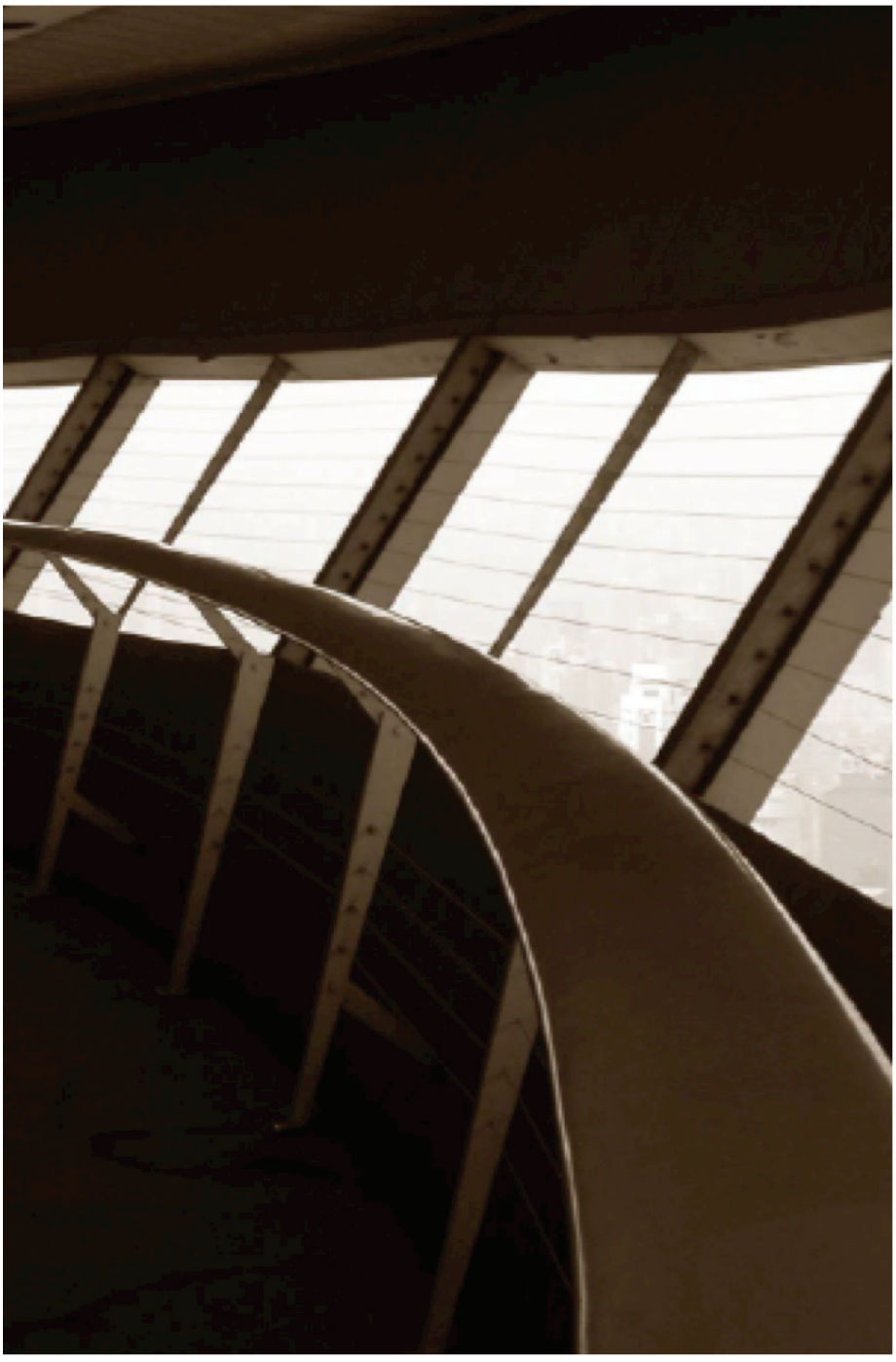
European CIIP Newsletter

July 15 – October 15, Volume 9, Number 2

CRITIS 2015

Call for Participation

Conference
Oct. 5-7, 2015 Berlin



ECN

Contents

Editorial

CI cascading effects, FP7 PREDICT

GCCS 2015

Netherlands: CI and earthquakes, Road-Access
Switzerland: PPP and SKI

High Voltage DC Transmission

Drought Risk Management Cascading Failures

TIEMS 2015
CRITIS 2015

Links

CIPedia@

CIPR Net

> About ECN
ECN is coordinated with
The European Commission, was initiated by Dr. Andrea Servida,
today funded by the European Commission
FP 7 CIP Research Net CIPRNet Project
under contract, Ares(2013) 312450

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Editoral		
Intro on using Synergies	Critical Infrastructures Trust and Public Private Partnership (PPP) by Micheline W.A. Hounjet and Bernhard M. Hämmerli	5
European and Global Activities		
CI cascading effects and FP7 PREDICT	CI cascading effects: from research into practice by Marieke Klaver and Nico van Os MPAN	7
FP7 CYSPA Project	Launch of CYSPA: the European Cyber Security Protection Alliance by Nina Olesen	9
GCCS 2015	Cyber security for critical infrastructures by Eric Luiijf	13
Switzerland: PPP & SKI	Public-Private Security Collaboration by Doron Zimmermann	15
Country Specific Issues		
Netherlands: CI and earth-quakes	The influence of triggered earthquakes on critical lifelines in the North of the Netherlands by Henk Kruse, Mandy Korff MSc and Jan Spiekhout	21
Netherlands: ROADAPT	ROADAPT: Roads for today, adapted for tomorrow by Thomas Bles	25

Method and Models		
High Voltage DC Transmission	Criticality of High-Voltage Direct-Current Power Transmission Systems by Nikolas Flourentzou	29
Drought Risk Management	System Robustness Analysis in Support of Flood and Drought Risk Management by Marjolein Mens	31
Conferences 2015		
TIEMS 2015	Evolving threats and vulnerability landscape: new challenges for the emergency management by Carmelo Di Mauro and Vittorio Rosato	35
CRITIS 2015 Berlin	CRITIS 2015: 10th International Conference on Critical Information Infrastructures Security – Call for Participation By Erich Rome, Marianthi Theocharidou, Stephen D. Wolthusen, and Cristina Alcaraz	37
Links		
Where to find:	• Forthcoming conferences and workshops • Recent conferences and workshops • Exhibitions • Project home pages • Selected download material	38
Media on C(I)IP		
CIPedia	CIPedia© is here! by Marianthi Theocharidou	39

Editorial: Critical Infrastructures Trust and Public Private Partnership (PPP)

In the frame of PPP information sharing is becoming popular and practice guides are available. NL EU Presidency will push this forward. Trust is the glue of our society, also in Cyberspace: But whom to trust.

The reaction on the big cut of trust in suppliers is becoming more and more evident: We have hardware, software, BIOS, middleware, applications, updates, crypto and other components of our ICT infrastructure which do serve the intended purposes, but support also other parties' interests. As a reaction to this tendency, nationalisation of ICT is a serious point of discussion. But do we really want this? Are there no other ways to balance leaking means and intended purpose, e.g. by behaviour

ICT infrastructure for CI should be bullet-proof and not manipulated to serve other purposes. In this context it is well understandable that weaponised infrastructures should be secured against any attack or malfunctioning.

Europe is reflecting how to react on this challenge, and how to bring the right knowledge together. The task is very challenging, but urgently needed for the sovereignty of nations and Europe in particular. A nation is defined by its sovereignty. We have to think about what this means in cyberspace in general and in the interconnected CI in particular. A huge challenge, but with preliminary discussions only: a need to be active!

The Netherlands are well known for taking care of flood protection, which stays a vital necessity. Next to that, earthquakes are happening more frequently in the northern part of the country. It is no surprise that next to the traditional CIP topics the connection between CI and emergency management is getting more attention. In the first half of 2016, The Netherlands have the EU presidency. It is the aim to use this opportunity to stimulate Information Exchange and Private-Public Partnerships in the area of CIP throughout Europe.

In addition, the Netherlands have contributed with the "Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach" https://www.gccs2015.com/documents/sharing-cyber-security-information of which the EU will publish soon chapter three "Voluntary Information Sharing" of the networking Information Security Platform NIPS.

Several articles in this volume give a broad overview on relevant projects and initiatives of the Dutch CI community: "CI cascading effects: from research into practice" by Marieke Klaver and Nico van Os, "Cyber security for critical infrastructures" by Eric Luiijf, "The influence of triggered earthquakes on critical lifelines in the North of the Netherlands" by Henk Kruse and Mandy Korff, "ROADAPT: Roads for today, adapted for tomorrow" by Thomas Bles and "System Robustness Analysis in Support of Flood and Drought Risk Management" by Marjolein Mens. In a couple of these projects described, the partnership between government, water boards, security regions and private companies are already taking form.

We would like also to remind you that the CIP community has a rendezvous in Berlin at the 10th edition of the CRITIS conference which is scheduled October 5-7. The programme will be enhanced with several distinguished keynote speakers and includes about 25 very carefully selected scientific contributions. The young scientific community is involved again and in the frame of CIPRNet Young CRITIS Award all participants are invited to follow the competing youngsters and contribute with their opinion to the election of the best contribution.

Enjoy reading this issue of the ECN!

PS: Please have a look at CIPedia©: http://www.cipedia.eu.. Please bring your knowledge in to contribute to a real CIP compendium!

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

Micheline W.A. Hounjet

Her background as an engineering geologist, she is not only active in the cross-over between technical disciplineshrough cascading effects.

e-mail: micheline.hounjet@deltares.nl

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

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

CRITIS 2015

10th International Conference on
Critical Information Infrastructures Security

October 5–7, 2015, Fraunhofer Forum, Berlin, Germany

www.critis2015.org

With

2nd Young CRITIS Award Competition

Take your chance and be audience voting member
to promote the CIP youth

CI cascading effects: from research into practice

This article gives an introduction on the collaboration between R&D and emergency management organisations in the Netherlands. The collaboration is aimed to improve the assessment of CI cascading effects in emergency management.

Introduction

Critical Infrastructure Protection (CIP) has been a research topic in the Netherlands for quite some years. Until recently, most of the research was aimed at the national level, e.g. on identifying Critical Infrastructure (CI), performing risk assessment and analysing dependencies.

Recently, the relationship between CI and emergency management is increasingly getting attention.
The 25 Dutch safety regions ("Veiligheidsregio's") play an important role in Dutch emergency management structure and processses. These Safety regions increasingly include CI in their risk assessments and emergency plans.
This article describes how a close collaboration is developing between research organisations and the emergency management organisations regarding CI and their dependencies. In particular, we describe the collaboration between TNO and the Safety region South-Holland-South. This article will discuss how this collaboration builds on the results from earlier research and how these results are used in the development and assessment of a case study.

Earlier results on CI and emergency management

Empirical evidence from reports about emergencies and disasters in various regions in the world shows that CI disruptions may cause unwanted extensions of the duration, affected area and impact of emergencies with more casualties, more suffering, and more damage. It is therefore important to include the possible impact of CI disruptions in the risk assessment and preparation processes of emergency management organisations at the local level.
One of the main lessons learned from CI disruptions all over the world is that the set of CI dependencies changes with the mode of operation. When an organisation enters another mode of operations, e.g. due to the failure of a CI, its operational continuity depends on a different set of CI. For example, the availability of diesel, roads and oil trucks are of no importance to the operation of a hospital until it has to switch on its backup generators due to a power failure.

> Emergency plans should take into account non-normal mode of operation dependencies and common cause failures

Empirical evidence also shows that CI operators and emergency management planning mostly understand and plan for possible CI disruptions critical to normal operations. However, it is much harder to understand and prepare for CI dependencies which occur in the non-normal modes of operations and when multiple CI fail simultaneously (common cause failure), e.g. due to an extreme weather event. This crucial kind of dependency analysis is often some levels of analysis too deep for most public and private sectors to plan for.

In addition to the direct impact on CI, more damage may occur due to cascading effects, e.g. the loss of electricity may lead to loss of all information and communication technology (ICT) dependent services and by that cause an impact on hospitals and the transport system. The cascading effects may refer to the cascade of disruptions across multiple CI within an area covered by the emergency management organisation, but may also refer to cascading effects outside that area.

Marieke Klaver (TNO)

Dr. Marieke works as programme manager on research in Critical Infrastructure Protection (CIP) and Cyber Security.
Her research focusses on CI dependencies, risk analysis and cyber resilience.

Phone ++31 (0)88 866 38 68
e-mail: marieke.klaver@tno.nl

Nico van Os MPAN

Nico works as project manager for EU projects at the Safety Region South-Holland South.

e-mail: n.van.os@vrzhz.nl

For instance, due to the structure of the power grid, the loss of electricity will almost certainly not be limited to an inundated area.

A systematic approach to assess the dependencies

As part of the EU FP7 project PREDICT (PREparing for the Domino effect in Crisis siTuations), a methodology was developed to systematically assess the CI dependencies and the impact for emergency planning at the local level.

The methodology provides seven steps in order to systematically:

- assess the threats to be taken into account for the considered area;
- Identify the CI;
- Identify the key CI elements;
- characterise the vulnerability of the key CI elements to the threats;
- assess the first order impact of the threats on the CI elements;
- describe the dependencies between the CI elements;
- assess the CI cascading effects.

For each of these steps, supporting tools such as checklists or algorithms can be established based on results of earlier research.

A case study of large scale flooding

In order to test this methodology, a case study was developed. The case study describes a developing dike breach near Gorinchem, The Netherlands which directly leads to failure of the quays directly behind the dike. As a result, the influx of water will threaten the polder 'Alblasserwaard' lying directly behind these quays.

Such a large scale flooding will have impact on almost all CI within the affected area. The seriousness of the scenario is increased by the short timelines: the western area of the polder will flood in a period of approximately sixteen hours.

In order to assess the effects for all CI, the assessment is performed in a close dialogue with all stakeholders within the Safety region South Holland South, including operators of the main CI within the region, emergency management organisations and research organisations.

Figure 1: the location of the Alblasserwaard

Based on this close collaboration, the methodology is tested and the required level of detail can be established that is needed to support the decision making process. The case study is also used to assess the availability of the Information needed.

An initial result is that the assessment methodology does not require highly detailed CI information; understanding the main issues, decision points and time characteristics for the CI operators is often sufficient for proper emergency management planning and operations.

Next steps

The main results of the case study will be discussed in a workshop with the main stakeholders in South Holland South end of May 2015.

The EU project PREDICT will use the methodology and findings from this and other use cases to develop supporting tools.

Finally, in close collaboration between TNO and the Safety Region South Holland South an extensive scientific paper is being written that describes both the methodology and the results of the case study.

Acknowledgement

The PREDICT project has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement no 607697.

This article reflects only the authors' views. The European Union is not liable for any use that may be made of the information contained therein.

http://www.predict-project.eu/

PREDICT
PREparing for the Domino effect in Crisis siTuations.

