



PROJECT FINAL REPORT

Final Publishable Summary Report

Grant Agreement number: 312450
Project acronym: CIPRNET
Project title: Critical Infrastructure Preparedness and Resilience Research Network
Funding Scheme: Collaborative Project – Network of Excellence (NoE)
Period covered: **from** March 1, 2013 **to** February 28, 2017

Name of the scientific representative of the project's co-ordinator, Title and Organisation:

Dr.-Ing. Erich Rome,
Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung e.V.

Tel: +49 2241 14 2683

Fax: +49 2241 14 4 2683

E-mail: erich.rome 'at' iais.fraunhofer.de

Project website address: <http://www.ciprnet.eu>

Authors	Erich Rome (Fraunhofer) Eric Luijff (TNO), Vittorio Rosato (ENEA), Elias Kyriakides (UCY), Nikolas Flourentzou (UCY), Marianthi Theocharidou (JRC), Micheline Hounjet (Deltares)
Contributors	Stefan Rilling, Jingquan Xie, Norman Voß, Betim Sojeva, Thomas Doll (Fraunhofer)

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

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

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	1
2	SUMMARY DESCRIPTION OF PROJECT CONTEXT AND OBJECTIVES.....	2
2.1	Project context	2
2.2	Project objectives	2
2.2.1	New capabilities.....	3
2.2.2	Scenarios & Architecture	3
2.2.3	Capacity building	4
2.2.4	The CIPRNet Community	4
2.2.5	Integration.....	4
3	MAIN SCIENTIFIC AND TECHNOLOGICAL RESULTS/FOREGROUNDS	5
3.1	Advanced Decision Support	5
3.1.1	Events prediction.....	6
3.1.2	Damage Scenario.....	6
3.1.3	Impact Scenario	6
3.1.4	Consequence Analysis.....	9
3.1.5	Web Interface	9
3.1.6	Report.....	9
3.1.7	Data Exchange with CI operators.....	10
3.1.8	Simulation Mode.....	11
3.1.9	Other Operational Modes	13
3.1.10	Validation, test and final demo.....	14
3.2	‘What if’ analysis for exploring different courses of action (Fraunhofer)	15
3.2.1	Introduction	15
3.2.2	Scenario design and modelling.....	15
3.2.3	Federated simulation in CIPRTrainer.....	18
3.2.4	Realising ‘what if’ analysis with consequence analysis in CIPRTrainer.....	19
3.2.5	Consequence analysis in CIPRTrainer.....	20
3.2.6	CIPRTrainer’s training concept	21
3.2.7	CIPRTrainer’s graphical user interface	22
3.2.8	Interface to CIPCast/RecSIM	24
3.2.9	Validation, test and final demo	24
3.3	Supporting the secure design of Next Generation Infrastructures	25
3.4	The VCCC Services.....	26
3.4.1	The VCCC services framework	26
3.4.2	Ask the Expert (AtE)	28
3.4.3	Knowledge repository	28
3.4.4	Initial CIP reference benchmark set	28
4	POTENTIAL IMPACT AND MAIN DISSEMINATION ACTIVITIES	29
4.1	Potential Impact	29
4.2	Main dissemination activities.....	31
4.2.1	Website.....	31
4.2.2	Publications (peer-reviewed, books, theses).....	31
4.2.3	CIPedia©.....	32
4.2.4	European CIIP Newsletter.....	33
4.2.5	Dissemination material	33
4.2.6	Conferences	34
4.2.7	CYCA (CIPRNet Young CRITIS Award)	34
4.2.8	Cooperation workshops	34
4.2.9	General public	34
4.2.10	Demonstrations	34
4.2.11	Stakeholder contacts.....	35

4.2.12	<i>Exploitation results</i>	35
4.2.13	<i>Lectures</i>	35
4.2.14	<i>Training events</i>	36
4.2.15	<i>e-Learning platform for Massive Open Online Courses (MOOC)</i>	36
5	PROJECT WEBSITES AND CONTACT DETAILS.....	37
6	ANNEX: LIST OF ACRONYMS.....	38
7	ANNEX: REFERENCES.....	38
7.1	References for the main scientific and technological results/foregrounds	38
7.2	Peer-reviewed CIPRNet papers	39
7.3	CIPRNet Books	41
7.4	CIPRNet book chapters.....	41
7.5	CIPRNet invited papers.....	43
7.6	Theses within CIPRNet	43
7.7	CIPRNet public deliverables	44
7.8	Links to conferences organised by CIPRNet	46

1 Executive summary

The **Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet)** was a **Network of Excellence** in Critical Infrastructure (CI) Protection (CIP). CIPRNet has been co-funded by the European Commission's 7th Research Framework Program. The **mission** of CIPRNet was to enhance the resilience of CI by improving the understanding, preparation and mitigation of the consequences of CI disruptions following an all hazards approach. Within its four years' term, the CIPRNet consortium made a decisive effort towards providing sustained support from the CIP research communities to CIP stakeholders like emergency responders, governmental agencies and policy makers. CIPRNet enhanced their understanding of and preparedness against service disruptions of Europe's complex system of interconnected and dependent infrastructures. CIPRNet achieved its main scientific and technological objective, since it developed **new capabilities for national and multi-national emergency management and CI owners**:

- The capability to **analyse consequences** of various short and long term courses of actions based upon statistical data, status information of involved CI, meteorological data and more. CIPRNet implemented and extended the **Decision Support System (DSS) CIPCast**. CIPCast provides a new capability with added value to crisis managers in cold and warm phases of crises and emergencies related to or affecting CI. CIPCast is in test use by Italian CI operators and has been used by Italian national and local civil protection authorities. A novelty is that CIPCast can assess the relation between the potential impact of a disaster and the influence of mitigation actions on the impact according to the cross-cutting criteria specified in the European CIP Directive: casualties' criterion, economic effects criterion and public effects criterion.
- The capability to **explore various courses of action ('what if' analysis)** by employing advanced modelling, simulation and analysis technologies. The implementation of this capability is **CIPRTrainer**, a training system for small crisis management teams at the operational-tactical level. Here, consequence analysis is employed to compare the consequences of the scenario evolution considering the effects of the taken courses of action. This enables finding out which course of action was beneficial to keeping the overall consequences low.
- A study on how to support the secure **design of Next Generation Infrastructures (NGI)**.

CIPRNet achieved another objective by building the required **capacities** for implementing the new capabilities and for performing **education, training and dissemination** activities for spreading the excellence. CIPRNet performed and organised a total of 158 dissemination and training meetings, including four dedicated cooperation workshops, seven conferences, three CIPRNet Master Classes and three CIPRNet Courses for training and hands-on experience with the new capabilities, 48 stakeholder meetings, 41 CIPRNet lectures, and three demonstration events. In terms of publications, CIPRNet published 31 peer-reviewed papers, edited six books, wrote and edited an entire book on its results, published twelve issues of the ECN newsletter (including 61 articles of CIPRNet staff), four PhD theses, a Master thesis, invited papers, and technical reports.

For achieving a **long-term impact** and improvement, the new capabilities were consolidated. Associated web services are sustained beyond the end of the project. For the development, consolidation and dissemination of the new capabilities, CIPRNet has established—as a first step—a **virtual centre of competence and expertise in Critical Infrastructure Protection**, the **VCCC**. The VCCC provides a number of services to CIPRNet's audiences, accessible via the CIPRNet website. The services include CIPedia©, a comprehensive online glossary of CIP terms, an e-learning platform for CIP, CIP bibliographies and project lists, web demonstrations of the new capabilities, and a CIP benchmarking reference dataset.

The VCCC is a virtual facility since it is neither a legal body nor does it have a built structure. But it serves as a foundation for **EISAC**, a European Infrastructures Simulation & Analysis Centre, with the ultimate goal of sustaining the new capabilities and further analysis, assessment and response capabilities beyond the duration of CIPRNet. As an intermediate step between the VCCC and EISAC, CIPRNet partners have founded an **association** by German law, **2E!SAC**, for fostering activities towards EISAC beyond the project end of CIPRNet.

2 Summary description of project context and objectives

2.1 Project context

As it considers the security and safety of European citizens, the economy, the ecology, and the freedom to govern, the protection of its **Critical Infrastructures (CI)** is of utmost importance to the European Union and its Member States (MS). Consequently, the European Commission has issued the European Council Directive 2008/114/EC for fostering the implementation of measures for **Critical Infrastructure Protection (CIP)** in all Member States [ECI08]. Progress has been made both in MS and at the European level. Some MS have passed national CIP plans or established offices or agencies responsible for CIP. Research activities in civil security, funded by national and different EU programmes, complement these CIP activities.

The **Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet)** project commenced on March 1, 2013, and ended on February 28, 2017. CIPRNet was a **Network of Excellence** project in CIP. CIPRNet has been co-funded by the European Commission's 7th Research Framework Program.

2.2 Project objectives

The **mission** of CIPRNet was to enhance the resilience of CI by improving the understanding, preparation and mitigation of the consequences of CI disruptions following an all hazards approach. Within its four years' term, the CIPRNet consortium made a decisive effort towards providing sustained support from the CIP research communities to CIP stakeholders like emergency responders, governmental agencies and policy makers. CIPRNet enhanced their understanding of and preparedness against service disruptions of Europe's complex system of interconnected and dependent infrastructures. At the end of the project, we can assess CIPRNet's objectives in retrospect.

CIPRNet achieved its main scientific and technological objective, since it developed **new capabilities for national and multi-national emergency management and CI owners**:

- The capability to analyse the various courses of action (**'what if' analysis**) by employing advanced modelling, simulation and analysis technologies.
- The capability to **analyse consequences** of courses of actions on short and long term based upon statistical data, status information on involved CI, meteorological data and more in a **Decision Support System (DSS) with added-value** to emergency responders and CI operators. Particularly, the relation between the potential impact of a disaster and the influence of mitigation actions on the impact has been assessed according to the set of cross-cutting criteria specified in the European CIP Directive: casualties' criterion, economic effects criterion and public effects criterion.
- A study of how to support the secure **design of Next Generation Infrastructures (NGI)**.

CIPRNet achieved another objective by building the required **capacities** for implementing the new capabilities and for performing **education, training** and **dissemination** activities for spreading the excellence. To mobilise a critical mass of experts, technologies, and knowledge in this highly specialised and fragmented area of security research, community building and integration of resources was performed.

For achieving a **long-term impact** and improvement, the new capabilities were consolidated. Associated web services will be sustained beyond the end of the project. For the further development, consolidation and dissemination of the new capabilities, CIPRNet has established—as a first step—a **Virtual Centre of Competence and expertise in Critical Infrastructure Protection, the VCCC**. The VCCC is a virtual facility since it is neither a legal body, nor does it have a built structure. But it serves as a foundation for **EISAC**, a European Infrastructures Simulation & Analysis Centre, with the ultimate goal of sustaining the new capabilities and further analysis, assessment and response capabilities beyond the duration of CIPRNet. As an intermediate step between the VCCC and

EISAC, CIPRNet partners have founded an **association** by German law, **2E!SAC**, for fostering activities towards EISAC beyond the end of the CIPRNet project.

2.2.1 New capabilities

Reaching and maintaining the required level of preparedness requires adequate and fast adaptation to on-going changes of CI. CIPRNet implemented two advanced modelling, simulation and analysis-based capabilities for supporting more effective responses to disasters and emergencies that affect or originate from multiple CI.

CIPRNet created added-value decision support capabilities for national and multi-national emergency management and for CI operators. The first new capability, CIPCast, delivers warm and hot phase support of emergency managers and CI operators. CIPCast models CI and their dependencies. CIPCast includes and assesses the behaviour of these CI under severe perturbations, resulting from natural or man-made events and technical failure. For instance, CIPCast uses prediction of weather events (nowcasting and forecasting) for assessing the resulting risk for elements of the power, telecommunications and drinking water infrastructures and generating early warnings. This enables the CI operator switching distribution networks to a more robust configuration at precise points in time. For mitigation after a damaging event, CIPCast's subsystem RecSIM delivers optimal scheduling of recovery teams.

The second new capability, CIPRTrainer, is an application for training crisis management (CM) staff at the operational-tactical level. It enables exploring different courses of action and comparing their consequences («what if» analysis) in complex simulated crisis and emergency scenarios. The simulation employs threat, impact, and damage models and is based on federated modelling, simulation and analysis (fMS&A) of CI. The system fosters the better understanding of the behaviour of CI in crisis and emergency situations and will lead to better-informed decisions.

CIPRNet's work on consequence analysis also addressed a knowledge gap: As mentioned earlier, the EU directive on CIP (European Council Directive 2008/114/EC) recommended assessing the consequences of CI disruptions along the three cross-cutting criteria. Yet methods for implementing such assessment were missing. In this respect, CIPRNet's work on consequence analysis provides a novel and comprehensive methodological basis that could help taking the discussion of assessing the impacts and consequences of CI disruptions to a better-informed level.

An implicit sub-goal was creating mature prototypes of the new capabilities with added value for end users and deploying them. CIPRNet wanted to make a decisive effort for transferring research results into practical application. A successful transfer could contribute to trust building, which in turn could facilitate future transfer activities of research results. CIPRNet considered this crucial for paving the way for deploying services of the VCCC and EISAC.

2.2.2 Scenarios & Architecture

CIPRNet created scenarios at different scales—local, regional, cross-border—for developing, testing and training the new capabilities. A regional Italian scenario considered several infrastructures under threats like floods, heat waves, and earthquakes. A scenario in a region of the border between The Netherlands and Germany considered cross-border emergencies (a cargo train derailment and an extended regional flooding).

The development of the new capabilities started with gathering general requirements for decision support and simulation systems from potential end users by means of questionnaires. The system architecture followed a model-based systems design approach. Key elements of this approach were scenario orientation, requirements engineering, and use cases. As a field test of the new capabilities, CIPRNet demonstrated timely, actionable, risk-informed CIP analysis and strategies for in The Netherlands, Germany, and Italy.

2.2.3 Capacity building

To provide long lasting support from the research communities, CIPRNet contributed also to building the required capacities. A total of 158 dissemination and training activities contributed to this aim, including but not limited to the following. Dedicated cooperation workshops with other projects and networks in the field contributed to a better coherence in the distributed multi-community of CIP researchers and experts. Dedicated training activities—three Master Classes—familiarised experts and potential end users with CIPRNet technology and knowledge in the area of CI-related modelling, simulation and analysis. Young researchers have been trained via 32 staff exchanges between CIPRNet partners and by integrating CIPRNet lectures into three editions of the Master in Homeland Security course at the Università Campus Bio-Medico in Rome. The CRITIS conference series (organised by CIPRNet from 2013 through 2016) contributed to dissemination and visibility of CIPRNet results.

2.2.4 The CIPRNet Community

From the start, CIPRNet involved its stakeholders in the design of the new capabilities. This has been accomplished both by the International Advisory Board of end users and other stakeholders, and by targeted workshops and training events. The International Advisory Board consisted of members from civil protection authorities, ministries, industry, and associations fostering security and CIP. An Independent Ethics Board of experts in data protection and privacy ensured compliance of the project results with legal and ethical standards by providing ethics guidelines and by evaluating the implementation of the guidelines at the end of the project.

2.2.5 Integration

A general objective of Networks of Excellence as funded by the EU's research framework programs is integration of the partners. CIPRNet fostered the integration between partners with its program of activities, consisting of joint research and development activities, joint dissemination activities, internal and external training, and a special staff exchange program that provided incentives for the participants and generated tangible added-value results. For long-term integration, CIPRNet partners planned –and achieved– submitting new joint research proposals on topics in CIP, concluded mutual agreements on mobility programs, and founded the 2E!SAC association for fostering the idea of EISAC. Apart of CIPRNet partners, other organisations already joined 2E!SAC.

The integration achieved during the project's lifetime also forms a basis for a long-term integration of the partner CIP R&D activities. In this respect, CIPRNet succeeded. CIPRNet partners have coordinated their research agendas in the field of Critical Infrastructure Protection and Resilience (CIP/CIR) to a considerable degree, since they submitted ten joint research proposals (at least two successful) and established four mobility collaborations (ERASMUS+). Some partners have made CIP/CIR a new focus field for their research and others have extended their CIP/CIR activities. The partners have also been successful in establishing new collaborations and projects in CIP/CIR, both with stakeholders and research or academic partners.

CIPRNet measured and monitored progress regarding short- and long-term integration by means of integration benchmarking against predetermined performance indicators that had been defined at the beginning of the project. At the end of CIPRNet, nine out of ten benchmark target figures have been achieved or even significantly overachieved.

3 Main scientific and technological results/foregrounds

3.1 Advanced Decision Support

One of the tools which CIPRNet committed to realize there is a Decision Support System (DSS) to enabling a risk forecast for all the CI elements in a given area in relation to expected natural events. Such a DSS has been realized and called CIPCast.

CIPCast provides CI operators and Civil Protection (and other stakeholders engaged in the protection of citizens and assets) a risk forecast correlating the expected natural events (with their intensity) to the damages they could produce on one (or more) CI elements in a given area. CIPCast also produces, for the predicted damages, an assessment of the impact that they will produce (expressed in terms of reduction or complete loss of the service(s) that the hit CI deliver(s)). CIPCast takes possible cascading effects of the CI into account. The CIPCast database, in fact, contains Geographical Information Systems (GIS) data on the location (exact position in Longitude/Latitude coordinates) of the different elements of the different CI (electrical network, water pipeline, telecommunication network, gas pipelines, road and railways etc.) and contains their “dependency map”, consisting in the link connecting one CI to the others. These links are the channels through which perturbations spread from one CI to another.

The reconstruction of the “dependency map” in a complex environment like a large metropolitan area should be considered as one of the major achievement of the project. For the first time (to the best of our knowledge) a complete reconstruction of a dependency map in a city has allowed performing realistic simulation of the cascading effects propagating perturbations from the electrical distribution network to the telecommunication network. The dependency map between these two networks also implies a feedback loop, as mobile telecommunication network, enabling the tele-control operations on the electrical network, could inhibit this function, hindering the solution of the crisis of the electrical network. The CIPCast workflow is shown in Figure 1.

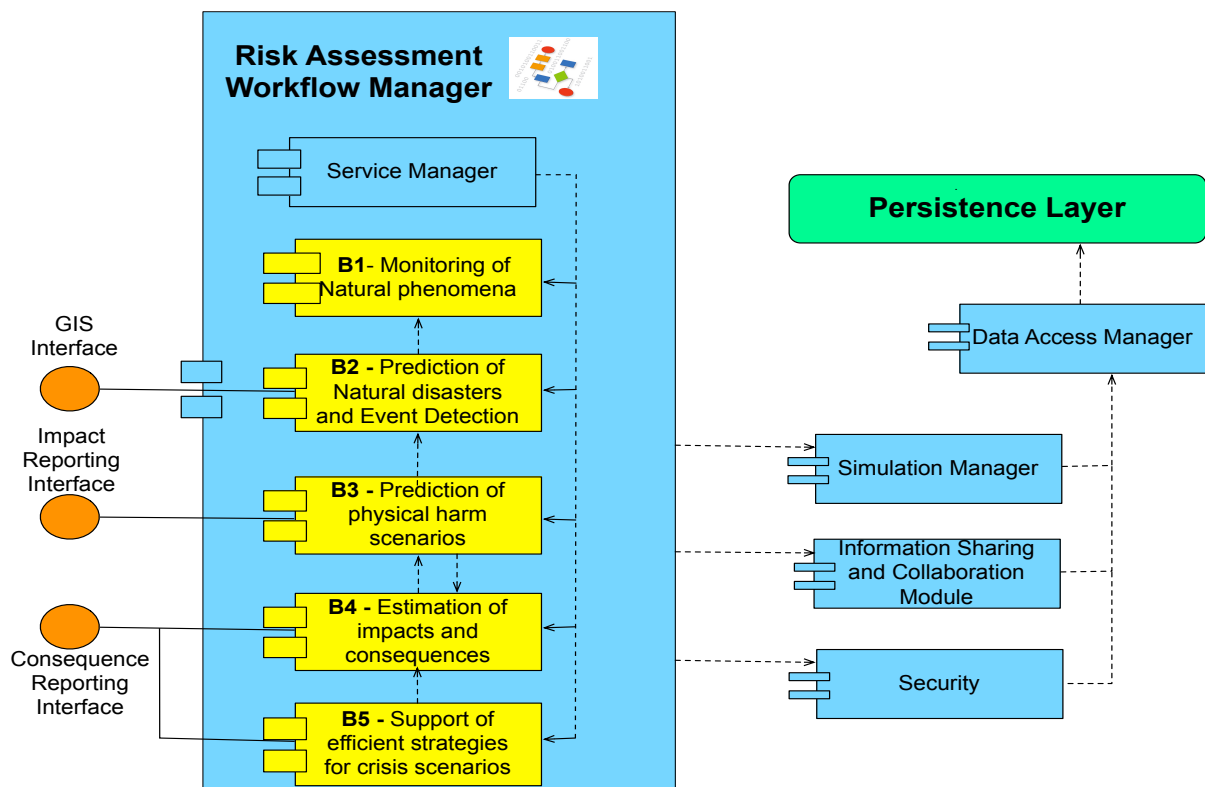


Figure 1: Functional workflow of the CIPCast application. Persistence layer represents the database where all data are contained. (ENEA)

In the following sections, we will briefly describe the CIPCast features.

