FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

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

D5.2 Services Specification

Due date of deliverable: 31/07/2014
Actual submission date v1: 31/07/2014
Actual submission date v2: 17/11/2014

Revision: Version 2

University of Technology and Life Sciences (UTP)

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

Author(s)	Michał Choraś (UTP) Rafał Renk (UTP) Rafał Kozik (UTP)
Contributor(s)	Witold Hołubowicz, Adam Flizikowski (UTP) Marianthi Theocharidou, Christer Pursiainen (JRC) Vittorio Rosato, Alberto Tofani (ENEA) Andrij Usov, Erich Rome (Fraunhofer) Eric Luiijf (TNO) Nikolas Flourentzou (UCY)

Security Assessment	**Erich Rome (Fraunhofer)**
Approval Date	28.07.2014
Remarks	No issues found.

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.

TABLE OF CONTENTS

List of abbreviations

Abbreviation	Meaning
API	Application Programming Interface
CI	Critical Infrastructure(s)
CIP	Critical Infrastructure Protection
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
CIPRNet DB	CIPRNet database
DIESIS	Design of an Interoperable European federated Simulation network for Critical InfraStructures
DSS	Decision Support System(s)
DSS-DAG	Data accessing and gathering service of CIPRNet DSS
DSS-TF	Threat forecasting service of CIPRNet DSS
DSS-TV	Threat visualisation service of CIPRNet DSS
EEA	European Environment Agency
EFAS	European Flood Awareness System
EISAC	European Infrastructures Simulation and Analysis Centre
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
FAQs	Frequently Asked Questions
GIS	Geographic Information System(s)
GUI	Graphical User Interface(s)
HTTP(S)	Hypertext Transfer Protocol (Secure)
I-EISAC	Italian EISAC node
INGV	Italian National Institute of Geophysics and Volcanology
ISPRA	Italian Institute for Environmental Protection and Research
ISTAT	National Institute of Statistics
JSON	JavaScript Object Notation
MS&A	Modelling, Simulation and Analysis
PDF	Portable Document Format
SAR	Synthetic-aperture radar
SLA	Service Level Agreement(s)
SMEs	Small and medium enterprises
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UML	Unified Modeling Language
VCCC	Virtual centre of competence and expertise in CIP
WCS	Web Coverage GIS Service
WFS	Web Feature GIS Service
WIA	What-if analysis
WMS	Web Map GIS Service
XML	Extensible Markup Language

1 Introduction

This document specifies the services relevant to the CIPRNet project. It provides the general specification as the basis for further development of the web-based services related to CIPRNet tools and products carried out in subsequent project work packages (e.g., WP4, WP6 and WP7) where more detailed/technical specification and implementation details will be shown. This specification is strongly influenced by end-users view. The list of end-users includes:

- National Civil Protection,
- Regional Civil Protection,
- Regional/local authorities,
- Crisis/Emergency Management Centres,
- Military Advisors,
- CI operators,
- Experts and Researchers related to the CIP domain.

The type of the specified web services, their functionalities and purpose specifications originate from:

- The CIPRNet Description of Work [DoW],
- CIPRNet consortium expertise,
- Analysis of the end-user requirements, needs and expectations [D5.1].

This document is structured as follows. Firstly, end-users requirements and key findings derived from the deliverable D5.1 "Formal Requirements Specification" [D5.1] are discussed. In the Section 3 non-technical aspects of using CIPRNet DSS services are presented.

Afterwards, the types of the services related to CIPRNet Decision Support System (DSS) are presented. Each service is detailed in a separate section using the following approach:

- Short description of the service with respect to the end-user requirements, including the role of the service, its key functionalities and expected outcome/benefits.
- Input and output information specification.
- Key actors and service functionalities presented by means of the UML Use Case diagrams.
- Relation to other services, elements, tools and products developed within the CIPRNet project.

The "Ask the expert" and "CIPedia" services are specified in the section related to VCCC, using the same template as the one presented above. Afterwards, this document introduces and generally describes the services that will not be developed during the CIPRNet project, but that may be relevant to the future EISAC deployment (see Annex A). Annex B includes the paper [End] discussing end-user views on needs and requirements for tools to support CIP. The publication was prepared based on the current deliverable and was published and presented at the First International Workshop on Real-time Big Data Analytics for Critical Infrastructure Protection (BIG4CIP 2014) [B4C]. Finally, the conclusions are given in the last section of this document.

This version 2 of the deliverable 5.2 implements the recommendations of the reviewers given after the first project review.

2 Key findings related to user requirements

The requirements identified in the D5.1 document are the basis for the development activities in WP7 ("Decision Support System with consequence analysis"). More precisely, they serve as guidelines for further work, such as the final system specification and in particular the CIPRNet DSS components development. Moreover, D5.1 also influences the work in WP6, complementing the description of the requirements for the cross-sector simulation environment and adding the end-user perspective into the development of application scenarios and the realisation of a demonstrator.

However, it should be mentioned that the CIPRNet general requirements were focused on the decision support front-end, rather than on the back-end (the back-end consists of the models and simulations that provide the input information for the CIPRNet DSS).

The end-users' needs, expectations and requirements (presented in D5.1) can be categorised on the basis of the following aspects they are related to:

- Decision support process,
- Simulation and modelling,
- Access to real-time data and critical information.

The key findings that have been identified after the analysis of the mentioned aspects are as follows:

1. The end-users expect more advanced, customised and tailored (to their needs) decision support solutions, which will allow for flexible spatial threat visualisation, easy integration with new data sources or other systems, and information sharing between different entities engaged into a crisis management process.

2. The end-users desire accurate models and simulation tools that will allow for consequences, impact and risk analysis of CI failures and cascading effects. The forecasting capabilities are emphasised as ones of the most desired.

3. The end-users articulated the need of access to information related to CI from various sectors. They emphasised difficulties in gaining the data related to the operational state of private sectors CI and the CI-related information across public-public and national-regional borders.

3 Non-technical aspects of CIPRNet DSS services

3.1 General non-technical aspects for CIPRNet DSS services

There are a number of non-technical aspects that have to be taken into account when developing the CIPRNet DSS and before its services are launched. They concern the legal, organisational and long-term customer support issues.

The analysis of these aspects has been divided into two groups. Firstly, the aspects related to some specific conditions under which services will be deployed during the runtime of CIPRNet are described. Afterwards, general requirements for future EISAC services are provided.

3.2 CIPRNet project

During the CIPRNet project the aspects related to the legal, organisational and customer support will be addressed differently in contrast to typical commercial solutions aiming at business continuity, growth, and ravenous.

It must be emphasised that CIPRNet is a research project and as such it may follow different (non-commercial) regulations and limitations when it comes to licences related to data sources (e.g. geospatial data), software components (e.g. libraries and software frameworks), and third party external services (e.g. Google maps). Typically, these licences allow the researches to use mentioned before resources freely without being charged. However, as far as access to data is concerned, the CIPRNet consortium will not offer/allow for access to any raw/input data we use, only aggregated data or the results will be provided. The handling of data is guided by CIPRNet's Ethics Guidelines [D2.51].

When it comes to the organisational and customer support, during the project CIPRNet lifetime, all aspects related to services maintenance, bug-fixing, and responsibilities management will be handled by organisations developing certain services or its components. It must be also mentioned that all services, being part of a CIPRNet proof of concept, shall clearly define terms of use. Therefore, the end-users must be appropriately acknowledged that they use the services on their own risk without any warranty and their authors will not be liable for any damages arising from their use.

3.3 EISAC services

These aspects are related, in the first place, to some formal arrangements as regards the functioning of EISAC – what legal form it will take (of a company, non-profit organisation, association) and to the final form the DSS will take.

Establishing EISAC as a legal entity involves taking into account different legal aspects, as e.g., the intellectual property, liability, licensing, data collection, administrative legal overhead, sharing and protection and flexibility. The intellectual property protection may refer to EISAC as a legal entity and would thus, e.g., involve the protection of the name (trademark) that will be established for it. It may also refer to the products and services of EISAC. The CIPRNet DSS will contain data, information, software or other items coming from external entities. Care has to be taken to sign appropriate contracts with each of them. E.g., the input data to the DSS (data registries, pieces of software) will come from different sources. Each time a new data source is planned to be added to the system, the license conditions for the use of the data need to be checked with the owner of the data source. Some sets of data (or software) will be free of charge but, still, an agreement for using them may be needed. Some other ones will have to be paid for and the payment might be one-time or recurring. The licenses

might be periodic (even if long-term) and so the procedures have to be installed in order to check the validity of a given license and, if needed, to prolong it.

Some input data coming from external sources may not be licensed but a permission to use it will have to be granted. Such copyright issues will have to be checked when the DSS will use the publications, research results, data on CI, etc., coming from external bodies. Likewise, copyright and terms of use of all EISAC materials/products should be defined and communicated to the users, in case it should be used by them for their own purposes (e.g. for research). This approach (of checking the licenses/copyrights issues) should be applied for all the items that will form part of the CIPRNet DSS.

The names of the products and services should be carefully chosen and registered. It has to be remembered that the new EISAC services / products / inventions should be checked as whether they could be patented.

In case there are consolidated data in the system, e.g. the licensed one with not-licensed, the data filtration feature should be provided (filtration by rows and attributes), for the users not having the license to use a particular data source (attributes). Different access levels should be defined in the system, in order to reflect the user privileges and licenses – some content will be restricted to some users. This should be followed by providing different GUIs (Graphical User Interfaces) for those different access rights.

The direct access to the raw/input data by end-users will not be possible. The CIPRNet consortium will only reveal the analysis/processing results, of course, after the careful check regarding their sensitivity and privacy.

The end-users will be asked to share their private data, and so the privacy-related aspects have to be dealt with when designing, developing and then using the CIPRNet DSS. The provisions of the EU directive 95/46/EC [ECdir] have to be respected. This directive regulates the processing of personal data within the European Union, specifying the rules for data collecting, storing and using. The end-users should be aware of which data they are providing is being stored in the system and for what purpose. Data should then be used only for that specific purpose. The system provider should secure the users' personal data and should not disclose it without their consent. The users should be given the information as to who is collecting their data and they should have access to their data and be able to modify or delete it. A privacy policy should be defined for all services within the DSS and the users should accept it prior to using the service.

The taxation issues should also be considered (who is required to pay taxes, in which circumstances etc.) – they should be regulated by the law in force in the country of operation of a given provider.

For each service available in the DSS different SLA (Service Level Agreements) should be established for those using the service. The SLA should be different for different client types etc. The payment policies should also be established – they should be the same for all services. The terms of use of the services should be specified and they should probably be the part of the SLA (specifying the party responsible for wrong decisions etc.).

It is important to have a clear vision of who will be the owner of the CIPRNet DSS and what will be the responsibilities related to providing the DSS services, which may be decided on when a legal form for EISAC is agreed on. The system could be owned by EISAC that would have the coordinating role as regards the operation of the system. EISAC local representatives (e.g. in Italy, Germany) would be responsible for the operation of a given local system – they would have the system translated into local languages and they would be providing the services, dealing with data providers and users, maintaining the system etc. The questions related to the ownership of the system and the relations between the EISAC and the local EISAC

bodies should be clearly defined. Specific aspects important in this regard are: data management, data security, database maintenance, license procurement, and SLA negotiation.

All legal issues related to the responsibilities of local EISAC bodies should be decided on in accordance with the local law regulations.

