrally gives a comprehensive view of the system, enabling better administration.

Unfortunately, the industrial control systems were not created with security features, hence as the industry becomes increasingly connected, the number of possible attack vectors increase. The new generation control systems are built with common off-the-shelf components, which on the one hand opens up for security functions like logging, white-listing and anomaly detection. On the other hand, the operating systems will, to a larger extent, be known and widely available to the attacker.

The number of published vulnerabilities in ICS is rising, because more and more vendors are either security testing their products or are more or less willingly being tested by security researchers. This has two sides. On the one hand the control system elements are finally being tested, but on the other hand the number of zero-days in control systems available to attackers will rise too (see figure 1).

With “smart meters” in all homes, and a legitimate desire to extract useful data to improve both new and old services, the industry is opening a door to a wider range of threats than most are prepared to meet. The maturity in digital security operations and incident response is still alarmingly low.

Attackers Enterprise Model

The attackers we face may be advanced or even just well-coordinated, but we also frequently see that attackers stumble across industrial control systems because they are too readily available. Today’s threat picture is complex, and the older model with hacktivists vs. criminals, spies or nation state does not cover today’s situation. It has become a many-tiered, distributed, enterprise model. In this model, you can find small time hackers that sell breached accounts or social engineering results, researchers that find and sell zero-day vulnerabilities in ICS, programmers that specialise in utilising these vulnerabilities to create an “attack software”, others that specialise in software designed to download the “attack software”.

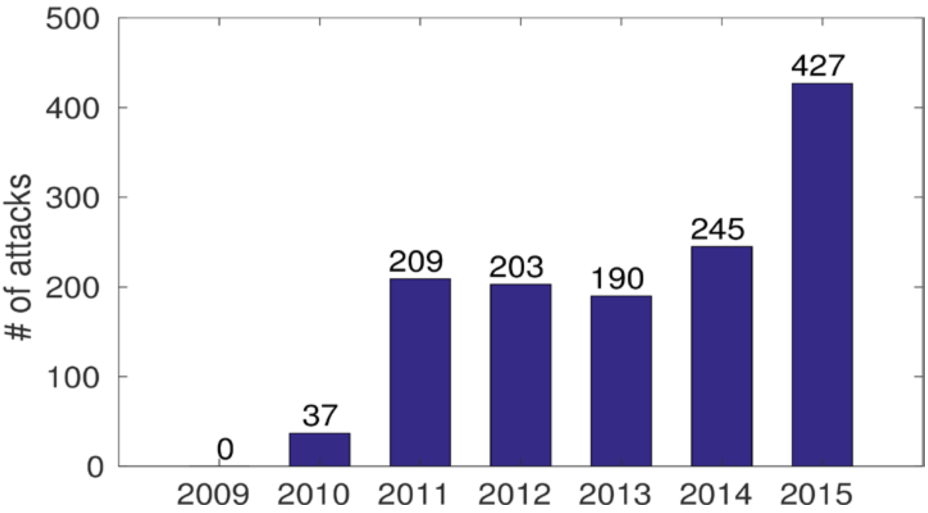


Figure 1: Vulnerabilities published through the ICS-CERT from 2009 - 2015

Margrete Raaum

has worked in information security since 1998, and later in incident response in academia where she started UiO-CERT, at the national CERT, NorCERT, and with the Norwegian TSO, Statnett. She wrote a master thesis on trust in information sharing networks in 2012 at HiG/NTNU. She is Chairman of the board of directors of FIRST (Forum of Incident Response and Security Teams), and CEO and team leader for KraftCERT, the Norwegian energy sector incident response team.

e-mail: margrete.raaum@first.org

www.first.org
www.kraftcert.no/english

The attacker utilising the tools does not have to be, and seldom is, a developer, and the parties ordering the attack may be anyone with no technical knowledge, just a desire to stage an attack. The world's attention is now on the energy sector and the control systems, especially after the Ukraine attacks, and the amount of damage that can be done is unfathomable. We need to look at the challenges ahead and apply appropriate measures.

Most industries have the basic passive defences like firewalls and anti-virus in place, but are relying too much on these defences. Several security experts in the energy sector talk about the dangers of relying on these passive perimeter defences, but are still caught off guard when attackers or malware pass these defences. Which is the last thing that should happen to the defenders of critical infrastructure: to be caught off guard.

The traditional defences are failing. Avoiding detection in firewalls is trivial, and even if signature based intrusion detection mechanisms are not a reliable defines alone, some are not even there yet. Before we can move on to active detection and defines, we need to have a sound architecture with a zone model and proper inventory in place. You cannot protect what you do not know you have. If you are in full control of inventory and traffic flows, it is possible to baseline traffic and equipment configurations, which is a much more powerful anomaly detection than a mainstream solution.

Passive defines is still worth something, but active defines reflects a cyber security maturity that prevents real damage. (see fig 2)

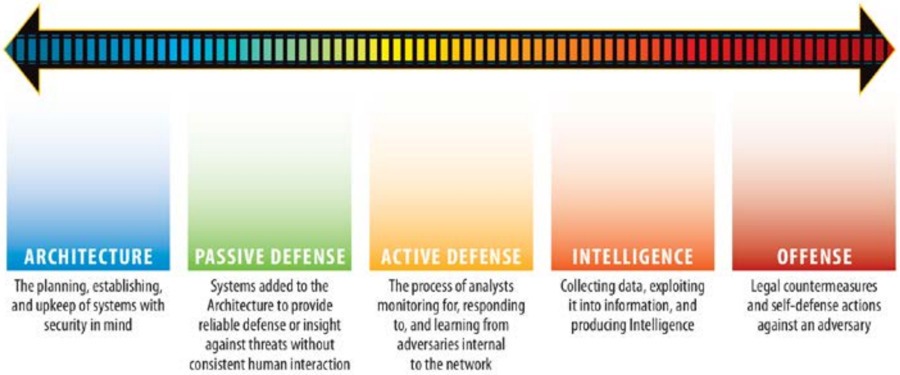

ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 2: The SANS sliding scale of cyber security by Robert M. Lee

Preparing for Breaches

Everybody must prepare for a breach, therefore we all need dedicated cyber incident response team. It can be argued that there is an advantage having sector based incident response teams: In a single sector the technology, the external threats and the vulnerabilities will be similar. Also, there is a common culture and even personal relationships so there will be a high level of trust. A high level of trust is crucial to be able to promote the sharing of incident information. If the reporting is forced, and not trust based, the sharing parties will likely not share more than is absolutely necessary.

> „Everybody must prepare for a breach: –
> this is why we need dedicated incident response teams"

When choosing the initial constituency for KraftCERT, the Norwegian Energy Sector CERT, these considerations were made. Also, a team serving the energy sector should have insight into ICS, ideally also into the local systems, and this requires a close relationship with absolute trust. Being able to see the specific needs of each constituent is important to be able to choose the most important focus areas for advisories and guidelines. The voluntary membership and sharing model does also seem to work, however, as predicted in *Flammini et al. [1]*, the amount of data is low when the general activity is low. We are currently working with the larger actors, under the assumption that if major actors start sharing, the activity level will rise.

The lack of political involvement has been a critical success factor, as the focus has been on close communication, high trust level and of identifying both the individual Achilles' heels and possible areas of cooperation. We have observed that in some sectors and countries, the creation of sector incident response teams or ISACs (Information Sharing and Analysis Centre) have turned into a political battle, and this is time wasted that should be spent building up capacity.

A crucial task for a sector incident response team is to keep updated on the threat picture. This requires tight connections to other teams in other countries. KraftCERT became a full member of Forum of Incident Response Teams (FIRST) in 2016 to enable sharing of threat intelligence and attack details with other teams worldwide.

International information sharing

FIRST (www.first.org) is an international umbrella organisation that brings together trusted computer incident security teams from around the world, from all sectors. Membership enables incident response security teams to handle security incidents more effectively and to better prepare for future attacks, and 369 teams from 76 countries participate in FIRST. The members develop and share technical information, tools, methodologies, processes and best practices, and helps nations all over the globe build national incident response teams. Within the organisation, there are special interest groups (SIGs) that bring people together in more tightly knit collaboration, e.g. the Special Interest Group for Industrial Control systems.

We must try to keep up with the threat picture and the adversaries together, and the key to this is information sharing and trust. We need to share, not only incident data, but tools and tricks of the trade. Not everybody should have to invent the wheel, and there should be trust enough to be able to share both strengths and weaknesses. We should take the time to assist others in securing their infrastructure by sharing our findings with the community. Offering information and tools without being explicitly asked is also a way to show the community what other actors in critical infrastructure are working on.

[1] *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues. Chapter 2: Trust networks among human beings by Hämmerli et al.*

Cyber Threat Simulation in Smart Grids: The TACIT solution

A smart approach to cybersecurity protection in critical infrastructures includes threat simulation for design validation and operator education.

Cyber threats in Smart Grids

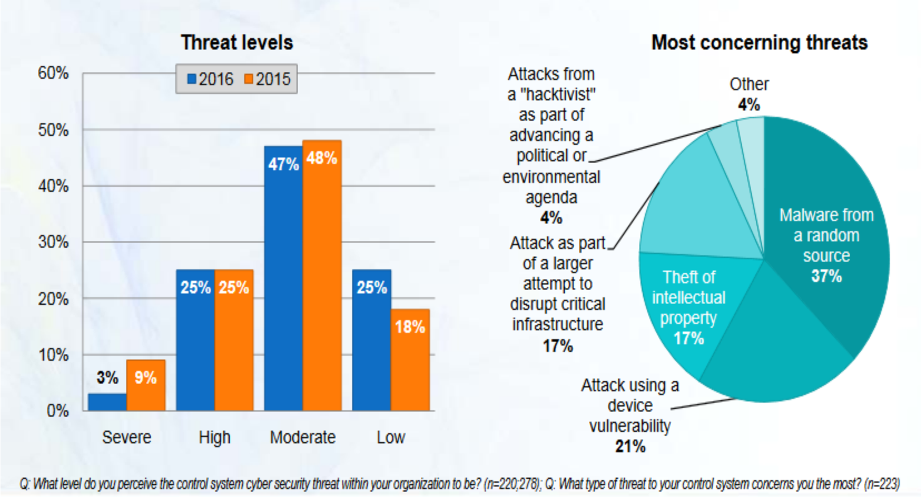
The digital transformation of the energy systems within EU is described in detail in the Digital Energy System 4.0 report by the European Technology Platform for Smart Grids [1].

As Smart Grids become more sophisticated and dependent on ICT systems, the exposure surface increases and threats diversify. According to ENISA [2][3], the Smart Grid threats can be classified by their intentional vs. accidental/inadvertent nature, and other detailed classifications may be made considering the target of attack, attack techniques used, etc.

Below is a classification of main threats over electricity grids identified by the EU-funded TACIT research project [4]:

- *Threats related to Smart Grid components and devices* in order to retrieve sensible data from them or interrupt (or hamper) their functioning, i.e. Denial of Service (DoS) attacks, which could make critical resources unavailable.
- *Device or system errors* caused by malfunctions or misconfigurations.
- *Component or device manipulation*, either software or hardware based (including changed behaviour, disabled functions or enabling remote backdoors, malware infection, etc.).
- *Unsafe communication networks and protocols*. Even if in the last years many efforts to secure the protocols used are being made, still some unsafe ones remain.
- *Unauthorised data leakage or distribution*. An attack where critical or technical data regarding a Smart Grid is made public could give place to further attacks based on such information.
- *Human factor threats* that include: i) external attacks that exploit social engineering techniques to harvest employee data or sensitive information, eventually targeting to gain access to internal resources, ii) insider attacks mainly from discontent employees, and iii) unintentional attacks due to the use of not sanitised own equipment and BYOD.
- *Physical threats* including sabotage, theft (device, media), fraud by physically acting on the device, etc.

The Cyber Security survey conducted by control Engineering [5] showed results on perceived threats on industrial control systems. A total of 72% of respondents considered their control system cyber security threat level to be low to moderate, and 37% are most concerned about malware threats coming from a random source.



Q: What level do you perceive the control system cyber security threat within your organization to be? (n=220;278); Q: What type of threat to your control system concerns you the most? (n=223)

Figure 5: Threats in control systems. Source: Cyber Security May 2016 by Control Engineering

Erkuden Rios

is R&D project manager in the ICT Division of Tecnalia. She is currently coordinator of the H2020 project on multi-cloud security (MUSA) [14], and the coordinator of the Data Protection, Security and Privacy in Cloud EuroCloudCluster of EU-funded projects, launched by DG-CNECT in April 2015 [15]

She is specialised in trust and security engineering technologies and has worked in a number of large European and Spanish national projects on the subject such as TACIT, RISC, ANIKETOS, SWEPT, CIPHER and SHIELDS. Erkuden collaborates with Technology Platforms and Forums such as ECSO and the Spanish Technology Platform on Trust & Security – eSEC.

After obtaining her MSc in Telecommunication Engineering at the University of Basque Country (Spain), she worked for Ericsson Spain for 6 years before joining Tecnalia in 2003.

e-mail: erkuden.rios@tecnalia.com

The TACIT solution

The TACIT solution was born within TACIT EU-funded research project, *Threat Assessment framework for Critical Infrastructures protection* [4], oriented to enhance the security of Smart Grids. The main objective of TACIT is the definition and development of a framework for the assessment of risk and impact of cyber-attacks in Smart Grids.
Four European companies participated in the project:

Fundación Tecnalia Research & Innovation (Spain) is a private, non-profit, applied research centre with strong market orientation through the innovation and technological development.

Everis Aerospace and Defense (Spain) is a division of Everis group that provides solutions for critical systems in aerospace, space, defence, security and emergency sectors.

D'Appolonia (Italy) is a private large engineering consulting company with European relevance, really focused on critical sectors in the market.

The Industrial Cybersecurity Center (Spain) is one of the main independent organisations for cybersecurity in Critical Infrastructures with relevance worldwide (Europe, South Arabia, etc).

> The TACIT solution is a Cyber Threat Simulator that enables to simulate and visualise the impact of cyber-attacks in electricity Smart Grids.

The TACIT project developed a proof of concept of a risk assessment framework for Smart Grids that was validated through a series of test cyber-attacks' simulations that led derive appropriate recommendations to enhance cyber security in Smart Grids.

To this aim the project developed a Smart Grid Simulator able to simulate how existent and recently discovered cyber-attacks are spread through actual end-user Smart Grid networks. The simulator allows for identifying the security issues and risks over different elements of the Smart Grid and helps estimating the associated impact.

Threats simulation

Threat simulation usually relies on a well-structured threat specification or modelling for the systematic execution of the simulation cases.

> Threat simulation relies on appropriate threat modelling for a comprehensive specification of the threats.

Threat modelling is a structured activity for identifying and evaluating application threats and vulnerabilities [6]. Perspectives may be adversarial or defensive. From the defensive perspective, the goals are to identify probable vulnerabilities, remove as many of the vulnerabilities as possible and employ countermeasures to reduce the attack risks. From the perspective of adversaries, the targets are to identify holes and vulnerabilities and exploit them to gain access to the objective.

Attack trees (Schneier **Fehler! Verweisquelle konnte nicht gefunden werden.**) aim at modelling security threats by focusing on the different ways attackers may try to attack systems. Based on this knowledge, system developers are more likely to design countermeasures that are able to hinder these attacks.

In attack trees, attacks against a system are represented in a tree structure where the root node represents the attack goal. Branches in the tree represent the different paths an attacker can follow to achieve his or her goal. OR-nodes represent alternatives, while AND-nodes represent subgoals, where all of these must be fulfilled in order for the attack to be successful. The trees can be shown graphically or be written in outline form.
Previous methods show the use of attack graphs to demonstrate the path of a single attacker [8]. But in such models creating an attacker profile is necessary which will not be feasible for unknown attackers. However, attack tree models excel at estimating the risk for situations where events happen infrequently or have never happened before.
While Attack tree technique shows how the system is threatened and exploited by attackers, **Misuse case** technique is "Inverse Use Case" [9] which aids in the analysis of the threats a vulnerability is exposed to, and identification of countermeasures to mitigate the exposure risk.

The attacker is represented as a misuser that initiates the misuse cases, either intentionally or inadvertently. Røstad **Fehler! Verweisquelle konnte nicht gefunden werden.** has extended the misuse case notation to also include the ability to represent insiders and vulnerable system functions as model elements.

The TACIT Threat Database

The TACIT Threat Simulator relies on a collection of cyber threats previously defined in the TACIT Threat Database. The Database is a novel product that includes threats not only over the IT systems but also over the OT systems and devices in the Smart Grid.

The threat modelling in TACIT adopted Attack tree technique mainly because they are simple, reusable, and relatively easy to understand which easies the communication to a non-security expert audience which is usually the case of critical infrastructure designers or operators

TACIT adopted the OWASP risk rating methodology [11] defining for each threat in the database the estimated likelihood and impact factors. The likelihood factors were defined for both vulnerabilities and threat agents, while impact factors included factors related to both business and technical impact
.
Once threat likelihood and impact are estimated, they can be combined to get a final severity rating for a risk. On top of TACIT threat models, it is possible to perform threat analysis based on indicators for cost, technical proficiency of attackers, breach of trust and noticeability.

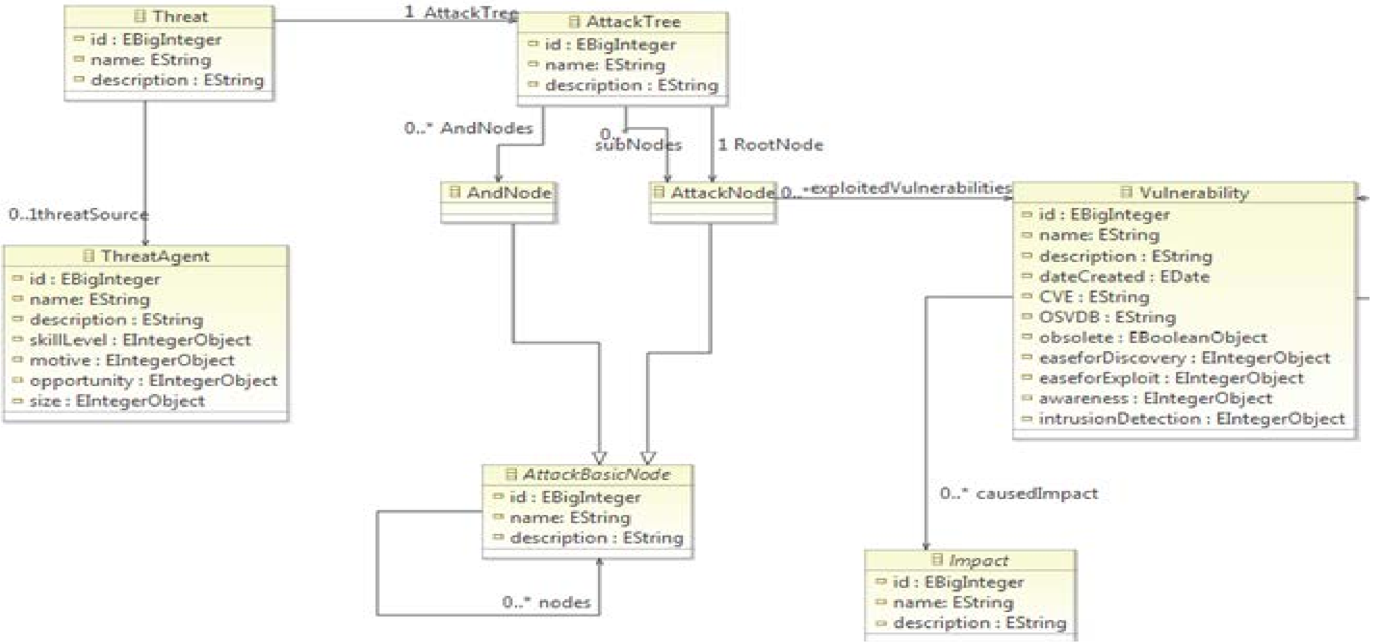


Figure 6: Excerpt of the TACIT Threat model.