Launch of CYSPA: the European Cyber Security Protection Alliance

The CYSPA Alliance is an initiative for EU stakeholders working together to articulate, embody, and deliver the concrete actions needed to reduce cyber disruption

CYSPA is a European-based Alliance that started as an FP7 EC-funded project (October 2012-March 2015) and which is now operating under the European Organisation for Security.

Managing cyber risks is not only a technical issue. Correctly managing cyber risks is a corporate level responsibility – it is not something that can be delegated, it is an issue that can bring down a company. This is the first pillar on which CYSPA built its approach from the start – the need for every organisation to protect their assets means that organisations need to be empowered to understand and be fully aware of which assets are at risk, which assets are more at risk than others, leading to a clearer view to investments and policy decisions.

The CYSPA Alliance aims to protect cyberspace, an environment characterised by its world-wide outreach and its speed – speed of propagation of information, unfortunately also matched by speed and ease of propagation of attacks. Over the last years, the key trends are driven by increasingly distributed operations, ranging from cloud-based platforms to mobile technologies, intelligent devices and bring your own devices. Of course, cyber-attacks take place on a global level, but over the last years, it has become evident that even analysing only at a European level, the cyber threat landscape has changed significantly. This, together with the fast paced nature of cyberspace, means that cyber security should be of paramount focus for every organisation in order to protect their assets.

Current evaluations of economic impact and costs are given at very high level (i.e. for a whole activity sector, or for a country) but the negative side of this macro-approach is that individual organisations cannot relate to such huge numbers – there is a strong need for more personalised evaluations of the impact of cyber-attacks.

Managing cyber risks is not only a technical issue. Correctly managing cyber risks is a corporate level responsibility – it is not something that can be delegated, it is an issue that can bring down a company. This is the first pillar on which CYSPA built its approach from the start – the need for every organisation to protect their assets means that organisations need to be empowered to understand and be fully aware of which assets are at risk, which assets are more at risk than others, leading to a clearer view to investments and policy decisions.

The European context

Since the start of CYSPA, another key evolution has taken place – the actions of the European Commission have been consolidated into a European cybersecurity strategy.

This is a key evolution in integrating the multiple dimensions of cyber-space because it is the first step towards implementation – implementation of new directives, of research opportunities, of procurement guidelines etc. It is key for each organisation to not only be aware of what is taking place at European level, but more importantly to understand how this can impact operations and to get involved in ensuring that the implementation path of the European strategy is aligned to one's needs.

Nina Olesen

Nina Olesen is a senior project manager at the European Organisation for Security. She is currently involved in different EU projects and is leading the operational management of CYSPA.
She was also the project coordinator for the CYSPA project.

e-mail: nina.olesen@eos-eu.com
European Organisation for Security
Rue Montoyer 10, BE-1000 Brussels
ww.eos-eu.com

CYSPA is therefore positioned across these two dimensions:

- The need to empower each organisation not only with awareness but also with the means to understand and prioritise how to protect its operations
- The need to be active at European level to contribute to the European cybersecurity strategy, to ensure that ultimately the various directives, policies and research activities are well aligned to the needs of each organisation's economic activity sector and operations.

Objectives

In order to reflect its vision statement of working together at European level and being active not only in defining but also in implementing actions, CYSPA has translated this approach into five core objectives.

The first objective of CYSPA focuses on specific campaigns, each campaign representing a concrete set of activities and outcomes. These campaigns aim to encapsulate the approach of getting members actively involved in CYSPA.

The second objective focuses on the need to identify and express the real impact of cyber threats at a level that is relevant to individual organisations. CYSPA is therefore focusing on a sector per sector approach – starting with the e-government, energy, finance and transport sectors. This approach delivers the right balance between organisations being able to access information that is relevant to their activities, while at the same time taking into account the sensitiveness of the information. CYSPA will add additional sectors (based on feedback from members) after the CYSPA model has been fully tested on the four current sectors of focus.

The third objective is to deliver concrete services to members – meaning that CYSPA is focused on supporting its members with approaches, tools and solutions to increase not only awareness but also their analysis capabilities of their own cyber risks.

The fourth objective is to promote an open culture of active participation. This means that for the different recommendations that CYSPA is working on in terms of identification of risks, methodologies to handle risks, solutions etc., members should not only elaborate them together but also take up these recommendations and implement them internally to then help evolve. By encouraging our members to implement in their own contexts and to then share feedback, the dynamic nature and complexity of the cyber security domain is better supported.

The fifth objective is the coordination and collaboration with other European-wide initiatives. For instance, CYSPA has consolidated results from its sector impact reports and the threat taxonomy coming from ENISA's threat landscape reports in order to feed into a risk self-assessment tool that is accessible to members via the CYSPA Community Portal.

Providing added value

Since CYSPA was created as a European project, numerous associations and alliances have emerged, focused on different aspects related to cyberspace. A valid question is therefore what CYSPA can bring of value – especially in a context where we want to avoid duplication.
First and foremost, CYSPA introduces a sector specific approach to cyber risks – moving to a level of granularity to make the impact of cyber risks relevant to individual organisations.

Secondly, CYSPA has developed a community approach, supported by an online portal for members, to ease interaction and access the value added services.

Thirdly, in creating a network between users, providers and public authorities not only as a meeting point, but also through concrete activities, an important contribution is being made to achieve the sharing philosophy without which cyber security will never become a reality.

Finally, CYSPA will be used as a gateway between needs and European policy makers, aiming to improve the alignment of policies to needs but also to speed up uptake.

CYSPA community

CYSPA is working with users, providers and public authorities in the context of cyber security.

Starting with the users, the benefits are clearly to move to numbers, approaches and solutions that are applicable to the specific sector in which a user operates.

For the providers, the benefits are to have faster, easier access to user needs – and as a consequence of increased user-provider collaboration decrease the time to market by earlier involvement of users and better alignment to already identified needs.

CYSPA involves public authorities in their role as policy providers, strategy promoters and awareness drivers – activities that require uptake by the actual industrial organisations.

Starting with the initial consortium partners comprising 16 organisations from industry and research, CYSPA has evolved its community to include national security clusters, SME's, national public administrations, and operators. CYSPA is also working on setting up national chapters, the first of which will be set up in Turkey.

CYSPA organisation

The CYSPA Alliance is a membership-based "de facto" association established under the European Organisation for Security (EOS). Organisations joining CYSPA need not be a member of EOS but EOS members are granted free access to CYSPA.

CYSPA is organised through a Board and operates through Sector Groups and Task Forces.

Sector Groups are used to create a focal point for stakeholders from each sector, a space of interaction for members operating in similar contexts, from transport to utilities, finance and e-government. Members can also propose new sectors of focus. Task Forces are used to implement focused activities with a defined duration and target result.

CYSPA is also supported by External Advisors.

How to join

CYSPA will be introducing membership fees as of July 2015. Until then, organisations can join free-of-charge via the Community Portal (https://cyspa.eng.it/).
The CYSPA Community Portal provides members of the Alliance with a comprehensive **online collaboration** platform designed specifically to enable and ease interactions between the CYSPA members.

The sector approach of CYSPA provides you with a unique opportunity to get a more precise view of the different needs of customers operating in your domain. In the dynamic context of cyberspace, no single company, no single organisation, no single country can work ALONE in tackling the challenge of cyber threats.

CYSPA focuses on defining action lines that require a community to deliver value and on encapsulating the results of these activities as services to deliver value back to its members.
CYSPA builds these action lines across three pillars:

1. By actively contributing to policy at European and national level
2. By building the capacity of CYSPA members to assess the vulnerabilities, prioritise how critical those vulnerabilities are to their own operations and identifying solutions
3. By creating cyber knowledge

By joining CYSPA, you choose to participate to one or more of these action lines – turning your effort and involvement to those activities that are the closest to your needs.

If you would like to know more about CYSPA please visit our website and Community Portal:

www.cyspa.eu
https://cyspa.eng.it/

Watch our video: "CYSPA Launch Alliance":
https://www.youtube.com/watch?v=YdJq0_Hb_wg

For more information on membership (fee structure, statutes, etc.), please contact nina.olesen@eos-eu.com)

CYSPA
EUROPEAN CYBER SECURITY PROTECTION ALLIANCE

TIEMS 2015 Annual Conference

TIEMS 2015 Annual Conference in Rome
30th September - 2nd October 2015

http://tiems.info/tiems-2015-annual-conference.html

TIEMS 2015 Annual Conference which takes place in Rome.

TIEMS Italy Chapter is conference host, see:

Italy Chapter WEB-site

Registration coming soon:

http://tiems.info/tiems-2015-annual-conference.html

Cyber security for critical infrastructures

A vision for action and two good practice booklets were launched at the fourth Global Conference on CyberSpace (GCCS 2015): Sharing Cyber Security Information and Cyber Security of Industrial Control Systems.

The fourth Global Conference on CyberSpace (GCCS 2015) took place in The Hague, The Netherlands on April 16-17 2015. More than 1600 governmental, private sector and civil society representatives from 100+ nations gathered together to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behaviour in cyberspace.

Cyberspace is a domain that no single party or entity governs on its own. The internet houses multiple actors that are becoming increasingly interconnected and interdependent, in an enormous, complex environment where a balance must be struck between security, freedom and social and economic growth.

The Cyber Security track included a session on Building Public Private Cooperation in Cyber Security. In support of that topic, a number of documents were developed and handed over to the international community.
The Netherlands Organisation for Applied Scientific Research TNO was responsible for developing three of the deliverables which will be described below.

Towards Action

The first deliverable **From Awareness to action: bridging the gaps in 10 steps** is an interactive webpage. It is the result of the cyber security debates which take place at both the Board Level and the government policy levels at the earlier The Grand conferences (Amsterdam 2013, Rotterdam 2014), MERIDIAN and World Economic Forum (WEF) conferences. This deliverable is a stepping stone for the 2016 cyber security activities by the Dutch EU Presidency.

Information Sharing

The second deliverable is a booklet on **Sharing Cyber Security Information** which reflects the good practice stemming from the Dutch public-private participation approach. Moreover, knowledge collected about international good and bad experiences made its way into the booklet. Contributions by the Meridian CIIP community were included.

As the threat landscape is continuously changing, the sharing of cyber security related information between organisations – in a critical sector, cross-sector, nationally and internationally – is widely perceived as an effective measure in support of managing the security challenges. Information sharing, however, is not an easy topic as it comes with many facets.

> "Information Sharing is a mindset"

The booklet aims to support the cyber security and resilience governance. Its aim is to assist public and private policy-makers, middle management, researchers, and cyber security practitioners, and to steer you away from pitfalls.

Industrial Control Systems

The third deliverable is a booklet on **Cyber Security of Industrial Control Systems** (ICS). It was developed with support by the Meridian community and several associations and private organisations.

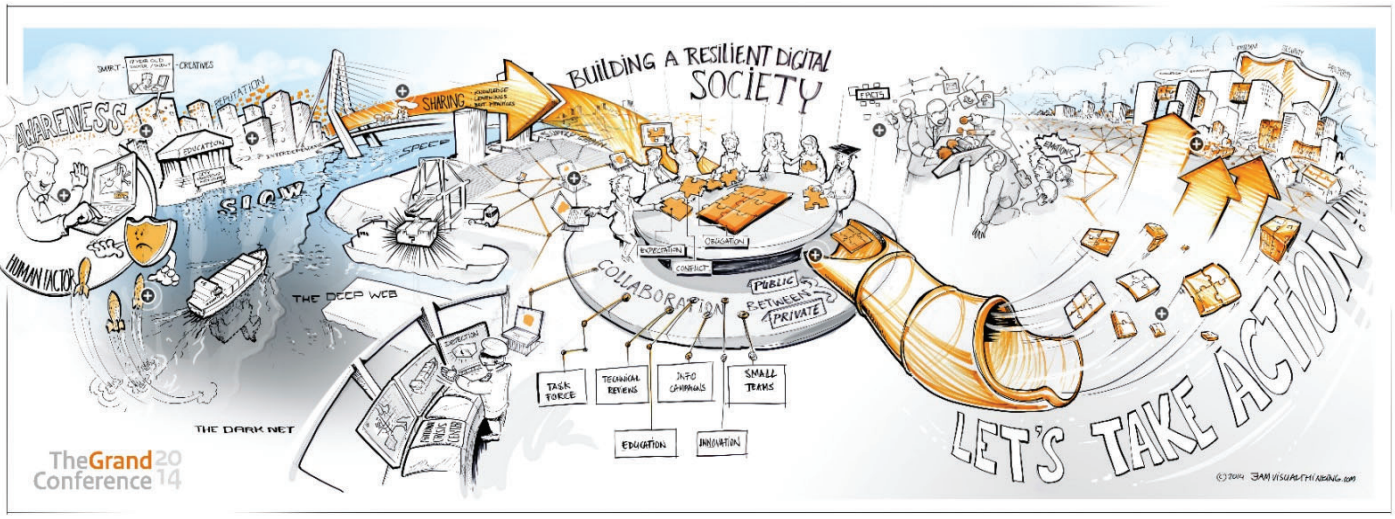
Crucial processes in most critical infrastructures, and in many other organisations, rely on the correct and undisturbed functioning of Industrial Control Systems (ICS)[1].

[1] ICS are also known under a wide variety of other names, such as SCADA, DCS, IACS, PLC, and PCS.

Eric Luiijf

Eric Luiijf is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. Since 2000 he contributed to many national and EU projects in the field of Critical (Information) Infrastructure Protection, both at the technical and policy levels. Eric has published many popular articles, reports, and peer-reviewed publications about cyber terrorism and warfare, C(I)IP, process control security, and cyber security. He has been interviewed many times by press, radio and TV on these topics.

e-mail: eric.luiijif@tno.nl



A failure of ICS may both cause critical services to fail and may result in safety risk to people and or the environment. Therefore, the cyber security and resilience of ICS is of utmost importance to society as a whole, to utilities and other critical infrastructure operators, and to organisations which use ICS.

> **"Good Morning with ICS"**
>
> Unconsciously you may have already met and used many ICS before taking the first sip of coffee."

Executive level

The good practice document first and foremost, provides private and public sector executives with an Executive Summary outlining the ICS risk and challenges. The document appeals to the executive leadership of organisations to address the clear and present cyber security danger to their organisations and our societies as a whole.

… and all others involved

Underpinning the Executive Summary, the good practice document provides governmental policy-makers, technical managers, ICS suppliers and others involved in the ICS domain with background and security awareness information about the cyber security challenges for ICS. Moreover, the document provides a perspective for action and pointers to seventy relevant resources.