One other non-technical issue that has to be taken into account when planning the CIPRNet DSS is the long-term customer support. Several issues related to this will have to be dealt with. Some of them concern the development phase, e.g., bug-reporting and solving and developing new features (who will pay for them). Long-term customer support also embraces issues related to infrastructure – who will pay for which part of it (hardware and software), how will the maintenance be dealt with, when should the hardware and software be replaced and who will cover the costs etc.

4 CIPRNet DSS services specification

In order to address the key end-users requirements, as described in the previous section, the following CIPRNet DSS services are specified in this document:

- Data accessing and gathering (DSS-DAG),
- Threat forecasting (DSS-TF),
- Threat visualisation (DSS-TV).

It is expected that the functionalities and the number of services provided by DSS will evolve over time. Therefore, a plug-and-play and easy to extend architecture of DSS is required (see Fig. 1).

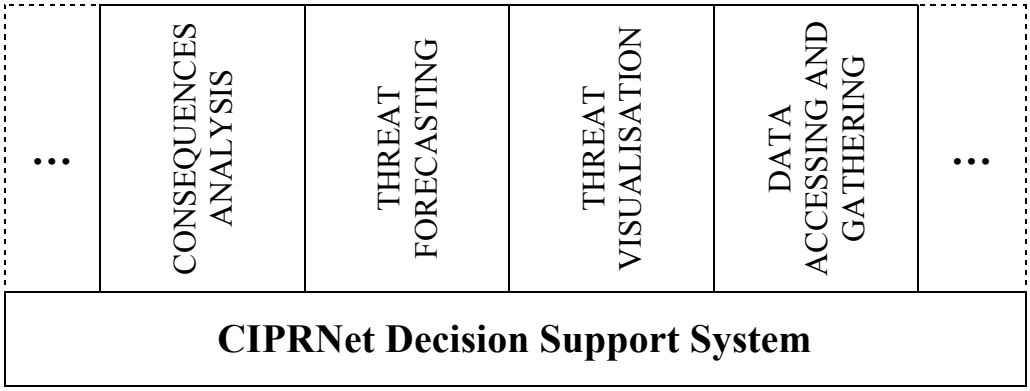

Fig. 1 Pluggable services provided by CIPRNet DSS

The CIPRNet DSS will have two distinctive operational modes, namely the "Hot Phase" and the "Cold Phase" decision support. The "Cold Phase" is dedicated to the Critical Infrastructure operators training purposes. It will be mainly based on historical data, modelling, simulation and analysis (MS&A). The "Hot Phase" includes continuous and real-time risk assessment, threat forecasting and consequences analysis conducted using real-time data during the real crisis.

It should be noted that the what-if[1] analysis (WIA) is not foreseen as one of the services of the DSS. The DSS and what-if analysis are developed within the CIPRNet project. The interaction between these two tools will be established through a dedicated interface and details will be provided in deliverable D7.5+D7.6 [D7.5+D7.6] and partially defined in D7.1 deliverable [D7.1].

4.1 Data accessing and gathering

4.1.1 Summary

Short name: **DSS-DAG**

This service allows the DSS to have available all data that is needed to run the CIPRNet DSS workflow and all information can be useful in order to mitigate and manage a crisis / emergency due to CI failures. In particular, the DSS-DAG service feeds data to the DSS-TF service (described in section 4.2) that has the aim to forecast the possible natural phenomena that, potentially, can produce physical damage to CI components in a given area.

[1] what-if analysis (WIA) – set of simulation tools that allows different courses of actions to be investigated.

4.1.2 Description

The DSS-DAG service will allow gathering and storing DSS relevant data to the CIPRNet DB (CIPRNet database). The data stored within the CIPRNet DB belongs, in general, to different pre-defined layers:

- Territorial layer,
- Socio-economical layer,
- Technological Infrastructure layer,
- Historical events layer.

Each layer can be divided into sub layers. For example, the historical events layer can be further divided into geological (e.g., earthquakes), geomorphological (e.g., landslides), hydro-meteorological (e.g., floods) historical events layer. The sources of data can be governmental repositories (e.g. the national GIS repositories as the Italian SINANET site, the Italian National Institute of Statistics – ISTAT), CI operators, data coming from simulation models such as the weather forecast data that needs to be logged in order to allow different kinds of offline analysis (e.g., statistical analysis).

In general, the data stored within the CIPRNet DB will require a different frequency of update operations. For example, the number of people living in a specific area needs to be updated once a year, while the historical events layer data (e.g., the earthquakes events in a specific area) needs to be updated with a frequency of minutes or hours. The update procedures will be performed using different modalities depending on data availability and update frequency requirements. In some cases the data updating operations will depend on authorised data scraping automated procedures. The CIPRNet DB will store the already available historical data (e.g. rain precipitation data) and will allow the development and the maintenance of historical series of data. The CIPRNet DSS can also use external repositories (e.g., via GIS WMS[2] protocols).

4.1.3 Input information

The Table 1 shows an example of the possible input information for the DSS running on the Italian EISAC node (I-EISAC).

Table 1: Input information for the DSS-DAG service

Data	Source	Availability	Layer	Update Frequency	Logging
Basic GIS Layers - Italy (Administrative boundaries, road network, railways, hydrograph, urban areas, etc.)	ISPRA – SINANET [ISP]	Full	Territorial	Occasionally	Yes
Digital Terrain Model (DTM, 20 m ground spacing)	ISPRA – SINANET [ISP]	Full	Territorial	-	Yes
Inventory of Landslide Phenomena in Italy - IFFI	ISPRA [ISP]	WMS	Territorial	Occasionally	Yes
Corine Land Cover - CLC (2006)	EEA [EEA]	Full	Territorial	6-10 years	Yes
Census Data, Parcels and	ISTAT	Full	Socio-	10 years	Yes

[2] Web Map Service (WMS) is a standard protocol for serving geo-referenced map images over the Internet that are generated by a map server using data from a GIS database.

Data	Source	Availability	Layer	Update Frequency	Logging
Indicators			economical		
Parametric catalogue of damaging earthquakes in Italy, Seismic risk maps	INGV [INGV]	Full	Historical events	Annual	Yes
Seismic event data (epicentre and magnitude), PGA and Shake Maps	INGV [INGV]	Via web	Historical events	10 Minutes	Yes
Nowcasting data and maps	Himet	Full	Historical events	Hourly	Yes

The end-user perspective

The DSS-DAG service capabilities are related to the end-users requirements and expectations, which have been presented in the deliverable D5.1 [D5.1]. Therefore, DSS-DAG should address the aspects specified in D5.1, presented in Table 2.

Table 2: General requirements related to the Data Accessing and Gathering service

Requirement ID	Description
FUNC_req#50	Allow for using real-time (or near real-time) sensorial data.
FUNC_req#60	Allow for using common geo-localisation data for analysed CI.
DATA_req#30	Provide analysed information (e.g. besides the raw data), however be able to provide the raw data, whenever it is needed.
DATA_req#40	Allow for integration of meteo-climatological data, predictions and simulations.
DATA_req#50	Include historical data (e.g. hydrological, statistics, lessons learned) in analyses.
DATA_req#60	Examples of the raw data to be considered are as follows: • seismic monitoring network (to obtain data about earthquakes such as localisation and magnitude), • meteorological satellites network, • now-casting radar monitoring network, • satellite images: multispectral and/or SAR (Synthetic-aperture radar), • geographic web services (via WMS, WFS, WCS protocols), • flood forecasting (e.g. EFAS).
DATA_req#70	This should engage push and pull models that will be capable of storing a subset of gathered data in the CIPRNet DB.
DATA_req#80	Use data coming from various sensors (e.g. meteorological data, hydrological models, etc.) and monitoring networks to forecast natural hazards such as precipitation abundance, wind speed etc.

4.2 Threat forecasting

4.2.1 Summary

Short name: **DSS-TF**

This service provides the DSS with the capability to forecast natural events that have the potential to harm the CI components (e.g., heavy rain, flooding, landslide, drought, heat wave, etc.).

4.2.2 Description

The capability to predict a possible natural phenomenon that, potentially, can produce physical damage to the CI components in a given area is one of the key features of the DSS. The DSS-TF is composed of different modules, each dedicated to a specific source of perturbation to be monitored. In particular, the DSS-TF through the data accessing and gathering services will acquire different kinds of data: weather forecast data, now-casting data, and earth observation data. Each module will use this data to run specific models to forecast specific threats on a specific area. For instance, the Flooding module will acquire data that can be used to forecast flooding events in a given area (e.g. abundant and prolonged precipitation, pluviometric monitoring sensor networks). The plug-and-play and easy to extend architecture of the DSS will allow connecting the CIPRNET DSS modules, which will be implemented to provide specific threat forecasting capabilities for specific areas. Indeed, the DSS-TF service can be configured in order to rely on already available data and models. For example, an instance of the DSS-TF Flooding module for the city of Rome can be configured to include the already available data, which is related to the monitoring sensor network owned by the Autorità del Bacino Tevere (Tiber Basin Authority). The main modules to be included in the DSS-TF service are:

- Flooding,
- Lightening,
- Landslide,
- Strong wind,
- Heavy snow,
- Heavy rain,
- Cold wave,
- Heat wave,
- etc.

The role of the service

For each CI component, the DSS-TF service will produce a threat strength matrix that represents the probability that the given threats will materialise in a given area and the related strength of a threat. Table 3 is an example of a threat strength matrix for a given CI component. The rows of the matrix represent the considered threats and the columns the threat strength. The matrix entries indicate the probabilities that the CI component will be affected by a threat of a strength as indicated in the column value. Considering the Table 3, the DSS-TF service indicates that the specific CI component will be impacted by a flooding event of strength 4 and by strong wind of strength 3.

Table 3: Threat strength matrix

Threat level	1	2	3	4	5
Earthquake (ground acceleration)	0	0	0	0	0
Strong Wind	0	0	1	0	0
Lightening	0	0	0	0	0
Heavy snowfall	0	0	0	0	0
Ice	0	0	0	0	0
Landslide	0	0	0	0	0
Flash flood	0	0	0	0	0
Flooding	0	0	0	1	0
Mud flows	0	0	0	0	0
Debris avalanches	0	0	0	0	0
Heavy Rain	0	0	0	0	0
Strom surge	0	0	0	0	0
...	0	0	0	0	0

The prediction matrix will be compared with the *vulnerability matrix* that represents the vulnerability of the considered CI element with regard to the predicted events. For example, let's suppose that the vulnerability matrix for the transformer TR1 states that the element is vulnerable to flooding of strength 4 and that the threat strength matrix indicates that this specific CI element will be impacted by a flooding of strength 4; then, in the subsequent flow of computation, the DSS will consider the TR1 element in fault.

The end-user perspective

The DSS-TF service is related and/or contributes to the satisfaction of to the general requirements, which have been presented in the Table 4.

Table 4: General requirements related to the Threat Forecasting service

Requirement ID	Description
FUNC_req#90	Support evaluation of vulnerabilities of different CI systems.
FUNC_req#120	Enable analysis of scenarios within different geographical range.
FUNC_req#130	Forecast damage scenarios involving components of CI.
DATA_req#100	Extract and manipulate DSS-TF input data in order to forecast natural hazards (e.g. uses nowcasting data to predict the amount of precipitation on a specific area)
GUI_req#10	Be able to provide local/global view according to current needs of the operator.
GUI_req#70	Show the current operational status of the system and visualise how it works.

The end-users of the DSS-TF service are mainly CI operators, Civil Protection operators and CIP analysts. The end-users trough the DSS-TV services will be able to visualise CI components *Risk Maps*. The Risk Maps will present, for each CI component, in a user-friendly way,

the CI threats strength matrix that represents the probability that the CI component will be impacted by the threats.

