European CIIP Newsletter

July 16 - October 16, Volume 10, Number 2

CRITIS 2016
Call for
Participation

ECN

Contents

CIPR Net

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

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Method and Models (continued)

Ads of upcoming Conferences and Workshops

Links

Media on C(I)IP

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

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

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

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

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

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

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

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

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

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

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

Enjoy reading this issue of ECN!

José R. Martí

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

Bernhard M. Hämmerli

Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

e-mail: **bmhaemmerli@acris.ch**

He is ECN Editor in Chief

European Safety, Reliability and Data Association

Clermont-Ferrand, France

October 20th – 21st, 2016

51st ESReDA Seminar on

Maintenance and Life Cycle Assessment of Structures and Industrial Systems

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

CIRAS: Critical Infrastructure Risk Assessment Support

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

Introduction

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

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

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

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

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

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

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

Project Outcomes

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

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

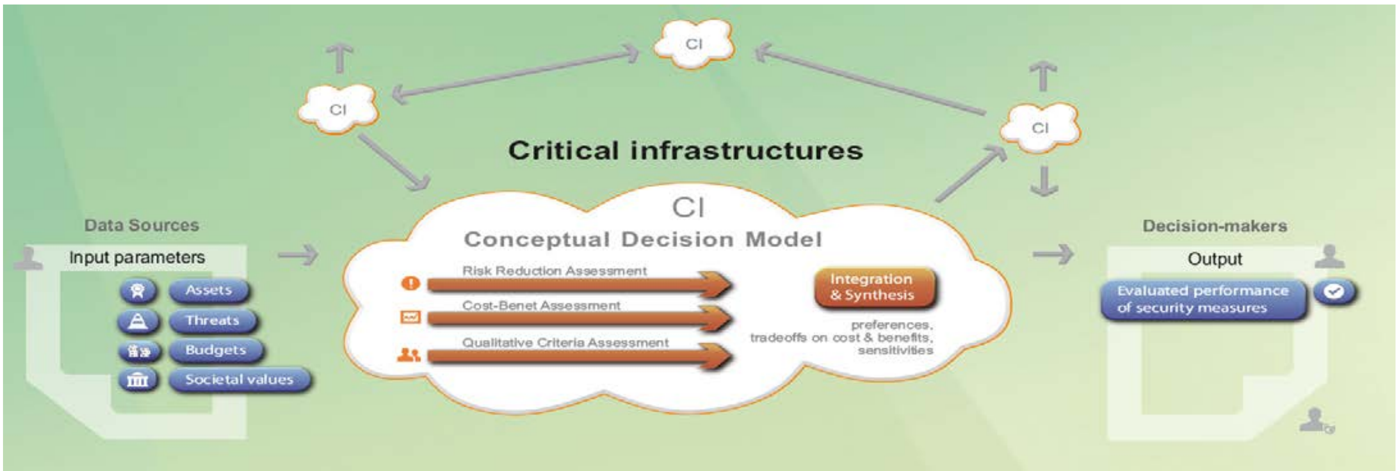
- **Risk Reduction Assessment (RRA):** for measuring the risk reduction capability of the different Security Measures and the Alternatives that include them. It implies two steps: first of all, an Asset oriented Business Impact Analysis is done to evaluate the consequences and impact levels in case of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

Jaime Martín Pérez

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

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

e-mail: jaime.martinp@atos.net


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

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

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

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

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

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

Conceptual Decision Model

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

Then several assessments are performed in parallel:

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

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

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

Engagement of stakeholders

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

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

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

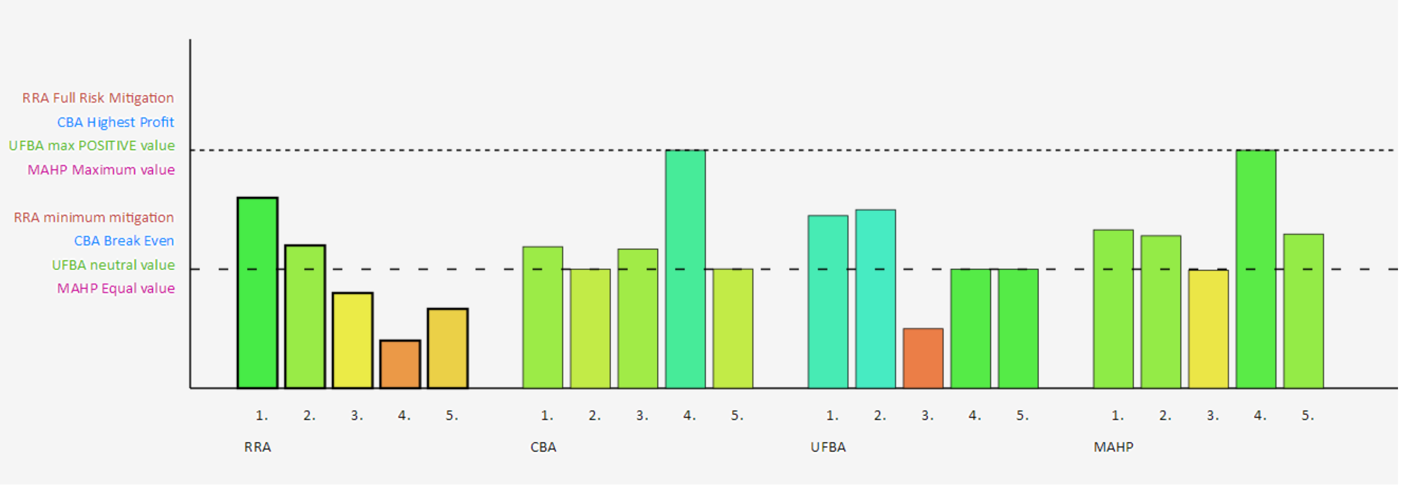


Figure 2: Example of aggregated result

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

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

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

Validation: Use cases

Six use cases were carried out with the following goals:

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

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

Transportation use cases

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

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

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

The use cases were the following:

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

Energy use cases

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

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

The use cases were the following:

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

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

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

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

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

The consortium

The CIRAS Consortium comprises three partners:

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

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

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

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

Air Traffic Management: moving towards Cloud Computing?

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

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

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

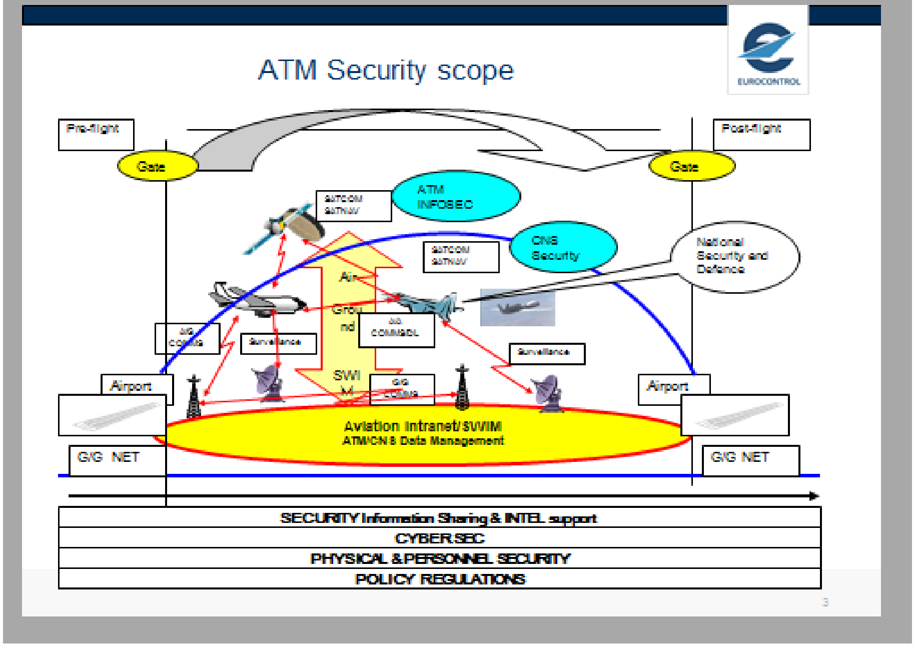
ATM Security

The protection of the ATM infrastructure follows a layered approach and is a combination of:
1. Legal framework: regulations, policies and standards.2. Personnel and physical security measures.
3. Cyber security, which in ATM includes information and communication security.
4. Security information sharing.
5. Intelligence support.