References

From Awareness to action: bridging the gaps in 10 steps:
https://zoom.frontwise.com/public/4/towardsgccs2015#

Sharing Cyber Security Information:
https://www.gccs2015.com/sites/default/files/documents/Sharing%20Cyber%20Security%20Information%20GCCS%202015.pdf
or: www.tno.nl/infosharing

Cyber Security of Industrial Control Systems:
https://www.gccs2015.com/sites/default/files/documents/Cyber%20Security%20of%20Industrial%20Control%20Systems%20GCCS2015.pdf

or: www.tno.nl/ICS-security

email eric.luiijf@tno.nl

Securing National Critical Infrastructure

The Role of Public-Private Security Collaboration

Introduction: The State of CIP in Switzerland

Historically, Switzerland has been the home to longstanding and successful public-private partnerships: the militia system that is a key feature of the post-1848 modern Republic of Switzerland has placed seasoned professionals into all tiers of government at the community, cantonal and (con-) federal levels and harnessed professional skillsets in the service of the state with considerable success. However, in terms of close cooperation between private corporate entities and government authorities for the protection of national critical infrastructure from a security angle, Switzerland is relatively new to the task. Most of the attention regarding CIP has been paid to its utility and safety aspects, based on a post-Cold War and quasi-isolationist assumption that infrastructure and services reliability primarily is a maintenance task. This observation stands in stark contrast with pioneering endeavours of other countries, or, for that matter, national public-private cyber security projects, i.e. MELANI[2] and in a manner is ironic in that the arguably intuitive integral security approach practiced with vigour during the Cold War in Switzerland has lagged behind the strides taken by dedicated government agencies to protect the computer systems of private critical infrastructure owners and operators.

Nevertheless, once awareness for the evolving threat scape – from physical, logical and personnel threats with all their attendant attack vectors – had reached critical mass with both public and private decision makers[3], it proved a compelling incentive to pose a fundamental query: how much can a private corporate entity achieve in pursuit of protecting the infrastructure it owns and, at least to some extent, is both responsible and liable for? The answer may prove more elusive than assumed, yet its pursuit usually leads to a corollary query: not if, but to what extent ought the state and its institutions be involved in protecting highly critical assets, the functioning of which not only ensure business continuity for the corporate owner and operator, but effectively constitute vitally important processes to the operation of that self-same state?[4]

Vulnerability and Impact

Particularly piquant in the context of this discussion eventually leading to an integral approach to public-private partnerships and even to an explorative form of collaborative governance of such joint ventures, are the implications of both the above queries with special reference to impact and consequence of a failure of national critical infrastructure.

[2] Cf. Critical Infrastructure Partnership Advisory Council, Annual Update, Department of Homeland Security, at http://www.dhs.gov/sites/default/files/publications/nppd/cipac-2012-final-508-compliant-versionv2.pdf ; also view http://www.melani.admin.ch/ for the Swiss federal cyber security organisation.

[3] Cf. the Swiss minister of defence's recent deliberations on the changing face of national security policy of 16 March 2013 in the context of which CIP mentioned as a priority at http://www.news.admin.ch/message/index.html?lang=de&msg-id=48186

[4] The Swedes have defined the roles, responsibilities and financial burden sharing between their regulator-cum-inspectorate Svenska Kraftnät (SVK) and privately held TSO and DSO infrastructure owners and operators. Thus, SVK bears the cost for securing highly critical substations that connect into the bulk electricity transport network (400KV) and those elements of the electricity distribution network that assumes TSO functions (130KV). Private communications on the occasion of a security cooperation visit, Swissgrid-Vattenfall, 19-21 March, 2013. Also cf. http://www.svk.se/Start/English/About-us/

Doron Zimmermann

Doron Zimmermann PhD read for his doctorate at Cambridge University. Over the past fourteen years, he has been a Senior Researcher at the Swiss Federal Institute of Technology (ETH) with Center for Security Studies and subsequently took up the position of head of political risk analysis for a special lines insurance company. He was an Assistant Professor for International Security Affairs at National Defense University in Washington and practiced what he had taught as Head of Interagency Intelligence Integration on the Swiss government cabinet's Security Committee staff. From 2012, he has worked as Senior Manager for Security Affairs at Swissgrid. From 2012-2014, he has worked as Senior Manager for Security Affairs at Swissgrid. At present, Doron is a Senior Risk & Security Consultant with ISPIN, a leading company in the field of information and data security located in Switzerland.

e-mail:
doron.zimmermann@cantab.net

The more advanced a country's critical infrastructures are, the higher is the likelihood of such assets' interdependency and, hence, their vulnerability to multiple, distributed points of failure, up to and including vulnerability risk concentrations in the shape of single points of failure. For obvious reasons, Western countries are particularly affected.

Arguably, the acuity in regard to an infrastructure's criticality is highest at the sequential beginning of any given national economic value chain; with no energy to supply communications, guidance systems and fuel for transportation, water and food supply, delivery of vital medical services, to name but a few interdependencies, not only economic, but also socio-political functioning of a state will within the space of a few days grind to a jarring halt. Imagine, quite literally, a domino effect: the interdependence in this instance is an effective "if/then" proposition. Within a week, if one scenario is to be lent credence[5], the affected state is not only facing crippling damage to its national economy, but is likely witnessing the first signs of a crumbling national cohesion, beginning with plundering and riots due to supply problems and the shortage of essential goods and services. In the case of Switzerland, the economic losses incurred on a per diem basis are estimated to be in the range of between 12 and 42 billion CHF.[6]

The exceptional criticality of the energy sector is, indeed, vested in its position within the sequence of a national economy's value chain. Therefore, the cascading effects its potential failure would have on any other "subsequent" sector of a national economy, with attendant spill-over consequences across borders of adjacent countries, even affecting countries with no shared borders, would almost certainly be catastrophic. In the case of the bulk electric transmission system operation, its criticality is even more pronounced vis-à-vis energy producers and distribution system operators: hydro- and nuclear energy production is the subject of considerable security investment, while decentralized ownership of distribution system operations mitigate the problem of single points of failure. To use an analogy from the energy sector, even pipelines tend to be better protected and less vulnerable than the bulk transmission system grid. Though both energy transport systems are usually built above ground, there is potentially fewer, geographically dispersed pipeline-miles to protect, than the spread out, highly complex bulk transmission grid has to offer. Or, in other words, the streamlined backbone of national and international oil transport may offer fewer vulnerabilities in structural terms than its equivalent in the power energy sector, albeit without taking into account either exposure to dynamic man-made risk or absolute dimensions.

The Swiss CIP Endeavour

The implications of criticality and vulnerability of key infrastructure dawned on the Swiss federal government at a comparatively late point in time: while in America the President's Commission on Critical Infrastructure Protection produced a seminal report published in October 1993, which acted as a harbinger of two Presidential Decision Directives, (PDD-62 & 63) addressing CIP in May 1998[7], no such equivalent was forthcoming in Switzerland until the early 21st Century. With what is today commonly known as the "SKI-Programme" (SKI stands for the German "Schutz kritischer Infrastrukturen")[8], the Swiss federal government launched a comprehensive yet pragmatic undertaking in the area of CIP that in its comprehensiveness is reminiscent of Switzerland's total defence approach cultivated after the Second World War: in this the SKI programme does not fall short of other national federal programmes' traditional emphasis on thoroughness. Accordingly, an all-hazards approach sets the stage with respect to the SKI related threat-analysis in accordance with the principle of comprehensiveness. To the keen observer, an "anthropologically" induced overreliance on impact analysis commonplace in a country dominated by its financial industry may mar the otherwise flawless execution of this sterling government initiative. All sectors of the economy have, since the inception of the programme, been mapped and their respective designated critical infrastructures are being inventoried in a continuous drive to keep this repository up-to-date. The programme, which in organisational terms is a part of the Federal Office of Civil Protection in the Swiss Ministry of Defence, had its major breakthrough with the adoption of the CIP basic strategy of July 2009 by the Federal Council; on 27 June 2012, the Swiss executive passed the CIP Strategy, which irrevocably established CIP as a priority subject on the national security agenda.

An offshoot of the SKI-programme, or rather, the key derivative of the 2012 CIP Strategy is the Guide to Critical Infrastructure Protection.[9] The Guide has been peer reviewed within the relevant departments of the federal administration in Berne, but remains an internal document and is as yet not published. In spite of the executive character of its parent document, the CIP Strategy,

[5] Cf. Marc Elsberg, „Blackout" (Blanvalet, 2012); http://www.blackout-das-buch.de/ ; the seminal study on the effects of a blackout used in Elsberg's dramatization "Blackout" was conducted by the Berlin School for Economics and Law and can be found at http://www.tanknotstrom.de/assets/content/images/pdfs/Szenario%20Berlin_2012.04.23.pdf, accessed 22 March 2013.

[6] http://www.stromzukunft.ch/versorgung/stromnetz/, accessed on 8 March 2013.

[7] Myriam Dunn Cavelty, Manuel Suter, „Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection, *International Journal of Critical Infrastructure Protection*, (August 2009), pp. 2-3.

[8] A recap of the SKI Programme can be found at http://cgd.swissre.com/global_dialogue/topics_info/risk_management_insurance/RDS_IRM_Fostering_Infrastructure_Resilience_Article.html, "Critical infrastructures in Switzerland and the provision of essential goods and services" by Willi Scholl, Stefan Brem and Ruedi Rytz in *Integrative Risk Management: Fostering Infrastructure Resilience*, pp. 72-83 (Rüschlikon, Swiss Re Centre for Global Dialogue, 2012); for further information cf. SKI website at www.infraprotection.ch

[9] „Leitfaden zum Schutz kritischer Infrastrukturen," internal draft document, Swiss Office of Civil Protection, 23 July 2012.

the Guide itself is currently not intended to represent a regulatory framework binding upon the owners and operators of national Critical Infrastructure, although these are its primary target group. Its significance, however, goes beyond an attendant optional or advisory DIY to the aforementioned national CIP Strategy and is borne out by the fact that its utility lies in its potential to close a gap in minimum security standards. To date, there is no applicable or binding minimum security standard for private owners and operators of national Critical Infrastructure in the energy sector, with the exception of energy producers using nuclear power technology.[10]

Standards in Energy Security and the Need for PPP Collaborative Governance

On 3 January 2013, the mandated national transmission system operator of Switzerland, Swissgrid, assumed control and, hence, responsibility for all the bulk transmission system infrastructures – from command and control systems, e.g. supervisory control and data acquisition (SCADA) systems, substations to approximately 15,000 pylons and 7000 kilometres of power grid. Previously spread across 18 corporate entities according to one account,[11] the consolidation had a variety of economic synergetic advantages, such as reducing the cost of bulk power transport, primarily by the reduction of disparate investments and duplications of maintenance and operations costs of previously multiple owners and operators. This change went hand in hand with the concomitant increase in national and international competitiveness; over time, we will likely see a decrease in absolute costs.

However, there is also a drawback from a security vantage in that the concentration of the assets also created a closer fusing of previously dispersed command and control nodes. The security dimension was either to be defined at a later stage at the time the decision was taken to incorporate a national transmission system operator, i.e. Swissgrid, or, considering Switzerland's record of neutrality and political stability, it was simply not considered relevant. Complicating the security situation is the historic circumstance that since Switzerland's transmission system grid had been an achievement of the post-World War II era, today stretches of it are older than 60 years and require not only maintenance, but replacement. Moreover, with transport capacity in the existing grid having reached its limit [12] , Switzerland's transmission system grid is in dire need of expansion. Expansion of the grid, in turn, will likely spark opposition and it is safe to assume that not all critics and sceptics will chose due process of law to vent their spleen. Consideration of legislations to shorten permit periods for the construction of additional pylons which are to mark the future landscape, as well as measures for the compulsory nationalization of assets and real estate towards the expanded grid are not likely to improve opponents' willingness to compromise and, in fact, will likely serve to harden attitudes in the future.

In spite of the undeniable relationship of energy security as a prerequisite for energy reliability, which in general cannot be said to constitute its ineluctable product, the former was never given its due consideration. As of this writing, though belatedly, the understanding that there simply cannot be energy reliability without first securing the energy infrastructure is making headway, albeit at a crawl. Arguably, the consequent cumulative security risk created with Swissgrid's incorporation coupled with the above explained structurally immanent vulnerabilities to the infrastructure have perforce created a potentially higher exposure to security risks from a multiplicity of attack vectors, including, but not restricted to, the logical, physical, organisational spheres. Moreover, in assuming responsibility for the bulk transmission system of Switzerland, Swissgrid as a legal corporate entity also assumed liability for the assets it had taken over. Would the implications of a future attack on the energy power hub represented by Swissgrid go well beyond the corporation's financial and security saturation capacity; and would it then almost certainly damage the national economy, impinge upon the capacity of Switzerland's neighbours to export or import energy transported through Switzerland's bulk transmission system grid and may such a scenario of a prolonged and regional or national blackout even lead to an aggravated security situation within Switzerland? If so, would the risk to Swissgrid have to be assumed to be at a sovereign level? These speculative questions do not yet have definitive answers. Yet the Swiss Office of Civil Protection's assessment in this regard puts paid to this claim.[13] The problem is that other than a threat passing the threshold to traditional interstate war, nobody really knows with whom and "where" the responsibility and liability of the corporation to protect the national critical energy infrastructure in its care begins or ends. It is as per the writing of this paper not clear at which point of an unfolding security-relevant event any given security related incident or crisis is to be considered as within the remit of the designated cantonal or federal government security agencies: the division of roles and responsibilities between private corporations and government agencies in matters security and critical infrastructure protection is anything but clear.

As if this inconclusive state of affairs in the face of a new cumulative risk to the energy transmission system operation of Switzerland were not enough, no responsible authority in the country presumably is in a position to either issue or regulate

[10] Cf. Swiss nuclear energy law and directives at http://www.admin.ch/ch/d/sr/7/732.1.de.pdf and http://www.admin.ch/ch/d/sr/7/732.11.de.pdf , respectively.

[11] Communication from Swissgrid's CEO, Mr P.-A. Graf, 14 March 2013.

[12] According to one account, the Swiss transmission system grid is at overcapacity during 1500 hours p.a.

[13] The Swiss MoD considers the energy sector to constitute one of the few „deep red" elements of the 31 listed critical sectors of the national economy. Cf. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/kritische_infrastrukturen.parsys.77606.downloadList.90979.DownloadFile.tmp/28teilsektorene.pdf

minimum security standards for energy security, not to speak of inspecting their implementation by owners and operators of national critical infrastructures. In the absence of robust, national security minimum standards, confronted with mounting attacks on the critical information infrastructure of Swissgrid or corporate entities in the country [14] and in the face of increasingly urgent queries by senior management regarding the state of security, the Corporate Security branch was compelled to "borrow" appropriate standards. The challenge of finding relevant standards is that generic standards, e.g. the 2700x series of standards by the International Standards Organisation[15], are too broad or too shallow due to their non-industry specific nature and thus rarely provide feasible and pragmatic application opportunities in the context-sensitive security TSO environment, especially its pronounced vulnerability problem with respect to the exposed grid cable and multitude of potentially neuralgic pylons. It is for this reason that Swissgrid Corporate Security eventually elected to benchmark its logical security measures against the CIP standards issued by the North American Electricity Reliability Corporation. Known as the NERC-CIP standards, and divided into nine segments (NERC-CIP 001-009) [16], Swissgrid since their adoption has concentrated on the implementation of standards 002-009, which for the most part address cyber security measures. NERC-CIP 001[17], the standard which addresses security challenges of a more integral nature, notably sabotage and insider threats, was for the time being set on the backburner and hence opened yet another kink in the armour in the sense that all the focus on highly sophisticated cyber-warfare and its equally complex body of countermeasures left, figuratively speaking, the door ajar to low-tech, but no less perilous, attack vectors, such as conventional terrorist operations, sabotage and traditional industrial and economic espionage.

