European CIIP Newsletter

March 14 – July 14, Volume 8, Number 1

ECN

Contents:

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

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

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

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

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

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

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

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

> Spelling:
British English is used except for US contributions

Editoral

European Activities

Country Specific Issues

Method and Models

About Associations

Books on C(I)IP

Conferences 2014

Links

Editorial: Cyber-attacks with physical impact: reality?

After Snowden's disclosure we know how often systems are under control by others than the owner: is this real and what does this mean for CIP?

Eduard Snowden has given us references to facts that an Information Infrastructure insider knew before. With the references given by Snowden we can start a broader community discussion on what this means for us, when we operate systems that we cannot rely on, or not trust. In everyday ICT we depend on the services; however, we can build a trade-off between how much more efficient we work with these marvellous ICT tools, and the small likelihood that sometimes the system does not do what we want.

In Critical Infrastructures and its critical services by definition we care for best availability and resilience: if this fails, large economic damage, high negative impact on citizens and society is presumed. The name "Critical" is descriptive for what could happen and indicates a zero failure policy.

In crises situations with potential harm to critical infrastructures we depend on our monitoring systems. There are two cases that we would like to share with you:

- Fukushima Nuclear Power Station, March 16, 2011 case: When the catastrophe was evolving, the power went off. As a reaction the engineers went for batteries to supply the most important instruments in the control room. Connecting these to power, the personnel obtained measurements from the reactor. At this time nobody thought that these measurements could be erroneous, and personnel in the control room believed, that water in the reactor is still sufficient. Later investigation disclosed that the water was at this time nearly completely exhausted.
- During the Honours Colloquium 2011 "Cyber Warfare" min 45-47 www.youtube.com/watch?v=wRttZgeTrZQ, Richard Clarke – a long year security advisor of the White House explains how Israeli Air Forces attacked Syria without being attacked by air defence weapons. This worked as follows: The Israeli hackers penetrated the air control room software, such that they could make the system see a clear airspace during the bombing attack operation. Literally, Israeli hackers switched off air control systems of Syria.

  With this hack, the control room of a critical infrastructure preserving the air space of Syria was under control of Israel: a fact that we could not explain that well to the public before Snowden.

Reflecting on cyber depending infrastructures, the CRITIS community has to engage even more than before to:

1. Promote C(I)IP on national level as well as universities.
2. Work towards diversity in the C(I)IP community by including the younger generation because they have a different perception of ICT and were completely, differently, systematically and profoundly educated in ICT.
3. Work towards architecture with fallback positions on minimum operational level, when the cyber dimension is harmed.

The EU FP7 NoE project CIPRNet has initiated a **Young CRITIS Award (CYCA)** exactly for attracting young researcher to this very interesting interdisciplinary work domain. It is a unique chance for young experts to be recognised. Young experts are encouraged to participate in this competition, where useful feedback will be provided by established community experts. For more information:

http://cyca.critis2014.org

As always, selected links – mostly derived from the articles – enhanced with some insider hints, events and exhibitions conclude this issue.

Enjoy reading this issue of the ECN!

PS. Authors willing to contribute to future ECN issues are very welcome.

Elias Kyriakides

is an Assistant Professor at the Dept of Electrical and Computer Engineering and the Associate Director for Research at the KIOS Research Center for Intelligent Systems and Networks, University of Cyprus

e-mail **elias@ucy.ac.cy**

Bernhard M. Hämmerli

is Professor at Lucerne University of Applied Sciences and Gjøvik University, CEO of Acris GmbH and President of Swiss Informatics Society SI www.s-i.ch

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

He is ECN Editor in Chief

CRITIS 2014

9th International Conference on
Critical Information Infrastructures Security
October 13-15, 2014, Limassol, Cyprus

www.critis2014.org

With

Young CRITIS Award Competition

http://cyca.critis2014.org

(see last article
and last page)

Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (CI)

On 24-25 April, in Paris, the first edition of the training course arranged inside the FP7/ NoE CIPRNet will be held, to contribute towards the CIP community in Europe and as a step towards the creation of the EISAC (European Infrastructure Simulation and Analysis Center)

The European Council Directive 2008/114/EC pushed the EU and Member States to address the CIP topic, but there is still a lack of common taxonomies, ontologies, metrics, and risk management frameworks for CIP-related risks and threats that represent serious barriers which need to be overcome. Moreover, the capabilities towards better understanding CI dependencies, cascading failure, and subsequent societal impact are still limited and need to be improved. This is because the CI in European countries form a gradually changing and increasingly complex system; as their interconnectivity continues to increase, so too do their vulnerabilities. To name just two: (1) CIs are becoming increasingly vulnerable to cyber threats and (2) the disaster risk due to natural hazards (e.g. floods) is increasing due to land use expansion and climate change. In addition, disasters involving or affecting CI may be caused by a wide variety of trigger events, (e.g., earthquakes, terrorist attacks, forest fires, human errors and technical failure). Each disaster has its individual course of events, a fact that makes effective responses difficult to plan, train for and subsequently apply. To effectively respond to a large disaster, it is mandatory to perform an adequate pre-event analysis of the threats, possible impacts, and the design, deployment and test of emergency plans, to include the training of the different operators.

Hence there is a need to "bust-up" the capability of emergency management response centres to assess the consequences of potential courses of action (CoA) in order to make well-informed decisions. Assessment of the (possible) effects of concurrent CI disruptions and cascading failure (electricity, drinking water, transportation, etc.) via "what-if" analysis and serious crisis gaming is of increasing importance to the CoA analysis. These comprise the prevention, preparation, response, and recovery/restoration phases of emergency management. The analysis of the CoA consequences on the short and long term shall be based upon real-time and statistical data, current CI status, meteorological and economic data, and more.

For these reasons, in the last two decades the world has seen an increase in the research of computer-based Modelling, Simulation and Analysis (MS&A) of Critical Infrastructures (CI). This multi-disciplinary field of Critical Infrastructure Protection is both an essential method for analysing the complexity of CI systems and an additional means of training crisis managers in complex scenarios involving disruptions of multiple CI. MS&A is reaching a level of maturity which is graduating out of the research centre and into the actual design and management of complex systems for stakeholders.

In this framework, the CIPRNet consortium would like to contribute towards the growth of the CIP community via a series of training events with the focus to **remove**

Roberto Setola

Roberto Setola is professor of Automatic Control at University Campus Bio-Medico of Rome and head of the COSERITY Lab (Complex Systems & Security Lab). He is also the director of the Post Graduate program in 'Homeland Security, Systems and methods and tools for security and crisis management'.

He is the coordinator of the EU DG HOME project FACIES on the automatic identification of failure / attack in critical infrastructures, and the EU DG HOME project SLO on the professional figure of the Security Liaison Officer. He has been the coordinator of the EU DG JLS project SecuFood on security of the food supply chain, and was involved in many other CIP projects.

e-mail: **r.setola@unicampus.it**

some of the barriers for faster progress in CIP. For example, addressing the lack of comprehensive 'repositories' (i.e., the results are dispersed among several sources) and the absence of a common vocabulary / language.

The main goal of the Master Class is to illustrate methodological instruments to forecast the behaviour of Critical Infrastructure during their nominal operational conditions and during crisis situations. This will allow us to estimate the direct and indirect impact(s) on other infrastructures, the environment and the population.

The Modelling Simulation and & Analysis tools of CI have matured out of the research centre and into the field to become a valuable tool capable of supporting design, management and supervision of CI

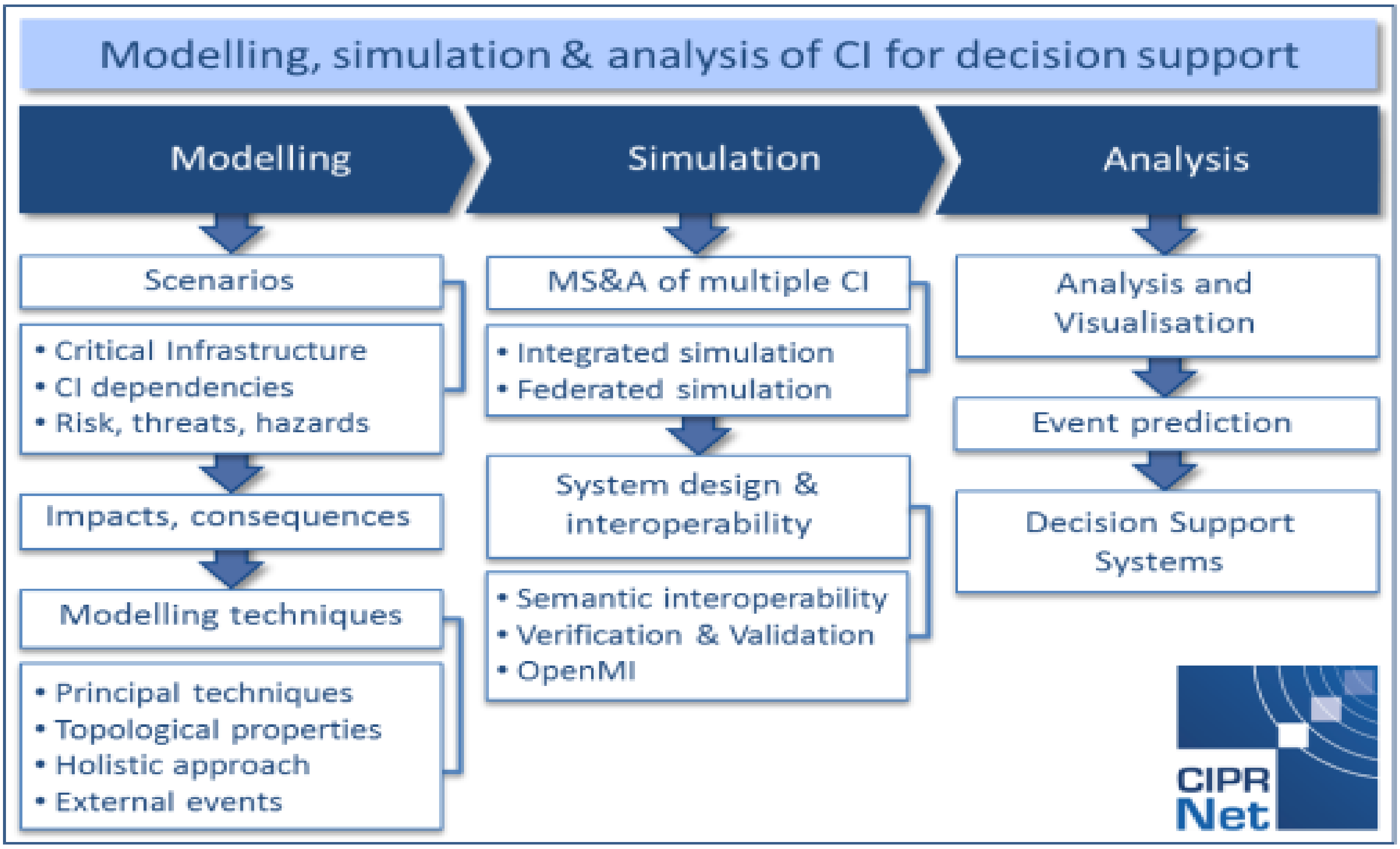
During the 1.5–day training event to be held inside the UIC headquarters on 24-25 April in Paris, top-class experts in Europe in the field of CIP will provide a strong multi-disciplinary and stimulating environment where they will share valuable knowledge about several topics related to CIP.

