European CIIP Newsletter

November 14 – February 15, Volume 8, Number 3

ECN

Contents

CIPR Net

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

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

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

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

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

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

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

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

>Spelling:
British English is used except for US contributions

Editoral

European Activities

Country Specific Issues

Method and Models

About Associations

Conferences 2014

Books on C(I)IP

Links

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enjoy reading this issue of the ECN!

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

Roberto Setola

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

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

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH

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

(This page is intentionally left blank)

Securing Infrastructures & Services in Europe

ENISA role in protecting European Citizens.

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

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

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

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

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

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

Threat Landscape

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

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

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

Evangelos Ouzounis

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

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

Rossella Mattioli

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

Rossella.Mattioli@enisa.europa.eu

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

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

Electronic communications

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

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

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

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

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

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

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

Network Infrastructure

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

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

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

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

In 2014, ENISA will focus its efforts on:

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

Cloud Computing

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

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

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

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

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

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

ICS SCADA and Smart Grids

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

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

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

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

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

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

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

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

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

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

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

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

The Finance Industry

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

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

The findings of the study are as follows:

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

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

National Cyber Security Strategies (NCSS)

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

Securing Europe's Infra-structure and services

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

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

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

2nd ERNCIP Operators' Workshop

Assessment, selection & deployment of technological security solutions.

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

ERNCIP Mission:

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

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

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

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

Workshop's Theme & Sessions

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

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

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

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

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

Marianthi Theocharidou

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

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

Carl-Johan Forsberg

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

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

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

Each session was centred on a driving question:

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

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

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

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

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

General observations

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

Harmonised EU Legislation

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

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

Cross-sector approach

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

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

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

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

Harmonised EU-wide Training & Certification

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

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

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

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

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

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

Learning from experience

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

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

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

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

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

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

Learning from research

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

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

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

Risk Assessment

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

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

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

New concepts for CIP

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

ERNCIP's role

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

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

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

Acknowledgements

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

References

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

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

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

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

ENISA: Certification in industrial environments

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

Security certification schemes are scarce in industrial environments despite the growing number of cyber-attacks that affect what is considered EU Member State Critical Information Infrastructure (CII). Many actions have been taken in this direction in recent years, however, the community questions remain unanswered: Are the industrial Control Systems (ICS) often used as part of Critical Infrastructures (CI) secure? How secure are they?

To date, in the absence of EU approved standards, harmonised testing and corresponding certification schemes for ICS, answering these questions remains elusive.

Addressing this topic requires understanding the current challenges for security certification. This paper will address some of these challenges; it will draw the conclusion that the identification of an implementation strategy which delivers results in a coordinated, balanced and cost-effective manner for society and industry alike is needed.

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

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

Adrian Pauna

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

Email:
adrian.pauna@enisa.europa.eu

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

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

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

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

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

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

Certification Challenges

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

ICT drives ICS product lifecycles resulting in the following challenges:

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

High security certification setup costs, especially for ICS asset owners

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

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

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

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

Threat-oriented ICS security certification is volatile and uncertain

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

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

ISA/IEC 62334 focuses on all ICS ecosystem certifiable objects (polices-procedures-system-component) and consists of thirteen distinct parts (standards)[10]. Two parts are currently published, two other parts are published under review, while seven parts are still under development, and two parts are planned.

Process Hazard Analysis (PHA)

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

Recommendations

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

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

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

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

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

Manage volatility

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

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

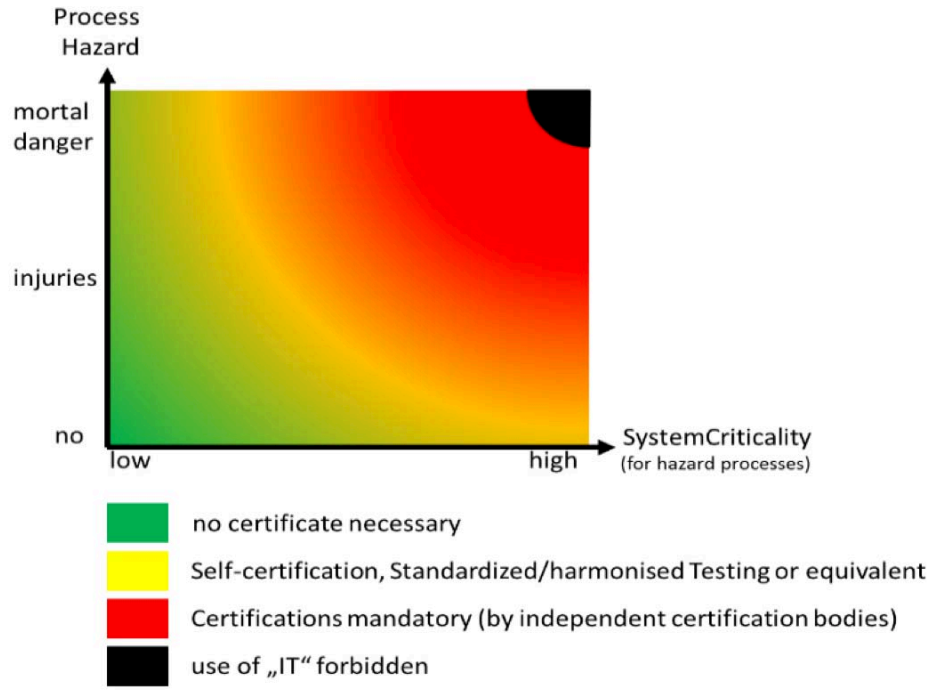
The ENISA recommendation is to certify aspects related to the known process hazards and manage volatility with dynamic certifications.