Based on the all-hazards risk analysis approach and a continually groomed inventory of infrastructures, as well an understanding of their relative interdependencies, the SKI-programme's Guide emerges as the compendium of best practice for national CIP. Albeit not industry-specific and therefore potentially imbued with a "weakness" similar to that of the corresponding ISO security standards, the SKI Guide has the advantage of addressing the subject of CIP-specific integral security with the 28 Swiss economic sectors in mind, whose risk analytic properties, i.e. the threats to them and their respective weaknesses, shaped its outlook. The Guide at a minimum partially bridges the gap between the depth of the NERC-CIP's industry specificity and the horizontal breadth of ISO security standards, while being a "native" product designed to meet national challenges.

The SKI-Pilot Project

With the passage of the SKI Strategy through the Swiss Federal Council in July 2012, the eponymous Guide, though still in a mature drafting stage, was upgraded in the sense that post-ratification it was considered part and parcel of a CIP programme underwritten by the government's executive branch. Though not having the force of law once finalized and ratified, to some it has become clear that the SKI-Guide will at the very least constitute the foundation or a capstone of any future regulatory framework – and for lack of viable alternatives, some would say it does so today. With this understanding in mind, Corporate Security at Swissgrid was well placed to promote the case for proposing to the relevant government entities, starting with the originator of the SKI-programme at the Office of Civil Protection, and including the federal agencies for national supply (BWL), energy (BFE) and two federal security organizations, that Swissgrid offer itself as a "pilot project" for the application of the SKI-Guide. Additionally, the regulatory authority, the Electricity Commission's (Elcom) participation is designed into the project-plan as an indispensable partner in this venture. Thus, following months of preparatory "shuttle diplomacy" between Berne and Swissgrid's offices, the SKI Pilot Project was launched in the autumn of 2012; it held its initial meetings, during which the project scope and time-table were agreed upon by the participants, in early 2013. The project's governance is collaborative: though it is a public private partnership, the driving interest behind the project may not only be a mutually beneficial arrangement, but instead may well be impelled by a maturing and more thorough understanding of the shifting threat-scape; and the forbearance thus engendered in the parties involved. The background to this observation is a nascent collective understanding among the participants of not only the high interdependency between the state with its sovereign responsibilities of national supply on the one hand, and the owners and operators of national critical infrastructure with special reference to TSOs on the other. The mutual dependency between the two parties is both fundamental and in terms of the complexity of modern societal infrastructural interlacing, near absolute. The first workshop addressing the identification of critical processes at Swissgrid was scheduled for late March 2013; several other gatherings focussed on themes such as threat- and vulnerability-scapes [18], which eventually are to coalesce into a comprehensive risk analysis; it, in turn, is the basis for a gap analysis, from which recommendations are to be derived from both the corporate and CIP perspectives. The SKI Pilot Project was slated to run for approximately two years and move through the currently undisclosed risk analytic and management steps of the SKI Guide in order to produce a short final report featuring, inter alia, the previously mentioned recommendations regarding security measures. This final report is intended to be submitted to the

[14] Regarding the most recent cyberattacks, purportedly carried out by, or with the connivance of, Chinese government organisations cf. http://intelreport.mandiant.com/mwg-internal/de5fs23hu73ds/progress?id=ZCJjbRfMGl

[15] Cf. http://www.27001-online.com/

[16] NERC's CIP standards are listed on the standards site at http://www.nerc.com/page.php?cid=2%7C20

[17] Op. cit. http://www.nerc.com/files/CIP-001-2a.pdf

[18] No final decision has as yet been taken on whether to address exposure to risk as a set part of the SKI Pilot Project.

office of the head of the Swiss Federal Department of the Environment, Transport, Energy and Communications (UVEK/DETEC) with the ultimate goal of pinpointing need for action in the sphere of energy security and the protection of critical energy infrastructure protection.

Conclusion: Challenges to Collaborative Governance in Public Private CIP Partnerships

The SKI Pilot Project is a pioneering undertaking in the area of public private security cooperation in Switzerland and stands out due to its genuinely collaborative governance framework underpinned by its participants' common understanding. It is, as explained above, well underway to produce a key gap analysis of the extent to which corporate entities can (afford to) secure assets within their remit as private organisations and the requirements as set by the federal and cantonal authorities with a view to national security and especially with regard to protecting highly critical infrastructures. Yet there are more elusive challenges to meet beyond articulating the divergences between private and public stakeholders potentially disruptive to any joint CIP project. A key obstacle to be surmounted is the application of the need-to-share principle between providers of early warning intelligence – especially of government provenance – and owners and operators of key critical infrastructures, up to and including the introduction of a clearance process [19] . But the information requirement, too, it should go without saying, is bidirectional. (Which is not necessarily the case, as corporate CIP owners and operators have in the past withheld information about being successfully targeted, e.g. by hackers or corporate or government spies. The reason is obviously to sustain good investor relations and avoid reputational impact). As Donahue and Zeckhauser put it:

The most consistently valid argument for a collaborative approach to infrastructure security turns on information. The government itself almost certainly lacks the fine-grained understanding of particular infrastructure assets..., necessary to mount the most robust and least costly defences. Yet the public sector likewise can have privileged or exclusive access to information and procedural options – intelligence data, negotiations with foreign governments, the right to detain a suspect or tap a phone line – that could, in principle, be extended to the private sector but generally are not.[20]

Alas, the latter issue still constitutes an impediment to effective public private security collaboration – at least formally. Discussions are underway to amend (others would argue to overhaul) the intelligence service law (NDB) to the effect of introducing dedicated security personnel of owners and operators of highly critical infrastructures into an expanded intelligence fusion platform operated by the Federal Intelligence Service [21] ; Swissgrid would, in all likelihood, qualify for membership.

As seen by the present writer, the key structural challenge that the SKI Pilot Project had to meet was the successful streamlining and management of the potential, even likely, fluid public-private divergence of priorities. For this reason, Donahue and Zeckhauser state:

Before designing a collaborative infrastructure security effort, government must first appraise the threat-reduction goal. It must map, as precisely as data permit, both the public and the private risks embodied in the status quo – the nature and dimensions of the threat, the degree to which public and private vulnerabilities overlap or diverge, and the major uncertainties surrounding this appraisal. This first step, in short, involves figuring out what success looks like.[22]

It is therefore imperative that public private governance in CIP formulate a clear, common goal based on a common understanding of mutual necessity.

In light of the responsibility for the national bulk power energy supply; an absence of binding regulatory security standards and the self-evident vulnerability of the arguably single most critical infrastructure with an immediate, palpable economic and public security impact across the length and breadth of the country, Swissgrid is well advised to encourage a collaborative governance CIP framework with the relevant federal government agencies. This set of circumstances applies with some urgency to the questions of roles, responsibilities and, from a corporate point of view in particular, to liabilities of privately organized owners and operators of highly critical national infrastructures. The reasons are not all self-evident, yet for that no less compelling: not only does the currently manifest endeavour at public private CIP collaborative governance, the SKI Pilot Project, come equipped with a government-cleared methodology of determining critical processes and, hence, protection targets, thus creating the foundation for defining a division of labour and clarifying responsibilities; it also gives Swissgrid the opportunity to provide direct input into what might well be tomorrow's regulatory capstones. Thus, the federal government benefits directly from the know-how and skills of the CI owner and operator; and the private entity, as a quid pro quo, can help shape the future regulatory environment. Ultimately, where there are real stakes for the involved parties, a mutual effort arguably has the best chance of succeeding.

[19] A proposal from the Swiss Ministry of Defence to provide clearances for key personnel employed by highly critical infrastructure owners and operators is under way concurrently with the Swissgrid CIP project.

[20] J.P. Donahue and R.J. Zeckhauser, „Public-Private Collaboration for Infrastructure Security," in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (Cambridge University Press, New York, 2006), pp. 429-456, p. 437.

[21] Also cf. fn. 17.

[22] Donahue and R.J. Zeckhauser, 453.

ARES Conference
The International Dependability Conference

Call for Participation

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

August 24–28, 2015

Université Paul Sabatier Toulouse, France

The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism

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

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

The aim of the **First International Workshop on Future Scenarios for CyberCrime and CyberTerrorism** is to anticipate the future of cyber-criminal activities, enabling governments, businesses and citizens to prepare themselves for the risks and challenges of the coming years. The first step towards the creation of a strategic roadmap for future research on cyber-crime and cyber-terrorism is the building of scenarios on the future transformations of the society, business activities, production of goods, commodities, etc. The aim of FCCT 2015 is to create a forum on scenario building and creation of research roadmaps for cyber-crime and cyber-terrorism. The building of future scenarios should allow the identification of the main driving forces and factors that will shape the evolution of cybercrime and cyberterrorism. A principled analysis of the differences between the current state of play and the future scenarios should allow drawing roadmaps and priorities of future research on cybercrime and cyberterrorism.

The influence of triggered earthquakes on critical lifelines in the North of the Netherlands

Introduction

The production of the gas fields in the North of the Netherlands leads to changing rock stresses in and around the reservoir. The change in stress on existing fault planes can lead to a sudden small slip of the plane with a release of seismic energy as a consequence. Since 1986, a low intensity seismic activity is present in the Groningen gas-field area (Netherlands), due to the tremors following the compaction of the gas reservoir due to stress decrease. An extensive study performed by the Dutch Meteorological Institute (KNMI), see Dorst et al. (2013), shows that in the last decades (2003-2013), the seismic activity changed from low intensity activity with a constant events rate per year to a higher rate with slightly increasing magnitude. The depth of the earthquakes is at 2.5 - 3 km, being the depth of the gas reservoir. The reservoir consists of Rothliegendes sandstone with a thickness of 150- 200 m. and is overlain by Zechstein salt . On 16 August 2012 an earthquake with a local magnitude of M = 3.6 occurred near Huizinge in the neighbourhood of Loppersum in the Northern part of the Province of Groningen. This earthquake is the largest earthquake so far.

In the North of the Netherlands and the rest of the world the energy and water pipelines and the electricity connections can be considered as the lifelines of our society. Damage to pipelines may lead to environmental disasters or can in worse case lead to casualties, in case of toxic or flammable substances transported in pipelines. The damage or the disruption of the electricity lines also will cause a major economic impact, especially for industrial areas, The Groningen gas field serves the rest of Netherlands and is also used for export. Furthermore imported Norwegian and Russian gas passes through the area affected by earthquakes. A large portion of the electricity production is located in the Eemshaven area and high voltage lines cross the earthquake affected area. Also, electricity power stations are present in the earthquake area. Furthermore production as well as gas transmission for a large portion depend on the availability of high voltage power.

Studies on the vulnerability of pipelines are available in literature (O'Rourke (1998) or Pitilakis et al (2010)) based on observational analysis of the performance of lifelines subjected to earthquakes of large magnitude. However in the north of the Netherlands the triggered seismic activity is not of tectonically nature and is characterised by short duration of the signal and triggering a local seismic response. Therefore recently several studies have been carried out to investigate the lifelines in the North of the Netherlands.

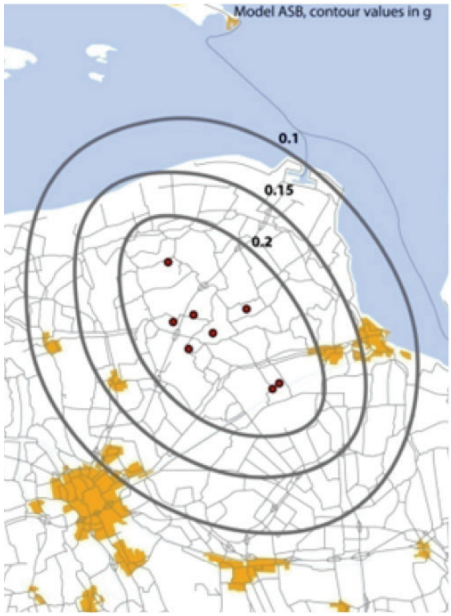


Figure 1: Contours for the highest median PGA due to a Mw=5 event in the area spanned by historical M≥3 events. Seismic sources are indicated as red circles, contours as grey lines. Median values are shown in g (Dost et al. 2013).

Henk Kruse
senior researcher at Deltares.

e-mail: henk.kruse@deltares.nl

Mandy Korff MSc
Business Development and Senior Advisor at Deltares.

e-mail: mandy.korff@deltares.nl

Jan Spiekhout Executie Senior Consultant at DNV-GL has contributed as well.

Earthquakes

The magnitude of an earthquake is often expressed using Richter's scale or by means of the peak ground acceleration (PGA). An earthquake leads to two types of soil deformations near the surface:

1) **Temporary soil movement** due to the soil vibration due to the passing of the waves. When the waves are near to the surface an increase of the wave amplitude is possible, where the soil properties and layering influences the amplitude of the vibrations.

2) **Permanent soil movement** can also be induced by the earthquakes. The following permanent movements can be distinguished:

- Liquefaction of loose packed granular soils.
- Densification of granular soils.
- Mass movements along natural or artificial slopes.
- (Tektonic) movement along faults.

The term "liquefaction" indicates a phenomenon for which a saturated, cohesion less soil loses its shear resistance due to the accumulation of plastic deformations caused by transient and cyclic force actions in un-drained conditions. Liquefaction can lead to large permanent soil deformations and is therefore an important mechanism in the evaluation of the effects of earthquakes. The Eurocode 8 (2005) is the guideline for the assessment of all types of structures such as pipelines and electricity pylons, but also the installations such as power stations and pressure units.

Figure 2: An example of liquefaction due to a tectonic earthquake (Roermond 1992)

Lifelines

Lifelines are often grouped into six principal types of systems (in alphabetical order): electric power, gas and liquid fuels, telecommunications, transportation, 3 wastewater facilities, and water supply. These systems share three common characteristics: geographical dispersion, interconnectivity, and diversity (O Rourke, 1998). Lifelines are geographically dispersed over broad areas, and are exposed to a wide range of seismic and geotechnical hazards. They are interconnected and interdependent. Each lifeline system is composed of many interconnected facilities and is influenced by the performance of other lifeline systems.

In this paper the vulnerability of the following groups of lifelines with respect to triggered earthquakes in the Netherlands are considered:

- Gas transportation network
- Electricity transportation network

The local distribution networks are not considered.

The subsequent figures show the two lifeline networks schematically.