Specifically the Master Class will illustrate the different methodologies and tools developed to model CI and their specific phenomena as dependencies and interdependencies. The class will further illustrate the effectiveness of the different approaches, in terms of capabilities, and provide the necessary information needed to set-up the different models. Finally, the class will demonstrate how external events, such as natural disasters, may be described and integrated into CI models.

Successively the Master Class will illustrate how the CI models have to be implemented into a simulation framework considering the aspects related with the verification & validation of the solutions. It will analyse the different simulation schemas with a strong focus on the federated simulation, which allows one to make interoperable CI specific simulators. Such a solution is possible thanks to the capability to re-use the existing code and minimize the need to share information. In this structure, a specific attention will be given to the OpenMi framework which recently acquired large interest from several specific domains.

The availability of a simulation tool is the basic element needed to design a DSS (Decision Support System) capable of providing an estimation of possible consequences to adverse events and comparing the effectiveness of different contingency strategies. Indeed the complexity of actual scenarios makes it impossible to correctly predict the impact of any event. The Master Class will illustrate the basic features of a DSS to be used for improved management of CI during a crisis. It will also illustrate schemas on how to relay real-time information on external conditions during a crisis.

The topics will range from the basic concepts of MS&A to advanced aspects related to federated simulation, Decision Support Systems (DSS), and the use of the Open Modelling Interface (OpenMI)



The Master Class will be repeated next year in Rome where additional focus on the design problem of DSS will be explored, allowing the attenders to perform real-scenario analysis exploiting the features of the CIPRNet DSS. The last edition of the Master Class is scheduled for 2016 in Bonn, where the focus will be on '"what-if" analysis.

For more information on the program and for registration please visit the following website:

The participation to the Master Class is free of charge, but for logistic reasons it is limited to 40 participants.

http://www.ciprnet.eu/enduserTraining.html

For any general questions regarding the Master Class, please contact: c.romani@unicampus.it

Master Class on

Modelling, Simulation and Analysis of Critical Infrastructures

International Union of Railways – UIC, Headquarters
Paris, 24-25 April 2014

www.ciprnet.eu

This Master Class is the first edition in a series of training events organised within the European Project ***CIPRNet – Critical Infrastructure Preparedness and Resilience Research Network,*** with the aim to perform training and activities for the *Critical Infrastructures Protection* community, in order to strengthen the links between different research institutions and create common views. In this two-day master class, basic concepts about MS&A (Modelling. Simulation and Analysis) of Critical Infrastructures and advanced aspects related to federated simulation, Decision Support System (DSS) and the use of the Open Modelling Interface (OpenMI) will be illustrated in a multi-disciplinary framework. Top experts from various backgrounds coming from all Europe will be presenting lectures. The master class is addressed to both researchers and technicians from different research communities and experts from CI operators and Public Authorities.

The event is free but limited to a maximum of 40 participants with a first-come, first-served basis. The application must be sent **no later than 9 April 2014**.
Detailed program and application http://www.ciprnet.eu/training.html
For more information and specific requirements c.romani@unicampus.it

uic
16 rue Jean Rey
F 75 015 PARIS
Tour Eiffel
Champ de Mars
La Seine
Rue Jean Rey
Avenue de Suffren
Rue de la Fédération
Quai Branly
Quai de Grenelle
Boulevard de Grenelle
RER
M
BUS
uic

Information about the Venue:

International Union of Railways – UIC
16 rue Jean Rey, 75015 Paris (France)

How to get there: http://www.uic.org/spip.php?article2689

The Master Class is organized by:
University Campus Bio-Medico of Rome, International Union of Railways,
and French Alternative Energies and Atomic Energy Commission

The Austrian approach to Critical Infrastructure Protection (CIP)

As one of the leading countries in the implementation and the support for the development of the European Programme on Critical Infrastructure Austria is now drafting a new Programme on CIP on the national level.

Fallowing the terrorist attacks in London and Spain in 2004, the European Union started with the development of a "European Programme for Critical Infrastructure Protection" (EPCIP). Since then, the importance of this topic as well as the awareness on governmental level have simultaneously increased.

Consequently, the EU Member States launched their corresponding national programs as encouraged by the European Commission.

The starting signal for the "Austrian Programme on Critical Infrastructure Protection" (APCIP) was in 2008 with a resolution of the Council of Ministers. The resolution accompanies the so-called "Masterplan" which sets forth the APCIP. The Austrian Programme is characterized by being based on the principles of EPCIP and being complementary to it.

> Critical Infrastructures are infrastructures, or parts of it, which are of strategic importance for the maintenance of fundamental social functions. The disruption or destruction of these infrastructures has severe implications on the health, security or the economic and social welfare of the society or the effective functionality of the public facilities.

The primary objective of APCIP is prevention. Contrary to other EU Member States, Austria has chosen a systemic approach for its programme. Therefore, it is not key if the infrastructure (e.g., electricity) is available, but if the system as a whole works. In addition, Austria abstains from a legal approach and seeks for cooperation between the administration, economy and academia. Hereby, the creation of mutual confidence is of particular importance and APCIP-partnerships are pursued.

Since 2008 Austria has implemented the measures as well as the action plan of the APCIP Masterplan of 2008. Hence, the further development of the Austrian approach was necessary, wherefore the APCIP Masterplan 2014 is now being drafted.

On the one hand, the new Masterplan is supposed to display the changed setting for CIP in Austria through the implemented measures and objectives of the 2008 Masterplan. On the other hand, it will take into consideration the acquired knowledge of the last years as well as intersecting themes like Cyber Security.

The most essential aims Austria has reached with the implementation of its Masterplan 2008 are the following:

Identification of Austrian Critical Infrastructure

The protection of Critical Infrastructures is vitally important for the Austrian Security Agencies in order to secure the maintenance of services for the public and with it the internal security. A crucial step therefore was the identification and designation of Austrian Critical Infrastructure (ACI). Significant criteria for the identification of ACI were

- the relevance of the infrastructure for life and health, public security, economic and social welfare of the population, as well as for the ecology;
- the avoidance of loss of service;
- the business location Austria and specialized services.

Beate Wegscheider

Beate Wegscheider is a Security Policy Officer at the Security Policy Centre in the Austrian Federal Ministry of the Interior in Vienna.

She received her Masters degree from the University of Vienna in 2008. Beate is currently in the process of finishing her PhD thesis in Political Science. In addition, she has completed several trainings in the field of Common Security and Defense Policy, Security Sector Reform, Peacebuilding and Peacekeeping as well as Election Observation. Her fields of interests include the demographic change and its implications for internal security, conflict transformation and management and European security policy.

She regularly participates at national and international conferences and workshops in the field of security and international politics.

e-mail:
beate.**wegscheider@bmi.gv.at**

For the allocation of the strategic infrastructures the ÖNACE-classification was used which enables national and international comparability.

The compiled list of ACI is a living document which needs to be evaluated and updated frequently.

Guideline for CIP Infrastructure

After having identified the Austrian Critical Infrastructures, a guideline was developed for operators and owners of ACI. The guideline is meant to raise awareness at the CEO level and to support the setting up of comprehensive security architecture within the Infrastructure.

Furthermore, it aims to increase the availability of services and products of vital importance for the public. For this reason the guideline is supposed to assist in

- the identification of risks for strategic infrastructures;
- the implementation of risk reducing measures and
- the implementation of preventive and reactive measures against extraordinary events causing damage.

On the one hand, the guideline describes international norms and standards relevant for risk management processes and indications for national and international best practice models and corporate security management. On the other hand, it also offers a self-evaluation in the form of a structured questionnaire to assist with the identification of risks and possible preventive and reactive security measures. Furthermore, it offers recommendations for improvement.

All identified ACIs have received the guideline for self-evaluation and were requested to announce a point of contact within the enterprise to attend the CIP public-private partnership.

Public-Private Partnership

In 2008, the European Commission also submitted a proposal on a Warning and Information Network for Critical Infrastructures (CIWIN[1]). After an intensive consultation process the European information platform finally went live in 2013. The platform offers registered members of the CIP-community the possibility to discuss and exchange relevant information, surveys and best-practice models. In addition, each EU member state was offered the opportunity to set up a national page on CIWIN-EU.

Austria has taken this opportunity and established a national CIWIN page for the Austrian CIP-community which will serve as an information platform on CIP.

Up to date Austria is the only EU Member State that has established a national CIWIN information platform.

The new Critical Infrastructure Unit

On the operational level, the Federal Agency for State Protection and Counter Terrorism has established the new unit “Critical Infrastructure Protection and Cybersecurity”. Primarily, the unit supports strategic infrastructures with the implementation of comprehensive security architecture. For this purpose it offers concerted consultations, identification of risks and threats and provides information about current threats.

Moreover, specific situation reports as well as information regarding available products, mentoring and trainings in the areas of e.g. physical protection, risk management, IT-security, business crime, economic and industrial espionage, terrorism and extremism will be provided.

Supplementary, a contact and reporting point for operators of critical infrastructure has been installed.