Focus on the content of certification

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

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

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



- Certifier

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

Zone grouping of Objects for ICS Security Certification

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

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

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

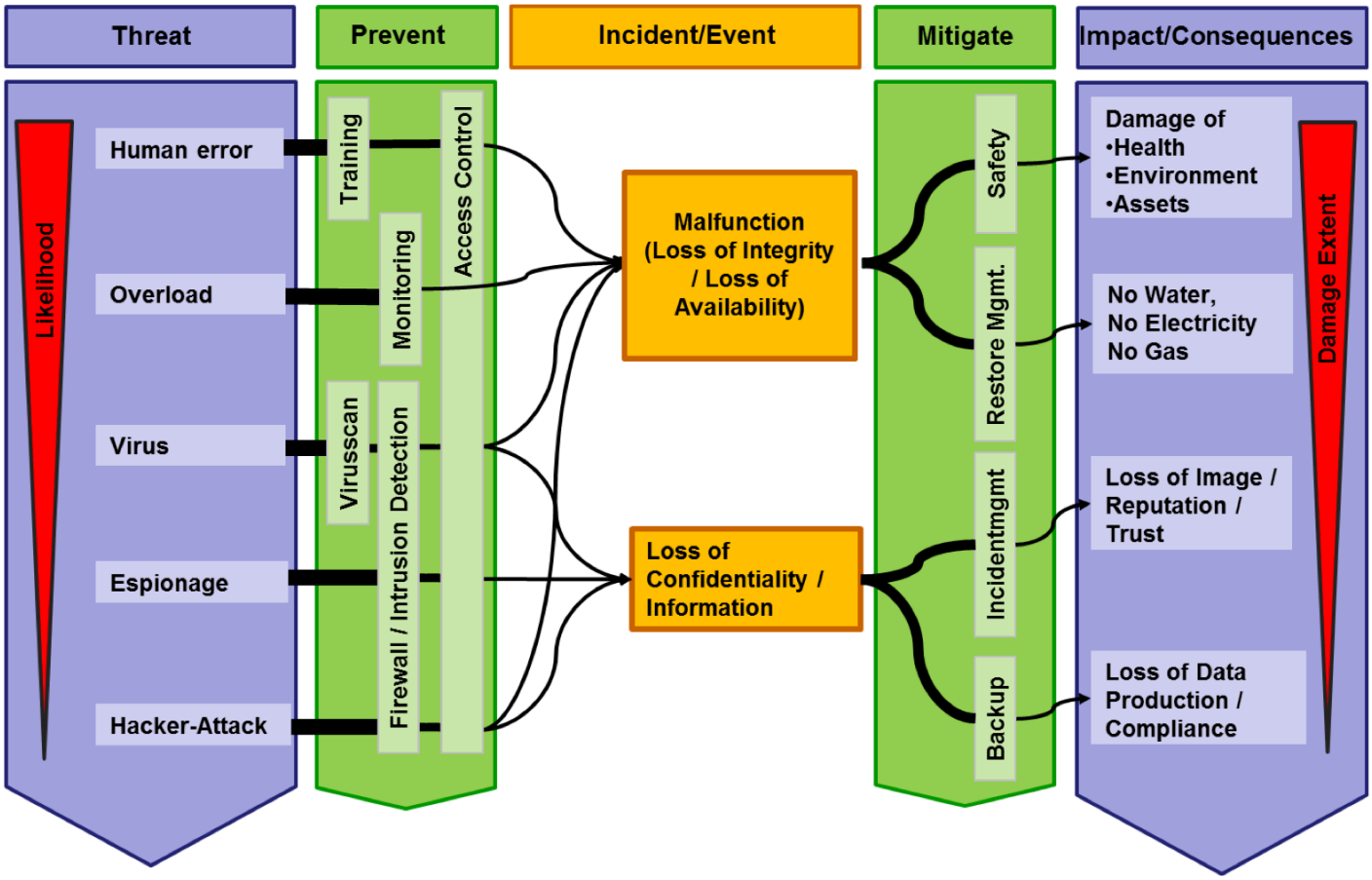


Fig. 2: ICS cybersecurity map

ENISA's 2014 activities on ICS

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

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

Conclusions

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

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

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

Water and waste water services are in general essential and decisive for the health of the population and the quality standard of life. They provide the basis for a sound economy and good development of industry. Water as "Foodstuff Nr.1" is not substitutable, this means in practice: "Without water no life". First aim, therefore to secure the processes, plants and resources of water and waste water services.

Considering IT Risks

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

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

Because of the importance of water and waste water services for population and industry in Germany high quality standards are set to protect the health of population and secure water protection. In the last decades the use of advanced control technologies for water and waste water services has increased constantly. Risk management may be more and more insufficient looking "only" to the security of water and waste water plants, networks, resources, and compensating measures. Even when until today many water and waste water services are still working without specialised computer aided systems, importance and protection of IT will attain more and more distinction according to their application.

The Water and Waste Water Sector in Germany

In Germany, water supply and waste water disposal are core duties of public services in the general interest with the competence of municipalities or other public corporations. In Germany there are approximately **6065 water supply enterprises and utilities**. These enterprises are predominantly small ancillary municipal utilities and owner-operated municipal utilities. In the water supply sector, public and private forms of organisation have co-existed for decades. In the waste water sector there are in total more than **6900 waste water disposal utilities** in Germany. The undertakings are predominantly operated by municipalities and owner-operated municipal utilities.

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

The most important regulations for water and waste water industries are the so called "Wasserhaushaltsgesetz" and the regulations of the Länder "Landeswassergesetze", which f.e. implemented the Water Frame Work Directive, the so-called "Trinkwasserverordnung", which implemented the Drinking Water Directive and the so called "Abwasserverordnung", which implemented the Urban Waste Water Treatment Directive into German law.