Evaluation fragility of lifelines

In order to evaluate the impact of a triggered earthquake on the electricity and gas network in the North of the Netherlands, a global analysis was carried out. In this analysis the strength of the different elements of the network was considered. The strength of the element was defined as the maximum peak ground acceleration at which

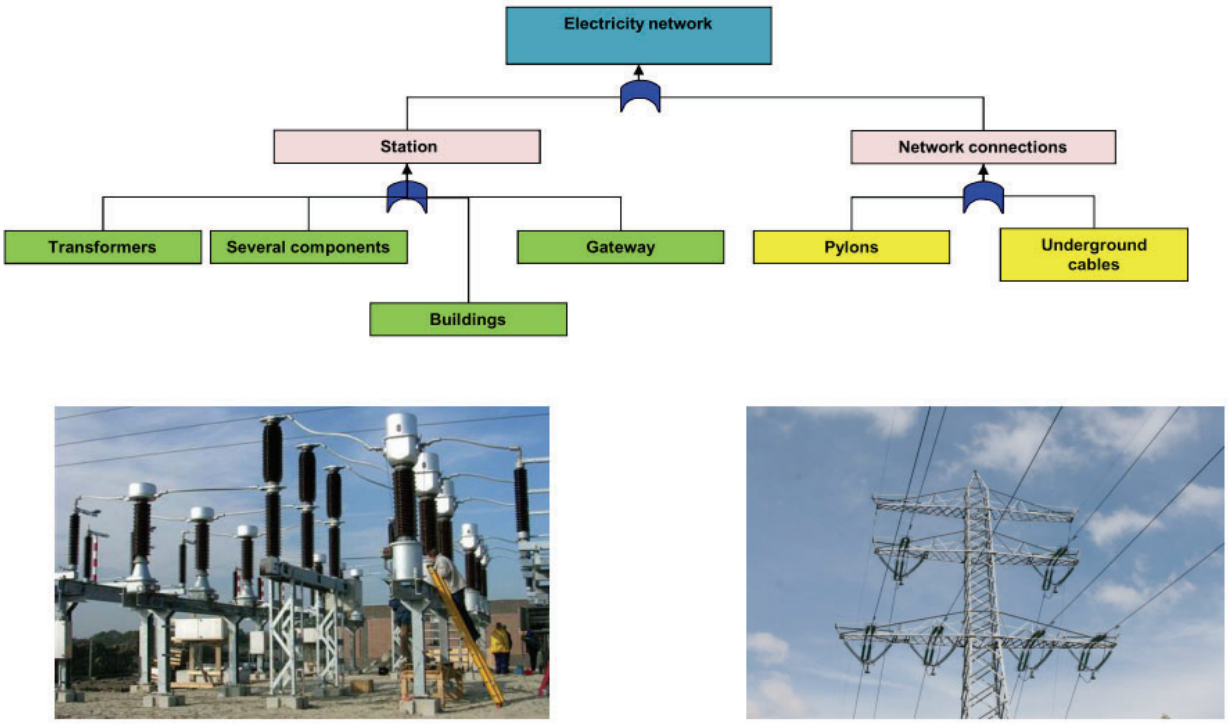


Figure 3: The Electricity transportation network

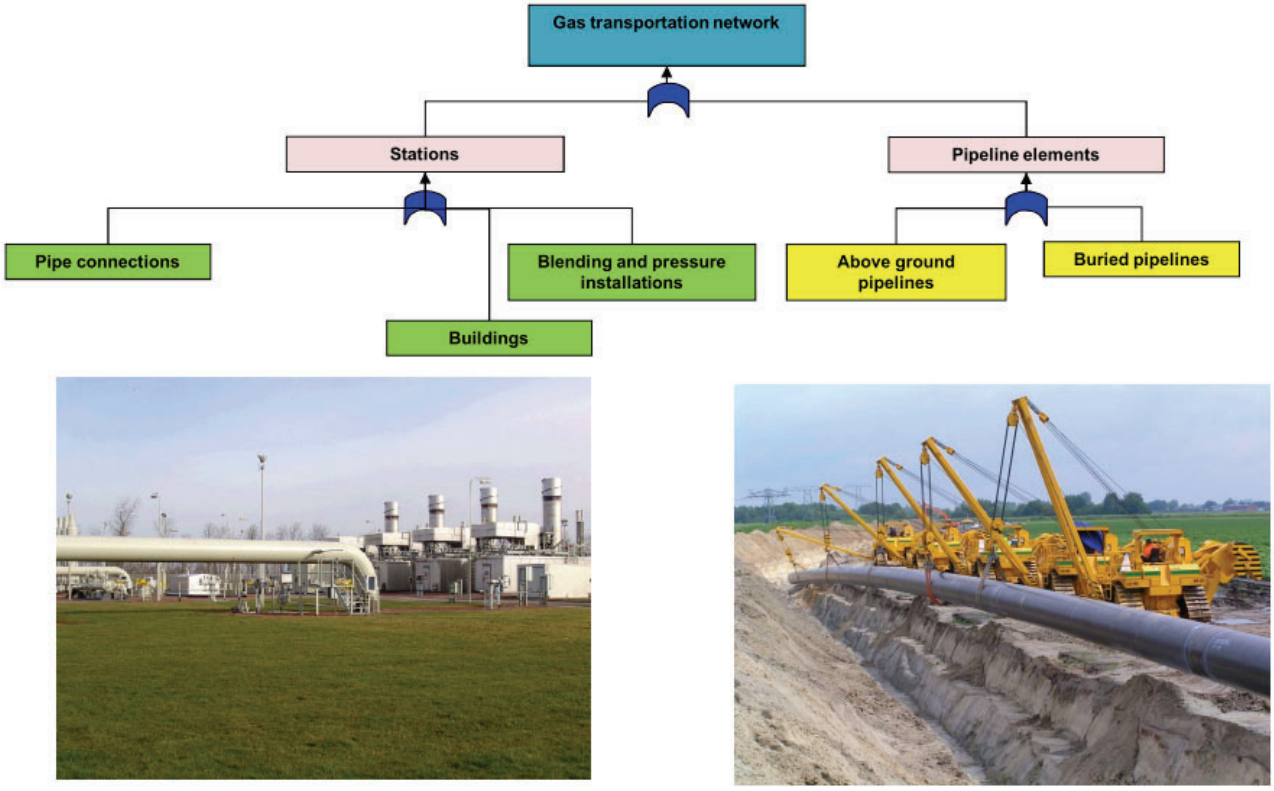


Figure 4: The Gas transportation network

damage could be expected. This maximum value was deduced by calculations or by specifications available for certain installations and components.

The gas transportation pipelines in the north of the Netherlands are buried and the soil cover is more than 1 meter. The predominantly steel pipes are able to withstand an earthquake of significantly more than 0,5 g. Some sections with curves or sections where the pipelines cross other infrastructure such as railways, river dikes and canals or rivers are less robust than the straight sections, but if the condition of the pipeline is good (some poorly welded pipeline sections can be expected to withstand a significantly lower earthquake level), these pipeline sections are also able to withstand an earthquake of about 0,5 g. The connections of the above ground pipelines at the blending and pressure stations are not yet all considered in detail, but it appears that the increase in stress level of the above ground pipelines is not extremely high. During the analysis (Korf et al 2013) was recognised that the configuration of the above ground pipelines and the presence of supports significantly influence the resonance effect.

The above corresponds to findings in international literature (ASCE 2011), about experiences with earthquakes:

Figure 5: Example of a designed bearing support that is not designed for earthquakes ("one foot support")

- Steel pipelines continuously welded and with good weld quality, are able to withstand the shaking effect induced by an earthquake.
- Piping on stations with simple piping configurations in general possess no problem with regard to the shaking effect from earthquakes.
- Machinery, if bolted to the floor, generally anchor bolts are oversized, possess no major problems with regard to the shaking effect from earthquake. Because of vibration there is a probability of a trip, but after the earthquake machinery can often be restarted.

Besides the evaluation of the so called piping systems, secondary mechanisms were also evaluated. Although a first consideration does not emphasize many risks, a further analysis showed the importance of the following mechanisms:

- Collapse of masonry buildings at the gas reception locations on operation equipment.
- Collapse of not well-designed bearing supports.
- Collapse of raised computer floors on which the operation system is situated.

Secondary mechanism both for the electricity network and the gas network can be important. Problems can be expected with the raised floors and control and computer cabinets in control rooms. Unreinforced raised floors with cabinets placed on the floor or cabinets which are not fixed, may cause significant damage to the control room. The consequence could be an out of service period with a duration of several months.

Figure 6: Raised floors and cabinets in control room on a raised floor.

Disruption of electricity lines is internationally rather common in case of earthquakes. Until now, no damage has been reported in the North of the Netherlands resulting from the gas extraction induced vibrations. The Netherlands is known to have a high level of supply security for high voltage. Although the stations with the transformers are not located in the area where the epicentres of the future highest magnitude earthquakes are expected, there is a possible malfunctioning of the different components of the transformer station. Most of the components belong to vibration class AF 3 (a maximum acceleration of 0,3 g), but some of them start mal functioning at 0.2 g. The transformers themselves are designed to withstand accelerations of 0.5 g and can be considered as robust, however because of wave effects (oil filled transformer) from the earthquake there will be a trip that can easily be restored after the earthquake. The different types of pylons can with stand an earthquake of 0,25 g without damage. It should be noticed that especially the new types of pylons can withstand an earthquake with a higher PGA. Besides the evaluation of the different components and the pylons, the secondary equipment such as operation devices need to be evaluated because it is expected that some devices can start malfunctioning at PGA levels of 0,1 or 0,2 g.

The above mentioned evaluation results are general results achieved by a global analysis. It should be mentioned that the effect of permanent ground deformation must be studied on a more detailed level for a final conclusion about the networks. The permanent soil deformations depend on the local soil conditions and are therefore site specific. Especially the effects of liquefaction require further investigation.

Conclusions

Recent developments in the analysis of seismic activity of the Groningen gas field showed that the estimated maximum magnitude for induced events in the region can be higher than previously thought. Due to the increase of the expected peak ground acceleration, the most important lifelines of the Northern Netherlands were evaluated with respects to earthquakes. The electricity network and the main gas transportation network were evaluated.

In the analysis carried out for the evaluation, the strength of the different elements of the networks was considered. The strength of the element was defined as the maximum peak ground acceleration at which damage could be expected. The results of the evaluation show which elements require attention and can be used for the definition of further research.

The permanent soil deformations depend on the local soil conditions and can be of major importance for a network. Especially the effects of liquefaction may yield large permanent ground deformations and require attention in further investigations

Literature

Dost B., Caccavale M., van Eck T., Kraaijpoel D. (2013). "Report on the expected PGV and PGA values for induced earthquakes in the Groningen area" Report KNMI (Koninklijk Nederlands Meteorologisch Instituut),Utrecht, The Netherlands.

Eurocode 8 (2005) Design of structures for earthquake resistance. General rules, seismic action, design rules for buildings, foundations and retaining structures. Tomas Telford books, first published in 2005

O'Rourke, T. D. (1998) An Overview of Geotechnical and Lifeline Earthquake Engineering, ASCE Geotechnical Special Publication No. 75, Pakoulis, P., M. Yegian, and D. Holtz, Eds., Reston, VA, Vol. II, 1998, 1392-1426.

Pitilakis K., Crowley H., Kaynia A.(2014) " SYNER-G: Typology Definition and Fragility Functions for Physical Elements at Seismic Risk" ISBN 978-94-007-7872-6. Spinger

Korff M., H.M.G. Kruse,. T.P. Stoutjesdijk, J. Breedeveld, G.A. van den Ham, P. Holscher, G. de Lange, P. Meijers, E. Vastenburg, Vermaas. And M.A.T. Visschedijk (2013) Effecten geïnduceerde aardbevingen op kritische infrastructuur Groningen Quick Scan naar de sterkte van de infrastructuur, Deltares report Delft

ASCE (2011) Guidelines for Seismic Evaluation and Design of Petrochemical Facilities, second edition, ASCE, ISBN 13: 978-0-7844-1140-7, Reston VA, 2011

ROADAPT:

Roads for today, adapted for tomorrow

The goal of CEDR project ROADAPT is to provide risk based methods and tools for assessing climate change risks for roads, towards an action plan for adaptation

Infrastructures are the backbone of our society. Citizens, companies and governments have come to rely on and expect uninterrupted availability of the road network. In the same time it is generally understood that the world's climate is changing and that this will have significant effects on the road infrastructure. Since road infrastructure is vital to society, climate change calls for timely adaptation.

However there are great uncertainties involved in both the projections of future climate change plus their effects on the road infrastructure and related socio-economic developments. In the meantime, there is a constant need for decisions and development of the road transport system.

The ROADAPT project is part of the CEDR Call 2012 'Road owners adapting to climate change' in which is stated that one of the most important tasks of the road owners is the prioritisation of measures in order to maximise availability with reasonable costs. This includes a risk based approach addressing causes, effects and consequences of weather related events to identify the top risk that need to be taken action on with mitigating measures. In this respect the RIMAROCC framework (Risk Management for Roads in a Changing Climate) has been developed within ERA NET ROAD in 2011.

Objectives

ROADAPT aims at a further development of this framework into practical and useful methods for road owners and road operators. Output of the ROADAPT project is one ROADAPT-RIMAROCC integrating guideline containing different parts (Figure 1):

A. Guidelines on the use of climate change projections.
B. Guidelines on the application of a QuickScan on climate change risks for roads.
C. Guidelines on how to perform a detailed vulnerability assessment.
D. Guidelines on how to perform a socio economic impact assessment.
E. Guidelines on how to come to an adaptation strategy.

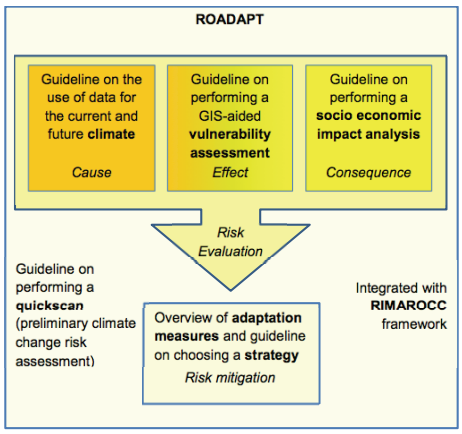


Figure 1: The ROADAPT guidelines

Output

Climate change

Part A provides background information and guidelines for tailored and consistent climate data and information for studies on the impact of the current and future climate for transnational road networks in Europe, suitable for National Road Authorities (NRA's). The document can be used by NRA's to judge the climate information that they receive from e.g. (impact) research institutes, consultancies, and to find answers to their questions. It can also be used by impact researchers and consultancies to select the most appropriate datasets and methods for a certain application. Also requirements related to climate data are included.

Thomas Bles

senior consultant at Deltares.

Thomas worked on the ERA NET ROAD project RIMAROCC (risk management for roads in a changing climate). The results of this research project have been applied on the Dutch national highway network, aiming at gaining insight in the risks for flooding plus an action perspective for keeping in control in the future.