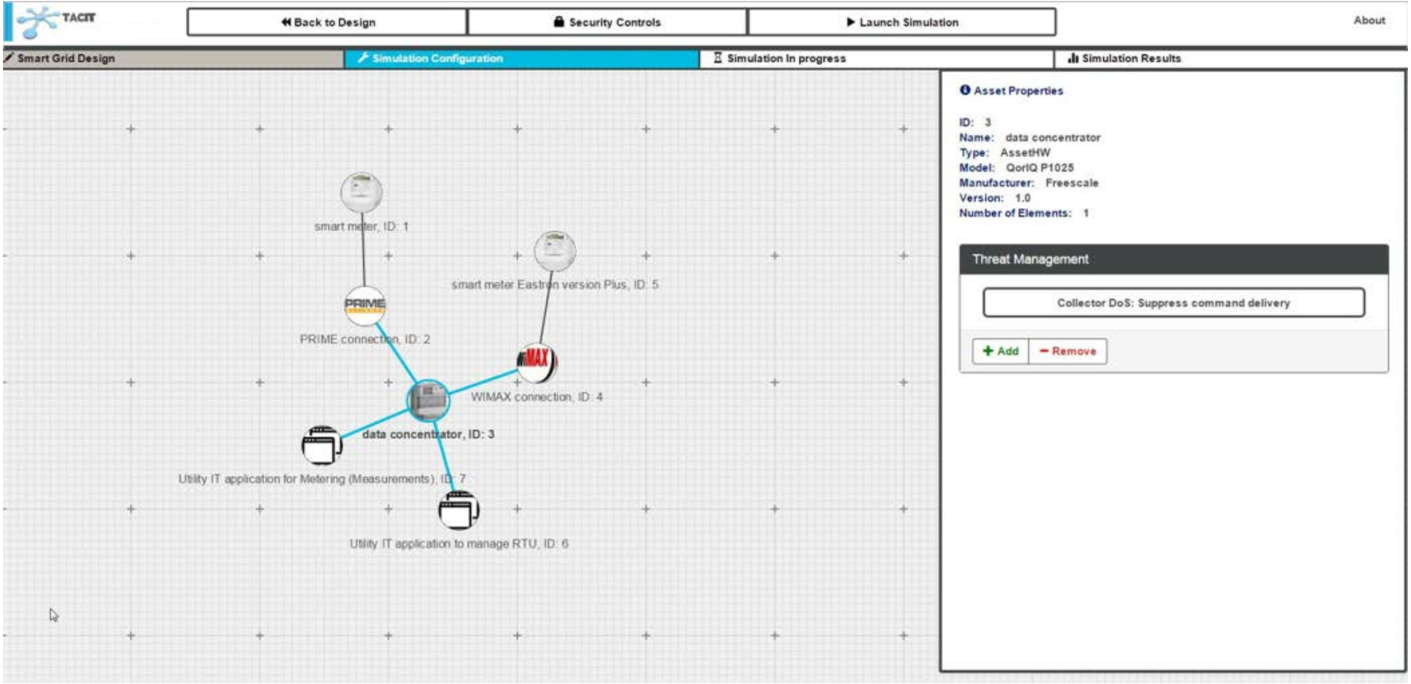
It is worth to note that for the TCP/IP related threats information enrichment, the TACIT Threat Database may be connected to *Vulnerability databases* such as Common Vulnerabilities and Exposures (CVE®) [12], that lists publicly known information security vulnerabilities and exposures, and Open Source Vulnerability Database (OSVDB) web-based vulnerability database [13].

For a more understandable visualisation of the threat impact, the Threat Database can also be connected to *Smart Grid layout databases,* usually owned by Smart Grid developers or Smart Grid owners, which include custom layouts defining the map of existing elements or assets in the Smart Grids.

The TACIT Threat Simulator

The TACIT Simulator enables three main tasks:

- Design the Smart Grid: define the Smart Grid elements and their architecture, including connections and protocols.
- Configure the simulation: define the desired (combinations of) attack(s) to be simulated over the Smart Grid.
- Check simulation results: besides graphically showing attack impact on the smart Grid elements in the layout, the simulator generates simulation logs and reports about:
    - *Simulation Test Case*: Information about Smart Grid assets and configuration, Attack tree branches simulated and attack nodes in the branches.
    - *Simulation details*: Information about the attack branches' simulation result, detailing for each attack node the exploited vulnerabilities.
    - *Impact*: Technical and Business impacts for each exploited vulnerability.
    - *Recommendations*: For each compromised asset, proposed security controls that could stop the attack.



Asset Properties

ID: 3
Name: data concentrator
Type: AssetHW
Model: QorIQ P1025
Manufacturer: Freescale
Version: 1.0
Number of Elements: 1

Threat Management

Collector DoS: Suppress command delivery

Figure 7: TACIT Simulator - Configuration of attack.

The way forward: Security 360º

Following the path of critical infrastructure protection solutions initiated by TACIT, Tecnalia started in 2015 an innovative endeavour named **Security 360º** for the comprehensive cybersecurity control in Critical Infrastructures such as Smart Grids.

> "Security 360º is a non-intrusive system for **detecting cyber security anomalies and operations** for the Smart Grid through the integral monitoring of communications."

Security 360º analyses traffic communications in the internal network of a substation and the content of exchanged messages, identifying deviations from the usual operation pattern of the facility.

The analysis is performed in real time and in a non-intrusive way, a particularly relevant feature in a sector with very high response requirements.

Security 360º has been specially conceived for the protection of the Smart Grid, so it covers sector specific standards and protocols.

The system includes machine learning capabilities which enable the detection of new attack patterns based on historical data. Since all data associated with communications is registered it allows forensic analysis of any incident.

References

[1] The Digital Energy System 4.0. Available from: http://www.smartgrids.eu/documents/ETP%20SG%20Digital%20Energy%20System%204.0%202016.pdf [Accessed 08/02/17].

[2] Smart Grid Threat Landscape and Good Practice Guide, ENISA, 2013. Available from: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide/at_download/fullReport [Accessed 08/02/17].

[3] Communication network dependencies for ICS/SCADA Systems, ENISA, 2016. Available from: https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport [Accessed 08/02/17].

[4] Threat Assessment framework for Critical Infrastructures protection, TACIT EU-funded project. Available from: www.tacit-project.eu [Accessed 08/02/17].

[5] The Cyber Security Report May 2016 by Control Engineering. Available from: http://www.controleng.com/fileadmin/content_files/ce/Control_Engineering_2016_Cyber_Security_Report.pdf [Accessed 08/02/17].

[6] T. Olzak, A Practical Approach to Managing Information System Risk, 2008.

[7] B. Schneier, Attack Trees. Dr. Dobb's Journal, vol. 24, pp. 21 - 29, 1999.

[8] J. Wing, Scenario Graphs Applied to Network Security, Y. Qian, J. Joshi, D. Tipper, and P. Krishnamurthy, Eds. Morgan Kaufmann Publishers, Elsevier, Inc., 2008.

[9] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," Requirements Engineering, vol. 10, pp. 34-44, Jan 2005.

[10] Hilpinen Risto, "Deontic Logic," in Goble, Lou, ed., the Blackwell Guide to Philosophical Logic. Blackwell, 2001

[11] The OWASP Risk Rating Methodology. Available from: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology [Accessed 08/02/17].

[12] Common and Vulnerabilities and Exposures (CVE®). Available from: https://cve.mitre.org [Accessed 08/02/17].

[13] Open Source Vulnerability DataBase (OSVDB). Available from: http://osvdb.org [Accessed 08/02/17].

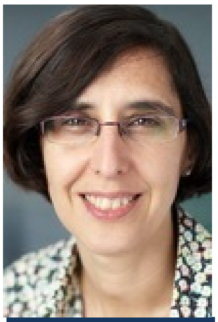
[14] MUSA www.musa-project.eu

[15] EuroCloudCluster https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud

Authors' Contributions

Eider Iturbe

Eider Iturbe is a research engineer of Cybersecurity and Safety team within Tecnalia. She is experienced in trust and security engineering technologies and is currently leading the architecture and integration work package in EU H2020 MUSA project, on multi-cloud secure applications. Eider graduated in Telecommunication Engineering from the University of the Basque Country (Spain) and in the European Master in project management at the same university.



Mª Carmen Palacios

Mª Carmen Palacios is a research engineer of Cybersecurity and Safety team within Tecnalia. Her knowledge and research interests focus on security and safety concepts applied to critical systems. She is currently involved in H2020 COSSIM and MUSA European projects. She is graduated in Physics (Electronics & Automation) from the University of the Basque Country (Spain).

Spatial-aware Iterative Integration of Crisis Management Information Systems

The goal of the FP7 project PREDICT is to provide a comprehensive solution for dealing with cascading effects in multi-sectoral crisis situations covering aspects of critical infrastructures. The result leverages on integrating specialised innovative information systems.

Information systems are playing an increasingly more important role in modern crisis management process. An integrated system with capabilities like foresight, prediction and decision support can provide substantial added-value for decision makers on both tactical and policy-making levels. It is however a challenging task to seamlessly integrate various systems with dedicated functionalities on functional and technical aspects, especially when these systems are developed independently from each other with substantially different design rationale and software technology. In this article, an iterative system integration approach is proposed by harmonising service-oriented, model-driven and agile system development. Several design principles and best practices from the software engineering community are adopted to facilitate the integration task. In addition, extra attention is paid to provide enhanced support for integrating spatial data into the crisis management workflow. This approach aims to provide a pragmatic system integration methodology to integrate crisis management information systems in a more effective and efficient fashion.

Iterative system integration

Working with partners from different organisations on the same software project can be difficult, especially when it comes to integrating new system features and providing system maintenance. It can yield unwanted dependencies and slow down the software development process. Therefore, a modular software architecture can help to manage system development and decouple component dependencies. In the following subsection, four major aspects of the integration approach are elaborated.

RESTful service-oriented architecture

Service-Oriented Architecture (SOA) is an architectural design pattern based on isolated and de-coupled software components—each provides dedicated services to the others, focusing on interoperability and re-usability. One approach to implement SOA capability is using RESTful web services, which provide lightweight and highly scalable solutions. Extensive programming language support and a large ecosystem make it ideal for integrating heterogeneous information systems used in the crisis management process. Figure 8 illustrates a system with three services and a proxy. All three services can be developed independently by different organisations. They are accessible by exposing themselves via the proxy, which decouples the service interface and the implementation. This kind of system isolation is crucial for developing different crisis management system components.

Iterative Integration

An iterative approach of system integration can be separated into three stages:

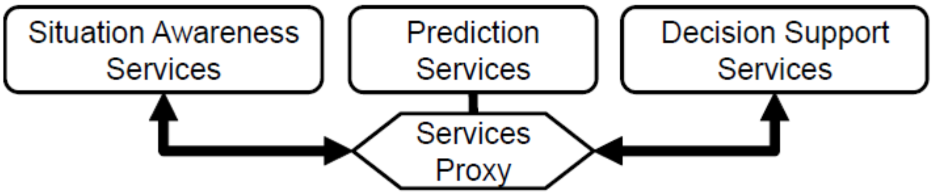


Figure 8: A service suite with three RESTful web services and one service proxy. Each of them provides dedicated services and can communicate with each other via the proxy

Jingquan Xie

Fraunhofer IAIS, Germany and has been working in projects focusing on Critical Infrastructure Protection (CIP): IRRISS, DIESIS, EMILI, VASA, CIPRNet and PREDICT. His main research interests are database management systems, knowledge engineering.

jingquan.xie@iais.fraunhofer.de

Betim Sojeva

Betim Sojeva is a research associate at Fraunhofer IAIS. He has experience in Computer Vision and Computer Graphics as well as in Web technologies and Geographical Information Systems (GIS).

betim.sojeva@iais.fraunhofer.de

1) Defining specification and requirement of the service. This includes developing use cases, formal specification, etc.
2) Writing service mock-ups and deploy them to the server for automated testing. After this stage, all unit tests should pass as required in classical Test-Driven Development (TDD).
3) Iteratively replacing mock-ups by real implementations. Each time, if a service mock-up is replaced, all unit tests must be executed to guarantee that the service implementation meets the requirements defined in the specification.

Embracing Software Containers

Component-based development is a technique to manage software artefacts on a single or on multiple host machines. A software container is an isolated and independent auxiliary software piece that hosts other software components. Once deployed, a software container can be considered as a running application with all the dependencies it needs. In the iterative approach used in PREDICT, several software components used for the deployed integrated system and during its development are "packed" into containers, including: the Web Server for the web based user interface, Documentation Server, Map Services, Data Storage, and Continuous Integration server.

Spatial Data Integration

Spatial data integration is an essential part in the modern crisis management process. Most of the objects that are of interest to the crisis management team have geographical locations—like a street, a telecommunication router, an electrical substation, etc. Crisis managers and situation operators need sufficient information about the states of these objects, in order to make reasonable decisions like whether to evacuate a certain region.

Modern geographical information systems consist of a set of standards like Web Map Service (WMS) and Web Feature Service (WFS) to facilitate the modelling of these objects. A dedicated map server can be set up as a container providing spatial data support. The descriptions of objects that need to be rendered by the map server can be extracted from another container that implements Data Storage.

Use case—the integrated PREDICT tool suite

The integrated PREDICT tool suite—iPDT for short—developed in the PREDICT project is an example that realises the proposed integration approach. The fully integrated system iPDT combines the component systems on both conceptual and technical level. Each of the blocks in Figure 9 corresponds to a Docker container—a proprietary implementation of software containers.

Services provided by component systems like PROCeed or MYRIAD are specified at the beginning and replaced iteratively by implementations provided by different organisations. This kind of isolation and decoupling make the distributed development and deployment more efficient. Moreover, information generated within iPDT can also be fed into other systems. For instance, the information forecast by PROCeed can also be fed into other systems by providing the standard mapping services on top of the Web. Currently a working group in the PREDICT project is focusing on integrating the Dutch national crisis management system LCMS with iPDT by applying this kind of spatial-aware integration approach. Finally, all the services are deployed by using the high performance reverse proxy server NGINX.

Based on current situation information, iPDT computes likelihoods of fictitious future scenarios and determines a set of most likely scenarios (SBR, scenario based reasoning). For these scenarios, iPDT provides information related to cascading CI effects (PROCeed tool). The combined results are fed into MYRIAD, which evaluates the situation information according to certain metrics in order to further eliminate less likely possible scenarios. For example, the fictitious future scenarios could describe CI outages of different lengths and indicate consequences of the outages and limitations of response and mitigation actions dependent on the duration of the outage.

The PREDICT Consortium

- Research & Technology Organisations: CEA, Fraunhofer, VTT, and TNO.
- End-user organisations: the International Union of Railways (UIC), the Safety authority of South-Holland-South Region, and the Finnish environment institute (SYKE).
- Large industry actors and SMEs with a strong expertise in crisis management: CEIS, Thales, and iTTi.

Find out more about PREDICT at www.predict-project.eu

Disclaimer: The project PREDICT has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° FP7-SEC-2013-607697. The contents of this article do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

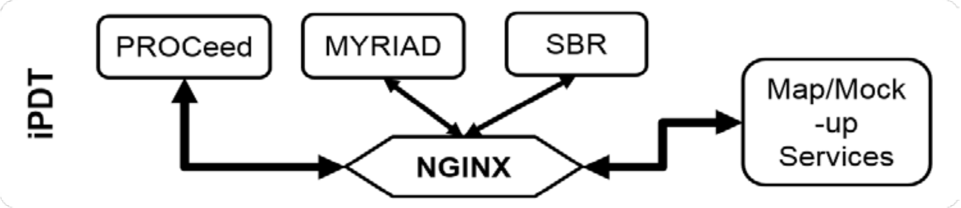


Figure 9: The integrated PREDICT tool suite consisting of three major components – PROCeed, MYRIAD and SBR including mapping service and the service mock-ups.

EU-CIRCLE: A pan-European framework for strengthening Critical Infrastructure resilience to climate change

The aim of the Horizon 2020 project EU-CIRCLE is to develop a framework and a set of tools that will enhance the resilience of interconnected Critical Infrastructure Networks to climate hazards under climate change.

Climate related hazards (e.g. floods, storms, extreme precipitation, wildfires etc.) have the potential to destroy or substantially affect the lifespan and effective operation of European Critical Infrastructures (CI), such as energy, transportation, ICT and water infrastructures. When infrastructure systems are damaged or fail, the smooth functioning of society is disrupted. To further complicate matters, modern infrastructures operate as a 'system of systems' with many interactions and interdependencies among these systems. Damage in one infrastructure system (e.g. ICT) can cascade and result in failures and cascading effects onto all related and dependent infrastructures (e.g. energy and water infrastructures).

Critical Infrastructures are designed and constructed in accordance with national building codes and infrastructure engineering standards (e.g. EUROCODES). These set out climatic design values that aim to build resilience to climate hazards, for example return periods for extreme weather events. Most existing infrastructures have been designed with the assumption of stationary climate conditions using historic values and observations. Stationarity assumes that although climate is variable, these variations are however constant with time, and occur around an unchanging mean state. This assumption of stationarity is still common practice for design criteria for (the safety / security levels of) new infrastructure.

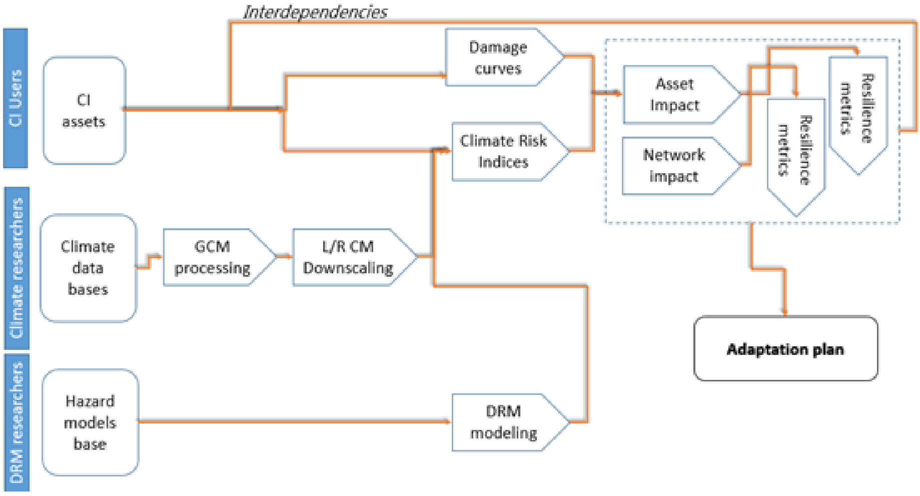
However, the climate is changing: the atmosphere and oceans have warmed, global temperatures have risen by 0.85 ° C, and sea levels have risen by 19cm since pre-industrial times. There is evidence that the increase in global temperatures has resulted in an increase in the ***intensity*** and ***frequency*** of extreme weather events. As return periods of extreme weather events are calculated using past historical climatic data, under climate change weather extremes will tend to exceed the design specifications for CI more frequently and earlier during the lifetime of an infrastructure, decreasing the durability and resilience of the structure. The changing climate will, in effect, shorten the lifespan of existing CIs in many regions.

The main strategic objective of EU-CIRCLE is to move towards an infrastructure network(s) that is resilient to today's natural hazards and prepared for the future changing climate. It aims to contribute to the EU's Adaptation Strategy through the promotion of better decision-making by addressing existing gaps in the knowledge on climate change impacts and adaptation in CIs. EU-CIRCLE aims to achieve this by defining a proper conceptual framework and development of tools for enhancing the resilience of critical infrastructures to climate stressors.

Athanasios Sfetsos

Dr. Athanasios Sfetsos is a Researcher at the National Center for Scientific Research "Demokritos". He is the coordinator of EU-CIRCLE project: A pan-European framework for strengthening Critical Infrastructure resilience to climate change. His research interests are related to the impacts of climate change and critical infrastructure protection.

e-mail: ts@ipta.demokritos.gr



EU-CIRCLE Resilience Framework

The EU-CIRCLE climate resilience management framework is based on: a) the identification of the critical assets/processes of an infrastructure network that provide essential services to society; b) the determination of the critical values and/or patterns of climate parameters that result in a change of state for these assets (in terms of performance or functionality); c) the analysis of the relative impact, determined using appropriate consequence or damage curves; d) consequence analysis to determine cascading effects arising from interdependencies (including physical, cyber, geographic, and logical) and their related impacts; and e) analysis of the coping and adaptive capacities of the asset/network/society (resilience) which in turn leads to the identification of adaptation plans/programmes/strategies and investment needs.

EU-CIRCLE Risk Assessment Framework

The first step to improving resilience of CI to climate change impacts is the identification of the risks of several climate hazards to interconnected and interdependent critical infrastructures i.e. risk assessment.

The EU-CIRCLE risk assessment framework includes:

- Assessment of the current risks of a specific climate hazard to a single CI or a CI network or even an area of interest with interconnected and interdependent CI.
- Examination of how climate change may alter risk in the future, or expose new risks. This analysis includes a baseline assessment of the risks to CI assuming no additional adaptation actions under various climate change scenarios, as well as a second assessment which considers how current or future potential adaptation actions will affect the overall scale of risk to CIs in the future under the same climate change scenarios.
- Identification of climate change adaptation or risk mitigation options and definition of priorities. This step examines alternative strategies for mitigating risks to CI and strengthening their resilience such as: enhancing the defences of interconnected infrastructures and implementation of long term adaptation options.

A comparative assessment of these scenarios using well identified criteria (e.g. cost – benefit analysis) will return scientific evidence for supporting informed decision making.

EU-CIRCLE Climate Resilience Platform

CI vulnerabilities to climate hazards and impacts from extreme weather events go beyond physical damages. EU-CIRCLE will provide an assessment framework that also takes into account the impacts to the services provided by CIs, the impacts associated with repair and/or replacement of services but also, societal costs, environmental effects, and economic costs due to suspended activities.

Such assessments will be carried out on a validated Climate Infrastructure Resilience Platform (CIRP). The CIRP is a standalone and comprehensive software toolbox that is able to accommodate different types of datasets (e.g. hazard, assets, interconnections, fragilities), file formats, and risk analysis algorithms. It is open, modular and extensible in order to support various risk and resilience assessment analysis tools.

> CIRP provides a platform for assessing the impacts of climate change and extreme events on interconnected critical infrastructures.

CIRP will provide users with access to diverse simulation, modelling and risk assessment solutions. This modelling approach will support planners, operators and authorities to assess the impact of alternate climate change scenarios on the operation and performance of CIs, including any potential cascading effects due to interdependencies between CIs. It is intended to be a user-friendly environment that will provide its users with the ability to analyse what-if scenarios: leveraging model selection, climate data repositories, and CI inventories in order to calculate damages for any kind of climate hazard and CI.