Michaela Schmitz

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

e-mail: michaela.schmitz@bdew.de

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

Structural and Quality aspects

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

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

Long-term nationwide protection of all waters is a national duty to which

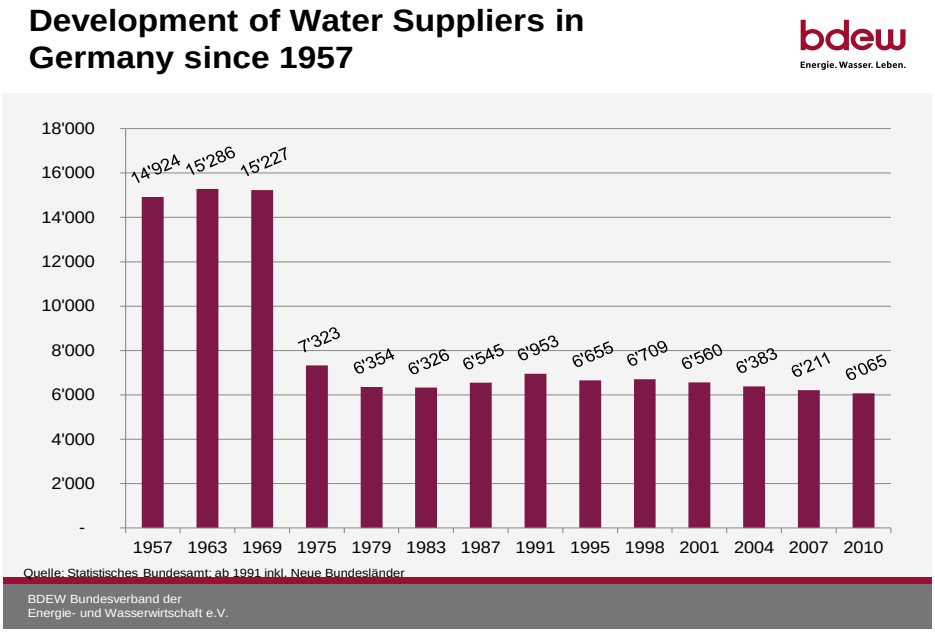


Fig. 1: from 1957 ongoing: Germany's water supply

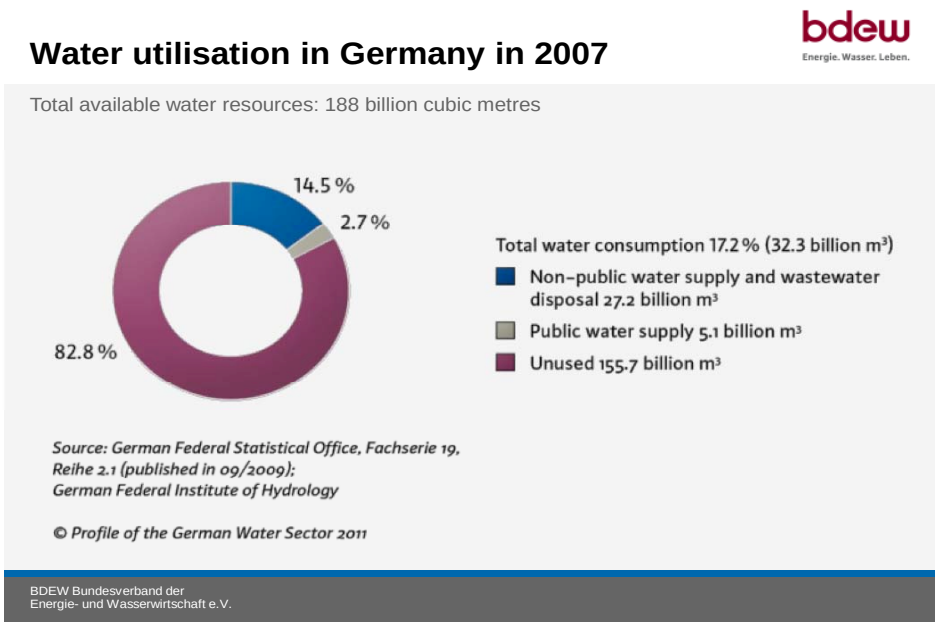


Fig. 2: Water utilisation2007 in Germany

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

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

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

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

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

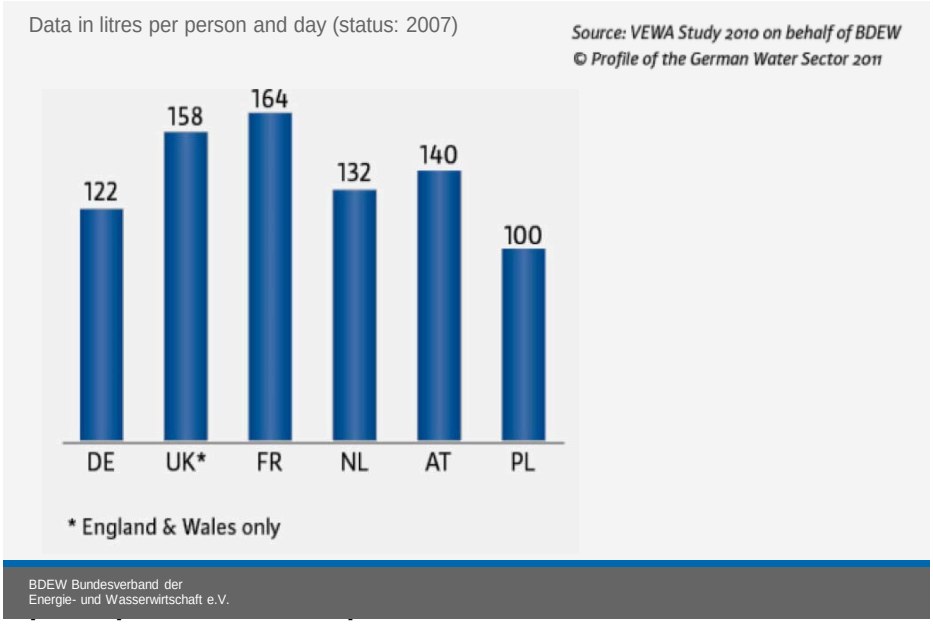
Since 1997, the rate of mains failures has decreased to 9.9 incidents per year and per 100 km of network length. This means a very low rate of damage compared with other European countries (England and Wales 18.7, Scotland 16.6) with a tendency to decrease further. There have been huge improvements particularly in the new German "Bundesländer" since reunification.

