



FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

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

D9.7 At Least seven CIPRNet Lectures

Due date of deliverable: 28/02/2017

Actual submission date: 02/02/2017

Revision: Version 1

Università Campus Bio-Medico di Roma (UCBM)

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

Author(s)	Roberto Setola (UCBM) Maria Carla De Maggio (UCBM) Clio Di Marcello (UCBM)
Contributor(s)	

Security Assessment	E. Rome (Fraunhofer)
Approval Date	02/02/2017
Remarks	No security issues found

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

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

TABLE OF CONTENTS

1	INTRODUCTION	4
2	CIPRNET LECTURES.....	6
2.1	CIPRNet lectures – Statistics.....	6
2.2	List of the lectures.....	11
3	CIPRNET ONLINE COURSE.....	25
3.1	Module A	27
3.2	Module B	28
3.3	Module C	29
3.4	Module D	30
4	REFERENCES	30

LIST OF ACRONYMS

Acronym	Explanation
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
DoW	Description of Work
DSS	Decision Support System
EISAC	European Infrastructures Simulation and Analysis Centre
FP	Framework Programme
I2SIM	Infrastructure Interdependencies Simulator
M&S	Modelling and Simulation
MS&A	Modelling, Simulation and Analysis
OpenMI	Open Modelling Interface
V&V	Verification and Validation

1 Introduction

Internal and external training activities are mandatory cornerstones in CIPRNet project aiming at building the European’s capabilities necessary for the realisation of European Infrastructures Simulation & Analysis Centre (EISAC). CIPRNet will supply, amongst others, specific training activities covering basic and advanced knowledge in Critical Infrastructure MS&A (Modelling, Simulation and Analysis) for a broad audience (including, but not limited to, local administrations, utilities personnel, emergency operators and managers, security & safety operators and managers, CIP researchers, CIP policy makers, etc.). Among the training activities there are “Master Classes” and “Lectures”. The main difference between the two types of activity is that while the Master Class is structured as a course with the aim to provide a coherent and complete set of knowledge about MS&A to the audience, the Lecture is more oriented to support information sharing on specific topics and to stimulate dissemination and cooperation. Consequently, while Master Classes are very structured and managed by the whole consortium, lectures are locally arranged by each partner. Moreover, the lecturers have been both members of the consortium (in order to share knowledge with the other partners and to promote the project outside the consortium) and experts coming from other organisations (in order to stimulate cooperation). Lectures have been arranged both inside the consortium organisations and in other places with the aim to provide large visibility to the events. For this reasons some of the lectures have been video-recorded and/or broadcasted via streaming.

Moreover, CIPRNet is active to prepare the EISAC (European Infrastructure Simulation and Analysis Centre) improving the competence and knowledge of the European CIP Expert community. Lectures hosted or performed by CIPRNet partners are thought for information exchange in this framework. Lectures cover all the main topics involved in the CIPRNet project, such as interdependency modelling, crisis management, DMCI, protection and resilience of critical infrastructures, MS&A and much more.

In [3], CIPRNet Lectures achievements have been summarised, according to the performance indicators listed in the CIPRNet DoW [1].

Table 1: CIPRNet Lectures achievements according to performance indicators.

CRITERION	ACHIEVEMENT	REQUESTED
Total number of lectures	41 -> 10.25 lectures per year	5 lectures per year
Total number of attendees	1312 (excluding Lecture 41)	No less than 400 attendees
Average number of attendees	32.8 (excluding Lecture 41)	At least an average of 20 attendees for lectures
Partners involved in lectures	All	Each partner should arrange at least one CIPRNet Lecture
Lectures from external experts	31.7% (14 lectures)	At least 25% from outside consortium

The present deliverable describes in some details the lectures in terms of events scheduling, statistics on lecturers and attendees (reported in Section 2).

Last, in Section 3 the MOOC platform developed by UCBM is described. Following a recommendation of CIPRNet's reviewers, CIPRNet implemented an e-learning platform for Massive Open Online Courses (MOOC) on CIPRNet's training material. MOOC is a modern means for increasing the impact of a project's training activities by reaching a larger and broader audience.

2 CIPRNet Lectures

The original purpose of the CIPRNet consortium was to hold “at least seven CIPRNet lectures” but as it turned out, this way of training has proved to be very successful and therefore in the period going from September 2013 to February 2017, 41 lectures have been held in most of the European Countries and by most of the members of the consortium.

2.1 CIPRNet lectures – Statistics

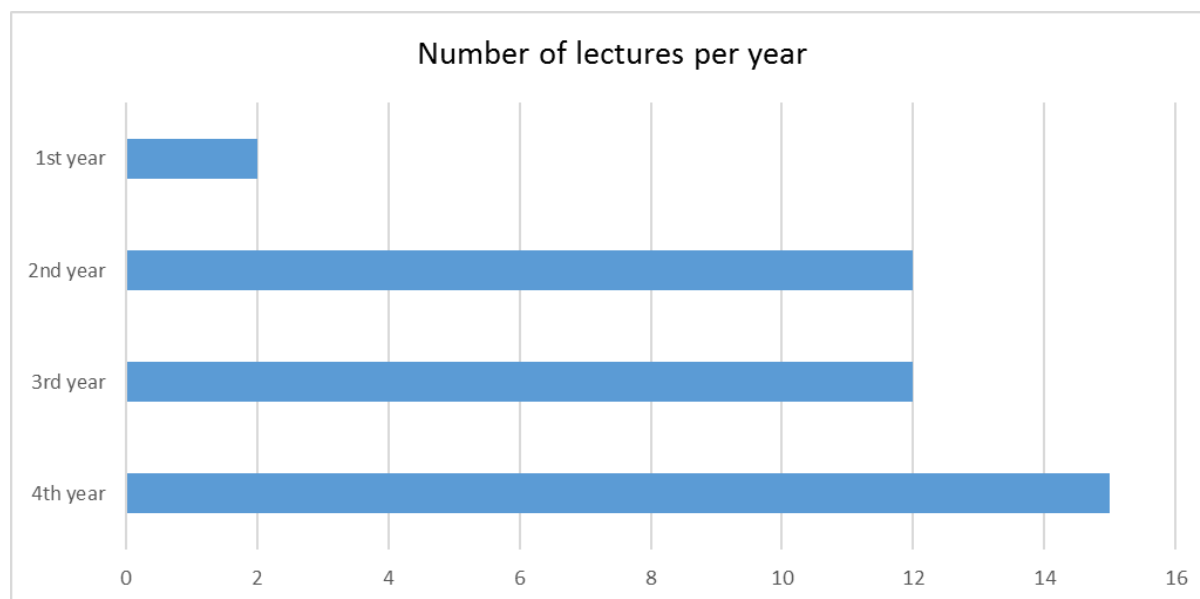


Figure 1: Number of lectures per project year.

As you can see from the graph in Figure 1, the number of the lectures grew over the years. Indeed, during the first year there have only been 2 lectures (due to the fact that this joint activity started in the second half of the first year of project, and to the “physiological” activity start up), followed by 12 lectures in both second and third years, and 15 in the fourth year. It is to mention that the lectures, as showed in Figure 2, have been hosted, with different percentages, by all the countries of the consortium, but also by countries that have not a “representative” in the consortium (Spain, United Kingdom, Lithuania). This demonstrates the interest in the project and how the efficiency of the promotion of project activities by the consortium expanded the cooperation area.

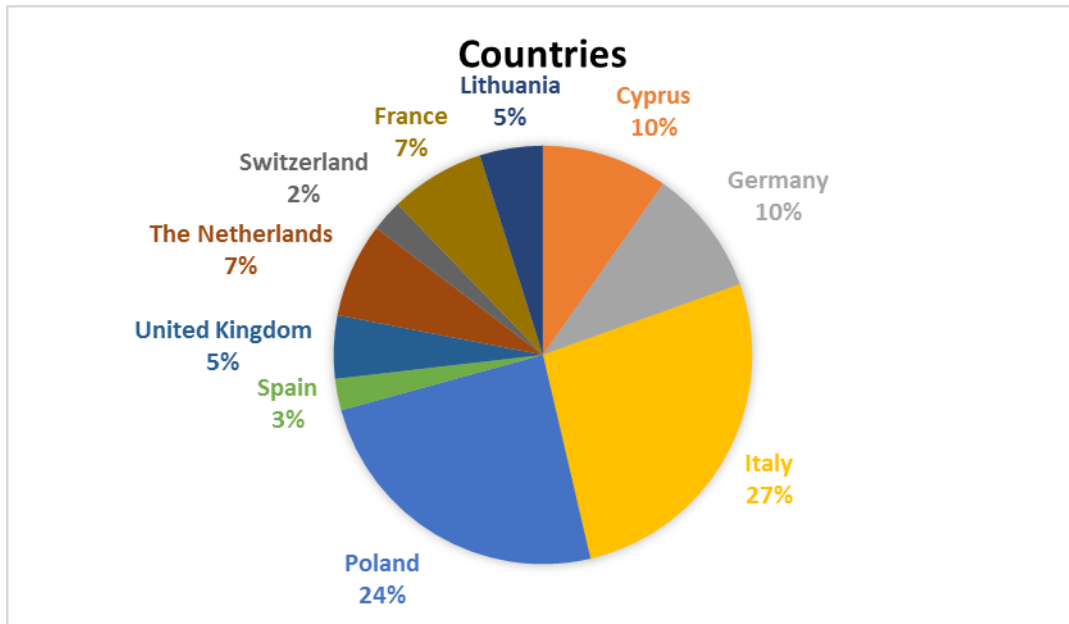


Figure 2: Lectures' host countries.