EU-CIRCLE Exercise

On 7 and 8 of March 2017, the EU-CIRCLE consortium will be conducting an exercise in Cyprus aimed at Critical Infrastructure Operators. The exercise is co-organised with the Cyprus Civil Defence (National Contact Point for EPCIP). The exercise will explore the effects of two scenarios: flash flooding and forest fires on critical infrastructure in Cyprus under conditions of climate change. The scenarios will model projected climate change for Cyprus based on the Representative Concentration Pathways (RCPs) of the Intergovernmental Panel on Climate Change (IPCC) and in particular RCP 2.6, RCP 4.5 and RCP 8.5 for the time period 2016 to 2050. The exercise will showcase the CIRP and show how the risk assessment and resilience frameworks developed by EU-CIRCLE can be used with CIRP to model the potential impacts of climate hazards in a changing climate and allow for adaptation plans to be developed.

The EU-CIRCLE Consortium

The EU-CIRCLE Consortium consists of 20 partners: National Center for Scientific Research –Demokritos (GR); Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (DE); Meteorologisk Institutt (NO); University of Exeter (UK);Gdynia Maritime University (PO); ARTELIA Eau et Environnement SAS (FR); SATWAYS Ltd (GR); Entente pour la forêt Méditerranéenne | Valabre (FR); D'Appolonia S.P.A. (IT); Državni Hidrometeorološki Zavod – Meteorological And Hydrological Service (HR); XUVASI Ltd (UK); MRK Management Consultants GmbH (DE); European University of Cyprus / Center for Risk and Safety in the Environment (CY); Center for Security Studies (KEMEA) (GR); University of Salford (UK); National Protection and Rescue Directorate of the Republic of Croatia (HR); ADITESS Ltd (CY); Torbay Council (UK); HMOD-Hellenic National Meteorological Service (GR); University of Applied Sciences Velika Gorica (HR).

If you would like to find out more about EU-CIRCLE please visit our website at http://www.eu-circle.eu

A Good Practice Guide on Critical Information Infrastructure Protection

A Guide for Governmental Policy-makers.

Early 2016, the Meridian Process and the GFCE tasked the Netherlands Organisation for Applied Scientific Research TNO to develop a Good Practice Guide on Critical Information Infrastructure Protection (CIIP) for governmental policy-makers [1]. The guide primarily aims at governmental policy-makers, but other stakeholders such as Critical Infrastructure (CI) operators may benefit from the guide as well. The guide starts at the bottom end where no experience exists with CI protection and CIIP, but also provides insights and angles of incidence which can be of help to those who already have taken steps towards a more mature CIIP posture.

Guide to assist nations in their CIP – CIIP journey

The Meridian Process [2] aims to exchange ideas and initiate actions for the cooperation of governmental bodies on CIIP. The Global Forum on Cyber Expertise (GFCE) [3] is a global platform for nations, international organisations and private companies to exchange and generate best practices and expertise on cyber capacity building. GFCE's aim is to identify successful policies, practices and ideas and multiply these on a global level by developing practical initiatives to build cyber capacity worldwide.

Structure of the GP Guide

The guide starts with an introduction explaining the need for CIIP, the distinction between CII, CIIP and cybersecurity, and how to use the guide. Six topic-oriented chapters follow, each with a general description, an explanation of the main challenges, good practices and references for further reading. The six key topics (see figure 3) are:

- National perspective
- Identification of national CI
- Identification of CII
- Developing CIIP
- Monitoring and continuous improvement
- Networking and Information Sharing

Understanding CII

The guide starts explaining that one needs to understand one's CI first. Although nations have defined the notion of CII (see: CIPedia© [4]), the identification of CII is difficult as it comprises two dimensions: the critical information and communication "backbone" (e.g. telecom, internet), and critical functions in CI such as the process control/SCADA environment in the energy sector, financial transaction systems, and alike.

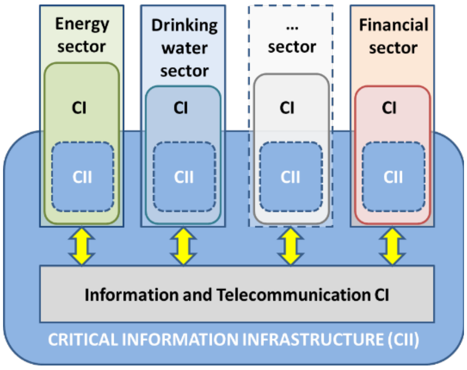


Figure 1: Critical Information Infrastructure

From Figure 1, it will be clear that CIIP efforts in many nations cross the boundaries of public and private organisations, and of CI sectors. CIIP also touches upon issues like trusted supply chains and trusted sourcing of hardware and software.

Highlights

The guide outlines five sequential steps to address the complex CIIP challenges (see Figure 3): the first five key steps mentioned in the list above. The sixth is both a topic and a step: 'networking and information sharing' is essential on its own and supports each of the first five key steps.

Under the national perspective topic, a national risk profile approach is proposed to balance the various threats with the need for protection of CI and CII. For example, in case the power grid is hampered by daily disruptions in its supply of energy, national priorities may less worry about CIIP. Moreover, CIIP requires a multi-stakeholder / multi-agency cooperation within administrations.

Eric Luiijf
is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. He contributed both at the technical and policy levels to many national and EU Critical (Information) Infrastructure Protection projects since 2000,

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

Tom van Schie

joined TNO as a junior consultant cyber security. He obtained his master degree in the United Kingdom and Germany on International Security. He has a keen eye for cybersecurity policy and governance issues, but also for technical developments. He has worked for the Dutch National Cyber Security Centre (NCSC) advising on international affairs, public-private partnerships and cybersecurity trends.

e-mail**: tom.vanschie@tno.nl**

Sometimes not easy but crucial for a balanced and effective approach.

Based on the national risk profile, one can identify the CI, CI sectors and critical services. A dependency analysis should follow, which takes cross-border aspects into account as well. It is beyond dispute that this requires interaction with all stakeholders: agencies and CI operators. The identification of the National CI (for definitions: see CIPedia [4]) is a required step before one should consider CIIP.

The identification of the CII is the next complex step. As discussed above, it requires the cooperation of multiple agencies and may also involve other organisations like CI operators. Note that the guide does neither presume, nor exclude a priori any specific government, legal, governance, or other structure. It merely mentions the issues and challenges to be addressed in one's own national context, way of working, etcetera.

One threat to be addressed comprises CII dependencies. The tricky aspect with dependencies is that they sometimes stem from unexpected sources. Or better said, overlooked critical services such as the national domain name registry, a certificate supplier, a crucial glass fibre, or a cloud services provider. New technologies may alter the set of CI/CII dependencies and thereby the risk landscape in a rapid way. The guide touches all these issues.
Note that some of these dependencies may not be recognised yet by nations which have a more mature posture in CIIP.
For that reason, the last section of the sequence

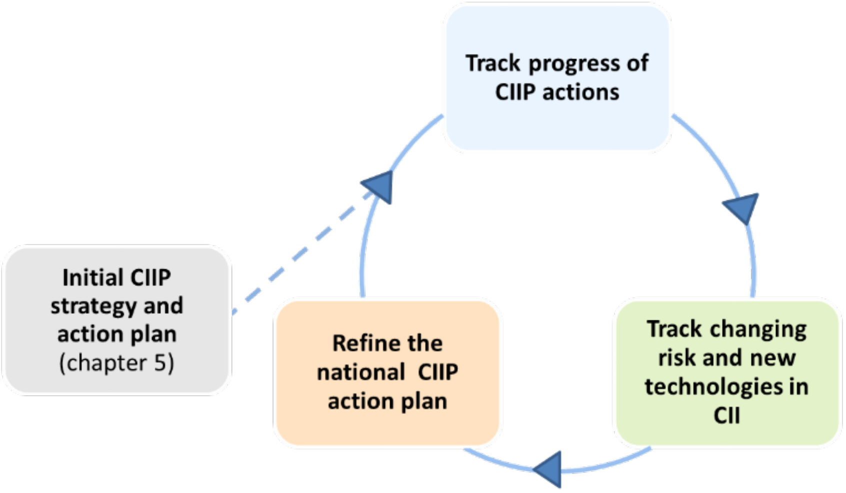

Track progress of CIIP actions
Initial CIIP strategy and action plan (chapter 5)
Refine the national CIIP action plan
Track changing risk and new technologies in CII

Figure 2: Continuous CIIP improvement cycle

Most communities today, are dependent upon critical infrastructure (CI): without power, water, sewage treatment, gas pipelines, road and communication networks, daily life would come to a standstill. On a day-to-day basis, thousands of people are working to ensure that these systems remain operational and that society benefits from the advances in technology.

If you are one of those thousands of people, I would like to challenge some of your perceptions and improve the quality of decision-making.

… and more

The guide was presented at the Meridian conference in Mexico City and can be downloaded for free since then. Translation from English into other languages is encouraged (see the colophon section of the guide). Actually, a Spanish translation effort has come to the attention of the authors.

References

[1] Eric Luiijf, Tom van Schie, Theo van Ruijven, Auke Huistra (2016), Good Practice Guide on Critical Information Infrastructure Protection (CIIP) for governmental policy-makers: https://www.tno.nl/gpciip/
[2] Meridian: www.meridianprocess.org
[3] GFCE: www.thegfce.com
[4] CIPedia©: www.cipedia.eu

email eric.luiijf@tno.nl

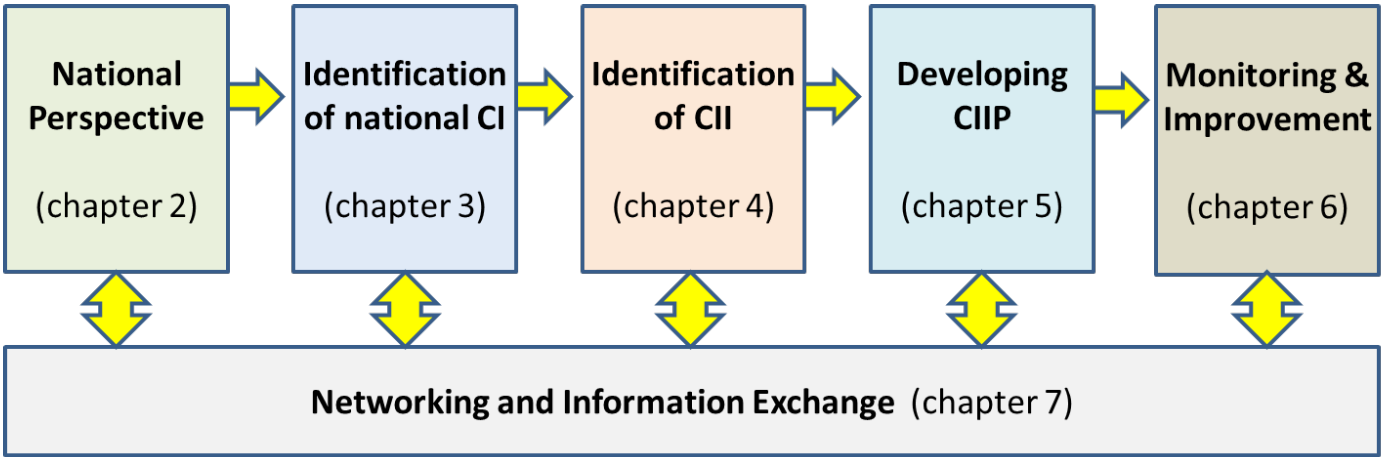

National Perspective (chapter 2)
Identification of national CI (chapter 3)
Identification of CII (chapter 4)
Developing CIIP (chapter 5)
Monitoring & Improvement (chapter 6)
Networking and Information Exchange (chapter 7)

Figure 3: Outline of the guide's topics

Human vulnerability mapping facing critical service disruptions for crisis management

The goals of these researches are to improve the automated assessment of consequences facing simulated scenarios of critical service disruption. They are situated at the crossing between the FP7 project CIPRNet and the French project DEMOCRITE.

Civil safety institutions are well prepared to strong crisis, but it is known that the cascading effect management is a hard point of the preparation. It necessitates the understanding of each Critical Infrastructure (CI) functioning, but also the knowledge of the global system behaviour facing a crisis. For helping crisis managers to have a better awareness on cascading effects, some tools propose to model CI dependencies. However, the crisis management requires on top of these cascading effect simulations a timely, accurate and realistic assessment of the consequences of a scenario, especially on the population. This common concern has been identified by at least two research projects: CIPRNet and DEMOCRITE. Both are presented below and their new approaches of the consequences assessment are complementary.

The CIPRNet tools model cascading effects between CI and assess human impacts in an innovative but static manner: people are located at their census home; their sensibility to a resource lack varies during the day. The methodology developed for the DEMOCRITE project improves it by mapping people mobility. It focuses on location of people with regards to their activities and the time period (night/day, holidays), and discuss their sensibility to the lack of key infrastructure services.

The CIPRNet project and its method for assessing consequences

The Critical Infrastructure Preparedness and Resilience Research Network or CIPRNet is a European FP7 project that establishes a research network on CI Preparedness and Resilience. This project runs until February 2017 and is under the coordination of the Fraunhofer. The CIPRNet Decision Support System (DSS) already developed comprises five parts:

1. an operational DSS, gathering of real time external inputs like the weather forecast;
2. an event simulator, modelling of natural events for scenarios;
3. a harm simulator, estimating infrastructures damages;
4. an impact assessment tool, modelling cascading effect between CI;
5. a What-if analysis tool, comparing strategies of emergency response based on the consequences estimation.

We are interested here in this last part. Four criteria evaluate the consequences: the human impacts, the access reduction to primary services on the territory (access to wealth structures, schools, and so on), the economic losses and the environmental damages. They are caused either directly by the event, or indirectly by cascading effects. This point is measured by a service disruption in terms of electricity, telecommunications, water (drinking water, waste water), gas and other energetic products and mobility (availability of roads and railways transport).

Amélie Grangeat

PhD. student Amélie Grangeat is an engineer in risk management working in the CEA (Fr). She is currently involved in four research projects around the critical infrastructures protection: DEMOCRITE (Fr), CIPRNet (FP7), RESIWATER (Fr-Ge), and PREDICT (FP7). The two first projects are described here, the others concern the resilience of the water utilities for RESIWATER, and the crisis management for PREDICT. Her research has been awarded by the CIPRNet Young Critis Award 2016.

e-mail: **amelie.grangeat@cea.fr**
amelie.grangeat@orange.fr
CEA/Gramat
46500 GRAMAT
FRANCE

The human impact assessment method developed in CIPRNet uses an innovative perspective. Having no water is a problem only when you need it, and this remark may be applied to others critical services. For this reason, the CIPRNet consequences assessment is based on Service Availability Wealth (SAW) Indexes, determining the relevance of the service availability as a function of time and of the population's vulnerability. This last one is split into four categories: old, young, disabled people and others.
The CIPRNet team gathers statistical data on the consumption of primary technological and energy services like average monthly household expenditure on electricity or gas, to compute the relevance indexes of each service.

At the end, a typical day (working vs. non-working day) with time schedule and statistical activities is proposed. For instance, electricity use during a day is split into nine different functions: lighting, refrigerator/freezer, air conditioning, TV, oven, microwave, washing machine & dryer, and a global section for other appliances. Evaluating the importance of various activities requiring services within a daily time schedule, CIPRNet project obtains a normalised indicator of relevance of services (SAW Indexes) for each service and each category of citizen every 30 minutes.

The CIPRNet method on consequences assessment crosses the SAW indexes with the availability and the quality of the critical service as a function of time and localisation. It enables by this way to compare the gravity of the different calculated scenarios in an automated manner with an innovative approach.

However, this approach of assessing human impacts by using citizen's activities at home is static. For instance, the relevance of service availability in accommodations drops to zero during the working hours because people are outside. But it does not grow in other buildings because we don't know the people localisation during these working hours. In order to improve it, it seems necessary to complete this assessment by the human density mapping and its daily evolution. This work has been done with the DEMOCRITE project, presented below.

The DEMOCRITE project presentation and its method for mapping the human vulnerability

Having statistical information on people location is a significant help for safety institutions. Accurately estimating the population exposure is important for assessing crisis consequences. This precision means to understand the spatiotemporal variation of the population distribution and not to rely only on census static data. The Ile-de-France French civil safety institution handles a research project named DEMOCRITE to map dynamically (among other tasks) human vulnerability in Paris. We define "human vulnerability" of one territory as the spatiotemporal distribution of people: the more concentrated is the population, the more important is the human vulnerability. They are a "vulnerability" in the sense that people are the main stake to protect during a crisis, facing a threat. The method developed in this project is presented below and on the figure.

A week has been divided into three periods (Weekdays, Saturdays, Sundays) and each day has been divided into four time slots: the morning rush hour, the daytime, the evening and the night.

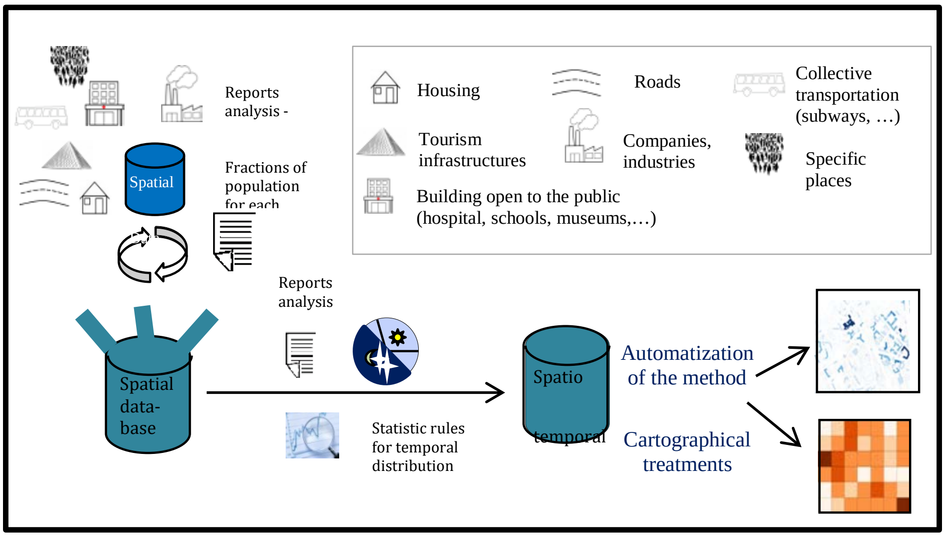
In total, more than 70 spatial databases were used. Only the more complete and accurate were retained. The main challenge was to transform these spatial databases into a spatio-temporal database.

The temporal distribution is calculated according to statistic treatments of available reports concerning the living habits in Paris (opening hours of museums, underground frequentation during a working/non-working day and so on). It enables us to simulate how many people may be in the buildings as a function of the buildings categories and the time slot.

For instance, based on geographical census data and of various statistics on population (age, unemployment, etc.), it is possible to deduce the percentage of people staying at home, including the percentage of unemployed people, young babies and retired people. The same statistical approach is used to estimate people present in shops: based on the shopping surfaces of buildings, one can deduce the maximum capacity of shoppers, and based on statistics on hourly shopping habits, one can calculate the potential numbers of people in these places.

In the same way, education buildings are assumed to be full during class hours but empty during the night, such as the companies' buildings and so on. The visitor numbers of museums and tourist sites are investigated and are associated with their opening hours. Moreover, the number of subway users is also analysed to obtain temporal distribution of people in the subway stations.

Even if this database is not exhaustive and has some imprecisions, it is nevertheless a very useful tool to assess the statistic spatiotemporal distribution of population in Paris.



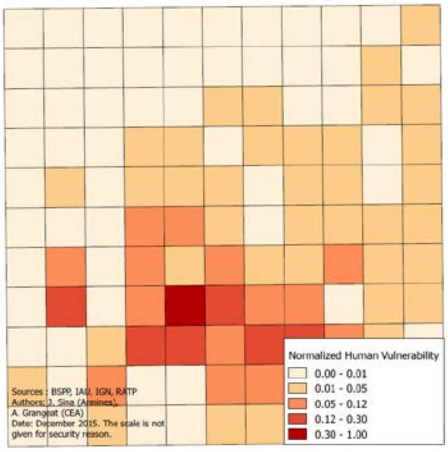
Flowchart of the DEMOCRITE methodology

Finally, the method is automated and proposes maps of vulnerability by counting people present in each mesh composing the territory for the different period of times identified.

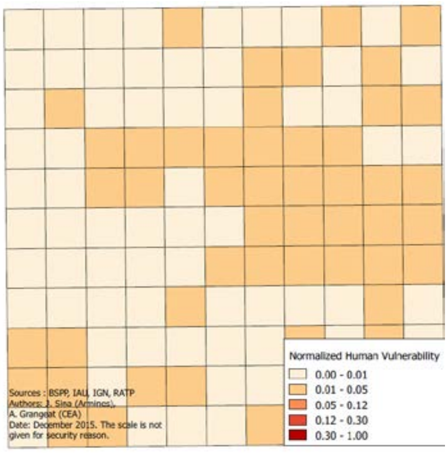
Human vulnerability Mapping: some results

The following maps (illustrative examples) show the evolution of human vulnerability between the night (census data and hostel occupancy rate) and the working hours. The information concerning people's locations and number is gathered and aggregated in a grid mesh (the scale and localisation is not given for security reasons). The represented value in each small mesh is the number of persons present in this small mesh normalised by the highest value obtained over all the periods studied and over the overall mesh.