The key properties of the service

Fig. 2 shows the main components of the DSS architecture that realise the DSS-TF.

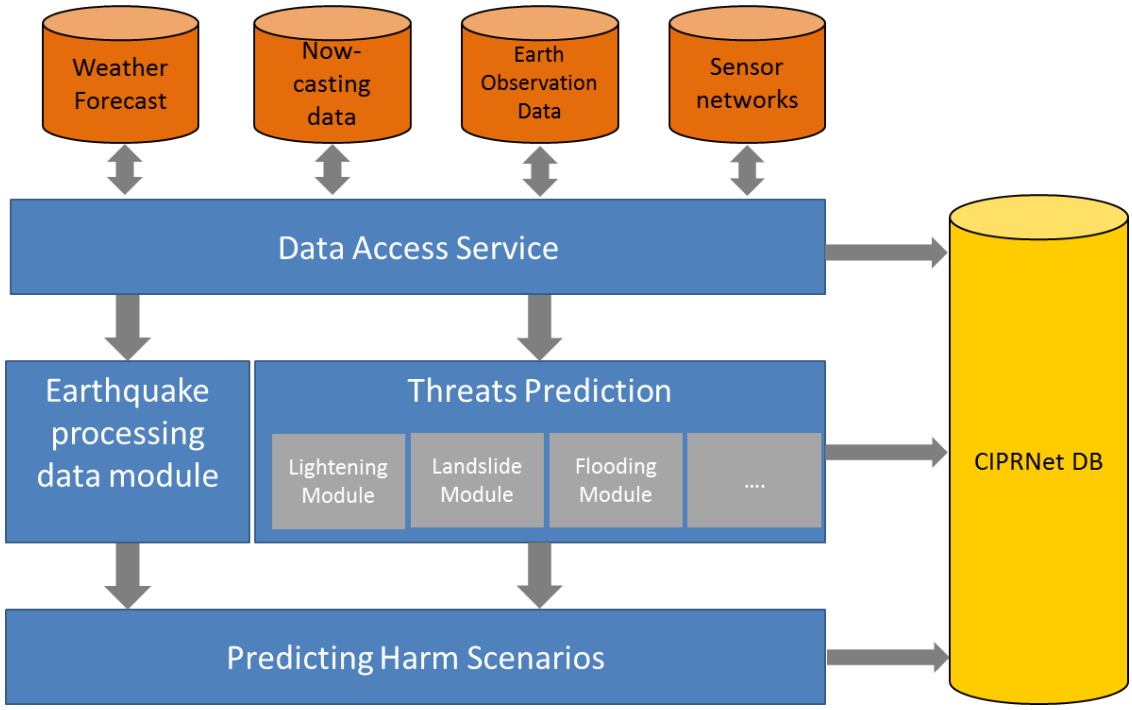

Fig. 2: DSS Threat forecasting architecture

The Data Accessing Service, a component of the Data Accessing and Gathering Service, acquires data from external sources. This data is acquired and stored within the CIPRNet DB. This data is used by the different Threat Prediction modules for forecasting the threats and to build, for each CI component, the Threat Strength Matrix. The DSS-TF realises a specific workflow for the earthquake case. Indeed, the earthquake events are monitored by the DSS through the acquisition of seismic sensor networks. This data (e.g., earthquake epicentre and magnitude) is used by the earthquake processing data module to compute detailed shake-maps. Those will be used to assess the impact of an earthquake event In particular, for the earthquake workflow, it is possible to define the following specific requirements:

Table 5: Earthquake workflow requirements

Requirement ID	Description
FUNC_req#91	Support evaluation of vulnerabilities of different CI systems w.r.t earthquake events
FUNC_req#131	Using epicentre, location and estimated magnitude of important (i.e. above a fixed threshold) the DSS must produce theoretical shake-map
FUNC_req#132	Using theoretical shake-map and GIS territorial, infrastructure data produce excepted damage map
FUNC_req#133	The DSS should acquire actual earthquake event shake maps
FUNC_req#134	The DSS should produce refined damage maps
DATA_req#101	Acquire epicentre location and estimated magnitude of earthquake

	from national sensor networks.
GUI_req#11	Visualize earthquake events on the map. The visualization must help the user to clearly and easily understand the magnitude of the earthquake event.
GUI_req#71	The DSS must show earthquake event excepted damage map.
GUI_req#72	The DSS should show earthquake event refined damage map.

For natural threats that can be predicted, as for example, abundant rain precipitation The DSS-TF service implement the general requirements of Table 4.

4.2.3 Input information

The input to the DSS-TF service includes different sources, namely:

- Meteorological data,
  - Weather forecast data,
  - Now-casting data;
- Sensor networks data;
- Earth Observation data;
- Historical data,
  - Landslide data,
  - Lightning data.

4.2.4 Output information

The *Threat Strength Matrix* established for each CI component represents the output of the DSS-TF service.

4.3 Threat visualisation

4.3.1 Summary

Short name: **DSS-TV**

This service provides the DSS with a variety of visualisation capabilities.

4.3.2 Description

Visualisation is one of the key functionalities of the decision support systems. This section introduces the key functionalities that a visualisation service should provide in order to fulfil the CIPRNet end-user requirements.

The role of the service

The role of the service is to use different means to visualise a wide variety of aspects related to the decision support process, such as:

- Consequences analysis (e.g., consequence of impact on CI or its components).
- Threat forecasting (e.g., prediction of natural disasters like flood which may impose threats to CI).
- Risk assessment (e.g., with respect to the CIPRNet project consequences criteria).

- Analysis of emergency situations/scenarios, and assessment of how such scenarios may evolve, including the visualisation of possible courses of actions.
- Assessment of how big is the geographical area that has been impacted by the natural hazard.
- Prediction of possible effects of the natural hazards (e.g., using cross-referenced layers of geographical regions combining spatial information about the CI and natural hazards).
- Identification of the factors that may have influence on further development of the crisis scenario (changing weather conditions, probable threats coming from objects or CI located in impacted area).

The examples of the visualised capabilities may include:

- Prediction of a threat by means of aerial or GIS maps (e.g. Fig. 3).
- Measured/Predicted CI services disruptions.
- Measured/Predicted level of damage (caused by natural hazards, like floods earthquakes, etc.).
- Expected/Predicted second order consequences of natural hazards (e.g. influence of abundant precipitation on the electrical, gas, and transportation domain).

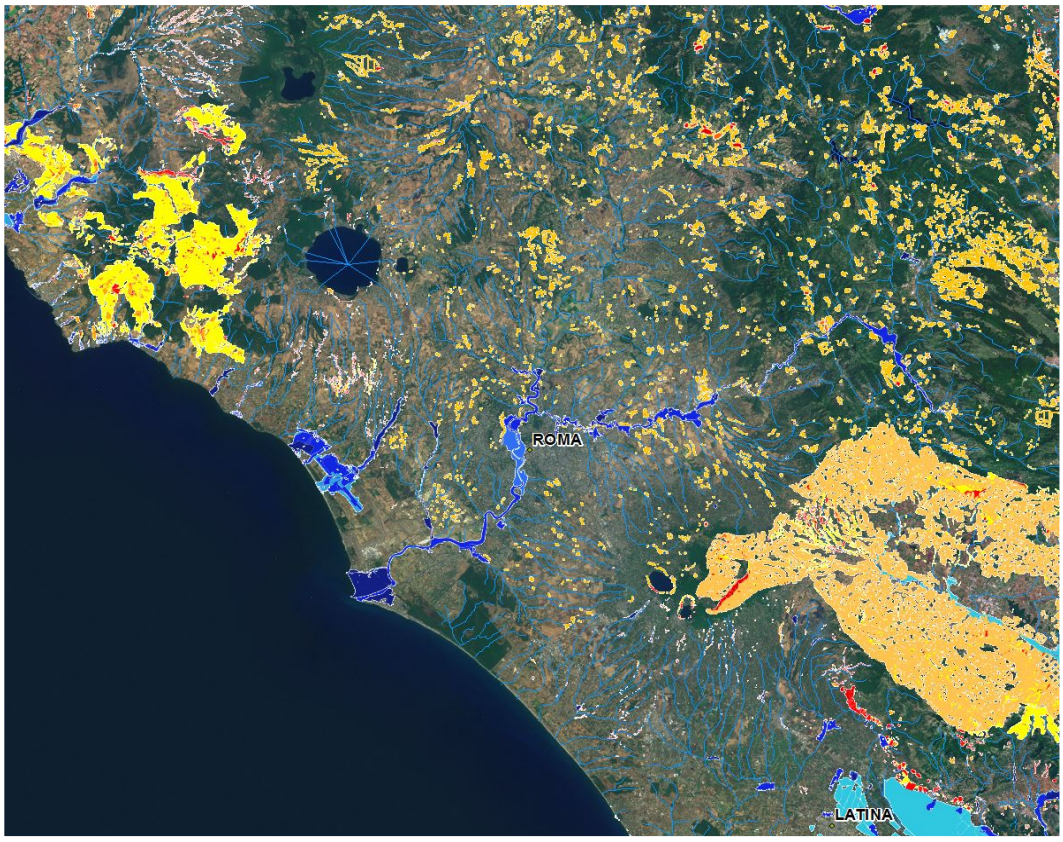

Fig. 3 Example of hydrogeological risk map

The end-user perspective

The DSS-TV service capabilities are strongly related to the end-users requirements and expectations, which have been presented in the deliverable D5.1. Therefore, DSS-TV should address the aspects specified in D5.1, presented inTable 6.

Table 6: General requirements related to visualisation aspects

Requirement ID	Description
GUI_req#10	Be able to provide a global/local view (e.g. zoom to a specific part of an analysed region).
GUI_req#20/30	Be intuitive and user-friendly (e.g. use common/national format for visualising icons).
GUI_req#50	Be able to support maps with multiple CI layers including identification of their state.
GUI_req#60	Be able to integrate with other threat visualisation systems/maps (e.g. interoperability in cross-border emergency management).

There are also other aspects related to the functional capabilities of the visualisation service, which are connected with the interaction between the end-user and the service, namely:

- View navigation,
  - Intuitive zooming and view panning,
  - Object selection,
  - View rotation;
- Customisation of viewed items,
  - Colours customisation,
  - Icon customisation,
  - Text and fonts customisation;
- Layers support (in order to view some different information on a different layer);
- Intuitive switching between the visualised layers;
- Ability to connect to databases/data sources containing spatial information;
- Different GUI for different types of users (some information may be restricted to a particular group of users, thus DSS-TV shall provide user authorisation).

The key properties of the service

Typically, the key element in the architecture of the decision support systems for emergency management is the GIS. Therefore, the DSS-TV should incorporate this visualisation technique in order to communicate wide variety of decision support aspects. Particularly, such visualisation must:

- Provide an efficient and flexible way to access the threat visualisation data (e.g. web-based trough web-browser or desktop GIS clients). An example of web-browser GUI is shown in Fig. 4.
- Provide the ability to handle multiple simultaneous requests for visualisation (e.g., centralised web-based repository that is able to handle multiple read/write concurrent connections).
- Provide the ability to share the provided visualisations among private and public stakeholders, emergency managers and common citizens involved in the disaster response.