As statistics shows (Figure 4), most of the lectures have been held by internal speakers but there has been a wide contribution from external experts. Performance indicators listed in the project DoW requested that all the partners of the consortium have to be involved in the organisation of at least one lecture. This target has been successfully reached, and Figure 3 shows as a great part of lectures has been organised by the academic partners UCBM (WP leader) and UTP, followed by the coordinator Fraunhofer.

The same can be stated about the performance indicator dealing with the external lecturers: in fact, as shown in Figure 4 external experts held 32% of the lectures (against a minimum threshold of 25%).

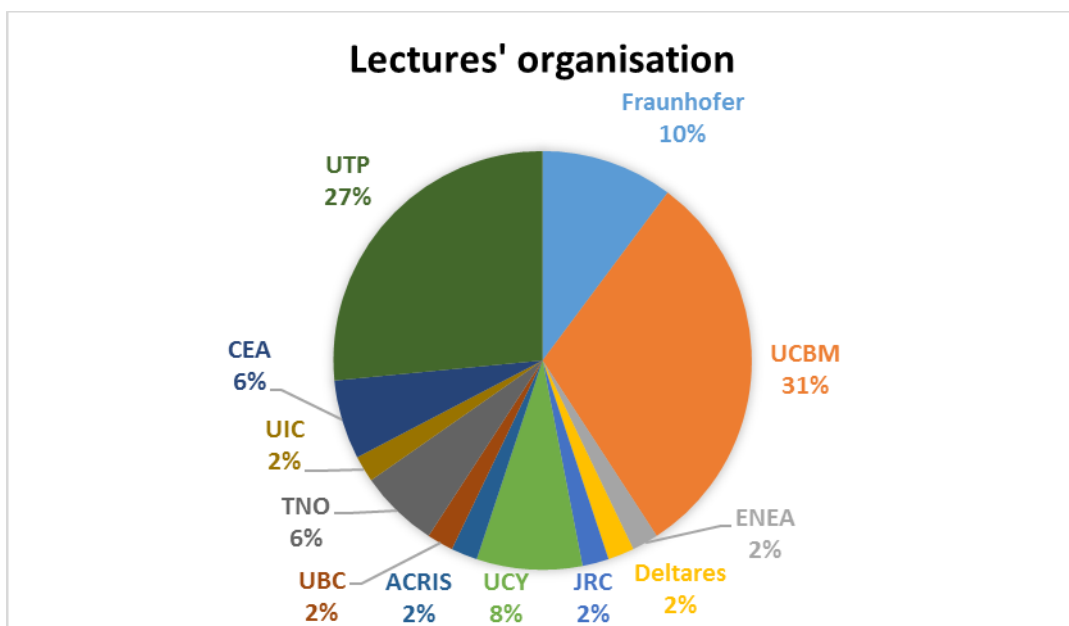


Figure 3: Lectures' organisers

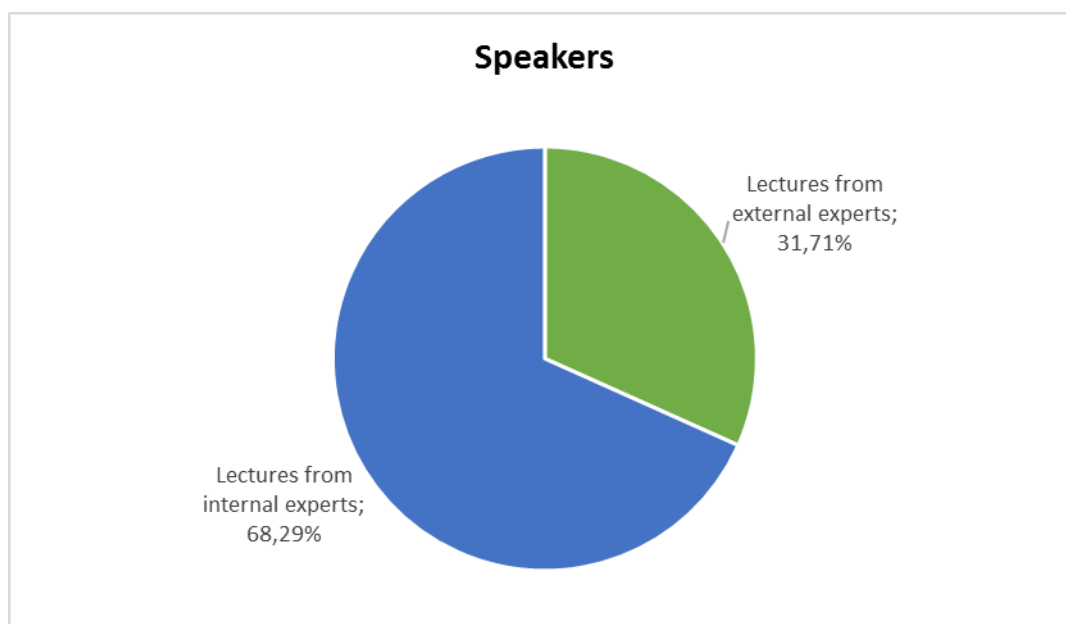


Figure 4: Percentage of internal and external speakers.

As suggested by CIPRNet reviewers during the first project periodic review, in order to foster the involvement of a higher amount and different «types» of interested people, the CIPRNet consortium decided to organise different forms of lectures, e.g. events with the participation of more than one speaker, coming from different type of organizations - research, industry, public institutions, etc., and events broadcasted via web streaming.

Specifically, the lectures held by more than one speaker are:

- Lecture 15: Modelling IT networks with Riverbed Modeller
- Lecture 18: Selected aspects of Critical Infrastructures cybersecurity
- Lecture 19: Railway Infrastructure Security
- Lecture 25: Cyber-physical security solutions for critical infrastructure protection
- Lecture 29: CIPRNet OpenMI-Webinar

A relevant aspect of this kind of lectures were the remarkable discussions emerged among a variety of experts who provided their different points of view on the topics and who stimulated the attendance to consider different perspectives.

About lecture 29 it must be mentioned that the OpenMI Webinar was recorded and made available on the internet.

The lectures who gave the opportunity to be attended via web are:

- Lecture 8: Power grids, smart grids and complex networks
- Lecture 10: Dynamic Functional Modelling of vulnerability and interdependencies of CIs
- Lecture 13: A unified approach for 2D and 3D coverage problems in omnidirectional and directional sensor networks
- Lecture 14: Optimal device placement in wireless sensor networks
- Lecture 16: Optimal Security Investments for Critical Infrastructure Systems
- Lecture 29: CIPRNet OpenMI-Webinar

The latter has been given only as a webinar. The previous five lectures, given both in person and via web streaming, showed that only a few people (with respect to the total) attended via web, and the possibility to attend in person was more encouraging to participate.

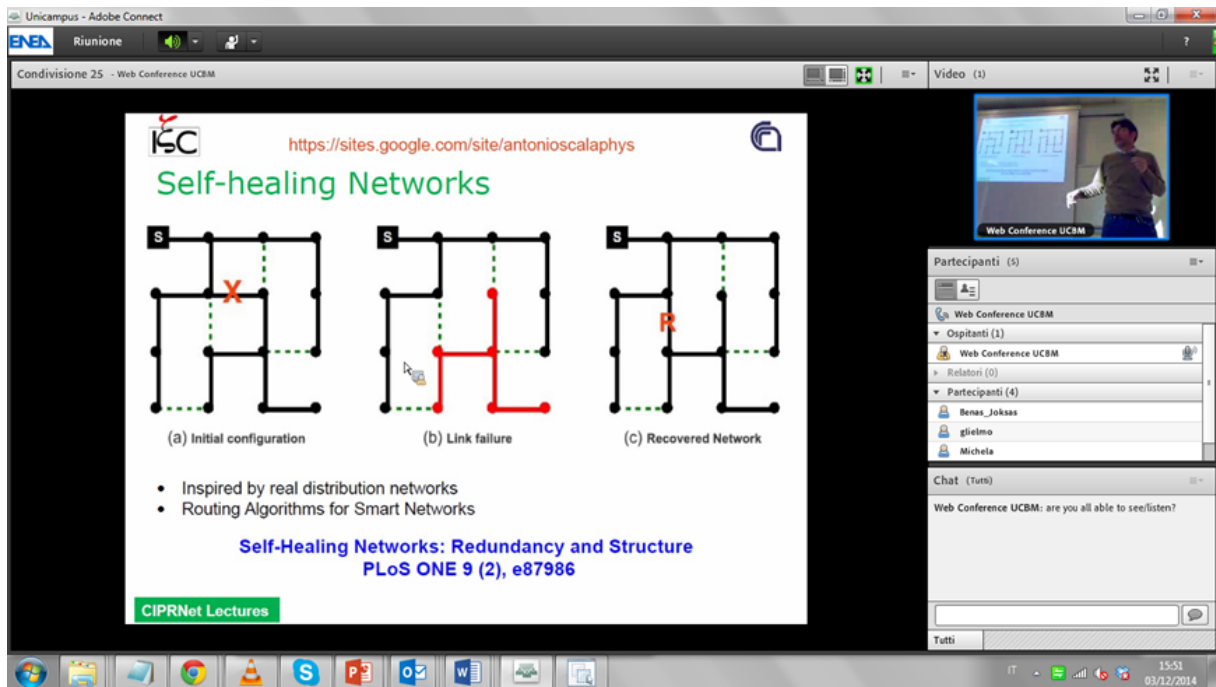


Figure 5: CIPRNet Lecture 8 web streaming.

