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

D7.1 Design of the DSS with consequence analysis

Due date of deliverable: 28/02/2014
Actual submission date v1: 04/07/2014
Actual submission date v2: 16/01/2015

Revision: Version 2

Italian National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA)

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)	

Authors	Antonio Di Pietro (ENEA) Luigi La Porta (ENEA) Maurizio Pollino (ENEA) Vittorio Rosato (ENEA) Alberto Tofani (ENEA)

Security Assessment	Hanneke Duijnhoven (TNO)
Approval Date	02/07/2014
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.

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

TABLE OF CONTENTS

1 Introduction

1.1 Purpose of the document

The objective of this document is to present the design principles of one of the outcomes of the CIPRNet project, the Decision Support System (DSS). The CIPRNet DSS will accomplish the tasks of providing a new technological tool enabling to increase the resilience of CI by predicting impact scenarios produced by natural hazards and by estimating the impact of CI components failures on the infrastructure's services (in terms of service loss or reduction) and the consequences that these services perturbations might have on population and environment.

Those capabilities can improve the management options for mitigating the risks for emergency managers. In particular, when the DSS estimates that the consequences are severe for specific assets (e.g., for the citizens), the What-if analysis capability of the DSS can estimate the relative consequences relative to specific contingency plans provided by the CI operators in order to find the actions that can reduce the risks on the specific assets. In fact, considering that, the mitigation procedures that each CI operator takes cannot be proposed by the DSS (the DSS does not have access to physical data managed by a generic CI and to contingency plans), the DSS can be a valid means to evaluate the *effect* that specific procedures, proposed by CI operators, can have on specific assets. In addition, considering that the DSS can provide an outcome in advance w.r.t. the time where a physical damage (and its effect) is expected to occur, this allows to refine the consequences estimation over time with increasing up-to-date forecasts.

The proposed DSS will be also one of the key capabilities of the long standing objective of the CIPRNet NoE consortium, that is, the establishment of the EISAC initiative (European Infrastructures Simulation and Analysis Centre). In Annex 1, we will briefly sketch the type of functionalities that an Italian EISAC Centre (I-EISAC) could display and an example of its institutional allocation in the Italian governance of CIP. These themes will then be the object and the starting point for a further deepening of this topic, expected to be treated in D4.7 (see [1]). The aim of the present document is thus the presentation of the design of the DSS that will constitute a central asset empowering the EISACs constellation.

1.2 Document structure

The present document is organised as follows:

- **Chapter 2** describes the main ideas, concepts, terminology and the theoretical framework underlying the CIPRNet DSS;
- **Chapter 3** describes a refinement of the functional and non-functional requirements of the DSS identified in [3];
- **Chapter 4** describes the architectural concepts of the DSS, its realization and two scenarios to provide some hints about its possible implementation;
- **Chapter 5** draws some conclusions and discusses the links of the presented document with other deliverables;
- **ANNEX I** presents a possible organisation and management organisation of the Italian node (I-EISAC) of the pan-European networked organisation named EISAC (to be used as entry point for the D4.7 activities);
- **ANNEX II** contains a description of the Secure Information Exchange platform named NEISAS (National and European Information Sharing and Alerting System), the result of an ENEA collaboration within a EU DG-HOME project;

- **ANNEX III** describes the open source platform GeoPlatform used to implement rich Web GIS applications based on geospatial web-based software. The GeoPlatform is the geospatial web-based software that will be used to implement some components of the final GUI of the DSS platform.

This version 2 of D7.1 includes amendments requested by CIPRNet's reviewers at the first project review. A further refinement of this document [31] will be delivered at approximately M18.

2 Rationale of the DSS

As stated in the DoW document, the new capabilities that will be developed within the CIPRNet project and in particular the Decision Support System with consequence analysis for CI preparedness and resilience have been in part inspired by the 'Protecting Critical Infrastructure in the EU' [1] document, a report of the **Centre for European Policy Studies** (CEPS). In particular, this Report recommends:

- ✓ "The key pillars of a European CIP policy are then the development of standards and best practices, education and training, R&D and information-sharing, and modelling and EU wide simulation capabilities. [CEPS, p. 89]"
- ✓ "In the ex-ante phase of CIP policy, infrastructure risk assessment plays a key role, and should be subject to further research and standardisation. [CEPS p. 48]"
- ✓ "The EU must empower a single agency to deal with CIP and CIIP [Critical Information based Infrastructures Protection] issues adopting an all-hazards approach. [CEPS, p. 89]"

The critical issues and the relative recommendations show the need for today's emergency planners to have available a platform that integrates the prediction of natural disasters and the consequent estimation of impacts on CI, and prediction of the consequences on the environment and the society. The latter issues are relevant for a correct evaluation of risks and the setting of appropriate preventative measures, mitigation and healing strategies.

The DSS design is based on the idea that necessary prerequisites for addressing efficient crisis management options are:

- to have a reliable platform for the prediction of events,
- to be able to correlates events and physical harms produced on the infrastructures,
- to have models/frameworks for the computation of the impact of the damages in terms of reduction of functionalities for the whole "system of technological systems",
- to have models/frameworks for the estimation of the consequences that all phenomena might have on population, environment, the industrial sectors and the services allowing citizen's lives.

Following this idea, we identified the following core functionalities/products that should be included in the designed architecture:

1. **Threat Forecasting**: responsible for the monitoring of natural phenomena, the prediction of natural disasters, the detection of events, the prediction of physical damage scenarios and the estimation of impact on the CI;
2. **Threat visualization**: consisting of high-usable graphical interfaces for end-users allowing the visualization of the GIS data regarding the forecast of natural phenomena, the estimated impact report on CI, and the estimated consequences report on the society, the environment and the industrial sector;
3. **Consequence Analysis**: responsible for the estimation of the consequences and for the support of efficient strategies to cope with crisis scenarios.

2.1 Connections of the DSS with other CIPRNet products

In this section, we attempt to identify the connections of the DSS (and its components) with other CIPRNet products showing also the interaction of users with the different products.

In Figure 1, we show the overall technological platform that will emerge from the CIPRNet activities. In this scheme, the functionalities of CIPRNet products are reported, together with the explicit mention of the services and products that will be produced and the indication of their relative workflow.

The services that the CIPRNET framework will realize will allow different end users to use a variety of products/services. In the following, the main services of the CIPRNET framework are presented:

- **Communication service**: this is an ancillary functionality that CIPRNet will provide to its end-users that, aside to standard communication means (email, voice call etc.) will also have the availability of a Secure Information Sharing Platform which will enable users to talk to each other (by creating pool of trusted users), to talk with CIP experts, to interact with CIPRNet staff;
- **Risk Assessment service**: it consists of the DSS including the functions for threat forecasting and visualization, the What-if analysis [4] system and the Consequence Analysis system (see 4.2.4.4);
- **Data service**: it allows end-users to access the GIS Information Database and the Database of the major CI outages occurred in Italy starting from January 2014 (for both databases see [5]);
- **Other services**: it consists of a portal named Virtual Centre of Competence and expertise in CIP (VCCC) that allow CIP experts to actively disseminate knowledge and experience, organise workshops, take part in conferences, moderate discussions, and finally, organise and provide a set of lectures to relevant communities. These services are provided by the Ask the Expert [6] and the CIPedia service [7];

Considering the Risk Assessment service layer, the interactions among the DSS and the What-if analysis system may be clearly identified. In particular, two scenarios may be produced:

- a coarse grain **predicted scenario** (see 4.2.4.2) that is automatically produced by the DSS through the use of simulation models and forecast;
- a fine grain **synthetic scenario** produced by the What-if analysis module.