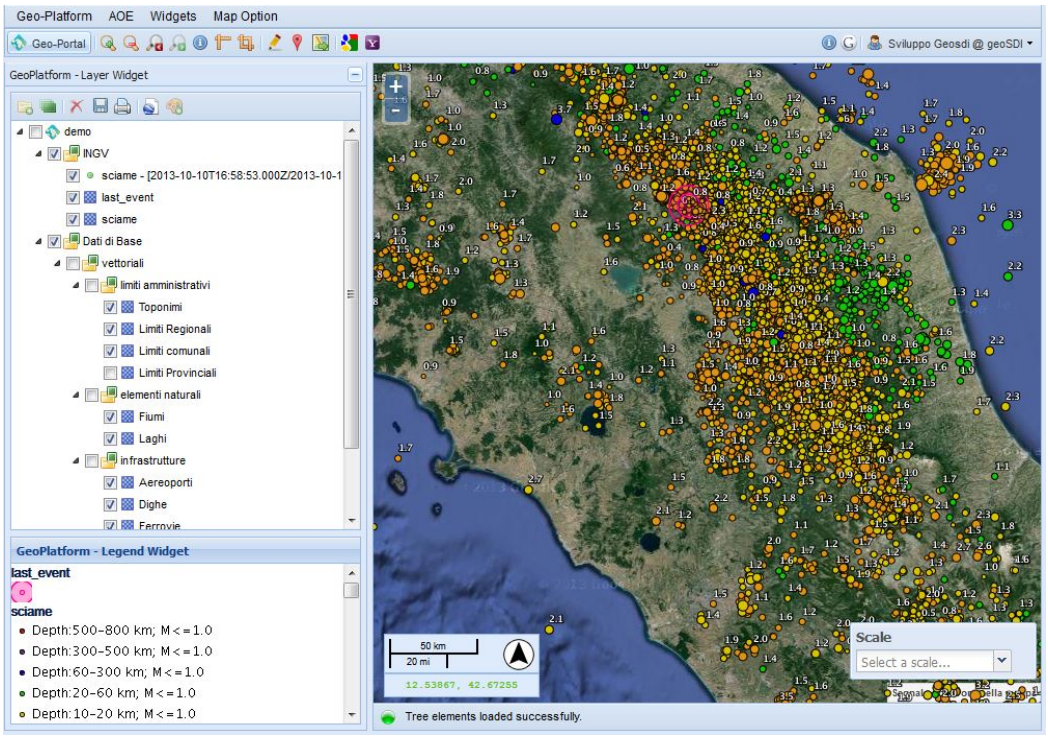

Fig. 4: Example of web-based DSS GUI

Fig. 5 shows exemplary layers which visualise the impact of a natural hazard on the geographical region. The most common visualisation map is shown on the left-hand side image of Fig. 5. The data that is visualised indicates the flooded area and can be obtained either in real-time (e.g. via sensor networks) or from simulations tools. The data is geo-referenced with the map of the impacted region and allows the user to evaluate the impact of the natural hazard and conduct the further investigation. The second map (right-hand side image of Fig. 5) shows the second step of impact analysis. The map with the impacted area of the geographical region has been geo-referenced with the layer containing the information about the transportation infrastructure. The red colour indicates the high impact while the green colour suggests that roads in the given regions that remain undamaged.

Fig. 5: Examples of different layers. Left-hand side image indicates the flooded area (blue region). The right-hand side image shows the transportation infrastructure that has been impacted by flood (red colour)

In Fig. 6 the map of the flooded area has been additionally geo-referenced with geographical position of key elements of electrical infrastructure like electrical transformers, high-voltage power lines, etc.

Fig. 6: Example of a layer showing electrical infrastructure impacted by flooding

4.3.3 Input information

The input information will include both real-time and historical data. The visualised data will also include complete and partial results obtained from simulations and multi-domain data analysis.

4.3.4 Output information

The output will be in the form of:

- Interactive geographical maps (e.g. geoSDI, Google Maps, openmaps, WebGis),
- Interactive tabular data,
- Data streams, serialized objects (e.g. JSON, XML) accessible via RESTful API (or SOAP).

4.3.5 UML deployment diagrams

The general deployment diagram is shown in the Fig. 7. The visualisation service will expose a typical web-based client-server architecture. The client will communicate with the web server over the HTTP(S) protocol. The visualisation will strongly depend on WebGIS (responsible for spatial data manipulation) module and CIPRNet DB.

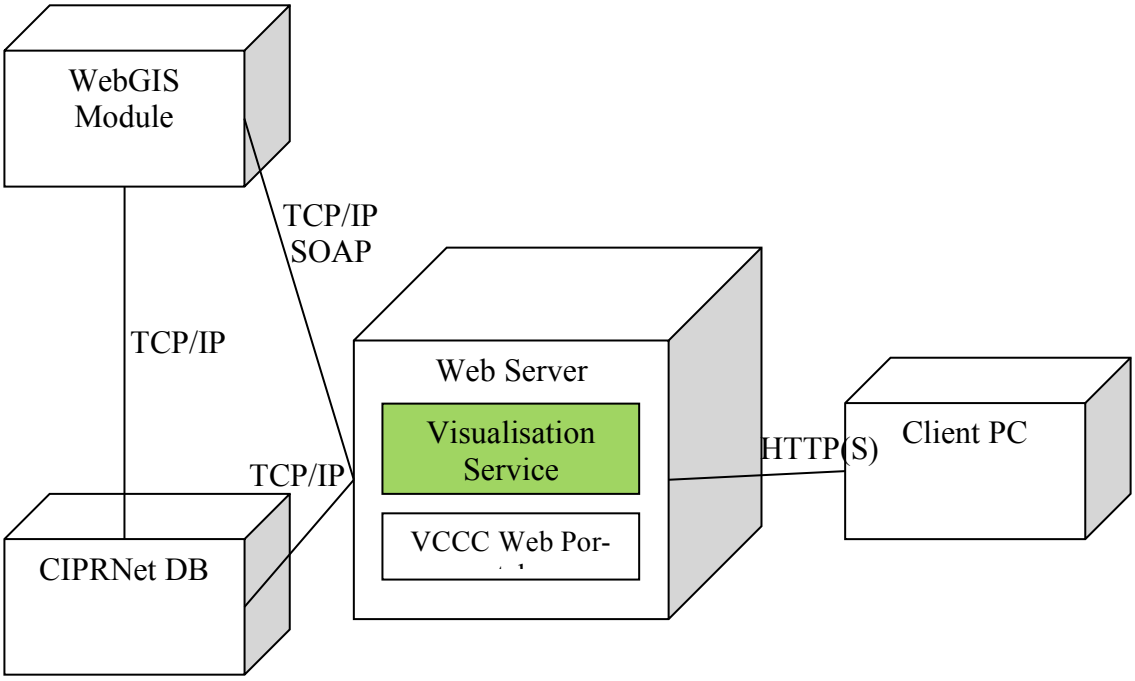

Fig. 7: Visualisation Service – deployment diagram

4.3.6 UML use cases diagrams

In this section general use cases for the visualisation service have been presented. The key goal is to highlight the most important functional elements of this service with the focus on its users (actors).

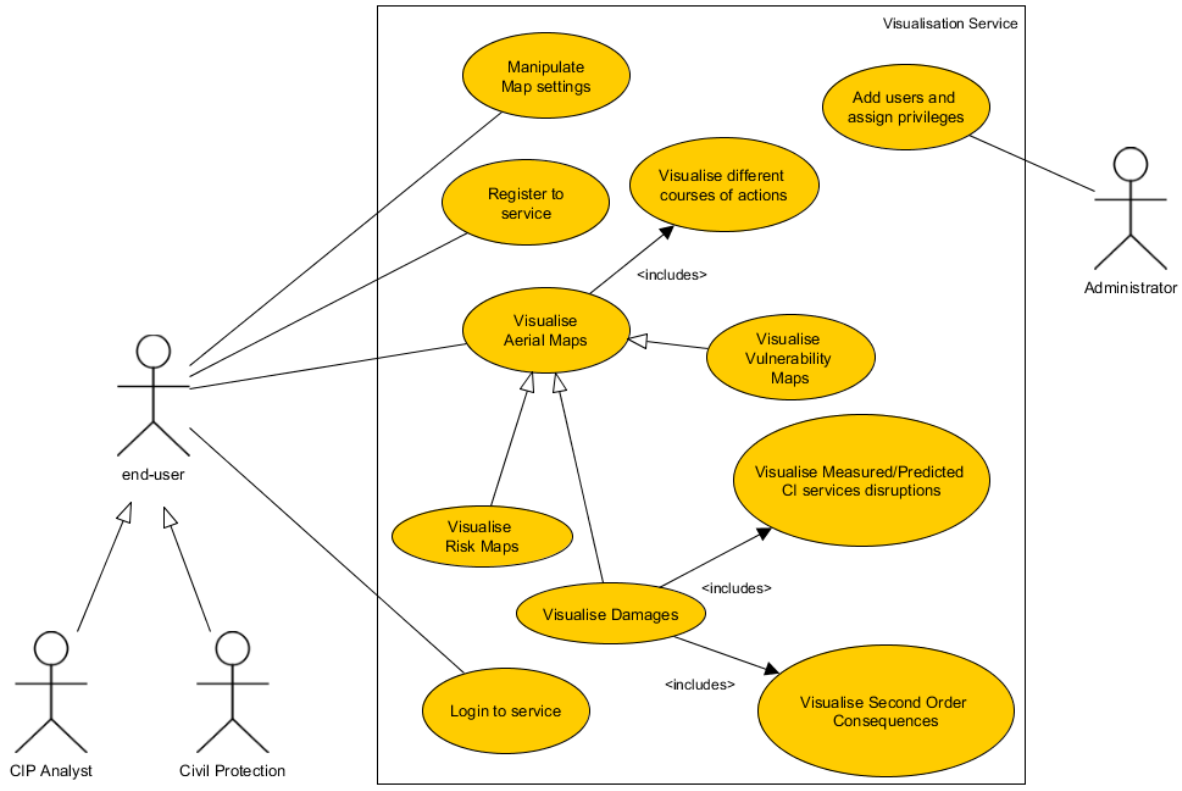

Fig. 8: Use cases diagram for visualisation service

4.3.7 Detailed descriptions of use cases

Use case id	UC-DSS-TV-01
Use case name	Visualise Aerial Maps
Actors involved	End-user
Description	1. System visualises aerial images that are relevant to the analysed scenario. 2. System interacts with the map intuitively, zooming the view, dragging the map and switching between different layers.
Pre-conditions	User is registered and logged to the service.
Post-conditions	User can generate the hard copy of the visualised map (e.g. PDF format or printed version).
Quality expectations	Maps are rendered on screen without significant delay.

Use case id	UC-DSS-TV-02
Use case name	Visualise Risk Maps
Actors involved	End-user
Description	1. System visualises risk maps. 2. Different colours allow the user to indicate the risk values. 3. System visualises the risk factors in a tabular form.
Pre-conditions	User is registered and logged to the service.
Post-conditions	User can generate the hard copy of the visualised map.
Quality expectations	Maps and tabular data are rendered on screen without significant delay.

Use case id	UC-DSS-TV-03
Use case name	Visualise Vulnerability Maps
Actors involved	End-user
Description	1. System visualises vulnerabilities of a given CI to a given threat. 2. Different colours allow the user to indicate the vulnerability values.
Pre-conditions	User is registered and logged to the service.
Post-conditions	User can generate the hard copy of the visualised map.
Quality expectations	Maps and tabular data are rendered on screen without significant delay.

Use case id	UC-DSS-TV-04
Use case name	Visualise Damages
Actors involved	End-user
Description	1. System visualises damages to a given CI. 2. User reads the level of damage using colours present on map.
Pre-conditions	User is registered and logged to the service.

Post-conditions	User can generate the hard copy of the visualised map.
Quality expectations	Maps and tabular data are rendered on screen without significant delay.