Nexus Cyber Security

A close content-related correlation exists between Cyber Security and the Protection of Critical Infrastructure. The Austrian Cyber Security Strategy provides measures for the protection of critical infrastructures in the field of action 4 and other areas. The Operational Coordination Structure (OCS) will support the ACIs on operational level and in particular in the event of failure of information and communication structures. Through the OCS they will also be provided with information on the dangers of the Internet. According to the Austrian Cyber-Security Strategy, cyber-safety standards for ACI need to be defined and crisis and continuity plans for the common overall cyber crisis management compiled.

Furthermore, the Austrian Cyber Security Platform will be established as a public-private partnership. The aim of the platform is to facilitate ongoing communication with all relevant stakeholders of the administration, economy and academia.

A legal regulation on the notification requirement for severe incidents for strategically important infrastructure needs to be prepared.

The corresponding task forces are currently incorporating these requirements in their work.

As outlined, Austria has made some considerable steps forward in the enhancement of the protection of its critical infrastructures. With the new Masterplan of 2014 the renovation of the Austrian programme will be brought forward.

If you would like to find out more about the work of the Federal Ministry of the Interior please visit our website www.bmi.gv.at.

[1] Critical Infrastructure Warning and Information Network

Simulation and Reality:
Coincidence in Crisis happening

Severe accidents and crises are the result of the unlikely accumulation of many random hazardous events. Some would call that "black series" or "bad coincidences". But coincidences are unlikely to happen twice!

Formal sciences ultimate target is to represent the reality of our surrounding world. Many philosophers and scientists believe that the reality revealed by Science offers only a "veiled" view of an underlying reality that Science cannot access. These are mainly because of two reasons: formal sciences are imperfect and what we call "reality" is the projection of the inaccessible "Reality" on our world. We will call this projection on our world "the reality". It is the only reality we are talking about through our article. More interesting points of views may be found in ([1],[2])

Struggling to approach their ultimate target, formal sciences construct objects in which small parts of the reality are grasped and formalised. These objects could be called "models". Because we are limiting our interest only to formal sciences and engineering, these objects are mathematical models. That covers both conceptual and phenomenological models. Models are first validated before being admitted in the global modal of the reality.

Engineering sciences are amongst the most active in producing, validating and applying mathematical models in different aspects of our daily life. Based on the models, engineers and researches are developing robust simulation capabilities of the reality making use of the modern capabilities of performing intensive and coupled calculations. The ambition is to simulate not only independent isolated phenomenon but also of interacting phenomenon belonging to different physics at varying scales.

Regarding our main concerns of protecting critical infrastructures and helping in decision-making in case of severe accidents or crises, advanced simulation capabilities play a decisive role. The simulation of well-defined sequences of events leading to major potential crises is of great help in:

- Decision making in order to elaborate the best strategies in managing crises and severe accidents.
- Helping operators to prioritize actions in real situation facing systems' primary failures and their propagation.
- Helping designers to improve systems' design in view of minimizing failures' frequency and failures propagation and of maximizing consequences mitigation.
- Training future technical staff and qualified persons who will be engaged in systems design, systems operation and crisis management.

Developing powerful integrated simulation capabilities is a serious challenge to all the scientists and the engineers in the field. This ambition gives birth to two major challenges:

- Developing and validating models considering dependencies and interfacing between different physics at varying scales.
- Integrating stochastic and random phenomenon in a global coupled modelling process.

Both challenges are of the same importance but we will focus on the stochastic aspects of events initiating severe accidents. Major crises result very often from the occurrence of some sequences of random events that are combined with some systems' failures, resulting at the end of the sequence serious hazards.

We can mention some examples such as: the Concorde crash (AF4590, Paris-New York, 25 July, 2000) [3][3], the EU Blackout (Saturday-Sunday 4-5/11/2006, EU) [4] or the Fukushima accident (11 March, 2011, Japan) [5]. All are cross-border accidents. In all these cases, it was the sequential accumulation of independent random events that led to the severe accident. Let's take the crash of the Concorde in order to identify the sequence of the

Mohamed Eid

Mohamed Eid is a Senior Expert in the French Commissariat of Atomic Energy & Alternative Energies (CEA) and an Associated Professor in the National Institute of Applied Science (INSA) of Rouen. His research and teaching activities cover fields such as: Probabilistic Risk Analysis, System Reliability and Safety, Monte-Carlo simulation, Multi-States System Modelling, Systems Dependency and Interdependency. He is the author of some 50 scientific papers in the field of systems safety, reliability and stochastic modelling.

He is a member of many editorial boards of scientific journals in the field of system reliability, safety and maintenance.

An active member in many EU networks: ESReDA, CIPRNet, …
An active member in many EU conference series programme committees: ESRel, ESReDA, SSARS, Lambda-Mu etc.

email: **mohamed.eid@cea.fr**

independent random events that led to the major event. We will not go through the details of the accident analysis report, [3]. We will only underline the sequence of these random events.

The post-accident investigations revealed that:

- The aircraft was over the maximum take-off weight for the ambient temperature and the other conditions, and 810 kg over the maximum structural weight. (It is useful to underline that the total fuel capacity is 95 680 kg and the max take-off weight is 185 065 kg).
- The load was distributed such that the centre of gravity was excessively far to the rare.
- Fuel transfer may have overfilled the wing tank number five.
- Five minutes before the Concorde, a Continental Airlines DC-10 departing for Newark, New Jersey, had lost a titanium alloy strip, 435 millimetres long and about 29 to 34 millimetres wide, during take-off from the same runway.
- This piece of debris, still lying on the runway, cut a tyre, rupturing it, during the Concorde's subsequent take-off run.
- A large chunk of tyre debris (4.5 kilograms) struck the underside of the aircraft's wing at an estimated speed of 140 metres per second. The strike sent out a pressure shockwave that ruptured the number five fuel tank at the weakest point, just above the undercarriage.
- Leaking fuel was most likely to have been ignited by an electric arc in the landing gear bay or through contact with severed electrical cables.
- The flame before the Concorde was airborne.
- With only 2 km of runway remaining and travelling at a speed of 328 km/h, the only option was to take off. The Concorde would have needed at least 3 km of runway to abort safely.

Let's now identify the random events that led to the major accident event. In that very succinct description of the sequence development, one may identify the random/stochastic independent events as following:

- Overloading: what is the probability for the Concorde to be overloaded by a factor less than or equal to 0.5% of its take-off weight, considering the ambient temperature and other conditions? Knowing that the ambient temperature and the other meteorological conditions are themselves stochastic (random with time).
- Load distribution: what is the probability that the load (overloaded or not) is not correctly distributed and results in an excessive offset of the plane gravity centre?
- Foreign objects on the runway: what is the probability of introducing a metallic object on the runway between two successive runway inspections?
- Detecting objects on the runway: what is the probability of not detecting a metallic strip (40x30cm) on the runway in 5 minutes?
- Tire collision with a metallic object on the runway: what is the probability that one of the tires of an airplane hits a metallic object on the runway during take-off?
- Tyre blow out: what is the probability that the hit tyre blow out?
- Heavy chunks production as a result of a tyre blow out: what is the probability that the blown tyre sends out heavy chunks (> 2-3kg)?
- Collision with a fuel tank: What is the probability that the flying heavy chunk strikes violently (> 100 m/s) any of the wing fuel tanks?
- Tank puncture by direct impact of a heavy chunk at high speed: what is the probability that the violent strike punctures the tank?
- Tank rupture by shockwave propagation: what is the probability that the violent strike produces a shockwave capable to rupture the tank at any of its weak points, if the tank was not punctured first?
- Fuel fast ignition: what is the probability that the leaked fuel could be ignited within a very short time (~ few seconds after leak)?
- No abortion possibility: what is the probability of a successful abortion as function of the run distance and airplane speed?
- Fuel slow ignition: what is the probability that the leaked fuel could be ignited within a longer time (~ the first 30 minutes, hour, 2 hours, ...)? After taking off and attending heights where the ignition conditions are not favourable!

The sequence of interest is then defined by 11 independent events: airplane overloading (~0.5%), inadequate load distribution, introduction of a large foreign object on the runway, non-detection of large foreign object on the runway within 5 minutes, collision of an existing object on the runway with one of the tyres during take-off run, tyre blow out as a result of a collision with a large metallic object (435 mm long and 29 to 34mm wide), fragmentation of a blowing tyre into heavy chunks (> 2-3 kg), collision of a heavy flying chunk with one of the fuel tanks, rupture of the collided tank (directly or indirectly) following the collision, immediate ignition of the leaked fuel and no more enough distance on the runway to abort safely. This is a sequence of 11 independent and random / stochastic events (coincidence?).

The same demarche of analysis can be performed for the EU Blackout (Saturday-Sunday 4-5/11/2006) and for the Fukushima accident (11 March, 2011, Japan) in order to identify the sequence of independent random/stochastic events that led to the final hazard. However, we will only recall succinctly the description of the final hazard in both accidents.

In the case of EU Blackout (Saturday-Sunday 4-5/11/2006), [4]: A power imbalance in the Western area induced a severe frequency drop that caused an interruption of supply for more than 15 million European households (for about 2 hours). The detailed analysis of the events and the sequence identification are given in [4].

In the case of the Fukushima accident (11 March, 2011, Japan), [5], following a strong earthquake and a strong tsunami. The nuclear power plant of Fukushima (4 reactors) had lost the electrical supply from the grid and the emergency electrical supply units on the site. Subsequently, that resulted in a significant loss on different control capabilities and the loss of the reactor cooling systems of three reactors. The overheating of the reactors lead to the production of a significant quantity of hydrogen in one of the reactors which exploded on 12 March resulting in the blowing out of the ceiling of the reactor building number one. A significant release of radioactive materials had subsequently been monitored. The detailed analysis of the events and the sequence identification are given in [5]. Some analysts may think that strong earthquakes result always in strong tsunamis. This full correlation between these two events is not proven. A probabilistic correlation exists however less stronger earthquakes can still result in strong tsunamis, ([6],[7]). In all cases of severe accidents and crises it is a matter of a sequence of ordered well-defined random / stochastic events.

Coincidence?

Severe accidents and crises are the result of the unlikely accumulation of many random hazardous events. Some would call that "bad coincidences" or "black series".