The fine grain synthetic scenario can represent a refinement of a coarse grain predicted scenario in order to perform what-if analysis on a synthetic but realistic scenario.

Both scenarios are then provided to the **Impact analysis** modules to estimate the impact of failures (estimated or real) on CIs on the degradation of the services provided by the CIs. For a predicted scenario, the impact module will be based on an Interdependency simulator (e.g. I2Sim, see [8] and 4.2.4.4) whereas for the synthetic scenario it will be based on Federated Simulation [9]. The two impacts scenarios resulting from the two Impact analysis modules will then be sent to the **Consequence analysis** module (see 4.2.4.4) which will estimate the consequences of the failure on CIs on the society, the environment and the industrial sectors.

What-if module could also be used, whenever data are available, for the testing of actions to be taken by operators or by emergency managers, to validate their strategies.

The Communication layer will consist of a Secure Information Sharing Platform that will allow CI operators to insert their prediction about the possible evolution of their system due to the predicted and synthetic harm scenario that is sent to them through the same platform.

The DSS and What-if Analysis system will rely on a persistence layer provided by the GIS Information Database, which will store public available data (i.e. data that can be accessed by CIPRNet end-users through web applications, web services etc.) and private data (i.e. CI components vulnerability data, CI operators shared information data, CI network topologies data, CIPRNet analysis data, historical events and scenario data).

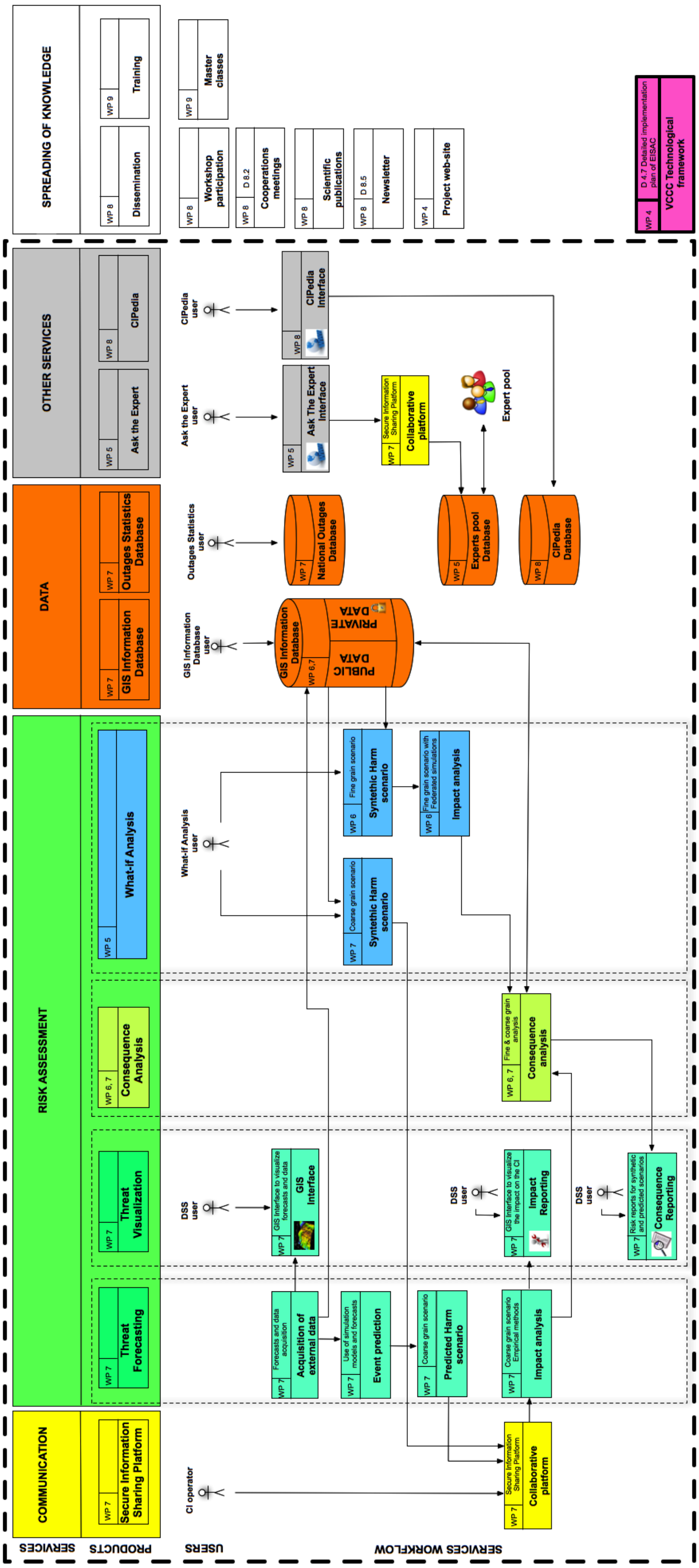

Figure 1: Connections of the DSS with other CIPRNet WPs.

2.2 Remarks on terminology

This section introduces the terminology and definitions used throughout the CIPRNet project. Due to its multi-disciplinary nature, the CIPRNet project uses terms from various scientific and technical domains and extends a glossary of terms and definitions started in earlier related projects [10]. The document covers topics in the domains of critical infrastructures (CI) and their protection (CIP), security, safety, some fields within computer science, some CI sectors and more. However, recent developments and the specific nature of CIPRNet require both an extension and an update of the terms and definitions. In particular, existing standards on vocabulary should be taken into account and used.