Human vulnerability maps during a working day


Normalized Human Vulnerability
0.00 - 0.01
0.01 - 0.05
0.05 - 0.12
0.12 - 0.30
0.30 - 1.00
Sources : BSPP, IAU, IGN, RATP
Authors: J. Sina (Armines),
A. Grangeat (CEA)
Date: December 2015. The scale is not given for security reason.

Human vulnerability maps during the night


Normalized Human Vulnerability
0.00 - 0.01
0.01 - 0.05
0.05 - 0.12
0.12 - 0.30
0.30 - 1.00
Sources : BSPP, IAU, IGN, RATP
Authors: J. Sina (Armines),
A. Grangeat (CEA)
Date: December 2015. The scale is not given for security reason.

Conclusion and perspective

The high difference of human density between these two maps shows the importance to take into account the mapping of the human vulnerability when assessing consequences of the scenarios. Maps on the other time slots are discussed in the CRITIS article[1].

This human vulnerability mapping is complementary of the CIPRNet consequences assessment method. Indeed, it enables the possibility to extend the use of relevance index to other places and activities (schools, museums, and so on) and to combine it with the number of people concerned by one critical service disruption. This means improving the accuracy of the consequences assessment.

Once the automated assessment of the scenarios consequences has reached a reliable level and provides accurate information, the next step concerns the huge debate on the definition of quantitative gravity state. How to identify the minimum duration of critical service disruption before being in a crisis, as a function of its localisation? This question has to be studied from a societal and political point of view, and is not closed to have a fix answer.

> Human vulnerability maps of Paris area during periods of a working day time show the importance to take into account people mobility when assessing crisis impacts.

Article and co-author

This work is the result of collaboration and has been published with more details in the following reference.

[1] Grangeat, A.[a] , Sina J.,[b] Rosato V.[c] Bony, A.[b], Theocharidou M.[d] (2016) Human vulnerability mapping facing critical service disruptions for crisis managers. To be published in the Revised Selected Papers on the 11th *International Conference, CRITIS,* Paris, France, October 10-12 2016. 12p.

a. CEA, DAM, GRAMAT, F-46500 Gramat, France
b. Institut des Sciences des Risques – Centre LGEI, Ecole des mines d'Alès, 30100 ALES, France *julie.sina@hotmail.fr aurelia.bony-dandrieux @mines-ales.fr*
c. ENEA Casaccia Research Centre, Roma, Italy vittorio.rosato@enea.it
d. European Commission, Joint Research Centre. Space, Security and Migration. Technology Innovation in Security Unit, Ispra (VA) Italy *marianthi.theocharidou @jrc.ec.europa.eu*

CIPRNet Consortium

All the information on CIPRNet may be found on the CIPRNet project website: http://ciprnet.eu

DEMOCRITE consortium

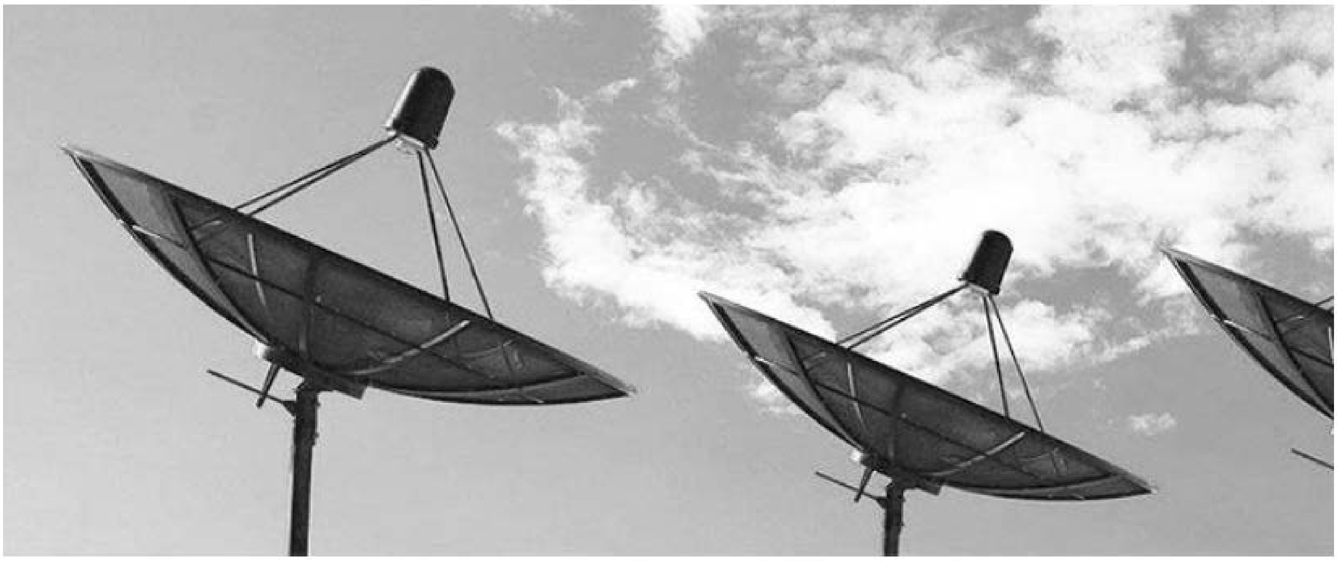
All the information on DEMOCRITE may be found on the DEMOCRITE website: www.anr-democrite.fr

Acknowledgments

The work presented in this paper has been also partially funded by the CIPRNet (Grant agreement no: 312450) European project. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Commission. The authors want to thank also the French DEMOCRITE (ANR-13-SECU-0007) project for the partially funding of these researches.

euconcip European Cooperation Network on Critical Infrastructure Protection

(/index.php)



IFIP 2017 - International Conference on Critical Infrastructure Protection

The Eleventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will take place in **Arlington (Virginia, USA) on March 13th-15th, 2017**.

The conference will provide a forum for presenting original unpublished research results and innovative ideas in the field of critical infrastructure protection.

Papers are solicited in the following areas of the critical infrastructure protection domain:

- Infrastructure vulnerabilities, threats and risks
- Security challenges, solutions and implementation issues
- Infrastructure sector interdependencies and security implications
- Risk analysis, risk assessment and impact assessment methodologies
- Modeling and simulation of critical infrastructure
- Legal, economic and policy issues related to critical infrastructure protection
- Secure information sharing
- Infrastructure protection case studies
- Distributed control systems/SCADA security
- Telecommunications network security

The deadline for paper submissions is **January 10th, 2016**; notification of acceptance will be communicated by February 3rd 2016. A selection of papers from the conference will be published in an edited volume – the eleventh in the series entitled ***Critical Infrastructure Protection*** (Springer) – in the fall of 2017.

For further information on the event please proceed to the following link

www.ifip1110.org/Conferences

Protecting Industry 4.0 against Advanced Persistent Threats

As APTs will undoubtedly target Industry 4.0 deployments, it is essential to develop detection mechanisms and architectures tailored to this context

CIIP and the Industry (4.0)

The SADCIP project has arisen from the need to deal with increasingly intelligent and autonomous industrial and monitoring systems, capable of collaborating with each other to meet a common objective: provide efficient and real-time manufacturing and logistics from anywhere, at any time and anyhow [1]. However, any new condition that implies open communication with the Internet and the adaptation of heterogeneous (wireless) systems can, certainly, bring about numerous interoperability and security problems [2].

What types of problems? From a slight fault or anomaly within the operational applications, to massive and distributed attacks of a subtle and potentially damaging nature. Such problems can even have an aggressive effect on the welfare of other critical infrastructures. It is not the same to protect all those operational elements involved in the construction of each component that forms, for example, a bicycle, as the components that comprise a system of transport of greater reach, such as, a plane or a train. Therefore, it is self-evident that there is a relationship between the need to protect today's industry and the need to ensure protection, at all levels, of the rest of the dependent, critical infrastructures. In addition, this characteristic underlines the criticality degree of a new paradigm related to the Internet of Things known as Industry 4.0, which in itself, can also be considered as a critical infrastructure.

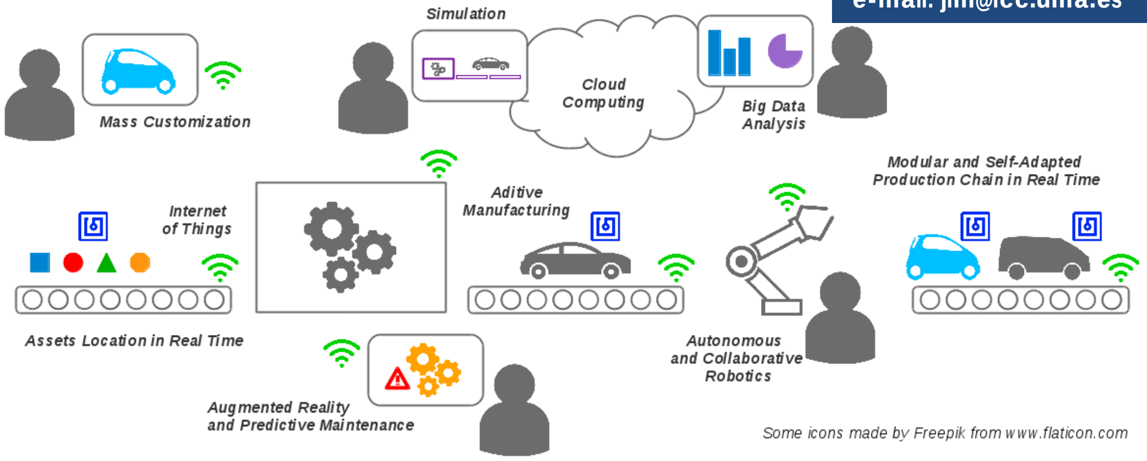
Industry 4.0 (cf. Figure 1) constitutes a technological progress within the traditional industry. Here, both novel and existing systems coexist and share, in a centralised or decentralised way, resources, data and actions. As a result, novel services are enabled, and efficiency is increased. However, the nature of this context makes it difficult to trust fully on the goodness of the whole system, as multiple vulnerabilities are born mainly because of its complexity and heterogeneity. Moreover, in this particular context, one of the most dangerous threats are advanced persistent threats, or APTs. Therefore, SADCIP looks towards improving the state of the art, trying to find the necessary tools to a) monitor the technical capacities of the operational elements in the field, and b) detect relative evidence that, if applicable, should be addressed through optimal proactive response systems [3].

> "Any novel scenario that implies open communication with the Internet will bring numerous security problems"

Javier Lopez

Prof. Javier Lopez is Full Professor in the Computer Science Department at the University of Malaga, and Head of the NICS Lab. His research activities are mainly focused on information security, future Internet security, and critical infrastructure protection, and has lead several international research projects in those areas. Prof. Lopez is Co-Editor in Chief of IJIS journal and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.

e-mail: jlm@lcc.uma.es


Simulation
Mass Customization
Cloud Computing
Big Data Analysis
Modular and Self-Adapted Production Chain in Real Time
Internet of Things
Aditive Manufacturing
Assets Location in Real Time
Autonomous and Collaborative Robotics
Augmented Reality and Predictive Maintenance

Some icons made by Freepik from www.flaticon.com

Figure 10: Scheme of an enhanced Industry 4.0 factory.

The threat of APTs

Nowadays, Industrial Control and Automation Systems have been affected by an increased number of inside and outside threats, mainly due to the interconnection of industrial environments with modern ICT technologies. Beyond traditional IT threats (e.g., malware, spyware, botnets), one major issue is the existence of Advanced Persistent Threats (APTs). They consist of a new class of emerging and sophisticated attacks that are executed by well-resourced adversaries over a long time period. By combining multiple attack vectors that include the exploitation of zero-day vulnerabilities, together with stealthy and evasive techniques [2], many APTs go undetected over time. Although APTs were used against military organisations in the first term, they are now targeting a wide range of companies, hence drawing the attention from researchers focused in the industrial security sector [4].

> "The flexibility and intelligence of Industry 4.0 factories comes at a cost: APTs will be able to influence over industrial processes in subtler ways."

Stuxnet was the first attack of this kind, reported in 2009, which sabotaged the Iranian Nuclear Program by causing physical damage to the infrastructure and therefore slowing down the whole process for four years. Ever since, the number of reported vulnerabilities concerning the Industrial Control Systems has increased dramatically, as the research community has incremented its interest and new attacks have been disclosed: in total, 1309 vulnerabilities have been reported by ICS-CERT between 2010 and 2015 (see Figure 2 showing this growth [5]).

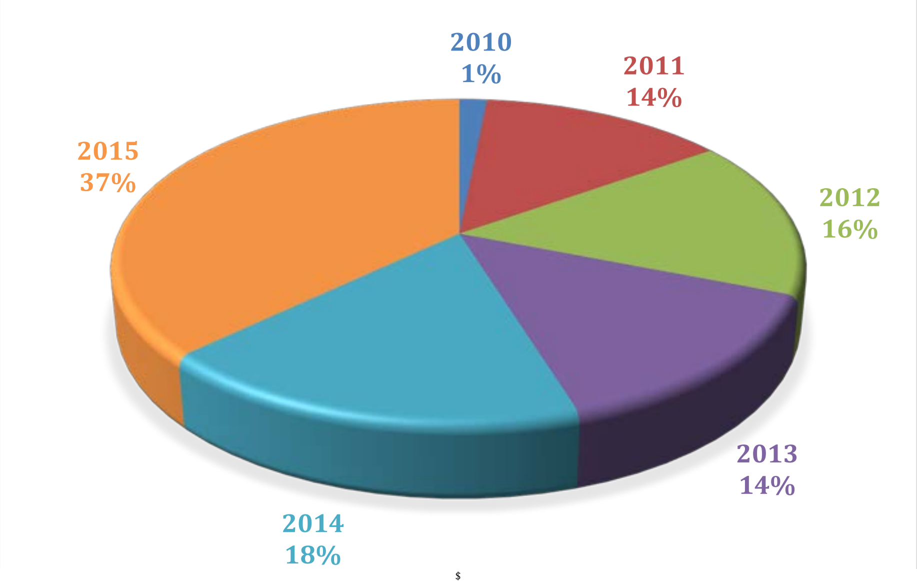


Figure 2: Reported vulnerabilities from ICS-CERT [5]

As Stuxnet, every APT follows multiple steps, beginning with an initial intrusion commonly using social engineering (e.g., by means of fraudulent e-mails containing Trojans). A successful intrusion results in the installation of a backdoor from which the attackers connect to the target network. Then, several exploits and malware are used to compromise as many computers in the victim network as possible (which is known as lateral movements), to ultimately modify the productive process or exfiltrate information back to the attacker domain. During the whole process, the threat actors make use of multiple tools to avoid detection and encrypt the external communication through publicly available services such as the Tor Anonymity Network.

Consequently, an additional effort is needed to mitigate the risks posed by these threats, which implies the effective detection of APTs through traditional countermeasures (e.g., intrusion detection systems, firewalls, antivirus) along with novel security services in continuous evolution within the company, involving all the organisation with effective security awareness training and gaining knowledge from old use cases. Numerous surveys show the evolution of awareness about this field in the industry. Specifically, we can highlight the ISACA Advanced Persistent Threat Awareness Study [6], carried on in July 2015, that provides a view of the APT perception from security professionals belonging to many industries, mostly technology services, financial, military, telecommunications and manufacturing companies. Among all the statistics, it is worth commenting an increment of 4 percentage points in security training and an increase in security budget in the 53% of the entities surveyed compared to 2014. Concerning the technical measures to protect against APT attacks, a very high percentage of those enterprises (95 percent) report that they are using antivirus and traditional network perimeter technologies (e.g., firewalls), while they increasingly leverage a variety of preventive, detective and investigative controls to help reduce the likelihood of a successful APT breach. This includes mechanisms like critical controls for mobile devices, remote access technologies (RATs) or sandboxing.

Industry 4.0 and APTs

The industry as a whole is aware of the problems posed by persistent attacks, and there are already various mechanisms that aim to facilitate their detection. Yet the solutions that are used in traditional industrial control and automation systems are not directly applicable to Industry 4.0 contexts. The integration of Industry 4.0 principles, such as interoperability, decentralisation, service oriented management, and interactivity, will fundamentally change all aspects of the industry: from the collaboration among supply chain partners, to the interactions between operators and machinery at the factory floor [7]. Yet it will also exacerbate the risks associated to APTs.

On the short term, industrial protocols like IO-Link and OPC UA will facilitate the interaction between existing and novel services. These and other technologies, like the Internet of Things, recognition services, and location services, will allow all individuals – from operators to administrators and executives – to access any relevant information anywhere at any time, helping them to make better decisions. Yet this interconnected ecosystem not only increases the attack surface, but also expands the influence that an APT can have in all actors once it has infiltrated into the system.

The deployment of open integrated factories and the integration of intelligent, dynamic processes are some of the medium and long-terms goals of the Industry 4.0, respectively. Such goals will enable the creation of flexible workflows and production processes, the deployment of intelligent assistants using novel HMI interfaces (e.g. wearables, augmented reality), and the advent of novel services such as the “digital twins” (maintenance and management through simulation), amongst other benefits. Yet this flexibility and intelligence comes at a cost: APTs will be able to influence over the behaviour of factory processes in subtler ways.

Moreover, we also should consider how the Industry 4.0 and the Internet will be closely linked. Beyond the use of IoT devices, and the convergence of IT/OT infrastructures, there are novel approaches, such as cloud manufacturing, that will allow traditional manufacturing components to become virtualised and deployed in the cloud. These novel approaches will be surely become a target of APTs.

SADCIP Project Goals

Given the effect that APTs will have over present and future Industry 4.0 deployments, it is essential to understand the potential risks and to develop an integrated solution that can effectively detect and react against APTs. Therefore, the specific goals of the SADCIP (Advanced System for the Detection of Persistent Cyberattacks in Industry 4.0) Project [8], which is funded by the Spanish Ministry of Economy, Industry and Competitiveness, are as follows:

- Analyse and investigate the characteristics of the most relevant cyber-attacks for Industry 4.0 environments.
- Develop security guidelines for Industry 4.0 environments, which not only serve to design safer infrastructures, but also to deploy defence mechanisms in a more optimal way.
- Create the basic components of a modular, flexible and easily adaptable intrusion detection architecture for Industry 4.0 scenarios, capable of cooperatively monitoring the existence of cyber-attacks that affect its fundamental elements (IoT, cloud / fog).
- Design and develop various transversal services that support the various elements of the detection system, including security services such as trust management systems, fog-based control services, etc.
- Develop relevant analysers for industry 4.0 environments, including scanners capable of detecting the lateral and data exfiltration attempts associated with APTs movements. These analysers will be platform agnostic, allowing their integration with other systems beyond the SADCIP architecture,

The proposed architecture and analysers are being developed in conjunction with the project coordinator, S2Grupo: a Spanish cybersecurity firm specialised in the development and integration of security solutions against APTs. In order to validate the results, these components will be integrated and validated in a testbed, where multiple attacks will be launched. Moreover, this testbed will also serve as a demonstrator of the resulting product.

References

[1] *J. Wan, H. Cai and K. Zhou, “Industrie 4.0: Enabling technologies”, Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things, Harbin, pp. 135-140, 2015.*

[2] *L. Cazorla, C. Alcaraz, and J. Lopez, "Cyber Stealth Attacks in Critical Information Infrastructures", In IEEE Systems Journal, issue 99, IEEE, pp. 1-15, 2016.*

[3] *C. Alcaraz, L. Cazorla, and J. Lopez, "Cyber-Physical Systems for Wide-Area Situational Awareness", In Cyber-Physical Systems: Foundations, Principles and Applications, no. Intelligent Data-Centric Systems, Academic Press, pp. 305 - 317, 2017.*

[4] *P. Chen, L. Desmet, C. Huygens. “A study on advanced persistent threats”. In IFIP International Conference on Communications and Multimedia Security, pp. 63-72, September 2014.*

[5] *ICS-CERT. Year in Review 2015. https://ics-cert.us-cert.gov*

[6] *ISACA. Advanced Persistent Threat Awareness Study Results. http://www.isaca.org*

[7] *J. Smit, S. Kreutzer, C. Moeller, M. Carlberg. “Industry 4.0”. European Parliament, Directorate General for Internal Policies, February 2016.*

[8] *SADCIP project, UMA, Spain. https://www.nics.uma.es/projects/sadcip*

Authors’ Contributions

Prof. Javier Lopez is the principal co-investigator of the SADCIP project, and is in charge of studying the specific security challenges of Industry 4.0 scenarios.

Cristina Alcaraz

Cristina is an Assistant Professor at the Comp. Science Department of the University of Malaga. She is involved in all aspects related to detection and reaction of APTs in Industry 4.0 environments.

Jesus Rodriguez

Jesus is a computer science engineer working at the University of Malaga. He is analysing and developing the protection mechanisms for Industry 4.0 environments that will be applied in the SADCIP project.

Rodrigo Roman

Rodrigo is a Ph.D. researcher at the University of Malaga. He is studying the architecture of SADCIP, and analysing the protection mechanisms of IoT-services for the Industry 4.0.

Juan Enrique Rubio

Juan Enrique is a PhD Student in the University of Malaga. His main research includes the design and implementation of security services in the context of Industrial Control Networks and the Smart Grid.

The 52nd ESReDA Seminar On Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity

52nd ESReDA seminar will be held on May 29-31, 2017 in Lithuania

Announcement and Call for papers

Critical Infrastructures Preparedness and Resilience (CIP&R) is a major societal security issue in modern society. Critical Infrastructures (CIs) provide vital services to modern societies. Some CIs' disruptions may endanger the security of the citizen, the safety of the strategic assets and even the governance continuity.