Figure 6 shows the number of attendees per lectures, including web attendance. Please note that statistics of Figure 6 and Figure 7 does not include the attendees of Lecture 41, because it has been held after the editorial deadline of this deliverable.

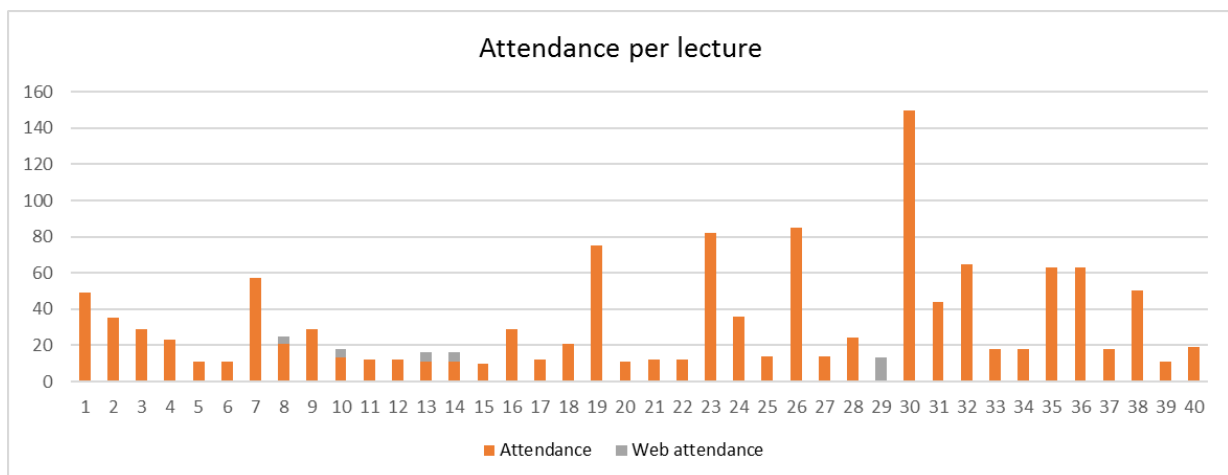


Figure 6: Attendance per lecture

Finally, it has to be stressed, as pointed out by Figure 7, that the average of the attendees in the first year has been unusually much higher compared to the other three years, indicating that the topic of this new project was considered very appealing. In the following years the number of the attendees has, however, been growing over the years.

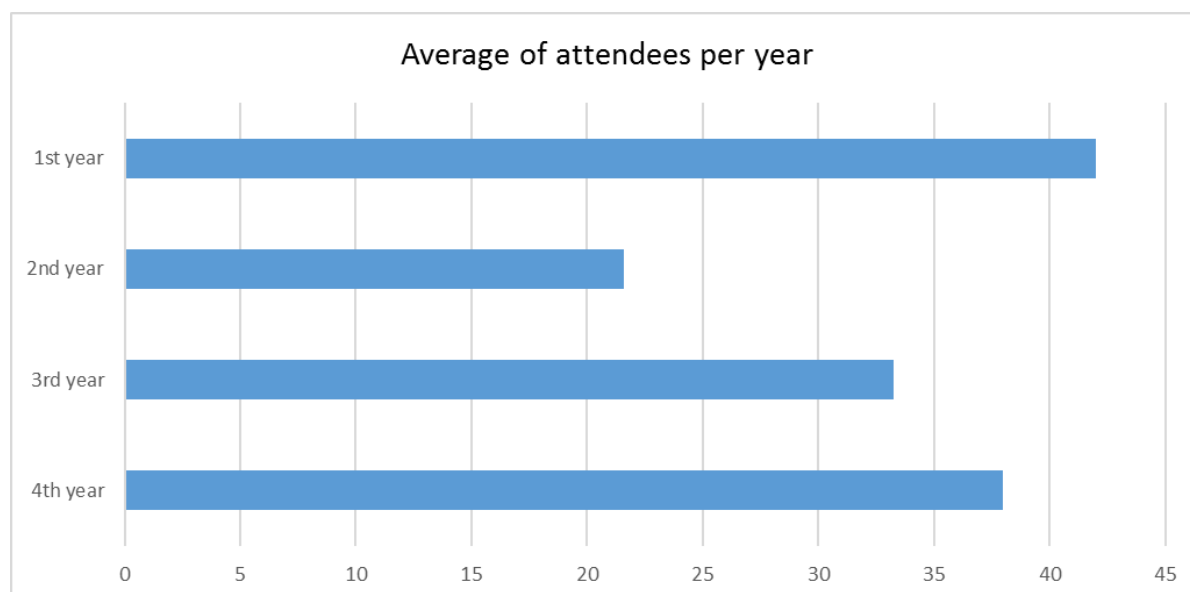


Figure 7: Average of attendees per year

A simple procedure was created to organize, control and monitor CIPRNet Lectures. The lecture promoter had to inform the WP9 (Training Activities) leader about the lecturer(s), subject and logistics of the lecture. These data were used to disseminate the event via the CIPRNet project website. During the lecture, the promoter collected the list of attendees, some pictures and the material used by the lecturers (if internal lecturers, the presentations were assessed by the project Security Advisory Group). All these data have been collected by UCBM to monitor the lectures activities.

Following the project reviewers' suggestion of enlarging the training events' recipients, also a MOOC platform has been designed and delivered, as described in Section 3.

In Section 2.2 all the lectures are listed in chronological order.

2.2 List of the lectures

More details at <https://www.ciprnet.eu/lectures.html>.

2.2.1 Lecture 1: Interdependency Modelling

by Roberto Setola (UCBM) at University of Cyprus, 20th September 2013.

In the last years we observed a significant development of scientific, technological and public initiatives about Critical Infrastructures (CI) and their protection. A cornerstone concept in many of these initiatives is the one of ‘Interdependency’, assumed as one of the most relevant and innovative elements to be considered in order to define effective management and protection plans. The talk illustrates such phenomena, their causes and some modelling approaches in the line of developed solutions able to improve resilience and robustness of CI.

Number of attendees: 49

2.2.2 Lecture 2: Modellierung, Simulation und Analyse für den Schutz Kritischer Infrastrukturen

English title: Modelling, Simulation and Analysis for Critical Infrastructure Protection

by Erich Rome (Fraunhofer) at BAKS, Berlin, 24th September 2013.

Event: Seminar Staatliche Sicherheitsvorsorge – Audience: Public stakeholders

The lecture covered basic topics like general approaches to modelling, simulation and analysis (MS&A) for Critical Infrastructure Protection (CIP). It tried to give answers to fundamental questions like: What types of data are required for this task? What can computer-based MS&A do and what not? What would be the potential benefit of this type of simulation and analysis for civil protection and for crisis and emergency management? What is the state of the art in CIP research and its transfer into application? How could sustained support from the CIP research communities be realised?

Number of attendees: 35

2.2.3 Lecture 3: Recent advances in CIP research and policy support to EPCIP

by Georgios Giannopoulos (JRC) at University Campus Bio-Medico of Rome, 18th March 2014.

Dr. Giannopoulos presented a comprehensive overview of the recent advances in CIP policy at EU level and the impact on research development in the domain of Critical Infrastructures. In addition, he presented the challenges of translating policy needs to scientific research and how this has taken place in JRC. Finally, he provided a thorough presentation at technical level on the tools and methodologies that have been developed or are under development in JRC in order to improve the security of Critical Infrastructures against all hazards. The seminar also included interdependencies assessment tools, fault detection techniques and in general tools that help towards improving situational awareness of critical infrastructures.

Number of attendees: 29

2.2.4 Lecture 4: Crisis management

by Rafal Renk (UTP) at Gniezno, University of Adam Mickiewicz, 9th April 2014.

This CIPRNet training lecture was a part of the broader course on crisis management at special MBA studies. The course covers the following aspects: introduction to crisis management (functions, phases), crisis management in Poland, analysis of selected cases (e.g. train accident near Szczecociny, Sandy hurricane), critical infrastructure (including EU projects results), selected technical aspects (like communication, GIS systems, IT solutions), social media in crisis management and simulation and modelling. The CIPRNet training lecture contained information about critical infrastructures protection and resilience, cyber protection of CI, CIPRNet project and CIPRNet DSS services.

Number of attendees: 23

2.2.5 Lecture 5: Modelling interdependency in tightly coupled critical infrastructures

by Gabriele Oliva (UCBM) at University of Cyprus, 7th May 2014.