Terms	***General definition***	***CIPRNet DSS definition meaning***
Hazard	a dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage [UN-ISDR]	
Natural Hazard	the potential source of harm based on a natural phenomenon For more detail please refer to UN-ISDR natural hazards classification [UN-ISDR]	the potential source of perturbation to CI originating by natural phenomenon (example: thunderstorm, earthquake, drought, heat wave).
Threat	the possibility that something bad or harmful could happen	
Event	occurrence or change of a particular set of circumstances (e.g. a physical failure of a CI component)	
Anthropic event	An event that is directly consequence of a human action	
Incident		a generic term indicating that something happened producing a perturbation to a given CI
Harm (or physical damage)		physical perturbation (or destruction) produced by an event on a CI element (bridge collapse due to an earthquake, short circuit of a telecommunication system due to the flooding of the Telco substation). Here we could adopt even a more specific indication: (1) direct harms (i.e. bridge collapse due to an earthquake, overload of a transformer due to lightening etc.) when the physical damage is produced directly by the natural hazard (2) indirect harm in that case where the damage is indirectly produced by the natural hazard: an electrical line break-

		down induced by large energy flow associated with an extra electrical demand for air conditioning, for instance, in case of an heat wave. In this case, in fact, the harm is not produced directly by the natural hazard but is produced by a more complex chain of events that, although originating by a natural hazard, cannot (strictly speaking) be considered a direct consequence of it.
Direct harms		Damage caused directly by a realised hazard
Indirect harm		Damage caused indirectly by a realised hazard (e.g., as an impact of direct or indirect harm)
Impact		direct consequences of the harm at the level of the service provided by the perturbed CI.
Consequences		the resulting perturbations in all sectors supplied by CIs (economic, industry, population, services). Consequences could be either produced by the harm itself (oil spill from a drilling platform due to a hurricane), or produced (indirectly) by the Impact affecting CI (like e.g. the interruption of the hospital services is a consequence of the impact on electric distribution produced by the physical damage of an electrical substation).
Risk	the probability and the amount of harmful consequences or expected losses resulting from interactions between natural or human induced hazards and vulnerable conditions…" (UN/ISDR, 2002)	a numerical value enabling to indicate the link connecting the probability of a given natural hazard to the number of consequences that its manifestations might have on CI elements
Vulnerability	the conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards [drm.cenn.org cap5]	the maximum extent (strength) CI components can stand without being structurally (and thus functionally) perturbed by a natural hazard

2.3 Risk analysis

Critical Infrastructures (CI hereafter) are the set of technological systems whose integrity is a major concern of modern countries: their efficient and continuous functioning allows to provide citizens of primary services. CI are mobility networks (roads, railways), telecommunication networks (cables, wireless), energy-distribution networks (electrical networks for transmission and distribution, gas and oil pipelines), water and sewage pipelines. These infrastructures, in turn, in their different implementations, provide supporting technological functions to other vital such as Galileo satellite constellation and EuroControl, the managing system for civil aviation in EU. These two CI along with the energy and oil pipelines have been recognized as EU-relevant CI and their protection have been committed to national Member States via appropriate protection strategies.

Protection of these assets is a complex tasks as these CI have progressively entangled each other because their functional role. One infrastructure, for instance, provides a necessary service to one (or more) of the others; its fate (and its functioning) can thus determine the state of functioning of the others. If the electrical distribution system experiences an outage due to some perturbation which damages one (or many) of its elements, other infrastructures will suffer and will reduce (or even loss) their functionalities due to the lack (of reduction) of electrical services. This dependency mechanism might produce so-called cascading effects able to amplify the Impact of the initial outage, spread it to other primary services and producing an ultimate set of Consequences on citizens which could be even much bigger than those associated only to the primary (electrical) outage.

Risk analysis attempts to evaluate, for a given scenario (i.e. a set of interconnected CI) the extent of the damages (and of their consequences) related to the hit that an external perturbation could infer to it. At a scale of a CI elements which constitute the scenario, the Risk analysis concerns with the evaluation, for a given element CI_j^x of a system X submitted to some external perturbation source T, of a function linking the probability that the event i.e. the perturbation occurs with a given intensity $P(T_S)$, able to produce a *damage* to the element, and the Consequences that the damage produced on CI_i^x could further propagate on other systems to which the hit network X are functionally dependent.

Let us recall the following definitions before defining the risk:

- *events* represent the occurrence or change of a particular set of circumstances (e.g. a physical failure of a CI component)
- *physical damages* are the physical harms produced by events on CI elements;
- *impact* is the reduction or loss of services due to expected damages;
- *consequences* are the ultimate effects produced by damages and impact on a set of specific *sectors*;
- *service* is the resource that is produced by a certain CI (e.g. electricity is a resource delivered by a power grid);
- *sectors* define the societal assets where we assess the consequences due to physical damages and impact are evaluated i.e. citizens, primary services, industry, environment;

Let us thus define $R\left(T_i, CI_j^x\right)$ the risk associated to the damage of the Critical Infrastructure component j belonging to infrastructure x, let's call it CI_j^x due to Threat manifestation T_i:

$$\boldsymbol{R}\left(\boldsymbol{T_i}, \boldsymbol{CI_j^x}\right) \propto \mathbf{Pr}(\boldsymbol{T_i})\, \boldsymbol{V}(\boldsymbol{CI_j^x}, \boldsymbol{T_i})\boldsymbol{I^T}(\boldsymbol{CI_j^x}) \qquad \textbf{(1)}$$

Equation 1: Risk function of a generic critical infrastructure component affected by a threat.

where:

- $\mathbf{Pr}(\boldsymbol{T_i})$ is the probability of occurrence of the threat T_i
- $\boldsymbol{V}\left(\boldsymbol{CI_j^x}, \boldsymbol{T_i}\right)$ the specific Vulnerability of the element CI_j^x to that manifestation (a specific element could be less vulnerable to some threat and much more vulnerable to others)

- $\boldsymbol{I^T}\left(\boldsymbol{CI_j^x}\right)$ measures the effects that the damage of that physical component produces on the system of systems (called *Impact*) and the ultimate effects (called *Consequences*) produced on sectors.

The $\boldsymbol{I^T}\left(\boldsymbol{CI_j^x}\right)$ term can be further refined as follows:

$$\boldsymbol{I^T}\left(\boldsymbol{CI_j^x}\right) = \sum_{k=1}^{N} \boldsymbol{I_k}\left(\boldsymbol{CI_j^x}\right)\boldsymbol{C_k^T}\left(\boldsymbol{CI_j^x}\right) \quad \textbf{(2)}$$

with:

$$\boldsymbol{C_k^T}\left(\boldsymbol{CI_j^x}\right) = \sum_{s=1}^{4} \boldsymbol{C_s}(\boldsymbol{k}) \quad \textbf{(3)}$$

where $C_s(k)$ is the consequence on sector s of the Impact by CI k induced by the loss of element CI_j^x of CI x. Impact could be weighted by evaluating the consequences that they could produce on population, environment, primary services, and industrial sector. At the end, the Risk equation could be written as follows:

$$\boldsymbol{R}\left(\boldsymbol{T_i}, \boldsymbol{CI_j^x}\right) \propto \mathbf{Pr}(\boldsymbol{T_i})\, \boldsymbol{V}\left(\boldsymbol{CI_j^x}, \boldsymbol{T_i}\right) \sum_{k=1}^{N} \boldsymbol{I_k}\left(\boldsymbol{CI_j^x}\right) \sum_{s=1}^{4} \boldsymbol{C_s}(\boldsymbol{k}) \quad \textbf{(4)}$$

Moreover, it is worth stressing that Equation 1 and its refined version in Equation 4:

- depends on the composition of 3 factors, which individually or together produce an high Risk value (probability of occurrence of a given threat in a specific location, the specific vulnerability of an element to some threat, the large impacts and consequences that could be associated to a physical damage of a CI element). The functional dependency of the Risk on the Impact allows correctly evaluating the risk associated to low frequency phenomena ("black swan") when they can strike with large impacts/consequences.
- with respect to the threat $\boldsymbol{T_i}$, rather than to a threat itself, Risk equation makes reference to a specific threat *manifestation*. A natural hazard (e.g. a tropical typhoon) constitutes a threat for the CI systems as it is associated to several "physical manifestations" (e.g. abundant rainfalls, strong wind, lightening etc.) whose impact on the infrastructures can produce harms (i.e. winds could highly stress mechanical structures, flooding could strike on physical CI elements located in flooded areas, lightning could damage electrical systems etc.). In this respect, we will use $\boldsymbol{T_i}$ to indicate a specific manifestation of a given natural hazard; for a given predicted natural hazard, we will specify which of its manifestations will be used to evaluate the Risk of;
- should be not meant as an algebraic equation to be solved but rather as a methodological equation stressing which are the terms to be appropriately considered to make a complete risk estimate. The first two terms on the r.h.s. of eq.1 are probabilities (that of occurrence of a specific threat manifestation, the other the probability that a specific element will be damages, to a certain extent, by the threat manifestation predicted to manifest with a specific strength). The dimension of the third term (either an Impact or a Consequence of the Impacts) will provide the ultimate dimension with which the Risk will be evaluated. From the dimensional point of view, Pr(T) is a probability, the Vulnerability term will be expressed in an arbitrary dimensionless scale (from 1 to 5) while the Impact will be expressed in a dimensionless unit indication the fraction indicating the reduction with respect to 100% (which is the ideal Quality of Service).

Under these premises, the Risk equation will produce a dimensionless value raging from 1 to 5. However, as a further element that the DSS workflow will able to provide, there will be the measure of Consequences that the predicted Impact might produce.

Example: The Risk that a specific region is facing due to the occurrence of a specific weather scenario will be ultimately evaluated in terms of Impact (by estimating the reduction of the Quality of Services of one, or more, CI providing services to that region).
The gravity scale (from 1 to 5) of the Risk equation could be further specified in terms of expected Consequences in the different sectors (e.g. population, environment, industrial sectors, primary services) by estimating in terms of specific metrics the reverberation of these Impacts on the above-mentioned sectors.

In this respect, the Consequences on industrial sectors will be quantified in GDP losses (dimension: currencies), in terms of citizen affected (dimension: a number, which could be eventually "weighted" in some specific vulnerability index of specific classes of population for a given outage is given), in terms of surface affected by the environmental perturbation and in terms of reduction (dimension= a percentage) of primary services (care capacity of the hospitals, school's activity reduced etc.).

2.3.1 Risk assessment workflow

Based on the prediction of natural disasters and the detection of seismic events, the DSS is able to produce a **Physical Harms Scenario (PHS)** consisting of a vector containing the set of affected CI physical components together with an extent of the estimated physical damage. The PHS can be generically represented as:

$$\boldsymbol{PHS} = (\boldsymbol{CI^T}, \boldsymbol{D^T})$$

Equation 2 Physical Harm Scenario (PHS)

where:

- $CI^T = (CI_1^{S_1}, \dots, CI_H^{SH})$ is the set of CI components that have high probability to be damaged
- $D^T = (D_1^{S_1}, \dots, D_H^{SH})$ is the set containing the extent of estimated damage of each CI component
- H is the total number of physical components that are supposed to be damaged
- $s_i, \in \{1, .., N\}$
- N is the total number of CI considered

Based on the PHS and the specific procedures (discussed in section 4.2.4.4) that are applied to propagate the damage of the H physical components, the DSS is able to produce an **Impact Scenario (IS)** consisting of a vector containing the set of the variations of the Quality of Service (QoS) associated to each CI. The IS can be generically represented as:

$$\boldsymbol{IS} = (\boldsymbol{\Delta Q_1}, .., \boldsymbol{\Delta Q_N})$$

Equation 3 Impact Scenario (IS)

where:

- $\boldsymbol{\Delta Q_i}$ is the variation of the QoS of the generic infrastructure $i \leq N$
- N is the total number of CI considered in the PHS.

Based on the IS and the specific procedures (discussed in section 4.2.4.4), the DSS is able to produce a **Consequence Estimate (CE)** that measures the *consequences* due to the PHS and the IS affecting a set of sectors identified in Table 1 together with its relative factors.

This way, the estimated consequences will be function of the damages and the variation of QoS of the considered services.

In general, the CE is a vector containing the set of consequences divided by specific sector:

$$\boldsymbol{CE} = (\boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, \boldsymbol{C_4})$$

Equation 4 Consequences Estimate (CE)

In Section 4.2.4.4, we will give a numeric example of how the DSS produces a CE.

2.3.1.1.1.1 Sector number	***2.3.1.1.1.2 Sector name***	***2.3.1.1.1.3 Factors***
2.3.1.1.1.4 1	*2.3.1.1.1.5 Citizens*	2.3.1.1.1.6 Income, gender, race, age, education, occupation [37]
2.3.1.1.1.7 2	*2.3.1.1.1.8 Industrial*	2.3.1.1.1.9 Number of plants affected, Number of employees, Amount of production of these plants, number of commercial activities
2.3.1.1.1.10 3	*2.3.1.1.1.11 Environment*	2.3.1.1.1.12 Type of toxic material released, quantity of toxic material released, weather conditions, type of affected area (urban/rural)
2.3.1.1.1.13 4	*2.3.1.1.1.14 Primary Services*	2.3.1.1.1.15 Number of hospitals, schools, governmental offices in the affected area

Table 1: Examples of factors representing the sectors considered in the DSS.

3 Requirements of the DSS

The template of CIPRNet requirements is presented in

Table 2 and consists of the following fields:

- **ID**- is a unique identification number of the requirement, combined of the type and number of requirements (FR: Functional Requirement, NFR: Non-Functional Requirement).
- **Priority** (MoSCoW) – is determined by the importance of the requirement for end-users. Importance is determined by M(ust), S(hould), C(ould) and W(ould) markers.
- **Source** - indicates the origin of a given requirement (e.g. DoW, Consortium experience, end-user/stakeholder).
- **Version** - shows the evolution of the requirement.
- **Description** – provides explanation of the requirement.
- **Comment** – additional, relevant information can be placed here, e.g. reference requirements, comments, examples, etc.

ID		**Priority (MoSCoW)**	
Source		**Version**	
Description			
Comment			

Table 2: CIPRNet requirements template.

In the following we present a classification in terms of functional and non-functional requirements. Each main category is further classified according to the main functionalities of the DSS that are described in section 4.2.4. The present list of requirements represents a further refinement of the requirements reported in [1].

3.1 Functional requirements

ID	FR#10	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise End-users	**Version**	V3
Description	The DSS MUST be able to deal with several types of natural hazards and all their manifestations. As such, it MUST be able to integrate and analyse different types of data from diverse data sources		
Comment	The DSS MUST gather sensor data concerning natural phenomena and their manifestations such as: • Raw data from seismic monitoring networks • Pre-analysed data from specific seismic authorized information sources (e.g. INGV [18] in Italy) with the assessed seismic parameters (loca-		

	tion, magnitude, depth, time of occurrence of the event); • Raw data from meteorological satellites networks; • Raw and pre-analysed data from nowcasting radars (X- and C-band); • Raw and pre-analysed satellite images: multispectral and/or SAR (Synthetic-aperture radar) images; • GIS data acquired from external repositories/sources; • Raw and pre-analysed data for water basins flux meters; • Raw and pre-analysed data from local geo-seismic equipment (like e.g. tuned poles). Raw data will be properly transformed, georeferenced (if necessary) and stored in the DSS Persistence Layer as GIS interoperable formats (compliant to OGC [19] standards).