Use case id	UC-DSS-TV-05
Use case name	Manipulate Map Settings
Actors involved	End-user
Description	User manipulates/customises different types of settings of the maps: • Level of details, • Colours to display different aspects (e.g., level of risk), • Customised icons to display different aspects (threats, resources, etc.), • GUI schema.
Pre-conditions	User is registered and logged to the service.
Post-conditions	User can generate the hard copy of the visualised map.
Quality expectations	-

Use case id	UC-DSS-TV-06
Use case name	Visualise measured/predicted CI services disruption
Actors involved	End-user
Description	System visualises CI service disruption.
Pre-conditions	User is registered and logged to the service.
Post-conditions	User can generate the hard copy of the visualised map.
Quality expectations	Maps or tabular data are rendered on screen without significant delay.

Use case id	UC-DSS-TV-07
Use case name	Visualise Second order consequences
Actors involved	End-user
Description	System visualises second order consequences.
Pre-conditions	User is registered and logged to the service.
Post-conditions	User can generate the hard copy of the visualised map.
Quality expectations	Maps are rendered on screen without significant delay.

Use case id	UC-DSS-TV-08
Use case name	Register To service
Actors involved	End-user
Description	User registers to the service.
Pre-conditions	Administrator activates to registered accounts and assigns privileges.
Post-conditions	User can only access to these resources which have been restricted by the administrator.

Quality expectations	-

Use case id	UC-DSS-TV-09
Use case name	Login to service
Actors involved	End-user
Description	User logs in to the services with credential provided by the administrator.
Pre-conditions	User is registered.
Post-conditions	-
Quality expectations	-

Use case id	UC-DSS-TV-10
Use case name	Add users and assign privileges
Actors involved	Administrator
Description	1. Administrator adds new users. 2. Administrator assigns privileges to users. 3. Administrator restricts access to different resources with respect to the assigned privileges.
Pre-conditions	-
Post-conditions	-
Quality expectations	-

4.4 Consequence analysis

Basic specification of the "Consequence analysis" service is provided in the separate CIPRNet deliverables – D6.1 [D6.1] and D7.1 [D7.1]. A joint additional document describing the common conceptualisation of Consequence Analysis is currently under preparation. Moreover, more precise descriptions of the implementation of the Consequence Analysis module will be provided in forthcoming Deliverables D7.3, D7.4 and D6.4 (see CIPRNet DoW [DoW]).

5 VCCC (Virtual centre of competence and expertise in CIP) services specification

CIPRNet's VCCC (Virtual centre of competence and expertise in CIP) is a predecessor of the planned facility EISAC (European Infrastructure Simulation and Analysis Centre). The VCCC will provide certain added-value services to its audiences. These services will be delivered by means of the VCCC web portal to the audiences. Some of the services are related to the new capabilities that CIPRNet is currently developing for its initial audience. This section describes the services that will be deployed through the VCCC web portal.

5.1 "Ask the expert" service

5.1.1 Summary

Short name: **Ask the Expert**

During CIPRNet, this end-user service will be provided for a limited period of time and will allow CIP stakeholders to:

- Request the information about any CI aspect related to the CI operation, threats, management, etc., and to
- Get feedback on such query from the CIPRNet community of experts.

5.1.2 Description

The "Ask the Expert" service will accessible via the CIPRNet VCCC portal. End-users will submit questions and requests for information from the CIP domain. Questions can be related (however, not limited) to:

- Technical CIP-related issues,
- CI management, crisis management for CI,
- CI-related documentation, e.g. national and EU regulations, policies, public reports and statistical data,
- Practical aspects of CI functioning.

The expected users of this service include public authorities, CI stakeholders (operators, administrators), SMEs, research & academia and society. The effects of using this service can be two-fold:

- If the question is pertinent with the CIPRNet aims and scope, end-users will receive a short answer by the CIPRNet expert and/or links to publicly available sources (if this is justifiable in the context of a given question),
- For more complex questions, the requesting user will be put in contact with the most appropriate CIPRNet expert(s), selected from the pool of experts, based on the subject raised by the user.

The "Ask the Expert" service will incorporate a number of procedures to guarantee possible anonymisation of the query, to protect data and queries from being publicised (if requested) and to ensure the secure protocols for the authentication of the user.

The main functionalities of the service include:

- Requesting the information via a pre-formatted form (e.g. a form with such fields as: subject, description, domain type/name, etc.),

- Registration of request and its maintenance,
- Maintaining the database of experts providing the knowledge for the service purposes. Such database should contain at least the following information: expert status (available/non-available), contact info, domain of expertise, scope of the possible issues to be solved,
- Filtering of requests (e.g. to reject nonsense, out of the service scope, or too trivial requests, spam messages, etc.),
- Queuing (including storage of waiting requests with their status – e.g. solved, in progress, unsolvable, etc.) and sorting the requests based on category/topic,
- Distribution of particular requests to the most appropriate CIPRNet experts,
- Replying to the question by the expert,
- Safe storage of (anonymised) past questions and answers in order to:
    - Control the utilisation of experts,
    - Control the distribution of topics, themes and question categories,
    - Control the quality of service (e.g. issues unsolved vs. overall number of investigated issues),
- Building the repository of the frequently asked questions (FAQs) and answers to optimise the utilisation of expert resources (by an automatic reuse of the most relevant answer to a given frequently asked question),
- Privacy and security functions and settings, e.g. to define the anonymity level of a request, whether the query/request will be publicised and available for a wider audience, etc.
- Detailed specification of the "Ask the Expert" service will be provided in separate deliverable (D5.3 "Ask the Expert capability")

Due to the limited resources and time frame of CIPRNet, CIPRNet will provide the "Ask the Expert" services only for a limited time. If the service proves useful for CIPRNet's audiences, it would be included in the roadmaps for EISAC, such that EISAC could make that a permanent service.

5.1.3 Input information

The main input information for this service will be the practical and theoretical knowledge of the CIP experts that will serve as a source of the CIP-related information and expertise. Additionally, resources collected for the CIPedia service (e.g. links to the CIP documents) could serve as background resources for the "Ask the Expert" capability, complementing the experts' answers.

5.1.4 Output information

The output information during the service operation will be:

- The experts' answers to the particular questions,
- A list of frequent (historical) questions and answers that the user can investigate (and find solution) before contacting the expert.

5.2 CIPedia service

5.2.1 Summary

Short name: **CIPedia**

This service provides the access to the CIP-related information shared for and by the CIP community.

5.2.2 Description

CIPedia is one of the means providing the innovation of the CIP domain by the CIPRNet project and is defined in deliverable D8.4 [D8.4]. CIPedia is a multi-disciplinary online glossary of terms related to CIP. The rationale for CIPedia is the need for common understanding of the CIP-related context by the multi-disciplinary CIP community. To date, there is no comprehensive glossary covering the terms that are important for CIP.

CIPedia is also a participatory platform for cross-domain community building. Each member of this community can bring his/her view on particular CIP knowledge elements and share it. In this sense, CIPedia will be the place in which different visions, definitions and points of view are mixed, in order to develop a common understanding of the CIP-related aspects. In result, CIPedia will foster an international collaboration of experts from the CI domain and will improve the cross-communication and creative discussion between them. The main assumption is that CIPedia will be a multinational, multidisciplinary and cross-sector tool for anyone looking for CI- and CIP-related definitions.

The role of the service

CIPedia is an online glossary, similar to other Wiki-like services (such as the Wikipedia). CIPedia is already online [CIPedia] and will be one of the components of the CIPRNet's VCCC web portal.

The main characteristics of Wiki-like services (thus also CIPedia) include:

- Simplicity of content creation (using simplified mark-up language), moderation and maintenance,
- High usefulness, easiness of navigation and content searching,
- Openness for adding new content and improving the existing information.

The initial content provided by the service was the CIP glossary, developed in the IRRIIS and DIESIS projects, and glossaries created as part of ERNCIP activities. These glossaries have been converted into a Wiki-like online service [CIPedia]. In a longer perspective, CIPedia will contain also information on European and international CIP policies, links to main policy and regulatory documents, CIP-related inventories and databases, etc.

The target audiences for CIPedia are all groups of stakeholders, including policy-makers, competent authorities, CIP operators and owners, manufacturers, CIP-related facilities and laboratories, and the society.

The end-user perspective

From the perspective of the CIPedia users, the service will allow for:

- Applying for a user account,
- Logging in / Logging out to/from the service,

- Creating a new content and organising it in the CIPedia structure (assigning a given article to the particular category, linking the part of the newly introduced content to the existing content using hypertext links),
- Searching for the information and navigating within the available content categories and articles,
- Modifying the existing content, including enhancing the article by the new information and deletion of particular parts of the article,
- Viewing / tracking the history of the articles (reviews and amendments),
- Viewing a particular article in different languages (if translation is available).

The key properties of the service

From the perspective of the CIPedia administration and maintenance, the service will allow for:

- Creating an account of the CIPedia user and registration for the purposes of using CIPedia,
- Verifying the newly created accounts (including security verification, e.g. anti-botnet measures),
- Assigning the newly created accounts to the pre-defined groups of users (e.g. administrators, moderators, reviewers, standard users, etc.),
- Safe storage of the online identities owned by the registered users of the service,
- Safe storage and indexing of the online content (actual and backups of historical articles, articles discussed before verification, etc.),
- Organising the content in various (Wikipedia-like) categories. The specified categories (e.g. one for glossary, another for policies, law acts, etc.) will improve the usability of the service and improve the effectiveness of the navigation, while using the CIPedia.
- Verifying, reviewing and (in result) accepting or not the user created content. Such mechanisms are necessary to maintain the reliability and trustworthiness of information generated by users. Other purpose of these functionalities is the security of users which should assure that e.g. external HTTP links placed in the article text will not redirect them to a malicious website,
- Tracing and logging the activities performed on content, as well as viewing the past versions of a given article, in order to restore it in the case of so-called “online vandalism”.

The security-related functionalities result from the fact that both the CIPedia and Wiki services are focused on openness and allow the broad spectrum of users (often anonymous in terms of expertise, knowledge, intentions) to access. Therefore, mechanisms such as access control, verification of user-generated content and other security measures are essential to keep order and provide the quality of the collected content.

5.2.3 Input information

Input information for the CIPRNet CIPedia service will be the CIP glossary developed during the project by the CIPRNet consortium, standard definitions of terms from other sources, national working definitions, and further CI-related knowledge introduced to the repository as user-generated content.

5.2.4 Output information

Output information will be the Wiki-like pages and articles, organised in a structured manner and containing CIP-related knowledge and information (cf. [D8.4] and [CIPedia]).

5.2.5 UML deployment diagrams

The CIPedia service will not require any pre-installed services (mentioned in this document) to operate. It can be deployed on the same web server as the VCCC Web Portal. It will require any relational database where the content will be stored. For performance and security reasons it is suggested to run the database on a dedicated server (e.g. a different database server from the VCCC-dedicated one). The deployment diagram is shown in the Fig. 9.