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

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

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


ATM Security scope

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

Antonio Nogueras

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

e-mail:
antonio.nogueras@eurocontrol.int

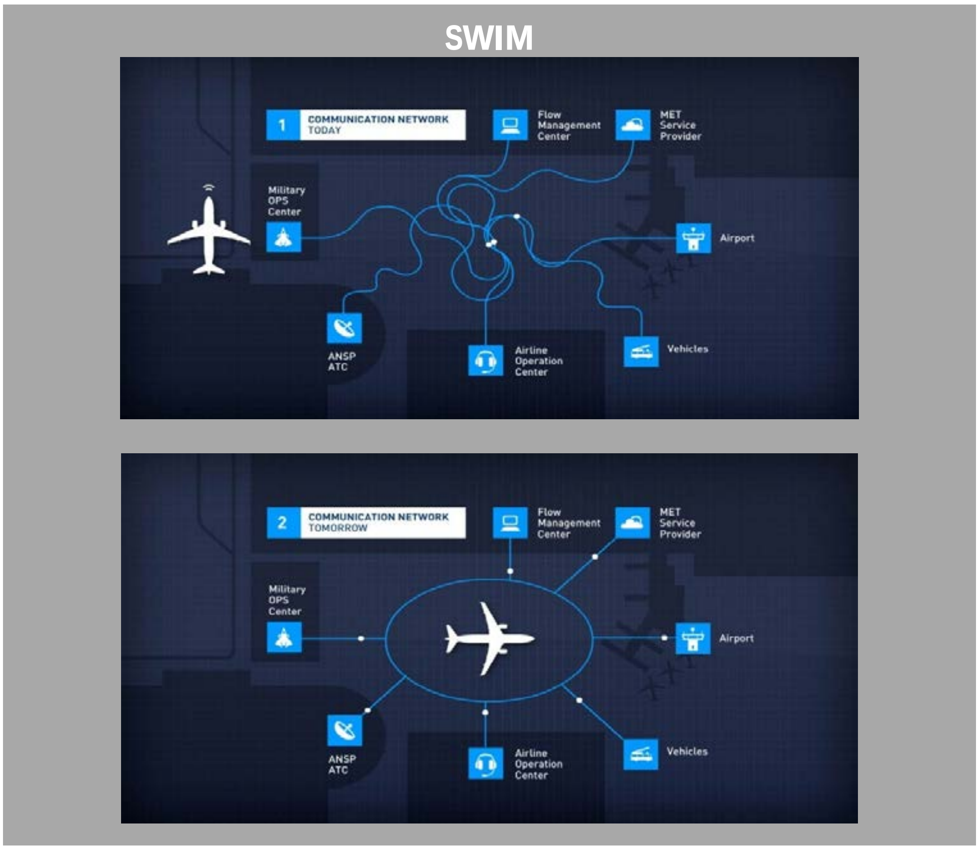
EUROCONTROL
96 Rue de la Fusée, 1130
Brussels, Belgium