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

IT-Security: National and European Legislation in Progress

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

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



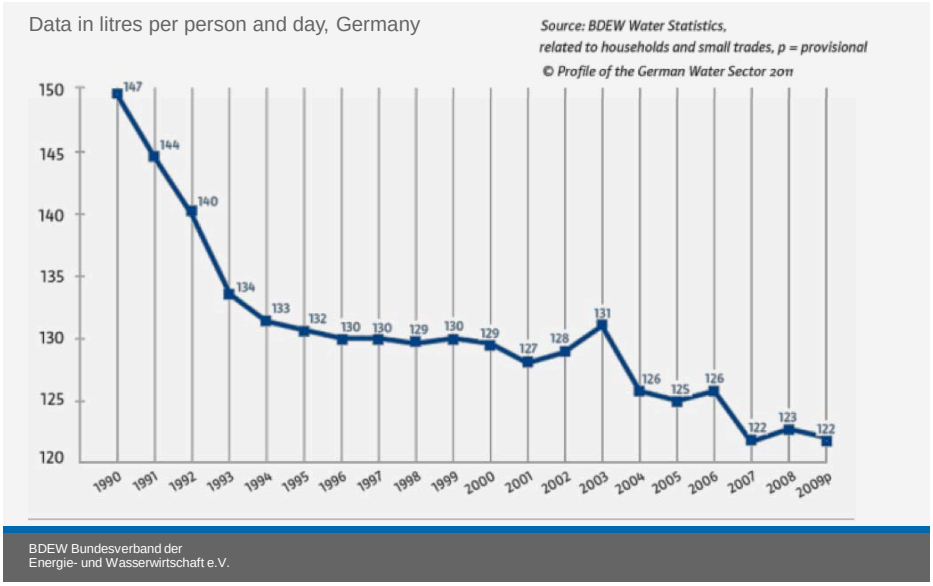
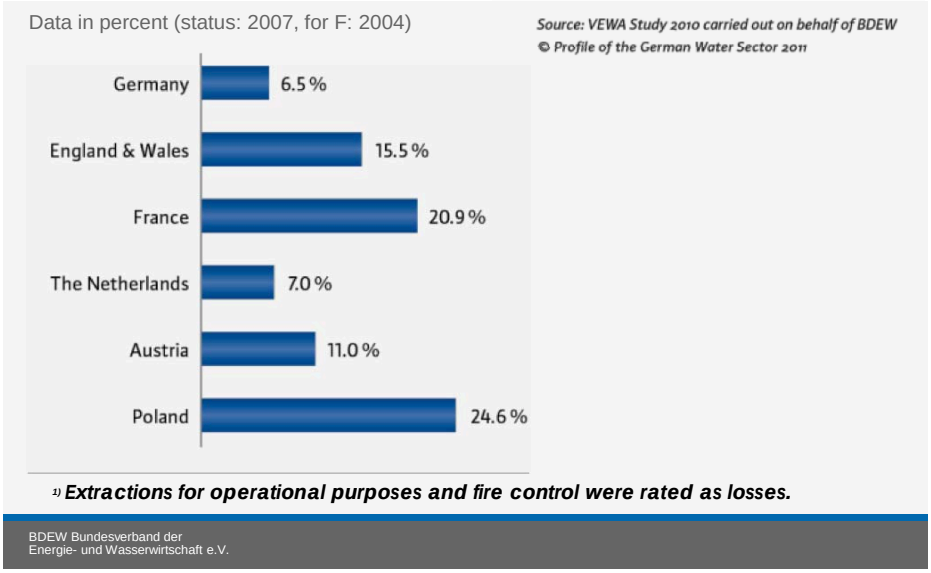


Figure 5: Water losses in the public drinking water network[1]: most important indicator of network quality and safety of supply



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

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

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

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

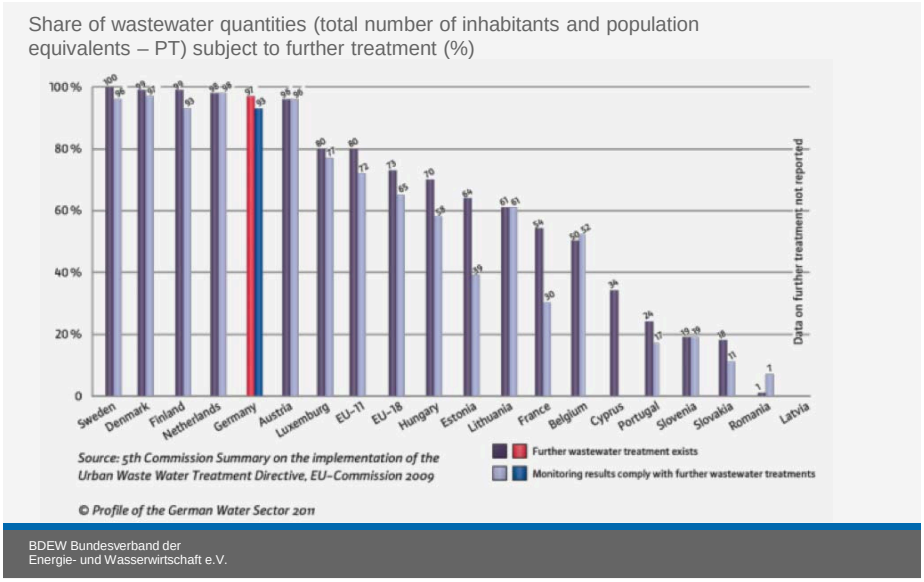
BDEW believes that the projected obligation to report should apply only to serious IT-security incidents with impacts to security of supply or public safety. BDEW also requires observance of existing obligations to report, with no approval of double-point information and extra bureaucracy. As technical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

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

References

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

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



Intelligent network modeling in the electric power grid

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

Electric power system is one of the most critical and strategic infrastructures of industrial societies. Power utilities face the challenge of using information and communication networks more effectively to manage the demand, generation, transmission, and distribution of their commodity services. The capabilities

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

of networking these systems provide unprecedented opportunities to improve productivity, reduce impacts on the environment, and help provide energy independence. Communication network constitutes the core of the electric system automation applications, the design of a cost-effective, and reliable network architecture is crucial. To resolve this difficulty we study the integration of advanced artificial intelligence technology into existing network management system.

Recent years have seen explosive growth in the areas of power system monitoring using intelligent agents and distributed intelligence. This project differs from previous work because we present a technique for the design and implementation of a security intelligent system that is designed through the normalisation and integration of knowledge management. We describe an intelligent technique, which processes management knowledge collected by intelligent agents and uses it to detect and to resolve the network anomalies and security faults. This work focuses on an intelligent framework and a language for formalising knowledge management descriptions and combining them with existing Open Systems Interconnection (OSI) management model. The goal is the assignment and dispersed intelligent control of network resources, pertaining to hardware as well as software, to help operators manage their security networks more effectively and also to promote reliability in network services.

Systems Management Overview

Telecommunication systems are essential elements to improve efficiency and economy in energy operation, transmission, distribution, storage, and utilisation. There are two dominant network management models, which have been used to administration and control the most of existing networks: Telecommunications Management Network (TMN) and Simple Network Management Protocol (SNMP). In the public environment, a more heterogeneous mix of de facto telecommunications industry standards has prevailed, with a move toward TMN support. TMN was the first who started, as part of its OSI program. OSI architecture for network management involves five major functional areas: fault, configuration, accounting, performance, and security management, which facilitate rapid and consistent progress within each category's individual areas [1].