The critical role that CIs play in the security of modern societies is a direct effect of the ever-increasing spread out of the information technology (IT) in every smallest task in man's daily-life. The continuous progress in the IT fields pushes modern systems and infrastructures to be more and more: intelligent, distributed and proactive. That increases the productivity, the prosperity and the living standards of the modern societies. But, it increases the complexity of the systems and the infrastructures, as well. The more complex a system is, the more vulnerable it will be and the more numerous the threats that can impact on its operability. The loss of operability of critical infrastructures may result in major crises in modern societies.

To counterbalance the increasing vulnerability of the systems, engineers, designers and operators should enhance the system preparedness and resilience facing different threats. Much interest is currently paid to the Modelling, Simulation & Analysis (SM&A) of the CI in order to enhance the CIs' preparedness & resilience.

The European Safety, Reliability and Data Association (ESReDA) as one of the most active EU networks in the field has initiated a project group (CI-PR/MS&A-Data) on the "Critical Infrastructure/Modelling, Simulation and Analysis – Data". The main focus of the project group is to report on the state of progress in MS&A of the CIs preparedness & resilience with a specific focus on the corresponding data availability and relevance.

In order to report on the most recent developments in the field of the CIs preparedness & resilience MS&A and the availability of the relevant data, ESReDA will hold its 52nd Seminar on the following thematic: "***Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity***".

Topics

Threats identifications & specifications
CIs disruptions MS&A
CI's vulnerability MS&A
CIs' dependencies and interdependency MS&A
Data and Databases
Emergency and crises management models & tools
IT inferences on CIs preparedness & resilience
Standards & Ontology in the domain of CI protection (CIP)

Critical Infrastructures Sectors

Air-transport & airports
Electrical power generation & supply
Gas & Oil production, storage & transport
ICT networks
Massive data storage & servers
Maritime transport & ports
Medical & health care
Process industry
Railway transportation
Supply chain process
Water supply and water works

Threats

Extreme weather conditions
Natural threats
Earthquake
Flood
Forest fire
Landslide
Torrential rain
Tsunami
Volcanic eruptions
Industrial & technological accidents
Financial & stock market perturbation
Wastes disposal

www.esreda.org/event/52nd-esreda-seminar/?instance_id=39

Effective Defence against Zero-day Exploits Using Bayesian Networks

The goal of the work is to develop a Bayesian Networks based approach to maximise the system tolerance against zero-day attacks. A case study about ICS security management is demonstrated.

We investigate the possibility of improving the tolerance of Industrial Control Systems (ICS) against zero-day attacks by defending against known weaknesses of the system. We propose a metric to measure the system tolerance against zero-day attacks. We apply this metric to evaluate different defensive plans to decide the most effective combinations of available controls that maximise the system tolerance. A case on ICS security management is demonstrated in this paper.

Industrial Control Systems (ICS) play a crucial role in controlling industrial processes. Cyber security of ICS has increasingly become an urgent problem, owing to the wide use of insecure-by-design legacy systems in ICS and the physical damage of breached ICS to plants, and human health. Zero-day exploits (i.e. unknown exploits) have demonstrated their essential contributions to causing such damage by *Stuxnet*. The threat from zero-day exploits is still on the rise, but little effort has been done to combat them, because they are often unknown to the vendor.

Proposed Approach

It is extremely difficult to detect and defend against zero-day exploits. Sophisticated hackers are able to discover zero-day exploits before the vendors become aware of them. We consider the problem from a novel perspective, by seeking a way to make ICS sufficiently robust against zero-day attacks.

As shown in Fig. 1, a typical APT attack targeting ICS has to exploit a chain of vulnerabilities at different hosts to eventually breach the control devices (e.g. PLCs). The involved exploits use either known or zero-day vulnerabilities to propagate across the network. Whilst we can hardly defend against the exploitation of zero-day vulnerabilities, we can alternatively deploy effective defences against the known vulnerabilities such that the risk of the whole attack chain being exploited can be overall reduced.

A key attribute "exploitability" of weaknesses is borrowed from CWE to reflect the sophistication of a zero-day weakness. Weaknesses with higher exploitability are likely to cause higher risk. With regard to an acceptable level of risk, we define the tolerance against a zero-day weakness by the minimal required exploitability of the weakness to cause the system risk exceed the acceptable level. By using Bayesian Networks, we can prove that defending against known weaknesses is able to increase the tolerance, and find out the defence that maximizes the tolerance.

Tingting Li

Dr. Tingting Li is currently a Research Associate at the Institute for Security Science & Technology, Imperial College London. She is working on the project *Research Institute in Trustworthy Industrial Control Systems (RITICS)* which mainly focuses on producing models and tools in support of effective defence for protecting ICS from cyber attacks. She obtained her PhD degree in Artificial Intelligence from University of Bath in 2014. She also received her MSc degree in Computing (Imperial College London, 2009) and her Bachelor degree in Information Security (Xidian University, China, 2008). Her research primarily lie in cyber security for ICS, logic-based knowledge representation and reasoning, multi-agent systems and agent-based modelling.

Email: **tingting.li@imperial.ac.uk**
https://www.doc.ic.ac.uk/~tl308/

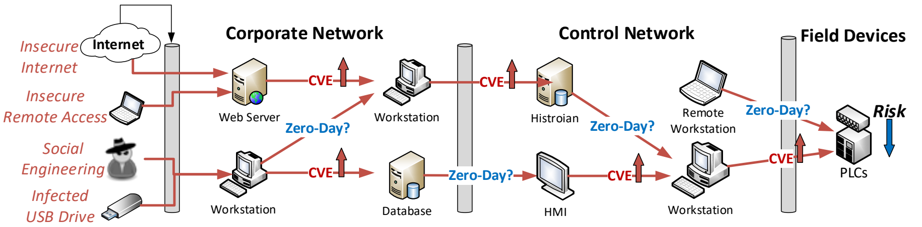


Figure 1: Multi-step Vulnerability-based Propagation across a typical three-zone ICS

Problem Modelling

We formally use Bayesian Networks (BN) to model ICS-targeted attacks with zero-day exploits involved and evaluate the risk. A discrete random variable is captured by a chance node in BN with a finite set of mutually exclusive states and a conditional probability distribution over the states. We further defined three types of chance nodes for different purposes: (i) *target nodes* indicate valuable assets in ICS with a set of known and zero-day weaknesses, (ii) *attack nodes* captures available attack methods between a pair of targets, and (iii) *requirement nodes* are designed to model particular objectives for evaluation. A *Bayesian Risk Network* is established based on the three types of nodes, where complete attack paths are modelled by target and attack nodes, and the damage of successful attacks are evaluated against requirement nodes.

We build a Bayesian network at the level of assets and model multiple weaknesses between a pair of assets by a single attack node, rather than multiple attack edges. Each attack node hence becomes a decision-making point for attackers to choose a (known or zero-day) weakness to proceed. Such Bayesian networks enable us to model zero-day exploits without knowing details about them (e.g. prerequisites or post-conditions), but focus on analysing the risk caused by zero-day exploits.

A defence control is able to reduce the exploitability of its combating weaknesses to certain degree subject to the effectiveness of the control. We select a particular node *N* to define the risk κ, which could be a valuable target node or a critical requirement. Thus κ is defined by the likelihood of *N* being compromised or violated, e.g. the likelihood of a requirement being violated must be less than 30%. The presence of a zero-day exploit at any target is likely to increase the likelihood as its exploitability increases. Thus, we define the tolerance by the minimum required exploitability of a zero-day exploit at each target to violate κ, or alternatively the maximum exploitability of a zero-day exploit the system can tolerate subject to κ.

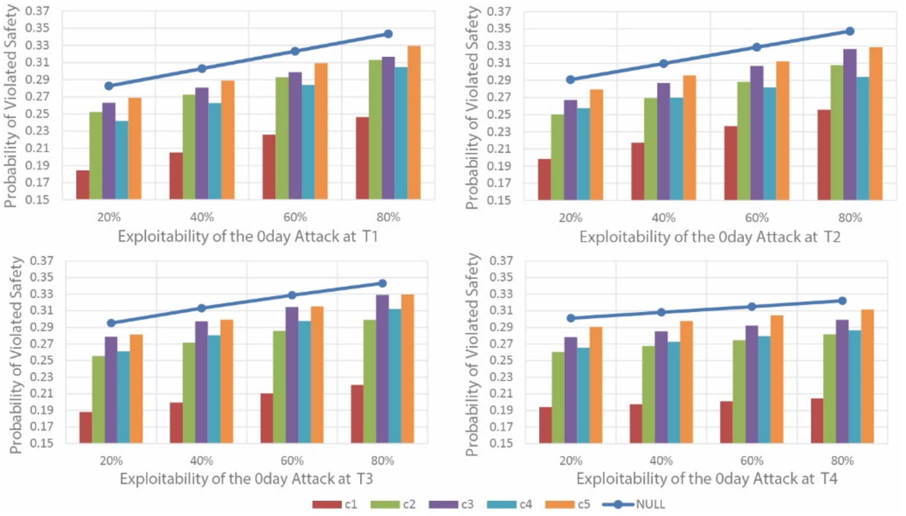


Figure 2. Risk distribution by single controls on each target with a 0day exploit

ICS Security Management

We used a hypothetical example to demonstrate our approach. A simple network is constructed consisting of common types of assets in ICS – a HMI, a workstation, a PLC and a RTU. The four assets are modelled as four target nodes *{T1, T2, T3, T4}* of a Bayesian network. We also selected five common weaknesses *{w1, w2, w3, w4, w5}* and five controls *{c1, c2, c3, c4, c5}* from the *ICS Top 10 Threats and Countermeasures*. These weaknesses are attached to relevant attack nodes between a pair of targets. In this case study, we consistently convert different levels of the CWE attribute "*Likelihood of Exploit*" into certain values. For instance, weaknesses that are identified as "*Very High*" by CWE are set to *0.8*

To model the cyber-physical effects of potential exploits, we consider three key requirements in the example. We use the likelihood of violating the requirement on *control availability* to measure the *risk* in this example.

Results

We construct the corresponding *Bayesian Risk Network* for the case study, and run four trials of the experiment in each of which a zero-day exploit is added to each target. In each trial, different defence controls are individually deployed and the updated risks over scaled exploitabilities of the zero-day exploit (e.g. *20%, 40%, 60%* and *80%*) are computed. In the four charts of Fig.2, the upper curve with markers illustrates the trend of the risk with none control. The mitigated risk by deploying each control are indicated by the coloured bars respectively.

The existence of zero-day exploits generally increases the risk. The zero-day at *T2* is the most threatening one as it brings the greatest increment to the risk, while that at *T4* is the least threatening one. This is because *T2* influences more subsequent nodes than *T4*. The control *c1* is the most effective one to reduce the risk. The tolerance against zero-day has been improved by deploying controls. From Fig.2, at least a zero-day exploit with exploitability *31%* is needed at *T2* to reach the critical level. By applying *c2*, a zero-day exploit with much higher exploitability *74%* at T2 is required to reach the same level of risk.

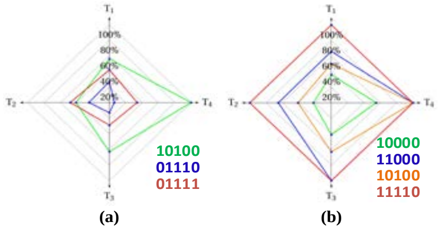


Figure 3: Zero-day Tolerance Coverage

In addition to applying single controls, we also run experiments to find out the most effective combinations of controls (i.e. defence plans). We use *bit vectors* to represent including or excluding a control in a plan. For instance, a plan *10011* indicates to apply *c1, c4* and *c5*. We looked at the impact of each plan on the maximal risk when the zero-day exploit at each target reaches its maximal exploitability, the risk reduction over different targets and tolerance.

We convert the tolerance value at each target into a radar chart as shown in Fig.3. From the Fig.3 (a), we can see that deploying more controls does not always guarantee a larger tolerance coverage. Each control combats different weaknesses that are distributed over different nodes. Defending against more widespread weaknesses would generally produce more risk reduction across the network. Besides, weaknesses near the attack origin tend to have greater impact on the risk of all subsequent nodes, and hence applying defences against earlier attacks are relatively more effective. The tolerances against a zero-day exploit at four targets are expanded at various rates. From the Fig.3 (b), the zero-day exploit at *T4* seems to be the easiest one to be defended, while *T1* and *T2* are the most difficult ones. Three out of the four plans in Fig.3 (b) make the system immune from the zero-day exploit at T4, but only *11110* can protect the system from the zero-day at *T1* and T2.

CYCA 2016

This work was accepted as a regular research paper at the 11th International Conference on Critical Information Infrastructure Security (CRITIS 2016), and presented in the CYCA session at Union Internationale des Chemins de fer (UIC) in Paris.

Tingting was very fortunate to be awarded the CIPRNet Young CRITIS Award (CYCA). We are sincerely grateful to have received this recognition from CIPRNet.

Collaborator

This work was collaborating with Prof. Chris Hankin. Prof. Hankin is Director of the Institute for Security Science and Technology and a Professor of Computing Science at Imperial College London. He was Deputy Principal of the Faculty of Engineering from September 2006 until October 2008. He was Pro Rector (Research) from June 2004 until September 2006. He was Dean of City and Guilds College from 2000-2003. His research is in theoretical computer science, cyber security and data analytics. He leads multidisciplinary projects on developing advanced visual analytics and providing better decision support to defend against cyber attacks.

He is Director of the CPNI/EPSRC Research Institute on Trustworthy Industrial Control Systems (RITICS). He is the immediate past President of the Scientific Council of INRIA, the French national institute for research in computer science and control. He is Chair of the Academic Resilience and Security Community (Academic RiSC) and sits on the ministerial oversight group of the Security and Resilience Growth Partnership and the steering group of the Home Office Security Innovation & Demonstration Centre.

Research Institute in Trustworthy Industrial Control Systems (RITICS)

This work is supported by Research Institute on Trustworthy Industrial Control Systems (RITICS), co-funded by EPSRC and CPNI (EP/L021013/1). The research project is coordinating with other four universalities in the UK: City University, University of Birmingham, Lancaster University and Queen's University Belfast.

Originally designed as isolated networks, ICS have evolved to become increasingly interconnected with IT systems and other, wider, networks and services – particularly as the technologies needed to deliver all manner of computing tasks have converged and proliferated. Whilst offering great efficiencies in terms of setup and running costs this trend has exposed ICS to a growing range of vulnerabilities and the potential for large inter-organisational impacts.

In recognition of these trends *RITICS@Imperial* focuses on five key areas: 1) Investigating the level of connectedness in different scales of organisations to understand the complexity of network topology and interconnections between critical infrastructures; 2) Conducting quantitative studies on the likeliest propagation paths of potential attacks; 3) Predicting ongoing persistent attacks; 4) Evaluating economic consequences of threats for various scales of organisations including an analysis of a loss of key assets and reputation; 5) Finding the most effective interventions to mitigate the risks for ICS.

If you would like to know more about RITICS please visit our website: http://www.ritics.org

If you would like to access this publication and other related publication, please visit Tingting's University profile: https://www.doc.ic.ac.uk/~tl308/

If you would like to know more about the Institute for Security Science and Technology at Imperial College London, please visit our homepage: http://www.imperial.ac.uk/security-institute

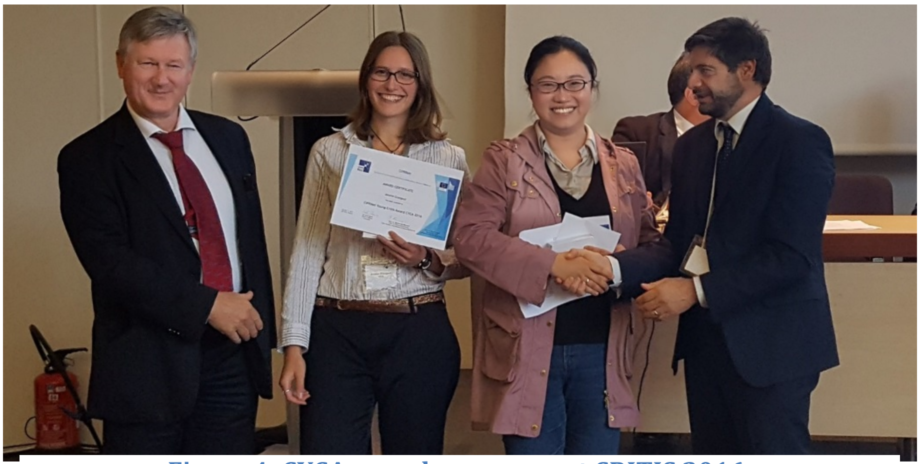


Figure 4: CYCA award ceremony at CRITIS 2016.

This page is intentionally empty.

Ensuring Network Security for Critical Information Infrastructures

Network Security and Resiliency

Network Security

Many critical information infrastructures encompass multi-site connectivity. Metropolitan Area (MAN) and Wide Area Network (WAN) security is deployed at the edge of each site. A viable solution must provide network security and resiliency. This requires overall security and resilience, encompassing device, data plane, control plane and management plane.

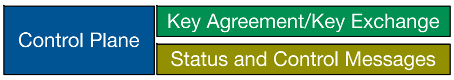
A single weakness in one of those four areas will compromise security and resiliency. A secure device is the foundation. Dedicated network encryption appliances can provide the level of security and resilience required for critical information infrastructures. Multi-purpose solutions embedded in network appliances and virtual appliances tend to fail to provide a secure and resilient device.

Data Plane Security and Resiliency

The data plane carries the network traffic that travels between the sites. This traffic should be encrypted using authenticated encryption with additional authenticated data. AES-GCM with a key size of 256 bit can provide the desired security. Line rate encryption/decryption and forwarding even at small frame/packet sizes (64 bytes) is mandatory to maintain network performance and ensure resiliency against denial-of-service attacks. As multi-site networks are static, a regular change of the session key (data encryption key) is required. AES-GCM uses a counter and for any key a counter state can only be used once. Session key changes must take place without interrupting the network traffic. To protect the network against traffic flow analysis, traffic flow security can be added to the data plane to obfuscate the actual network traffic. There are two different approaches to traffic flow security: (1) Using uniform frame/packet sizes, and (2) injecting synthetic network traffic into the traffic flow. Uniform frame/packet sizes have a negative impact on latency and overhead. Moreover, the supported use case is often limited to point-to-point connections. The injection of synthetic network traffic has a negligible impact on latency and overhead, especially if used in combination with frame/packet grouping, and it can support all network topologies. This method is challenging in terms of making the synthetically injected traffic look indistinguishable. Nevertheless, there is an increasing preference and demand for this approach.

Control Plane Security and Resilience

With most of the focus of network encryption being on the data plane security and resilience, it is easy to overlook the importance of the control plane security and resilience. Data plane encryption requires keys and these are provided over the control plane.

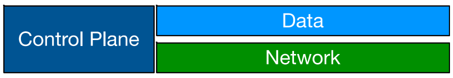


Control Plane

Key Agreement/Key Exchange

Status and Control Messages

Key agreement, key exchange and the transmission of status and control messages must be properly protected to ensure proper operation of the data plane security mechanisms. A successful attack on the control plane will disrupt the network encryption or even the entire network.



Control Plane

Data

Network

This mandates a resiliency against denial-of-service attacks, which can only be provided by direct line-rate

Christoph Jaggi

Christoph Jaggi works as technology, strategy and marketing consultant.

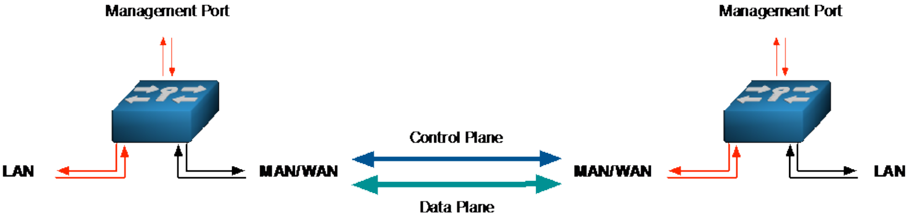
e-mail: cjaggi@uebermeister.com

http://www.uebermeisster.com

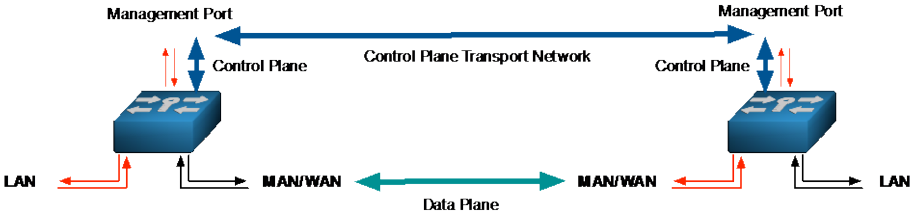
More detailed information is available on the author's website. (see the end of this article)

hardware support for the control plane encryption at the network layer used for the transport of the control plane. Otherwise the result is a cryptographically sound solution that can be easily disrupted.