The protection of the national infrastructures (e.g. energy grids, transportation networks, telecommunications systems, etc.), is one of the main issues for national and international security. Dr. Gabriele Oliva gave an overview of the techniques used to model interdependency and to assess the more vulnerable and more influential ones in the protection of critical infrastructures contest. Furthermore, it was shown how to cope with the lack of adequate quantitative data by resorting to a codification of the experience of stakeholders and infrastructure experts by means of the fuzzy formalism.

Number of attendees: 11

2.2.6 Lecture 6: Modelling complex systems

by Roberto Setola (UCBM) at Information Engineering School of the University of Malaga, Malaga (Spain), 18th June 2014.

A cornerstone concept in many initiatives, such as scientific, technological and public initiatives about critical infrastructures (CI), is the one of ‘interdependency’, assumed as one of the most relevant and innovative elements to be considered in order to define effective management and protection plans. This talk illustrates such phenomena, its causes and some modelling approaches in the line towards developing solutions able to improve the resilience and robustness of CI.

Number of attendees: 11

2.2.7 Lecture 7: System of Systems Simulation in a Cooperative Multinational Environment

by José Martí (UBC) at CRITIS 2014, Limassol, Cyprus, 13th October 2014.

Interdependencies among Critical Infrastructures play a major role in understanding the complex physical, economic, and social systems that constitute the fabric of modern societies. Aristotle’s principle of causality is not enough to understand the karmic effects of actions and consequences. Feedback loops are needed to complete the cycle of interactions. The CIPRNet effort and other efforts seek to integrate multiple Critical Infrastructures (electricity, water, communications, and others) from the perspective of understanding their interactions and coordinating their responses across jurisdictions and national borders. This presentation will

address the development of a system of systems simulator capable of linking multiple agents in a cooperative environment to best optimise common objectives. The lecture is structured in the following four parts; a) World Models, b) MATE and i2Sim System of Systems Simulation, c) Federated Simulation (DR-NEP & DIESIS) and d) Sample Scenarios.

Number of attendees: 57

2.2.8 Lecture 8: Power grids, smart grids and complex networks

by Antonio Scala, at University Campus Bio-Medico of Rome, 3rd December 2014.

The objective of the lecture is to present some possible Complex Networks approaches to study and understand Power Grids and to improve them into Smart Grids. We first sketch the general properties of the Electric System with an attention to the effects of Distributed Generation. We then analyse the effects of renewable power sources on Voltage Controllability. Afterwards, we study the impact of electric line overloads on the nature of Blackouts. Finally, we discuss the possibility of implementing Self Healing capabilities into Power Grids through the use of Routing Protocols.

(web streaming available)

Number of attendees: 21

2.2.9 Lecture 9: Crisis management

by Rafal Renk (UTP), at Gniezno, University of Adam Mickiewicz, 15th January 2015.

This CIPRNet training lecture is a part of the broader course on crisis management at special MBA studies. The course covers the following aspects: introduction to crisis management (functions, phases), crisis management in Poland, analysis of selected cases, critical infrastructure (including EU projects results), selected technical aspects (like communication, GIS systems, IT solutions), social media in crisis management and simulation and modelling.

The CIPRNet training lecture also contains information about critical infrastructures protection and resilience, cyber protection of CI, CIPRNet project and CIPRNet DSS services.

Number of attendees: 29

2.2.10 Lecture 10: Dynamic Functional Modelling of vulnerability and interdependencies of Critical Infrastructures (DMCI)

by Paolo Trucco, at ENEA, Rome, 20th January 2015.

DMCI proved to be suitable for the analysis of heterogeneous infrastructure systems, dynamic dependencies between energy and transport services. A web-based software tool has been developed to implement DMCI, where both the instantiation of CI nodes and the results of simulations are graphically supported by a GIS map. According to Ouyang's literature review on different approaches to modelling and simulation of interdependent critical infrastructure systems, DMCI belongs to the group of network based approaches, those with the best capabilities to support resilience analysis of interdependent CI. DMCI has been used to model the regional infrastructure system and support preparedness activities under the Lombardy Government's Programme on CIP.

(web streaming available)

Number of attendees: 13

2.2.11 Lecture 11: Methods for increasing protection and resilience of critical infrastructures

Polish title: Działania w zakresie ochrony i zwiększenia niezawodności infrastruktury krytycznej

by Michal Choras (UTP), at UTP, Bydgoszcz, 22nd January 2015.

This CIPRNet training lecture will contain information about threats to critical infrastructures and methods for CI protection and resilience. Among the presented methods, the CIPRNet solutions such as modelling and simulation, decision support services, what-if analysis etc. will be described.

Number of attendees: 12

2.2.12 Lecture 12: Selected aspects of cybersecurity of critical infrastructures

Polish title: Aspekty bezpieczeństwa cybernetycznego infrastruktur krytycznych

by Rafal Kozik (UTP), at UTP, Bydgoszcz, 22nd January, 2015.

Nowadays, cyber threats are considered as a serious danger to critical infrastructures. Therefore, this CIPRNet training lecture will contain information about solutions and methods to detect cyber attacks and increase the resilience of ICT part of critical infrastructures.

Number of attendees: 12

2.2.13 Lecture 13: A unified approach for 2D and 3D coverage problems in omni-directional and directional sensor networks

by Antonio Sforza, at University Campus Bio-Medico of Rome, 13th February 2015.

The presentation proposes a unified and stepwise solving approach for two and three dimensional coverage problems to be used in omni-directional and directional sensor networks, schematizing the region of interest and the sensor potential locations by a 2D or 3D grid of points, and representing the sensor coverage area by a circle or by a circle sector. The built model constitutes the optimization module of a smart tool for the protection of a railway infrastructure protection, developed for the European project METRIP. The presentation concludes with an application of the proposed approach to a real test case and a discussion of the obtained results.

(web streaming available)

Number of attendees: 11

2.2.14 Lecture 14: Optimal device placement in wireless sensor networks

by Dr Claudio Sterle, Rome, 13th February 2015, (Lecture part I, 11.00 h)

Venue: University Campus Bio-Medico of Rome (Italy) and web at <https://connect.portici.enea.it/unicampus/>

The problem of covering, monitoring and/or controlling a region of interest by wireless sensor networks (WSN) has been widely treated in literature. The presentation resumes the main ILP optimization models, providing also a discussion on some straight extensions and variants which allow to take into account the specific features of the sensors, related monitoring tasks and strategic decisions in WSN design.

Number of attendees: 11

2.2.15 Lecture 15: Modeling IT networks with Riverbed Modeler**At UTP, Bydgoszcz, 12th March 2015 (Thursday)**

The CIPRNet training lecture (Hands-On) about “Modeling IT networks with Riverbed Modeler” will be held in form of a workshop. During practical hands-on labs participants will have an opportunity to learn how Riverbed Modeler solution could be used for planning, modeling and analysing of critical IT network infrastructure.

Topics covered by the workshop include:

- Predicting traffic volume growth and IT network load,
- Identifying network bottlenecks and preventing overload,
- Network failure survivability analysis,
- Preventing network outages with effective change control.

Number of attendees: 10

2.2.16 Lecture 16: Optimal Security Investments for Critical Infrastructure Systems**by Maria Paola Scaparra, at University Campus Bio-Medico of Rome, 26th March 2015.**

A crucial issue in today's distribution, supply and emergency response systems is to guarantee continuity and efficiency in service provision in the face of a variety of potential disruptions. Planning against possible disruptive acts of nature or sabotage is an enormous financial and logistical challenge, especially if one considers the scale and complexity of today's infrastructure systems. Since it is generally impractical to secure all assets, it is important to optimize the protection of key system components. Protection investment problems against worst-case losses are typically formulated as bi-level or tri-level optimization problems. This lecture presents some recent optimization models for identifying efficient investments in protection and security measures for distribution and transportation systems. These models incorporate a variety of different issues such as: capacity restrictions; correlation of disruptive events and disaster propagation effects; dynamic investments; different objectives (demand coverage, cost, travel time, passenger flow); stochastic aspects (e.g., extent of the disruptions); and resiliency aspects (e.g., recovery times of the disrupted components and disruption frequency). Efficient solution methodologies for solving these complex models will also be briefly discussed.

(web streaming available)

Number of attendees: 29

2.2.17 Lecture 17: Innovative Cybersecurity methods for Next Generation Infrastructures**by Wojciech Mazurczyk, at UTP, Bydgoszcz, 7th May 2015.**

Topics covered at the lecture include:

- Current threats and trends in cybersecurity,
- New malware trend: utilization of information hiding techniques for improved stealthiness,
- Bio-inspiration as an innovative approach for cybersecurity.

Number of attendees: 12

2.2.18 Lecture 18: Selected aspects of Critical Infrastructures cybersecurity

by **Rafal Kozik, and Michal Choras, (UTP)**, at Technical University Poznan (PP), Poznan, Poland , **21st May 2015**.

Topics covered at the lecture include:

- Current cyber threats for critical infrastructures
- Current trends in CI cybersecurity
- Machine learning methods for CI cybersecurity

Number of attendees: 21

2.2.19 Lecture 19: Railway Infrastructure Security

At University Campus Bio-Medico of Rome, 4th June 2015.

The security of railway mass transportation systems represents today a challenge, given their complexity and peculiarities, both from technological and logistic points of view. However, it is mandatory to increase the protection of those systems due to the current sociopolitical scenario and the centrality of Italy in the year of EXPO 2015.