Since 2012 he is the coordinator of the CEDR ROADAPT project that aims at developing hands on methods as an extension to the RIMAROCC framework. The gained experiences are now used for the FP7 INTACT case study that focuses on extreme weather impacts on the functioning of the Rotterdam harbor with its hinterland connections.

e-mail: thomas.bles@deltares.nl

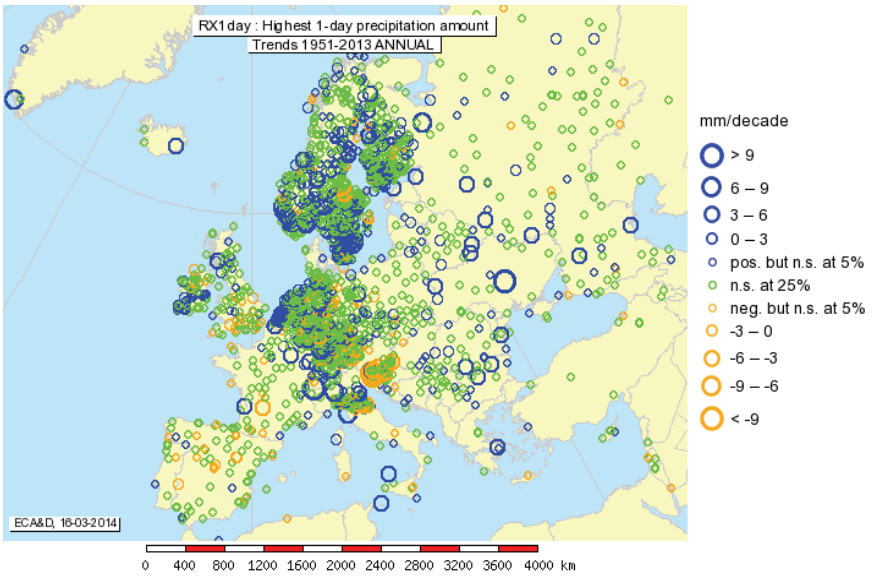


Figure 2: Trend in highest 1-day precipitation amount per year over the period 1951-2013 (ECA&D)

QuickScan

Part B provides a QuickScan method that preliminary estimates the major risks that can be associated with weather conditions both in the current climate and in the future, together with an action plan for adaptation. The identification and light-assessment of top risks allows a road authority and/or road operator to consciously and effectively focus on specific areas in their network and/ or on specific threats.
A founded first impression of climate (change) risks plus an action plan for adaptation is assessed in the QuickScan, by bringing all available knowledge, information and especially experiences of stakeholders together in three workshops. During implementation of the QuickScan method in the case studies it was learned that the brainstorming process in the QuickScan method showed to be important in terms of team building. The approach develops awareness on climate change issues, and climate related risks in general. This helps developing adaptation strategies.

Vulnerability assessment

Part C provides efficient tools for assessing vulnerabilities within the TEN-T road network. A new vulnerability assessment method, *ROADAPT VA*, has been developed. Vulnerability is assessed in a GIS using geographically distributed vulnerability factors describing the infrastructure and the area surrounding the road. The output is a GIS layer with areas with prerequisites for the analysed risk, and vulnerability scores. ROADAPT VA can be used for all climate-induced risks.

Socio Economic Impact Assessment

Part D of the ROADAPT guideline deals with the socio-economic impact assessment of road traffic event. It is based on three levels of analysis:

- Network level: considering potential impact on traffic; delays, risk of accident, GHG emissions, etc.
- Local territory level: the territories that are served by the road network with impact on economic activity.
- Economic system as a whole: at wider scale the potential impact at corridor or inter-regional, national or cross-border level (including potentially very long distance re-routings on the TERN, passing through different countries).

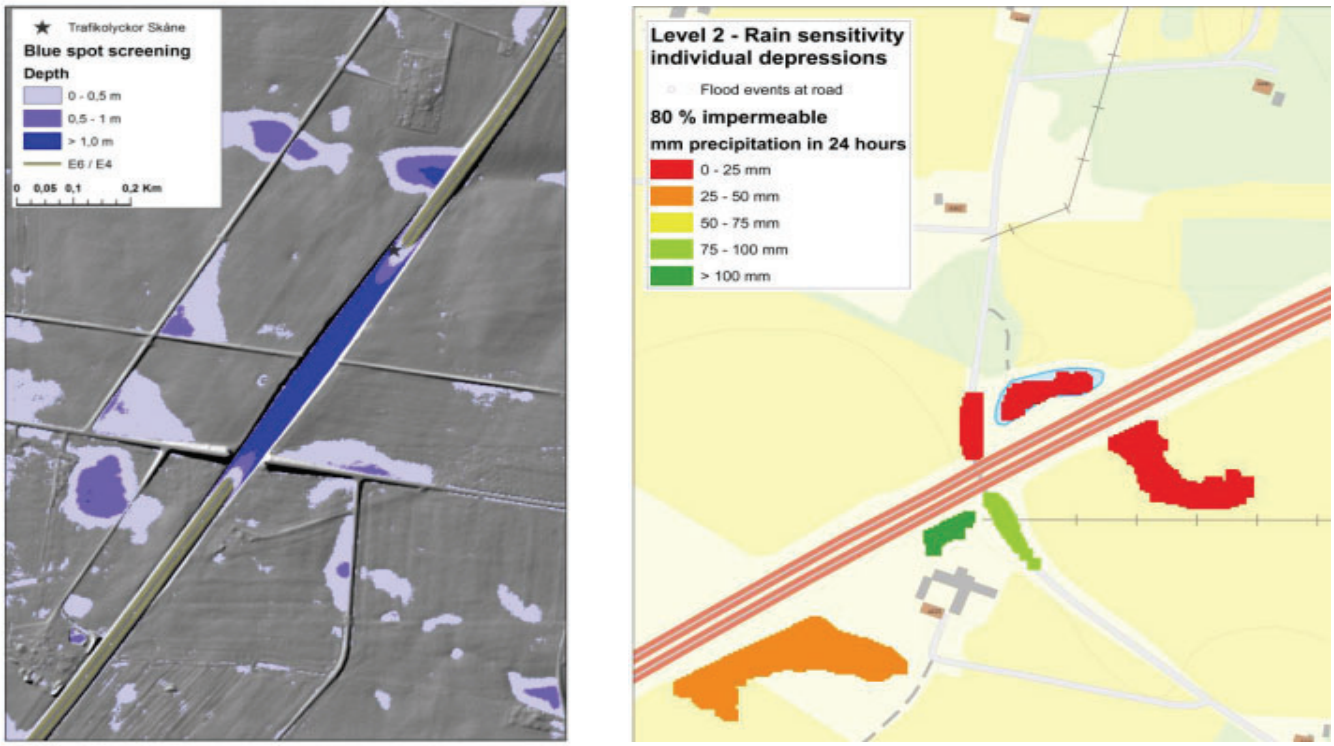


Figure 3: Vulnerability assessment of a road

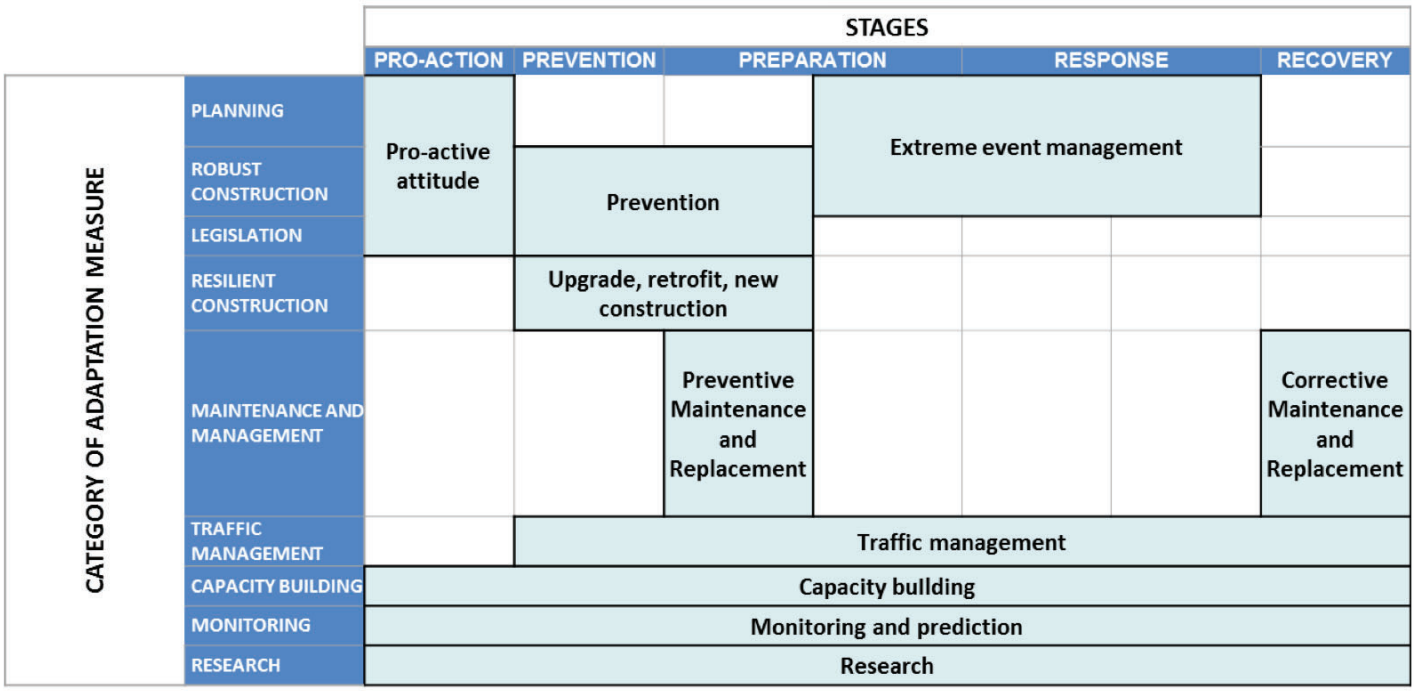


Figure 4: Policy matrix

For each of these three levels, the guideline describes methodologies that enable to evaluate the risk consequences of events linked to climate change, and in a broader manner, provides necessary information to identify the strategies to adapt to climate change.

Adaptation measures and strategies

Part E of the ROADAPT guideline presents an overview of adaptation measures and helps in selecting an adaptation strategy. This part of the guideline provides practical support in RIMAROCC step 5: Risk Mitigation. The selection of the adaptation strategies follows a 10 step approach that is applied to ten specific climate change related threats. Starting from the specific road owner's needs, the 10 step approach helps her/him to identify relevant damage mechanisms, design models, climate parameters for assessing the resilience of the asset in the current and future situation. Next, the approach identifies adaptation measures and strategies, assesses consequences of selecting measures and strategies, and identifies stakeholders to be involved. Knowledge gaps in climate change projections, adaptation technologies and essential construction and site specific data are identified. The time to market of innovative adaptation technologies is estimated to help in the development of technology roadmaps. The guideline is supported with the ROADAPT database with over 500 adaptation measures for geotechnical and drainage assets, pavements and traffic management.

Case studies

Three case studies have been carried out for validation and demonstration purposes. These are the A24 in Portugal, the Rotterdam-Ruhr corridor and the Öresund region. The latter one includes all ROADAPT outputs, where the other only focus on the QuickScan method. The case study report will become available together with the ROADAPT guideline.

More information

The ROADAPT guideline will be available in spring 2015. For more information about the project you may contact Thomas.Bles@deltares.nl (coordinator ROADAPT project) or Kees.van.Muiswinkel@rws.nl (project manager CEDR).

The research being done within the ROADAPT project is carried out as part of the CEDR Transnational Road research Programme Call 2012. The funding for the research is provided by the national road administrations of the Netherlands, Denmark, Germany and Norway. The ROADAPT consortium consists of the following partners: Deltares (the Netherlands, coordinator), SGI (Sweden), Egis (France) and KNMI (the Netherlands).

SGI

egis

Koninklijk Nederlands Meteorologisch Instituut
Ministerie van Infrastructuur en Milieu

Deltares
Enabling Delta Life

This page intentionally left blank.

Criticality of High-Voltage Direct-Current Power Transmission Systems

The complexity of modern Power Systems requires supplementary resilience to prevent undesired consequences not only of the Power System itself but also of other Critical Infrastructures. HVDC technology has the capability to reach this goal.

The continuous increase in electrical power demand and the environmental needs for adopting more Renewable Energy Sources (RES) to the generation blend alter the pattern of the state-of-the-art power systems. The large-scale power generation plants (both fossil fuel and RES generation) are often located far away from the consumers requiring transmission infrastructure to deliver the power to the residential and industrial areas. Whereas the small-scale RES offers advantages to the distribution system only when the stability of the grid can be maintained, the high Voltage Direct Current (HVDC) systems enable low loss transmission and also add stability to the grids making the power system more resilient to unexpected contingencies. HVDC technology can contribute toward future electrical power system grids in many ways:

- **Resilience:** the flexibility of HVDC system is well suited for quick responses to both operational changes and customer needs;
- **Preparedness:** HVDC network reliability assures both quality of supply and immunity/isolation between uncertainties/hazards healthy consumers'/producers' networks;
- **Economy:** HVDC technology provides efficient operation and energy management, and the flexibility to adapt to new regulations;
- **Awareness and sustainability:**the feasibility of development options given environmental constraints.

Resilience

The word resilience is specified by several definitions which, more or less, have a common meaning [CIPedia/Resilience]; "the recovery after physical stress." In Power Systems it is assumed that the resilience can be achieved by decreasing the possibility of failure, along with the reduction of the recovery time and also the limitation of the consequences from such failures.

The resilience index can be measured in the three following indicators:

- Social Indicators such as human life behaviour and blackout consequences;
- Environment Indicator;
- Economic indicator such as electricity and investment costs.

The resilience which is achieved by the HVDC technology is significant not only for the Electrical Power System but also for the other Critical Infrastructures (CIs) which are interconnected to the Power System. The so called "Cascade Effect" of generic interdependencies among CI sectors is analysed in the literature [Zimmerman, "Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction"]. The Cascade Effect by Electrical Power System disruption on some CIs is summarised as follows:

- Oil and gas: electricity for extraction and transport;
- Transportation: power for overhead transit lines;
- Water: electric power to operate pumps and treatment;
- Communication: energy to run cell towers and other transmission equipment.

Preparedness

The preparedness of the HVDC system is characterised by the robustness of the transmission, redundancy and rapidity.