Antonio Martín

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

mail: **toni@us.es**

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

Integration of Intelligent Agents

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

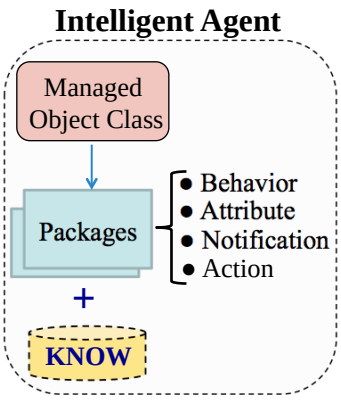


Fig. 1: Template relations in GDMO+ standard

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

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

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

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

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

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

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

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

The application Model

In order to validate our approach, we have developed intelligent control architecture in an electric power system. This system integrates the management knowledge into the network resources specifications. We study an example of alarm detection and intelligent resolution of incident concerning a private network. We have used a telecommunications network that belongs to a company in the electrical sector in Spain.

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

The Spanish power grid company has got a network using wireless on the regional high-tension power grid. Part of long-distance traffic in this net is controlled by a wireless intelligent system distributed throughout this private network. The use of integrate knowledge in agents can help the system administrator in using the maximum capabilities of the intelligent network management platform without having to use other specification language to customize the application [4]. Our system has three major components: an inference engine, a knowledge base, and a user interface, figure 2.

- The inference engine is the processing unit that solves any given problems by making logical inferences on the given facts and rules stored in the knowledge base.
- The knowledge base is the core of the system. This is a collection of facts and if-then production rules that represent stored knowledge about the problem domain. The knowledge base contains both static and dynamic information and knowledge about different network resources and common failures.
- Human Machine Interface reports to human operators over a specialised computer called Human-Computer Interface (HCI). Each device provides a time-stamped message on events (starting, tripping, activation, etc.) through the bus.

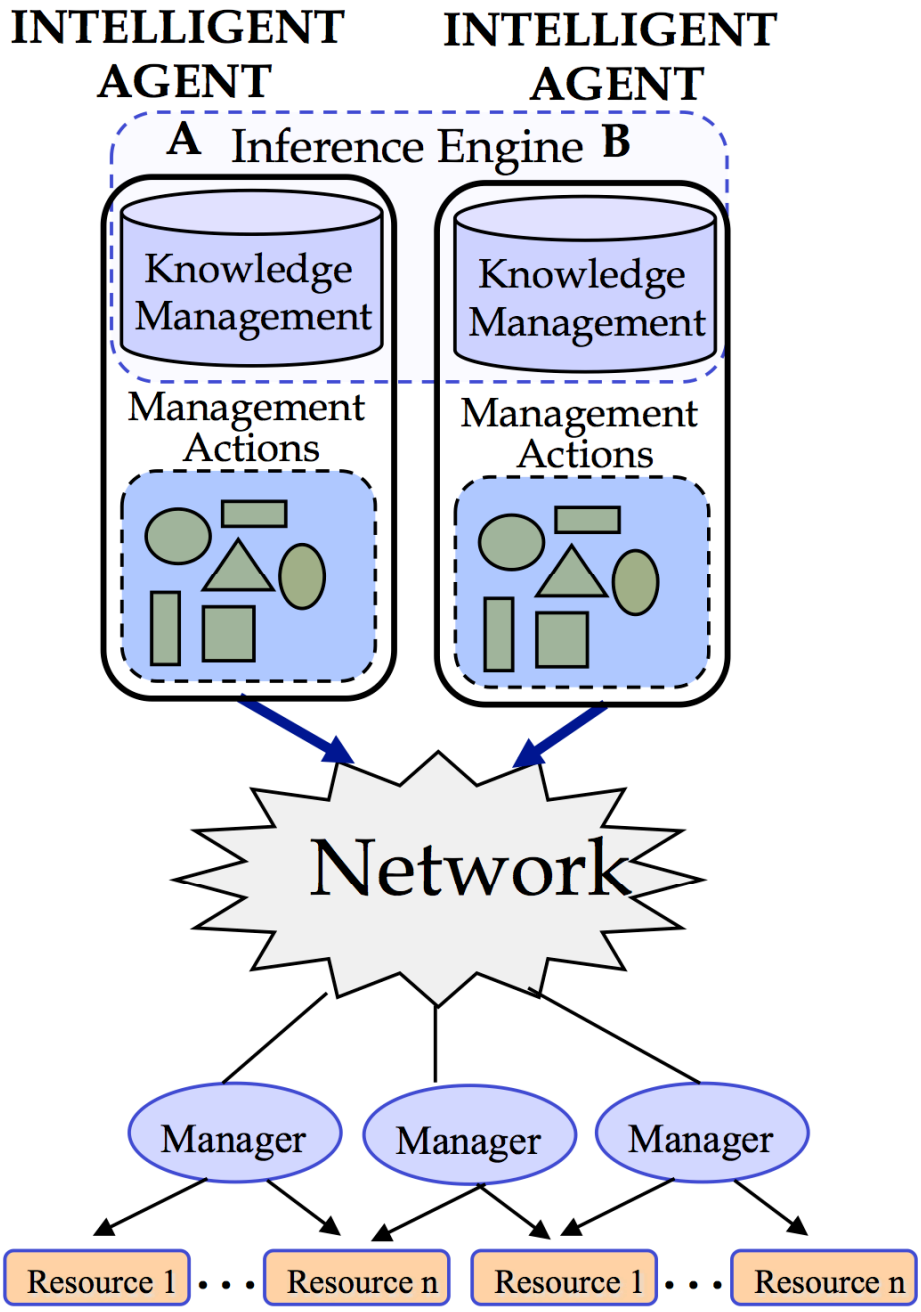


Fig. 2: Architecture System

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

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

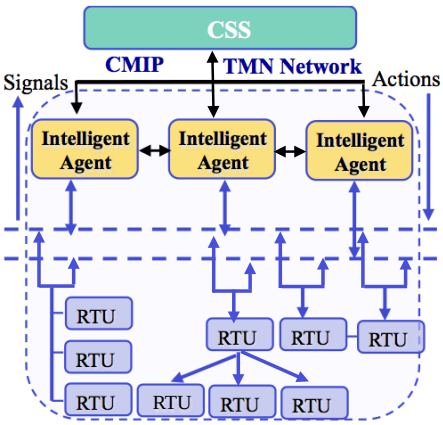


Fig. 3: Communication Supervisory System (CSS)