SWIM
future aviation intranet

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

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

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

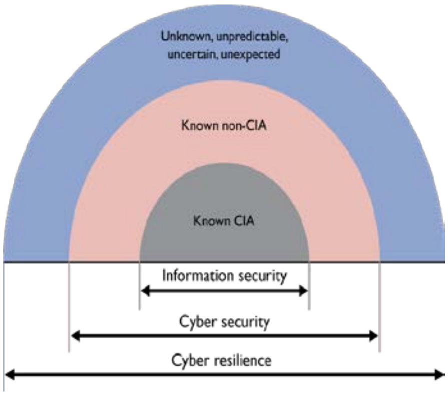


The goal: cyber resilience

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

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

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



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

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

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

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

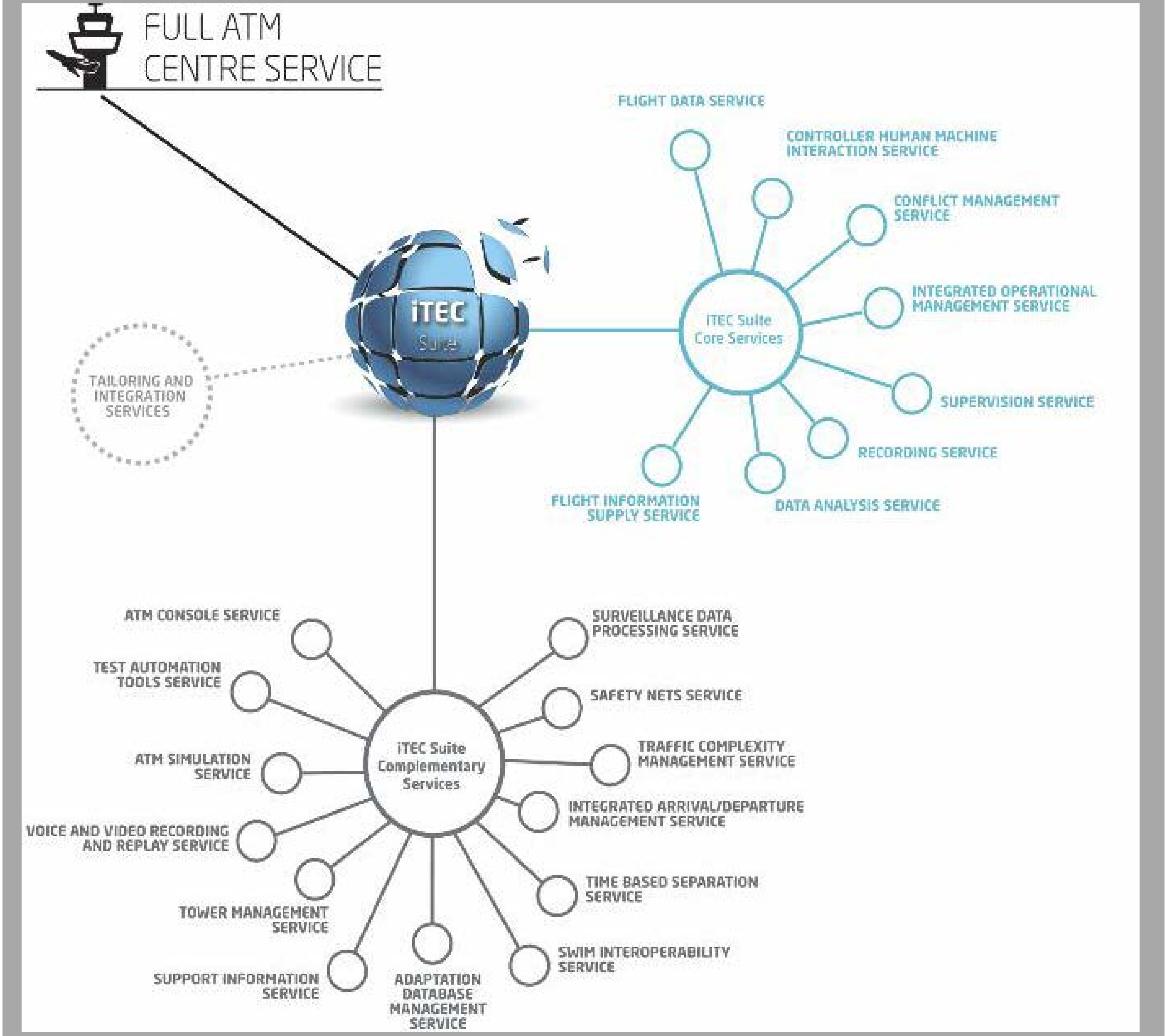
ATM on the move

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

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

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

iTEC Cloud


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

© EUROCONTROL- Skyway Autumn/Winter 2015

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

Industry paving the way

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

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

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

ATM as critical infrastructure

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

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

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

Final thoughts

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

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

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

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

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

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

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

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

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

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

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

CIPRTrainer system

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

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

Scenarios for training

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

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

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

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

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

Federated CI simulation

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

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

»What if« analysis

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

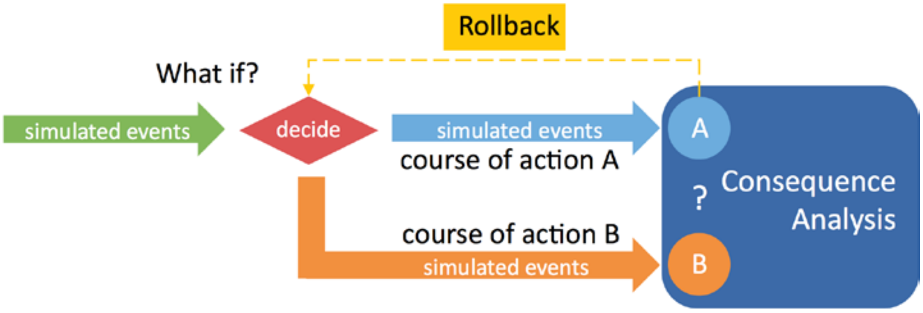
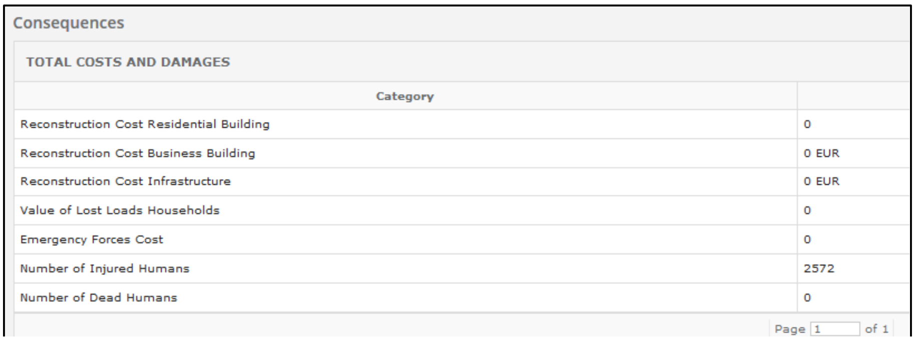


Figure 1: »What if« analysis: After taking course of action A, roll back to decision point, and take different course of action B. Use consequence analysis to compare the overall consequences of both scenario evolutions.