ID	FR#11	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise End-users	**Version**	V3
Description	The DSS MUST be able to deal with several types of natural hazards and all their manifestations. As such, it MUST be able to integrate and analyse different types of data from simulation results of numerical models		
Comment	The DSS MUST gather and analyse simulation results, released by authorized sources, concerning forecast of natural phenomena and have the option to refine official data with its own simulation results (like e.g. high resolution weather predictions): • Weather forecast data (as received from authorised sources) • Earthquake data and shake maps (as received from authorised sources)		

ID	FR#20	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise	**Version**	V3
Description	The DSS using external raw data, results of simulations made by authorized parties, its own models MUST be able to forecast the probability of the following events: rain and other water-based precipitation and their abundance; landslides, lightening, flooding (upon abundant precipitation), heat waves, fires, tsunami following earthquakes.		
Comment	In particular, the DSS will be able to estimate: • the rainfall in a given area for the next RAFI (see 4.2.4.2) time interval • the lightning events in a given area for the next RAFI time interval • the areas where the risk to have flooding events is greater than a given threshold • the areas where the risk to have landslide events is greater than a given threshold		

ID	FR#30	**Priority**	M

		(MoSCoW)	
Source	CIPRNet consortium expertise	**Version**	V3
Description	The DSS MUST be able to compute the Damage Probability of each CI component in the specified RAFI time frame		
Comment	This phase will involve the evaluation of the damage that different CI are likely to undergo and the estimate of their specific loss (or reduction) of functionality.		

ID	FR#40	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise	**Version**	V3
Description	The DSS MUST be able to estimate the impact on CI of natural hazard phenomena.		
Comment	Damage scenarios will individuate the CI elements (on a single CI or on multiple CI) whose damage probability will be above a given threshold. This information is rapidly provided to operators of the involved CI. They will be asked to provide, as output of the system input, the reduction (or the loss) of functionality of their infrastructures as a consequence of the element fault. They should provide resulting data by using their simulators, fed with data representing the effective state of their infrastructure at the time when the fault could occur. The DSS should thus receive back, from the single CI operators, the estimated impact list.		

ID	FR#50	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise	**Version**	V3
Description	The DSS MUST be able to assess, using a multi-infrastructure simulator (e.g., I2Sim by UBC), the consequences of multiple impacts on a system of *interdependent* infrastructures.		
Comment			

ID	FR#60	**Priority (MoSCoW)**	S
Source	CIPRNet consortium expertise	**Version**	V3
Description	The DSS SHOULD evaluate the social impact due to the loss of CI components and/or services.		
Comment	Such impact may be estimated by crossing the resulting impact on the CI system with information layers of the DB (e.g. in case of an electric outage of an area, the number of electric users residing in such an area and impacted by the outage may be calculated).		

ID	FR#70	Priority (MoSCoW)	S
Source	CIPRNet consortium expertise	Version	V3
Description	The DSS should automatically provide to the end users (Military Advisor, CI operators, Civil Protection, Regional Civil Protection, Regional/Local authorities) daily reports (twice a day) containing CI risk assessment information		
Comment	Assessment of risk of CI (24/7 operations during both alert and non-alert conditions e.g. issued by Civil Protection) to assess the dynamic risk which they are subject in relation to weather-climatological and geophysical forecast. The DSS service availability will be implemented by SPEE ([20]), an external contractor with high-level IT-security skills. SPEE will be involved in the implementation of the I-EISAC operational centre (within an Italian R&D project called RoMA jointly with ENEA); their solutions will be based on DSS mirroring in order to improve the operability of the DSS service. Moreover, all the relevant data used by the DSS, will be periodically cached in the local database of the specific DSS instance.		

3.2 Non-functional requirements

ID	NFR#10	Priority (MoSCoW)	M
Source	CIPRNet consortium expertise End-users	Version	V3
Description	The CIPRNet DB data storage procedure MUST implement a security policy to ensure access control, authentication, integrity		
Comment	The data will be accessed using pre-defined data access rules. Various actors can have different access privileges to the stored data.		

ID	NFR#20	Priority (MoSCoW)	M
Source	CIPRNet consortium expertise End-users	Version	V3
Description	The CIPRNet DB data owners SHOULD be able to specify data access rules		
Comment	For example CI operators may specify specific restrictions and/or constraints for the usage of their data within experiments (mainly what-if analysis)		

ID	NFR#30	Priority (MoSCoW)	M
Source	CIPRNet consortium expertise DoW	Version	V1
Description	The DSS MUST have a usable GUI.		
Comment	The GUI must be accessible via a web browser.		

	It must support a user-selectable language interface. The prototype DSS must preferably support a base set of Dutch, English, French, German commands and responses.

ID	NFR#40	**Priority (MoSCoW)**	S
Source	CIPRNet consortium expertise DoW	**Version**	V3
Description	The DSS should operate on a 24 hours per day, 7 days per week (24*7).		
Comment	The availability of the DSS services will depend, among the others, on the provision of raw data provided via web by different sources (see requirement FR#10). Also data availability should be ensured (e.g. through distributed databases replica solutions).		

ID	NFR#50	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise DoW	**Version**	V3
Description	The DSS MUST have the capacity to service a different of *users* simultaneously.		
Comment	Considering the different users that may interact with the platform during a crisis scenario (i.e. CI operators and Decision makers), we estimate that the maximum number that may interact with the system may be approximately 100.		

ID	NFR#70	**Priority (MoSCoW)**	M
Source	CIPRNet consortium expertise DoW	**Version**	V2
Description	The DSS MUST have high performance in order to produce every hour forecasts against natural hazards.		
Comment	e.g., quick response and short start time to calculate the GIS specific operations that may be computational expensive.		

4 Architectural approach

This chapter describes the ideas and architectural principles underlying the realisation of the CIPRNet DSS platform. To this aim we will adopt a four-layered schema named MCRI already used within the **FP7 DIESIS project** ([27]). The MCRI approach describes the architecture with a layered structure consisting of 4 layers:

- mission layer (M)
- concepts layer (C)
- realisation layer (R)
- implementation layer (I).

as shown in Figure 2, MRCI architectural description is a pyramidal scheme useful to better define, describe and motivate the implementation decisions and details.

The pyramid describes the following aspects of architecture step by step:

- **Mission** What are the goals of the architecture?
- **Concepts** Which are the (up to) 10 core ideas underlying the architecture?
- **Realisation** How will core ideas be turned into ICT solutions? What ICT methods shall be applied?
- **Implementation** How will the realisation be assured by means of tangible ICT solutions, what ICT systems will be used?