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

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

Concluding Remarks

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

References

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

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

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

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

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

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

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

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

Creative Modelling of Emergency Management Scenarios

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

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

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

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

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

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

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

Challenging Case Studies

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

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

Antonio De Nicola

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

e-mail: antonio.denicola@enea.it

Maria Luisa Villani

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

e-mail: marialuisa.villani@enea.it

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

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

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

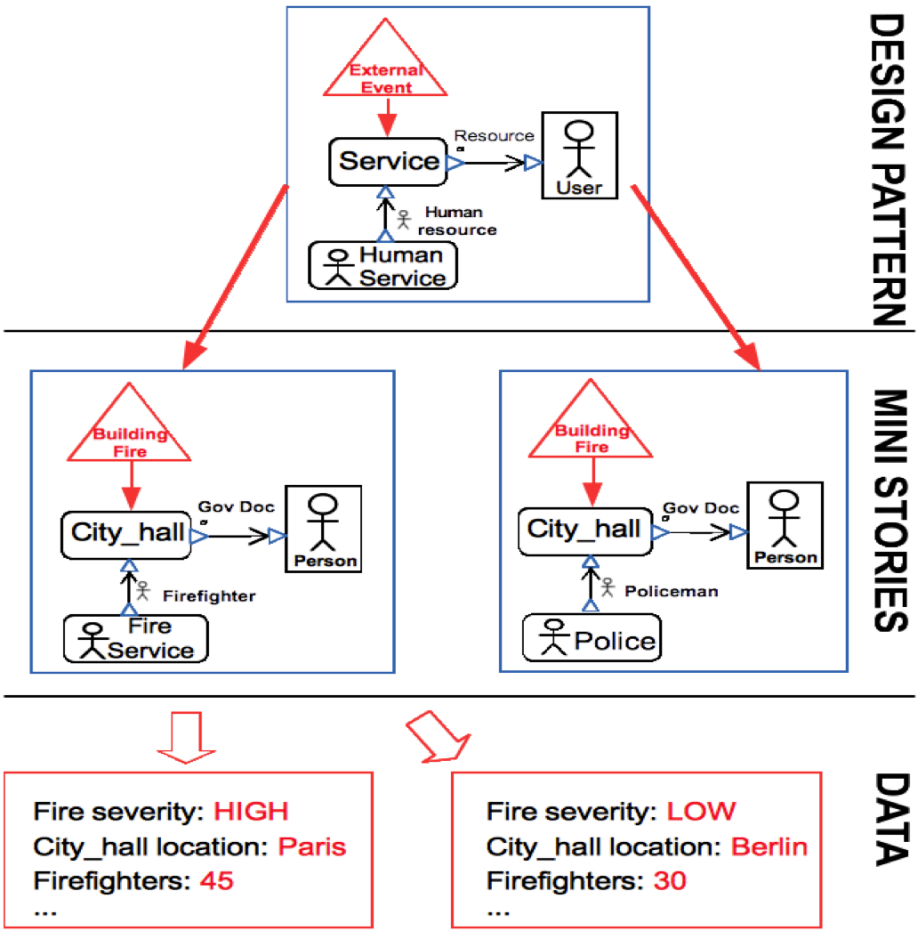


Fig. 1: The three types of knowledge of a EM scenario model

EM Scenarios Modelling and creativity

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

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

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

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

building fire. The other mini-story depicted on the right, instead, describes an unusual case where policemen resolve the fire. However, such mini-story can be considered as possible in an emergency scenario. Indeed, in case of large scale emergencies the availability of the most appropriate human resources cannot be granted since they could be occupied elsewhere.

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

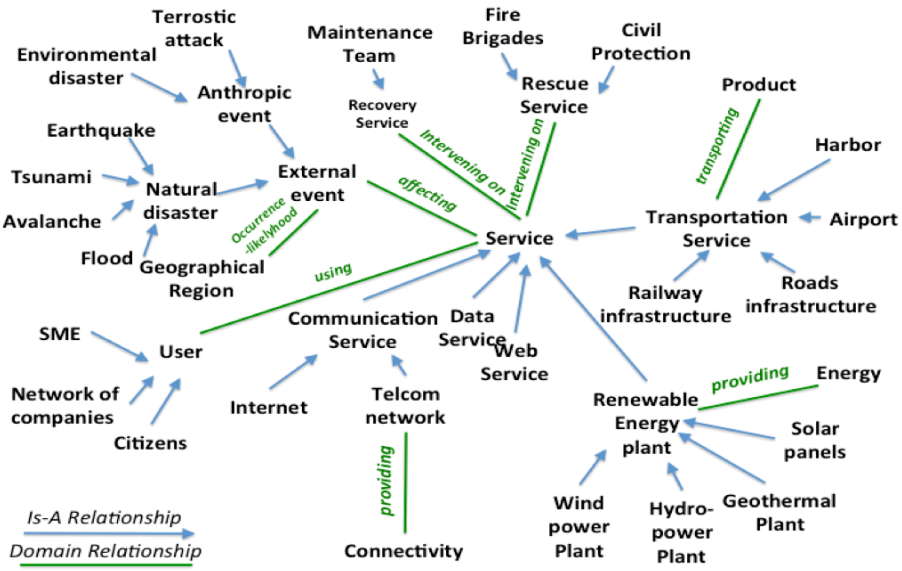


Fig. 2: An excerpt of the EM and domain ontology

Technology support

Our methodology for EM scenarios modelling can be implemented through a suite of tools, as shown in Fig. 3, interacting with a knowledge base. Some of these tools are used in the design phase, for the construction of the knowledge base, and others at run time, to generate and validate mini-stories.

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

A CEML model is presented with a graphical notation and consists of a structural diagram, that is, a representation of a set of active entities that are linked to exchange objects of some nature. To the diagram, a set of behavioural specifications has to be attached, describing the computational steps that the entities of the model perform during a simulation.