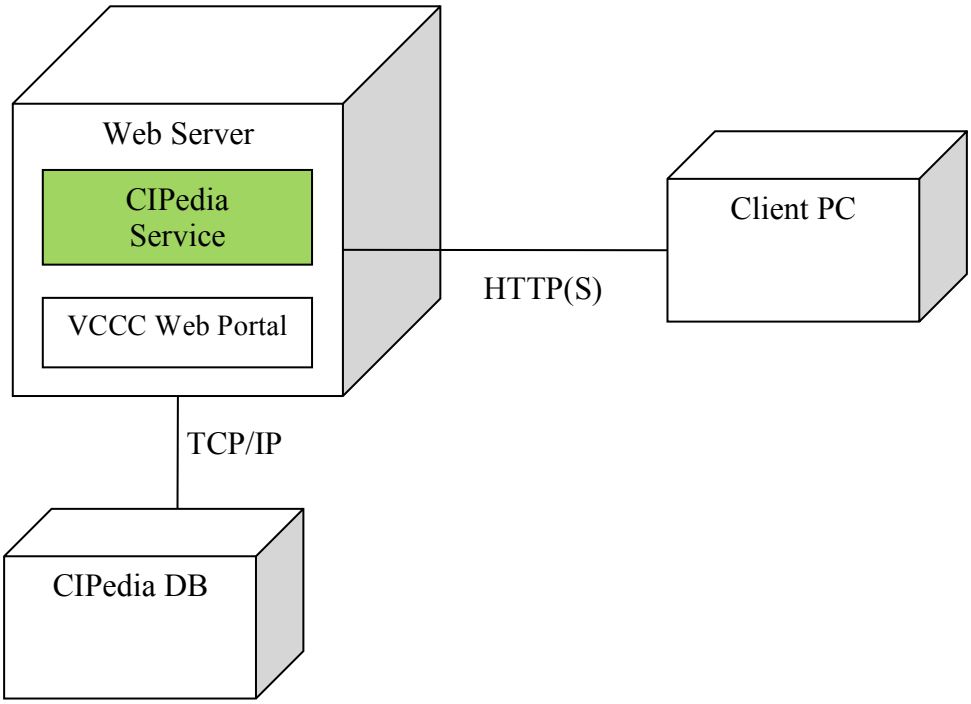

Fig. 9: CIPedia service deployment diagram

5.2.6 UML use cases diagrams

The CIPedia use cases diagram is shown in the Fig. 10. There are two distinctive actors of this service, namely: User and Administrator. Detailed description of each use case is provided below the diagram.

Fig. 10: CIPedia service use cases diagram

Use case id	UC-CIPedia-01
Use case name	Manage accounts
Actors involved	Admin
Description	Administrator makes one of the following actions: 1. Activates the accounts created by the user. 2. Deletes accounts. 3. Modifies privileges.
Pre-conditions	Admin must be logged.
Post-conditions	-
Quality expectations	-

Use case id	UC-CIPedia-02
Use case name	Register
Actors involved	User
Description	User registers to CIPedia trough a dedicated online form. User must fill all the required data.
Pre-conditions	-
Post-conditions	User account is created but not active.
Quality expectations	CIPedia must avoid dealing with any personal data.

Use case id	UC-CIPedia-03
Use case name	Login
Actors involved	User, Admin
Description	User or Admin login to the service using credentials.
Pre-conditions	-
Post-conditions	-
Quality expectations	-

Use case id	UC-CIPedia-04
Use case name	Manage Content
Actors involved	User, Admin
Description	Depending on action the actor intends to do, it is possible to: 1. View Content. 2. Create New Content. 3. Modify Content. 4. Review Content. 5. Accept/Reject New Content.
Pre-conditions	1. Actor is logged in to the service. 2. Privileges allow the actor to perform a given action.
Post-conditions	-
Quality expectations	-

Use case id	UC-CIPedia-05
Use case name	Search information
Actors involved	User
Description	User searches the CIPedia content using different criteria.
Pre-conditions	User is logged in.
Post-conditions	-
Quality expectations	Result is returned without any noticeable delay.

5.3 "What if" analysis function principle service

5.3.1 Summary

Short name: **"What if" analysis mock-up (WIA mock-up)**

An interactive "what if" analysis mock-up will be created for demonstrating the functional principle of the new capability of "what if" analysis. It will allow

- Simplified visualisation of the evolution of a predefined crisis scenario.
- Choosing from a menu of possible decisions at a certain point of time or for a certain event in the scenario.
- Displaying the pre-computed consequences at the end of the crisis simulation.
- "Rollback" and choosing a different course of action.
- Displaying the pre-computed consequences of both courses of action.
- Displaying an assessment of which course of action had less severe consequences.

5.3.2 Description

The new capability of "what if" analysis will consist of a complex backend system setup including a distributed federated simulation, database components, and additional modules like Consequence Analysis. A full deployment of the new capability as stand-alone web application seems currently not advisable, since the usage of the capability requires end-user training and modelling support. Therefore, the VCCC portal shall provide an interactive "what if" analysis mock-up for demonstrating the functional principle of CIPRNet's "what if" analysis capability. The interface of the mock-up needs to be simple and intuitive, so that no special training for its use is required.

The expected users of this service include the management level of public authorities and CI stakeholders. The effects of using this service can be two-fold:

- Dissemination of knowledge and added-value of CIPRNet's WIA capability,
- Attracting end-users to CIPRNet's training events on the real WIA system.

5.3.3 Input information

The input information for the service would comprise:

- Pre-computed scenario evolution (could even be a recorded movie),
- A pre-selected list of courses of action (no less than two and no more than five),
- A pre-computed set of consequences for the chosen courses of action,
- The user's selection (Start, stop, select course of action, rollback).

5.3.4 Output information

The output information during the service operation will be:

- A short textual description of the scenario situation,
- Start/stop/rollback buttons,
- A situational display of the scenario evolution,
- A menu displaying the possible courses of action at a predefined point of time,
- A display of pre-computed consequences for each chosen course of action at the end of the crisis simulation mock-up,
- A display of the comparative assessment of the choices made.

6 Conclusion

In this deliverable, the services for CIPRNet DSS and VCCC are specified. The goal was to initially specify and describe the following services:

- Data Accessing and Gathering (DSS-DAG)
- Threat Forecasting (DSS-TF)
- Threat Visualization (DSS-TV)
- Ask the expert service
- CIPedia service

While specifying the services, we addressed the role of the service, input and output information used by services, as well as we presented deployment and use cases diagrams.

Moreover, the services that may be relevant to the future EISAC were also included (in Annex A). Those are: Crowd management/mapping, Resources and capability management, and Bidirectional communication with society.

The services will be later delivered within the course of the CIPRNet project either as a part of CIPRNet DSS or VCCC portal [D5.3][D6.4][D7.4][D4.5][D4.6].

Additionally, Annex B contains the publication “End-users needs and requirements for tools to support critical infrastructures protection“, which summarizes this deliverable.

7 References

[DoW] Annex I – Description of Work (Annex to the Grant Agreement of CIPRNet).

[D2.51] Fraunhofer and Ethics Board: CIPRNet deliverable D2.51: "Initial ethics report", 2013

[D4.5] CIPRNet deliverable D4.5: "Implementation of services of the 'what if' analysis demonstrator for the VCCC web portal", to appear

[D4.6] CIPRNet deliverable D4.6: "Implementation of the DSS services for the CIPRNet web portal", to appear

[D5.1] UTP: CIPRNet deliverable D5.1: "Formal requirements specification", 2013

[D5.3] UTP: CIPRNet deliverable D5.3: "Formal requirements specification", to appear

[D6.1] Fraunhofer: CIPRNet deliverable D6.1: "Conceptual design of a federated and distributed cross-sector and threat simulator", 2014

[D6.4] CIPRNet deliverable D6.4: "Implementation of the integrated CIP MS&A based 'what if' analysis", to appear

[D7.1] ENEA: CIPRNet deliverable D7.1: "Design of the DSS with consequence analysis", 2014

[D7.4] CIPRNet deliverable D7.4: "Implementation of the DSS with consequence analysis", to appear

[D7.5+D7.6] ENEA: CIPRNet deliverable D7.5+D7.6: "Integration of meteo and climatological simulators, flood forecasts, earthquakes data and analysis and Interface to the technical demonstrator for 'what if' analysis", to appear

[D8.4] JRC: CIPRNet deliverable D8.4: "Publicly Announced CIPedia", 2014

[ECdir] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML Website with amendments and consolidated reference text: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

[Nieuwenhuijs] Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver M.H.A., "Modeling Critical Infrastructure Dependencies", in: IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, (Boston: Springer), October 2008, pp. 205-214, ISBN 978-0-387-88522-3.

[CIPedia] Fraunhofer, JRC: CIPedia: http://www.cipedia.eu

[ISP] Italian Institute for Environmental Protection and Research. SINANET is the ISPRA environmental and territorial data repository: http://www.sinanet.isprambiente.it/it

[EEA] European Environment Agency: http://www.eea.europa.eu/publications/COR0-landcover

[INGV] Italian National Institute of Geophysics and Volcanology: http://www.ingv.it/eng

[End] Choras Michal, Kozik R., Renk R., Holubowicz W., End-users needs and requirements for tools to support critical infrastructures protection, EDDC 2014, BIG4CIP 2014, arXiv:1404.7564.

[B4C] http://www.big4cip.org

Annex A: Other services relevant to EISAC

The services specified in this section will not be developed within the CIPRNet project. However, due to their importance in relation to the future deployment of EISAC, these services should be foreseen as vital elements in the roadmap of EISAC.

A1. Crowd management / Crowd mapping

Crowd mapping is the concept that aims at large-scale sharing of user-related information (e.g. geo position). Typically, crowd-mapping platforms have capabilities for gathering information from a wide range of sources like mobile devices, web pages or news. Such platforms also support different aspects of information visualisation. Crowd mapping can also refer to management of crisis situations during the evacuation.

An example of a successful application of such a platform is a smart phone application used during the Olympic Games in 2012. The apps installed by users (e.g. visitors to London) were integrated with crowd monitoring technology that allowed for real-time people tracking. Besides the tracking capabilities, the application also allowed for information sharing between London Police and visitors. For example, it was possible to send to a group of users the evacuation routes or information explaining how to prepare in case of emergency.

Functionalities

- Real-time human tracking (if the user agrees to that).
- Crowd management: evacuation routes.
- Communication with citizens: information about natural hazards, information explaining how to behave in case of emergency.

Benefits of reusing crowd-mapping technology by EISAC

Deploying crowd mapping platforms in EISAC nodes can have beneficial impact for EISAC, EISAC end-users and citizens, namely:

- With real-time human tracking, EISAC can estimate the impact of a natural hazard more precisely.
- EISAC can use “human sensors” as an additional source of information in order to increase the overall situational awareness.
- EISAC can use such a platform to identify where people are located in order to incorporate such information into simulations and to have a bigger picture of a crisis situation during the process of decision making.
- End-users (e.g. Crisis Response Centres) can benefit from real-time information sharing with citizens.
- Crisis Response Centres can use the information from crowd mapping systems for better resource planning (e.g. where to send food supplies, emergency response teams, etc.).

A2. Resources and capability management

Crisis management entities during a CI-related disaster need to quickly assess what capabilities are at their disposal and what other capabilities might be necessary to deal with a specific situation. They must be able to make this assessment quickly, to decide upon the right actions, not only to prevent the spreading of the crisis situation but also to minimise the impact in terms of casualties, injuries, shock, fear and further damages. It should be emphasised that for

the purposes of the service description, capability should be understood as a combination of specific means necessary to perform a given action. For example, capability can be "restore the damaged part of gas pipeline", while the capable resources are human personnel, materials, specialised equipment and expert knowledge.

Therefore, the future CIPRNet capability management service should be designed in a way that will allow for automatic matching of relevant crisis circumstances to the capabilities and resources that crisis management entities have at their disposal. It will increase the chance for prevention of a negative impact of a crisis situation and for a timely intervention during crisis.