Robustness of HVDC transmission: most of the HVDC systems transmit power through high-power HVDC transmission cables (a pair of cables

Nikolas Flourentzou)

Nikolas Flourentzou (PhD) is a research fellow at KIOS Research Center for Intelligent Systems and Networks of the University of Cyprus. He received the BEng degree in Electronics and Communications Engineering from the University of Birmingham, in 2002, the joint MSc degree in Power Electronics and Drives from the University of Birmingham and the University of Nottingham, in 2003, and the PhD degree in Power Systems from the University of Sydney, in 2010.
He has received the first prize of ElectricaAwards 2010 international innovation contest for the future of electricity networks by AREVA T&D (now known as ALSTOM Grid). His fields of interests are Critical Infrastructure Protection, HVDC power transmission systems, converter topologies and integration of renewable energy systems.

e-mail: flourentzou.nikolas@ucy.ac.cy

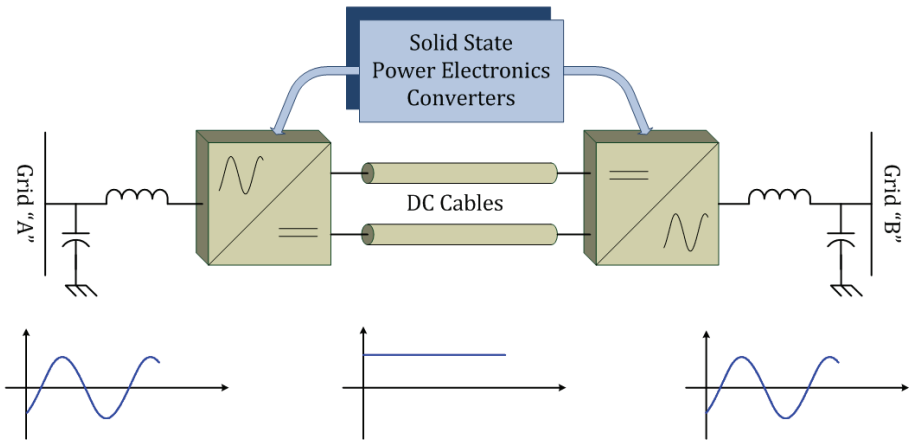


Figure 4: HVDC connection of two AC grids

instead of at least six overhead lines for equivalent power rating – High Voltage Alternating Current (HVAC) transmission through cables is extremely and unreasonably expensive over long distances and producing reactive power). The cables are much more robust than the vulnerable to extreme weather conditions overhead lines. The HVDC does not require additional vulnerable apparatuses such as high-voltage transformers which as necessary for the long distance HVAC transmission.

Redundancy: there are several methods for power redundancy on HVDC systems over faults. The simplest method for redundancy is to construct more than one HVDC systems with a pair of transmission cables each; this however would be a costly option. Since most of the recent HVDC systems are constructed in bipolar configuration, the midpoint can set to ground to allow the bipolar system operating as two monopolar systems, and therefore even during damage of one of the poles (either converter fault or cable fault) the HVDC can operate in more than half of the power-rating; the power-rating of the monopolar with the over-voltage capabilities. The midpoints of the converter stations must be capable to transfer electrical current; either by electrodes (earth return) or by conductor. A number of ground electrodes and sea electrodes are available for ground power transmission and offshore transmission, respectively. However, due to recent environmental concerns, the new HVDC systems have limitations on the continuous allowed time of operation through electrodes. Therefore, the midpoint current return through an additional conductor seems an attractive solution when the construction budget allows. The three options of midpoint current return are the neutral metallic wire, the medium-voltage DC cable and the third HVDC cable.

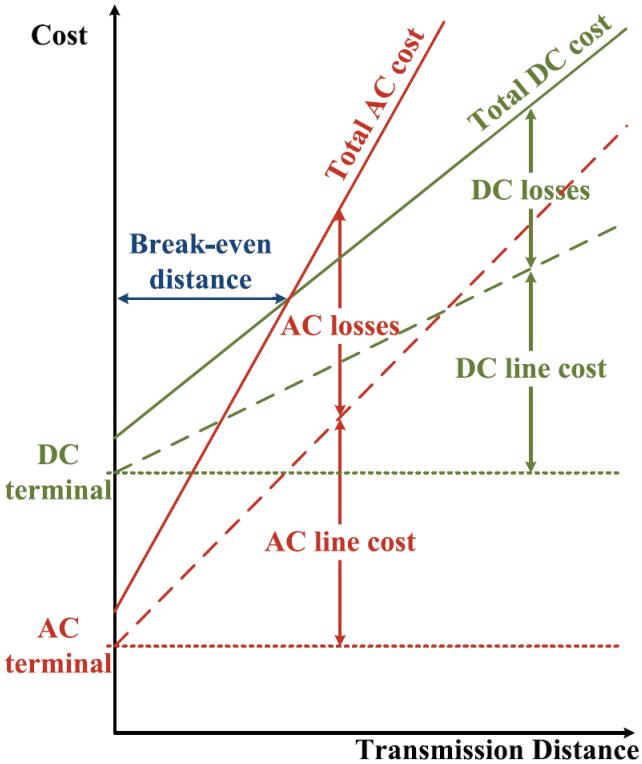


Figure 5: High-voltage transmission cost

- During a pole fault (converter fault or cable fault), when the bipolar HVDC system has midpoint current return through a neutral metallic wire, the HVDC system can operate in half power but the transmission losses are increased; this setup can operate until the fault is repaired.
- During a pole fault (converter fault or cable fault), when the bipolar HVDC system has midpoint current return through a medium-voltage cable, the HVDC system can operate in half power and has the overpower capability as well; this setup can operate until the fault is repaired.
- During a pole fault, when the bipolar HVDC system has midpoint current return through a third HVDC cable (identical to the cables of the two poles), the HVDC system can instantly operate in half power with overpower capability; if the fault is a converter error this setup can operate until the fault is repaired but if the fault is cable error the faulty cable can be replaced by the third HVDC cable within hours and the HVDC system can operate at full power.

Rapidity: HVDC does not suffer from power inertia like HVAC does. Since synchronisation is not required between the stations of the DC grid, it is easy to synchronise each station with the AC network (if required). Therefore, the HVDC system provides immunity between two or more AC sides, while offering simplicity in the transmission system and prevention of synchronisation errors. Recent HVDC technologies have advanced control capabilities to overcome some AC faults such as unbalanced of the three phases, frequency errors, and voltage dips. Recent HVDC technologies allow "low-voltage ride through" capabilities to support the network during a voltage dip without any power interruption.

Economy

Investment on resilience and preparedness over the threads of critical infrastructures is an important dynamic element of CIP. Studies demonstrate the economic benefits of increasing electric grid resilience to weather outages.

- HVDC systems are the widely known economical solution for bulk power transmission over long distances. The investment cost is

lower after the break-even distance (Figure 5);
- The number of transmission lines for HVDC transmission is much less which reduces the material required and hence the cost;
- The HVDC system requires simple power transformers instead of phase-shifting transformers. Therefore, they are simpler to design and manufacture, do not require additional material and hence the cost is reduced.

Awareness & Sustainability

For the sustainability and awareness of the HVDC systems is explained by its resourcefulness. Studies on the total amount of material required for bulk power transmission over long distances determines the economic, environmental and life-time benefits of HVDC over HVAC transmission.

- HVDC systems are the widely known for the power sea-crossing and off-shore connections capabilities;
- The transmission corridor required for HVDC system is significantly narrower than the corridor required for HVAC system (Figure 67) – using HVDC cables instead of overhead lines the area required is much less and by considering sufficient laying depth agricultural activities are safe above the cables (Figure 78);
- The number of transmission lines or cables for the HVDC system is much less, which, from the environmental point of view, means less material is required per Watt;
- The DC transmission does not require phase-shifting transformers to control the power flow through specific lines in a complex power transmission network. The phase-shifting transformers are vulnerable and involve additional material, cost and special designed according to individual factors (such as voltage, power, climate, system topography, sound level and many more);
- The latest HVDC technologies are capable to provide the amount of reactive power required for the load regardless of the reactive power produced by the generation, thus, the effort of maintaining the stability of the power system is prevented;
- Supports reliable connection and interconnection of very weak AC systems.

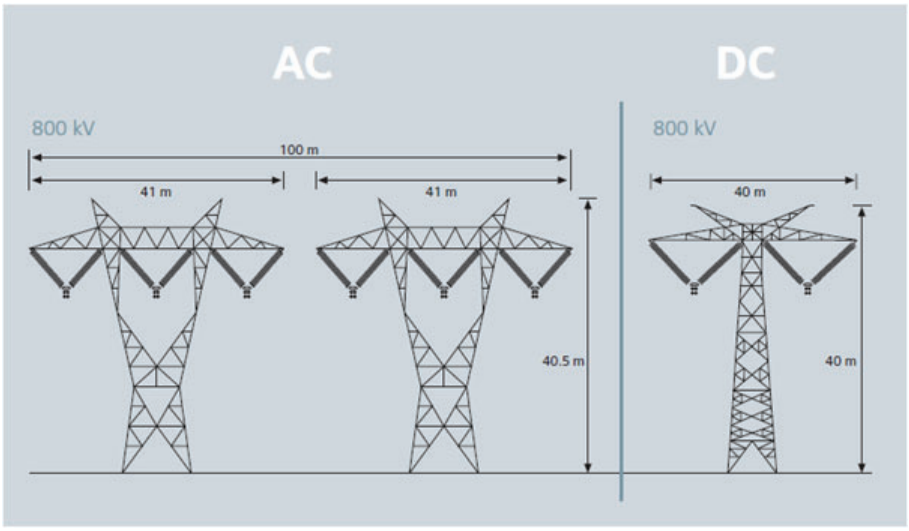


Figure 6: Transmission corridor width of HVAC vs. HVDC [SIEMENS.com]

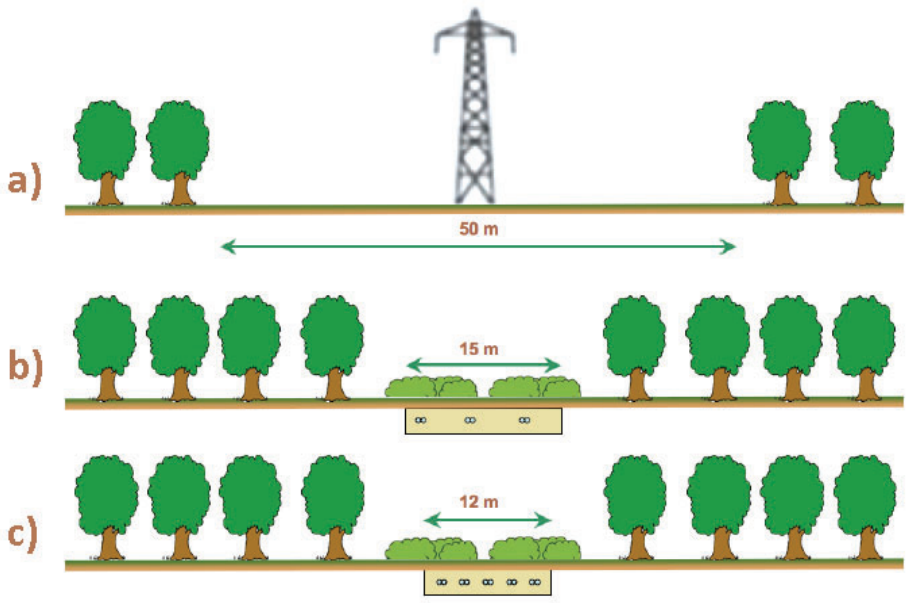


Figure 7: Transmission layouts for 5 GW HVDC systems; a) 800 kV overhead lines, b) 3 pairs of 500 kV MI cables, c) 5 pairs of 320 kV XLPE cables [europacable.com]

These are the characteristics that have been inspiring the engineers of more than half century to design a more sustainable, more efficient and less polluted power system.

Threats to CIs

The numerous disastrous events of the last decades proved us that modern societies depend on CIs. The vulnerability of the CIs is reminded not only by the natural hazards but also from events caused by humans.

The "anthropogenic threats", such as the terrorist attacks of 9/11 (2001), Madrid (2004) and London (2005) but also the system failures of Eschede train disaster (1998) and Vasilikos Power Station explosion (2011) specify the need for substantial CI resilience and preparedness.

Infrastructures are also at risk from natural disasters such as hurricane "Kyrill" (2007), the heat waves of recent years (for example 2003), the drought in Africa (2011), or the great floods in China (1998) and Pakistan (2010) and the tsunami in Fukushima (2011).

The hazards which pose the highest threat to Critical Infrastructures can be categorised as follows:

Natural threats:
- storms, tornadoes

- extreme rainfall, flood
- droughts
- earthquakes
- epidemics / pandemics

Anthropogenic threats:
- accidents
- system failures
- sabotage, malicious programs
- terrorism
- war

The HVDC power transmission systems are more resilient during storms, tornadoes, extreme rainfall, droughts and earthquakes compared to AC power transmission. Since the sensitive apparatuses are enclosed into a solid building the risks from the above threats are not as high as if they would be on a power yard. Furthermore, in most systems built with the latest HVDC technology, the power is transferred through underground and/or submarine cables which are less vulnerable on weather conditions than transmission lines.

Although, the HVDC systems do not offer any significant advantages over anthropogenic threats, special design considerations are usually applied over cyber-attack, physical-attack, hybrid-attack (combined cyber and physical) and several accidents.

Further Information

Energy saving, emission reduction and low carbon economy seems to be major global targets of our era. Long term projects (such as DESERTEC Foundation, Mediterranean Solar Plan and Medgrid among others) aim to accomplish the above targets by energy utilisation and integration of the optimum mixture of RES to the Electrical Power Grid. Such goal can be achieved by introducing several HVDC systems to connect/interconnect large areas, islands, countries and even continents. Therefore, a vast area (i.e., entire Europe) can be connected by an enormous DC Grid, having different weather conditions at each end of the grid (i.e., from Ireland to Greece), allowing reduction of conventional power generation and hence reduction of fossil/nuclear fuel consumption and reduction of CO_2 gas emission.

A lot of investments are devoted in research to find ways to increase the power-rating and efficiency of the HVDC systems, while keeping the controllability and reliability at the high standards of the recent HVDC technologies. The recent trends involve the development of the high-temperature superconducting DC power cables, high-power gas-insulated transmission lines, hybrid DC circuit breakers and super-conducting switching valves, along with the invention of several high-voltage apparatuses such as vacuumed-channel transistors, new materials etc.

One of the major drawbacks of creating a multi-terminal HVDC grid is the lack of DC circuit breakers. Latest invention of hybrid circuit breakers which combine mechanical and semiconductor technologies seem promising to reach the voltage-ratings required for the grid of the near future. Therefore, further control and security will be added to the DC transmission grids.

Existing overhead AC lines can be converted to overhead HVDC lines. Such a conversion can increase the AC power level by a factor of more than 2.5 for the same current density [ABB review]. The specific transmission losses are reduced by more than half. Converting existing AC power lines to HVDC not only to increases the power transmission capacity and efficiency but also to increase the resilience of the long distance interconnected areas.

System Robustness Analysis in Support of Flood and Drought Risk Management

Summary of a PhD Study

Flood and drought impacts are increasing

Floods and droughts cause increasingly large impacts on societies worldwide. The probability of these extreme events is also expected to increase due to climate change. Water management primarily tries to protect against floods and droughts, for example by building flood protection infrastructure and reservoirs. Despite structural measures to prevent flooding and water shortage, 100% protection can never be provided.