3.1.1 Events prediction

The prediction of natural events expected in a given area is not carried out directly by CIPCast that, in turn, leverages on public and validated sources. The only prediction performed by CIPCast with its own data source is the nowcasting. CIPCast also leverages on real-time data coming from public sensors that can be freely accessed (in particular hydrometers, weather station data and hydrometers placed along the main rivers, enabling the monitoring of the water level to alert possible flooding pre-conditions).

Lightning forecast is obtained by further post processing of nowcasting data. Contacts have been taken with a company releasing lightning occurrences, made on the bases of a worldwide sensor network.

To summarise the forecast achievable by CIPCast, we can quote:

- weather prediction and precipitation abundance (12-24—36-48 hours),
- weather nowcasting and precipitation abundance (each 15 min for the subsequent 90 min),
- lightning prediction (up to 45 min),
- Tyrrhenian and Mediterranean sea states (waves height and directions) for the forthcoming 12 hours.

Landslides and earthquakes are not predicted but assessed through a constant accession to the site of the National Institute of Geophysics and Volcanology (INGV) which constantly triggers the occurrence of these events (other than volcanic eruptions) by immediately providing, on a public website, the related data.

Through an agreement between the ENEA team and the project APHORISM ([7], headed by INGV), the CIPCast system will benefit of receiving data from the analysis of ash clouds released from ongoing volcanic eruptions after data elaboration (data coming from SEVIRI and SENTINEL satellites constellations). Time sequences of volcanic ash clouds (described in terms of density and height on the sea level) can be reproduced on the GIS map and provided to the airport control and to the Civil Aviation Authority.

3.1.2 Damage Scenario

Based on the assessments of the environmental conditions and/or occurred events, CIPCast attributes a “perturbation intensity of a given type” (according to the type of expected event and the type of physical perturbation they are able to produce) to each affected geographical point. The knowledge of the CI assets present in the perturbed area (and the corresponding vulnerability matrix, associating level of damage to the local perturbation intensity) allows producing a damage scenario, constituted by a list of the CI elements that are expected to be severely damaged by the perturbation and thus expected to fail. The damage scenario is contained in the report provided to the CI operators and to other stakeholders (see Section 3.1.5). It is then used as input to the following CIPCast modules (i.e. RecSIM) which transforms damages of CI elements into service(s) outages.

3.1.3 Impact Scenario

The task of transforming damages into service(s) outage is performed by the module called RecSIM. The RecSIM code, based on the damage scenario and the complete reproduction of the network topology of the distribution electrical network and of the other networks to which it is linked (like e.g. the telecommunication and the water networks), through the state analysis in time of the different involved resources, can predict the sequence of failures induced by the physical failure of the damaged CI elements.

To briefly explaining the main features of the algorithm running into RecSIM, it applies to a model of the interacting technological networks as described in Figure 2 (the model in Figure 2 is related only to the interaction of the electrical and the mobile telecommunication networks, for clarity).

In Figure 2 it is clear the level of details that must be achieved in the description of the electrical and the telecommunication networks:

- the electrical network is represented as a number of medium tension lines (placed among two high-to-medium Voltage transformer substation, PS) where a number of secondary substations (SS) containing medium-to-low Voltage transformers are placed;
- the telecommunication antennas (BTS) providing tele-control functions to PS and SS, with the indication of which SS is tele-controlled by its service and which SS supplies energy to it.

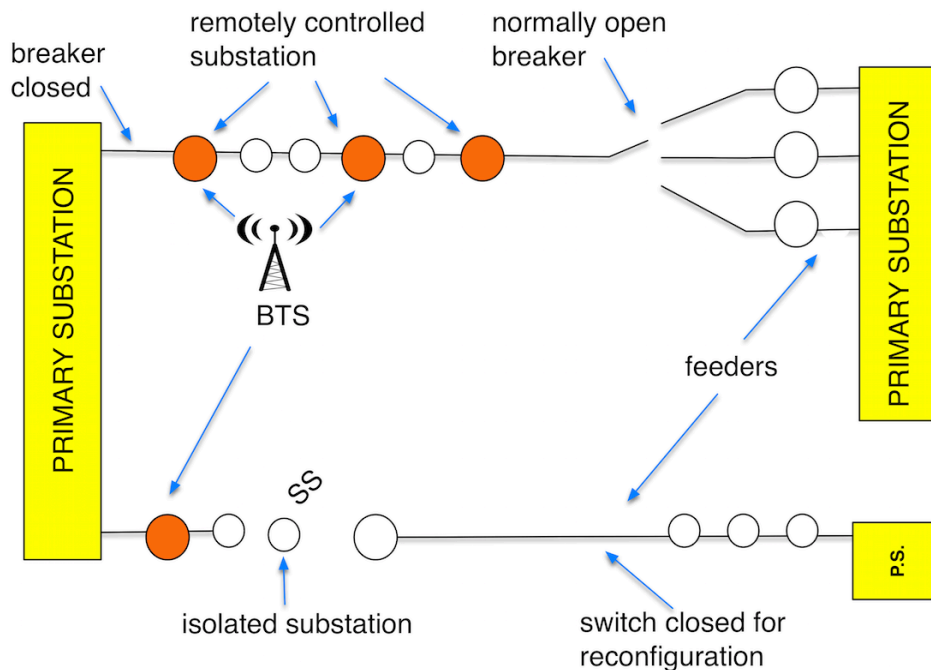


Figure 2: Typical electro-telecommunication network interaction. Legend of symbols explained in the text. (ENEA)

RecSIM estimates the cascading effects that are produced within the electrical network and outside of it (through the functional dependency link towards the other networks). The latency of cascading effects ranges from a fraction of seconds (action of the protection switches which open along the hit medium tension line) to several hours (end of electrical supply and subsequent failure of telecommunication antennas left without energy after the termination of the electrical supply provided by their electrical power generators (UPS)). All these latency times can be modulated through an appropriate input interface provided by RecSIM.

Further data that can be input from the RecSIM interface concerns with the typical times of interventions of the technical teams of the CI operator available in the field. Their number and typical times could be input in the model (at a later stage of the RecSIM development, the interventions times will be calculated based on traffic data and of their dislocation in the city area at the time of the event, by automatically estimating the travelling times from the position to that of the requested intervention).

At the end of the first step of its activity, RecSIM estimates the number and the position of all the SS which are hit by the initial (instantaneous) cascading effect, thus defining the $t=0$ list of devices which should be restored, either with tele-control actions (if possible due cascading effects possibly propagating toward other infrastructures) or manually (through the sending of a technical team on site to restore the element, through a simple action or, in case of a damaged infrastructure, through the shortcutting of the element through an electrical generator to be set on place to restore electrical continuity to the area initially served by the damaged SS).

Given these initial ($t=0$) data, RecSIM starts producing the most complex task consisting in the definition of the optimal sequence of interventions needed to solve all the problems present along the

line(s) involved in the outage, dispatching the technical teams in a way to rapidly and efficiently solving the outages.

To perform such an optimisation task, CIPCast has been provided of two optimisation functions to be minimised to produce the optimal choice among all the possible sequences of interventions¹:

- the first is related to a key indicator for the electrical operator (the Service Continuity indicator, defined as the sum of the number of the minutes of outage suffered by all electrical customers involved in the outage, measured in *kmin*, thousands of minutes)
- the second is related to the economic losses provoked by the outage due to the unavailability of primary service(s) induced by the outage (each service outage has an impact on the production of revenues different for each economic activity).

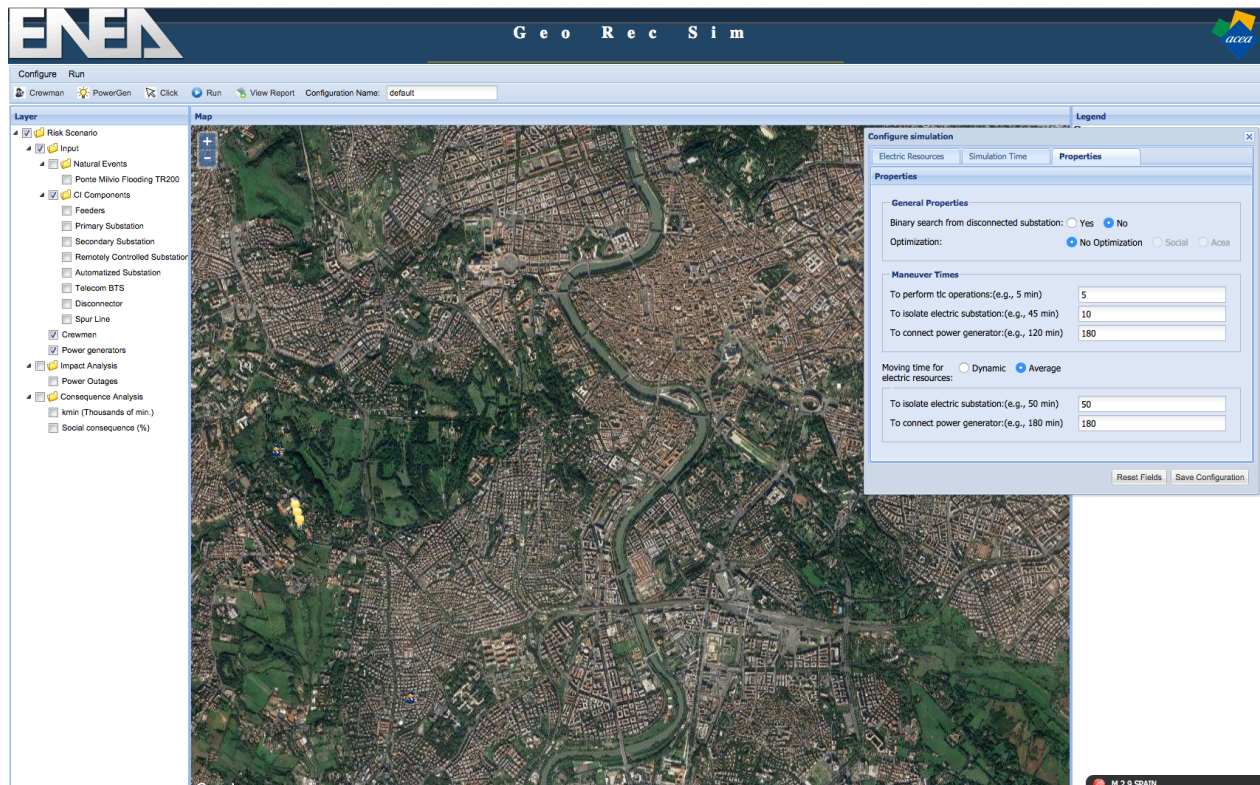


Figure 3: RecSIM interface. On the left column, the number of visible information layers; on the top right, the popup allowing the user to insert the simulation parameters (if not previously defined) such as: number of technical teams, number of electrical generators available for the crisis solution, characteristic times for the solution of a specific activity by the technical team etc.). On the left of the map, the presumed position of electrical generators (lamps, in yellow) and the current location of the technical teams (small worker icon). (ENEA)

The two optimisation properties have not been used simultaneously: the optimal sequence is usually performed first to reduce the number of *kmin* characterising the outage and then eventually recalculated on the bases of minimising the economic losses. However, it must be said that the electric grid operator by contract and under the constraints imposed by the Regulatory Agency (like, e.g., the Authority for Energy in Italy) is constrained to respond on the basis of the *kmin* optimisation. Figure 3 shows the RecSIM webGIS interface with the input window enabling the introduction of the scenario parameters.

¹ The optimal sequence of interventions must be evaluated each time the number of technical teams available in the field is smaller than the number of CI elements to be restored. In such case the dispatching sequence of the interventions is crucial for a rapid and efficient restoration that possibly minimises wealth reduction to citizens.

3.1.4 Consequence Analysis

Consequence Analysis is the module that estimates the ultimate “societal” effects of the outage of one (or more) services in a given area. This task has been performed by associating to the unavailability of primary services (such as electricity, water, telecommunications etc.) a “reduction of wealth” experienced by the different societal domains: citizens and industrial activities. Each societal sector will “perceive” the loss of one or another service in a different way: some industrial sector could be more vulnerable to the electricity loss, other to that of telecommunication or water etc. An appropriate theoretical framework has been purposely introduced to estimate the incidence of the loss of the different services on each societal sector: from citizens (classified as a function of their age and abilities) to industrial activities (classified on the base of their NACE code²).

The Consequence Analysis module starts from the identification of the relevance of the presence of services (delivered by CI) for the achievement of a “wealth” which is identified as:

- the possibility of living in ordinary conditions, with the full availability of all services (electrical power, telecommunication, water, gas, public services etc.), in the case of citizens,
- the possibility of producing the expected average amount of revenues, for the industrial activities.

The lack of each of the services supplied by CI is responsible (to a certain fraction) of reducing the level of wealth of a given sector. The extent of the produced wealth reduction is thus considered as the metric to assess the relevance of the crisis scenario: larger the wealth reduction, larger the relevance of the crisis scenario. In these cases, the optimisation procedure of RecSIM could be performed to minimise one (or both) these wealth reductions.

As previously said, a third metrics has been introduced (the *kmin*) which has been proposed by the electrical operator, being the optimisation of the value of the wealth expressed in *kmin* the only optimisation function that they are mandatory constrained to follow.

3.1.5 Web Interface

The web GIS interface has been particularly cared, taking in consideration the different requirements gathered by the end-users. The GIS interface can be customised for the different end-users, by providing clear indication of the available information layers. The interface has been cared:

- to properly present the information layers classified with a clear ontology,
- to avoid overwhelming (useless) information,
- to be easily customisable by the user to its own convenience,
- to contain buttons to launch specific applications or GIS functions (without affecting the clarity of the information layer description).

A typical web GIS interface of a service devoted to the real-time risk analysis is shown in Figure 4.

3.1.6 Report

At the end of the workflow, CIPCast drafts a report of the crisis scenario by summarising the main elements enabling to fully describe the crisis scenario. This is done in terms of:

- total duration of the outages,
- number and identification of the damaged infrastructure elements,
- number and identification of the infrastructure elements involved in the outage due to cascading effects (intra-CI or expanding to other CI different from those effectively hit by the perturbation),
- identification of the area of the city which will mainly feel the outages having sizeable consequences. As the end-user of this service is the electrical network operator, the report contains the estimated consequences on the basis of the *kmin*-metrics.

² Consequence Analysis theoretical framework has been introduced and detailed in CIPRNet deliverable D7.4.

A snapshot of a typical report is shown in Figure 5.

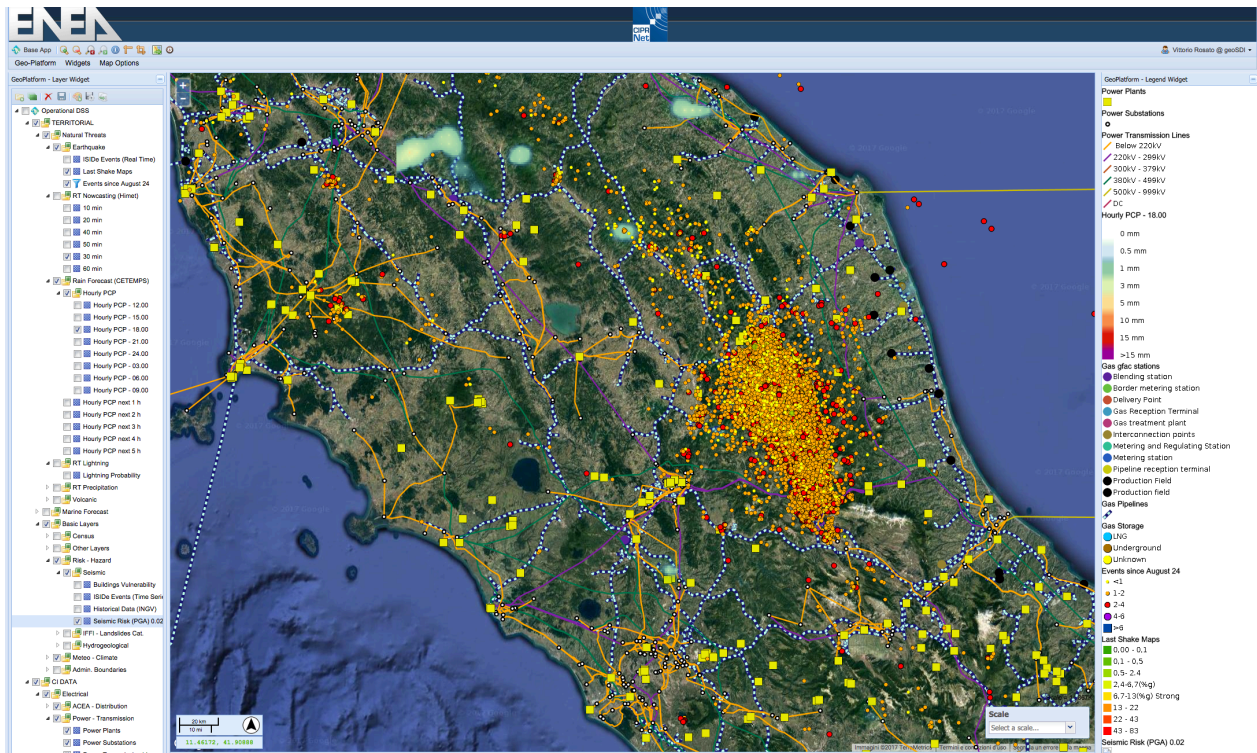


Figure 4: Web GIS interface of the real-time risk forecast operation mode of CIPCast. On the left side, the column containing the available information layers; on the right column, the legend of symbols and metrics used in the different information layers. (ENEA)

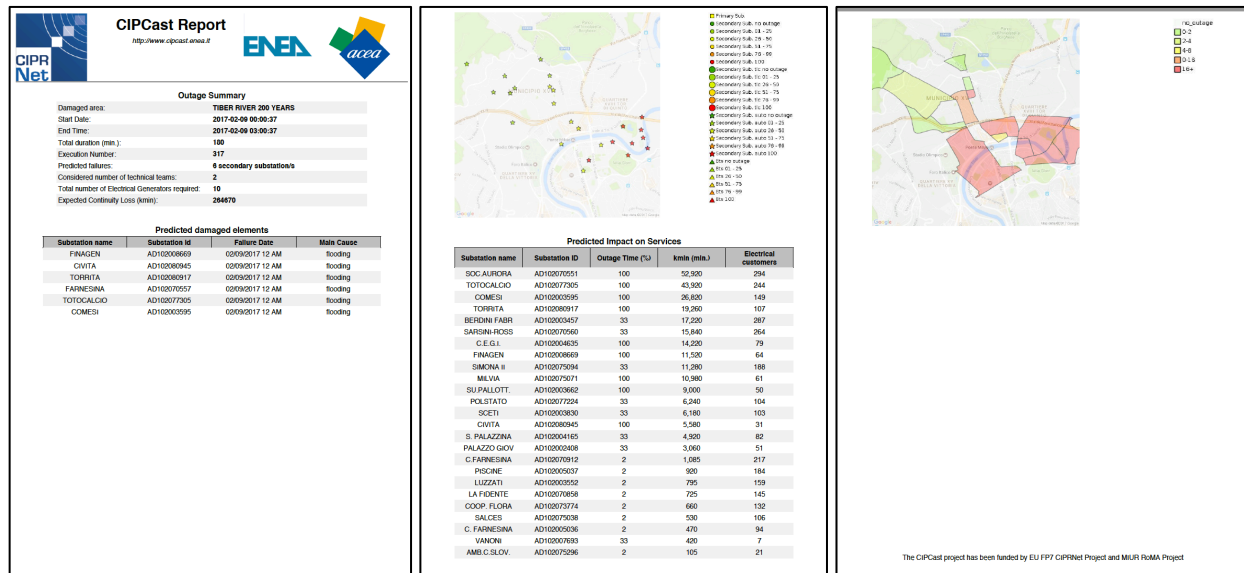


Figure 5: Typical CIPCast report containing the different sections (damage, impacts and consequences). (ENEA)

3.1.7 Data Exchange with CI operators

The topology of many networks (the most relevant is the electrical distribution network) is continuously modified (via tele-control operations); modifications essentially involve the opening/closure of switches along the different Medium Tension (MT) lines, to accommodate the capability of the network to sustain the electrical loads or to operate the network with a higher (or lower) robust-

ness. In fact, robustness (i.e. resistance to possible faults) and efficiency (i.e. reduction of power losses along the lines) anti-correlates. Thus, operators should modify the overall (or local) topology to better define the network properties. These topology variations should be communicated and inserted into the CIPCast database to allow RecSIM to simulate the outage propagation in the network that has the topology of the network in operation (thus providing the operator with a reliable assessment of the possible impact of the predicted faults).