Service functionalities

- Identifying which means (resources) or sensors are best suited to react in a current crisis situation,
- Prioritising the identified means taking into account:
    - Specific circumstances related to the given crisis (e.g. limitations, type of disaster, affected CI, etc.),
    - Predefined importance of the capability properties (e.g. availability, reliability, time-to-deploy, effectiveness),
- Visualisation of the geographical dependencies between the available capabilities and crisis location, where they would be deployed (e.g. visualisation of the flood location and the location of specific resources that can be used for restoring the damaged flood bank).

Benefits for EISAC

- The capability management service will increase the situational awareness of the decision makers by providing the information on capabilities and resources that are actually available.
- While using this service, it will be possible to increase the effectiveness (in terms of accuracy, time and costs) of decisions made during a CI-related crisis by complementing the decision maker view on a current crisis.

A3. Bidirectional communication with society

The purpose of the EISAC service described in this section is to provide bidirectional communication between the entities involved in a CI-related crisis management and affected or unaffected part of the society.

The rationale for above functions of such a communication service is the fact that natural emergencies regularly may affect multiple CI (common mode failure). As explained by [Nieuwenhuijs], the shift in mode of operations causes other CI dependencies while these may be disrupted due to the common mode failure. Moreover, this may amplify the risk of cascading disruption of CI. Therefore, in case of power outage, the unavailability of traditional communication channels (e.g. fixed telephony, 112 emergency number, etc.) can be expected. In such a case, citizens should have the possibility to communicate with responsible authorities using other ways than only the traditional crisis communication channels.

Service functionalities

Considering the basic functionalities related to the communication between CI decision makers and citizens, the service should allow for (at least):

- Posting the information through social media in both directions (i.e. from and to citizens),
- Online messaging using other Internet-based channels (e.g. e-mails, application-based messages),
- Information exchange via mobile devices (including SMS, automated alerting based on geo-localisation of mobile devices, mobile applications/messengers, geo-tagging capabilities, etc.),
- Confidence check.

Integration with EISAC

The bidirectional communication service can be realised in the form of the online platform for data/information exchange, which integrates the various information sources and online services such as social media, crowd sourcing tools and messaging services. What is important, such platform would offer also capabilities for more effective cross-agency communication and data / information exchange. Such capability is particularly important during cross-border crises in which international communication is needed to coordinate crisis response and to minimise international impact of a crisis.

Benefits for EISAC

- Since the concept of this service assumes the communication in both directions, the crisis management entities could get more information from the site of the crisis. In this sense, the society using this service could serve as an additional "sensors", providing near real-time information and data.
- Similarly to the resources and capability management service, bidirectional communication during a CI-related crisis could provide a complementary view on the actual situation for decision makers, supporting the standard CIPRNet services and tools such as modelling, simulation and decision support.
- Enhanced situational awareness of crisis management authorities and decision makers by providing the shared societal view on the current crisis situation and it impact.
- Improved decision-making capabilities by providing the broader operational picture of a crisis situation.

Annex B: Paper titled: End-users needs and requirements for tools to support critical infrastructures protection

End-users needs and requirements for tools to support critical infrastructures protection

Michał Choraś and Rafał Kozik
Institute of Telecommunications
UTP Bydgoszcz
chorasm@utp.edu.pl

Rafał Renk and Witold Hołubowicz
Institute of Telecommunications. UTP Bydgoszcz
and
University of Adam Mickiewicz (UAM), Poznań

***Abstract*— The role of the services described in this paper is to support decisions in the Critical Infrastructure Protection (CIP) domain. Those services are perceived as the most fundamental functionalities, that will serve as a basis for the planned European simulation centre for modelling the behaviour of Critical Infrastructures (CI). The proposed services are: CI-related data accessing and gathering, threat forecasting and visualisation, consequence analysis, crowd management, as well as resources and capability management. In general, services proposed in the current paper will contribute to reducing the problem of overwhelming decision makers by too large amount of information. In the crisis, their decisions are made on the basis of the large amount of data related to the current situation, such as the status of CI, localisation of capabilities, weather and threat forecasts etc. The design of the services has been established with the help of the future end-users. The work presented in this paper is the result of preliminary activities performed in the FP7 project CIPRNet.**

***Keywords*— CIP, CIPRNet project, decision support, services**

I. INTRODUCTION

According to [1] Critical Infrastructure (CI) can be described as asset, system or part thereof, which is essential for the maintenance of societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a given country or region.

The importance of CI-related aspects stresses the fact that many research activities have been recently conducted in order to address different problems, including CI behaviour simulations [2], natural threat prediction and its impact evaluation [3], CI resilience [7], and cyber security of CI [8].

Protection of CI is a specific type of task. On the one hand, decisions taken for CIP purposes may impact human lives and material goods, threatened by both natural phenomena and as the consequence of human errors. On the other hand, such decisions must be taken in real-time – particularly during CI-related crisis. Most often, such decisions are taken by analysing a large amount of heterogeneous data.

In this paper, the services for CIP community and decision makers are presented to support decision making process in CIP, both in the preparedness ("cold") phase, as well as in the crisis ("hot") phase.

The goal of such services development is to increase the situational awareness of decision makers by extraction of the most necessary information from the large amount of heterogeneous data coming from different sources (such as real-time sensorial data).

Specification and development of the services proposed in this paper are the objectives of the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project – ongoing security research, co-funded by the European Commission's 7th Research Framework Program (FP7) [2].

In the first phase of the project, the end-users community was asked to express and share their needs and expectations related to increase of the effectiveness of modelling, simulation and CIP-related analysis environment and decision making process.

In this paper, the analysis of their requirements is provided, as well as the description of the demanded services which will later be designed in the CIPRNet project.

The rest of this paper is structured as follows:

- Section II includes the methodology and means used to collect end-user viewpoints in the CIPRNet project, the analysis of the end-user perspective drawn from this research and the summary of the key findings.
- In section III, the services to support CIP decision makers are presented. The proposed services include: data accessing and gathering, threat forecasting, threat visualisation, what-if and consequence analysis. Additionally, the services such as crowd management and resources and capability management are presented.
- In section IV, the general conclusions are presented.

II. END-USER NEEDS AND EXPECTATIONS

A. CIP end-user views collection

The identified stakeholders relevant to the project are representatives of the public, private, research and academia

domains. The methods for gathering user views in the CIPRNet project were face-to-face meetings, remote user interviews and the CIPRNet questionnaire, filled in by the project end-users and domain experts. Outcomes of the collected questionnaires were a starting point in requirements specification process and in the specification of solutions described in this paper.

The questionnaire was designed in order to provide a broad view on current end-user problems, limitations and expectations, including big data issues. The most of the questions are open or semi-open. Therefore, respondents were neither limited in the expression of their opinions, nor biased by pre-defined options to choose.

Generally, the questionnaire has been divided into four blocks of questions, namely:

- General information about the respondents, particularly their organisations, range of activities, area in which he/she acts,
- Questions related to accessing the information, particularly concerning the availability of information about CI coming from private and public sectors and used during CI-related crisis,
- Questions about using decision support systems during respondent duties, providing information about decision support mechanisms and tools, their limitations, data exchange, standards, etc.,
- Questions about simulation and modelling for CI crisis management purposes.

The analysis of the CIPRNet questionnaires filled in by the CIPRNet end-users can be found in the next section.

B. *Questionnaire analysis*

Respondents who filled in the questionnaire are representatives of various organisations – from local and regional CI-related organisations to pan-European agencies, and from academic and applied researchers to CI operators. However, the majority of respondents are representatives of organisations that operate within nationwide range, and usually are from public emergency/crisis management centres.

The respondents assessed the availability of various information related to CI from various sectors and sources and gave them ratings. According to respondents ratings, generally there are no significant differences between the levels of availability of information, when comparing public and private sectors. The average ratings for public vs. private CI information availability (e.g. geo-localisation data, operational data and sensitive data about these infrastructures) are at the similar level. Considering the information about CI dependences, it is noticeable that such information during normal operation is significantly more easily accessible than during non-normal state of the CI functioning [3].

The questionnaire analysis shows that the hardest categories of information to be accessed include:

- Operational data of private sector CI,
- Information about CI across the national/regional borders,
- Information about CI across public-private sector borders,
- Information about CI dependencies during non-normal state.

In addition, respondents indicated that reliable data of CI financial aspects and CI failure status are also not easy to obtain from CI management entities.

According to end-users,

- climatic and weather information for specific (emergency) area, and
- geo-location information about public / private sector CI,

are described as the relatively easiest to obtain.

Concluding, most of the categories of information considered in the questionnaire (excluding e.g. the mentioned climatic/weather data) were assessed as relatively hard to obtain. This observation indicates a serious problem related to information accessibility, and what is worth noticing, challenges related to acquisition of necessary information exist regardless of the CI functioning sector (i.e. private versus public).

About 40% of respondents reported that they do not use any ICT-based support for their decisions. The majority of remaining 60% of respondents stated that they (or their organisations) use internally developed tools for specific purposes of their organisation, or alternatively, that they use various loosely coupled data sources (such as GIS resources, the weather data, etc.) to support decisions. Considering specific decision support tools (DSS) used by interviewees, examples such as C3M, IPCR or WebEOC have been listed. These systems are exploited for the crisis response planning, reporting, procedure and policy creating, resource allocation and tracking.

When asked about the analytical capabilities, as well as about usefulness and effectiveness of these systems during crisis-related decision-making, respondents presented different views. About half of them admitted that the used (decision support) systems do not meet their needs and that these systems are not tailored to the specific needs of their operation. As respondents emphasised, the main weakness of these systems is the need for advanced customisation (costly in terms of time, efforts, financing, etc.).

Other drawbacks include:

- lack of interconnectivity with the other systems (e.g. used by entities cooperating with stakeholder's organisation during CI-related crisis),

- lack of possibility to integrate the data from other entities/systems, hampering the cooperation between various organisations,
- limited capabilities of spatial visualisation of threats, and
- lack of capabilities to support comparison of the current situation to earlier forecasts.

Cross-border decision-making is another open gap of the used systems, impacting end-user operation.

The interviewees also listed various kinds of the information sources that are used for building the situational awareness in the emergency response efforts. These include mainly external sources such as cooperating entities and agencies involved in emergency response, which provide hydrological data, weather forecasts and the information about CI (including geo-location). Other sources of information are direct reports from the field/emergency area. Usually, such information is not publicly available. However, end-users can access that information in real-time or near real-time.

Respondents stated that the primary need for simulation models relates to consequences of CI object failure, employing e.g. cascade models of infrastructure failures. End-users indicated different scales of such consequences, varying from impact on another single system, up to consequences for national security, societal impact, national economy, etc.

Moreover, respondents noticed the lack of models supporting the estimation of CI restoration time, the identification of critical nodes (supporting CI objects prioritisation) and the simulation models relevant to a given, specific sector (e.g. applicable for health care services during CI failure).

Asked for the opinion on what should be improved in relation to decision-support for emergency management, respondents identified four main areas of interest:

1) Simulation and modelling, in particular the development of threat modelling and forecasting tools, e.g. for simulation of the consequences of possible decisions.

2) Estimation of crisis impact, both at a low level (e.g. impact of CI object failure on e.g. the hospital functioning), as well as at a higher level – for example estimation of CI failure costs, national economy losses, etc.

3) Emergency communication, namely:

- information/data sharing,
- timeliness of received information,
- exchange of information among cooperating agencies and organisations in real-time,
- compatibility of data formats,
- mechanisms to support informing about hazards, etc.

4) Cooperation and training between solution providers and emergency management teams.

According to the respondents, closer public-private cooperation also could improve the current situation in decision-making.