In collaboration with national and international experts, this lecture aims to highlight the main risks and the most modern solutions used for the protection of railway systems.

(web streaming available)

Number of attendees: 75

2.2.20 Lecture 20: Stepwise Cloud Migration

by **Bernhard Hämmerli (ACRIS)**, at **CRITIS 2015, Berlin, Germany, 7th October 2015**.

Abstract: Cloud Computing creates in any infrastructure operator bad feelings. Operators don't want the infrastructure and think this is a significant loss of control. However, when looking in more detail we realize that the facts contradict our feelings: The workforce of Cloud Services is better educated, has often 24by7 security and reaction, has more and quicker option to reconfigure and has often fewer outages. An in-depth analysis discloses a fine grade change of bought and completely self-operated infrastructure towards growing cloud inclusion. An easy to understand example is malware protection: Even when we own the software, unless daily updates from the cloud with newest script files and signature we will not be secure anymore. And it shows perfectly, how the inclusion of the cloud takes place stepwise. The big picture of Cloud Migration: Usually it starts with hybrid solution, where on-premises and cloud are both operating and delivering its part to the overall solution. The seven steps towards cloud migration are:

1. **Know your asset (inventory)**
This includes knowing your architecture, the connection between systems, the mutual impacts etc.
2. **Know your data, including control data**
3. **Risk Analysis** starts by classifying the data and deciding which data are suitable for the cloud. Risk is assessed by evaluation how much it would cost, if the data are completely lost or leaked through the cloud. Thereby different data categories such as direct personal and other very sensitive data and general data must be distinguished.
4. **Vendor Contracting** – Within this stage prior findings on specification and requirements should be presented to the vendors. In following discussions the vendors should

have the chance to formulate “how he can support the customer” and to explain “how customers benefit from experience and support for presented top management”.

Security requirements must be clearly communicated up front.

5. **Commissioning and performance acceptance test** should be defined up front. A good approach is running each service up front as internal IT process, fully managed and successfully practiced. Afterwards specific services are outsourced successfully. Note: In the discussion the following statement was made: “There is a significant difference between outsourcing and cloud services, with the former being less anonymous than the latter.”
6. **Communication with top management Conclusion:** Consolidate all prior findings and present them to top management. Be concise and well prepared when presenting security and compliance dimension and free of preferences: good attitude is defining the challenges and offering solutions including price tag and personnel effort.
7. **Compliance Analysis** is usually performed by IT in cooperation with legal, audit and other internal or external parties. The compliance team’s tasks include compliance of all issue-relevant state regulations, business branch authority compliance rules and other stakeholder’s demands such as business partners etc.

If following this path, we recommend considering the following three issues: **Data classification, IT Architecture Integration** and a sound level of **organizational maturity**.

Number of attendees: 11

2.2.21 Lecture 21: Cyber Security Aspects of Critical Infrastructures Protection

by **Rafal Kozik (UTP), at University of Glasgow, 26th October 2015.**

Abstract: As our world becomes more and more connected via open networks with the cyberspace, many new challenges arise. Therefore, there is a significant effort focused on national critical infrastructures evaluation, simulations and threats analysis. In this presentation current situation and challenges related to cyber security of Critical Infrastructures (CI) are discussed. Presented study shows that cyber-related threats should be concerned as important factor incorporated into strategic analysis of infrastructure disruptions, consequences evaluation, and assessment of systems dependencies.

The lecture covered the following topics:

- General overview of FP7 CIPRNet project
- Current challenges of Critical Infrastructures Protection (CIP) in the area of cyber security
- The problem of increasing number of dependencies and interdependencies between industrial control systems (ICS) and ICT systems
- General overview of recent cyber attacks impacting Critical Infrastructures
- Overview of different approaches and practical examples of cyber attacks detection.

Number of attendees: 12

2.2.22 Lecture 22: Afhankelijkheden en meer [Dependencies and more]

by **Eric Luijff (TNO), at TNO Soesterberg for the Dutch National Network for Risk Management (NNR), 26th October 2015.**

Since about 2007 the NNR, the National Network Risk Management, operates. In September 2012 the informal network has been turned into an association. Various organizations already

operate in the field of risk management and related areas such as security. NNR functions as an umbrella organisation. Although professorial chairs have been set up, journals, and several trade unions exist, risk management as a discipline is still not sharp profiled and the attention to risk management is not yet sufficiently anchored in the top of many companies. It therefore seems appropriate to promote contacts between science, government and industry. The NNR organizes 5 to 6 times a year a meeting with speakers from outside and / or from their own circle.

Number of attendees: 12

2.2.23 Lecture 23: Secure Estimation for Wireless Control under Denial-of-Service Attacks by Gabriella Fiore, at University Campus Bio-Medico of Rome, 10th November 2015.

Cyber-Physical Systems (CPSs) are systems found in a wide range of application fields such as power grids, smart buildings, transportation systems and unmanned vehicle systems. CPSs integrate physical processes, computational resources and communication capabilities. The feedback loop between the physical and the computational world through a (wireless) communication network increases the vulnerability of the entire system to failures or to malicious and intentional attacks by an external attacker.

In this talk a novel methodology is presented to estimate the state of the CPS when measurements and control inputs are corrupted by sparse attacks based on compressed sensing and error correction techniques.

Specifically, conditions are given for the system to be resilient against packet losses and adversarial attacks (e.g., DoS), characterizing the maximum number of corrupted signals that can be tolerated in order to perfectly recover the true system state.

The methodology was demonstrated with respect to a scenario where UAVs cooperatively transport a flexible payload.

Number of attendees: 82

2.2.24 Lecture 24: Praxiserfahrungen beim Technologietransfer und Kriterien für Usability im Bereich KRITIS und Bevölkerungsschutz

(engl: Practical experiences in technology transfer and criteria for usability in the areas of Critical Infrastructure Protection and Civil Protection)

by Erich Rome (Fraunhofer IAIS), at Tagungslounge Leipzig, 4th December 2015.

Event: SIFO-Fachdialog „Konturen eines technik- und sozialwissenschaftlichen Sicherheitsverständnisses“

Abstract: The presentation looked into experiences of conditions of successful cooperation between science and users. The CI area is characterised by specific security challenges (complex, interdependent, sometimes cross-border, constantly changing systems; cascading effects; limited access to sensitive information) and the interplay of a wide range of stakeholders (politicians, authorities, operators, civil / Civil Protection, Research Funding / Community). Research in this area requires the establishment of a relationship of trust with operators and a multidisciplinary, mind-set. A key factor of successful technology transfer is the usability of the developed solutions, for example, decision support systems (that can be used in normal operation and emergency situations). Besides that, a pecuniary value added in industrial operation raises the incentive for investment by operators. The research must closely follow the requirements of end-users from the earliest possible stage on (including support for

established standards; links to existing systems; interoperability with existing processes; focus on sense-making, a simple representation and interpretability of results and concrete recommendations for action; fast, time-stamped provision of situational relevant information) and develop easy-to-use solutions that bring real support from the perspective of practitioners.

Number of attendees: 36

2.2.25 Lecture 25: Cyber-physical security solutions for critical infrastructure protection

by Michal Choras and Rafal Kozik (UTP), at University of Cagliari, 16th February 2016.

Abstract: During the lecture the overview of practical cyber-physical security solutions for CIP were presented. Moreover, the results and approach of the CIPRNet project were discussed.

Number of attendees: 14

2.2.26 Lecture 26: Avoid enlarging a disaster: take care of critical infrastructure

by Eric Luijff (TNO), at TU Eindhoven, 20th February 2016.

Event: Annual Symposium of Engineers Without Borders of the Netherlands (EWB-NL)

The theme of the Symposium is “Technical Challenges in Disaster Response”. Logistics, averting bottlenecks, coordinating governmental efforts and those of aid organizations – they quickly become the preoccupations of those overseeing disaster relief operations. We all feel compelled to help and we would like to contribute. However, this does not always have to be by donating money. Clever ideas and practical solutions are just as valuable. Whether it is to create an app to locate people or an easy to put up construction for shelter, all ideas are useful after a disaster where people are left without anything.

Number of attendees: 85

2.2.27 Lecture 27: Introduction to CIPRNet

by Erich Rome (Fraunhofer IAIS), at Sankt Augustin, 1st March 2016.

Event: periodic meeting of the VRGeo consortium

A general introduction to the project CIPRNet, with a focus on one of its new capabilities: 'what if' analysis based on federated modelling, simulation and analysis of the behaviour of Critical Infrastructures in crisis situations. The capability shall enable crisis managers of civil protection agencies to explore different courses of action in training situations. A new method for consequence analysis enables the comparison of the overall outcomes of different courses of action.

Number of attendees: 14

2.2.28 Lecture 28: Introduction to Critical Infrastructures (CI) & dependency phenomena

by Eric Luijff (TNO), at Cyber Security Academy, The Hague, 11th March 2016.

A general introduction on Critical Infrastructures, addressing the following topics:

- What are critical infrastructures?
- Importance of critical infrastructure to society
- Background of activities by EU and nations

- Most important phenomena
- Awareness of R&D in this field

Number of attendees: 24

2.2.29 Lecture 29: CIPRNet OpenMI-Webinar

by Bernhard Becker and Andreas Burzel (Deltares), 21st April 2016.