In the case of the Concorde crash, we have too many unlike and independent random and stochastic events in one sequence! Even if some are highly probable such as: the blowing out of a tyre after the collision with a heavy metallic object and the tank rupture following a violent collision with a heavy object flying at high speed. Others are not, such as: the introduction of a large foreign object on the runway between 2 successive take-offs runs and the collision of a heavy chunk with one of the fuel tanks.

In these long sequences of random events, it is enough that a few events show low occurrence probabilities so that the occurrence probability of the whole sequence becomes very low. For example we may imagine that if the occurrence probability of the event "inadequate load distribution" was knowing that the overloading was within a very low range (< 0,5%) and if the occurrence probability of the event "non-detection of a large foreign object on the runway within 5 minutes" was in the range of 10-3-10-4, the occurrence probability of the sequence would already be in the rage 10-6-10-7 per take-off run, assuming that all the other 9 events had occurrence probabilities close to one (~ 100%).

What is "Coincidence"? I would answer "Coincidence" would be underlined in two manners:

- Objectively: when some random unlikely events included in a well - defined sequence occur in a given order. Here, we are more interested in the occurrence probabilities of the individual events and less interested in the sequence occurrence probability itself.
- Subjectively: when a sequence with a very low occurrence probability occurs to "Me".

We will be interested in the object (mathematical) perception of the "Coincidence". Coincidences do objectively occur whatever is the low occurrence probability of the whole sequence. Coincidences have a sense when it is a matter of: many events (not only one event), random (/stochastic) and in a given occurrence order.

Probabilistic Modelling

More complex are the systems man designs, more complex are the hazardous sequences in case of severe accidents and crises. Integrating probabilistic approaches would allow constructing global models in order to deal with phenomenon of different nature at varying scales.

Mitigation

Analysing sequences of events lead systematically to improving the mitigation of the consequences of each individual random/stochastic event involved in.

Back to the Concorde crush, analysing the sequence of the individual events would suggest to:

- Improve the detection of foreign objects on the runway (this is not out of reach of our modern technology)
- Improve the resistance of tyres for collision with metallic heavy objects at high speed (~ 300 km/h)
- Improve the tyre's materials and fabrication process such that only small and very small chunks would be produced when blowing out.
- Improve the shielding against and the resistance of the fuel tank structure to the collision with heavy objects at high speeds.
- Find out design modifications to prevent the ignition of the spelled fuel during take-off.

What if?

One way to cope with hazardous sequences is to question systematically us, what if:

- Such or such occurrence probability was less or higher?
- Such or such occurrence order was followed?
- Such or such component was lighter or heavies?
- Such or such shielder was thinner or thicker?

Models & Simulation

Models and simulation do not describe exactly the reality. But they are perpetually in improvement to come closer and closer to the reality. We still talk about our local reality (the projection on our world) not the real Reality, which is certainly inaccessible. However, models and simulation help us to improve the quality of life and make it safer, every day

Robust models and powerful simulation capabilities are necessary in order to perform efficient "What if" analysis and to verify the validity of the different mitigation measures. We recall that we consider both conceptual and phenomenological models. It is the only way to perform, a priori, investigations of accidents and crises. Otherwise, we are condemned to perform posteriori investigations to come up with the same improvements. It is to say to wait for the occurrence of severe accidents and crises. But coincidences are unlikely to happen twice.

References

[1] Christian Hennig, "Mathematical Models and Reality – a Constructivist Perspective." Research Report No.304, Department of Statistical Science, University College London, June 2009. http://www.ucl.ac.uk/statistics/research/pdfs/rr304.pdf.

[2] John Byl, "Mathematical Models and Reality." Proceedings of the 2003 Conference of the Association for Christians in the Mathematical Sciences.

[3] BEA final report, 'Accident on 25 July 2000 at La Patte d'Oie in Gonesse (95) to the Concorde registered F-BTSC operated by Air France.' F-BTSC - 25 July 2000.

[4] UCTE Investigation Committee report, "Final Report System Disturbance on 4 November 2006." Union for the Coordination of Transmission of Electricity, 30 January 2007. https://www.entsoe.eu/news-events/former-associations/ucte/other-reports/

[5] NAIIC report, "The Official Report of Fukushima Nuclear Accident Independent Investigation Commission – Executive Summary." The National Diet of Japan, 2012. http://www.nirs.org/fukushima/naiic_report.pdf

[6] Hiroo Kanamori, "Mechanism of Tsunami Earthquakes." physics of

the earth and planetary interiors journal, 6, 346-359, 1972, North Holland Publishing Company.

[7] Eric L. Geist and Uri S. Ten Brink "NRC/USGS Workshop Report: Landslide Tsunami Probability." U.S. Department of the Interior U.S. Geological Survey, Administrative Report, 2012

46th ESReDA Seminar on

Reliability Assessment and Life Cycle Analysis of Structures and Infrastructures (May 29th - 30th, 2014)

Politecnico di Torino, Turino, Italy

ESReDA Reliability Assessment and Life Cycle Analysis of Structures and Infrastructures

The aim of the 46th ESReDA seminar is to bring together scientists, engineers and decision makers in the field of structural safety and risk management, in order to present and discuss innovative methodologies and practical applications related to structural reliability and life cycle cost: assessment, testing, analysis, design, monitoring, maintenance and optimization. Scientific methodologies, theoretical issues and practical case studies are expected to cover all the range from academic to industrial applications, including mechanical and civil engineering. A selection from seminar papers will be published in the book edited by ESReDA on Reliability based Life Cycle Cost Optimization of Structures and Infrastructures.

ABOUT EUROPEAN SAFETY, RELIABILITY & DATA ASSOCIATION

European Safety, Reliability & Data Association (ESReDA) is a European Association established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability.

For more information please visit the ESReDA home page: http://www.esreda.org/

Economic Perspectives on Security Management

Critical Infrastructure Security and Return on Security Investment (ROSI)

In view of growing threats to public safety and security and increasing budgetary restraints, risk management in government and industry must be both effective and cost-efficient. To this goal, recent advance in the econometric and operational sciences can be exploited to develop and apply a generic quantitative risk assessment methodology as a security planning and management device to protect public infrastructures and large-scale industrial systems. The concept of quantitative risk assessment thereby means the coherent intrinsic, or "fair", pricing of risks. It implies considerably more than risk measurement in the sense of statistical risk analysis ("intrinsic" refers to risk quantification within a given accounting system rather than to risk prices extrinsically determined by the market for risky goods or services).

It is evident that the practical use and public policy implications of a coherent approach to measure the intrinsic value of any given risk would be considerable. It could help to determine, in a realistic and systematic way, the amount of risk reduction achieved per euro invested in technologies and management efforts to prevent safety and security incidents in large-scale systems and public infrastructures, or mitigate the damage arising from such incidents. As for security management, this is exactly what is otherwise known, though largely missing in practical applications, as calculating the Return on Security Investment (ROSI).

Quantitative risk assessment and the pricing of risk

Risk management has long been suffering from the fact that risk is an elusive concept. Correspondingly, existing methods to assess risks and risk reduction measures tend to be ambiguous and controversial, if not manifestly inconsistent, for one of the following two reasons. They are either *ad hoc* rather than systematic, meaning that they lack theoretical coherence, or hard to operationalise. In either case, they may not provide the reliable information decision makers need to solve their problems.

Advance has recently been made on the basis of novel methodological approaches to economic utility theory and the statistical foundations of quantitative risk assessment [1, 2, 3, 4].

> It is evident that the practical use and public policy implications of a coherent approach to measure the intrinsic value of any given risk would be considerable.

These approaches have in part been developed and applied within research projects on infrastructure security and security economics co-funded by the German government (SiVe, 2008-2011) and the European Union (ValueSec, 2011-2014). More details can be respectively found at http://www.bmbf.de/en/13086.php and http://www.valuesec.eu

The methodology for optimal, cost-efficient risk and security management employed in these projects involved concepts of "generalised expected utility" that have been demonstrated to be able to admit coherent, explicit numerical representations of risk preferences, while accommodating basic empirical, individual and social attitudes towards risk. Most importantly, however, they have proven to be sufficiently simple for operational use in applied risk research. Meanwhile, "utility" has nothing to do with naïve views of "degree of individual satisfaction", "desirability" and the like: it is a technical term simply meaning a behavioural risk preference score.

Gebhard Geiger

Gebhard Geiger is a professor of methodology and philosophy of science in the Technical University of Munich, Germany (TUM). He is specialising in foundational problems of the operational sciences, especially mathematical methods in risk and security research. He holds doctoral degrees in theoretical physics (Ludwig-Maximilians-Universität München, LMU) and philosophy of science (Habilitation, TUM), and an MA in political science (UCLA).

e-mail: **g.geiger@ws.tum.de**

The core concept of quantitative risk assessment is the pricing of risk. Risks can be formally represented as probability functions $f(x)$ of the likely gains or losses x (in monetary terms or otherwise) obtained from safety or security incidents with uncertain consequences. A real number $c(f)$ is called the *certainty equivalent of the risk* $f(x)$, if $f(x)$ and the certain amount $c(f)$ of gain or loss are indifferent in preference terms. The certainty equivalent of a given risk can accordingly be viewed as the fair, or "intrinsic" price of that risk, considering that f and $c(f)$ are equal in preference. In practice, it can be explicitly calculated for every given probability function f.

Figure 1 illustrates important realistic features of the quantitative account of risk assessment. One such feature is the marked deviation of the fair price (curved line in Fig. 1) from the probabilistic mean value of a risk (straight line), thus expressing widely observed, non-neutral human attitudes towards risk. Another feature is the capacity of the present approach to accommodate patterns of variability of risk attitude across various dimensions of risk. Finally, this simple and straightforward concept of intrinsic pricing of risks provides a powerful management tool, admitting direct assessments to be made of the effectiveness and cost-efficiency of planning and decision-making under risk.