The data flux to/from the electrical operator (Areti SpA) has been established (thanks to the compliance of the electrical DSO operating on the Regione Lazio and in the area of Roma Capitale).

A point-to-point Virtual Private Network (VPN) between the ENEA and the Areti information systems has been established (Figure 6); the VPN – using the IPsec protocol – allows a secure, robust and reliable interaction link between the CIPCast system (and its database) and the Electrical Network Management System.

The VPN IPsec connection allows to receive real-time data related to the electrical distribution network and to send various types of data (e.g. historical meteorological data, damage scenario impact analysis) to the Areti information system (Figure 6). In operation time, the data link between the CIPCast server and the Areti server will carry on the following data:

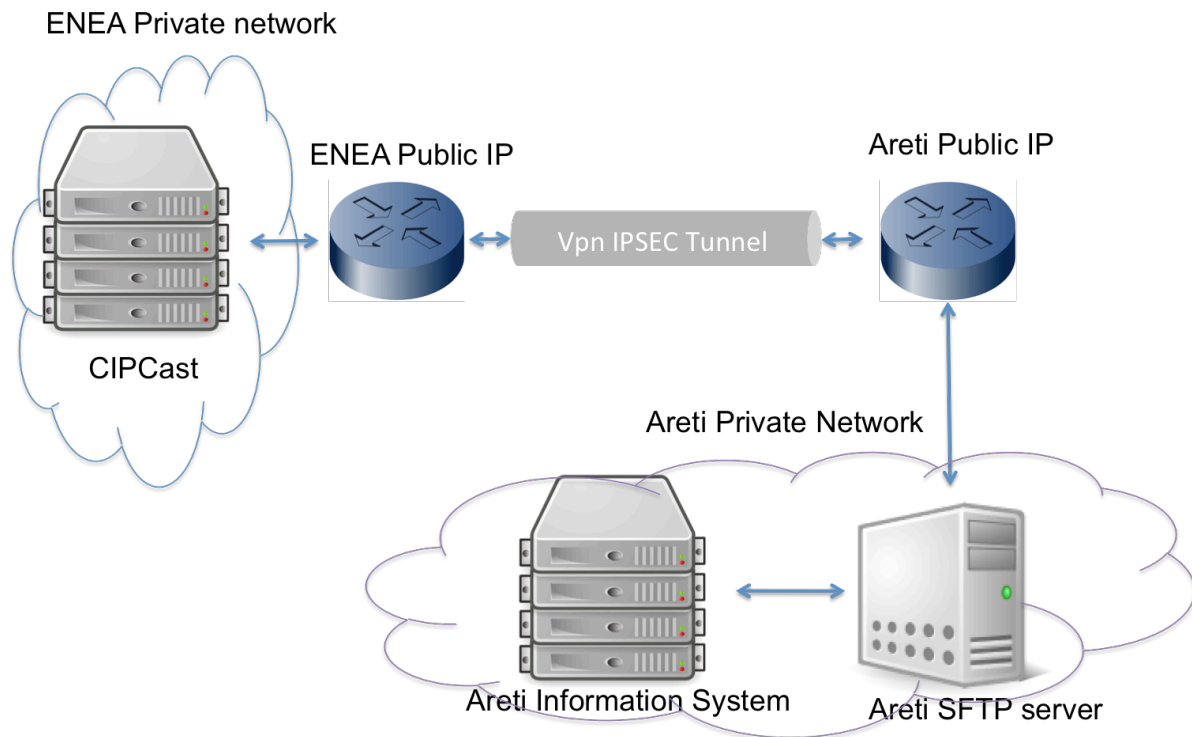


Figure 6: VPN IPsec implementation between CIPCast and Areti Servers. (ENEA)

3.1.8 Simulation Mode

One of the relevant objectives of CIPCast is its use as “Scenario builder”, i.e. the tool should realistically reproduce a hazard-related event whose impacts and consequences could be then estimated. During the course of the project and after a number on interactions with the end-users and stakeholders, it has been decided to invest a great deal of effort to reproduce earthquake scenarios. These might be extremely dramatic events producing large consequences to citizens and assets, as Italy is a land particularly exposed to earthquakes that represent a major source of threats. To date there is a great deal of attention on this domain (preparedness to seismic events, management of the aftermaths): it has been thus decided to invest most efforts to set up an advanced earthquake simulator enabling the reproduction of its effects on citizens, assets and CI. It will provide Civil Protections and CI operators a tool enabling scenario building and the preparation of appropriate contingency plan and preparedness measures.

Earthquake simulation

The application enabling the earthquake simulation has been produced by a large effort that has involved a number of ENEA partners, committed particularly in the validation and test of the resulting prediction. In fact, a major relevance has been provided to the validation of the resulting damage scenario predicted by the tool by verifying its accuracy against damages produced by events occurred in the past. The validation process has been performed by the collaboration with the Italian Institute for Environmental Research and Risk Mitigation in Prato (Tuscany Region).

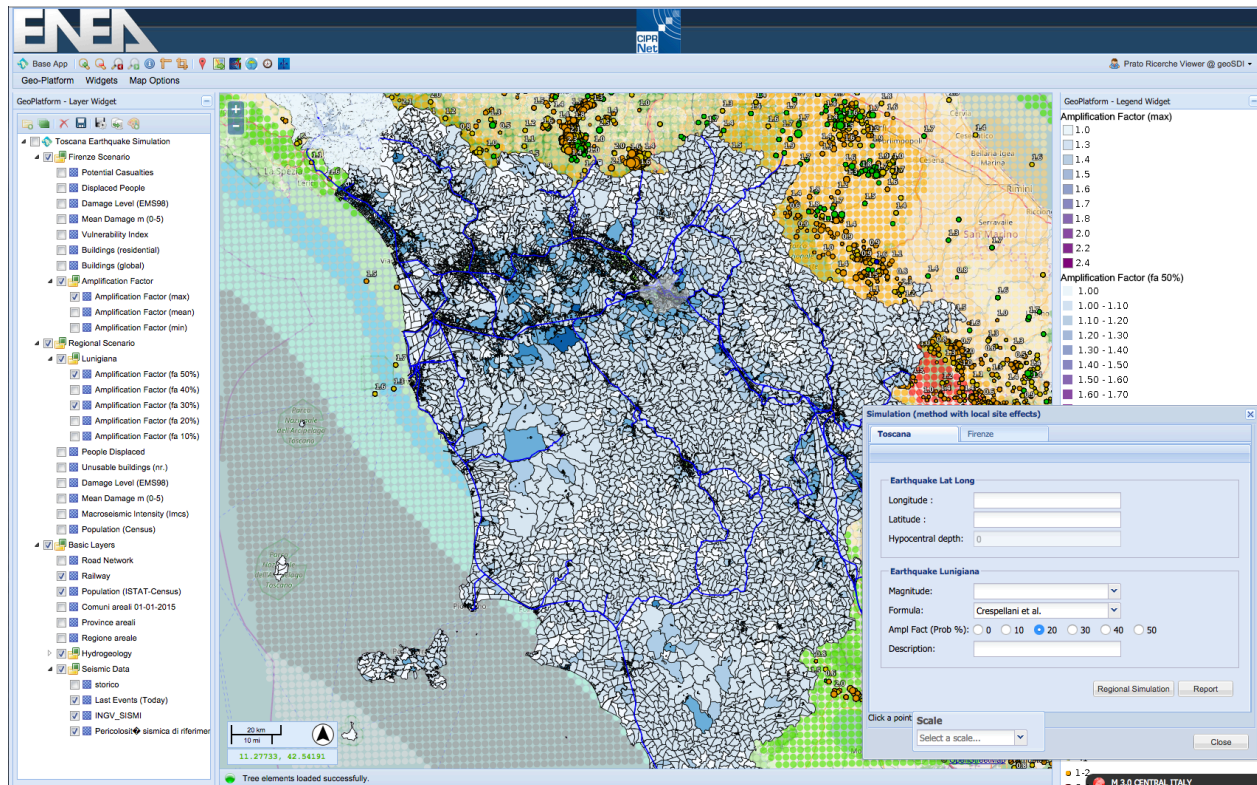


Figure 7: Web GIS interface of CIPCast in its “earthquake simulator” operation mode. In the horizontal bar are located several buttons enabling to launch the earthquake simulator (pop up containing the main data input at the lower right side). (ENEA)

They have provided the damage data recorded in several earthquakes occurred in Tuscany region during the 20th century. This has allowed tuning parameters and the choice of appropriate shock wave attenuation function to describe waves propagation in the medium. Moreover, they have provided the results of the seismic micro-zoning of the territory of the city of Florence, which has allowed to perform very accurate simulations on scenarios built on the city of Florence itself. Most of the scientific and technical work related to the setup of the model has been reported in a number of publications recently submitted to international, peer-reviewed journals [5][6].

The earthquake simulator web GIS interface is shown in Figure 7. The end user can input the epicentre coordinates, the magnitude of the shock, its depth, other than choosing the attenuation formula and the local amplification factors (if available) for a better simulation of the shock wave propagation in the medium.

It is worth noticing that, after simulation, the earthquake simulator summarises the resulting data in terms of expected number of casualties, number of citizens to be evacuated from their home, number of disrupted buildings, and number of severely damaged buildings. A GIS information layer is also associated to these figures, allowing the assessment of their geographic localisation. Aside to the social-related scenario analysis, the application allows to estimate the eventual damage to CI that, through the activation of the Impact analysis module, can also provide the expected service(s) outage, of great relevance for the setting up of the Civil Protection actions after the event.

3.1.9 Other Operational Modes

CIPCast and its application can be used for other types of applications. We will briefly describe two of them that have been already set in place for specific end-users.

1) Civil Protection application for debris volume visualisation and estimate

CIPCast has attracted much attention by the Italian National Civil Protection Department (DPC). As CIPCast is based on the same standards used by DPC for their database and as the webGIS technology used in CIPCast is the same of that used by DPC, it was straightforward to comply with the request of the Civil Protection authorities to provide them with the large number of information layers that CIPCast has collected in its database (related to the area where the earthquake started striking since August 2016).

The availability of the large set of geo-morphological data in the area and the needs to make a rapid estimate of the volumes of debris to be evacuated from the area, has induced DPC to ask the ENEA team to store, in the CIPCast database, a large number of orthophotos of the areas and the results of LIDAR campaigns performed in the area by using DPC drones and to perform (through an appropriate analysis of these data) an estimate of the debris volumes. This can be done by subtracting from the resulting DSM (Digital Surface Model) estimated on the bases of LIDAR data, the DEM (Digital Elevation Model) of the area (i.e. the estimated terrain profile with no buildings on it). See Figure 8 for details. Drones data acquisition campaigns have been performed under the DPC and the Army supervision, in full compliance with current rules for the privacy protection of citizens.

This has allowed a first relevant application of the CIPCast system in a non-conventional operation mode; however, the technology set up to comply with the DPC request is now contained in the CIPCast functionalities and it can be further deployed in case of needs by the DPC.

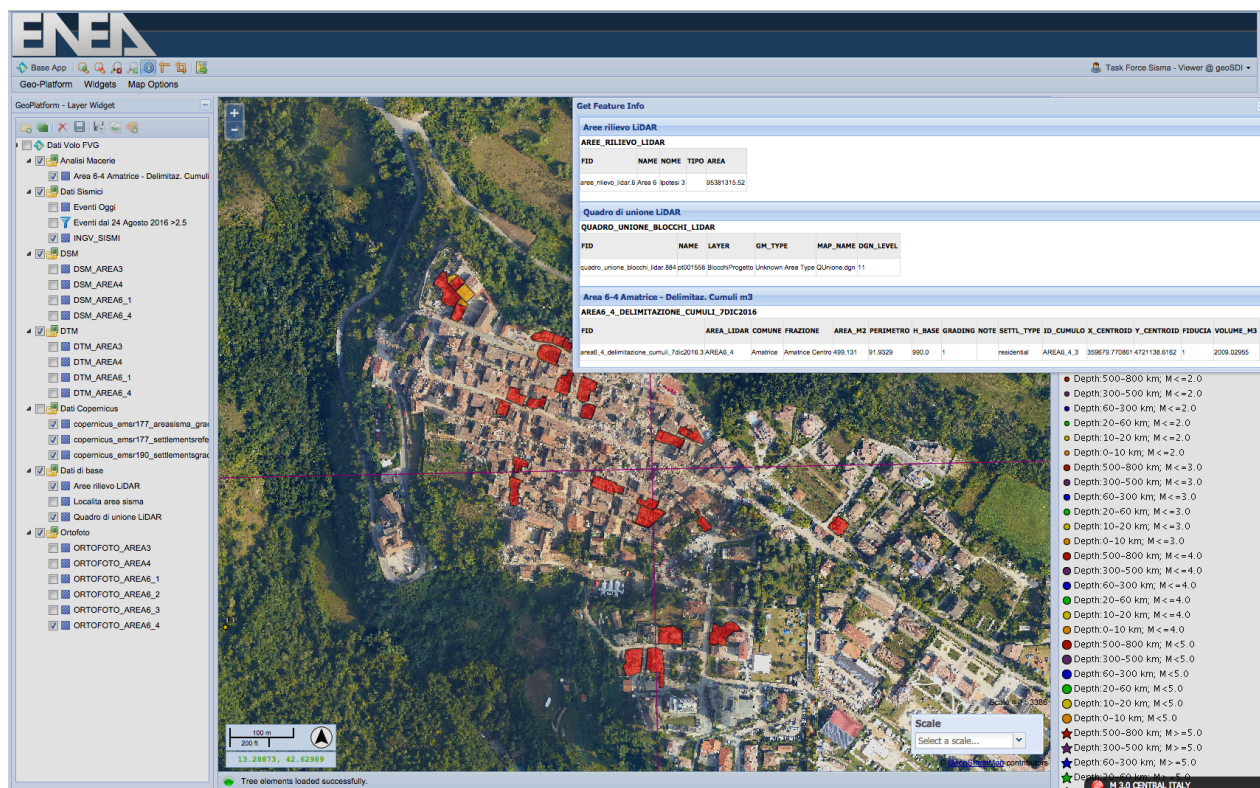


Figure 8: Web GIS interface of CIPCast in its “DPC debris volume” operation mode. On the top of a high-resolution orthophoto, there are the area (brown colour) indicated as debris areas. For each selected debris areas, the database query provides a number of data concerning the input data used for debris volume estimate and the resulting value of the volume (last figure in the bottom row of the inset).

2) Estimate of resilience variation upon technological improvement on the network

As a further model for CIPCast “vertical” deployment, CIPCast (and its component RecSIM) are going to be used as “resilience” indicator of a given technological system. This application domain has been suggested and required by the Roma Capitale electrical operator (Areti SpA) to make an overall assessment of their network, also in relation to the integration of their network within the city and the other infrastructures to which it is functionally related (i.e. the telecommunication network enabling electrical network tele-control).

The proposed metrics to achieve an estimate of the electrical network resilience has been related to the extent of outage (measured in $kmin$) that a fault of each Secondary Substation (SS) failure can produce.

As explained in Section 3.1.3, given the number of available technical teams, the number of available electrical generators, the “standard” times for the different interventions, the “normal” topology configuration of the network, RecSIM can perform different simulation by synthetically producing the failure (one at a time) of each single SS of the entire network. At the end of each simulation we could associate, to the specific faulted SS, the associated value of the crisis $kmin(SS)$ that it would produce. At the end, we will thus have a “basic” assessment of the resilience of the network (given the input parameters as above) by getting the distribution function of all the $kmin(SS)$ ($\mathcal{D}_0(kmin)$, say).

Starting from this assessment, similar assessments could be performed by making variations to one or more parameters (technologies, number of technical teams etc.) and repeating the same procedure (i.e. putting in failure, once at the time, each SS of the network). The comparison of the integral of the resulting $kmin$ distribution function will provide an indication on the extent of resilience enhancement obtained by the proposed variations.

This approach has been suggested to Areti SpA to perform extensive calculation of the efficacy of the different policies to improve the resilience of the network by using a framework which correctly allows to make such estimate “embedding” their network into the realistic “system of systems” comprising the other network to which the electrical distribution network is functionally related. An appropriate “vertical” implementation of CIPCast to perform this estimate is going to be developed.

3.1.10 Validation, test and final demo

The CIPCast tool has been running for four months in on operational configuration, with the aim of testing its functionalities and validating its predictions with respect to faults and consequences.

The demo results, extensively reported in D8.700, has described the case of a large Tiber flooding (bi-centennial flooding) which has relevance in the city administration and for the CI operators in Roma Capitale as it has a sizeable probability of occurrence during the next ten years. The test allowed verifying the robustness of the electrical network whose components, in the area, have been highly automated in a way to promptly respond to an alert situation. The test has highlighted the possibility of a reasonable fast recover of the electrical service in the area which, through cascading effects has been predicted to extend well over the flooded area) with the usage of about ten electrical generators in a time which could be as low as three hours (in case of work completions without incidents or other unexpected causes of delays).

A similar demo has been proposed to Roma Capitale Civil Protection, who had also required the bi-centennial flooding scenario as test for the CIPCast capabilities. The demo has been extremely well welcomed; as a consequence of the awareness of the CIPCast capabilities, the Civil Protection has committed to ENEA a test (to be initially carried out in a single Rome borough) on the usability of the buildings and the lifelines selected by the Civil Protection in case of large emergencies (earthquakes, large flooding, other severe events implying the use of Civil Protection emergency measures).

3.2 ‘What if’ analysis for exploring different courses of action (Fraunhofer)

3.2.1 Introduction

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

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

CIPRTrainer is the software system developed by CIPRNet that realises this new capability. It enables crisis managers to train decision-making in crises involving cascading effects of CI. At the front end, the prototypical training system presents itself to the user as a single-page web application. Its backend includes a federated simulation of three independent CI simulators, a scenario database, a consequence analysis module, a complex event processor, and a threat simulation (flooding) [1].

One design goal of CIPRTrainer was a wide applicability of the system, including crisis situations with cross-border effects. We picked a region spanning both sides of the border of two countries represented in the CIPRNet consortium: Germany and The Netherlands. The geographical location is restricted to the Kleve district in Germany and the city region of Arnhem-Nijmegen in the Netherlands (Figure 9). The area is prone to flooding by high water levels of the river Rhine. Also, it contains a number of infrastructures, like the railway line connecting Rotterdam harbour with the European hinterland, including the harbour of Genoa in the Mediterranean Sea. It is the most important cargo train line in Europe. In this setting we designed two storylines in a complex scenario with cross-border effects [3]: A cargo train derailment in a German city and an extended flooding of the river Rhine in the considered area.



Figure 9: Region of the Dutch-German cross-border scenario. (Fraunhofer)

3.2.2 Scenario design and modelling

Data are the basis for modelling the scenario on the computer. Before we started the development of the scenario, we performed own research on information on CI and data from the considered region. For realising the scenarios for CIPRTrainer, we included electricity networks (power transmission and distribution), telecommunication including Internet, and railway infrastructure. Some of the modelled CI networks (power distribution and telecommunication) are fictive for two reasons: first, we did not have data on some of these networks and second, for security reasons, since we did not want to disclose sensitive information. For the modelling of CI and of threats, we employed the domain expertise of the consortium, including electrical and telecommunications engineers, security professionals, and experts in railway security, cyber security, crisis management, and the water domain. External expertise was provided by the head of the fire fighters in a large city, and experts from CIPRNet’s international advisory board.