Open Modelling Interface (OpenMI) is an OGC standard that allows time-dependent models to exchange data at run-time. When the standard is implemented, models can run simultaneously and share information at each time step, making model integration feasible at the operational level. The possibilities of model coupling with OpenMI to modellers and project managers in water related integrated modelling and other interested attendees will be showed. Different research projects and case studies will be presented, where OpenMI has been applied in the past and illustrate the added value of model coupling. The webinar includes the fundamentals about computer model simulations and computational grids, boundary conditions and model forcing.

The OpenMI Webinar was recorded and it is available here <https://www.deltares.nl/en/webinars/model-coupling-with-openmi-introduction-basic-concepts-and-live-demonstration/> and at security-learning.eu.

This webinar covered the following topics:

- What is OpenMI?
- Examples of water flow simulation models
- Coupling mechanisms
- The OpenMI configuration editor
- Setting up an OpenMI composition
- Migrate existing models to OpenMI compliance
- Demonstration of water related models using OpenMI 1.4 and SOBEK 3

Number of attendees: 13

2.2.30 Lecture 30: CIPRNet talk at SATW: "Aktuelle Forschung zu kritischen Infrastrukturen"

by Erich Rome (Fraunhofer IAIS), at ETH Zurich, 21st April 2016.

Event: SATW Fachveranstaltung "Cyber Security" (Technical event of the Swiss Academy of Technical Sciences)

A general introduction to the project CIPRNet, with a focus on one of its new capabilities: 'what if' analysis based on federated modelling, simulation and analysis of the behaviour of Critical Infrastructures in crisis situations. The capability shall enable crisis managers of civil protection agencies to explore different courses of action in training situations. A new method for consequence analysis enables the comparison of the overall outcomes of different courses of action. An extensive conclusion provides experiences and analyses of barriers and success factors of transferring research results on Critical Infrastructures into practical application.

Number of attendees: 150

2.2.31 Lecture 31: Hybrid Simulation of Distributed Large-Scale Critical Infrastructures**by Massimo Ficco, at UTP, Bydgoszcz, 8th September 2016.**

Critical infrastructures represent the pivotal assets and resources upon which the current society greatly relies to support welfare, economy and quality of life.

Nowadays, the trend is to restructure these infrastructures by applying a System of Systems (SoS) concept, where the sparse islands are progressively interconnected by means of proper middleware solution through wide-area networks. The huge complexity of such systems makes more complicated for designers and developers the task of facing integration and configuration issues of both pre-existing and under development systems. Indeed, integration among components may introduce unexpected system behaviours on dependability and performance that usually manifest during systems installation and execution time. Additionally, as they cannot be detected earlier, they require on-site maintenance operations resulting in increased maintenance costs and overspending in terms of personnel resources. A promising way to cope with these new systems, and to lower maintenance costs, is to reproduce such complex and distributed systems locally, and let them run prior to the actual execution on-site in order to get knowledge about their real behaviour and define mitigation means and improvement actions. Hybrid and distributed simulation strategies, supported by novel technologies for resources virtualization and working environment reproduction, represent the most promising way to define the needed strategies to actually support such paradigm shift.

Number of attendees: 44

2.2.32 Lecture 32: CEIP and Energy Security in Perspective of NATO Energy Security Center of Excellence**by Artūras Petkus, at CRITIS 2016, Paris, , 10th October 2016.**

Cyber attacks on key energy infrastructure - and on the electricity system in particular - are increasing, both in frequency and sophistication (U.S. Department of Homeland Security). Some countries adopt military doctrines, that could be called "Hybrid War". Unlike its conventional counterpart, hybrid war blends elements of diplomacy, clandestine action, disinformation, sabotage, irregular troops and standard kinetic force to achieve strategic objectives. While hybrid war takes place over several dimensions, it appears that critical energy infrastructure and energy industry of any country could be targeted as part of a wider campaign to reduce the county's ability and willingness to resist. Therefore, NATO strives to "continue to develop NATO's capacity to support national authorities in protecting critical infrastructure, as well as enhancing their resilience against energy supply disruptions that could affect national and collective defence, including hybrid and cyber threats" (NATO Warsaw Summit Declaration). NATO Energy Security Center's of Excellence contribution to this priority will be presented.

Number of attendees: 65

2.2.33 Lecture 33: Critical Infrastructures: How to deal with complex interconnected systems of systems to prevent and mitigate cascading failures?**By Yohan Barbarin (CEA), at National Institute of Applied Sciences (INSA), 18th October 2016.**

The world is getting more and more interconnected over the years. SCADA systems and large infrastructures follow the same path. Critical / Vital Infrastructures (CI) have been defined by

sectors and their interconnections can create severe cascading effects. Many examples of such cascading effects occurred over the last two decades. The goal of this lecture is to introduce the context of critical infrastructure protection (CIP), discuss the role of dependency and present ongoing research to prevent and mitigate cascading effect.

With the support of Modelling, Simulation and Analysis (MS&A) coupled to Geographic Information System (GIS), the EU project CIPRNet proposes an innovative solution for CIP. The CIPRNet project covers the 4 following area: CI identification, CI dependencies, risk management and crisis management. A system is being developed on the concept of "federated simulations".

The targeted audiences are the final courses engineers, PhD followers and professionals concerned by systems' reliability, safety and protection.

Number of attendees: 18

2.2.34 Lecture 34: Mathematical Modelling of CI Resilience with a focus on the Cascade effects

by Mohamed Eid (CEA), by National Institute of Applied Sciences (INSA), 18th October 2016.

Critical Infrastructures Protection (CIP) requires the development of robust mathematical models and powerful simulation algorithms and software tools. CIP activities aims principally to enhance the CIs resilience facing different kinds of threat. Then, one of the issues in CIP is the Modelling, Simulation and Analysis (MS&A) of the CI resilience.

MS&A of the CI resilience should consider the specific nature of each CI. CIs are generally distributed, connected, dependent and interdependent. They are also belonging to different types of technology and operating using several types of physical phenomena. A robust mathematical model would allow predicting the functional behaviour of a CI facing a well-define threat under given operational conditions. This would allow the crisis managers to take the best decision at the best moment in order to absorb, mitigate, share, lessen or accept the consequences of the loss of service supply by a set of CIs under a threat's action.

A general review of the concept of resilience and the existing lacks in the common understanding and the use of the concept. How cascade effects impact on the dynamics of the resilience mathematical mode and how dependency/interdependency increase the complexity of the models. A specific interest will be given to: the mathematical issues in describing cascade effects.

The targeted audiences are the final courses engineers, PhD followers and professionals concerned by systems' reliability, safety and protection.

Number of attendees: 18

2.2.35 Lecture 35: Increasing Security of Critical Infrastructures through intelligent even correlation

by Salvatore D'Antonio, at UTP, Bydgoszcz, 21st October 2016.

Security Information and Event Management (SIEM) is a consolidated technology that relies on the correlation of massive amounts of security-relevant information in order to detect ongoing attacks and intrusions. This correlation process is usually fed with logs generated by network devices and equipment, thus proving to be ineffective against attacks that affect multiple domains (e.g. physical, logical) or different architectural levels (e.g. network, operating

system, application) of a service infrastructure. To bridge this gap, a combination of physical and logical security is required that allows for a more effective protection of the infrastructure. Recently some achievements have been made. For example, SEM (Security Event Monitoring) and SIM (Security Information Management) have merged into SIEM, and LACS (Logical Access Control System) and PACS (Physical Access Control System) have merged into IM (Identity Management), Security Operation Center (SOC) technology has improved significantly, but much is yet to be done. In this talk an event collection and correlation approach is presented that brings a significant advancement in the convergence of physical and logical security technologies. In this context, "convergence" means effective cooperation (i.e. a coordinated and results-oriented effort to work together) among previously disjointed functions. The proposed approach relies on data fusion techniques to process heterogeneous data and spot evidence of security issues by using complex event pattern detectors that correlate information from multiple architectural layers and domains of the monitored infrastructure. This allows for dependable (i.e. accurate, timely, and trustworthy) detection and diagnosis of attacks, which will ultimately result in the achievement of two goals of paramount importance, and precisely: 1) Guaranteeing the protection of citizens and assets, and 2) Improving the perception of security by citizens. This approach has been validated in three real use cases, with two objectives: 1) Capturing the diversity of the requirements to be satisfied by a platform truly supporting the convergence of physical and logical security technologies; 2) Overcoming fragmentation of security approaches.

Number of attendees: 63

2.2.36 Lecture 36: Cyberbezpieczeństwo systemów sterowania elektrowni

by K. Świrski, at UTP, Bydgoszcz, 21st October 2016.

This lecture concerns the cybersecurity of DCS (Distributed Control Systems), in particular those controlling processes in critical infrastructures such as energy generation and distribution. Selected threats and examples of military malware are discussed. Practical solutions for protections as well as the relevant norms (e.g. NERC, NISA etc.) are overviewed. The consequences for hybrid conflicts and homeland security are presented.

Number of attendees: 63

2.2.37 Lecture 37: Critical Infrastructure Protection – CIP: Modelling, Simulation & Analysis (MS&A) of CI performances and resilience

by Mohamed Eid (CEA), at Lithuanian Institute of Energy, 25th October 2016

Critical infrastructures are complex systems supplying vital services to modern societies. They are more and more smart, connected and distributed. Their rupture can endanger the security of the citizen and the society. Robust models and simulation techniques should be developed in order to enhance the CI resilience and to better manage crises in case of CI rupture.