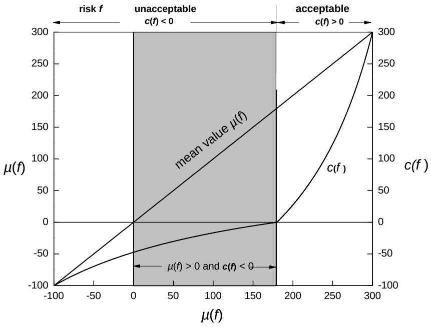


Fig. 1: Example of certainty equivalent c(*f*) and mean value μ(*f*) of probability function *f*.

Effectiveness of Security Risk Management

Real systems can generally be assumed to be operated with larger or smaller risk management effort. Two risks *f* and *g* linked to the effort aiming to mitigate them can be estimated, considering the likely consequences of security incidents affecting any such system considered. Furthermore, the risk prices c(*f*) and c(*g*) of the risks with and without appreciable risk management arrangements, respectively, can be calculated and compared. For example, the comparison c(*f*) ≥ c(*g*) shows the effectiveness of the measures planned or taken to reduce the risk *g* to *f*. In this example, the price difference c(*f*) – c(*g*) is positive. It measures the Return on Security Investment (ROSI) that can be gained when the system changes from the risky state *g* to the less risky state *f*. If, on the other hand, the difference c(*f*) – c(*g*) is small or even turns out negative, the risk management proves ineffective.

Cost-Efficiency of Security Risk Management

Let *k*(*f*, *g*) be the cost incurred by security managers to reduce the risk *g* to *f*. The ratio of ROSI to cost of the security arrangements made gives the amount of risk reduction per euro invested. It measures the cost-efficiency of the risk reduction achieved. Risk management is optimal if for given "*status quo* risk" *g*, the target risk level *f* is chosen so that the cost-efficiency ratio is at maximum within a given set of alternative risk mitigation choices.

A numerical example is shown in Figure 2. In the example, q is the rate with which a scanning technology detects explosives at the passenger and luggage checkpoint of an airport.

Without the scanning machine in operation, *x* is the number of passengers killed or lives saved with probability *g*(*x*) if a terrorist smuggles an explosive device into the check-in area of the airport where he detonates his bomb. The equivalent number of lives saved or lost increases from the *status quo* with c(*g*) = 0 and *q* = 0% to c(*f*), if money is invested to adjust q optimally. The cost-efficiency ratio c(*f*)/*k* reaches its maximum approximately at *q* = 58% in this example.

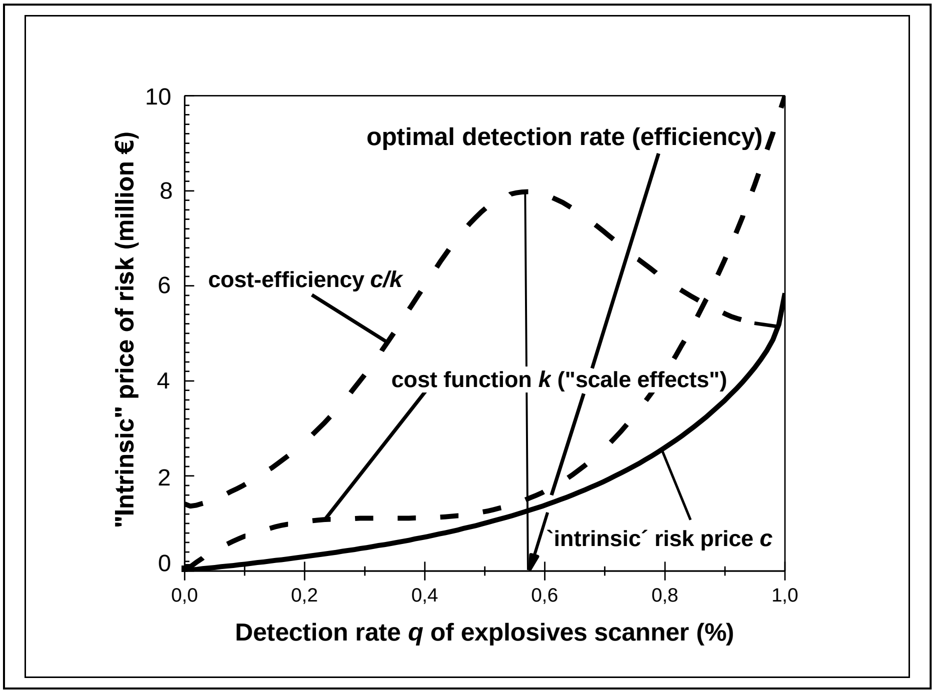


Fig. 2: Example of cost-efficiency of airport security management. After Goldner *et al*. [3].

This simple and straightforward concept of intrinsic pricing of risk provides a powerful management tool, admitting direct assessments to be made of the effectiveness and cost-efficiency of planning and decision-making under risk.

Modelling Airport Security Management

Safety and security planning in large-scale systems can be made very effective by combining scenario-based computer simulations of systems and processes (e. g., Monte Carlo simulations) with numerical estimates of damage probabilities in simulated safety and security incidents. The effectiveness and cost-efficiency of technical, organisational and procedural risk management provisions can thus be assessed quantitatively prior to their implementation.

Risk and security management as well as attacks can be modelled as processes. A process model may, in turn, help to identify all the relevant risks attached to a process itself or any further actions triggered by it. In airport security analyses, it is therefore important to develop a generic process model of terrorist attacks against airports first (Fig. 3).

Safety and security planning in large-scale systems can be made very effective by combining scenario-based computer simulations of systems and processes with numerical estimates of damage probabilities.

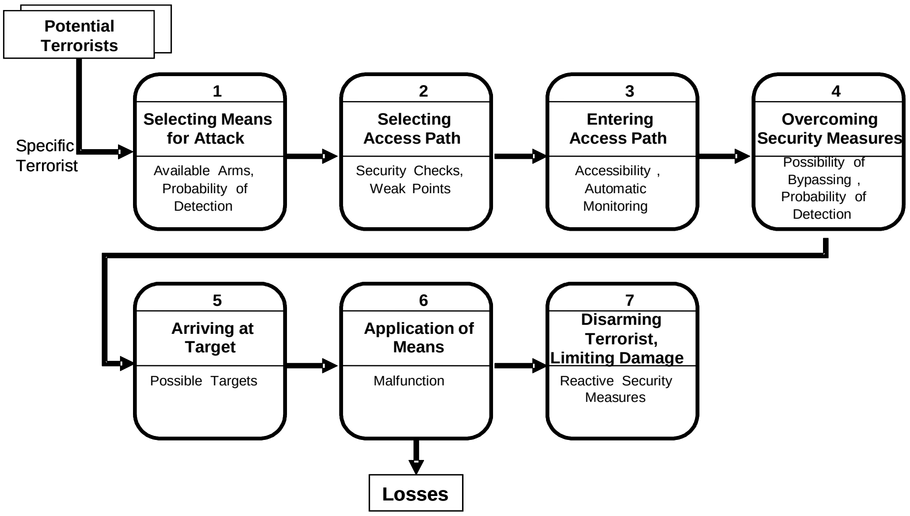

Potential Terrorists
Specific Terrorist
1
Selecting Means for Attack
Available Arms, Probability of Detection
2
Selecting Access Path
Security Checks, Weak Points
3
Entering Access Path
Accessibility , Automatic Monitoring
4
Overcoming Security Measures
Possibility of Bypassing , Probability of Detection
5
Arriving at Target
Possible Targets
6
Application of Means
Malfunction
7
Disarming Terrorist, Limiting Damage
Reactive Security Measures
Losses

Fig. 3: Generic process model of a terrorist attack on an airport. After Geiger *et al.* [1]

If, for example, a terrorist attack on airport security using liquid explosives (liquids, aerosols and gels, LAG) is considered, the analysis must be carried out considering the following possibilities.

1. A terrorist (suicide bomber) is assumed to arrive at the airport security check. The probability of attack = 1 (i. e., a "What if" scenario is used). The terrorist carries a liquid explosive to be detected with probability q ("detection rate", see Fig. 2) or else passes the security check undetected with probability 1-q. When detected he tries to detonate the explosive at the check point and kill himself and as many passengers as possible.
2. The situation is characterised by a number of parameters such as false clear rate, false alarm rate and other attributes of the operational performance of the LAG explosives scanning technology and staff such as quota q, if any, throughput time per passenger, number of passengers to be checked per hour operation time, etc.
3. If the terrorist succeeds to enter the aeroplane, with his liquid bomb undetected, the events occurring aboard generally depend on random factors: the terrorist attempts, more or less successfully, to mix components of liquid explosive; he may fail to get his bomb ready for use; he may be tackled and overpowered by passengers or crew (by an air marshal, if any); the bomb may fail to detonate; alternatively, it may be successfully ignited; the plane is severely damaged and crashes, with all passengers dead; or the plane may be damaged, but capable of continuing to fly and finally touch down; etc.
4. Most importantly, the screening for LAGs makes impact (imposes limits) on terrorist´s success: type and/or amount of usable LAG is restricted, detonator suboptimal or restricted (e. g., contains no metal parts), etc.
5. The possible courses of action aboard the plane are treated as outcomes of a random experiment. As such, they are assigned to (known, estimated, etc.) numbers of fatalities. The frequencies with which the fatalities occur are obtained in repeated (Monte-Carlo-like) trials of the experiment (in fact, each course of action is modelled as a "business process", using modern software-based processes modelling techniques).
6. The random simulations give the particular probabilistic distribution of fatalities involved in an incident. The extreme case is the detonation of the liquid bomb followed by an aeroplane crash, with all passengers and crew killed.
7. Using different fatality risk distributions f(x), g(x), … obtained in the simulation experiments, the effectiveness and cost-efficiency of the alternative LAG screening technologies to prevent or mitigate these risks can be directly estimated and analysed in quantitative terms, as outlined above.

Concluding Remarks

In view of the immense complexity of the infrastructures of modern society, incident simulation techniques and methods of quantitative risk assessment can be employed to prevent or mitigate damage from catastrophic events in systematic, practical, effective and cost-efficient ways. Some of the core problems involved here can be successfully addressed, combining methodological perspectives of modern systems analysis and simulation and econometric approaches to risk assessment.

References

[1] G. Geiger, E. Petzel and M. Breiing, "Process-Based Identification and Pricing of Risks: Methodological Foundation and Applications to Risk and Security Management". In P. Elsner (Ed.): Future Security – 4th Security Research Conference. Fraunhofer Verlag, Stuttgart 2009, pp. 208-220.