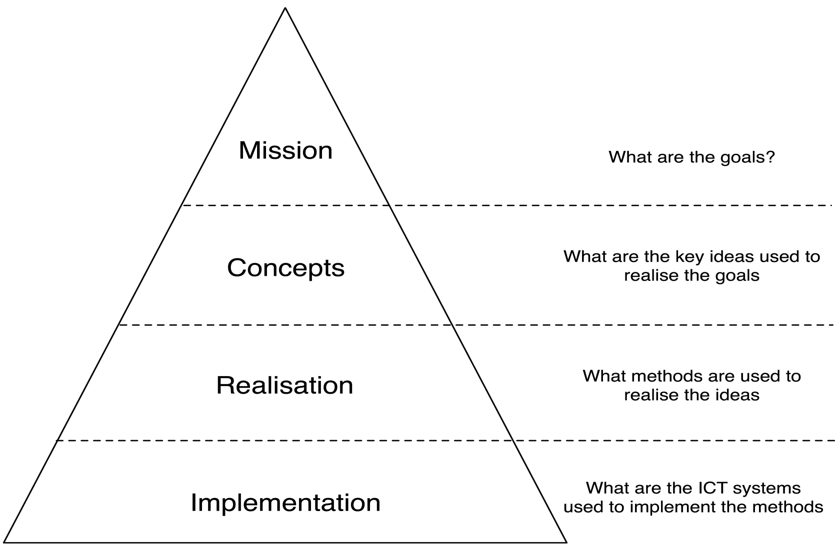

Figure 2: The MCRI four layers architectural description [27].

4.1 Mission

The main objective of the DSS is to provide a set of knowledge driven functions, information and suggestions to CI operators and emergency (crisis) decision-makers to be adopted for the daily analysis of the state of risk of their infrastructures and during crisis situations. In the latter case they should be able to suggest mitigation strategies and support for the decisions during emergency (crisis) management. The provided set of functions include:

- the prediction of the physical damages (harms) that the manifestations of the natural hazards will produce on CI elements
- the estimate of the impact (in terms of reduction, or loss, of services) on all CI as a consequence of the predicted physical harms of the CI elements
- the consequences produced by the predicted impacts on technological services, on population, the environment
- in some specific cases, the suggestion of possible strategies to be adopted to prevent the impacts and the consequences, and/or to mitigate the effects. All suggestions to support decisions will preliminarily verify the consequences of different possible technical options (and chosen on the basis of their compliance with ethical issues).

4.2 Concepts

The main objective of WP7 is the creation of the prototype of the CIPRNet DSS allowing the prediction of crisis scenarios, their impact on CI and the resulting consequences of CI reduction and/or loss of services on the population and the environment. The development and implementation of the prototype allows the identification and the refinement of a set of minimal requirements regarding DSS functionalities, the data and models needed to realize such functionalities and the related level of accuracy and granularity to guarantee the effectiveness of the DSS. In the future, the DSS prototype will evolve in a framework running within a national EISAC node (e.g. the I-EISAC node) that will be effective on all national territory (e.g. the Italian territory). The DSS outcomes will satisfy the minimal requirements and services identified within the CIPRNet project.

The proposed architecture is based on three main concepts

- *Clustered architecture*
- *4-Layer architecture*
- *Pluggable architecture*.

In the following sections, we will describe the rationale for these concepts.

4.2.1 Clustered Architecture

The *Clustered Architecture* is a concept related to the architecture of an EISAC national node (e.g. I-EISAC node). As stated in the previous paragraph, the DSS framework of an EISAC national node needs to be effective on all national territory. To this aim, different clusters will form the DSS framework, each running a specific and customised Critical Infrastructure Risk Assessment Workflow to reflect the peculiarities of specific territorial area. The national territory will be divided in different domains (this division could map the administrative organisation of the territory or be made for homogenously covering the whole national territory by having equivalent domain sizes in terms of population and complexity of the CI arrangement), each domain being allotted to a *Cluster*. The customisation of the DSS for the different domains allows the inclusion within the framework of specific external source of data (e.g. weather forecasts, nowcasting) and, in general, very specific impact and consequence analysis models (see 4.2.4.2). At the same time, each cluster may implement specific procedures to better meet the requirements of local authorities and local emergency decision makers.

Figure 3 shows the EISAC node clustered architecture and its main components:

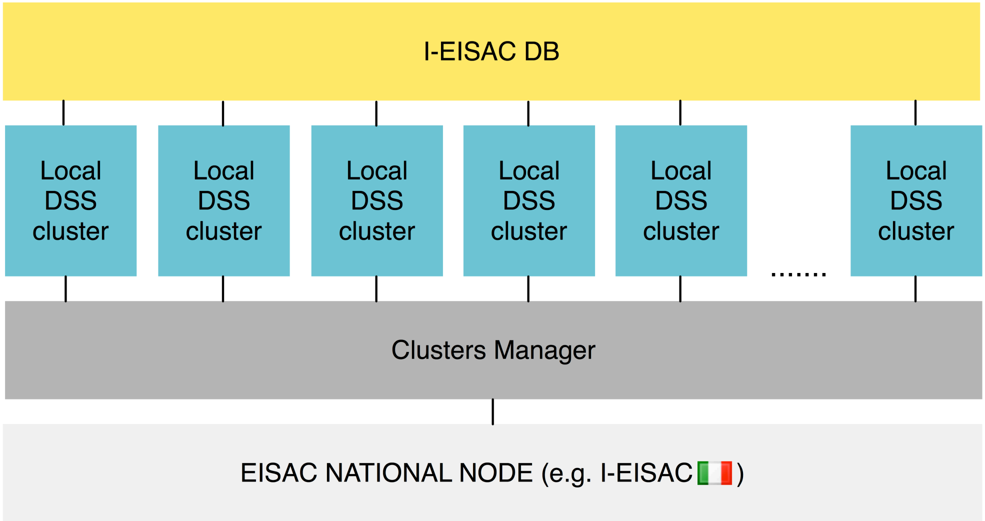

Figure 3: DSS Clustered Architecture

- *Cluster manager*: through this module, a EISAC super administrator will be able to control, monitor and configure each local DSS cluster;
- *Local DSS cluster*: a local DSS cluster runs the DSS core business logic for a specific area (e.g. Lazio region in Italy);
- *EISAC DB:* the EISAC node relies on a persistence layer containing:
  - information common to all local DSS cluster (e.g. national GIS data);
  - information for the administration of users, roles, and permissions;
  - information to be used by the different EISAC services (e.g. "ask the expert" and CIPedia services).

The main advantages of the clustered architecture are:

- easy customisation of specific territorial needs and requirements;
- incremental development of the national EISAC node;
- the cluster management allows the physical dislocation of local DSS clusters. An optimal and *ad-hoc* dislocation can improve the overall EISAC node resilience and robustness
- scalability of the solution

The next architectural concept extends the Clustered Architecture concept as it is related to the customization of each DSS cluster.