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

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



Consequences

TOTAL COSTS AND DAMAGES

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

Page 1 of 1

Figure 2: Tabular presentation of consequence analysis results

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

Consequence analysis

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

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

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

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

Graphical User Interface

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

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

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

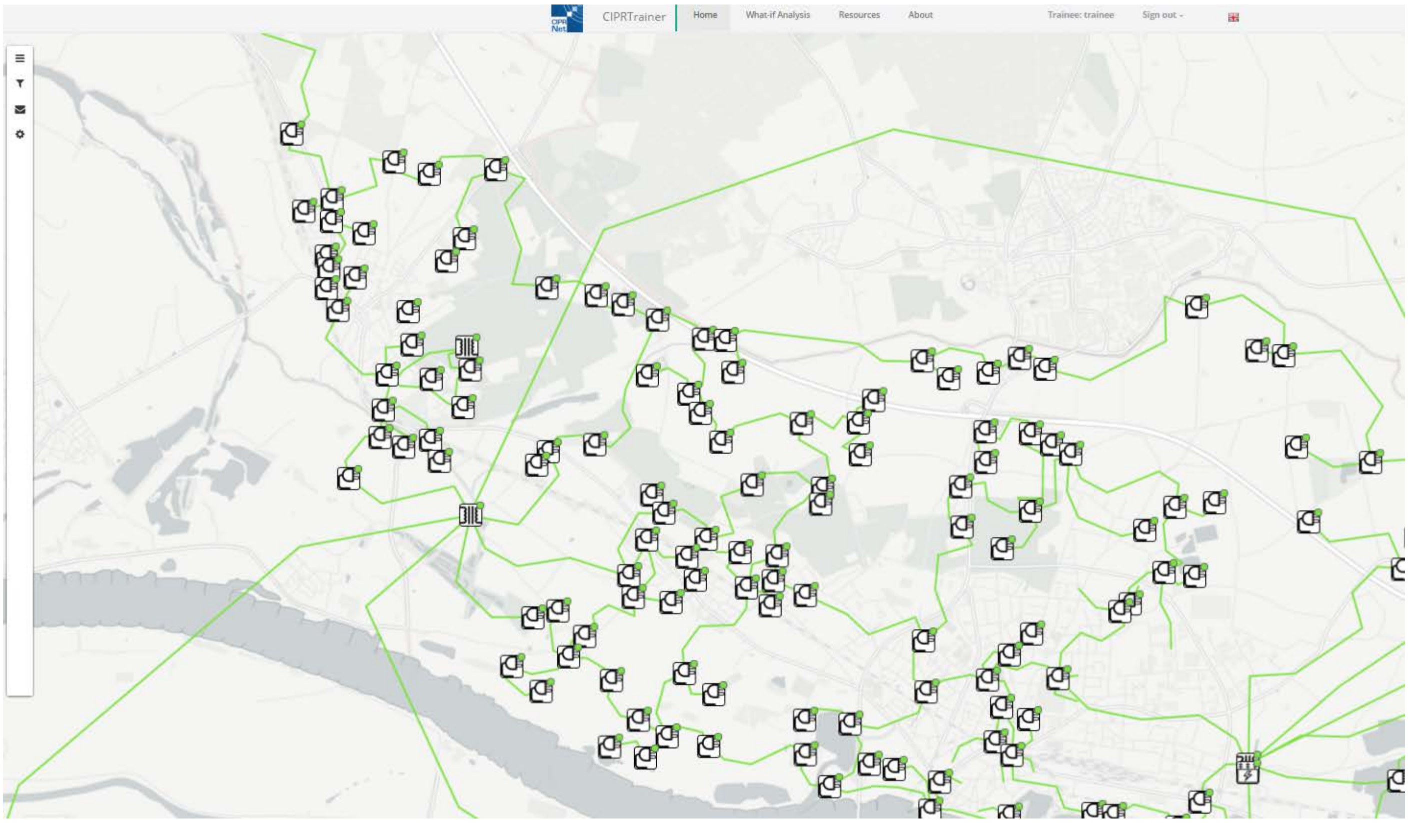


Figure 3: GIS functionality of CIPRTrainer: Information layer showing artificial telecommunication network. Green lines and green 'LED's at router icons indicate that the network is fully functioning