[2] M. Breiing, M. Cole, J. D'Avanzo, G. Geiger, S. Goldner, A. Kuhlmann, C. Lorenz, A. Papproth, E. Petzel and O. Schwetje, "Optimisation of Critical Infrastructure Protection: The SiVe Project on Airport Security". In E. Rome and R. Bloomfield (Eds.): CRITIS 2009. Lecture Notes in Computer Science 6027, Springer-Verlag, Berlin-Heidelberg 2010, pp. 73–84.

[3] S. Goldner, A. Papproth, E. Petzel and G. Geiger, "Improving the Security of Critical Transport Infrastructures - New Methods and Results". In J. Ender und J. Fiege (Eds.): 6th Future Security Research Conference – Proceedings. Fraunhofer Verlag, Stuttgart 2011, pp. 545-554.

[4] R. Hutter and C. Blobner, "How to rationalise and economically justify security for CIP". European CIIP Newsletter Vol. 7, No. 1, 2013, pp. 9-11.

(Left intentionally blank
for double sided printing)

The Global Risk Forum GRF Davos

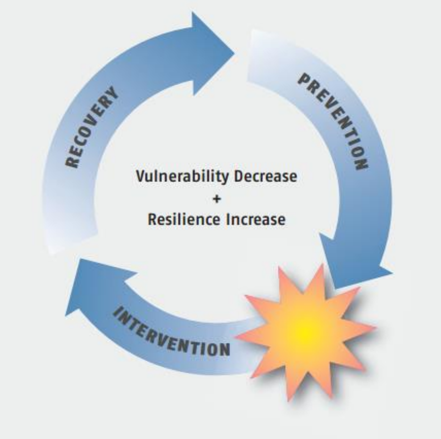
The Global Risk Forum GRF Davos promotes the worldwide exchange of know-how and expertise, creates solutions and fosters good practices in integrative risk management including climate change adaptation. The foundation aims to improve the understanding, assessment and management of disasters and risks that affect human safety, security, health, the environment, critical infrastructures, the economy and society at large.

Through its various activities GRF Davos aims at serving as a centre of knowledge and know-how exchange for the application of contemporary risk management strategies, tools and practical solutions. Thus, GRF Davos aims at reducing vulnerability for all types of risks and disasters to protect life, property, environment, critical infrastructure and all means of business for the worldwide community on a sustainable basis.

As recent mega-disasters and crises have shown, risk management from a single perspective is no longer adequate to address the complex threats to today's society. A truly integrated and participative approach is necessary. This approach ensures that lessons learned in risk reduction are covered interdisciplinary and applied correctly. This will create safer, more resilient and thus sustainable societies for the benefit of communities, countries and regions.

Integrative Risk Management

Integrative risk management stands for risk reduction and disaster management, and at the same time means vulnerability reduction and resilience increase. A multi-measures approach along the risk cycle including prevention, intervention and recovery is required.
Preventive measures like land-use planning, or technical and biological measures serve to reduce vulnerabilities.
Organisational measures such as early warning, contingency planning, emergency preparedness and emergency exercises, ICT and leadership in crisis response management are essential for resilience increase. Resilience measures are important for people and communities to render social groups more adaptable to disasters. The recovery process has to focus on build-back measures reducing vulnerability



GRF Davos Slogan

From Thoughts to Action

„We are bridging the gap between science and practice in the search for sustainable solutions."

International Disaster and Risk Conference IDRC Davos – Call for Abstracts

IDRC Davos builds bridges between science, technology, policy and practice.

IDRC, the International Disaster and Risk Conferences and workshops, organized by the Global Risk Forum GRF Davos, are the ideal platform for assessment and dissemination activities, and in particular for networking activities. IDRC is the interface for experts, practitioners and institutions from science, technology, business, politics, and civil society to create transparency and encourage synergies to reduce and manage risks worldwide.

Walter J. Ammann

Dr Walter J. Ammann, Founder and President of the Global Risk Forum GRF Davos obtained his MSc in Civil Engineering and his PhD in structural dynamics and earthquake engineering both at ETH Zurich. He is an expert in integrative risk management and its applications to all kinds of natural hazards and technical risks, in particular by considering the entire risk cycle with prevention, preparedness, intervention and recovery. He has additional interest in risk financing tools, critical infrastructures, and resilience, for emergency management and communication tools with a focus on early warning, and crisis management, He is author and co-author of over 250 papers, books and scientific reports and is a member of various national and international professional associations and expert consulting groups like the UN-ISDR Scientific and Technical Advisory Group, and is Visiting Professor at HIT in Harbin, China and at Michigan State University, East Lansing, USA.

e-mail:
walter.ammann@grforum.org

IDRC attempts to find solutions to today's challenges by managing risks, reducing disasters and adapting to climate change. It helps build stronger ties with adequate public private partnership models among risk management communities and sectors, enabling a move towards a truly integrative way of thinking about risks and disasters.

The 5th Edition of the IDRC conferences, the IDRC Davos 2014 will be held from 24 - 28 August 2014 in Davos, Switzerland and will focus on "Integrative Risk Management - The role of science, technology & practice". The conference will yet again cover topics in disaster and risk management amongst others also in cyber security as a major emerging risk, but also about the role of Information and Communication technologies within Disaster and Risk Management. A major obstacle for the Disaster Risk Reduction Community is the management of knowledge and information and its provision. New database management structures to ease the access and the sharing of knowledge would benefit the international DRR community.

Call for Abstracts:

The call for abstracts for papers for the 5th IDRC Davos 2014 is open until 15. April 2014 and contributions are welcome. To submit abstracts, please follow: http://idrc.info/programme/call-for-abstracts

IDRC Davos Conference Topics:

- Disaster Preparedness, Response
- ICT in DRR
- Country Risk Management
- Environmental & Ecological Risks
- Thinking the Unthinkable
- Technical Risks
- Urban Risks /Megacities
- Societal / Political Risks
- Resilience & Vulnerability
- Health Impacts and Medical Response
- Economic Disasters
- Business Continuity
- Financial Tools for Risk Management
- Communication & Outreach in DRR
- Education, Research & Capacity Building

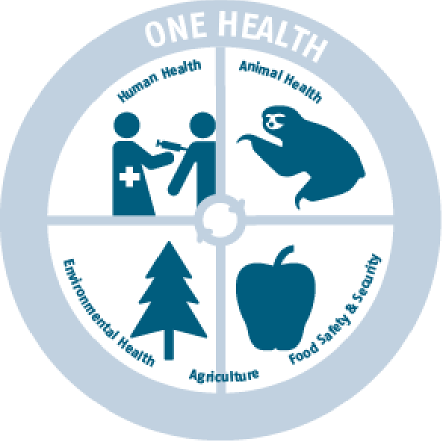
The outcomes of the IDRC Davos 2014 will be presented at the UN World Conference WCDRR in Sendai, Japan in March 2015 and aim to influence the post 2015 agenda such as the Post-2015 Framework for Disaster Risk Reduction (HFA2), the Sustainable Development Goals (SDGs) or the successor of the UNFCCC Kyoto Protocol.

GRF One Health Summit

For many years One Health was limited to an interdisciplinary collaboration in human and veterinary medicine with substantial added value in disease control. Most recently One Health has evolved to a broad and holistic paradigm which includes an environmental dimension, and also addresses economic and social challenges.

In 2012 GRF Davos launched an annual conference, the GRF One Health Summit to promote and foster such an integrative approach in managing health risks at the interface of human-, animal- and environmental health with a strong link to food safety and security. The upcoming GRF One Health Summit 2014 aims to strengthen an international research and education strategy for One Health.

GRF Davos promotes knowledge and best practices based on the One Health approach in to the
UN Sustainable Development Goals.



The GRF One Health Summits is an annual conference that promotes and fosters an integrative approach in managing health risks at the interface of human-, animal- and environmental health with a strong link to food safety and security and to agriculture. Striving for intensified collaboration among experts and practitioners from the different sectors and disciplines tangent to such a comprehensive health perspective, in particular the pharmaceutical and food industry as well as health insurers' engagement, will provide significant added value to identify cost-effective measures.

The **3rd GRF One Health Summit 2014 will be held from 05 - 08 October 2014 at the Davos** Congress Centre in Davos, Switzerland. The Summit will further develop and strengthen the One Health paradigm and its global movement. In particular this 3rd global gathering will focus on the added value of a global One Health approach and a stronger involvement of the private sector and policy.

The call for abstracts for papers for the 3rd GRF One Health Summit 2014 is open until 31 March 2014 and contributions are welcome. To submit abstracts, please follow: http://onehealth.grforum.org/programme/call-for-abstracts/?L=

Disaster Surgery Workshop

Disasters in recent years have revealed the crucial role of embedded medical teams providing disaster surgeries during the primary search and rescue operations, and the response phase as a whole. These operations are often additionally aggravated by extreme environmental conditions (cold, heat, high altitude, dust, heavy precipitation, etc.). Many of those people rescued after an earthquake or after an explosion as examples have life-threatening contrasting with a wider move in recent years to improve humanitarian intervention standards. GRF Davos addresses this issue during its annual Disaster Surgery Workshop Davos

The workshop is jointly organised by GRF Davos, AO Trauma and the AO Foundation. (http://www.grforum.org/risk-academy/disaster-surgery-workshop-2013/)

Research Projects

We place a particular focus on applied research and offer experience in Integrative Risk Management in various areas. Profound capacity for dissemination and knowledge transfer activities is also given. We facilitate the formation of efficient international project teams, link scientific institutions with practice and provide the necessary project management tools and support.

We are currently involved in two European research projects which cover different aspects of Risk Management.

The aim of the project **Public Empowerment Policies for Crisis Management PEP** is to investigate how the crisis response abilities of the public can be enhanced and what public empowerment policies are successful in realising this aim.

Public Empowerment Policies enhance crisis management as a coproduction of response organizations and citizens. The project will identify best practices in the community approach to crisis resilience and give directions for future research and implementation, including the use of social media and mobile services, to further citizen response. The input of the experts in the field of crisis management and communication is a key element in pursuing the goals of this project.