4.2.2 Pluggable architecture

As discussed in the previous section, each DSS cluster may use *ad hoc* models (e.g. CI network models, dependency/interdependency models), data (e.g. high resolution weather forecasting data, now-casting data) and simulators available only for specific areas. Furthermore, each DSS cluster may reflect the particular needs and requirements of specific areas (e.g. critical assets and the population near the coast are subjected to threats different from those of another area). Then, the DSS cluster architecture needs to be as flexible as possible in order to allow the easy customization of the core DSS functionality, that is, the CI Risk Assessment Workflow, to reflect the different territorial needs. The previous considerations bring to the architectural concept of *Pluggable Architecture*.

Each Local DSS Cluster will develop plugins to extend the architecture to include specific services and models. In the following, two examples of how the Pluggable Architecture concept is adopted will be shown.

4.2.2.1 Data Access Service plugins

The DSS needs to be fed with external data coming from different sources in order to run models/algorithms to predict the occurrence of natural hazards at an appropriate geographical scale and within a specified time interval. Figure 4 shows the possible different sources of data (e.g. weather forecast, seismic monitoring network) and the various *ad-hoc* plugins needed to be implemented in order to a) gather external field data, b) manipulate the data in order to make them compliant with the CIPRNet data formats and c) store the data within the CIPRNet DB. More specific plugins may be implemented in this module in order to acquire specific data only available for specific area as, for example, the now-casting forecast data related to a specific city.

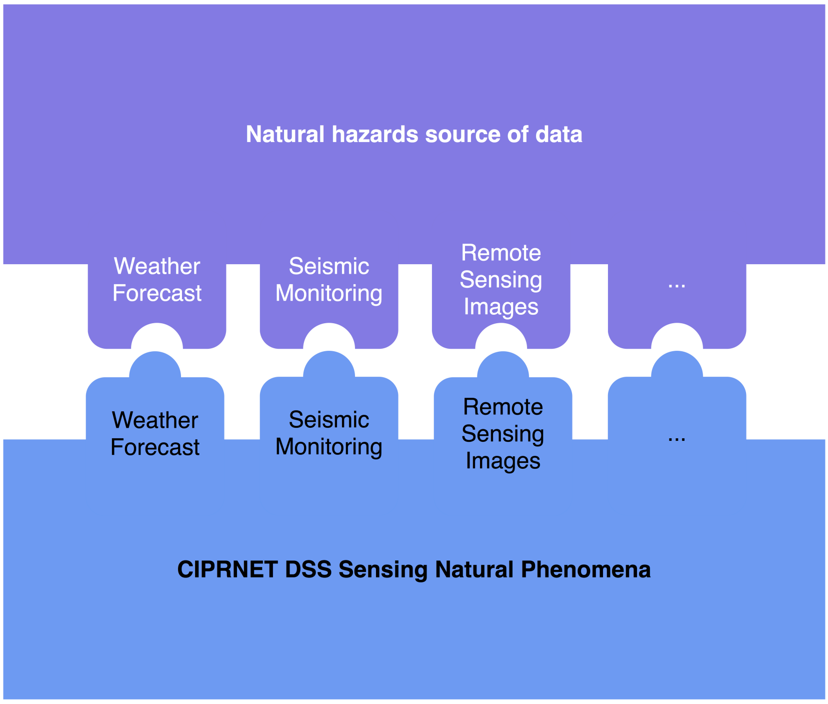

Figure 4: Data Access Service plugins

4.2.2.2 Simulation Service plugins

The *pluggable architecture* concept will be the basis also for the impact evaluation module where the DSS will run a multi-infrastructures simulator (e.g., I2Sim by UBC) to provide an assessment of the consequences of multiple impacts on a system of dependent and/or interdependent infrastructures (Figure 5). In order to guarantee the minimal requirements of functionalities, the multi-infrastructure simulator may need to run domain specific simulation invoking a specific domain simulator (e.g., PSS SINCAL for the power electric domain, NEPLAN for the gas domain) whenever it will be impossible to rely on CI operators data. In particular, the multi-infrastructure simulator may need to run a specific domain simulator to verify the feasibility of the various configurations computed during the simulation (e.g. to verify if a load shedding configuration for the electrical domain is feasible or not). As shown, each domain simulator will require the development of an *ad-hoc* adapter to allow the exchange of data, commands and configurations with the multi infrastructure simulator. The multi-infrastructures simulator may need to exploit a *federated simulation service* and in particular the services coming from the what-if analysis tool developed within the CIPRNet WP6.

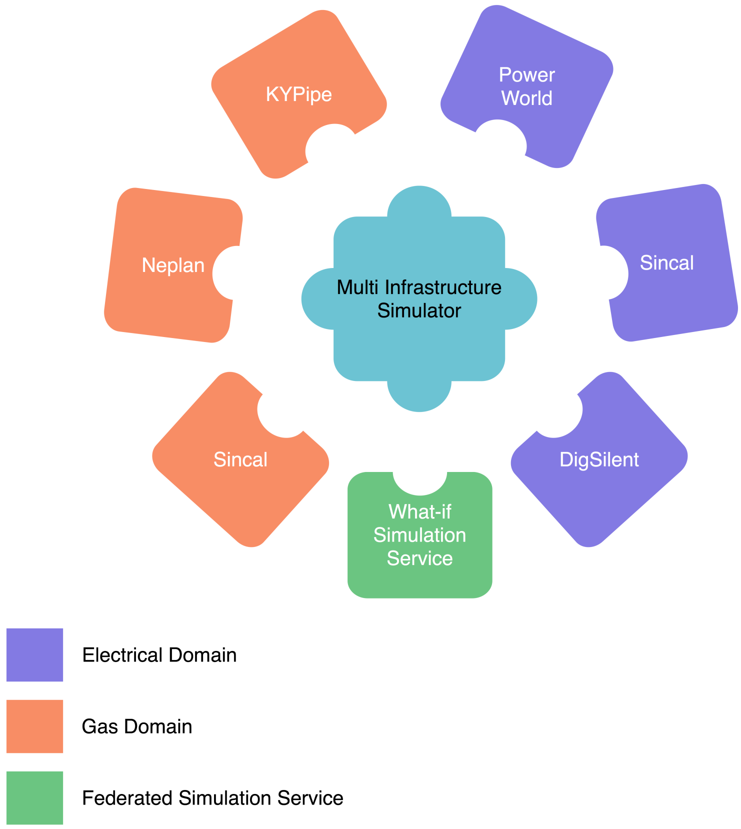

Figure 5: Plugin Architecture for Multi Infrastructure Simulator.