Conclusion and Outlook

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

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

Disclaimer and Acknowledgement

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

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

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

More information

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

www.ciprnet.eu

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

www.cipedia.eu

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

References

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

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

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

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

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

Smart Mature Resilience project: European Resilience Management Guideline

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

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

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

How the SMR project meets the challenge

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

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

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

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

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

Jose Mari Sarriegi

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

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

email: jmsarriegi@tecnun.es

The SMR Approach

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

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

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

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

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

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

The SMR Circle of Learning and Sharing

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

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

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

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

Expected impacts

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

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

The SMR Consortium

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

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

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

FS-ISAC: The Financial Services Information Analysis Centre

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

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

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

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

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

Threat Environment

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

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

Ray Irving

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

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

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

e-mail: rirving@fsisac.eu

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

Key Activities

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

FS-ISAC core activities include:

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

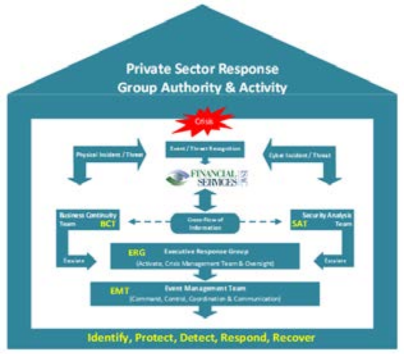
Circles of Trust

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

Incident response exercises and plans

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

Overarching methodology


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

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

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

Next Steps

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

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

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

Leontief's Production Model

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

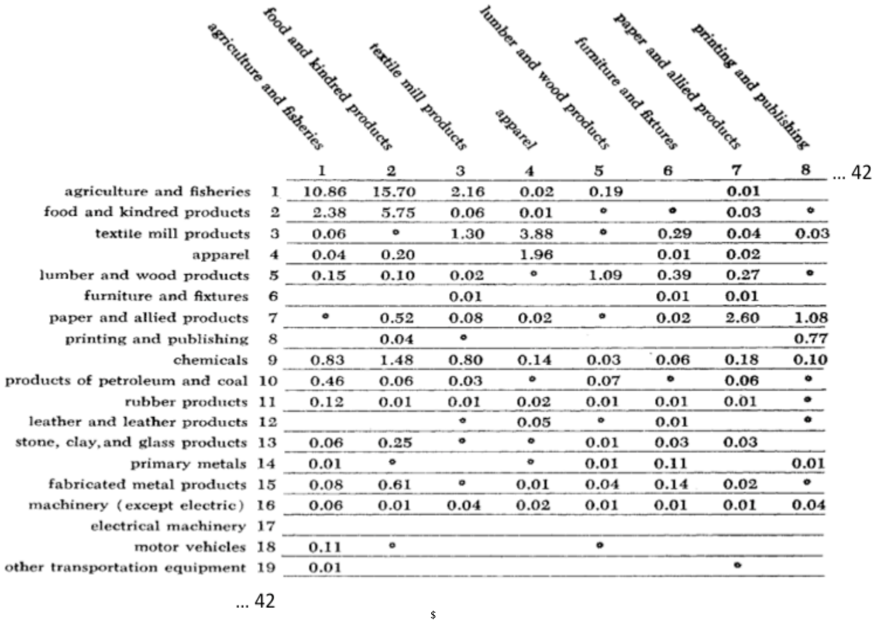
$$\overline{x}_L = A\overline{x}_L + \overline{f} \qquad (1)$$

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

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

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

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



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

$

Figure 4: Leontief's production matrix.

José R. Martí

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

e-mail: jrms@ece.ubc.ca

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

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

Human Wellness in the Production Model

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

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

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

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

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

which results in the equation

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

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

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

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

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

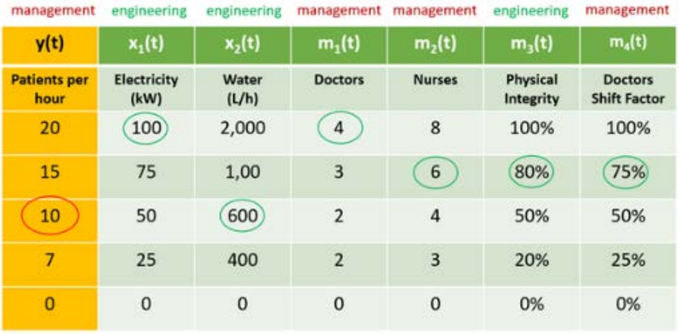
I2Sim Simulator to Integrate Physical and Human Systems

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

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

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

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



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

Figure 5: HRT for a hospital ER unit.