The respondents also indicated problems related to the current assessment of CI dependencies. The most significant examples include:

- Limited capabilities of simulations, particularly in terms of simulating interrelations between various CI and analysing the threats based on such relationships.
- Organisations and CI operators isolation. In other words, organisations often do not effectively take into account consequences of their infrastructure failures, exceeding beyond their organisations and impacting other sectors, companies, etc.
- Lack of systematic planning of CI protection and restoration after a crisis, as well as lack of procedures supporting such protection.
- Problems with identification of contact points that in the case of crisis should be immediately available for responsible entities.
- International standardisation in the CIP area.
- Information accessibility.
- Data validation and reliability.

C. Key findings

The end-users needs, expectations and requirements (presented in the previous subsection) can be categorised into the following aspects related to:

- decision support process,
- simulation and modelling,
- access to the real-time data and critical information.

The key findings that have been identified after the analysis of the mentioned aspects are as follows:

1) End-users expect more advanced, customised and tailored (to their needs) decision support solutions, which will allow for flexible spatial threats visualisation, easy integration with new data sources or other systems, and information sharing between different entities engaged into a crisis management process.

2) End-users lack accurate models and simulation tools that will allow for consequences, impact and risk analysis of CI failures and cascading effects. The forecasting capabilities are emphasised as one of the most desired.

3) End-users articulated the need of access to information related to CI from various sectors. They emphasised difficulties in gaining data related to operational state of private sectors CI and CI-related information across public-public and national-regional borders.

III. CIPRNET SERVICES

In order to cover the key findings (described in the previous section) coming from the end-user perspective analysis, the following decision support services have been specified:

- Consequence analysis,
- Threat forecasting,
- Threat visualisation,
- Data accessing and gathering,
- Crowd management / Crowd mapping,
- Resources and capability management.

It is expected that the functionalities and the number of services provided by the DSS will evolve over time. Therefore, a plug-and-play and easy to extend architecture of the DSS is anticipated (see Fig. 1).

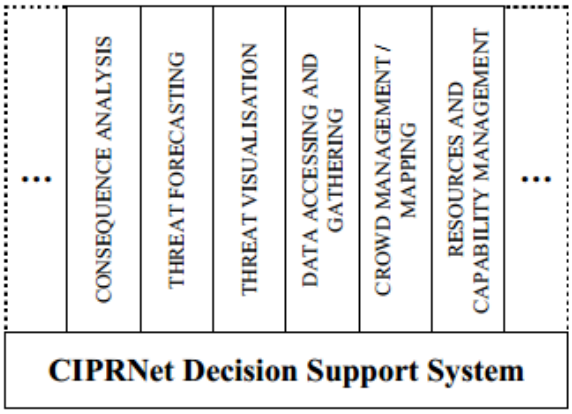

Fig. 1. Extendable DSS architecture

The proposed DSS will have two distinctive operational modes, namely "Hot Phase" and "Cold Phase" decision support (Fig. 2).

The "Cold Phase" is computationally intensive, therefore, it is dedicated to postmortem analysis and CI operators training purposes. Among others it will heavily rely on historical data, modelling, simulation and analysis (MS&A).

The "Hot Phase" includes continuous and real-time risk assessment, threat forecasting and consequence analysis conducted using real-time data during the real crisis. These aspects are explained in the next sections.

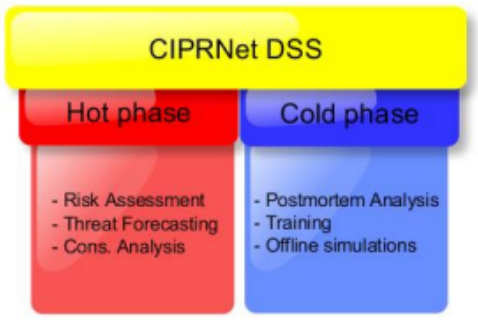

Fig. 2. Operational modes of the CIPRNet DSS

A. *Data accessing and gathering*

The data accessing and gathering service allows for collecting and storing the data relevant to decisions taken for CIP purposes. The data is stored in dedicated database. The purpose of this service is to provide all input data, necessary to support the decisions by the CIPRNet DSS. Particularly, the service provides the data used by the threat forecasting service.

The data stored in the database is structured, based on pre-defined layered model, including territorial, socio-economical, infrastructure, and historical data. Additionally, each layer can be divided into further sub-layers.

The sources of data can be e.g. governmental repositories, infrastructure operators and results of modelling and simulation activities.

B. *Threat forecasting*

The threat forecasting service is one of the key features of the DSS. This service provides the DSS with capability to forecast natural phenomena that can cause physical damages of CI and that can impact the normal operation of CI. Such phenomena include e.g. heavy rain, flooding, landslide, drought, heat wave, etc.

The threat forecasting service is designed in modular way. Each module being an element of the service is dedicated to forecasting a specific phenomenon. Particular modules are interconnected with the corresponding layers of "data accessing and gathering" service. Each module uses data coming from the specific layer to run the appropriate model and to forecast specific threats on a specific area.

C. *Threat visualisation*

This service is intended to provide DSS user the various visualisation capabilities. The role of this service is to use different means to visualise a variety of aspects, that may influence decision making process for CIP purposes. Therefore, visualisation service is oriented on the usability of the DSS, minimising the amount of data delivered to the decision makers and changing the form of these data from e.g.

tabular, raw data into more understandable and user friendly graphic presentation. Examples of the visualisation capabilities may include presentation of predicted CI affecting threats in aerial or GIS maps, as well as visualisation of damage level, that can be caused by a natural phenomenon. Threat visualisation service is strongly interconnected with other DSS services proposed in this paper, since the visualised data are provided e.g. by "data accessing and gathering" service and processed by the threat forecasting service. The main requirements that this service must satisfy include efficient and flexible access to the threat visualisation data, the ability to handle multiple simultaneous requests for visualisation and the ability to share provided visualisations among private and public stakeholders, emergency managers and common citizens involved in disaster response.

D. Consequence analysis

The consequence analysis is the service included in the CIPRNet DSS, that offers the added value to the decision making process. This service enables decision-makers and operators to analyse the impact of natural hazards on CI failures and to examine their possible short and long term consequences. The consequence analysis will rely on both real-time (sensorial, e.g. geo-seismic) data, as well as statistical and historical data about the past, similar incidents. Real-time status information about the functioning of a particular CI element and meteorological data are also involved in the consequence analysis.

E. What-if analysis

The "What-if analysis" is one of the CIPRNet services with the main goal to provide the end-user with the simulation capabilities, which allow CI-related aspects to be investigated. Among others, the "What-if analysis" will provide the end-user with tools, which will allow them to analyse different crisis scenarios that may affect critical infrastructures. The analysis will allow the end-user to investigate different courses of actions and to evaluate their consequences. The core functionalities of this service will be enabled with tools and frameworks for federated simulation [4]. The underpinnings for this have been established by DIESIS [5][6] project, of which CIPRNet is the successor.

F. Crowd management / Crowd mapping

The crowd mapping service aims at large scale sharing of user (citizen)-related information based on their geo-positioning data. Input data for the crowd mapping service is data coming from a variety of sources like mobile device or web pages, logging the physical localisation of a user. The main added value for the decision making process regarding crowd management for CIP purposes is support for evacuation management during a crisis situation. The main functionalities of this service include real-time human tracking during a given crisis situation and in a specific area, evacuation route analysis and communication with citizens established based on citizen geo-position.

G. Resources and capability management

The capability management service is designed in a way that allows the DSS operator to automatically match the capabilities and resources that crisis management entities have at their disposal to the relevant crisis circumstances. It will increase the chance for prevention of negative impact of crisis situation and for timely intervention during crisis.

The main service functionalities are:

- Identification of means (resources) and sensors that are best suited to react in the current crisis situation,
- Prioritisation of the identified means, taking into account specific limitations, type of CI failure and the properties of the identified capabilities (e.g. availability, reliability, time-to-deploy, effectiveness in a given situation, restoration time, etc.),
- Visualisation of the geographical dependencies between the available capabilities and the area affected by the crisis.

IV. CONCLUSIONS

In this paper we described the set of services composing the decision support system for Critical Infrastructure Protection (CIP).

These services are perceived as the most fundamental and were articulated by the end-users. Those functionalities will serve as the basis for the planned European simulation centre for modelling the behaviour of Critical Infrastructures.

The proposed services add value to current CIP efforts and are designed in a way that will improve effectiveness of CIP decision making. The proposed services are: data accessing and gathering, threat forecasting and visualisation, consequence analysis, crowd management, as well as resources and capability management.

Particularly, the threat visualisation, crowd mapping and resources (capability) management services will allow DSS users to deal with constantly changing information during CI crisis and to more effectively build a reliable view on a crisis situation. This will be achieved through a more clear and better tailored to user needs form of information presentation, including geographical representation of crowd sources, visualisation of CI elements, CI affecting threats and means for mitigating them in GIS-based and satellite maps.

In addition, the consequence analysis service will allow users to examine various crisis scenarios and to learn about the results of various possible decisions. The data accessing and gathering service is designed to provide only the most relevant and necessary data to particular DSS services, launched for specific purposes. Therefore, this service will also reduce the problem of overwhelming decision makers by too large amount of information.

Concluding, the services described in this paper are proposed to support decisions for CIP purposes. Such decisions are always influenced by the large amount of

information about the current situation, therefore the proposed services are the CIPRNet response to the big data problem, that CI decision makers must face.

ACKNOWLEDGMENT

This work is partly funded by the European Commission under grant number FP7-312450-CIPRNet. The support is gratefully acknowledged.

REFERENCES

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[2] CIPRNet project website, available: http://ciprnet.eu/summary.html

[3] Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver M.H.A., "Modeling Critical Infrastructure Dependencies", in: IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, (Boston: Springer), October 2008, pp. 205-214

[4] Erich Rome, Sandro Bologna, Erol Gelenbe, Eric Luiijf, Vincenzo Masucci (2009): DIESIS - Design of an Interoperable European Federated Simulation Network for Critical Infrastructures. In: Proceedings of the 2009 SISO European Simulation Interoperability Workshop (ESIW '09), Simulation Councils, Inc., San Diego, CA, USA, ISBN 1-56555-336-5, pp. 139-146. Conference: Istanbul, Turkey, July 13-16, 2009.

[5] Usov, Andrij; Beyel, Césaire; Rome, Erich; Beyer, Uwe; Castorini, Elisa; Palazzari, Paolo; Tofani, Alberto: The DIESIS approach to semantically interoperable federated critical infrastructure simulation. Williams, Edward (Ed.) et al.: SIMUL 2010 : the second International Conference on Advances in System Simulation, 22-27 August 2010, Nice, France. Los Alamitos, Calif. [u.a.]: IEEE Computer Society, 2010, pp. 121-128

[6] Vincenzo Masucci, Francesco Adinolfi, Giovanni Dipoppa, Paolo Servillo and Alberto Tofani (2009): Ontology-Based Modeling and Simulation of Critical Infrastructures. To appear in: Proceedings of the 2009 Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (IFIP CIP 2009). Conference: Hanover, New Hampshire (US) March 22-25, 2009.

[7] A. Amantini, M. Choras, S. D'Antonio, E. Egozcue, D. Germanus R.Hutter, The human role in tools for improving robustness and resilience of critical infrastructures, Cognition, Technology & Work Journal, Vol. 14, No 2, pp. 143-155, 2012

[8] R. Klein, The EU FP6 Integrated Project IRRIIS on Dependent Critical Infrastructures, Critical Information Infrastructures Security, Lecture Notes in Computer Science Volume 6712, 2011, pp 26-42