Therefore, over the past decades, water management has shifted to a risk-based approach. This means that policies do not only aim at reducing the probability of occurrence of floods and droughts, but also include actions to limit the consequences of potential flooding or water shortage. Both types of measures may aid to reduce flood and drought risk to an acceptable level.

Limitations of a risk approach

Even if the risk is reduced to an acceptable level, extremely large impacts are not avoided, as demonstrated by recent floods and droughts events with devastating impact. A risk approach considers ten casualties per year in 100 years equal to 1000 casualties at once during the same period. However, the latter have a much larger societal impact. Large impacts occurring at once are considered unacceptable when it is difficult to recover from them. Hence, not only the risk but also the potential impacts should be reduced to an acceptable level. There is a need for decision support methods that help avoiding unacceptably large impacts from floods and droughts.

Another reason why risk may not suffice as decision-criterion is that it is uncertain, under both current and future conditions. Estimating current risk requires assumptions on return periods of events that do not occur in measured data. Furthermore, it is uncertain how risks develop into the future, because of uncertain future climate (and climate variability) and socio-economic developments. It is therefore difficult to decide on the most cost-effective strategy in terms of the effect on risk. This further underpins the need for additional decision criteria that take uncertainty into account.

Robustness: a new perspective on dealing with extreme events

The concept of robustness seems useful for dealing with extreme events. Robustness is known from other areas such as engineering and biology, where networks or systems have to maintain their functionality even when some components fail. Areas prone to floods or droughts can be understood as systems. When these systems can remain functioning during flood and drought events, it is likely that unmanageable impacts (i.e. disasters) are avoided. In this thesis, the concept of robustness is made operational by proposing quantifiable criteria. These criteria were tested in two flood cases and two drought cases. The cases have demonstrated the applicability of the framework and have provided insight into the characteristics that influence system robustness.

Furthermore, the case studies demonstrated that assessing system robustness may change the preference ordering of management strategies.

Robustness = resistance + resilience

In the thesis, system robustness is defined as the ability of a system to remain functioning under a large range of disturbance magnitudes. Disturbances in this thesis are flood waves in river valleys that may cause flooding, and droughts (resulting from precipitation deficit or streamflow deficit) that may cause water shortage.

Marjolein Mens

Dr. Mens graduated in January 2006 at the department of Water Resources of Wageningen Univ. Since March 2006 she has been working at WL | Delft Hydraulics and later Deltares, where Ms. Mens now works as a researcher in the field of flood risk management. She has been involved in consultancy projects for the National Gov. to calculate flood risks and to advise on the national safety policy. Also, she has been working on decision support systems for a broad range of end-users. Because of her experience in flood risk management, Ms. Mens is frequently involved in climate change adaptation projects. For example, the European research project RIMAROCC and an advise about climate-proofing of the Netherlands. In 2015 ms. Mens finished her PhD-research on the use of robustness in decision-making for long-term water management.

e-mail: marjolein.mens@deltares.nl

To remain functioning' means either no impact from the disturbance or limited impact and quick recovery. System robustness is a function of two other characteristics: resistance and resilience. Disturbances that cause no impact are in the resistance range; larger disturbances that cause limited impact from which the area can recover are in the resilience range. Robustness analysis aims to identify these ranges for a specific system.

Three criteria to quantify robustness

To obtain insight into robustness, the thesis proposes three criteria to describe a system's response to disturbances:

1. The resistance threshold is the point where the impact becomes greater than zero;
2. The proportionality refers to the graduality of the response increases with increasing disturbance magnitudes;
3. The manageability is the ability to keep the response below a level from which recovery is difficult or impossible.

The **first criterion** refers to the smallest disturbance magnitude causing significant impacts and is strongly related to the system's design standard (e.g., protection against floods or reservoir capacity to prevent water shortage).
The **second criterion** originates from the flood risk literature; sudden floods are considered undesirable because people have too little time to prepare, leading to large impacts. Sudden events should thus be avoided in a robust system.
The **third criterion** compares the impact with a critical recovery threshold. This threshold represents the physical and socio-economic capacity to recover from the impacts of floods and droughts. When impacts exceed the critical threshold, it is assumed that the recovery time is long and that long-term impacts will be unacceptably high.

A robustness perspective may change decisions

In flood risk management, measures are often prioritized based on risk (a metric that combines flood probabilities and corresponding impact), in comparison to the investment costs. Both flood cases showed that a variety of measures may reduce the risk, but not all of those measures enhance system robustness. This means that different measures may be preferred when their effect on system robustness is also taken into account.

Three criteria to quantify robustness:

- Resistance threshold
- Proportionality
- Manageability

In drought risk management, measures are often assessed on the resulting water supply reliability (i.e., the probability of meeting water demand). The drought cases have demonstrated that not all measures that increase the supply reliability also reduce the drought impacts over the full range of plausible drought events. Thus, different measures may be preferred when their effect on system robustness is also taken into account.

What characterizes a robust flood risk system?

Systems with high protection levels for the entire river valley have high resistance against flood waves. However, when protection's levels are equal everywhere, sudden floods can still occur and affect a large and/or vulnerable area. Such a system is not considered robust to flood waves. Robustness of a system with a high resistance threshold can be increased by differentiating protection levels, so that least-vulnerable areas will flood first and more-vulnerable areas are relieved. Another option is to build virtually unbreachable embankments. This prevents sudden flooding and limits the inundation and thus the impact. A combination of unbreachable embankments that are also differentiated in height will further increase robustness to extreme floods. Finally, measures aimed at impact reduction increase robustness when they reduce the impacts below the recovery threshold.

What characterizes a robust drought risk system?

Drought risk systems have a high resistance threshold when their storage capacity is large compared to the demand, for example systems with large reservoirs. The resistance threshold is related to the supply reliability. A variety of supply sources will increase the supply reliability and the resistance threshold. When the objective is to reduce impacts from extreme drought events, demand reduction and temporary measures are more effective than increasing supply on a structural basis. In agricultural drought risk systems, crop diversity and having alternative sources of supply will enhance robustness to drought (see for example Figure 1).

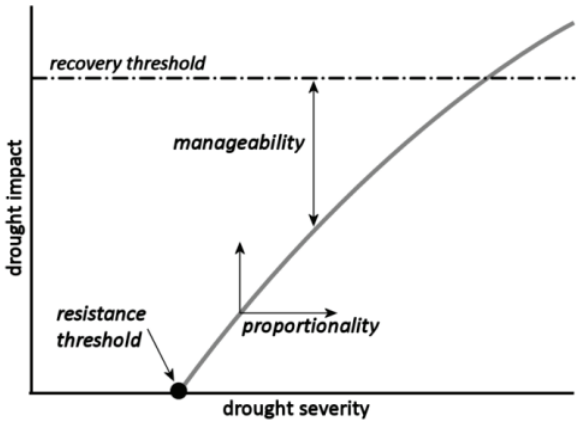


Figure 1: Example response curve: relationship between drought severity and drought impact and robustness criteria

Conclusion

In conclusion, this thesis contributed to decision making in flood and drought risk management, by developing and testing an additional decision criterion. A robustness analysis method supports the assessment of impacts from extreme events, and is applicable on flood and drought risk systems. A robustness perspective supports decision makers in exploring low-probability/high-impact events and considering whether these impacts are societally acceptable. Quantifying robustness inspires the development of strategies that reduce flood and drought risk in a way that disasters are avoided.

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

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

Communities rely on the use of advanced technologies and infrastructures. The term infrastructure has been used many different ways to include a variety of components. They are the "lifeline systems" that physically tie together urban areas, communities, and neighbourhoods, and facilitate the growth of local, regional, and national economies. These (inter)dependent systems work together to provide essential services of a modern society which rely on the exploitation of their capacities. ICT, energy and transport networks are enabling a change in the paradigm of citizen's interactions and reshaping relationships between communities, government, private sectors, non-profit communities and citizens.

Infrastructures play a crucial role to increase the capacity and efficiency of risk and disaster management and emergency response by providing advanced solutions and accurate information. People will be more and more involved to support public services and infrastructure systems (e.g. transportation, energy, education, health and care, etc.) for example through so-called open data, living labs and tech hubs. If from one side the future development will link networks supporting and positively feeding off each other, from the other one such (inter)dependency may be prone to failures that can propagate through a number of systems and that may results in a more severe impact for the communities. In other terms, future communities will count on more efficient services but, at the same time, can be more vulnerable due to complexity of interconnection of sophisticated infrastructure and services. This implies the need to develop new approaches and strategies to protect them, enhancing resilience and their capacity to survive to hazards and critical situations. In the recent years, **resilience** has become a key term in disaster risk management and the strengthening of infrastructures has been identified as an important field for disaster risk reduction.

With the aim of focusing on new technological and organizational trends in Emergency Management, the 2015 TIEMS Conference that will be held in Roma on September 30-October 2, 2015 at the ISA (Istituto Superiore Anticendi) will bring scientists, stakeholders and Public Authorities committed in Disaster response, emergency management and risk analysis to share their experiences and views, to present new technological tools coming from R&D projects, usually resulting from Public-Private-Partnerships.

This year is foreseen a special emphasis on Nepal Disaster after-maths. The Conference will host, among the other distinguished Keynote Lecturers, the President of the Nepal Center for Disaster Management and a Round Table Discussion (September 30, afternoon) on lessons learnt from this recent dramatic event.

Register for TIEMS now!

The TIEMS 2015 conference will be held in Rome on September 30th to October 2nd in Rome. Further information can found at the TIEMS Italian Chapter website: http://tiems.info/tiems-2015-annual-conference.html

Carmelo Di Mauro

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

e-mail: carmelo.di-mauro@jrc.it; carmelo.dimauro@riskgovernancesolutions.eu

Vittorio Rosato

Vittorio is the Head of the Computing and Technological Infrastructures Lab at ENEA Casaccia Research Centre

e-mail: vittorio.rosato@enea.it

CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (Edition 2)

Rome, 11th – 13th November 2015

Organised by University Campus Bio-Medico of Rome in coordination with ENEA (Italian National Agency for New Technologies, Energy and Sustainable Economic Development)

Scheme: 1 + 1 + 0.5 days lectures and training (3 optional modules)

Language: English

Description:

The second edition of the Master Class on Modelling, Simulation and Analysis of Critical Infrastructures will be delivered following a "module" approach. In each day an optional module will be delivered:

- Module 1 (11th November 2015): notions and theories regarding Critical Infrastructure modelling, simulation and analysis will be described in details. This module is particularly indicated for researchers and any professional needing a general approach to the topic;
- Module 2 (12th November 2015): Decision Support System and consequence analysis, description of the DSS tool developed by ENEA within the CIPRNet project. This module is particularly indicated for any type of audience, including CI operators;
- Module 3 (13th November 2015, morning): Hands-on exercises on DSS. This module is particularly indicated for technicians and researchers needing to practice with DSS.

Audiences:

- CIP Researchers and experts from different research communities (European and non-European);
- Public/governmental authorities in charge of Critical Infrastructure Protection or Civil Protection matters;
- Stakeholders from Critical Infrastructures' operators.

More information regarding the second edition of the CIPRNet Master Class and the registration form will be published soon at https://www.ciprnet.eu/endusertraining.html.

CRITIS 2015: 10th Int'l Conference on Critical Information Infrastructures Security
Call for Participation

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

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

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

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

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

Call for Participation

The CRITIS 2015 programme will be published on the conference web site http://www.critis2015.org shortly after publication of this ECN issue. Simultaneously, the registration will be opened.
The 2.5 days programme will consist of five keynotes, eighteen full paper and seven short paper presentations, demonstrations, the awarding of the second CYCA, a permanent poster exhibition, and more.

Venue

The venue is located in the heart of Berlin, vis-à-vis the Museum Island and close to railway station Hackescher Markt:

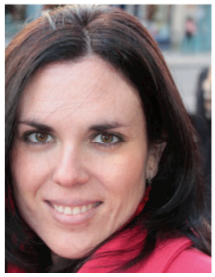
Fraunhofer Forum
Anna Louisa Karsch Street 2

Programme & Registration

To be published shortly on http://www.critis2015.org

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

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



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

Links

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

Forthcoming conferences and workshops

1st TELERISE	www.iit.cnr.it/telerise2015	Technical and LEgal aspects of data pRIvacy and Security
1st WS Cyber Crime & Terror	www.ares-conference.eu	Aug. 24 – 28, 2015, Toulouse, France
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016
TIEMS 2015 Annual Conference	http://tiems.info/tiems-2015-annual-conference.html	Sept. 20 - Oct. 2, 2015, Rome.
10th CRITIS Conference	www.critis2015.org	Call for Participation, Oct 5-7, 2015, Berlin
CIPRNet Master Class	www.ciprnet.eu/endusertraining.html	Rome, 11th – 13th November 2015
16th IEE El.Tech Conference	http://melecon2016.org	Call for Papers: open until Sept. 15, 2015
49th ESReDA Seminar	http://www.esreda.org/	Brussels, October 29-30, 2015

Institutions

National and European Information Sharing & Exchange	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange

Project home pages

FP7 CIPRNet	www.ciprnet.eu
FP7 CyberRoad	www.cyberroad-project.eu
FP7 CYSPA	www.cyspa.eu
ERNCIP Project	https://erncip-project.jrc.ec.europa.eu
FP7 INTACT FP7	http://www.intact-project.eu
PREDICT	www.predict-project.eu
ROADAPT	www.swedgeo.se/templates/SGIStandardPage____3218.aspx?epslanguage=EN

and Deltares Brochure:
https://www.deltares.nl/en/projects/climate-change-risk-assessments-and-adaptation-for-roads-the-roadapt-project/

Global Conference on CyberSpace www.gccs2015.com e.g.:
https://www.gccs2015.com/sites/default/files/documents/Cyber%20Security%20of%20Industrial%20Control%20Systems%20GCCS2015.pdf

Interesting Downloads

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

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Global Conference on CyberSpace	www.gccs2015.com e. g. on ICS: https://www.gccs2015.com/sites/default/files/documents/Cyber%20Security%20of%20Industrial%20Control%20Systems%20GCCS2015.pdf
From Awareness to action: bridging the gaps in 10 steps:	https://zoom.frontwise.com/public/4/towardsgccs2015#
Network Information Security Platform	https://resilience.enisa.europa.eu/nis-platform

Websites of Contributors

Acris	www.acris.ch
CEA	www.cea.fr
Deltares	www.deltares.nl/en
EU Organisation for Security	ww.eos-eu.com
Joint Research Centre	http://ipsc.jrc.ec.europa.eu
University of Cyprus	www.ucy.ac.cy/el/
TNO	www.tno.nl
University of Trento	http://r.unitn.it/it/sdc
Veiligheidsregio Zuid-Holland Zuid	www.vrzhz.nl/

www.cipedia.eu

CIPedia© is here!

An online community service by the CIPRNet Project.

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

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

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

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

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

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

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

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

Marianthi Theocharidou

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

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

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

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

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