PEP offers authorities and other non-governmental organisations a comprehensive information package about key enablers for public empowerment in the form of guides concentrating on best practices, community approach and human technology enhancing citizen response.

The Project DITAC (Disaster Training Curriculum) proposes to develop a holistic Training Curriculum for first responders and strategic crisis managers dealing with international crises. The DITAC Curriculum will address the key challenges for the management of disaster incidents. It will develop a standardised strong, comprehensive and efficient EU-wide approach to crises and disasters to feature the added value by EU co-ordinated actions in the field of crisis response. The Curriculum will also improve the preparedness and availability of trained personnel by providing a common language, common objectives and common tools leading to better results in the protection and assistance of people confronted with large-scale crises.

The focus lies on international crisis management, but the benefit of a standardised training programme in crisis and disaster response can also be used to increase Europe's resilience in facing disasters and crises within the European Union.

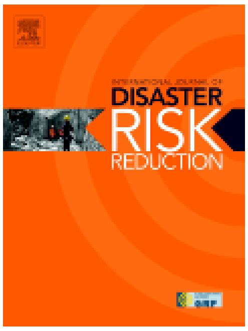
We additionally offer risk assessment and analysis for national, regional and local project; conduct research on regional climate change adaptation strategies and methodologies for the protection goal target settings in critical infrastructure protection.

GRF Davos e-Journals

GRF Davos publishes two online journals.

GRF Davos' **Planet@Risk** contributes to bridging the gaps between science, practice, and different sectors of academia. It fosters a multidisciplinary approach and presents the results of interdisciplinary and transdisciplinary research with a special emphasis on their application to practical problems. Information from data and reports which has been difficult or impossible to access, and whose quality has perhaps been hard to judge, can finally be put to use. Please submit your papers at: (http://www.planet-risk.org/).

The **International Journal of Disaster Risk Reduction (IJDRR)** is peer-reviewed journal that is published in close cooperation Elsevir. IJDRR publishes fundamental and applied research, critical reviews, policy papers and case studies focusing on multidisciplinary research aiming to reduce the impact of natural and technological disasters. IJDRR stimulates exchange of ideas and knowledge transfer on disaster research, mitigation, adaptation, prevention and risk reduction at all geographical scales: local, national and international.



http://www.journals.elsevier.com/international-journal-of-disaster-risk-reduction

Partnerships, Alliances and Initiatives

Meaningful partnerships are the foundation for success. GRF Davos takes the lead in partnering with international organizations and universities and in implementing innovative collaborations that enhance risk reduction and disaster management research and cooperation in combating climate change and desertification, land degradation and drought (DLDD).

If you would like to find out more about our UN Agreements, MoUs, and Alliances or GRF Davos in general please visit our website at: www.grforum.org or send an email to the GRF Davos secretariat: info@grforum.org

EAIS 2014: Emerging Aspects in Information Security

Special event of the international FedCSIS Multiconference is announced. ECN readers are invited to submit papers or participate in this event and the conference.

It would be difficult to point out a domain of social or economic life which is not dependent on the Information and Communication Technologies (ICT). ICT are broadly used to drive businesses, public, financial and health sectors, and industry. Individual citizens use ICT in their everyday lives.

ICT are used to produce, process, store and exchange a huge amount of information of crucial importance for the society and individuals. This information should be protected in the interests of its owners and consumers (stakeholders). Information security is identified with the protection of information integrity, availability and sometimes confidentiality.

ICT provide services, including transactions, for individuals, organizations and society. They should be available when needed and provided at the assumed quality level. ICT are a backbone of business, industry and society to secure the use of ICT. Other aspects are considered too, such as authenticity, reliability, accountability, nonrepudiation, privacy, anonymity, etc.

All these issues are encompassed within the security term. All factors breaching information assets or disturbing provided services should be identified and controlled. These activities are related to security management. The foundation of this management is risk management. Organizational and personal aspects play an important role in the security management.

Apart from organizational and procedural aspects, technical aspects are important. It is unquestionable that the applied technology should be modern and proven. This issue concerns hardware, software and composed systems. Communication aspects are important too – everything functions in a network today, with the omnipresent Internet. Reputable stakeholders as well as individuals entrust their information assets to ICT systems or use different IT services. They all require assurance from these technologies. It means that in the critical situation the users can rely on their ICT and no negative impacts will be exercised by the users. Assurance methods assume rigorous development, manufacturing and maintenance processes of ICT.

For the organizations strongly dependent on ICT, information security and business continuity are connected with each other. The integrated business continuity and information security management systems ensure the following:

- monitoring factors which cause crisis situations in institutions, i.e. when the continuity of business processes is disturbed or information security is breached by threats which exploit certain vulnerabilities,
- ability to reduce negative impact of business continuity disturbances or information security breaches (consequences),
- ability to recover business processes to their original form after different types of incidents.

The security issue concerns individuals, social groups, societies, and governments. In each country there are complex technical infrastructures. Some of these infrastructures have crucial significance to societies, like: energy, fuel, gas, water, food, telecommunications services, financial services, etc. They are classified as critical infrastructures (CIs). In today's world information and communication technologies support all critical infrastructures. What is more, societies develop distinguished infrastructures of strategic importance considered the Critical Information Infrastructures (CII).

Andrzej Białas
Institute of Innovative Technologies
EMAG, Katowice, Poland

Andrzej Białas: PhD, graduated from the Silesian University of Technology, Fac. of Automatic Control, Electronics and Computer Science in 1979. He has been in charge of numerous R&D projects and has carried out ICT trainings.

He is Associate Professor at the Institute of Innovative Technologies EMAG, leading R&D projects (national and EU FP6 CI^{2}RCO, FP7 ValueSec) on information security management, design and evaluation of IT security, business continuity, risk management.

He is also Associate Professor at the University of Economics in Katowice, providing lectures on software testing & quality, network information security management, cryptography and its applications.

Dr. Białas is an author of a vast collection of articles and other publications. He is a member of the IFIP WG11.1 Information Security Management group.

He is a Co-Chair of EAIS'2014.

e-mail: **a.bialas@emag.pl**

The broader the use of ICT is the stronger is dependence on it. All ICT issues (threats, vulnerabilities) can be transferred to business, public or social lives. For this reason, security issues are a matter of the utmost importance.

Security has a multidisciplinary character. Apart from technological, organizational and procedural issues, it takes into consideration human aspects (social, psychologycal, cultural, etc.).

Security cannot be bought as a miracle box taken down from the shelf. It is a time-related process. We should plan it, implement, check and maintain – security needs permanent care, i.e. the right management.

Complex technical systems, including ICT, are related to both security and safety. These issues are bound with each other – security can influence safety and vice versa.

Information security has many relations with other security domains. Methods, tools and techniques from one domain are checked in others. Researchers try to find synergy in this respect. Together they try to solve big multidisciplinary issues. This job requires knowledge exchange and common understanding. Knowledge engineering in the security domain is getting more and more important.

FedCSIS Multiconference

Security has emerged as an important scientific field of a multidisciplinary character. To review achievements, exchange experience and knowledge, and to set co-operation, a special event of the international FedCSIS Multiconference will be organized. It is called "Emerging Aspects in Information Security" (EAIS'2014).

FedCSIS – Federated Conference on Computer Science and Information Systems will be held in Warsaw, Poland, 7 – 10 September, 2014. This year's FedCSIS Multiconference features 28 different events: conferences, symposia, workshops, special sessions, each running over any span of time within the conference dates (from half-day to three days). The FedCSIS events bring together researchers, practitioners, and academia to present and discuss ideas, challenges and potential solutions on established or emerging topics related to research and practice in computer science and information systems. The proceedings of the FedCSIS conference have been indexed in the Thomson Reuters Web of Science since 2012.

Detailed information about FedCSIS multiconference:
https://fedcsis.org/

EAIS'2014 Event

EAIS'2014 is one of the events focused on different aspects of security.

The Emerging Aspects in Information Security (EAIS'2014) workshop deals with the diversity of the information security developments and deployments in order to highlight the most recent challenges and report the most recent researches. The objective of the workshop is to explore all information security technical aspects. Yet, it covers some emerging topics too, such as social and organizational security research directions. EAIS 2014 is to attract researchers and practitioners from academia and industry. It will provide an international discussion forum where experiences and ideas will be shared about emerging aspects in information security in different application domains. This way it will be possible to take up new research directions and respond to modern research challenges.

The objectives of the EAIS'2014 workshop can be summarized as follows:

- To review and conclude researches in information security and other security domains, focused on the protection of different kinds of assets and processes, and to identify approaches that may be useful in the application domains of information security.
- To find synergy between different approaches, allowing to elaborate integrated security solutions, e.g. integrate different risk-based management systems.
- To exchange security-related knowledge and experience between experts to improve existing methods and tools and adopt them to new application areas
- To present latest security challenges, especially with respect to EC Horizon 2020.

Topics of interest include but are not limited to:

- Biometric technologies
- Human factor in security
- Cryptography and cryptanalysis
- Critical infrastructure protection
- Hardware-oriented information security
- Social theories in information security
- Organization-related information security
- Pedagogical approaches for information security
- Individual identification and privacy protection
- Information security and business continuity management
- Decision support systems for information security
- Digital right management and data protection
- Cyber and physical security infrastructures
- Risk assessment and risk management in different application domains
- Tools supporting security management and development
- Emerging technologies and applications
- Digital forensics and crime science
- Misuse and intrusion detection
- Security knowledge management
- Data hide and watermarking
- Cloud and big data security
- Computer network security
- Security and safety
- Assurance methods
- Security statistics

Detailed information about EAIS'2014:
https://fedcsis.org/2014/eais

I would like to encourage the ECN readers to submit papers to this event and to participate in the conference.

CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security

Bringing together researchers and professionals from academia, industry and governmental organizations working in the field of the security of critical infrastructure systems. Announcing the **1st CIPRNet Young Critis Award** CYCA.

On behalf of the Steering Committee and the Local Organizing Committee we are excited to invite you to submit papers and attend the CRITIS 2014 conference. CRITIS 2014 will be held in October 2014 in Limassol, Cyprus and it continues a well-established tradition of successful annual conferences. It aims at bringing together researchers and professionals from academia, industry and governmenttal organizations working in the field of the security of critical infrastructure systems.