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

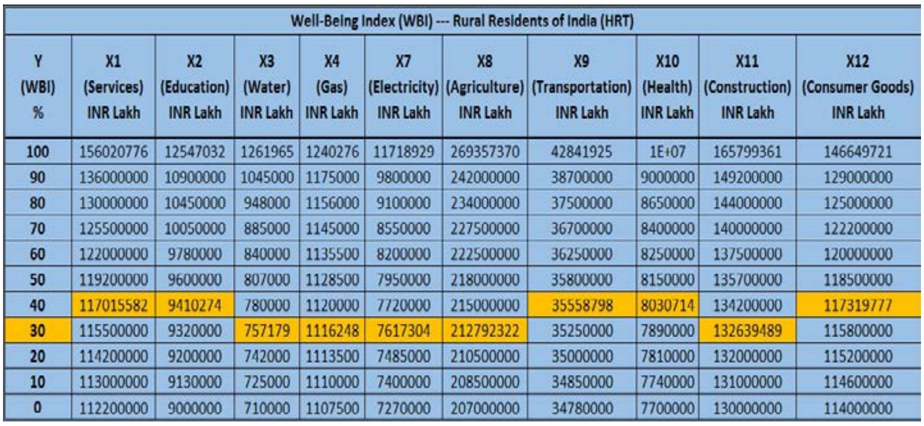
Because the HRT concept can relate variables that can be physical or human, it allows the extension of Leontief's production unit concept to incorporate human factors in the PC system matrix *B* (3). These factors are not considered in Leontief's system matrix *A* (1). In addition, while Leontief's requires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

Human Wellness Table (HWT)

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

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

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



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

Figure 6: Human Wellness Table (HWT)

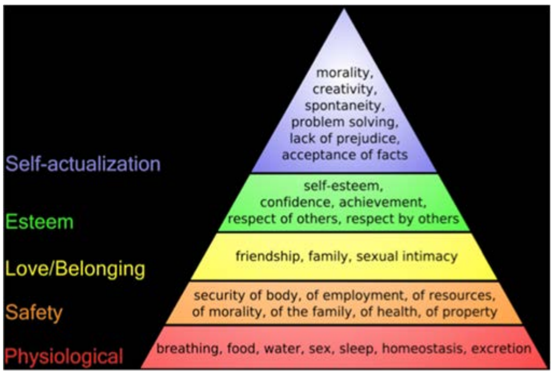

morality, creativity, spontaneity, problem solving, lack of prejudice, acceptance of facts
Self-actualization
self-esteem, confidence, achievement, respect of others, respect by others
Esteem
friendship, family, sexual intimacy
Love/Belonging
security of body, of employment, of resources, of morality,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

Figure 7: Maslow's pyramid of human needs.

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

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

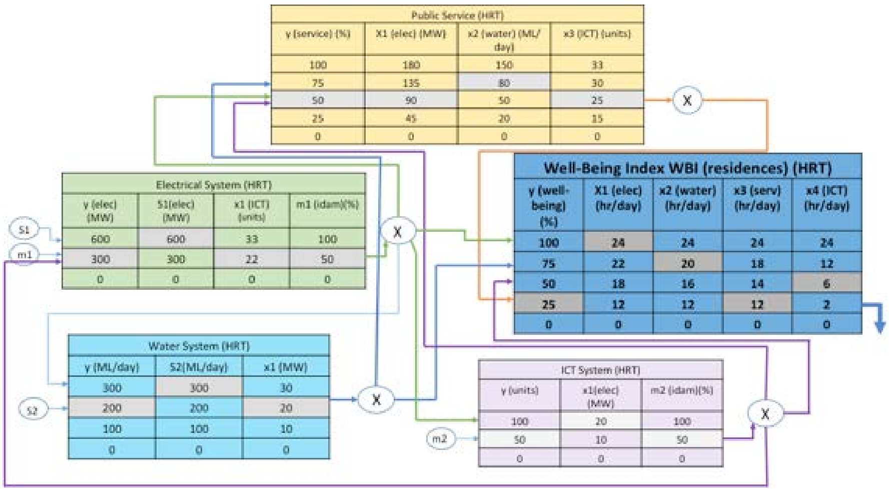
To achieve a coordinated growth of the sectors such that the next wellness level is achieved efficiently, a system optimization problem has to be solved. This solution needs to consider the interdependencies among production sectors and the geographical locality of the consumption. Since i2Sim can consider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

The Gross Domestic Wealth (GDW) Index

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

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

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



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

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

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

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

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

Figure 5: Interdependencies among city services providing human needs.