The lecture introduced the basic concepts in MS&A of CI resilience and performances.

Number of attendees: 18

2.2.38 Lecture 38: Dynamical robustness to synchronization of complex networks: methods and applications to electrical infrastructures

By Mattia Frasca, at University Campus Bio-Medico of Rome , 5th December 2016.

In this talk I will discuss dynamical robustness of a complex network to noise injected through one of its nodes. The focus is on synchronization of coupled nonlinear systems and, as a special instance of this phenomenon, the consensus protocol for linear integrators will be also addressed. An exact closed-form expression of the synchronization error for the consensus protocol and an approximate result for chaotic units is established. From this result, we derive that, while structural robustness is known to be significantly affected by attacks targeted to network hubs, in our case dynamical robustness is controlled by both the topology of the network and the dynamics of the units. We provide examples of networks of units where hubs perform better or worse than isolated nodes. I will then analyse the application of this method to power grids, by including a real example (the UCTE European High Voltage grid) and deriving some conclusions on the most and least critical nodes of this network.

Number of attendees: 50

2.2.39 Lecture 39: How to evaluate the risk for interdependent Critical Infrastructures scenarios

By Roberto Setola (UCBM), at University of Kent, Canterbury, 9th December 2016.

In the presence of complex scenarios characterized by the presence of several and interdependent actors and elements, the usual approaches for Risk Analysis based on the evaluation of likelihood and impact cannot be able to capture all the aspects, especially those related to “extreme events”. The lecture will illustrate such a phenomena suggesting to approach Risk Analysis in a holistic perspective adopting an All-Hazard framework.

Number of attendees: 11

2.2.40 Lecture 40: Cyber security and CIP - challenges and solutions

By Michal Choras and Rafal Kozik (UTP), University of Cyprus, 17th January 2017

In this presentation, current situation and challenges related to cyber security of Critical Infrastructures (CI) are discussed. Presented study shows that cyber-related threats should be concerned as important factor incorporated into strategic analysis of infrastructure disruptions, consequences evaluation, and assessment of systems dependencies. During the talk, selected innovative cyber security solutions and approaches will be presented.

Number of attendees: 19

2.2.41 Lecture 41: How to evaluate the risk for interdependent Critical Infrastructures scenarios

By Roberto Setola (UCBM), Lithuanian Institute of Energy, Kaunas, Lithuania, 8th February 2017

In the presence of complex scenarios characterized by the presence of several and interdependent actors and elements, the usual approaches for Risk Analysis based on the evaluation of likelihood and impact cannot be able to capture all the aspects, especially those related to “extreme events”. The lecture will illustrate such a phenomena suggesting to approach Risk Analysis in a holistic perspective adopting an All-Hazard framework.

Number of attendees not available (event held after the editorial deadline of this deliverable).

3 CIPRNet Online Course

On the occasion of the Edition 3 of Master Class on Modelling, Simulation and Analysis of Critical Infrastructures which took place on 23rd and 24th November 2016 at Fraunhofer Institute for Intelligent Analysis and Information System (IAIS) in Sankt Augustin (Germany), UCBM launched the CIPRNet online course on Modelling, Simulation and Analysis (MS&A) of Critical Infrastructures (CI).

The lectures currently contained on the website have been recorded during the third edition of the CIPRNet Course on MS&A of CI inside the post graduate Master in Homeland Security at UCBM (Module A, Module B, Lecture 2 of Module C), at ENEA premises (Lecture 1 of Module D) and at Deltares premises (Module D, webinar also accessible on Deltares website).

The CIPRNet online course is accessible at URL <http://www.security-learning.eu/>. Figure 8 shows the home page of the service.

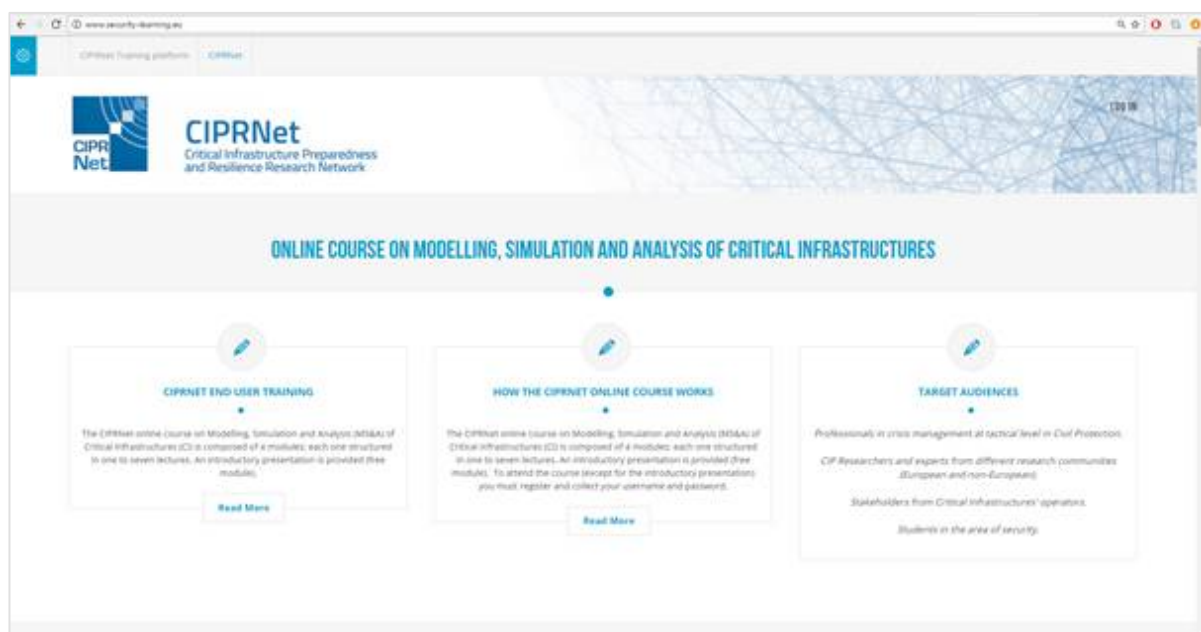


Figure 8: CIPRNet online course home page.

The Online Course is composed of 4 modules, better specified from Section 3.1 to Section 3.4 to (each one structured in one to seven lectures (Figure 9)).

An introductory presentation to CIPRNet is provided (free module).

The target audiences of the CIPRNet online course are:


- Professionals in crisis management at tactical level in Civil Protection;
- CIP Researchers and experts from different research communities (European and non-European);
- Stakeholders from Critical Infrastructures' operators;
- Students in the area of security.

The website is completed by the course information and instructions and by the lecturers' bios and contact details. After a stress test phase made by internal users, the online course has been also announced on the CIPRNet website (20.12.2016).


More details on the MOOC platform, including how to attend the course and how each lecture page is structured, are available in Section 9 of the Deliverable **D4.9** (Report on final status of the VCCC) [2].

CIPRTRAINER DERAILMENT SCENARIO WITH CROSS-BORDER ASPECTS
 Teacher: Stefan Rilling (Fraunhofer)

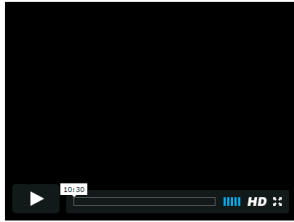
PART ONE



PART TWO



PART THREE




Topics:

- Scenario storyline
- Rules
- Scenario database

Abstract:

This lecture presents the crisis scenarios that have been developed for CIPRTrainer. The first scenario is a derailment of a cargo train in a German city near the Dutch border. The second scenario is a flooding of the river Rhine in the border region between Germany and The Netherlands. Both scenarios have cross-border aspects, and in both scenarios Critical Infrastructures are affected and produce cascading effects.

Download Presentation:




References

- EU FP7 CIPRNet, CEA, Deliverable D6.2 – Application Scenario, Gramat, 2014.
- EU FP7 CIPRNet, Fraunhofer, Deliverable D6.3 – Federate CI Models, Sankt Augustin, 2015.
- Xie, Jingqun; Theocharidou, Marianthi; Barbarin, Yohan; Erich, Knowledge-driven scenario development for critical infrastructure protection. In: Critical Information Infrastructures Security - 10th International Workshop, CRITIS 2015, Berlin, Germany, October 5-7, 2015. p. to appear. Lecture Notes in Computer Science, Springer, 2015.

TEST

The tests consist of 4 multiple choice questions randomly chosen, that will assess your comprehension of the lectures. To pass the test, you must answer correctly 3 questions over 4. The system will indicate your correct answers and allow you to re-attempt the test until you succeed it.

When all tests (of the module or of the whole course) are successfully completed, you can apply for your attendance certificate sending an email to info@security-learning.eu. We will check your data and will send you the attendance certificate as soon as possible.



You are logged in as [Maria Carla De Maggio](#) (Log out) | [Contact](#) | [Publishing Notes](#) | [Data Protection](#)

Figure 9: Single Lecture web pages of the CIPRNet MOOC training platform.