CIPRTrainer is a distributed heterogeneous system, i.e. it consists of a couple of independent systems and components that communicate with each other. Therefore, modelling in CIPRTrainer is also heterogeneous and takes place in several of its components. Figure 10 shows a simplified scheme of CIPRTrainer's main components. On the highest level, CIPRTrainer consists of just two building blocks: a design engine and a training engine. The design engine is based on the Fraunhofer tool SyMo, shown in the upper left of Figure 10. All other blocks in Figure 10 belong to CIPRTrainer's training engine, which will be explained a bit later.

The scenario modelling starts with creating a static scenario model in SyMo. This scenario model, similar to an ontology, describes the elements of the scenario. It contains classes (types) and instances of model elements like involved disaster area, incident elements, responders, response actions, etc. More detailed descriptions about the content of a scenario are discussed in a publication on the knowledge-driven modelling approach for CIP scenario development [2]. The design engine exports scenario models as plain scenario files, which are stored in a database and then are further enriched by rules, CI dependency information, and more. The CI dependency information is required for enabling the modelling and simulation of cascading effects, i.e. the propagation of failures from one CI to a dependent CI.

Relevant CIPRTrainer components for further modelling are:

- The CIPRTrainer database (❷ in Figure 10), containing the scenario file (❶ in Figure 10, produced by the design engine) and other data;
- The federation of CI simulators, each of which has its own (CI) model (❸ in Figure 10);
- The flooding simulator that uses pre-computed flooding models (also ❸ in Figure 10).

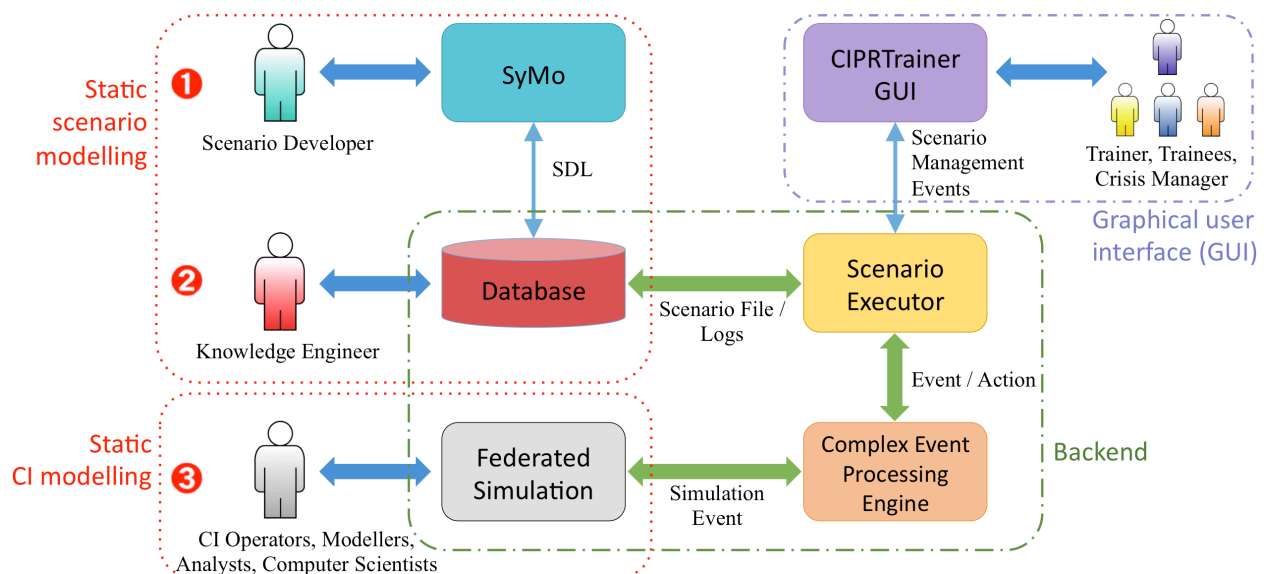


Figure 10: Simplified scheme of CIPRTrainer's main components. The design engine is represented by the block labelled "SyMo". All other shown components belong to CIPRTrainer's training engine. The most important element for users of CIPRTrainer is the CIPRTrainer Graphical User Interface (GUI), through which both trainer and trainees operate CIPRTrainer. As written in deliverables D6.3 and D6.4, two of the modelling activities for setting up the scenarios take place in the Federated Simulation part (Critical Infrastructure models) and in the Database part (definition of events, rules, and CI dependencies) (Fraunhofer)

In addition to the model elements mentioned above, the CIPRTrainer database contains also the socio-economic data for the consequence analysis, translation tables for the notions and phrases that are textual elements of the scenario and of the GUI, and a description of a scenario's storyline. The storyline consists of situation information (weather, time of day, etc.), representations of events that happen in the simulated crisis scenario, and rules. The representation of an 'event' consists of a time stamp, a textual description of the event, and other involved scenario elements. Rules consist of a condition that needs to be fulfilled and events that may or may not occur in the storyline, depending on if the condition is fulfilled. Rules introduce some variability in the training, since

they are employed for preventing some damaging events from happening in case the responders (trainees) perform the right actions at the right point in time with the right number of resources.

For achieving a plausible simulation of the behaviour of CI under severe perturbations, including failures and cascading effects that propagate failures to other dependent CI, CIPRTrainer employs two commercial simulators (SIEMENS PSS© SINCAL for electricity networks and OpenTrack for railway networks) and one free simulator (ns-3 for telecommunication networks). The modelling of the CI can be done separately in each of the component simulators. Figure 11 shows the artificial electricity network for a city in the scenario area as displayed on SINCAL's separate GUI. Information on dependencies between interconnected infrastructures, like which electricity CI element supplies which telecommunication CI element with power, are stored in CIPRTrainer's database.

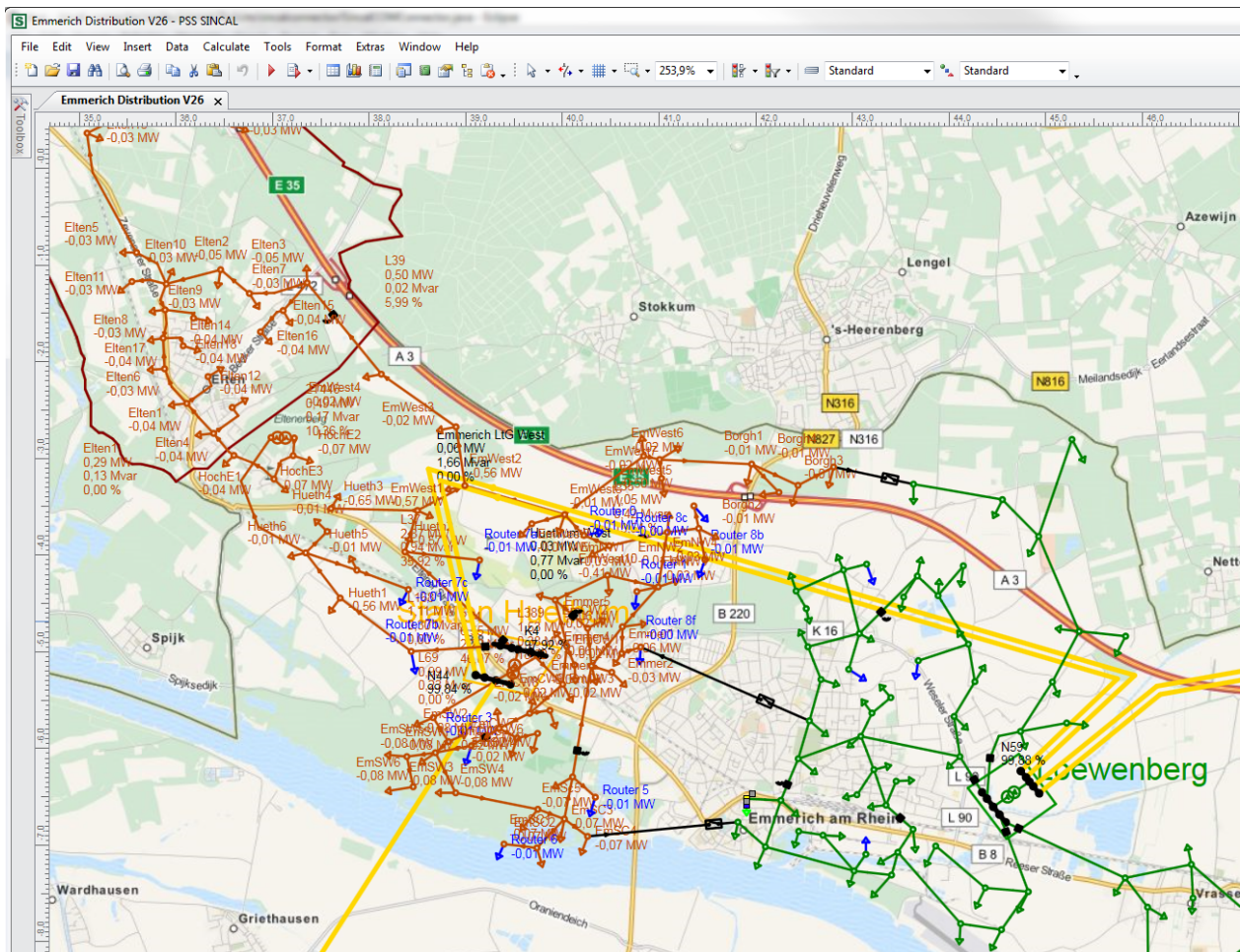


Figure 11: Screenshot of the PSS©SINCAL software. The graphical user interface shows the elements of the electricity distribution and transport network and their interconnections. The view can be enriched with geographical maps to support the modelling of real-world conditions. (Fraunhofer, Siemens)

CIPRTrainer employs two different threat simulations. For the cargo train derailment, it uses a simulation of the sprawl of a toxic gas cloud that emerges from a damaged and burning tank car. The data have been provided by the Analytical Task Force of the fire fighters of a German city (Figure 12, left). For the flooding of the river Rhine, CIPRTrainer gets flooding models from a server of CIPRNet partner Deltares. For simulating the flooding of the river Rhine, CIPRTrainer gets data from a server of CIPRNet partner Deltares. These data have been produced by sophisticated flood simulations provided by the Dutch Water Board Rijn en IJssel, based on models created by the EU project VIKING. The provider has computed several different water sprawl models that differ in the location of assumed dike breaches. Due to the high fidelity of the flood model, the duration of such a flooding (several days), and the extended flooding area, each model computation takes several days, which prohibits real-time simulation. Deltares' server provides pre-computed shape files that can be read by CIPRTrainer's GIS component (Figure 12, right).

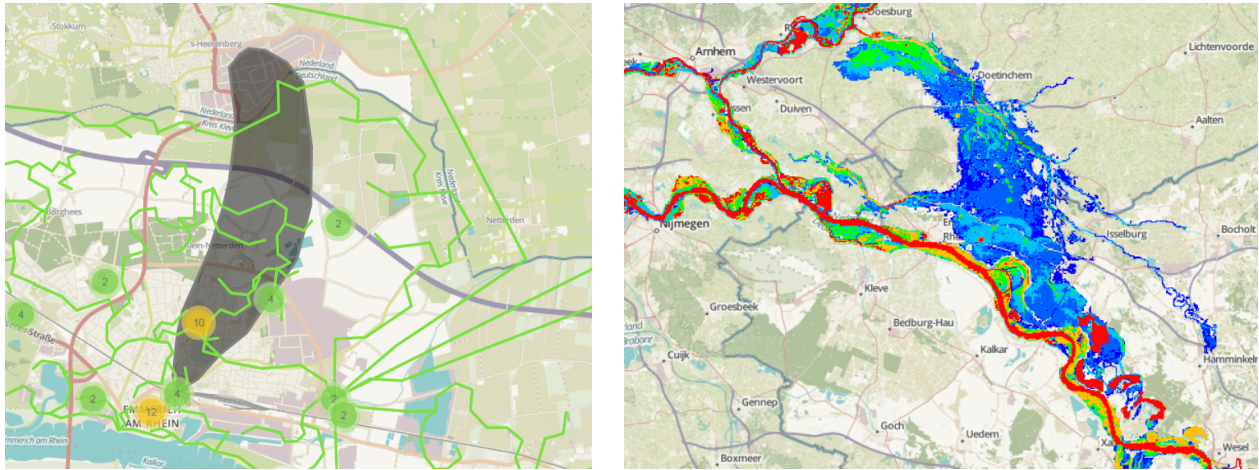


Figure 12: left: section of a screenshot of CIPRTrainer showing the simulated sprawl of a gas cloud. The green lines are power lines. Right: section of a screenshot of CIPRTrainer showing the simulated flooding of the Rhine. Primary colours (red, orange, blue, green) indicate different water levels. (Fraunhofer, Deltares)

3.2.3 Federated simulation in CIPRTrainer

For achieving a plausible simulation of the behaviour of CI under perturbations, including failures and cascading effects that propagate failures to other dependent CI, CIPRTrainer employs the independent simulators SIEMENS PSS© SINCAL, OpenTrack, and ns-3.

All these simulators are supplied with the models of CI in the scenario area, which are either real or realistic artificial CI models. Information on dependencies between interconnected infrastructures, like which electricity CI element supplies which telecommunication CI element with power, are stored in a database. A failure of the former element triggers a stressed state or failure of the latter element. This is implemented using simple rules like “if cabinet feeder X is inactive, router Y is inactive”. Such state changes are represented by software ‘events’ in CIPRTrainer. Each of the simulators is connected to the rest of the CIPRTrainer system by a special ‘adaptor’ that translates ‘events’ into a format that the simulator can understand. Such a setup of connected stand-alone simulators is called a federated simulation (Figure 13).

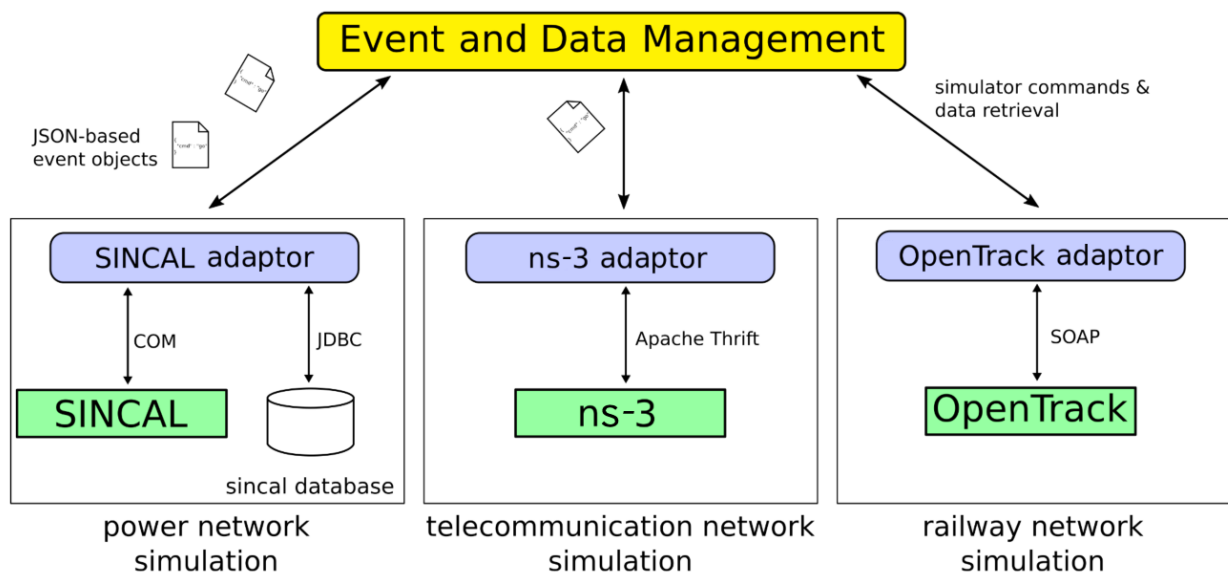


Figure 13: The simulator adaptors (violet colour) implemented for the CIPRTrainer with their connection to the specific simulators (green colour) and to the Complex Event Processing component (yellow colour) (Fraunhofer)

The ‘adaptors’ are also employed for synchronising the simulators and for enabling the rollback, that is, the ‘going back in time’, and for providing basic functionality like starting, pausing, resuming, and stopping a simulator. This altogether is called a federated simulation middleware that establishes interoperability between stand-alone simulators, which were not primarily designed for exchanging data with other simulators in a larger context. A detailed analysis of the state-of-the-art in federated simulation is provided in [16].

The orchestrators of CIPRTrainer are the Complex Event Processor (CEP) and the Scenario Executor (SE) components (Figure 10). The CEP handles the common ‘events’ communication data format. It triggers simulator functions, based on the time-stamped entries in the scenario file, or on user actions, or on rules the conditions of which are fulfilled, or on ‘events’ sent by simulators or other CIPRTrainer components. A more in-depth description of CIPRTrainer’s federated simulation please find in [30].

3.2.4 Realising ‘what if’ analysis with consequence analysis in CIPRTrainer

The new »what if« analysis capability enables trainees to explore different courses of CM actions in computer-based simulation (Figure 14). CIPRTrainer displays information on events that happen in the simulation, like a derailment of a cargo train. The system has an inventory of actions available for reacting on the occurring events. Rules within CIPRTrainer provide some additional flexibility. For instance, if a certain response action is being performed by the trainee within a given time window, then it would prevent some disastrous event from happening.

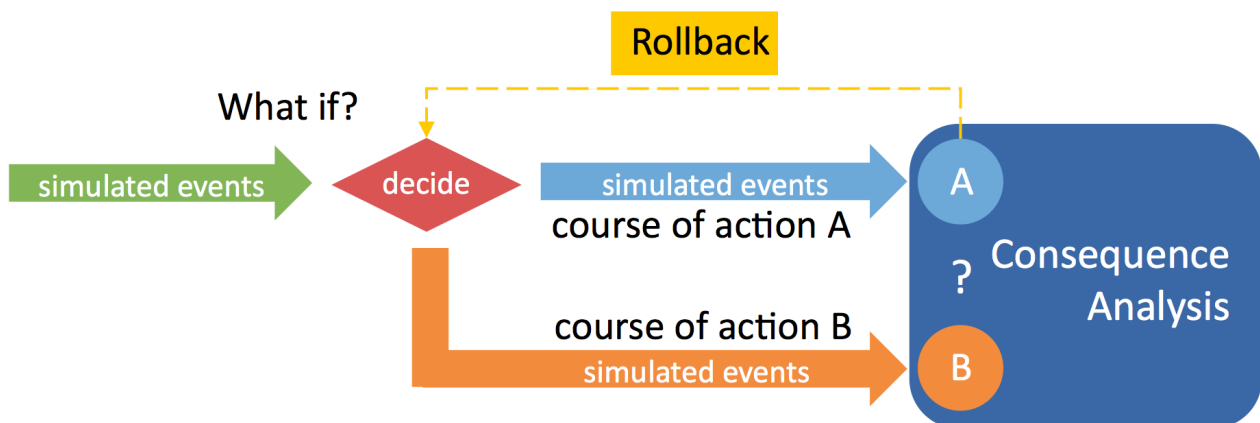


Figure 14: »What if« analysis: After taking course of action A, roll back to decision point, and take different course of action B. Use consequence analysis to compare the overall consequences of both scenario evolutions (Fraunhofer)

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

Such rollbacks can be performed multiple times. Since the history of all performed actions is recorded, the generated courses of actions form a tree-like structure, with the initial situation as a root. CIPRTrainer can display this structure for providing an overview of the training activities (Figure 15). The courses of action are represented by branches in the tree structure consisting of the sequences of those actions that the trainees executed.