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

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

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

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

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

Conclusion

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

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

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

References

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

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

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

Authors' Contributions

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

Ehssan Ghahremani

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

Andrea T.J. Martí

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

Open-source Network Defense: Protecting Critical Infrastructures with Bro

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

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

History

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

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

Capabilities

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

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

Robin Sommer

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

e-mail: robin@icsi.berkeley.edu

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

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

Critical Infrastructure

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

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

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

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

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

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

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

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

Enterprise Solutions

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

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

Conclusion

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

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

---

[1] https://bro.org

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

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

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

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

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

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

Organizational Barriers to Cloud Adoption in CI

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

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

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

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

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

Decision-making in Groups

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

5 Factors

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

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

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

Thomas Richard McEvoy

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

Email: richard.mcevoy@hpe.com

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

Emergent Markets

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

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

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

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

Language Issues

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

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

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

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

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

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

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

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

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

Power Relations

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

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

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

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

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

Surveillance

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

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

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

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

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

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

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

Values and Identity

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

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

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

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

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

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

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

Conclusions

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

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

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

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

CRITIS 2016: Call for Participation

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

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

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

Registration discounts

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

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

Peer reviewed papers

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

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

Keynote speakers

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

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

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

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

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

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

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

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

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

CRITIS 2016

uic INTERNATIONAL UNION OF RAILWAYS

Associated events

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

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

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

Call for Sponsors and Exhibitions

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

Venue

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

Key dates

CRITIS event:
10-12 October 2016

Associated events:
13-14 October 2016

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

Previous conferences

LNCS CRITIS 2014 and 2015 proceedings have been recently published:

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

Programme and additional information

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

Preliminary programme

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

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

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

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

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

Links

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

Forthcoming conferences and workshops

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

Institutions

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

Project home pages

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

Interesting Downloads

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

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

Websites of Contributors

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

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

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

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

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

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

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

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

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

Marianthi Theocharidou

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

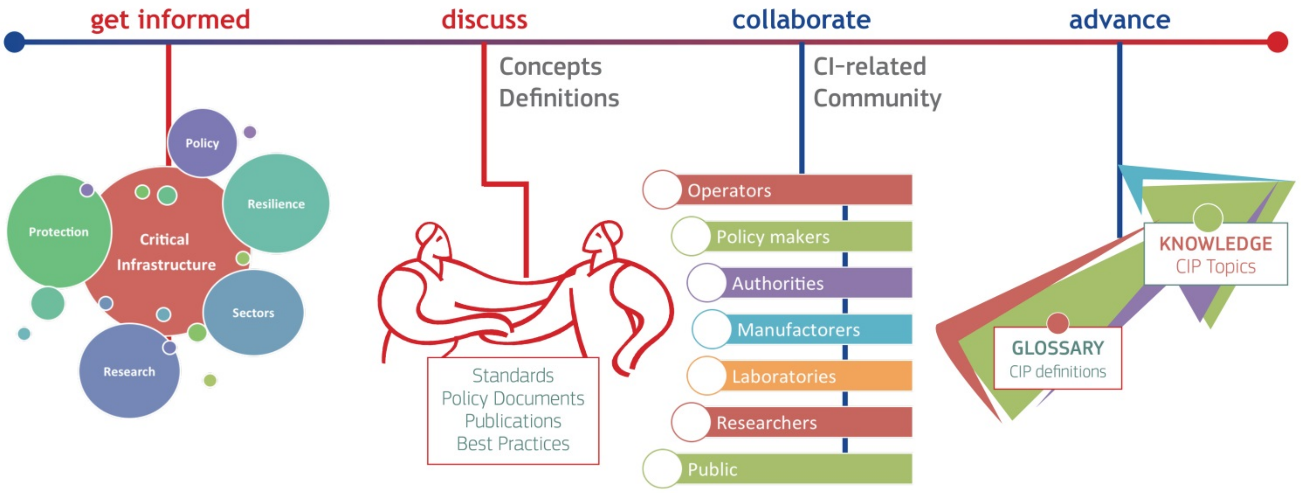
marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

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

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

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


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