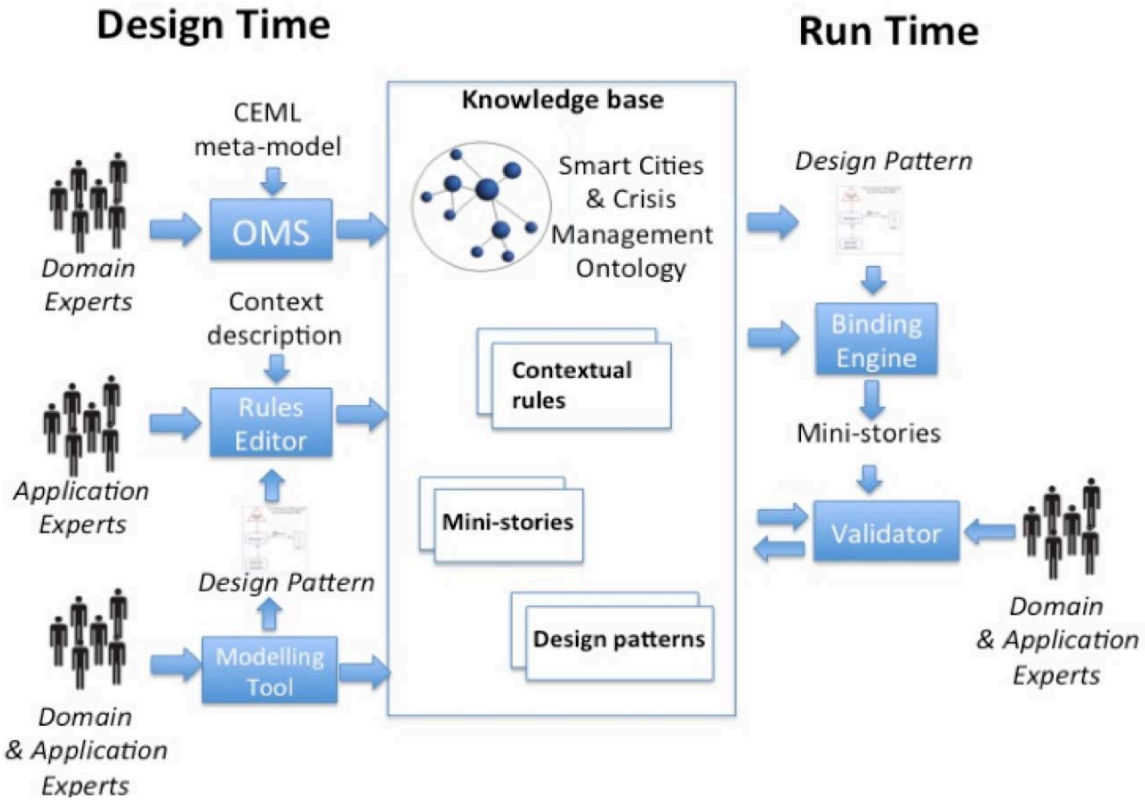


Fig. 3: The architecture for EM Scenarios Modelling

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

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

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

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

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

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

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

Conclusions

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

Acknowledgements

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

Introduction

For two case studies on critical infrastructure in the Netherlands open data was used for cascading effect analyses. The data alone was not enough to describe and visualise these effects, but interviews with network owners proved very valuable and gave insight in how the open data could be used at best.

It became clear that when data and knowledge was combined in a smart way, there is less need to access detailed data from the network owners themselves. The results of direct impacts from a flood and cascading effects were indicated as roughly the same or very likely by the network owners we talked to. Figure 1 shows the results of a possible electricity black-out during a certain flood scenario at a specific time step based on open data and network knowledge.

Because open data is widely available but knowledge is not, we created a stakeholder participation tool that gathers valuable knowledge on network behaviour and impact.

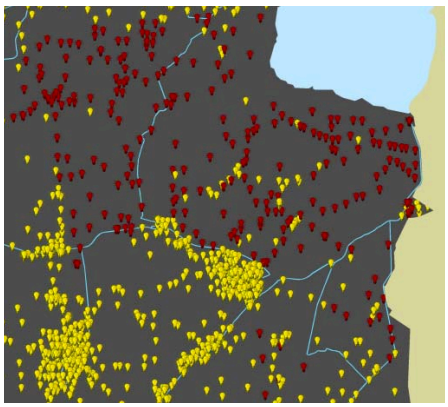


Fig. 1: Result of a possible electricity black-out during a flood based on open data.

Cascading Effects

Until now connections between Critical Infrastructure networks are hardly identified. Critical infrastructures are dealt with separately, even though different parties are aware of their (inter)dependencies and possible cascading effects in case of floods or other natural hazards. Still it is not clear if cascading effects cause a major part of the total impact or If these effects are relatively small. Moreover, data is mostly unavailable and dependencies are not automated, which makes it difficult to determine the effects on a certain location and hinders an adequate coordination and disaster management.

The reason why data (on for instance the energy networks) are not publicly available is that they are vulnerable for misuse. Network owners are often aware of the possibility of cascading effects and their connection with other networks or vulnerable objects, but struggle with the secrecy of network data. For two case studies, Deltares performed an analysis on possible cascading effects after a flood with the use of open data and expert knowledge, and tested the results with several network owners. Although detailed data was not used, still the results were evaluated by network owners to be adequate and close to reality.

Micheline W.A. Hounjet

Team leader of the Deltares Critical Infrastructures Team.

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

e-mail: micheline.hounjet@deltares.nl

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

Deltares
Enabling Delta Life

CIrcle

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

For this purpose CIrcle has been developed, a touch table application for workshops. Within workshops, different network owners, vulnerable object owners or governments can find out and discuss cascading effects together.

During the discussion, connections between the networks or objects are drawn and the causal relationships between them are collected in a database.

Examples of these causal relationships are:

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

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

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

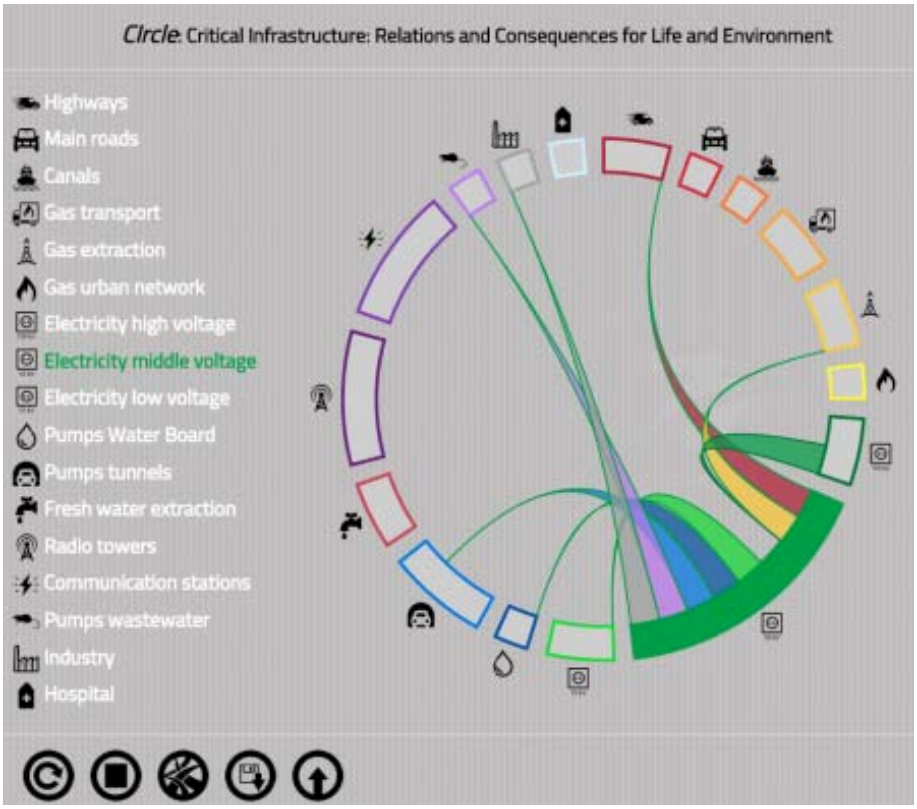


Fig. 2: Drawing of the connections between different Critical Infrastructure networks.