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

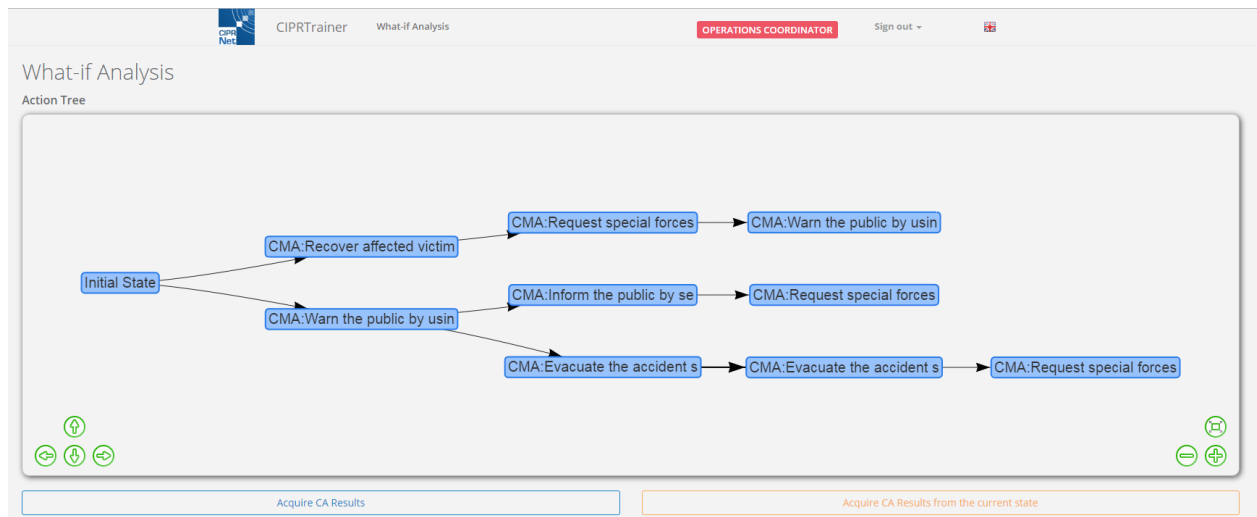


Figure 15: Tree-like representation of the courses of action that a trainee has explored. In the above example, the trainee jumped back in time twice, yielding three different courses of action. At the bottom of the figure, the buttons for initiating the consequence analysis computation are shown (“Acquire CA results”). (Fraunhofer)

3.2.5 Consequence analysis in CIPRTrainer

After having explored at least two different courses of action, trainees can perform ‘what if’ analysis. To find out which course of action contributed in a beneficial way to keeping the overall consequences low, the trainee can compare the consequences of the scenario evolution considering the effects of the taken courses of action.

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

There are three types of such methods: a) for direct consequences of specific (natural) hazards, like building damage caused by floods or storms; b) more general methods for loss of life [5]; and damage to property; and c) methods for indirect economic damage through the possible inoperability of (critical) infrastructure and economic sectors (input-output-model). The CAM estimates and provides the damages in two major categories: “human” and “economic”. As an ethical principle, both categories are kept separate to not value human lives in terms of money or other assets. Both categories have subcategories, for instance, “human” has the subcategories “injured” and “dead”.

The trainee can request consequence analysis results for all courses of action explored in the current training session. By selecting the command “Acquire CA results” (Figure 15), the trainee invokes the CAM. The CAM sends its results to the CIPRTrainer GUI to be displayed for the trainee. The GUI can display the consequences in three different ways: a) a tabular / textual representation; b) a geographically mapped and color-coded presentation; and c) a diagrammatic presentation, which is the easiest way for comparing the results (Figure 16). The side-by-side display of the consequences for all courses of action allows also direct comparison of consequences, like in which course of actions occur the least fatalities. Please note that a potential ethical issue could be that a user may weigh human losses against economic damage. It remains the utmost responsibility of the human end-user to comply with ethical standards.

An in-depth description of CIPRTrainer’s CA methods please find in [30].



Figure 16: Graphical visualisation of the results of the Consequence Analysis. The upper row compares consequences of courses of action by damage category (upper left for “human damages”, upper right for “economic damages”). The lower row shows consequences per course of action (lower left for “human damages”, lower right for “economic damages”) (Fraunhofer)

3.2.6 CIPRTrainer’s training concept

CIPRTrainer supports training a small crisis management (CM) team consisting of four trainees with different roles and action possibilities, including one offline trainee as head of the CM team. The four trainees represent a simplified general crisis management team, consisting of a decision-taker / situational awareness staff person, a lead person for responders, and a lead person for the local administration (Figure 17, left). For each of the roles, a specific set of actions can be performed in simulation. CIPRNet has chosen this approach for supporting the wide applicability of CIPRTrainer. A study of the EU project PREDICT showed that, although the CM governance structures in different countries vary to a great extent, there are some common roles of CM staff. CIPRTrainer supports the most essential of these roles. The small CM team is instructed to perform the repeated cycle of situation update, analysis, decision-taking, and action that is common in many CM scenarios. Situational Awareness observes the situation and convenes the CM team when the situation requires further action. In such an instance, the simulation is halted, and the CM team analyses the situation and pro-poses adequate response. The decision-taker decides upon the response. After the decision is taken, Situation Awareness resumes the simulation and the team executes the actions in CIPRTrainer that have been required by the decision-taker (Figure 17, right).

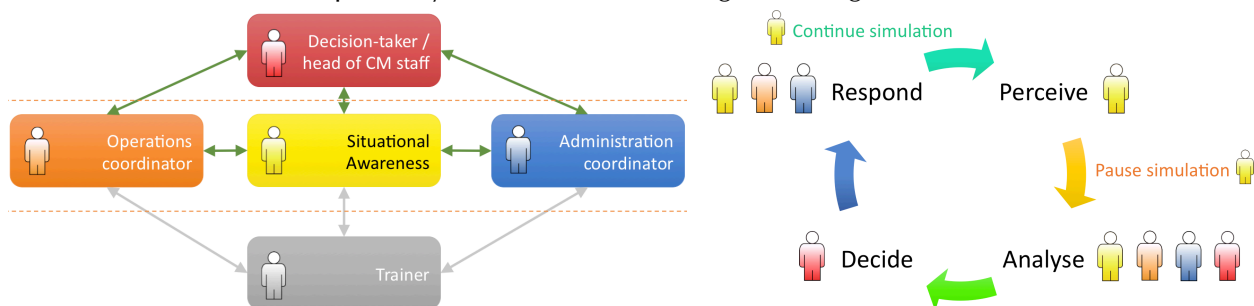


Figure 17: left: trainer and the crisis management team consisting of four persons: Situational awareness, operations coordinator, and administrative coordinator who operate CIPRTrainer; the decision-taker commands the team offline; right: Interaction of the CM team with CIPRTrainer, consisting of repeated cycles of perceiving the situation changes, analysing a new situation, deciding upon adequate actions, and responding accordingly. (Fraunhofer)

3.2.7 CIPRTrainer's graphical user interface

CIPRTrainer has been equipped with a web-based localised graphical user interface (GUI), providing menus in several languages. Figure 18 shows the trainer dashboard of CIPRTrainer, displaying that the three trainees of the CM team have logged in.

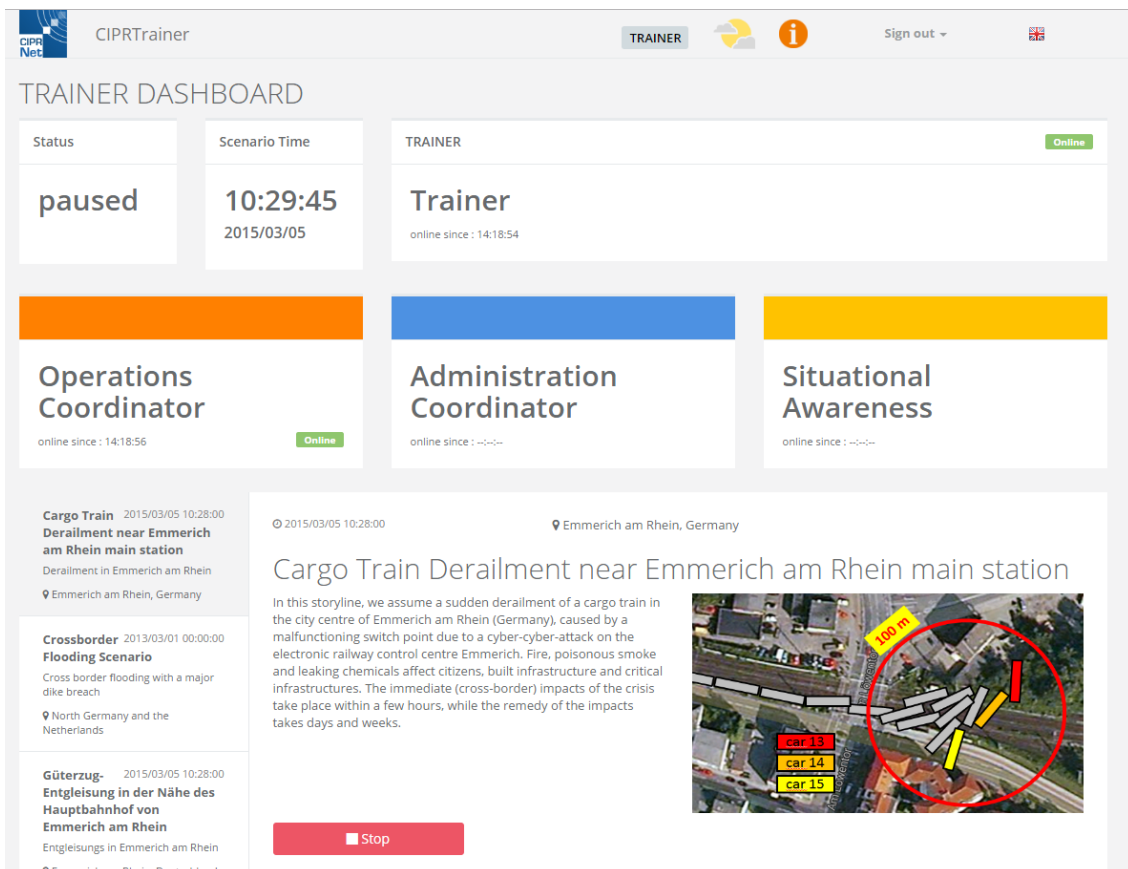


Figure 18: Graphical user interface of the demonstrator of the federated CIP MS&A based 'what if' analysis (CIPRTrainer). The screenshot shows the trainer dashboard, indicating that three trainees are online.

CIPRTrainer uses two sets of tactical CM icons (German and Dutch) for the cross-border scenario. Since In the CM icons are not internationally standardised, it is difficult for CM staff to recognise foreign icons. In the Dutch CIPRTrainer localisation, it is possible to see the Dutch icons on both sides of the border, since CIPRTrainer has an icon translation table (Figure 19). This table is an idea of the EU project FORTRESS and has been extended and updated as a result of cooperation between FORTRESS and CIPRNet. It facilitates identifying which forces or resources from the other country could be used in the local crisis or disaster.

Icon (Dutch)	Name (Dutch)	Name (English)	Name (German)	Icon (German)
	Ambulance post	Ambulance station	Rettungsdienst	
	Brandweerkazerne	Fire station	Feuerwehr	
		Technical relief station	Technisches Hilfswerk	
	Meldkamer; alarmcentrale	Emergency call center; dispatch room; command room	Notrufzentrale / Leitstelle	
	Politiebureau	Police station	Polizeistation	
	Treinstation	Train station	Bahnhof	

Figure 19: Part of the translation table (Dutch, English, German) of CM notions, tactical icons and their designations. (CIPRNet and FORTRESS)

The essential means of CIPRTrainer for displaying situational information on the crisis are maps. That is, CIPRTrainer uses known functions from GIS, like basic map layers and additional information layers for displaying regional maps, CI networks, positions of hospitals, police stations, and more (Figure 20). When the simulation runs, events are shown in a timeline (Figure 21).

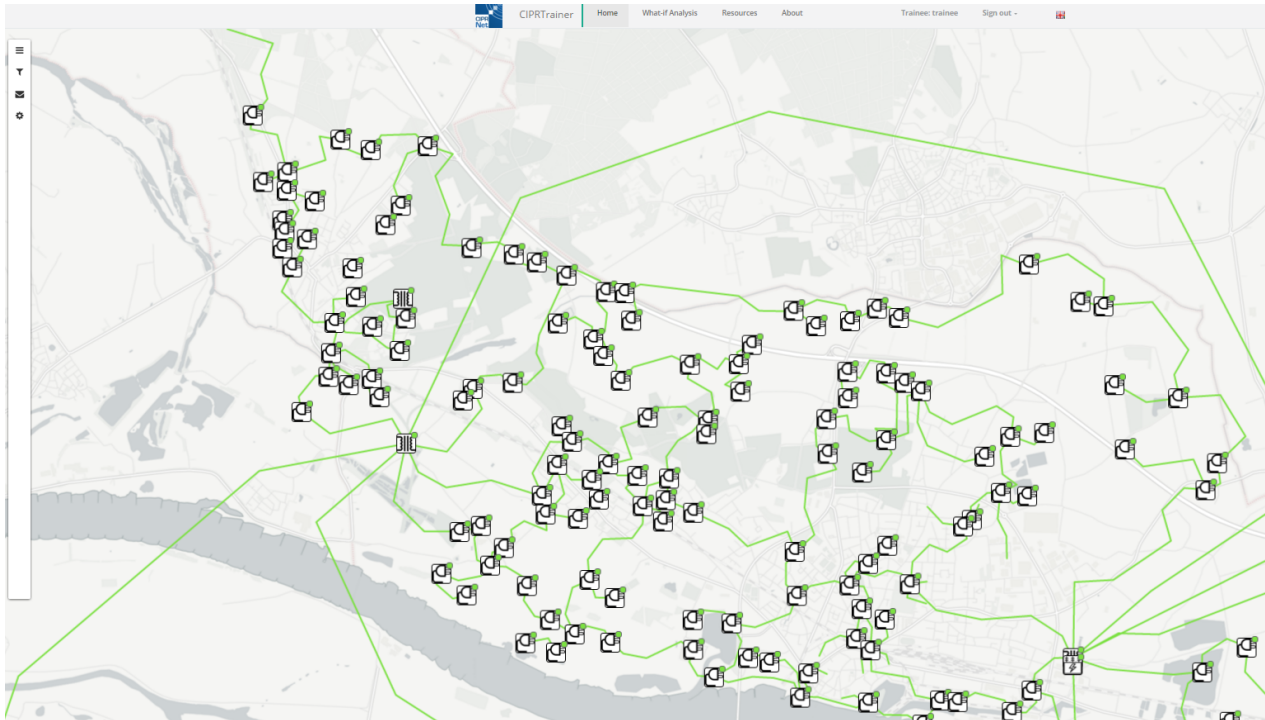


Figure 20: GIS functionality of CIPRTrainer: Information layer showing artificial telecommunication network. Green lines and green 'LED's at router icons indicate that the network is fully functioning. (Fraunhofer)

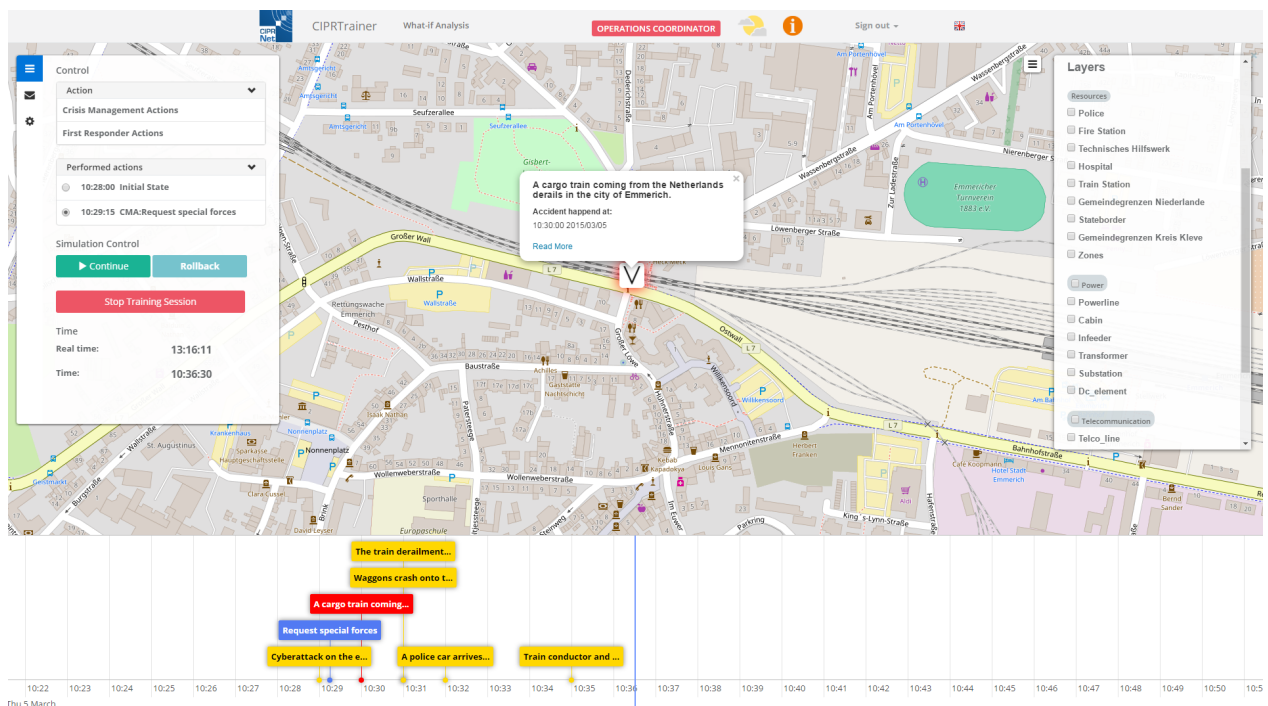


Figure 21: CIPRTrainer GUI showing the situation for the trainee 'Operations coordinator'. Control panel (left), GIS layers (right), timeline with events (bottom), events on map (centre). (Fraunhofer)

3.2.8 Interface to CIPCast/RecSIM

CIPRNet also achieved the integration of CIPCast and CIPRTrainer. The two systems can be used in different phases of the crisis management cycle. For example, in the crisis response phase CIPCast can be used to forecast extreme natural events (e.g. heavy rainfall) on a specific area. CIPRTrainer, starting from the damage scenario produced by CIPCast, can be used to analyse the different possible mitigation strategies. On the other hand, during the crisis preparation phase CIPCast can be used to simulate synthetic events (e.g. an earthquake in a specific area) and to assess their impacts and consequences. CIPRTrainer can be used to analyse various possible strategies that can be used to face the crisis. The integration implementation consisted of two steps:

1. Modelling of the Emmerich electrical distribution grid in RecSIM;
2. Implementation of RESTful API to allow CIPRTrainer using RecSIM.

3.2.9 Validation, test and final demo

CIPRTrainer has been demonstrated at three occasions, and there have been three dedicated training events where participants could perform hands-on exercises with CIPRTrainer. The latter ones were the CIPRNet Course 3 in Rome, the Master Class 3 in Sankt Augustin (Figure 22), and an additional training event in Sankt Augustin for German stakeholders BBK, AKNZ, BNetzA, and KaVoMa (see D8.700 for details)³. At each of the events, the consortium received feedback on the CIPRTrainer prototype, which helped to evolve CIPRTrainer.



Figure 22: Participants of the CIPRNet Master Class 3 in Sankt Augustin (2016) practising with CIPRTrainer. (Fraunhofer)

CIPRNet gathered feedback from its training events in a structured way, by means of questionnaires. At the CIPRNet course in Rome, the team used the general questionnaires on the event for getting feedback. For the Master Class 3, the consortium developed a comprehensive set of questionnaires, which also takes into account the different types of stakeholders (operations, crisis man-

³ AKNZ (Akademie für Krisenmanagement, Notfallplanung und Zivilschutz), the German Academy for Crisis Management, Emergency Planning and Civil Protection, associated to BBK; Bundesnetzagentur (BNetzA, Federal Network Agency); KaVoMa, a degree course at the University of Bonn on Disaster Prevention and Management.

agement, trainer). The same questionnaires have also been used at the extra training event in Sankt Augustin. Almost thirty questionnaires have been returned. They have been analysed and the results documented in a project report. The feedback was generally positive. The most requested feature of CIPRTrainer has been a clearer feedback on the success or failure of the executed user actions.