Table 2: Visitor statistics of CIPRNet’s e-Learning MOOC platform.

Period ending (Week)	Authenticated user on front page	Guest	Student	All
23 January 2017	0	199	0	199
16 January 2017	4	272	36	312
9 January 2017	0	156	0	156
2 January 2017	0	672	0	672
26 December 2016	10	86	15	111
19 December 2016	7	41	0	48
12 December 2016	3	19	7	29
5 December 2016	4	37	22	63
28 November 2016	175	458	208	841
21 November 2016	49	210	105	364
Totals	252	2150	393	2795

Visits at the website, two months after the launch of the online course, at 26th January 2017 are still low (in Table 2, visits per week) but pretty much stable over time, and the registered users are only nine (of which five from European research/academic institutions inside the consortium). For this reason, further dissemination efforts are required.

In the next sections the contents of each module are described.

3.1 Module A

Module A is about Critical Infrastructure Modelling, Simulation and Analysis and it is composed of the following seven lectures:

Lecture 1: From critical infrastructure protection to critical infrastructure resilience

Teacher: Marianthi Theocharidou (JRC)

A concept named “resilience” has become in recent years a new catchword in critical infrastructure debates. The lecture aims to explain what exactly resilience means, how CI resilience can be enhanced and how resilience can be measured and tested. The presentation offers a conceptual treatment of the issue, focusing especially on the technological dimension of critical infrastructure.

Lecture 2: Simulation of Critical Infrastructures (CI): relevant applications

Teacher: Eric Luijff (TNO)

Analysis of the different areas of application of Critical Infrastructure Protection (CIP) Modelling, Simulation & Analysis (MS&A), and the added value for stakeholders such as policy-makers, CI operators, emergency management (exercises, what-if, decision support). Overview of the current activities in CIP MS&A and future directions.

Lecture 3: Principal modelling techniques: applications and limitations

Teacher: Mohamed Eid (CEA)

Illustration of the concept of model and mathematical modelling. Analytical vs. simulation solutions of a model. Introduction to the systems composed by several and interacting components. Representation of CI as collection of heterogeneous interacting components. The concept of the system of systems.

Lecture 4: Modelling and investigating dependencies of CI

Teacher: Roberto Setola (UCBM)

Introduction to the concept of (inter) dependency and their classification. Elements to qualify and quantify dependencies. How to model some of the most common dependency phenomena Description of some of the most diffused holistic models illustrating their pros and cons (limits) with specific focus on IIM (Input Output Inoperability Model) approach.

Lecture 5: Introduction to federated simulation

Teacher: Edwin van Veldhoven (TNO)

Introduction to the simulation of complex system using the “federated” approach, i.e. allowing a set of simulators, each tailored to analyse a specific phenomenon or component infra-

structure, to share data in order to simulate complex scenarios where those elements have to interact with each other.

Lecture 6: Simulation approaches of System of Systems

Teacher: Alberto Tofani (ENEA)

Illustration of the main simulation approaches of System of Systems. Modern critical infrastructures (CIs) constitute large multilayered complex systems. Moreover, each infrastructure resorts to other CIs (typically, but not limited to, energy and ICT) to accomplish its goals: in other words, CIs are inter-dependent. Powerful methods are required to model and analyse these interdependent infrastructure networks from a “systems-of- systems” (SoS) perspective. The lesson shows as it is of fundamental importance to find an appropriate formal representation of the system of systems considering the available information and the analysis objectives. Moreover, a number simulation approaches are presented ranging from very abstract (topological approaches) to very detailed (physical simulators). These tools can be considered as the fundamental pillars of a CI MS&A platform allowing various kind of analysis for different end users and, in general, for different objectives of the analysis.

Lecture 7: Verification and validation techniques

Teacher: Edwin van Veldhoven (TNO)

After a brief introduction to V&V, an efficient and effective approach for organising the V&V activities for CI models is presented that leads to the choice of which V&V techniques to employ. An overview of the main V&V techniques is presented.

3.2 Module B

Module B is about “What-if” Analysis and the CIPRTrainer and it is composed of the following 5 lectures:

Lecture 1: CIPRTrainer – training the exploration of different courses of action

Teacher: Erich Rome (Fraunhofer)

This presentation provides an overview of one of CIPRNet’s new capabilities for stakeholders, the »what if« analysis based on modelling and simulation. This capability is provided as a training application for crisis management at the tactical level in civil protection, which is called CIPRTrainer. CIPRTrainer allows small crisis management teams exploring different courses of action and compare the overall outcomes of the scenario evolution. CIPRTrainer is equipped with two cross-border scenarios including two different threats (flooding and a cargo train derailment) that have also impact on CI.

Lecture 2: Federated simulation in CIPRTrainer

Teacher: Stefan Rilling (Fraunhofer)

This lecture gives a comprehensive insight of the federated simulation system adopted by the CIPRTrainer software. At first, the various critical infrastructure simulators and the corresponding simulation models are presented. Then, the software architecture of the federated simulation environment consisting of simulation adaptors and complex event processing is explained in detail. The course of a federated simulation and the occurrence of cascading effects are illustrated by a simple example.

Lecture 3: Consequence analysis as a basis for »what if« analysis**Teacher: Norman Voß (Fraunhofer)**

Consequence analysis (CA) clarifies the meaning of impacts for the population and the economy. The lecture aims to give an overview about the CA concept of the CIPRTrainer. It will explain which methods can be applied, which kind of data is needed and which data sources we used. Furthermore, the lecture shows some common issues of data elicitation and handling in the CIP domain and provides some advice how to tackle these.

Lecture 4: CIPRTrainer derailment scenario with cross-border aspects**Teacher: Stefan Rilling (Fraunhofer)**

This lecture presents the crisis scenarios that have been developed for CIPRTrainer. The first scenario is a derailment of a cargo train in a German city near the Dutch border. The second scenario is a flooding of the river Rhine in the border region between Germany and The Netherlands. Both scenarios have cross-border aspects, and in both scenarios Critical Infrastructures are affected and produce cascading effects.

Lecture 5: CIPRTrainer demonstration and hands-on experience**Teacher: Betim Sojeva, Erich Rome (Fraunhofer)**

In Part I, this lecture introduces the iconography and basic functions of the graphical user interface of CIPRTrainer. Part II presents the training concept in more detail. This includes the roles of the trainees in the small crisis management team that they form, the specific actions that the trainees –depending on their role – can perform, and the cycle of situation update, situation analysis, decision-taking and action that the team of trainees shall apply.

3.3 Module C

Module C is about Decision Support System and Consequence Analysis Description of the DSS Tool and it is composed of the following 2 lectures:

Lecture 1: Geographical information systems for visualization and analysis**Teacher: Maurizio Pollino (ENEA)**

Geomatics technologies can play a fundamental role both in risk assessment and management and in complex decision making in the course of critical situations due to dangerous events. This lecture describes basic concepts and functionalities of GIS (e.g. geoprocessing and mapping) and the capabilities of Web-mapping tools and applications (WebGIS).

Lecture 2: CIPCast – a decision support system for CI related crisis management**Teacher: Vittorio Rosato (ENEA)**

CIPCast is a Decision Support Systems allowing an operational forecast of the state of risk of a system of (inter)dependent Critical Infrastructures (CI). CIPCast is a complex software based on a GIS Database containing many information layers enabling the static and the dynamic description of a specific geographical area (from the scale of a city up to regional, or larger, scales). From external data (weather forecast, nowcast and other information on natural events and their manifestations), CIPCast determines the expected damage scenario (in terms of CI elements damaged by the expected events), transforms the expected damages into the

reduction of services which CI deliver (by also considering possible cascading effects) and estimates the societal consequences related to the reduction (or loss) of the primary services. CIPCast also support electrical operators by indicating possible strategies for a faster and more efficient restoration of their service. CIPCast, moreover, could be used as a scenario emulator, through the use of synthetic natural events whose resulting impacts could be examined.

3.4 Module D

Module C is about Decision Support System and Consequence Analysis Description of the DSS Tool and it is composed of the following lecture:

Lecture 1: Model coupling with OpenMI – Introduction, basic concepts and live demonstration

Teacher: Bernhard Becker, Andreas Burzel (Deltares)

Did you ever try to couple interacting processes, e.g. surface and subsurface water flow? OpenMI (Open Modelling Interface) is an OGC standard that allows time-dependent models to exchange data at run-time. When the standard is implemented, models can run simultaneously and share information at each time step, making model integration feasible at the operational level. In this seminar, we will show the possibilities of model coupling with OpenMI to modellers and project managers in water related integrated modelling and other interested attendees. We will present different research projects and case studies where OpenMI has been applied in the past and illustrate the added value of model coupling. You will also learn how the different processes were coupled. Ideally, you have basic experiences with computer model simulations and are familiar with computational grids, boundary conditions and model forcing.

4 References

- [1] Annex I – Description of Work (Annex to the Grant Agreement of CIPRNet).
- [2] EU FP7 Project CIPRNet, Fraunhofer, Deliverable D4.9 “Report on final status of the VCCC”. Sankt Augustin, Germany, 16.01.2017.
- [3] EU FP7 Project CIPRNet, Fraunhofer, Deliverable D2.22 “Report on measures for long-term integration”. Sankt Augustin, Germany, forthcoming 28.02.2017