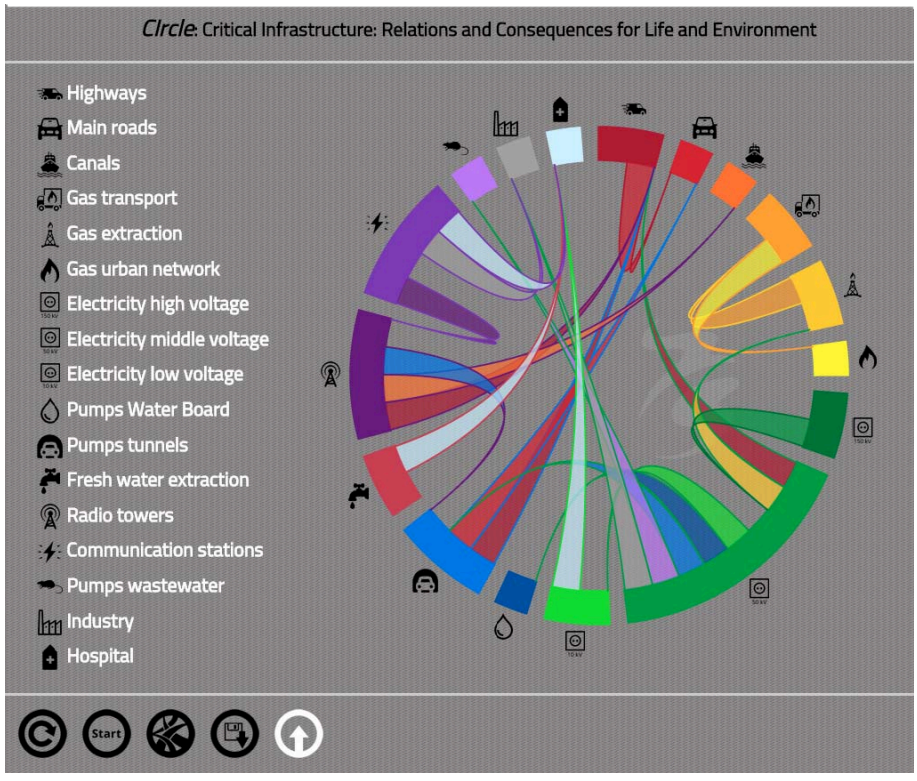


Fig. 3: Final result of the discussion where all the drawn connections are shown in one view.

Floods

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

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

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

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

(This page is left blank intentionally)

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

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

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

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

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

IDRC Davos 2014

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

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

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

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

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

Highlights from the IDRC Davos 2014 keynotes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The IDRC Davos 2014 Plenary Sessions

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

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

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

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

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

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

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

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

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

The 2014 RISK Award goes to ONG Inclusiva, Chile

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

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

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

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

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


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

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

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

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

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

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

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

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

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

CIPedia© is here!

www.cipedia.eu

An online community service by the CIPRNet Project.

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

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

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

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

Roadmap

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

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

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

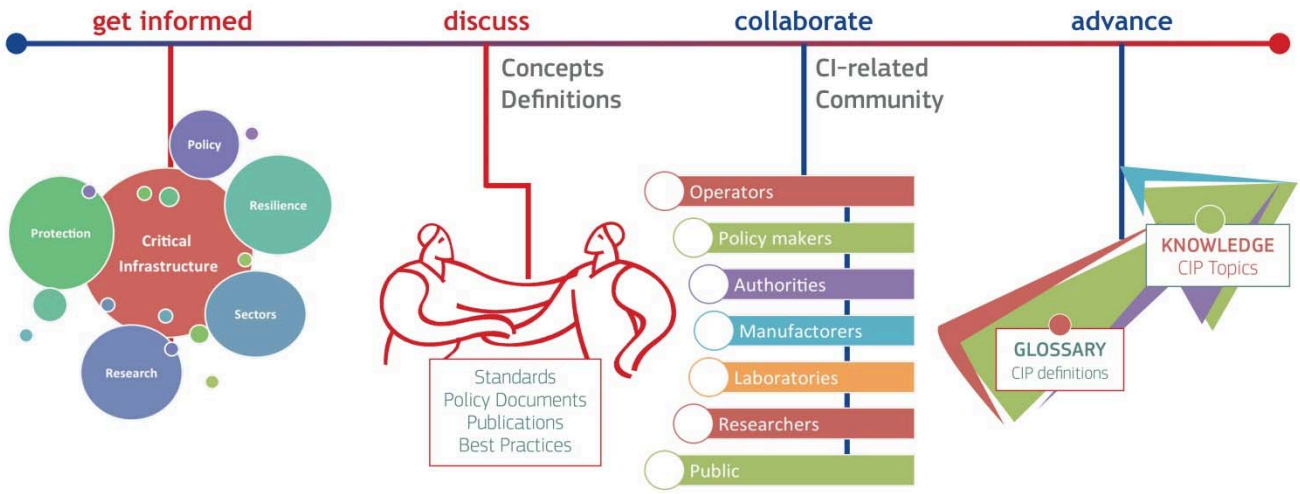
Future versions will be more dynamic; CIPedia© will allow stakeholders to update information capturing the evolution of the CIP domain, as new concepts emerge or receive different meaning.

Marianthi Theocharidou

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

marianthi.theocharidou@jrc.ec.europa.eu

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



Links

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

Forthcoming conferences and workshops

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

Exhibitions

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

Associations

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

Institutions

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

Project home pages

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

Interesting Downloads

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

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

Websites of Contributors

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