3.3 Supporting the secure design of Next Generation Infrastructures

Modelling, Simulation and Analysis (MS&A) technologies allow designers of Next Generation Infrastructures (NGI) to experiment with different architectures and to explore the effect of various design choices including the security architecture. MS&A allows assessing various options amongst different conditions, for instance varying in cyber threats, climate change effects, and other challenges. MS&A of (critical) infrastructures, their dependencies, vulnerabilities and related risk to the population may provide insight in the pros and cons of the various zoning options. The visualisation that MS&A provides may show benefits or disadvantages from the various options to all stakeholders. Therefore, CIPRNet started with the idea that the design of NGI requires new infrastructure models and efforts to federate existing infrastructure models and investigated in how the CI Protection and Resilience (CIR) CIP/CIR community may support developers of Next Generation Infrastructures (NGI):

- to validate the robustness of their architecture and resilience of the design,
- to verify the robustness and resilience of the NGI with respect to its critical dependencies with other Critical Infrastructures (CI),
- to validate the effectiveness of NGI emergency management processes in relation to new emergency challenges related to the NGI structure and CI dependencies.

As described in D5.5, extensive discussions with both the NGI research communities and (critical) infrastructure operators made clear that the design of NGI mostly uses single fine-grained technical models at the one end of the spectrum, or coarse grain (EU-wide) grid assessment models with a nation being a grid node.

When looking at the life cycle of infrastructures on the one hand, NGI stakeholders either look at the design and planning phase of infrastructures, and at the modelling of optimising maintenance of infrastructures from a cost perspective. Security aspects that are covered focus on the physical protection, and the security of supply of the service from a capacity-based point of view. On the other hand, the federated models that are used by, for instance, the CIPRNet community, mostly address the prevention, preparation, response and recovery phases of crisis management.

Currently, both communities are less overlapping than expected. On the other hand, the similar challenges have been encountered – often in between the lines – in the discussions with people in both communities:

1. Availability of data. It is often hard to acquire sensitive detailed data on the one hand, and to ask for the proper granularity of data for a proper model outcome on the other hand.
2. The cyber component in infrastructure and the cyber security of cyber-physical systems in (critical) infrastructures are hard to model, e.g. smart grids.
3. NGI often looks at the economic impact of infrastructure design and infrastructure use and maintenance redesign. The interaction of these economic models less often takes place in the realm of crisis management support, but could help in what-if analysis during the preparation and recovery phases.
4. Validation of models is not easy as there is a lack of proper reference data sets and studied outcomes.

Therefore, lessons have been identified and included in the long-term planning of activities beyond CIPRNet's project duration:

- *include human behaviour*: for the design of NGI the modelling of future human behavioural aspects is essential.

- *include economic aspects*: in developing NGI other aspects than security and protection are important, e.g. efficiency, viability or sustainability, maintenance and aging versus replacement or modality change, and market behaviour (e.g. life-cycle costing).
- *further develop knowledge brokerage*: to further develop the outreach to the NGI community, the VCCC website could provide special attention to dimensions that cover the main issues for the NGI community: technical, security, legal, economical, and organisational.

3.4 The VCCC Services

3.4.1 The VCCC services framework

The VCCC has been brought to life by implementing CIPRNet's agenda of research and technological development (RTD), training, and dissemination activities.

All CIPRNet activities were strongly oriented towards its initial audiences. Therefore, all these activities could also be considered being services to these initial audiences, where 'service' has a broad meaning. The RTD activities were aimed at realising new capabilities for CIPRNet's initial audiences. Training activities served capacity building in the multi-disciplinary community by training young researchers, professionals in civil security / CIP / CIR, and other stakeholders. Dissemination activities had a broad scope, including dissemination of research results to the scientific communities, targeted stakeholder contacts for disseminating CIPRNet's plans, but also for seeking advice for realising new capabilities and other VCCC services. Focused collaboration workshops and information for the general public complete CIPRNet's spectrum of dissemination activities.

The consortium has chosen a service framework for describing the offerings of the VCCC to its initial audiences, using a broad understanding of the notion of a 'service'. For instance, training and dissemination activities are services that CIPRNet has offered to its audiences. Other services are web based repositories (like a database of CIP related research projects) or facilities (like CIPedia© or demonstration services of CIPRNet's new capabilities). Using a service framework facilitated also formulating a business plan, i.e. the planned offerings of EISAC to its audiences. The following table shows CIPRNet's VCCC service framework.

Table 1: CIPRNet's VCCC services framework. (TNO)

SERVICE GROUP	Services	Examples in VCCC or envisioned in EISAC
Advanced Decision Support		
	- Decision Support System (DSS)	CIPCast demonstration CIPCast full service
	- What-if Analysis (WIA) in DSS	CIPRTrainer Web Demonstration Service
Training		
	Master Class CIP/CIR	Master Class offerings, e.g. CIPRNet Masterclass
	CIP/CIR course	CIP/CIR course offering, e.g. CIPRNet Course inside the post graduate Master in Homeland Security
	Lectures	Lectures by CIR/CIP experts
	MOOC CIP/CIR lecture offerings	Massive Open Online Courses (MOOC)
	Training support	CIPRTrainer demonstration CIPRTrainer (full) in Germany with embedded what- if analysis (WIA)
Information Brokerage on CIP/CIR		
	CIP/CIR Community service	CIPedia© including - CI Sector Glossaries - CI/CII Organisations - List of CIP/CIR Acronyms

SERVICE GROUP	Services	Examples in VCCC or envisioned in EISAC
	CIP/CIR Policies and Good Practices	Database access (closed service for consortium)
	Knowledge brokerage	Ask The Expert (ATE)
	Expert access	CIP/CIR consultancy
		Expert speakers
Research Platform for CIP/CIR Collaboration		
	Web Portal Research Platform	=> EISAC.EU with links to national nodes
	- Modelling, Simulation & Analysis	- Initial CIP MS&A reference set - List of Models and Data
	- Repository	Database access (closed service)
	- CIP research project list	CIP EU Research project list
	- CIP/CIR bibliography	CIP/CIR bibliography
Dissemination		
	Support CIP/CIR conferences	Support CIP/CIR conferences - list of events
	Support C(I)IP Newsletters	C(I)IP Newsletters - ECN (repository; requests) - link: DHS CIP Newsletters

All VCCC services are accessible via the VCCC Web Portal at the CIPRNet website: <http://www.ciprnet.eu/vccc.html> (Figure 23).



Figure 23: VCCC services page of the CIPRNet web site www.ciprnet.eu (Fraunhofer)

The VCCC web services page provides access to the following services:

- Decision Support System (DSS) CIPcast (web demonstration)
- What-If Analysis in CIPRTrainer (web demonstration)
- ‘Ask the Expert’
- Knowledge repository, including
 - restricted access to the CIPRNet inventory database
 - CIP research project list
 - CIP bibliography
- CIPedia©, the comprehensive and sought-after online glossary of CIP and CIR terms
- CIPRNet MOOC e-learning platform offering course material.

In the following sections, we briefly characterise some of the VCCC services not covered by other sections of this final report. A more in-depth description please find in CIPRNet’s deliverable D4.9.

3.4.2 Ask the Expert (AtE)

The new Ask the Expert (AtE) service has been deployed since January 2015. The “Ask the Expert” (AtE) service is intended to provide the CIP / CIR stakeholders with the capabilities:

- to pose a question about any CI aspect related to CI operation, threats, management, etc.
- to get feedback on such query from the registered CIPRNet community of experts.

AtE will be continued as a service after CIPRNet ends.

3.4.3 Knowledge repository

Part of the AtE service is a CIP/CIR knowledge repository that points to a large range of CIP/CIR assets and other resources. Accessing the database may help the community to get a quick answer, and helps experts to locate assets and resources.

3.4.4 Initial CIP reference benchmark set

CIPRNet has created an initial CIP benchmarking reference data set (see deliverable D4.8). It is an artificially constructed infrastructure data set for a fictional 100 x 100 km region. The data is provided at two different spatial scales: regional-level and urban-level. The following elements are present: urban areas, electric power transmission and distribution grids, telecommunication networks, railways and roads networks, and drinking water and gas distribution networks, as well as several dependency and threat typologies.

This initial CIP benchmarking reference data set can be used to perform comparative analysis of CIP models using this set as a ‘standard’. The reference data set is focused on the coupling and dependencies between different CI and their subsystems, leaving to the modeller of the simulation approach the task to account for the physical and functional/logical behaviour underlying the different CI. The reference set is beneficial for CI operators and for the CIP R&D community at large, as it represents a valuable benchmark for comparing CI dependency models at regional and urban scale. For researchers, the reference data set is beneficial because it allows a quick start of simulation and analysis activities. Moreover, the approach chosen allows for future extensions and enrichments of the data set.

4 Potential impact and main dissemination activities

4.1 Potential Impact

The Critical Infrastructure Preparedness and Resilience Research Network establishes a Network of Excellence in Critical Infrastructure Protection (CIP). In the past years, CIPRNet built the building blocks for this network: VCCC, knowledge portal, integrated tools, and the network of experts.

A network of excellence is built on trust between researchers working on CIPRNet and between these researchers and their stakeholders. Through the case studies, the work on different tools and especially the staff exchange program, the trust between the researchers has increased. Stakeholders have shown to trust the network by joining the case studies, finding the knowledge network through CIPedia© and the Ask the Expert function on the VCCC portal, and attending the training activities.

From this trust one sizable impact of CIPRNet consists in the constitution of the VCCC as a starting point for the long-term EISAC. The main purpose of the VCCC is reinforcing and intensifying the collaboration of key players in European CIP research, creating a kernel of substantial critical mass and high quality in the CIP area of security research. One of the most tangible CIPRNet assets was the exchange of top specialists in CIP and other key personnel of the CIPRNet partners to directly collaborate on CIP R&D issues, boost new ideas and approaches, and to disseminate CIP advancements through training events, guest lecturers and presentations for academic, public and private CI stakeholder audiences. Another relevant aspect was related to the large effort devoted to training activities that involved more than 1,500 people from 14 countries.

Another important component is CIPRNet's VCCC web portal that evolved from CIPRNet's project web site. It is the 'face' and base-tooling instrument of the VCCC, providing access to all VCCC services. This effort establishes a body of knowledge that is available to the community in order to improve their awareness as well as the respective preparedness, protection and resilience measures. All of the tools and services deployed by the VCCC positively impact the activity of the different end-users they are devised for.

One indication for this is the growing popularity of CIPedia©, which has exceeded 500,000 views (more details later). The VCCC portal also provides access to online training activities and will provide access to experts linked to the VCCC for each person wanting to learn more about CIP/CIR, through the AtE service. Moreover, special care was demonstrated to make this information publicly available after the duration of the project, as this is depicted by the Massive Open Online Course (MOOC) platform, an open access book, CIPedia© and more, which will remain available after CIPRNet ends. Such training activities raise awareness and enhance the protection and resilience capacities of stakeholders across Europe and across sectors, but also contribute to future research and innovation.

CIPRNet expects the scientific community to boost and co-ordinate its activities on CIP and to significantly enlarge the number of adepts to the field. In this respect, the current situation is promising. CIPRNet fostered already more intense collaboration with related projects (PREDICT, RESIN, FORTRESS, INTACT, IMPROVER, CI2C, RoMA) and across programmes (FP7, H2020, DG HOME, national funding). All these efforts ultimately provide support to MS in building their capacities in the field of CIP/CIR.

More specifically, the integrated CIP research community resulting from CIPRNet has demonstrated the capability to tangibly support national, cross-border and inter-regional emergency management in all the phases of the incident cycle. CIPRNet's DSS CIPCast has made a leap forward in this respect, since Italian national and regional civil protection (Rome, Florence, and the region of Mantua) have requested it. CIPRNet's 'what if' analysis capability, manifested as a new training system based on federated modelling, simulation, and analysis called CIPRTrainer, has been tested in training events dedicated to security professionals in civil protection. Two training institutions expressed their interests in using CIPRTrainer.

As an indirect effect of the CIPRNet knowledge dissemination, the stakeholders are expected to improve their knowledge of their CI dependencies, thus increasing the awareness of their vulnerability to cascading effects. This awareness, in turn, leads to the definition of coordinated multi-organisational contingency and recovery plans and thus to improved societal preparedness (as has been shown on limited scale by earlier CIP awareness-raising projects in some nations). Actually, the projects CIPRNet and RoMA have even made more progress in this direction, since they succeeded in collaborating with three Italian CI operators in identifying their real (inter-)dependencies. The VCCC has made concrete efforts to closely involve (multi)national and inter-regional emergency managers and CI operators in its activities. As a result, the overall preparedness of the 'European system' for an effective response to large (multi-)national and inter-regional emergencies related to or involving CI will be enhanced. Effective response to cross-border undesirable events is especially enhanced due to shared situational awareness based on using similar analytical tools and the same data.

Any problem with CI always brings economic losses and impacts the sense of safety of citizens; therefore, CI protection is crucial. CIPRNet's networking and dissemination activities increase the preparedness and resilience of both European and national CI. Achieving that goal benefits the European citizens who continuously use and rely on the undisturbed functioning of CI. Thus, the potential societal impact of disruptive events can be mitigated. Reliable CI means stability of the society, the well-being of European citizens and economic welfare. More resilient CI creates many benefits for national and local economies.

While the results of CIPRNet were derived in the European context, several of these contributions have an international outreach and impact. This includes the activities of the CIPRNet Cooperation Workshop International in Vancouver in 2016, the consultation of two Japanese delegations with Fraunhofer and one delegation with TNO for the purpose of CIP-related policy-making in Japan, the international audience from four continents of the CRITIS conferences, and the contributions that several CIPRNet partners make to the IFIP Working Group 11.10 annual international conference on CIP.

4.2 Main dissemination activities

For a Network of Excellence (NoE), dissemination and training activities are of equal importance as the research and technical development activities, since they contribute to spreading the excellence. CIPRNet performed 158 stakeholder meetings and dissemination and training events for its audiences of the multi-disciplinary CIP community. This section is a summary of the detailed description of CIPRNet's dissemination activities, which has been submitted as deliverable D2.34. Figure 24 visualises CIPRNet's areas of outreach.

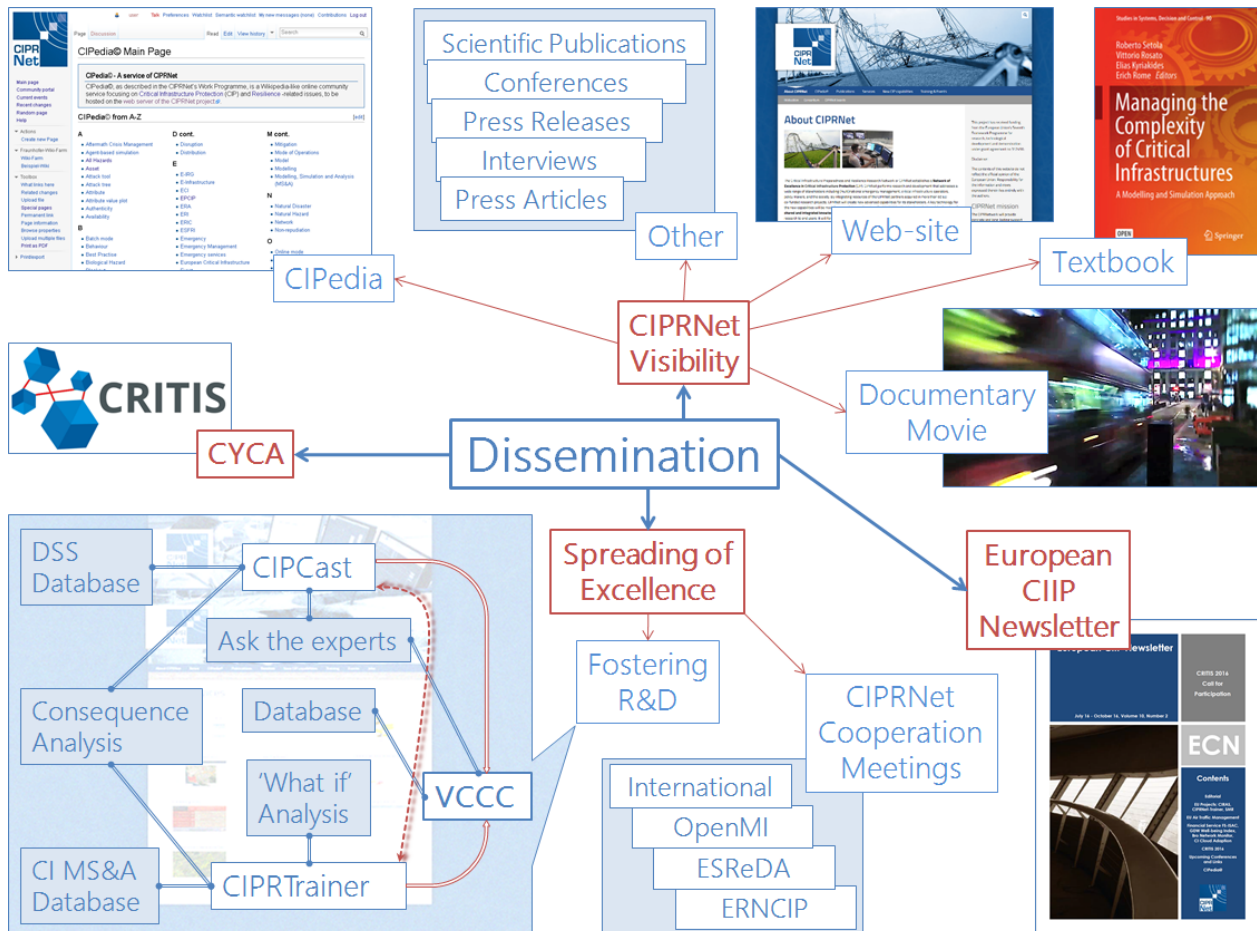


Figure 24: Diagram of CIPRNet's dissemination actions. (UCY)

4.2.1 Website

The CIPRNet web site is one of the major dissemination means of CIPRNet. It is also a comprehensive CIP information source that addresses all types of audiences: from other researchers, CIPRNet end users and stakeholders to the general public. The CIPRNet web site is the “face” of the Virtual Centre of Competence and Expertise in Critical Infrastructure Protection (VCCC), delivering certain services to the multi-disciplinary CIP communities and to end users, such as the “Ask the Expert” service, the CIPCast (DSS) web demonstration service, and the CIPRTrainer (WIA) web demonstration service are accessible via an own “VCCC services” page (see deliverable D4.9).

4.2.2 Publications (peer-reviewed, books, theses)

During the project, 31 peer-reviewed (27 published, four accepted for publication) scientific publications of CIPRNet partners have been published, thereof seven journal papers and eight joint publications. CIPRNet has edited seven books (conference proceedings of CRITIS 2013–2016 and Netonets 2013), edited one book on Critical Infrastructure Security and edited and written one

book on CIPRNet's training material. CIPRNet also contributed four book chapters to other books. The partners have also edited four pre-proceedings for CRITIS 2013–2017, published eight invited papers and released four technical reports. CIPRNet partners have achieved four PhD theses and one Master Thesis. 33 of all CIPRNet's publications are Open Access, that is, the electronic versions can be downloaded for free.



Figure 25: Some CIPRNet books. (Springer)

4.2.3 CIPedia©

CIPedia© is a Wikipedia-like online community service focusing on CIP/CIR-related issues. CIPedia© is a multinational, multidisciplinary and cross-sectoral web collaboration tool for information sharing on CIP/CIR-related matters. It promotes communication between the stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP/CIR-related facilities and laboratories, and the public at large. The CIPedia© service aimed at establishing itself as a common reference point for CIP concepts and definitions. It gathered information from various CIP/CIR as well as related civil protection and climate change sources worldwide and

combined them to collect and present knowledge on the CIP/CIR knowledge domain. It is dynamic, as it allows stakeholders to update information as the domain evolves and new concepts emerge or receive different meaning. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

Current contents statistics (28th February 2017): 3,829 definitions (3,098 national, 109 international standards, 145 EU, 180 from EU projects, 170 international organisations and 127 from other sources) for 358 different terms (358 pages of which 41 pages refer to other definitions and one page contains a set of external links) from 107 nations in 46 different languages. With over half a million total page views within almost three years and currently over 1,000 views per day, the comprehensive CIPedia© is sought after.