Modern society relies on the availability and smooth operation of a variety of complex engineering systems. These systems are termed Critical Infrastructure Systems (CIS). Some of the most prominent examples of critical infrastructure systems are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, and oil / natural gas pipelines.

Our everyday life and well-being depend heavily on the reliable operation and efficient management of these critical infrastructures. The citizens expect that critical infrastructure systems will always be available and that, at the same time, they will be managed efficiently (i.e., they will have a low cost). Experience has shown that this is most often true. Nevertheless, critical infrastructure systems fail occasionally. Their failure may be due to natural disasters (e.g., earthquakes and floods), accidental failures (e.g., equipment failures, software bugs, and human errors), or malicious attacks (either direct or remote). When critical infrastructures fail, the consequences are tremendous. These consequences may be classified into societal, health, and economic.

Conference web site:
http://www.critis2014.org

Conference dates
13-15 October 2014

The venue of the CRITIS 2014 conference will be the magnificent Grand Resort Hotel, in Limassol, Cyprus. The hotel is set in over 20,000 square meters of beautifully landscaped gardens with exotic trees and subtropical plants, which extend right down to the seashore.

Elias Kyriakides

is an Assistant Professor at the Dept of Electrical and Computer Engineering and the Associate Director for Research at the KIOS Research Center for Intelligent Systems and Networks, University of Cyprus

Left: Marios Polycarpou,
mpolycar@ucy.ac.cy
Director KIOS Research Center (RC)

Right: Demetrios Eliades
@: eliades.demetrios@ucy.ac.cy
Research fellow at the KIOS (RC)

Both: University of Cyprus

1. Conference Topics

- Infrastructure resilience and survivability
- Security and protection of complex cyber-physical systems
- Self-healing, self-protection, and self-management architectures
- Cyber security in critical infrastructure systems
- Critical (information-based) infrastructures exercises and contingency plans
- Advanced forensic methodologies for critical information infrastructures
- Economics, investments and incentives of critical infrastructure protection
- Infrastructure dependencies: modeling, simulation, analysis and validation
- Critical infrastructure network and organizational vulnerability analysis

Important dates

Deadline for invited session proposals: March 26, 2014

Deadline for submission of papers: April 2, 2014

Notification to authors: June 1, 2014

Camera-ready papers: June 25, 2014

- Critical infrastructure threat and attack modeling
- Public-private partnership for critical infrastructure resilience
- Critical infrastructure protection polices at national and cross-border levels
- Fault diagnosis for critical infrastructures
- Fault tolerant control for critical infrastructures
- Security and protection of smart buildings
- Detection and management of incidents/attacks on critical infrastructures
- Preparedness, prevention, mitigation and planning

2. Call for Special Sessions

Proposals for organizing special sessions during CRITIS 2014 are cordially invited. Special sessions will comprise 4-6 papers presenting a unifying theme of interest to the conference attendees from a diversity of viewpoints. Special Session proposals from active research projects are particularly welcomed. Proposals for special sessions must include the title of the session, a paragraph describing the theme of the session, names and affiliation of the contributing authors, and tentative titles of the contributions.

The component papers must be submitted separately, by the respective authors, as per the regular submission procedure. Each paper in a proposed invited session will be individually reviewed.

Any rejected papers submitted as part of an invited session will be removed and appropriate contributed papers may be substituted, at the discretion of the Program Committee. Likewise, selected papers from rejected invited sessions may be placed into other sessions. Further exchanges may be made to ensure coherence of the sessions, at the discretion of the Program Committee.

Organisers and Contact Information

General Co-Chairs:
- Marios Polycarpou, University of Cyprus
- Elias Kyriakides University of Cyprus

Program Chair
- Christos Panayiotou, University of Cyprus

Program Co-Chairs
- Vicenç Puig, Universitat Politècnica de Catalunya
- Erich Rome, Fraunhofer Institute for Intelligent Analysis and Information Systems

Publications Chair
- Georgios Ellinas, University of Cyprus

Publicity Co-Chairs
- Demetrios Eliades, University of Cyprus
- Cristina Alcaraz, University of Malaga

For more information
Elias Kyriakides, elias@ucy.ac.cy

Conference Webpage:
www.critis2014.org

3. CIPRNet Young CRITIS Award (CYCA)

An award for outstanding research in Critical Infrastructure Security (CRITIS) and protection sponsored by EU FP7 NoE CIPRNet will honour winners at CRITIS 2014.

CIPRNet Young Critis Award 2014: Are you the Winner?

Who should apply?

Every young engineer / scientist interested in CRITIS and in CRITIS community and is less than 32 year old by May 1st, 2014 is invited to apply. We explicitly invite junior experts and researchers form universities, research organisations and industry to apply.

In general, a mature piece of work is expected such as a PhD thesis in final or near final status, as well as outstanding works from young industry or research organisations researchers.

3.1 General information

Junior experts less than 32 years old may apply for the CIPRNet Young CRITIS Award CYCA. Three CYCA applicants per year will be selected for presenting their work at CRITIS conference (in 2014 in Cyprus) in the CYCA award session.

The ranking of up to three winners (depending on the number of applications and the paper quality) will be done at the conference itself, and the awards will be presented to the winners at a closing ceremony.

Limited travel funding opportunities are possible under conditions (please contact the organiser for details and conditions).

> CIPRNet Young CRITIS Award 2014
>
> There is never a better point in time to apply than right now!

3.2 Evaluation process

- The CYCA papers will be rated by at least three experts from the CYCA award committee according to the same evaluation criteria as the papers proposed in the conference.
- Up to five highest rated papers will be reviewed by the experts. They will select who will qualify for the CYCA award slot, but limited to three papers maximum.
  Note: If you get a positive evaluation, but you are not selected for CYCA award, your paper will be presented at the conference in the regular slots as all other papers. Therefore, you can only win by applying for CYCA.
- The total available award money is around 2000 Euro.

The ranking of the first three papers will be done at the conference, as follows:

a) All in the audience vote on the ranking of the presentations ➔ 40% weight
b) CYCA award committee (written paper) rating ➔ 40% weight
c) CYCA award committee (oral presentation and interactivity) rating: ➔ 20%
d) The CYCA award committee will have a meeting after the session, where the final ranking will be made.

3.3 Evaluation Committee

The Evaluation Committee consists of the Award Committee and Experts from the CRITIS Steering Committee according to the needs and the number of submitted papers

3.4 How to apply?

CYCA papers are normally submitted as other papers through the Easychair conference system of CRITIS.

Additionally, a CIPRNet Young CRITIS Award questionnaire should be submitted (available from April 15, 2004 on the website). This questionnaire has the following purpose:

- Contact details
- Info on birth data of all the authors
- To provide a statement of honesty: You declare that all citations are declared correctly (anti plagiarism)

The questionnaire and the CV must be sent to the moderator of CYCA: Prof. Dr. Bernhard M. Hämmerli

Please send as soon as possible, but no later than June 15, 2014

e-mail: bmhaemmerli@acris.ch
usually your delivery is preferred with cc to: Bernhard.Haemmerli@HSLU.ch

post mail: Bodenhofstrasse 29, CH-6005 Lucerne, Switzerland

If you do not get a confirmation of receipt, please try to resend or call on +41 79 541 7787 in order to exclude transfer problems.

3.5 Award Committee

CIPRNet Young CRITIS Award

Moderation

- Bernhard Hämmerli University of Applied Sciences Lucerne School of Engineering and Architecture
- Javier Lopez, University of Malaga

Committee

- Jose Marti, University of British Columbia
- Mohamed Eid, French Commissariat of Atomic Energy & Alternative Energies
- Elias Kyriakides University of Cyprus
- Roberto Setola, University Campus Bio-Medico of Rome

See also:
http://cyca.critis2014.org

Links

ECN home page	http://www.ciprnet.eu
ECN registration page	free registration on www.ciip-newsletter.org

CIPRNet Young CRITIS Award: Unique opportunity to jump into a CRITIS Career!
Award for talents below 32 years http://cyca.critis2014.org

Forthcoming conferences and workshops

Master Class ModSim & Analysis	www.ciprnet.eu/training.html : A CIPRNet community support effort		
ESReDA	http://www.esreda.org/Events/tabid/1489/Default.aspx	29-30.05.14	Torino, Italy
IDRC 2014	http://idrc.info/programme/call-for-abstracts Call for abstracts open till 15.4.2014	24-28.08.14	Davos, Switzerland
EAIS 2014	https://fedcsis.org/2014/eais Call for papers open till 11.4.2014	7-10.09. 14	Warsaw, Poland,
CRITIS 2014	www.critis2014.org Call for papers open till 26.4.2014	13-15.10.14	Limassol Cyprus
CIPRNet Young Critis Award	see www.critis2014.org open till 26.4. 2014		

Exhibitions

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

Associations

European Safety, Reliability & Data Association	www.esreda.org
Global Risk Forum Davos	www.grforum.org
FedCSIS – Federated Conference on Computer…	https://fedcsis.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu
FP7 ValueSec	www.valuesec.eu
FP 7 PoSecCo	http://www.posecco.eu/?id=354
ERNCIP	http://ipsc.jrc.ec.europa.eu/index.php/ERNCIP/688/0/

Interesting Downloads

Critis'12 Conf. Proceedings:	www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8
Critis'13 Conf. Proceedings:	http://link.springer.com/book/10.1007/978-3-319-03964-0

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"
ENISA www.enisa.europa.eu/activities/Resilience-and-CIIP

Dutch Intersectional Study (in Dutch): http://www.wodc.nl/onderzoeksdatabase/vertaling-afhankelijkheden-van-zweedse-methode-naar-nederlandse-situatie.aspx?cp=44&cs=6796#publicatiegegevens

Websites of Contributors

Austrian Security Policy Centre	www.bmi.gv.at

CIPRNet Young Critis Award 14: Are you the Winner?

Less than 32 years by May 1, 2014?

Attractive prizes,
A lot fun to join!

Please see details on:

http://cyca.critis2014.org

All participants get qualified coaching by European leading experts on C(I)IP

Don't miss this chance!

CRITIS 2014

9th International Conference on
Critical Information Infrastructures Security
October 13-15, 2014, Limassol, Cyprus
www.critis2014.org