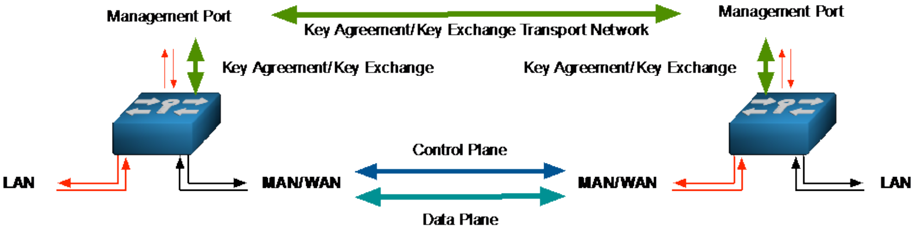
The control plane can be transported in-band together with the data plane. The session key used for the control plane should be different from the key used for the data plane and it must not be the same key as the key encryption key used for encrypting the data during the key exchange.



In some environments it is preferred to separate the transport network for the key agreement/key exchange from the transport network used for the data plane. There are two scenarios: (1) The entire control plane is transported over a separate network, and (2) only the key agreement/key exchange is transported over a separate network, while the status and control messages use the same transport network as the data plane.



The dedicated management port of the encryption appliance is used to hand over the entire control plane or the key agreement/key exchange to the management section of the LAN. Network security and resilience for the transport are provided by an encryption appliance that acts as gateway to the transport network used for the control plane or the key agreement/key exchange. From a security and resilience point of view it makes only sense to separate data plane and control plane, if the security and resilience provided on the alternative transport network is equal or higher than the one provided by the encryption appliance for the data and control plane.


Management Port
Key Agreement/Key Exchange Transport Network
Management Port
Key Agreement/Key Exchange
Key Agreement/Key Exchange
Control Plane
LAN
MAN/WAN
MAN/WAN
LAN
Data Plane

Management Plane

Access to device management must be restricted to the management port. Different access methods use their own private and public keys, such as SSH. Overall security is compromised if the different access methods are not properly secured or if the different management roles are not properly separated.

Using COTS (commercial off-the-shelf) Equipment

Custom-built high-assurance solutions that are certified for "confidential", "secret" and "top secret" tend to come at a high price and suffer from limited availability due to low production volumes, high development cost, high evaluation cost and limited export permissions. They also tend to be engineered for a limited number of scenarios. For most critical information infrastructures, commercial off-the-shelf (COTS) equipment can provide the required protection level at a much lower price point and with much better availability; but only if the COTS equipment fulfils the extended security requirements. Such equipment is normally evaluated and certified for government use for information classified as "restricted". Some of the COTS equipment fulfils the requirements for "confidential" and can be used for such environments if the national authorities agree to such use, even if the basic approval of the equipment is limited to "restricted".

COTS Equipment, Evaluations, Certifications and Approvals

Using COTS equipment for network security can be in many cases a viable option for securing critical information infrastructure. It is however a challenge to find and select a solution that provides the network security and resilience needed for critical information infrastructures. This is caused by the different evaluation, certification and approval requirements and processes. FIPS has issues in terms of the evaluation as overall US security requirements are lower than in some other countries, the evaluation does not go into such detail as source code analysis and security architecture. The evaluation is limited to the cryptographic algorithms and to the cryptographic modules. The latter can be part of a system and thus be dependent on the overall security of such a system. This results in security incidents affecting products that use FIPS-certified cryptographic modules. It is important to take a close look at the evaluation reports for a product to understand what has been evaluated and certified before deciding to use such a product. The result are security incidents affecting products that are FIPS-certified.

For the transport of classified data with a low classification level the U.S. National Security Agency (NSA) thus proposes to use a double encryption (inner and outer tunnel) on different layers when using COTS equipment for multi-site connectivity. The assumption is, that even if the security provided by one COTS equipment is insufficient, the use of a second COTS equipment for adding another layer of encryption could compensate for it. This is only necessary if the COTS equipment used does not provide the required security level and it does not guarantee that the required security level is actually achieved. This approach also has a noticeable impact on latency and overhead. It is much wiser to use COTS equipment that provides the required security levels without needing a second layer of encryption at network level. The German BSI and other national information security agencies use this approach, as it is more cost-efficient and much better suited for networks. A Common Criteria evaluation and certification depends on the profile that is used for the evaluation and the evaluation level. The evaluation depth of profiles can differ substantially. There is at least one US profile for network encryption that equals security and device boundary and makes the assumption that the device is secure. To properly assess the value of a Common Criteria certification it is therefore necessary to look at the profile used, the depth of the evaluation and the detailed test report.

Links to in-depth background:

www.uebermeister.com/files/inside-it/2014_Introduction_Encryption_Metro_and_Carrier_Ethernet.pdf
www.uebermeister.com/files/inside-it/2014_Evaluation_Guide_Encryptors_Carrier_and_Metro_Ethernet.pdf
www.uebermeister.com/files/inside-it/2015_market_overview_Ethernet_encryptors_for_Metro_and_Carrier_Ethernet.pdf

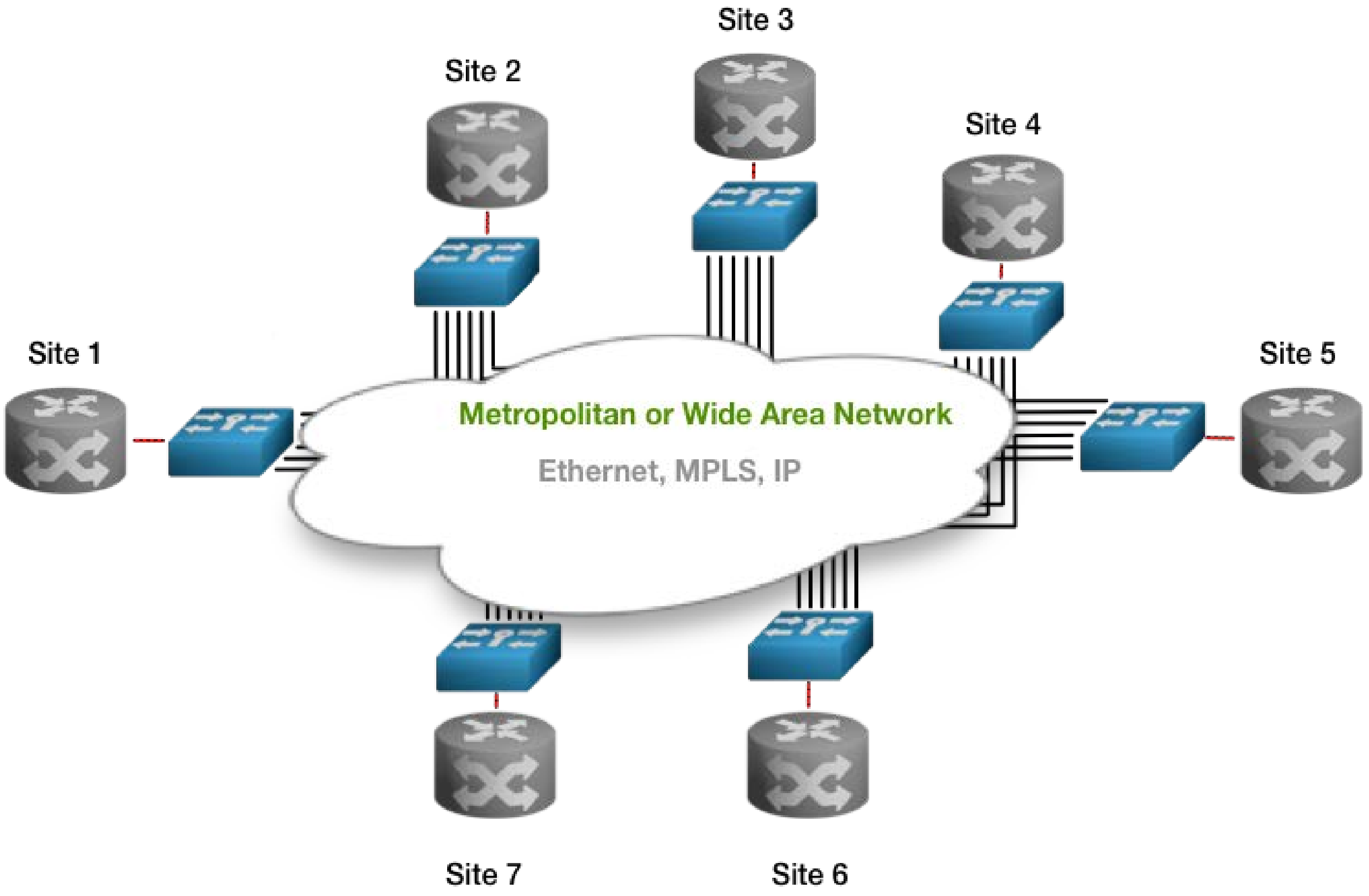


Figure: Multisite Connectivity MAN-WAN

This page is intentionally empty.

A taxonomy of tools for CI Security Testing

Critical Infrastructure Security Testing must not be overlooked.

Introduction

The fundamental objective of Critical Infrastructure Protection is the development, implementation or enhancement of Security, both in its physical and logical / cybernetic aspects since they are both inherent master pieces of such systems, as it is represented in Figure 1. In particular, the management of Cybersecurity of the components of Infrastructures, (equipment, networks and systems in which the information is logged), whether critical or not, is a fundamental task. It is therefore fundamental the identification and valuation of assets of an organisation, the identification of threats and vulnerabilities, the estimation of their frequency of occurrence and associated impacts, for the calculation of risks that both individual devices and Industrial Control networks as a whole can suffer. In this sense, it has to be taken into account that the concept of Security of the information systems that support these infrastructures has, as main objective, to guarantee its reliability. Particularly, control automation & supervision, the integrity of the information handled, and the availability of such systems.

This focus leaves in the background aspects such as those related to confidentiality of information (which, on the other hand, they must be observed carefully in particular scenarios (e.g., telemetering and remote management.)

SCADA (Supervisory Control And Data Acquisition) is a software system capable of communicating with different devices and exercising actions on them from a management panel. This software allows control from industrial automation networks to manage and interpret telemetries belonging to machines in production.

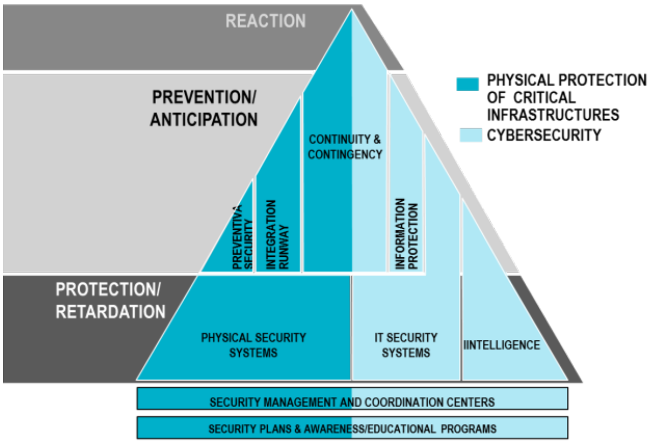


Fig 11.CI Physical & Logical Security sides

The diversity and convenience provided by SCADA software has spread its use in the industrial field, being its role to control most of the critical infrastructures of the countries.

As in less critical systems, the fact that a software is in charge of the management of most relevant assets, makes it an appetizing target for cybercriminals or adversary governments. The first known Advanced Persistent Threat (Stuxnet) was directed against the SCADA system of an Iranian nuclear enrichment plant and gained control of its system through the monitoring and manipulation of plant's processes.

Despite Stuxnet demonstrated that such type of critical systems is vulnerable, there are still in place SCADA systems that remain exploitable. The reason is that traditionally, the administrators of this type of systems believed that they were secure because the systems were not connected to the internet and their code was kept internally hidden. This belief also released them from applying proper security mechanisms. Fortunately, nowadays the "security by obscurity" principle is defeated by Kerckhoff's second principle, i.e., "The security of the system should not depend on its design being a secret." Moreover, the uttermost importance of the security of national critical infrastructures is recognised such that is mentioned, for instance, in the Cyber

Marina Egea

Dr. Marina Egea is the Head of the Tiger Team, Cybersecurity Operations at Minsait (by Indra).

e-mail: msegea@minsait.com

Luis Miguel Cerrato (left)

is Cybersecurity Analyst in the Tiger Team at Minsait, and GCIH, GIAC Certified Incident Handler.

Jose Boix a (right)
is in favor of offensive security is a security analyst of the Tiger Team of Minsait (Indra)

Alejandro Espinosa)

is a Cybersecurity Analyst of the Tiger Team of Minsait (Indra)

Defence pledge published by NATO after the Varsovia summit in 2016.[1]

In this paper, we focus on highlighting the importance of the logical security of SCADA systems and how it can be tested. In particular, we provide a taxonomy of existing tools to perform penetration tests on SCADA systems. We do not intend to build here an exhaustive list but, at least, to differentiate those analysis tools which are SCADA-specific from those "usually employed" security testing tools which are still valid to perform pentesting tasks for SCADA systems.

Selected tools have been classified according to the following categories:

- Information gathering
- Traffic analysis
- Vulnerability scanning
- Vulnerability exploitation

Also, we have included Linux distributions which are oriented to help testing the security of SCADA systems.

In the following sections, we will first describe the different components that are usually found in SCADA systems. Then, we will explain the different categories of tools that exist and their role in the context of a pentesting process.

SCADA components

In order to understand what is involved in a pentesting process of a SCADA system, we describe here briefly its conceptual components.
SCADA systems allow to transmit individual device status, manages energy consumption by controlling devices, allow direct control of power system equipment and even chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, etc.

A SCADA system usually has the following components:

- SCADA WorkStation: which is a device operated by a human operator that allows to command a central SCADA console.
- HMI (Human-Machine Interface): It's usually a piece of software and hardware that allows the human operator to monitor the state of the processes which are under control, to modify control settings, manually override auto-control operations, etc. Namely, the HMI is the human-friendly interface that provides access to the SCADA workstation.
- Data Historian: This component is in charge of gathering and storing information from the system with the aim of facilitating accurate post-analysis.
- SCADA Server MTU (Master Terminal UNIT): This component is a device that issues the commands to the Remote Terminal Units (RTUs) which are located at remote places from the control so as it can gather the information that is distributed, processes and displays it.
- RTU (Remote Terminal Units): These are the connecting sensors which report or actuate according to the local information that they obtain from the supervisory systems.
- PLC (Programmable Logic Controller): This component automatically performs the main site control process which controls the operation of industrial equipment.

The SCADA server MTU and the RTU or PLCs are in communication through specific SCADA protocols. The main ones are i) DNP3 (Distributed Network Protocol)[2] used for communications between the MTU and RTU through port 20000 TCP/UDP; and ii) ModBUS[3] which is typically used for SCADA-style network communication between devices implementations over serial TCP/IP (standard port 502 TCP). In a nutshell, RTU collects data from sensors which sends to the MTP using either DNP3 or ModBus protocols. The main drawback of these protocols is that they were not designed having security in mind (no authentication, no encryption, no validation).

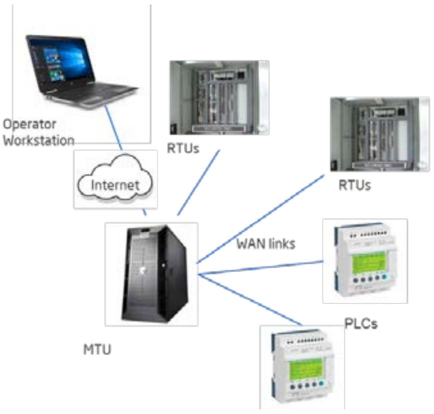


Figure 12. SCADA Industrial Control System Concept

Attack vectors for SCADA systems

Once we have described the conceptual architecture of a SCADA system, we will review some attacks vectors that may impact such architecture.
Taking into account the weakest link in the security chain, we have to say that Administrators and Operators many often have very few security knowledges.
From SCADA protocol descriptions we infer that SCADA systems share the same threats to any other TCP/IP-based system. Also, we have to mention that PLCs and RTUs usually use vendor-specific network and protocols.
Since many SCADA systems are incorporating web application interfaces to allow remote access by administrators, widely known web vulnerabilities must be considered. Thus, some of the following attacks which particularly affect to availability and integrity of the systems might succeed:

- Denial of Service against the MTU, RTU or PLCs.
- SQL injections to delete or modify data history, which would lead to loss of operations.
- Infect the system with a piece of malware, e.g., a Trojan to take control or spy the behaviour or industrial sensitive information of the system.
- Vulnerabilities known on communication protocols including non-secure design or wireless communications vulnerabilities, e.g., negotiated keys or full communication hijacking.
- Exploit commonly known web vulnerabilities[4]
- Scan the network topology and associated technologies to search for non-updated operating systems, open ports, etc.

In summary, we need to be aware that at the end of the day we are

[1] http://www.nato.int/cps/en/natohq/official_texts_133177.htm

[2] https://standards.ieee.org/findstds/standard/1815-2012.html

[3] http://www.modbus.org/specs.php

[4] https://www.owasp.org/index.php/Top_10_2013-Top_10

dealing with devices, operating systems, protocols over TCP, databases and firewalls. It is known that security mechanisms to mitigate known weaknesses already exist, however, the deployment of these mechanisms in SCADA architectures is not always that feasible.

Pentesting tools for SCADA systems

The phases of a pentesting for a SCADA system are the same that are used for any other IT system. We illustrate them in Figure 3 (starting with the Information gathering phase).

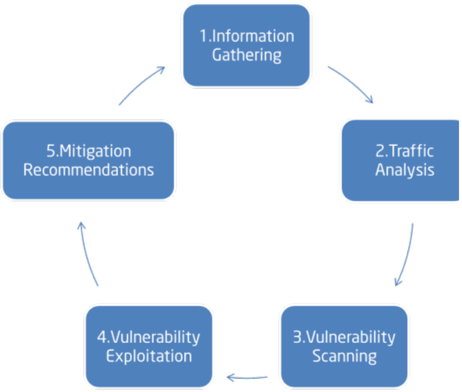


Figure 13. Pentesting phases

1. Information gathering

The aim of this phase is to gain as much information as possible about the target system.

- **Shodan:** Many control panels of SCADA systems are connected to the internet to allow remote control. Remote control is very convenient for system administrators, but opens an attack vector that can be exploited to manipulate the system. Shodan is a search engine capable of finding systems exposed on the internet, performing a comprehensive scan and indexing of the information. It permits to know if a system is exposed to the Internet being classified as vulnerable. Shodan offers a very versatile API that is exploited by cybercriminals through bots, able to re-compile the information needed to later perform brute force attacks. In order to determine that a system on which a pentesting is to be performed is safe, the first thing to check is whether the system appears in Shodan and if the access to it is vulnerable. [https://www.shodan.io]

- **ZoomEye ICS:** ZoomEye is a search engine that allows grabbing data from publicly exposed devices and web services. The ZoomEye ICS is mainly focused on finding ICS (Industrial Control System). It offers the chance to perform easy custom searches based on a list of protocols and products available. Moreover, more specific searches can be performed through its web or with its public API. Search filters are available to get accurate results, like application, software, product, version, device, Operating System, country or IP, among others. [http://ics.zoomeye.org]

- **Nmap:** Nmap is an open source tool for network discovery and services and ports scanning. Each open port is a possible access to the system, hence a port scanning is a technique commonly performed by any attacker who want to exploit a system (not only a SCADA system). [https://nmap.org/]

  - **ICScanner:** ICScanner is a tool used for enumeration of devices on SCADA network environments. It supports reconnaissance of many SCADA protocols, i.e. Modbus serial, Modbus TCP, DNP 3, Profinet, Siemens SIMATIC Step 7, etc.. [https://github.com/0xICF/ICScanner]

  - **PLCScan:** PLCScan is a tool that allows scanning PLC devices over s7comm or Modbus protocols.

    [http://www.digitalbond.com/tools/plcscan/]

2. Traffic analysis

The main goal of traffic analysis in a pentesting process is to identify certain patterns after getting information about the network flow.

- **Wireshark:** Wireshark is a network protocol analyser. It allows live monitoring and saving traffic captures for further analysis. Wireshark functionality in SCADA traffic analysis can be increased through the use of plugins like Siemens s7 Wireshark dissector. [https://sourceforge.net/projects/s7commwireshark/, https://www.wireshark.org/]

- **Scapy:** Scapy is a packet manipulation program, available as a Python library as well as a CLI (Command Line Interface). It allows any kind of operation with network packets, even at bit-level. Useful for industrial environments thanks to its capability of working with custom, specific protocols. Feature that makes it especially suitable for the analysis of SCADAs' protocols. [http://www.secdev.org/projects/scapy/]

3. Vulnerability scanning

Vulnerability scanning is performed to identify operating systems, services and vulnerabilities present on a target system. Several commercial and open source scanners allow scanning SCADA systems in order to identify certain vulnerabilities.