4.2.4 European CIIP Newsletter

The European CIIP Newsletter (ECN) is a focused dissemination organ for fostering the cooperation between the CI(I)P research communities and CI and CII stakeholders. The ECN addresses the CIP and CIIP research communities, policy makers, CI operators, crisis managers and civil protection agencies. Between 2006 and 2010, 13 issues of the ECN have been published, partly supported by the EU projects CI²RCO and IRRIS. CIPRNet continued to support the publication of twelve more issues (15-26) until early 2017. CIPRNet partner ACRIS has been in charge of the ECN from the first issue in 2006. All other CIPRNet partners assigned a co-editor for each CIPRNet supported ECN issue, and we had one external co-editor. External authors contributed 86 C(I)IP articles to the twelve latest ECN issues, while CIPRNet members contributed 61 articles on CIPRNet topics.

The ECN includes editorials, articles on issues in CIIP and CIP, feature articles on recent research results, articles on C(I)IP policy making, presentations of new research projects, conference announcements, experience reports of conferences and other C(I)IP related events, and links to information resources.

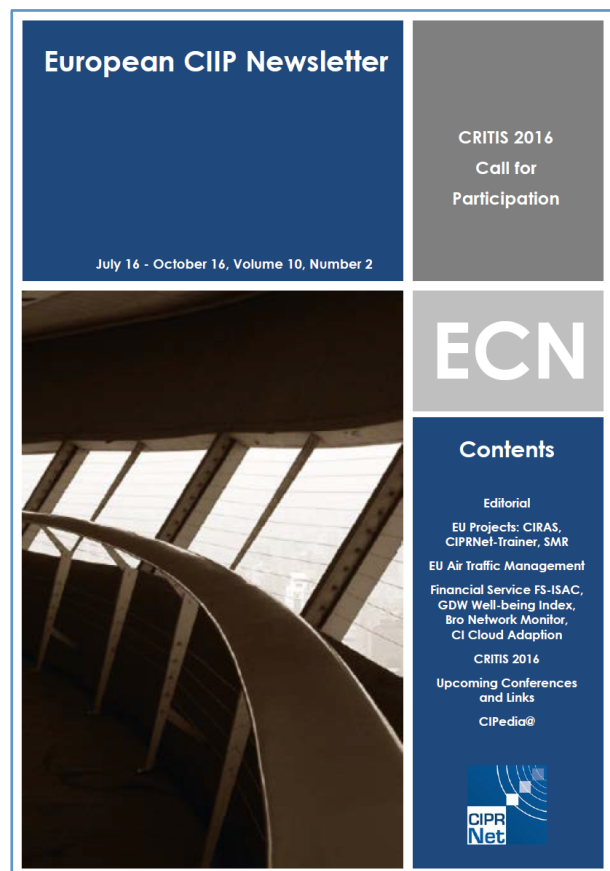


Figure 26: European CIIP Newsletter (ECN) (Acris)

4.2.5 Dissemination material

CIPRNet partners have released twelve posters and flyers. The posters and flyers have been disseminated at conferences (CRITIS), meetings (12th European Congress on Disaster Management) and on the web (automatic.it). The project was disseminated in 15 press articles; 14 of them were articles by CIPRNet partners and one was by the Ministry of Security and Justice of the Netherlands (VITEX Exercise guide) that disseminates CIPedia©. The partners disseminated CIPRNet in newsletters (Fraunhofer, Deltares, UIC), magazines (journalriskcrisis.com, nctv.nl, adnkronos.com, ictsecuritymagazine.com) and online press (EUCONCIP, The CIP Report).

4.2.6 Conferences

CIPRNet contributed to the multi-disciplinary research community. The partners organised several conferences (CRITIS 2013–2016, The Grand Conference 2013, Netonets 2013, TIEMS 2015, MELECON 2016 and ESReDA workshops 46–52), and supported the organisation of CRI!SE 2013–2015. CIPRNet was involved in 47 conferences by attending and/or by presenting their work; SRA-Europe, ERNCIP 2013, ICIA 2013, CIPRE 2014, HIC 2014, ICCST 2014, CP Expo SRC 2014, 9th IFIP Working Group 11.10, ERNCIP 2014, SAFECOMP 2015, EUCONCIP, COMPENG 2016, 6th International Disaster and Risk Conference IDRC.

4.2.7 CYCA (CIPRNet Young CRITIS Award)

To promote and support young researchers operating in the CIP framework CIPRNet established a grant for the best young researchers' paper in Critical Infrastructure Protection. The award has been granted during the annual CRITIS conferences in 2014, 2015 and 2016.

- At CRITIS 2014 in Limassol, Cyprus, the first CYCA has been bestowed.
- The second CYCA has been bestowed at CRITIS 2015 in Berlin, Germany.
- The third CYCA has been awarded at CRITIS 2016 in Paris, France.

The organisers of CRITIS 2017 have raised some funds for continuing the award as “Young CRITIS Award” (YCA) beyond CIPRNet.

4.2.8 Cooperation workshops

The first cooperation workshop was the ERNCIP-CIPRNet meeting, which was organised by JRC, Brussels, Belgium, 13th September 2013. CIPRNet participants plus several ERNCIP members discussed coordination of several activities. The second cooperation workshop was the ESReDA-CIPRNet meeting with the ESReDA association. It was organised by CEA and took place in Torino, Italy, 29th–30th May 2014. The CIPRNet-OpenMI Cooperation Meeting was the third CIPRNet workshop and it was held at Deltares in Delft, the Netherlands, 31st October 2014. The CIPRNet-OpenMI Cooperation Meeting aimed at bringing the scientific communities together and to elaborate future cooperation possibilities. During the cooperation meeting Erich Rome (Fraunhofer) gave a presentation about CIPRNet and on the DIESIS interoperability approach, Bernhard Becker (Deltares) presented a selection of water-related applications of OpenMI and Antonio Di Pietro (ENEA) presented i2Sim. The fourth and final workshop was the International CIPRNet Cooperation Meeting, which was organised by UBC. The meeting was held at the UBC campus, British Columbia, Canada, on the 14th–15th June 2016. During the cooperation meeting Erich Rome (Fraunhofer) gave a presentation about the CIPRNet project and the EISAC perspective, Vittorio Rosato (ENEA) presented the CIPCast and CIPRTrainer tools and Bernhard Hämmerli (ACRIS) presented a sharing approach of CIP information. ERNCIP (2013), OpenMI (2014), ESReDA (2014), International @ UBC (2016).

4.2.9 General public

CIPRNet was promoted in three press releases and three interviews. The partners produced a documentary movie for promoting the dissemination activities and for preparing a strategic campaign towards stakeholders and decision-makers in favour of EISAC.

4.2.10 Demonstrations

CIPRNet capabilities have been demonstrated in the following three events:

- VITEX 2016 was the first EU-wide exercise focussed on the effects of large-scale failure of critical (electricity) infrastructure across Europe,

- Demonstration of CIPCast functionalities at the Areti SpA Headquarters; for validating secure data collection and CIPCast capabilities, and for providing forecasts related to the transformation of damages into impacts and consequences during extreme weather events,
- Demonstration and training event on CIPRTrainer for German institutions (BBK, AKNZ, BNetzA and KaVoMa)⁴.

4.2.11 Stakeholder contacts

CIPRNet has conducted 47 face-to-face meetings with end-users and other stakeholders, including meetings with agencies like the German BBK, the fire-fighters of Mannheim, Cyprus Civil Protection, ARETI, the Italian national coordinator for Security and Counterterrorism and national Cyber Security policies, Milan Metropolitan security manager, and the Dutch Ministry of Security and Justice, two Japanese delegations preparing CIP policies, among others. A comprehensive description of these meetings please find in deliverable D2.34.

4.2.12 Exploitation results

The Decision Support System CIPCast will be further used by Italian CI operators and stakeholders. Also, CIPCast will be further developed in the Italian RoMA project, which will run until 2019. The training system CIPRTrainer will be employed for a paid training event for the German national academy for crisis management training. Negotiations with CIPRNet partner UCBM for using CIPRTrainer in the degree course Master in Homeland Security are on-going.

The training material used for the preparation of the Master Classes, including the lectures available on the CIPRNet online course, has been collected and published in 2017 in a (e-)book “Managing the complexity of Critical Infrastructures, A modelling and simulation approach”, edited by Springer and published at <http://www.springer.com/it/book/9783319510422>. This Open Access publication will foster the dissemination of CIPRNet project and its training activities even after the project completion.

Sustained activities beyond the end of the CIPRNet project include:

- Part of the exploitation will take place in and by the 2EISAC community. Business plans for seven national EISAC nodes and a central EISAC node have been developed or are under construction to establish EISAC nodes in the period between now and 2020;
- The award for the best young researchers’ work, the “CIPRNet Young CRITIS Award”, will be continued in 2017 as “Young CRITIS Award”;
- Several VCCC services will be maintained, including CIPedia©, the comprehensive glossary of CIP terms and CIP/CIR information source, and **security-learning.eu**, CIPRNet’s MOOC platform;

4.2.13 Lectures

CIPRNet conducted 41 lectures on topics in C(I)IP. Lecturers were either CIPRNet members (27 lectures) or invited external experts (14 lectures). Lectures took place either at locations of CIPRNet partners or in external places in ten different European countries. Some lectures were also available online for live participation. By this means of dissemination, CIPRNet reached a total audience of over 1,300 people.

⁴ BBK, the German Federal Office for Civil Protection and Disaster Assistance; AKNZ, Akademie für Krisenmanagement, Notfallplanung und Zivilschutz), the German Academy for Crisis Management, Emergency Planning and Civil Protection; KaVoMa, a degree course at the University of Bonn on Disaster Prevention and Management

4.2.14 Training events

During CIPRNet lifespan 7 training events have been conducted. These activities covered basic and advanced knowledge in CI 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.).

Three types of event have been realised:

- the first event, held at Delft in February 2014, was an internal rehearsal: this pre-edition (Edition 0) of the training event, has been arranged for an internal audience with the aim of testing lesson topics and the accompanying pedagogical material.
- Master Classes have been realised along three editions, scheduled as follows: the first edition in 2014 in Paris, the second one in 2015 in Rome and the third one in 2016 in Bonn. All the editions of the Master Classes will consist of a general, introducing part, treating basic knowledge in MS&A (repeated at each edition), followed by a more advanced part, specific for each edition, as follows:
 - Edition 1: Federated Simulation and OpenMI platform
 - Edition 2: Decision Support System (DSS)
 - Edition 3: 'What-if' Analysis and the CIPRTrainer
- Courses inside the postgraduate Master in Homeland Security at UCBM (Rome, Italy), realised along three editions reflecting the topics of the respective edition of the Master Class. The audience was mainly composed of students of the Master, i.e. young security managers, public authorities' representatives, young security or CIP researchers, and law enforcement officers.

The CIPRNet training events reached a total number of 225 participants, from 14 different countries, of which 120 people were external to the consortium.

4.2.15 e-Learning platform for Massive Open Online Courses (MOOC)

The CIPRNet online course on MS&A of CI has been launched on November 2016 to foster and enlarge the training activities promoted by the consortium also after the end of the project. It is accessible at URL <http://www.security-learning.eu/>.

5 Project websites and contact details

Main CIPRNet project website	ciprnet.eu
Online glossary CIPedia©	cipedia.eu
Newsletter ECN	ciprnet.eu/ecn.html
VCCC services	ciprnet.eu/315.html

Co-ordinator contact details



Name	Dr.-Ing. Erich Rome
Email	erich . rome 'at' iaais . fraunhofer . de
Phone	+49 2241 14 2683
Web	https://www.iaais.fraunhofer.de
Postal address	Fraunhofer IAIS Schloss Birlinghoven 53757 Sankt Augustin Germany

Partners' websites:

- | | | |
|----|---------------------------|---|
| 2 | ENEA, Italy | http://www.enea.it/ |
| 3 | TNO, The Netherlands | https://www.tno.nl/ |
| 4 | UIC, France | http://www.uic.org/ |
| 5 | CEA, France | http://www.cea.fr/english-portal |
| 6 | JRC, EU | https://ec.europa.eu/jrc/en/ |
| 7 | Deltares, The Netherlands | https://www.deltares.nl/en |
| 8 | UCY, Cyprus | http://www.kios.ucy.ac.cy/ |
| 9 | UTP, Poland | http://www.utp.edu.pl/en |
| 10 | UCBM, Italy | http://www.coseritylab.it/ |
| 11 | UBC, BC, Canada | http://ece.ubc.ca/ |
| 12 | Acris, Switzerland | http://www.acris.ch/ |



6 Annex: List of acronyms

Acronym	Meaning	Acronym	Meaning
2EISAC	Association towards EISAC	ECN	European CIIP Newsletter
AtE	Ask the Expert	EISAC	European Infrastructures Simulation and Analysis Centre
CI	Critical Infrastructure	fMS&A	federated MS&A
CIIP	Critical Information Infrastructure Protection	GIS	Geographical Information System
CIP	Critical Infrastructure Protection	MOOC	Massive Open Online Course
CIR	Critical Infrastructure Resilience	MS&A	Modelling, Simulation & Analysis
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network	NGI	Next Generation Infrastructure
CM	Crisis Management	NoE	Network of Excellence
DSS	Decision Support System	VCCC	Virtual Centre of Competence and expertise in Critical Infrastructure Protection
ECI	European Critical Infrastructure		

7 Annex: References

7.1 References for the main scientific and technological results/foregrounds

- [1] Luiijf, E., Klaver, M. **Insufficient Situational Awareness about Critical Infrastructures by Emergency Management**. In: Proceedings Symposium on “C3I for crisis, emergency and consequence management”, Bucharest 11–12 May 2009, NATO RTA: Paris, France. RTO-MP-IST-086
- [2] Xie, J., Theocharidou, M., Barbarin, Y., Rome, E.: **Knowledge-driven scenario development for critical infrastructure protection**. In: Rome, E., Theocharidou, M., Wolthusen, S.D. (Eds.), Critical Information Infrastructures Security, 10th International Workshop, CRITIS 2015, Berlin, Lecture Notes in Computer Science, Vol. 9578, Springer, Heidelberg, 2016, pp. 91–102
- [3] Klaver, M.H.A., Luiijf, H.A.M., Nieuwenhuijs, A.N., Van Os, N., Oskam, V., **Critical Infrastructure Assessment by Emergency Management**. In: Rome, E., Theocharidou, M., Wolthusen, S.D. (Eds.), Critical Information Infrastructures Security, 10th International Workshop, CRITIS 2015, Berlin, Lecture Notes in Computer Science, Vol. 9578, Springer, Heidelberg, 2016, pp 79-90
- [4] Jonkman, S. N.; Lentz, A.; Vrijling, J. K. (2010): **A general approach for the estimation of loss of life due to natural and technological disasters**. In: Reliability Engineering & System Safety 95 (11), p. 1123–1133
- [5] L. Matassoni, A. Fiaschi, S. Giovinazzi, M. Pollino, L. La Porta, V. Rosato, **A geospatial decision support tool for seismic risk management: Florence (Italy) case study**, submitted to *Natural Hazards*
- [6] L. Matassoni, A. Fiaschi, S. Giovinazzi, M. Pollino, L. La Porta, V. Rosato, **Seismic scenarios for the northwestern Tuscany (Italy)**, submitted to *Engineering Geology*
- [7] <http://www.aphorism-project.eu/> (FP7 GA n.606738)

7.2 Peer-reviewed CIPRNet papers

- [Saga16] Saganowski L., Andrysiak T., Kozik R., Choras M., **DWT-based anomaly detection method for cyber security of wireless sensor networks**, in Security and Communication Networks, Volume 9, Issue 15, Wiley, October 2016.
- [Rosse16] Rossebø, J. E. Y., Fransen, F. and Luijff, E., **Including Threat Actor Capability and Motivation in Risk Assessment for Smart Grids**, in IEEE Xplore, October, 2016. DOI: 10.1109/CPSRSG.2016.7684094.
- [Xie16b] Xie J., Kozik R., Flourentzou N., **An Integrated Modelling Approach for Spatial-aware Federated Simulation**, in the 8th International Conference on Advances in System Simulation (SIMUL2016), Rome, Italy, Copyright© IARIA, ISSN: 2308-4537, ISBN: 978-1-61208-501-2, 21st August 2016, pp. 40-45, 2016.
- [Kozik16a] Kozik R., Choras M., Renk R., Hołubowicz W., **Cyber Security of the Application Layer of Mission Critical Industrial Systems**, in Saeed K., Homenda W. (Eds.): Computer Information Systems and Industrial Management - 15th IFIP TC8 International Conference, CISIM 2016, Vilnius, Lithuania, September 14-16, 2016, Proceedings. Lecture Notes in Computer Science 9842, Springer, 2016, ISBN 978-3-319-45377-4.
- [Luijff16a] Luijff H.A.M. and Klaver M.H.A., **Information Sharing of Cyber-security Related Information: A Decomposition**, accepted for publication, Critical Infrastructure Protection IX - 9th IFIP WG 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 2014, Revised Selected Papers. IFIP Advances in Information and Communication Technology, Springer, 2015.
- [Oliva16] G. Oliva, R. Setola and S. Panzieri, **Critical Clusters in Interdependent Economic Sectors. A Data-Driven Spectral Clustering Analysis**, The European Physical Journal Special Topics (EPJ-ST), vol. 225, no. 10, pp. 1929–1944, 2016 (doi:10.1140/epjst/e2015-50321-0).
- [Sterg16a] Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., **Time-based Critical Infrastructure Dependency Analysis for Large-Scale and Cross-Sectoral Failures**, in International Journal of Critical Infrastructure Protection, Elsevier, Vol. 12, Mar. 2016, p. 46–60, doi:10.1016/j.ijcip.2015.12.002.
- [Xie16a] Xie J., Theocharidou M., Barbarin Y., Rome E., **Knowledge-driven Scenario Development for Critical Infrastructure Protection**, in conference proceedings Critical Information Infrastructures Security, 10th International Workshop (CRITIS2015), Berlin, LNCS vol. 9578, Springer, Heidelberg, 2016, pp. 91-102.
- [Grang16] Grangeat A., Bony A., Lapebie E., Eid M., Dusserre G., **The challenge of critical infrastructure dependency modelling and simulation for emergency management and decision making by the civil security authorities**, in conference proceedings Critical Information Infrastructures Security, 10th International Workshop (CRITIS2015), Berlin, LNCS vol. 9578, Springer, Heidelberg, pp. 255-258, 2016.
- [Alutaibi16] Alutaibi K., Alsubaie A., Marti J.R., **Resilience Assessment of Interdependent Critical Infrastructure**, in conference proceedings Critical Information Infrastructures Security, 10th International Workshop (CRITIS2015), Berlin, LNCS vol. 9578, Springer, Heidelberg, pp. 43-55, 2016.
- [Klaver16a] Klaver M., Luijff E., Nieuwenhuijs A., van Os N., Oskam V., **Critical Infrastructure Assessment by Emergency Management**, in conference proceedings Critical Information Infrastructures Security, 10th International Workshop (CRITIS2015), Berlin, LNCS vol. 9578, Springer, Heidelberg, pp. 79-90, 2016.
- [Luijff15b] Luijff E., **Cyber (In-)security of Industrial Control Systems: A Societal Challenge**, in: F. Koornneef and C. van Gulijk (Eds.): SAFECOMP 2015, LNCS 9337, pp. 7–15, 2015. DOI: 10.1007/978-3-319-24255-2 2.