- **Nessus:** Nessus is a cross platform vulnerability scanner. It is a commercial tool that checks whether a system is vulnerable or not through a set of plugins written in NASL (Nessus Attack Scripting Language). Reports can be generated following the severity of the vulnerabilities found. [https://www.tenable.com/products/nessus-vulnerability-scanner]

- **OpenVAS:** OpenVAS (Open Vulnerability Assessment System) is an open source framework of services and tools used for vulnerability scanning and vulnerability management. Given that OpenVAS is a fork of Nessus, some similarities exist between them. OpenVAS checks if a target is vulnerable through a scanning using a set of plugins written in NASL. After the scan has finished, the vulnerabilities are classified by its severity. **[http://www.openvas.org/]**

- **Splonebox:** Splonebox is an open source network assessment tool. One of its main features is the availability of custom plugins, including some specific to analyse industrial communication protocols. [https://splone.com/sploneb ox/]

Vulnerability exploitation

- **SCADA Shutdown Tool:** It allows the pentesters to detect and interpret all the controllers of the system and later modify their registers in order to explore the limits of the system. [https://github.com/0xICF/SCADA ShutdownTool]

- **PLCinject**: With the PLCinject tool you can enter code inside the devices commonly known as PLCs. One can test if they can be altered by certain vulnerabilities. [https://github.com/SCADACS/PLCinject]

- **Metasploit**: Metasploit is an open source penetration testing software. It is written in Ruby and gives multiple options for different phases of a pentesting, not only for the vulnerability exploitation phase. Its modularity is a great advantage given that different modules can be added to increase its functionality. In terms of SCADA exploitation, a set of modules have been developed to take advantage of vulnerabilities in different products and vendors. [https://www.metasploit.com]

- **SCADAPASS:** It allows brute-force attacks on SCADA systems based on dictionaries containing commonly used default passwords. Although the security of these systems is critical, it is surprisingly often to find weak or default passwords protecting the access. [https://github.com/scadastrangelove/SCADAPASS]

Linux pentesting distributions (SCADA oriented)

Although a number of tools exist to support a pentesting process, configuring them properly for a SCADA system is not an easy task. Because of this reason tailored pentesting distributions for SCADA systems were created. The main ones are:

- **Moki Linux:** a distribution of pentesting tools to analyse SCADA systems. It can be used to extend Kali Linux OS, so it is not necessary to install an extra operating system.
- **Quickdraw:** SCADA Snort Rules.
- **PLC Scan:** PLC scanning tool.
- **CoDeSys exploit:** Remote buffer overflow exploit for CoDeSys Scada web-server.
- **Modscan:** Application designed to operate as a MODBUS Master device.
- **Siemens s7 metasploit:** Auxiliary module of metasploit for Siemens S7
- **Siemens s7 wireshark dissector:** plugin for Wireshark to detect Siemens S7 traffic

[https://github.com/moki-ics/moki]

- **SamuraiSTFU:** it is the most famous distribution for pentesting on SCADA. It includes a great set of tools and it is capable of emulating SCADA systems so that a laboratory for testing purposes can be created. [http://www.samuraistfu.org/]

After reviewing these phases and tools, we notice that, in summary, for SCADA systems we can audit:

- Network Infrastructure: router configurations, switch tables, DNS tables, traffic analysis.
- Host operating systems: version, patch level, password strength, authentication and authorisation policies, and access points.
- Applications: ports and services, remote access, protocols.
- For PLCs and RTUs: Review patch levels, password quality, packet sniffing (incl. wireless). Check whether physical attacks are possible.
-

Conclusions

Traditional approaches to “security by obscurity” in SCADA systems are not sufficient to protect this type of systems nowadays. Especially since common hacking techniques can be employed to attack these systems, as we have reviewed in this article. In order to ensure a good level of security in SCADA systems, the following mechanisms should be taken into account:

- Network segmentation or the creation of DMZs to separate privilege levels, access to data, etc.
- Robust communication protocols.
- Firewalls properly configured and without making dangerous exceptions (as often we find while auditing systems).
- Proxy serves to mediate between the traffic originated in the internet and internal traffic.
- Effective security policies which coordinate physical and logical security as well as management of systems by the operators.

Security training for the staff who needs to operate the system which is essential for preventing attacks or the materialisation of misuse cases.

iHoney Project: New concepts in honeypot development for ICS cybersecurity

The ever-increasing need for a realistic honeypot calls for a two-sided approach: IT and OT Engineers working together.

Abstract

Honeypots are an important tool that can be deployed for critical infrastructure protection. In addition to this, intelligence gathered from realistic honeypots exposed to the Internet is a useful input for the development of specific security capabilities. IT and OT systems present relevant differences that have to be accounted for when designing, implementing, deploying and running an ICS honeypot. This article focuses on these specific issues and presents the results of the research carried out by the S2 Grupo ICS Security team, highlighting the basic principles and the insights gained from the iHoney R&D project.

Introduction

Many critical infrastructures (CI) depend on industrial control systems (ICS) for their normal operation. ICS security is, thus, becoming a major concern in critical infrastructure protection (CIP). Since Stuxnet was reported in 2010 [1], ICS Security has evolved into a brand new field for cyber security companies and the rest of the stakeholders. As such, a new body of knowledge and tools (software, hardware…) suitable for industrial environments are being developed and deployed. There are two basic requirements that such a tool should meet:

- Use of technical auditing software should not, under any circumstances, disturb or disrupt the regular operation of the infrastructure in which it has been deployed. Limits to this requirement shall be determined by the owner of the IC assets.
- When talking of cyber security monitoring systems (i.e. IDS/IPS) this requirement should be extended to guarantee that the equipment and network connections deployed for monitoring purposes do not weaken the security perimeter by opening new vectors in de CI, even if the probes are compromised by malware or attackers.

However, for the time being, most of the tools available in the market are a mere application of the IT cyber security methodologies, practices and software into the ICS environment. This is the result of a state of mind that regards ICS as a bunch of IT components, failing to grasp the essential point: even if these systems are becoming more and more similar to standard IT environments (Linux/windows OS, TCP/IP communications, servers, workstations, etc.), the people behind and the way they are operated by them are totally different.

So we need new tools to be developed specifically for ICS protection, and this can only be accomplished with sound knowledge of this field, as well as with a clear awareness of IT/OT differences. This has been the main objective of the iHoney project, which also included the development of an ICS honeypot as a means of gathering first-hand information on the kind of threads a CI is exposed to. This has shown to be a valuable source of intelligence on: typology of attacks, frequency, strategies, tools… which in turn has complemented the experience and knowledge of the interdisciplinary team of process, security and communications engineers that have been involved in the project.

The honeypot is one of the project's most innovative milestones, because beyond the immediate practical applications summed up in the aforementioned purposes, its development has been intended to provide an answer to the following questions:

- Who is interested in causing damage to a CI? How many of these individuals/organisations are out there?
- Do they have the skills and motivation required to perform successful attacks?
- What are their goals?
- And, above all:

Oscar Navarro

Óscar Navarro is an electrical engineer. He has a wide experience in SCADA and ICS systems and worked for engineering and construction companies before joining S2 Grupo. Currently he leads the S2 Grupo ICS cybersecurity team.

He is an expert in anomaly detection in SCADA systems and ICS security management.

e-mail: onavarro@s2grupo.es

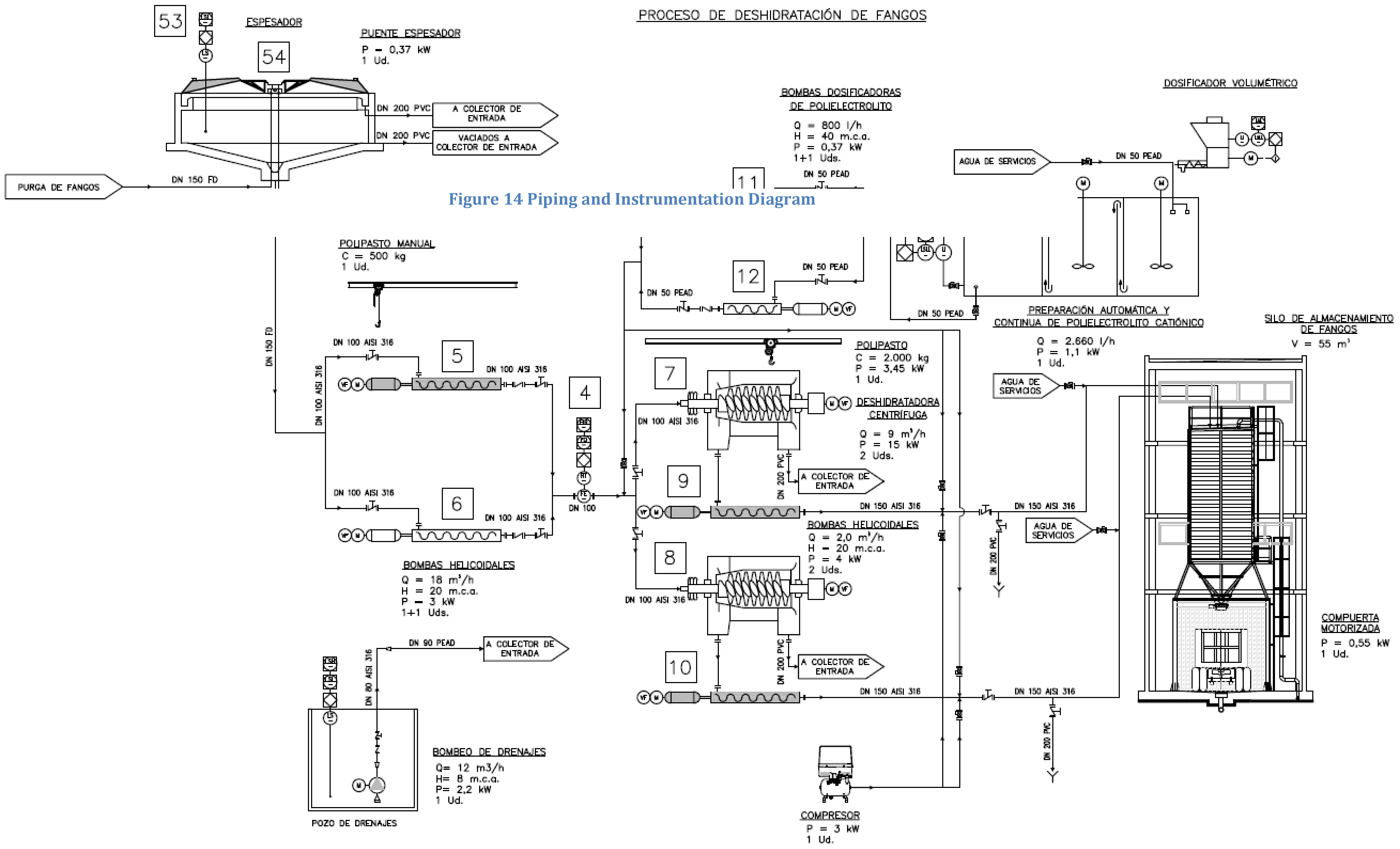


Figure 14 Piping and Instrumentation Diagram

Do they have skills and knowledge on ICS (design, operation, etc.) good enough so as to plan and execute sophisticated attacks resulting in damage for physical equipment and processes?

Building a realistic honeypot

A review of the state-of-the-art of ICS honeypots carried out during the initial phases of the project (see for example [2]), showed that there were common pitfalls that should be avoided right from the start. A brief list of the most relevant among them follows:

- ICS honeypots tend to be oversimplistic when it comes to industrial processes. The reviewed cases didn't match any realistic process and, what's more, consisted only in software simulations running in a computer which had some common ICS protocols ports open.
- Physical equipment was lacking or scarce. A typical configuration was that of a single PLC (Programmable Logic Controller) communicating with a computer.
- Typically, ICS honeypots are too simplistic to allow any complex interaction with a potential attacker, thus preventing any sophisticated actions from taking place.
- A tendency to over-promote the honeypot on the Internet as a means to enhance its visibility and attract attackers, complemented with just too evident vulnerabilities put in place 'to let the bad guys in'.

Summing up: Attackers with a sound knowledge on industrial processes and ICS technology are not likely to be deceived by the reviewed honeypots, which look far too much IT-inspired. The most probable 'victims' of these honeypots are casual or conventional attackers, biasing the data on malicious activity obtained in this way.
In order to answer the questions asked above, a brand-new approach is required. So, right from the onset of the design activities, some important basic premises were stated:

- The simulated infrastructure must be a realistic one, comparable to those a modern society relies upon.
- The honeypot must be realistic enough so as not to raise suspicion, not only in casual or IT aimed attackers, but also in personnel with experience in ICS and industrial processes.
- The honeypot must allow for a degree of interaction high enough for complex attacks to take place. More precisely: in order to keep an attacker engaged for as long as possible, the system must show some kind of response to malicious actions. In fact, this action/reaction pair should match reality as close as possible. For example, if an attacker expects, as a result of his actions, a pump to stop, flow through the corresponding pipe should drop to zero smoothly, just as the real thing would do.
- Contrary to IT honeypots, cyber security monitoring must be almost invisible. The reason is that currently most SCADA systems lack complex monitoring infrastructures and an attacker would find an IDS in operation suspicious.

The iHoney honeypot (*i* stands for *industrial*) has been designed, built and operated on these principles. The project was planned and executed just as the ICS for an actual infrastructure would have been. The main milestones were:

1. Fake infrastructure design. For this project, a water treatment plant was selected. The design involved treatment process definition and associated calculations, equipment selection (pumps, blowers, instrumentation...). Summing up: all the requirements to design an actual plant like the one selected.
2. Automation and ICS system design: controllers, communication buses and protocols, architecture, etc.
3. Graphic interface development for the SCADA HMI interface (Human-Machine Interface). This task was carried out in a realistic manner because of the blueprints already designed in the previous phase. In addition to the plant layout, other common screens were also developed: alarms, historian, etc.
4. Physical processes modelling by means of logical and mathematical expressions that involve the considered state variables. This is the core of the process simulator.
5. Cyber security monitoring subsystem design: architecture, software, communication networks, connection to the Internet, etc. A set of hardware and software was deployed for monitoring purposes. By employing S2 Grupo CERT technology, generated alerts were directed towards the CERT to be managed by S2 Grupo specialists.
6. ICS system implementation. ICS hardware was deployed and programmed as an actual system would have been. This task was accomplished with help from a specialised contractor.

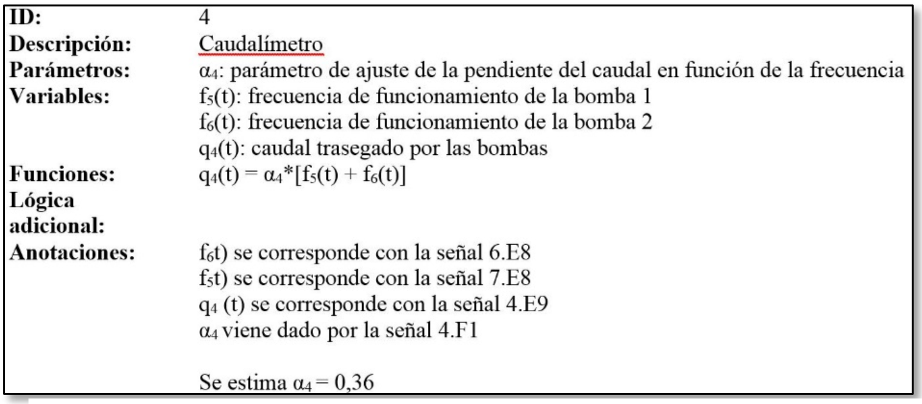
So, the iHoney ICS honeypot consists of three differentiated modules:

- The ICS system, composed of an SCADA server/HMI, a control network of PLC that regulates the several processes and the associated industrial communication protocols.
- The simulation system, that evaluates the process status variables in real-time and interacts with the ICS inputs (legitimate or not) generating the appropriate outputs (as the actual system would). This system provides 'plant operators' with an interface that enables them to interact with the physical system: physical buttons and switches to operate manually, drives and panels, local interfaces to manually change setpoints, etc.
- The cyber security monitoring infrastructure.

Overcoming challenges

During the project execution, some important issues have required special attention. Here follows a list of the most relevant:

- Some compromises were necessary to ensure, on the one hand, a realistic enough fake system and, on the other hand, an adequate level of complexity. So some simplification has been made in the mathematical relations between physical variables. Of course, there is a limit to this imposed by the need to keep the system simple but realistic.
- Choosing an infrastructure prone to be cyber-attacked. This is kind of a goldilocks problem: attractive enough but not so notorious that it raises suspicion. For example, choosing a big airport may not be such a good idea as it seems: it is difficult to simulate in a realistic manner; it is not likely that serious attackers take a singular infrastructure overexposed on the internet for the real thing; the possible impact of a casual attack on such a notorious thing may dissuade most individuals.



ID:	4
Descripción:	Caudalímetro
Parámetros:	α_4: parámetro de ajuste de la pendiente del caudal en función de la frecuencia
Variables:	$f_5(t)$: frecuencia de funcionamiento de la bomba 1 $f_6(t)$: frecuencia de funcionamiento de la bomba 2 $q_4(t)$: caudal trasegado por las bombas
Funciones:	$q_4(t) = \alpha_4*[f_5(t) + f_6(t)]$
Lógica adicional:	
Anotaciones:	f_6t) se corresponde con la señal 6.E8 f_5t) se corresponde con la señal 7.E8 q_4 (t) se corresponde con la señal 4.E9 α_4 viene dado por la señal 4.F1 Se estima $\alpha_4 = 0,36$

Figure 2: Mathematic modeling function example

- Implementing the honeypot so as to render the simulation module invisible. One of the key factors to achieve this is the use of 24 V DC signals in the communication between the ICS and the simulating module.
- Simulating the response of physically driven relays built in some actual equipment (for example, overheat emergency switches in submersible pumps) and safety interlocks.
- Developing a high-quality set of layout blueprints as a template for the SCADA HMI interfaces.
- Integrating the simulation module and the ICS one accounting for the tight requirements of ICS systems regarding real time processing, stability and network latency.
- Customizing the monitoring system to conceal the generation and exfiltration of information on attacks (logs, etc.)

Once the design and construction stages were over, the iHoney honeypot entered the operational phase. A maintenance and operation plan was designed that included activities such as:

- Scheduled maintenance stops.
- Scheduled operations (on a daily, weekly and monthly basis).
- Scheduled equipment failure simulation.

This plan was put in place to keep the infrastructure 'alive', as any potential attacker would expect from an actual plant.

Lessons learned

The iHoney was exposed to the Internet for over 1.5 years while S2 Grupo ICS cyber security team detected, analysed and recorded all the malicious activity taking place in the system.

When the operational phase was over, a thorough analysis of the compiled data was carried out, and in fact, is still in progress. However, some important lessons learned can be highlighted:

- Most of the registered attacks are automated and are directed against the IT components of the SCADA system. Now that Industry 4.0 is the new paradigm, and it is becoming harder to draw a line between IT and ICS systems, the cyber security of these systems must be approached globally.
- When properly configured and updated, it is not easy for attackers to get into the system. So, the importance of a good security management can hardly be overstated. In fact, this is prompting attackers to explore other ways in, such as social engineering (see next paragraph).
- The iHoney project was strongly technology-oriented. However, a certain number of attacks were directed against the operators behind the machines. Since human operators are the weakest link in the cyber security chain, this is a factor that any future (ICS) honeypot must account for. iHoney is very realistic from a technical point of view, but lacks the corporate and human components. This is an important insight for future experiences.

References

[1] *Gregg Keizer, "Is Stuxnet the 'best' malware ever?". InfoWorld, 16 September 2010.* *http://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html*

[2] *Kyle Wilhoit. "Who's Really Attacking Your ICS Equipment?". TrendMicro, 2013.* *https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf*

.

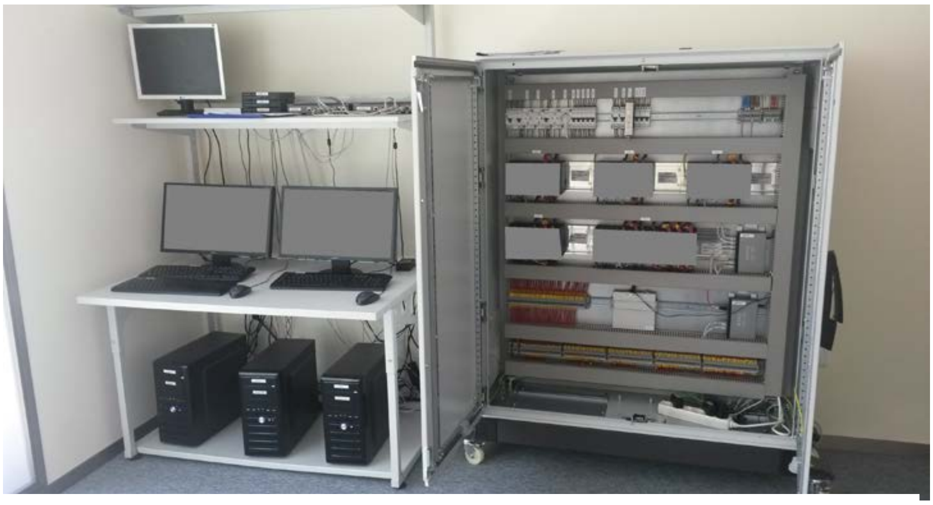


Figure 3: SCADA real equipment

CRITIS 2016: Conference Highlights

The 11th International Conference on Critical Information Infrastructures Security (CRITIS) took place in Paris, France, on 10–12 October 2016

The 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016) was held at UIC Headquarters, Paris, from 10 to 12 October 2016.

The conference was organised by the International Union of Railways (UIC) with co-chairing support from Campus Bio-Medico University of Rome (UCBM) and Ecole des Ingénieurs de la Ville de Paris (EIVP). The conference provided a global forum for constructive exchanges between experts from governments, regulators, scientists, academics, service providers, and other stakeholders on topics concerning Critical Information Infrastructure Security and Critical Infrastructure Protection at large.

10-12 October 2016
UIC HQ Paris, France
CRITIS
2016
11th International Conference on Critical Information Infrastructures Security

Key figures

CRITIS 2016 marked the beginning of the second decade of CRITIS. The participants and speakers came from fourteen European countries (Belgium, France, Germany, Italy, Lithuania, Luxemburg, Portugal, Romania, Russia, Slovenia, Spain, Switzerland, the Netherlands, United Kingdom) and six countries from other continents: Morocco, Japan, Singapore, South Africa, South Korea, and USA. The conference participants had the opportunity to enjoy an excellent technical program, at UIC Headquarters, in the very heart of Paris, between the banks of the Seine and Champs de Mars, only a foot away from the Eiffel Tower.