- [Sterg15b] Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., **Risk mitigation strategies for critical infrastructures based on graph centrality analysis**, in International Journal of Critical Infrastructure Protection, accepted for publication – September issue, <http://dx.doi.org/10.1016/j.ijcip.2015.05.003>, Elsevier, 2015.
- [Luiijf15a] Luiijf E., & Klaver M., SYMPOSIUM ON CRITICAL INFRASTRUCTURES: RISK, RESPONSIBILITY AND LIABILITY - **Governing Critical ICT: Elements that Require Attention**, European Journal of Risk Regulation, Vol. 6, Issue 2 (2015). pp. 263–270.
- [KyrPol15] Kyriakides E. and Polycarpou M. (Eds.), **Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems**, Studies in Computational Intelligence, Berlin: Springer-Verlag, ISBN: 978-3-662-44159-6, 2015.
- [Sterg15a] Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., **Using centrality measures in CI dependency risk graphs for efficient risk mitigation**, in Ninth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, SRI International, Arlington, Virginia, USA, 16th–18th March 2015.
- [Kozik15a] Kozik R., Choras M., Flizikowski A., Theocharidou M., Rosato V., Rome E., **Advanced services for critical infrastructures protection**. Journal of Ambient Intelligence and Humanized Computing, p. 1-13. Springer Berlin Heidelberg, ISSN 1868-5137, <http://dx.doi.org/10.1007/s12652-015-0283-x>, 2015.
- [DiPietro14] Di Pietro A., La Porta L., Pollino M., Rosato V., Tofani A., Martí J.R., Romani C., **A Decision Support System for Emergency Management of Critical Infrastructures subjected to Natural Hazards**, in 9th Critical Information Infrastructures Security Conference, Limassol, Cyprus, 13th–15th October 2014.
- [Burzel14] Burzel A., Hounjet M., Becker B., di Pietro A., Pollino M., Rosato V., Tofani A., **Towards a decision support system for consequence analysis of flooding on critical infrastructure**, 11th International Conference on Hydroinformatics, Paper 99. New York, USA, 17th–21st August 2014.
- [deBoer14] De Boer G., Baart F., Becker B., Jagers B., **Overview of coupling of data, models and information through the web using existing standards**, 11th International Conference on Hydroinformatics, Paper 405. New York, USA, 17th–21st August 2014.
- [Agresta14] Agresta A., Fattoruso G., Pollino M., Pasanisi F., Tebano G., De Vito S., Di Francia G., **An ontology framework for flooding forecasting**, 14th International Conference on Computational Science and Its Applications (ICCSA 2014), Springer, LNCS, Vol. 8582. doi 10.1007/978-3-319-09147-1_30, pp. 417–428, 2014, 30th June 2014.
- [Alsu14] Alsubaie A., Alutaibi K., Martí J.R., Di Pietro A., Tofani A., **Resources Allocation in Disaster Response using Ordinal Optimization Based Approach**, IEEE Canada International Humanitarian Technology Conference (IHTC 2014), Montreal, 1st–4th June 2014.
- [Choras14] Choras M., Kozik R., Renk R., Holubowicz W., **End-users needs and requirements for tools to support critical infrastructures protection**, in 1st International Workshop on Real-time Big Data Analytics for Critical Infrastructure Protection (BIG4CIP 2014), Newcastle, the UK, May 2014.
- [Formi14] Formicola V., Di Pietro A., Alsubaie A., D'Antonio S., Martí J.R., **Assessing the Impact of Attacks on Wireless Sensor Nodes that Monitor Interdependent Physical Systems**, Critical Infrastructure Protection, Springer Berlin Heidelberg, Vol. VIII, pp. 213–229, 1st January 2014.
- [Marti14a] Martí J.R., **Multisystem Simulation: Analysis of Critical Infrastructures for Disaster Response**, in: D'Agostino, G., Scala, A. (Eds.), Network of Networks: the last Frontier of Complexity, Springer, Cham Heidelberg, pp. 255–277, 2014.
- [Tofis13b] Tofis, Y., Yiasemi, Y., Kyriakides, E., A Plug and Play, **Approximation-Based, Selective Load Shedding Mechanism for the Future Electrical Grid**, in: Critical Information

Infrastructures Security, Luijff, E and Hartel, P. (Eds.), Springer, LNCS Vol. 8328, Dordrecht, pp. 74–83, 2013.

- [Kozik13] Kozik, R, Choras, M, **Current Cyber Security Threats and Challenges in Critical Infrastructures Protection**, in: The Second International Conference on Informatics and Applications (ICIA2013), 23-25.09.2013, Lodz, Poland, pp. 93–97, 2013.
- [Tofis13a] Tofis, Y., Yiasemi, Y., Kyriakides, E., A Plug and Play, **Approximation-Based, Selective Load Shedding Mechanism for the Future Electrical Grid**, in: Pre-Proceedings of 8th CRITIS Conference on Critical Information Infrastructures Security, 16-18.09.2013, Amsterdam, the Netherlands, pp. 89–98, 2013.

7.3 CIPRNet Books

- [8] Luijff E., Hartel P. (Eds.), **Critical Information Infrastructure Security - 8th International Workshop, (CRITIS'13)**, revised selected papers, Proceedings, Springer, LNCS Vol. 8328, DOI 10.1007/978-3-319-03964-0, Dordrecht, 2013.
- [9] D'Agostino G., Scala A. (Eds.), **Network of Networks: the last Frontier of Complexity**, Springer, Cham Heidelberg, ISBN 978-3-319-03517-8, (2014).
- [10] Panayiotou C.G., Ellinas G., Kyriakides E., Polycarpou M.M. (Eds.), **Critical Information Infrastructure Security - 9th International Workshop, (CRITIS'14)**, revised selected papers, Proceedings, Springer, LNCS Vol. 8985, ISBN 978-3-319-31664-2, Limassol, 2014.
- [11] Rome E., Theocharidou M., Wolthusen S. (Eds.), **Critical Information Infrastructure Security - 10th International Workshop, (CRITIS'15)**, revised selected papers, Proceedings, Springer, LNCS Vol. 8985, ISBN 978-3-319-31664-2, Berlin, 2015.
- [12] Kyriakides E. and Polycarpou M. (Eds.), **Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems**, Studies in Computational Intelligence, Berlin: Springer-Verlag, 2015 (ISBN: 978-3-662-44159-6).
- [13] Setola R., Rosato V., Kyriakides E., Rome E. (Eds.), **Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach**, Series: Studies in Systems, Decision and Control, Vol. 90, Springer, ISBN 978-3-319-51042-2, 2017. **OPEN ACCESS**.
- [14] Setola R., Nassopoulos, H., Havarneanu G. (Eds.), **Critical Information Infrastructure Security - 11th International Workshop, (CRITIS'16)**, revised selected papers, Proceedings, Springer, LNCS, to appear 2017.

7.4 CIPRNet book chapters

- [15] Kozik R, Choras M, **Current Cyber Security Threats and Challenges in Critical Infrastructures Protection**, in: The Second International Conference on Informatics and Applications (ICIA2013), 23rd–25th Sep. 2013, Lodz, Poland, pp 93-97.
- [16] Rome E., Langeslag P., Usov A., **Federated Modelling and Simulation for Critical Infrastructure Protection**, in: D'Agostino, G., Scala, A. (Eds.), **Network of Networks: the last Frontier of Complexity**, Springer, Cham Heidelberg, (2014).
- [17] Martí J.R., **Multisystem Simulation: Analysis of Critical Infrastructures for Disaster Response**, Book: Networks of networks: the last frontier of complexity, Springer International Publishing, pp. 255-277, 1st January 2014.
- [18] Luijff, Eric, **National Cyber Security Organisation Part I. The Netherlands**, Chapter 6 in: Lech J. Janczewski, William Caelli, **Cyber Conflicts and Small States**, Ashgate, 2016, pp. 71-101.

- [19] Sullivan D., Luiijf E., Colbert E., **Components of Industrial Control Systems**, Chapter 2 in: Edward J. M. Colbert, Alexander Kott, Cyber Security of SCADA and other Industrial Control Systems (2016) DOI 10.1007/978-3-319-32125-7_2.
- [20] Luiijf E., **Threats in Industrial Control Systems**, Chapter 5, in: Edward J. M. Colbert, Alexander Kott, Cyber-Security of SCADA and other Industrial Control Systems (2016) DOI 10.1007/978-3-319-32125-7_5.
- [21] Setola R., Luiijf E., Theocharidou M., Critical Infrastructures, **Protection and Resilience**, Chapter 1 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_1.
- [22] Setola R., Theocharidou M., **Modelling Dependencies Between Critical Infrastructures**, Chapter 2 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_2.
- [23] Eid M., Rosato V., **Critical Infrastructure Disruption Scenarios Analyses via Simulation**, Chapter 3 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_3.
- [24] Di Pietro A., Liberto C., Flourentzou N., Kyriakides E., Pothof I., Valenti G., **Physical Simulators of Critical Infrastructures**, Chapter 4 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_4.
- [25] Tofani A., D'Agostino G., Martí J., **Phenomenological Simulators of Critical Infrastructures**, Chapter 5 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_5.
- [26] Huiskamp W., van den Berg T., **Federated Simulations**, Chapter 6 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_6.
- [27] Chora M., Kozik R., Flizikowski A., Hołubowicz W., Renk R., **Cyber Threats Impacting Critical Infrastructures**, Chapter 7 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_7.
- [28] Voogd J., **Verification and Validation for CIPRNet**, Chapter 8 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_8.
- [29] Di Pietro A., Lavallo L., La Porta L., Pollino M., Tofani A., Rosato V., **Design of DSS for Supporting Preparedness to and Management of Anomalous Situations in Complex Scenarios**, Chapter 9 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_9.
- [30] Rome E., Doll T., Rilling S., Sojeva B., Voß N., Xie J., **The Use of What-If Analysis to Improve the Management of Crisis Situations**, Chapter 10 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_10.
- [31] Becker B., Burzel A., **Model Coupling with OpenMI Introduction of Basic Concepts**, Chapter 11 in: Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach, Springer, DOI 10.1007/978-3-319-51043-9_11.

7.5 CIPRNet invited papers

- [32] Luijff H.A.M., Klaver M.H.A., **“Expand the Crisis? Neglect Critical Infrastructure! (Insufficient situational awareness about critical infrastructure by emergency management – Insights and Recommendations),”** in: Tagungsband 61. Jahresfachtagung der Vereinigung des Deutschen Brandschutzes e.V., 27th–29th May 2013 Weimar, Germany, pp 293-304.
- [33] Rome E., **“Modellierung, Simulation und Analyse für den Schutz Kritischer Infrastrukturen,”** in: Tagungsband 61. Jahresfachtagung der Vereinigung des Deutschen Brandschutzes e.V., 27th–29th May 2013 Weimar, Germany, pp 569-586.
- [34] Pires J. invited paper at CPExpo 2014, Genova, Italy, 9th–11th December 2014; for the thematic session **“Disaster resilience: critical infrastructure protection and business continuity.”**
- [35] Setola R. invited paper at CPExpo 2014, Genova, Italy, 9th–11th December 2014; for the thematic session **“Disaster resilience: crisis management and civil protection.”**
- [36] Kozik R., Choras M., Holubowicz W., Renk R., **“Increasing Protection and Resilience of Critical Infrastructures – Current challenges and approaches,”** in Proc of: Critical Infrastructures Preparedness: Status of Data for Resilience Modelling, Simulation and Analysis (MS&A), ESReDA Workshop, Wroclaw, 28th–29th May 2015.
- [37] Tofani A., Di Pietro A., Lavallo L., Pollino M., Rosato V., Alessandroni S., **“CIPRNet Decision Support System: Modelling Electrical Distribution Grid Internal Dependencies,”** in Proc of: Critical Infrastructures Preparedness: Status of Data for Resilience Modelling, Simulation and Analysis (MS&A), ESReDA Workshop, Wroclaw, 28th–29th May 2015.
- [38] Eid M., Barbarin Y., Sérafin D., **“A resilience model based on Stochastic Poisson Process,”** in Proc. of: Critical Infrastructures Preparedness: Status of Data for Resilience Modelling, Simulation and Analysis (MS&A), ESReDA Workshop, Wroclaw, 28th–29th May 2015.
- [39] Rosato V., **“A Decision Support System for the Risk Forecast on Critical Infrastructures due to Natural hazards,”** in Smart City Summit & Expo 2017, Taipei, Taiwan, 21st–24th February 2017.

7.6 Theses within CIPRNet

- [40] Khouj M.T., **“Resource Allocation Optimization of a Disrupted Interdependent System Using Machine Learning,”** Ph.D. Thesis, University of British Columbia, April 2014.
- [41] Di Pietro, Antonio: **“Methodologies for Emergency Management in Critical Infrastructures,”** Ph.D. dissertation, University Roma Tre, Rome, Italy, April 2015.
- [42] Betim Sojeva, **“Using Web GIS for Designing Added-Value Training Systems for Crisis Managers,”** Master’s Thesis, University Koblenz-Landau, Germany, 2015.
- [43] Alsubaie A., **“Improving critical infrastructure resilience with application to power distribution networks,”** Ph.D. dissertation, University of British Columbia, Vancouver, Canada, July 2016.
- [44] Amélie Grangeat **“Vulnérabilité, résilience et effets cascade entre réseaux techniques: apports de la modélisation systémique et spatiale pour la planification et la gestion de crise au profit des opérateurs de réseau et de la sécurité civile,”** Ph.D. Thesis, Ecole des Mines ParisTech, Paris, France, 07/12/2016.

7.7 CIPRNet public deliverables

Number	Bibliographical information
[D3.3]	EU FP7 Project CIPRNet, CEA, Deliverable D3.3 "Report on identification of mobility funding programmes". Gramat, France, 16.10.2013
[D4.5]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D4.5 "Implementation of the WIA services for the CIPRNet web portal". Sankt Augustin, Germany, 21.09.2016
[D4.6]	EU FP7 Project CIPRNet, ENEA, Deliverable D4.6 "Implementation of the DSS services for the CIPRNet web portal". Casaccia, Italy, 29.06.2016
[D4.8]	EU FP7 Project CIPRNet, UCBM, Deliverable D4.8 "Initial CIP Benchmarking reference set". Rome, Italy, 10.10.2016
[D4.9]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D4.9 "Report on final status of the VCCC". Sankt Augustin, Germany, 16.01.2017
[D5.2v1]	EU FP7 Project CIPRNet, UTP, Deliverable D5.2 v1 "Services specification". Bydgoszcz, Poland, 31.07.2014
[D5.2v2]	EU FP7 Project CIPRNet, UTP, Deliverable D5.2 v2 "Services specification". Bydgoszcz, Poland, 17.11.2014
[D5.3]	EU FP7 Project CIPRNet, ENEA, Deliverable D5.3 "Realisation of "ask the expert" function". Casaccia, Italy, 30.11.2014
[D5.4v1]	EU FP7 Project CIPRNet, ENEA, Deliverable D5.4 v1 "Report on end-user aspects to be considered in demonstration". Rome, Italy, 29.07.2016
[D5.4v2]	EU FP7 Project CIPRNet, ENEA, Deliverable D5.4 v2 "Report on end-user aspects to be considered in demonstration". Rome, Italy, 01.02.2017
[D5.5]	EU FP7 Project CIPRNet, TNO, Deliverable D5.5 "Report on support for secure design of NGI". The Hague, The Netherlands, 01.02.2017
[D6.2]	EU FP7 Project CIPRNet, CEA / Fraunhofer, Deliverable D6.2 "Application scenario". Gramat, France, 14.07.2014
[D6.3]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D6.3 "Federate CI models". Sankt Augustin, Germany, 31.08.2015
[D6.4]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D6.4 "Implementation and integration of the federated and distributed cross-sector and threat simulator". Sankt Augustin, Germany, 30.03.2016
[D6.5]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D6.5 "Documentation and user manual of the CIP MS&A based 'what if' analysis demonstrator". Sankt Augustin, Germany, 31.05.2016
[D6.7]	EU FP7 Project CIPRNet, TNO, Deliverable D6.6+D6.7 "Questionnaires for preparing the CIP MS&A based 'what if' analysis knowledge report and 'What if' analysis knowledge report". The Hague, The Netherlands, 22.02.2017
[D7.1v2]	EU FP7 Project CIPRNet, ENEA, Deliverable D7.1 v2 "Design of the DSS with consequence analysis". Casaccia, Italy, 16.01.2015
[D7.3]	EU FP7 Project CIPRNet, ENEA, Deliverable D7.2+D7.3 "Database of the DSS with consequence analysis and Assessment and selection of vulnerability and risk estimators". Casaccia, Italy, 06.05.2015

Number	Bibliographical information
[D7.4]	EU FP7 Project CIPRNet, ENEA, Deliverable D7.4 “Implementation of the DSS with consequence analysis”. Casaccia, Italy, 28.07.2015
[D7.5]	EU FP7 Project CIPRNet, ENEA, Deliverable D7.5+D7.6 “Integration of meteorological simulators, flood forecasts, earthquakes data and analysis tool and Interface to the technical demonstrator for federated CIP MS&A”. Casaccia, Italy, 24.03.2016
[D7.6]	EU FP7 Project CIPRNet, ENEA, Deliverable D7.6 “Integration of meteorological simulators, flood forecasts, earthquakes data and analysis tool and Interface to the technical demonstrator for federated CIP MS&A”. Casaccia, Italy, 15.02.2016
[D7.8]	EU FP7 Project CIPRNet, ENEA, Deliverable D7.7+D7.8 “Crisis scenarios and impact evaluation and Results of a 3-months test-run of the DSS”. Casaccia, Italy, 27.02.2017
[D8.110]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D8.110 “CIPRNet project website design: technical report on project website design and built up”. Sankt Augustin, Germany, 13.02.2014
[D8.212]	EU FP7 Project CIPRNet, CEA, Deliverable D8.212 “CIPRNet cooperation meeting: ESReDA”. Saclay, France, 14.07.2014
[D8.213]	EU FP7 Project CIPRNet, Deltares, Deliverable D8.213 “CIPRNet cooperation meeting: OpenMI”. Delft, The Netherlands, 18.02.2015
[D8.300]	EU FP7 Project CIPRNet, UCBM, Deliverable D8.3 “Textbook: Training Material on DSS and Training Material on CIP MS&A based ‘what if’ analysis”. Rome, Italy, 16.01.2017
[D8.400]	EU FP7 Project CIPRNet, JRC, Deliverable D8.4 “Publicly announced CIPedia”. Ispra, Italy, 02.06.2014
[D8.511]	EU FP7 Project CIPRNet, ACRIS / Fraunhofer, Deliverable D8.511 “European CIIP Newsletter issue 15”. Lucerne, Switzerland / Sankt Augustin, Germany, 12.07.2013
[D8.514]	EU FP7 Project CIPRNet, ACRIS, Deliverable D8.514 “European CIIP Newsletter issues 16–18”. Lucerne, Switzerland, 08.07.2014
[D8.518]	EU FP7 Project CIPRNet, ACRIS, Deliverable D8.518 “European CIIP Newsletter issues 19–22”. Lucerne, Switzerland, 21.10.2015
[D8.522]	EU FP7 Project CIPRNet, ACRIS, Deliverable D8.522 “European CIIP Newsletter issues 23–26”. Lucerne, Switzerland, 17.02.2017
[D8.600]	EU FP7 Project CIPRNet, ENEA, Deliverable D8.6 “Screenplay and direction of a documentary movie to be used for dissemination activities and to prepare a strategic campaign towards stakeholders and decision-makers in favour of EISAC”. Casaccia, Italy, 31.07.2016
[D9.1]	EU FP7 Project CIPRNet, UCBM, Deliverable D9.1 “Training plan”. Rome, Italy, 14.02.2014
[D9.20]	EU FP7 Project CIPRNet, Deltares, Deliverable D9.2 “Draft training material OpenMI”. Delft, The Netherlands, 05.03.2014
[D9.30]	EU FP7 Project CIPRNet, ENEA, Deliverable D9.30 “Draft training material of

Number	Bibliographical information
	the DSS demonstrator system". Casaccia, Italy, 06.11.2015
[D9.40]	EU FP7 Project CIPRNet, Fraunhofer, Deliverable D9.40 "Draft training material of 'what if' analysis demonstrator system". Sankt Augustin, Germany, 11.07.2016
[D9.51]	EU FP7 Project CIPRNet, UCBM, Deliverable D9.51 "Periodic training event internal". Rome, Italy, 28.05.2014
[D9.70]	EU FP7 Project CIPRNet, UCBM, Deliverable D9.7 "At least seven CIPRNet lectures". Rome, Italy, 02.02.2017
[D9.81]	EU FP7 Project CIPRNet, UCBM, Deliverable D9.81 "Courses inside the Homeland Security Master (course, report)". Rome, Italy, 30.10.2014
[D9.82]	EU FP7 Project CIPRNet, UCBM, Deliverable D9.82 "Courses inside the Homeland Security Master (course, report)". Rome, Italy, 28.07.2015
[D9.83]	EU FP7 Project CIPRNet, UCBM, Deliverable D9.83 "Courses inside the Homeland Security Master (course, report)". Rome, Italy, 29.07.2016

7.8 Links to conferences organised by CIPRNet

Netonets 13 <http://netonets.org/>
 CRITIS 13 <http://www.critis2013.nl/>
 Grand 13 <https://www.thegrandconference.org/programme/2013>
 CRITIS 14 <http://www.kios.ucy.ac.cy/critis2014/>
 TIEMS 15 <http://tiems.info/tiems-2015-annual-conference.html>
 CRITIS 15 <http://www.critis2015.org/home/>
 CRITIS 16 <http://critis2016.org>