Following the call for papers, we received 58 high-quality submissions, which were thoroughly reviewed by the expert members of the International Programme Committee (IPC). Out of the total submissions, 22 papers were accepted as full papers with eight further papers accepted as short papers offering work in progress.

Programme summary

The 2.5-day technical programme consisted of 30 papers grouped into sessions that included topics on: innovative responses for the protection of cyber-physical systems, procedures and organisational aspects in C(I)IP and advances in Human Factors, decision support, and cross-sector C(I)IP approaches.

As in previous years, invited keynote speakers and special events complemented the technical programme. The four keynote interventions were the following:

Dr Arturas PETKUS (NATO Energy Security Centre of Excellence, NATO ENSEC COE, Lithuania) talked about CEIP and Energy Security in Perspective of NATO (CIPRNet Lecture) see https://enseccoe.org/en .

Commander Cyril STYLIANIDIS (Ministry of Interior, General Directorate for Civil Protection and Crisis Management, France) provided an overview of "The Crisis Interministerial Cell (CIC), the French tool for interministerial level crisis management", illustrated with recent examples from France.

Mr Kris CHRISTMANN (University of Huddersfield, Applied Criminology Centre, UK) gave an overview of the "Findings from the PRE-EMPT Project: Establishing Best Practice for

Grigore M. Havârneanu

Traffic and Transport Psychologist with a PhD in Social Psychology. Research Advisor within the International Union of Railways' Security Division

Programme Chair of CRITIS 2016 and new member of the CRITIS Conferences Series Steering Committee

e-mail: **havarneanu@uic.org**
www.critis2016.org

Reducing Serious Crime and Terrorism at Multi-Modal Passenger Terminals (MMPT)".

Dr Paul THERON (Thales Communications & Security, France) presented "A way towards a fully bridged European certification of IACS cybersecurity", related to the work of DG JRC's ERNCIP Thematic Group on IACS cybersecurity certification.

The PDF files of the presentations can be found on the CRITIS2016 website:

www.critis2016.org/programme

Furthermore, in continuation of an initiative first taken up at the 2014 CRITIS, the conference also included an award for young researchers in the area (the 3rd CIPRNet Young CRITIS Award), seeking to recognise and encourage the integration of talented younger researchers into the community. Six of the accepted papers were presented during a dedicated CYCA Session. The winners were Amalie Grangeat (CEA France) and Tingting Li (Imperial College London, UK). This award was sponsored by the FP7 Network of Excellence CIPRNet.

CRITIS 2014 and 2015 proceedings have been published in Springer LNCS 8985 and 9578 respectively.

CRITIS 2016 proceedings are currently with Editor aiming for a release in Springer LNCS in the second quarter of 2017.

In addition, some of the CRITIS 2016 participants had the opportunity to attend (within the limited number of places) an associated event organised at UIC the next day after CRITIS. The IMPROVER Workshop: "Meeting public expectations in response to crises" – addressed an important topic in C(I)IP, aiming to discuss how infrastructure operators meet these requirements today and how this can be improved.

Acknowledgements

It is our pleasure to express our gratitude to everybody that contributed to the success of CRITIS 2016. In particular, we would like to thank the General Chair Jean-Pierre Loubinoux (UIC Director-General) and the local UIC hosts Jerzy Wisniewski (Fundamental Values Department Director) and Jacques Colliard (Head of UIC Security Division) for making CRITIS possible at UIC Headquarters in Paris.

Further, we would like to thank the members of the Programme Committee who did a tremendous job under strict time limitations during the review process. We also thank the CRITIS 2016 Co-Chairs Prof. Roberto Setola (UCBM, Italy) and Hypatia Nassopoulos (EIVP, France) and the members of the Steering Committee for the great effort and their continuous assistance in the organisation of the conference. We are also grateful to the Publicity Chair and to the UIC Communications Department for their excellent dissemination support, and to the CIPRNet Network which was an active supporting community.

We are equally grateful to the keynote speakers who accepted our invitation and agreed to round off the conference programme through presentations on hot topics of the moment.

Finally, we thank all the authors who submitted their work to CRITIS and who shared their new ideas and results with the community. We hope that these ideas will generate further new ideas and innovations for securing our critical infrastructures for the benefit of the whole society.

The next edition of the International Conference on Critical Information Infrastructures Security

CRITIS 2017

will be hosted in Lucca, Italy between 9 and 13 October, 2017

to continue the successful CRITIS conferences series.

www.critis2017.org

CRITIS 2017: 12th International Conference on Critical Information Infrastructures Security – Call for Papers

CRITIS 2017

The 12th edition of CRITIS will take place at IMT in Lucca, Italy, October 9–13, 2017

In 2017, the International Conference on Critical Information Infrastructures Security will celebrate its 12th anniversary. This year edition continues the efforts to bring together scientist, experts, policy makers and professionals from academia, industry and govern-mental organisations engaged in the field of the security of critical (information) infrastructure systems.

As in previous editions, invited keynote speakers and special satellite events will complement a programme of original research and stakeholder contributions. The conference provides a bridge for the different research communities and disciplines involved in the C(I)IP while encouraging discussions, conceptualisations and modelling, especially when based on multi-disciplinary approaches.

> CRITIS 2017 will push forward the tradition of presenting original research, whilst exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP). To this purpose special efforts will be devoted to foster the dialogue with stakeholders and assess a common language and vision.

Conference Organisation

CRITIS 2017 will be organised according to six different topics which correspond to six virtual sessions.

CS “Cyber Security”: Modern society and especially the CI’s are experiencing continuous changes toward the smart paradigm. Each device is nowadays endowed by an intelligent controller while being part of a complex system controlled by sophisticated and increasing smart electronics.

> Submission of papers:
> **June 2-nd 2017**
>
> Registration open:
> **July 1-st 2017**
>
> Acceptance Notification
> **July 15-th 2017**
>
> Camera-ready papers:
> **September 1-st 2017**
>
> CRITIS Conference
> **October 9/11-th 2017**
>
> CRITIS Satellite Workshops
> **October 12/13-th 2017**

In other words, countries at elevated level of development are following a path toward the advent of “smart society”. Smart grids, smart water supply, smart cities do represent the eventual evolution of our present infrastructures. Recent attacks to CIs via the cyber side demonstrate how thin is the boundary between the cyber and the physical world. For these reasons, cyber security plays a central role in any complex human activity, especially in CIP. In particular, enhancing the cyber security of SCADA systems or designing and building intrinsic fault tolerant automated adaptive systems by new generation cyber controllers represent extremely interesting issues.

TR: Transports. Following the positive experience of the past edition at UIC, a specific session will be devoted to transports. Railways, highways and their integration represent one of the most dwelling subjects, both on the scientific and the technological sides. The increase automation of transports also raises specific issues concerning security. Similarly, due to deliberate hostile human activities such as terrorist attacks, vandalisms, thefts, etc, specific actions and protections need to be enforced.

Antonio Scala CNR (left)
General Chair CRITIS 2017
Professor Institute of Advanced Studies IMT (Lucca)
e-mail: antonio.scala@cnr.it

Gregorio D’Agostino, ENEA (right)
Program General Chair
Lectutet at Univ. Roma II “TorVergata” and President Netonets Association (www.netonets.org).
gregorio.dagostino@enea.it

Programme Co-Chair:
Cristina ALCARAZ, Univ. Malaga
e-mail: alcaraz@lcc.uma.es

Grigore HAVARNEANU, Research Advisor, UIC Security Division
e-mail: havarneanu@uic.org

Poster Co-Chair:
Hypatia NASSOPOULOS, Ecole des Ingénieurs de la Ville de Paris
hypatia.nassopoulos@eivp-paris.fr

Local Co-Chairs:

Guido Caldarelli (left) full professor in Theoretical Physics at IMT

Rocco De Nicola full professsor Computer Science IMT Lucca

The IMT - Institute of Advanced Studies IMT (Lucca)
Is the main organizer of the Conference.
Meeting will be hosted in the ancient scenario of the San Francesco area: a gothic Complex built between the 14- and the 17-th centuries.

UR: Urban Resilience. The exploding human concentration in the urban areas, would be, on its own sake, a reason to devote a specific session to this significant subject. More importantly, urban areas do involve a huge number of different interdependent infrastructures that represent an un-paired scenario where to test modelling and managing capabilities developed insofar by the scientific community. One of the most delicate points is the cost/benefit analysis related to the allocation of redundant resources required to improve resilience. In particular, the security of smart buildings, smart districts and smart cities are requiring increasing efforts.

TIS: Trust Information Sharing is the elective paradigm that is commonly invoked to deploy any collaboration among different stakeholders. The creation of shared contingency plans and other forms of collaboration to deal with undesired events represent one of the most effective means to increase the global resilience of any system of systems. It is worth stressing that complex interdependent systems are not limited to the regional or national level, but may also involve cooperation at European or transborder level. TIS is also at the basis of any Public-Private Partnership, which represents a promising means to improve preparedness, share the risk and handle contingencies.

HF: Human Factors. Modern infrastructures and their aggregations are exhibiting a constant trend toward automation. However, the humans will always continue to play an essential role in several respects. Decision makers will always be central while facing unpredicted contingencies. People behaviour as local operators and especially as customers and citizens can highly influence the resilience of the society both by collective un-reasonable (psycho-social) behaviours or by cooperative synergistic actions, or even by providing creative unplanned resilient solutions. Modelling and training of decision makers and population's behaviours represents one of the most advanced sectors of research performed by theoretical conceptualisations, realistic modelling and real gaming experiments.

EM: Emergency Management. Last but not least, this topic presents a great deal of efforts from both academic and applied sides.

Generally speaking, it is the most critical part of the Preparation Cycle. The Planning, the Early Warning, the Recovery Phase, the Optimisation of the residual resources, the coordination of different actors, are just some of the issues involved when facing a catastrophe or a crisis. Floods and earthquakes represent the most common hazards; specific works to face such events are solicited. Population awareness and the role of the media during crisis also represent significant issues.

The former scheme represents just a preliminary organisation of topics. However, all advances related to the resilience enhancement or assessment and the protection of human beings and our society are welcome; including new technologies to improve quality of life or preserve our historical heritage and natural environments.
Similarly, standalone studies on Modelling, Analysis and Simulation of CIs deserve special attention regardless of their application to any specific session above. In particular, emergent behaviours (such as financial crisis or psycho-social hysteresis) have been demonstrated to be a mere consequence of the complexity (systemic risk) of the systems, not of some specific characteristics. The same considerations apply for forensic issues and policy making and enforcements by authorities of any level, from mayors to European Deputy Members.

Conference Chairs and Organisers

Antonio Scala has been appointed general chair of the conference by the Critis Steering Committee. He combines experience in Interdependent Critical Infrastructures both at theoretical and applied level (especially in the Electric System). Due to their long-standing collaboration, Gregorio D'Agostino has been also involved as Program General Chair. Following the success of 2016 organisation and to insure continuity with the previous edition, last year cochairs have been confirmed, while further including Cristina Alcaraz.

Local organisers will be two outstanding full professors of the IMT hosting institution: Guido Caldarelli and Rocco De Nicola.

Critis 2017 novelties

The format of the conference has been preserved. However, some novelties have been introduced.

The **poster session** has been extended: about a third of the applications will be presented as a poster. The cloister of San Francesco complex in Lucca will host the event in an amasing environment.

YCA: Young Critis Award. Along the line of the CRITIS tradition, special attention will be devoted to young talents. To this purpose a prize will be awarded to the best contribution presented by a young author. During the last three years this prize has been supported by the CIPRNET European network of excellence (www.ciprnet.eu) and named CYCA (CIPRNET Young Critis Award); this year it will renamed generically YCA (Young Critis Award) and it will be organised in collaboration with the International Research Institute "Res on Network" (www.resonnetwok.it) and in particular with its Scientific Director Prof. **Marco Santarelli.** Three finalists will be selected based on their contributed abstracts and will present their work to the CRITIS audience, which will provide a second evaluation. Eventually a commission of academics and experts, chaired by Prof. **Bernhard Hämmerli**, will provide a third and conclusive evaluation to achieve the final response. Detailed rules for eligibility of candidates and evaluation procedure can be found on the CRITIS2017 web-site (www.critis2017.org/YCA.php).

Beside the main conference presentations there will be two **Satellite Workshops** on **Energy** and **Water**, respectively. This two workshops will take place on October 12-th and **13-th**. The workshop on Energy will be chaired by **Angelo Facchini** (IMT) and **Antonio Scala**, while the workshop on Water will be chaired by Angelo Facchini e **Gabriele Oliva** (University Campus BioMedico). Specific calls for contribution will be made available on the website for this satellite events.

Participants interested in Energy and Water issues are encouraged to participate to both the main conference and the specific workshops.

One of the aims of the CRITS series of conference is to provide a bridge between the Operators and experts from academy or research institutions. To this purpose a specific **"Operator Session"** is planned where Operators will present specific issues or their innovative solutions. It is worth stressing that, while the participation to this session does not require the submission of an abstract, nor the publication of any proceedings, the Operators may also participate to the conference as any other contributor.

To the purpose of providing a dissemination opportunity, a **"Project Session"** is also planned where each project on C(I)IP will be given the opportunity to present its state of the art, preliminary results and ongoing work.

Beside the planned satellite workshops, other events can be possibly hosted upon request. In this respect, Projects on CIP will be given the opportunity to organise their **dissemination events** during CRITIS conference.

Paper submission

We encourage submissions containing original ideas that are relevant to the scope of CRITIS 2017. 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 which 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". A paper can be also marked as "Poster" in case, this form of presentation is preferred.

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.

Paper submission will occur via the EasyChair conference system at the following url: "https://easychair.org/conferences/?conf=netonets2017". Submitted papers (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 2017 continues the "Young CRITIS Award" activities for fostering open-minded young talents. CIPRNET European Network of excellence cooperated and supported this activity, which this year will be continued in collaboration of Res on Network (www.resonnetwork.it) a European research Institute.

Acceptance policy

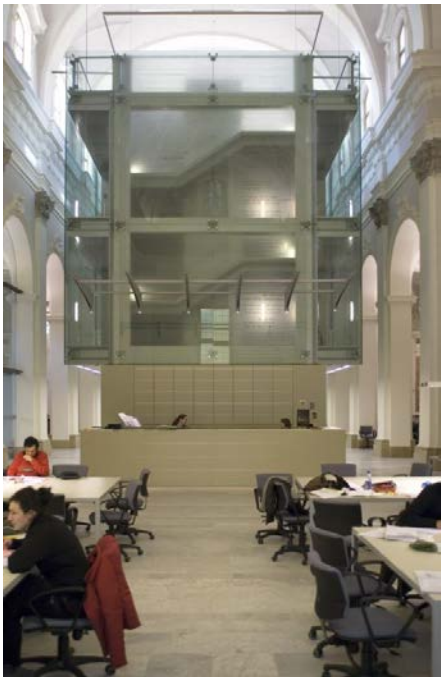
For publication in the CRITIS 2017 proceedings, all accepted oral papers (full and short) must be presented at the conference; at least one author of each accepted paper must register to the conference by the early date indicated by the organisers. Papers accepted as posters will not be published in the final proceeding, but will be included in the program and in the pre-proceedings.

The conference **pre-proceedings** will appear at the time of the conference. All accepted papers (including posters) will be included in full length in the pre-proceedings.

As in previous years, it is planned that **post-proceedings** are published by Springer-Verlag in their Lecture Notes in Computer Science (LNCS) 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.

Joining CRITIS 2017 In Lucca



Venue

CRITIS 2017 will take place at the IMT – School of advanced Studies premises, in San Francesco complex - Lucca.

Lucca is a renascent City grown on a roman original plant, which keeps its original walls intact. They are presently a pleasant pedestrian promenade. The city is overflown by churches and buildings of renaissance-era. Some of those buildings, including San Frediano Complex and San Francesco Complex have been donated to IMT which can now resort of a campus of about 10.000m2.

IMT Attractions: famous Library, hosted in San Frediano church, which represents a remarkable example of modern classical co-existence. For further information on IMT, please visit its web-site at https://www.imtlucca.it

More information

For further information on CRITIS 2017, lodging, travel directions, preliminary programme, etc., please visit the website at www.critis2017.org

Figure 15: The famous IMT Library in the former church of San Ponziano

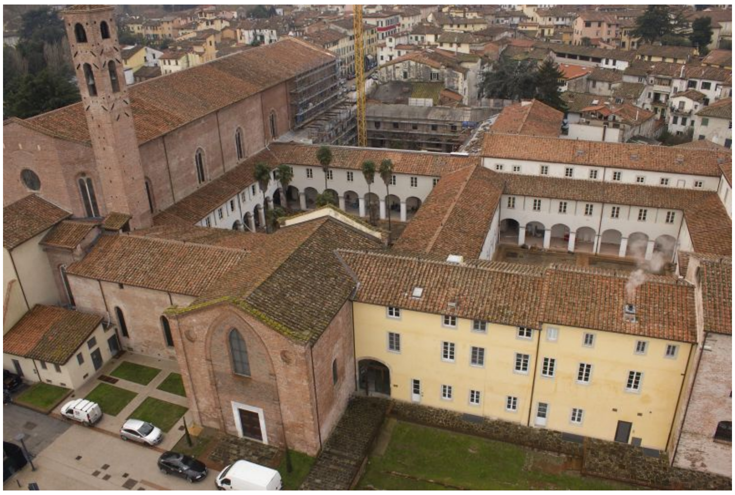


Figure 16: San Francesco historical complex, now part of the IMT premises (left)
Figure 3: Shah Italy - Lucca - view from Torre Guinigi (right)

See you at CRITIS 2017 in Lucca

www.critis2017.org

Links

ECN home page	www.ciprnet.eu	
ECN registration page	www.ciip-newsletter.org	Please register free of charge
CIPedia©	www.cipedia.eu	the new CIP reference point

Forthcoming conferences and workshops

CRITIS 2017	www.critis2017.org	9-13 October, 2017, Lucca Italy

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu
European Organisation for Security	www.eos.ecom
Netonets organisation	www.netonets.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu

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” In this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security	https://resilience.enisa.europa.eu/nis-platform
Platform Current policy debates	http://digitalwatch.giplatform.org
GFCE-MERIDIAN Good Practice Guide on CIIP	https://www.tno.nl/gpciip/

Websites of Contributors

Acris	www.acris.ch
Campus Bio-Medico di Roma	www.unicampus.it
EC Joint Research Centre	https://ec.europa.eu/jrc
Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS	www.iais.fraunhofer.de
TNO	www.tno.nl/en/
H2020	http://ec.europa.eu/programmes/horizon2020

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

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

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

> Within two and a half years, CIPedia© reached 475,000 total views, at a current average of 480 views per day.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardisation, 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**.

> Your contribution is essential for putting value in the CIPedia© effort.

In future stages, CIPedia© will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

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

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

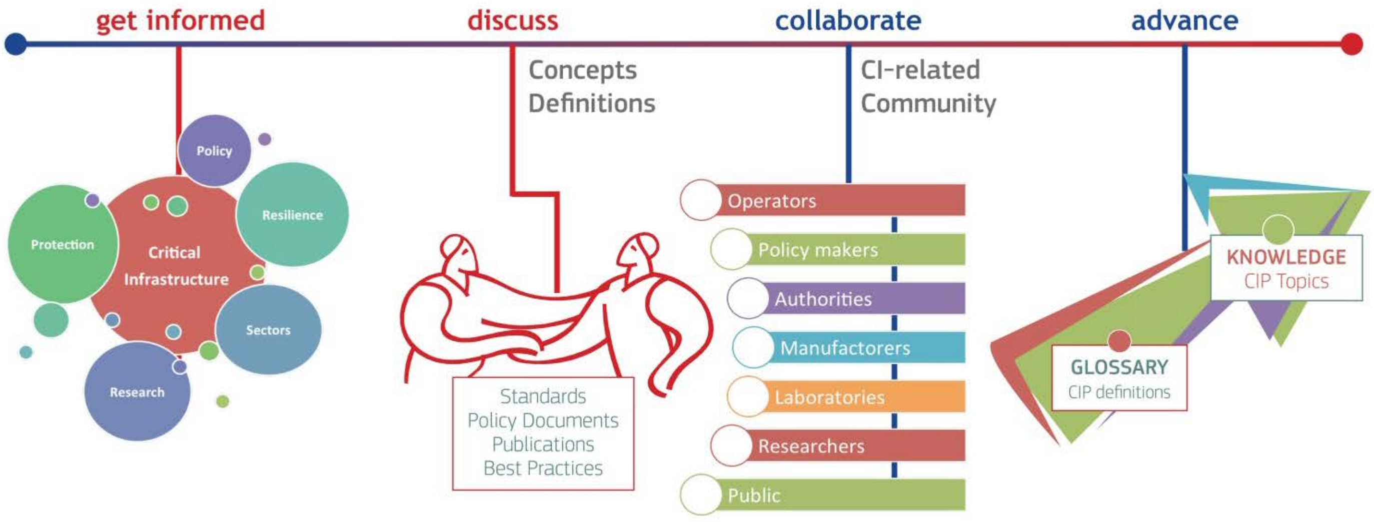
marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.


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