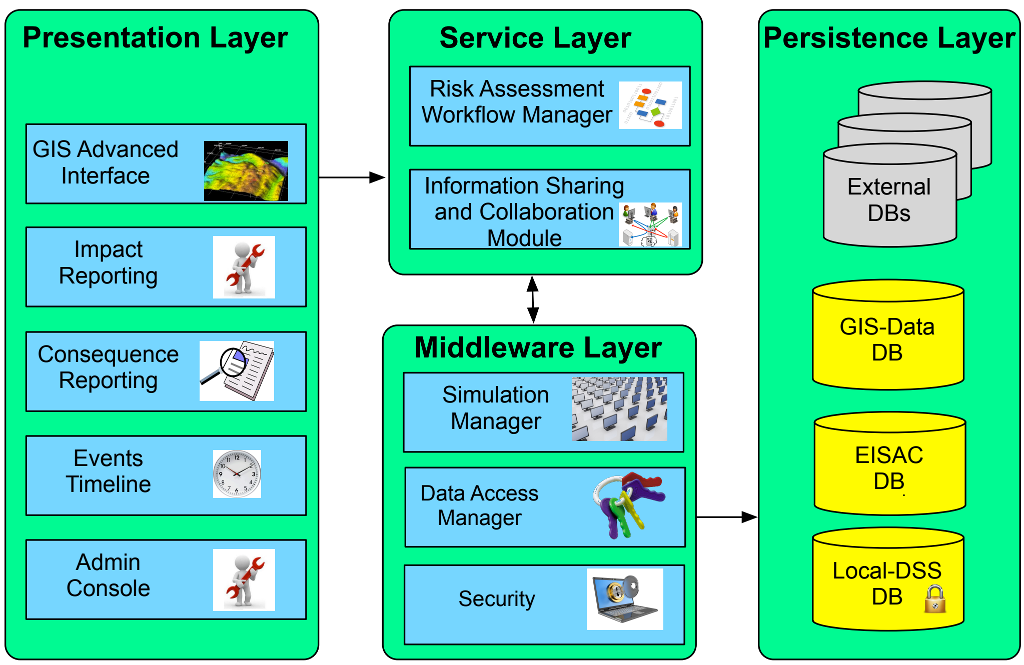

Figure 6: Local DSS 4-tier architecture diagram.

4.2.3 4-Layer Architecture

The architecture of each DSS cluster is based on the well-known 4-Layer architectural pattern for web applications. The different layers are conceptually and physically (if needed) separated. Figure 6 shows the 4 Layer architecture for the local DSS cluster that is composed of a Presentation layer, a Service layer, a Middleware layer and a Persistence layer.

In the following, all components of each layer will be further discussed.

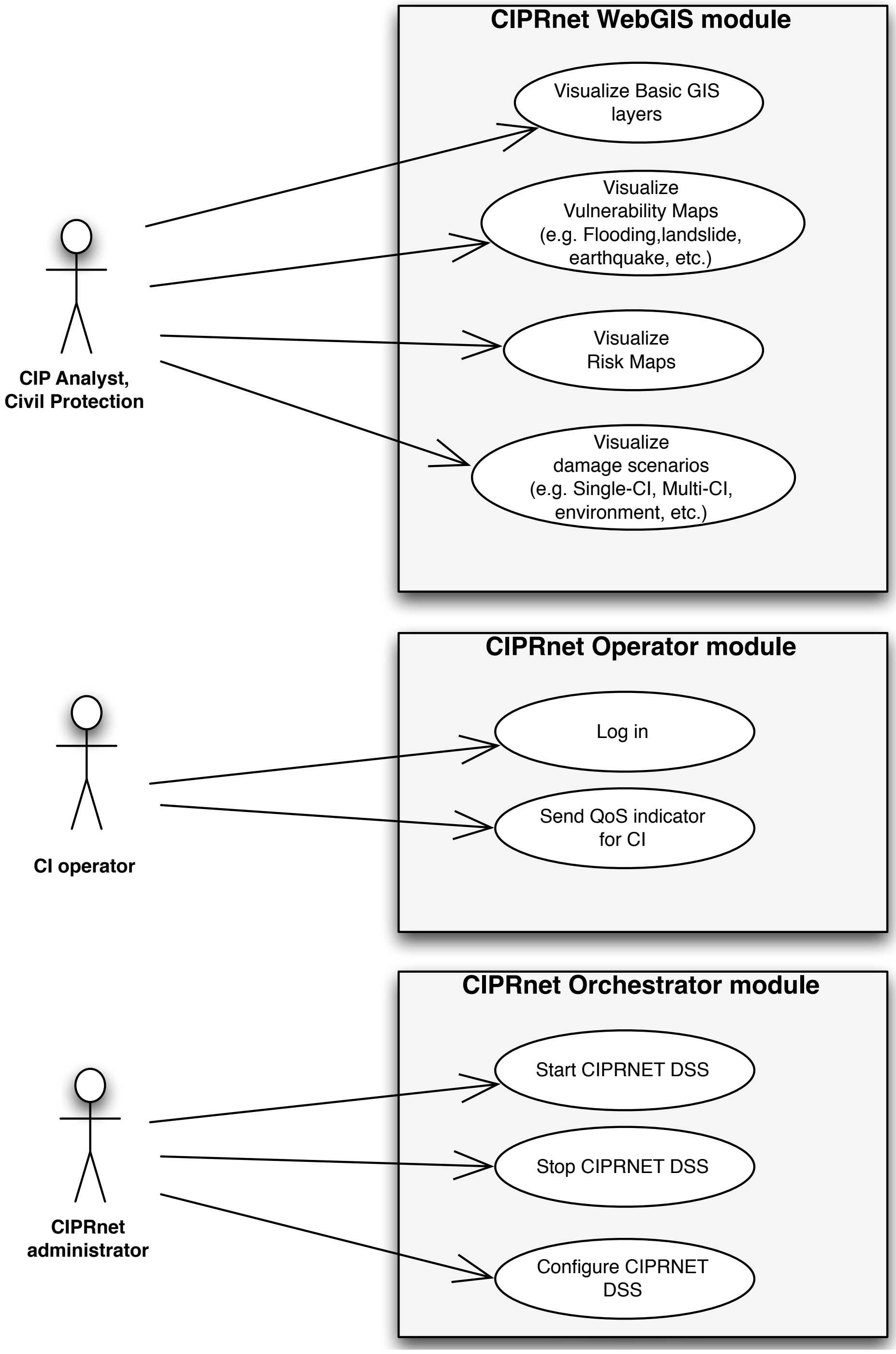

Figure 7 UML DSS use-cases diagram.

4.2.3.1 Presentation Layer

This layer, in general, will contain the components that implement the different GUI used by the DSS platform end-users. Such components are based on GeoPlatform, an Open Source Framework for creating Rich Web GIS Applications based on geospatial web-based software and using an open source approach (see Annex 3). The use of GeoPlatform allows building the so-called *thin clients* that do not require any installation w.r.t. *desktop clients*. In addition, being based on web browsers, GeoPlatform can also be used without providing admin rights on those networks where software installation may be restricted for security purposes.
In the following, the main components of this layer will be briefly described.

4.2.3.1.1 GIS Advanced Interface

The GIS Advanced interface integrates public available WMS and/or WFS layer to visualize different thematic maps. For example, this feature can be used to display seismic risk maps and hydrogeological risk map. The system also integrates data coming from the Italian National seismic monitoring networks thus being able to capture seismic events occurring in Italy. To this regard, the system can display public available shake-maps and/or the result of the DSS computation for the impact estimation of the seismic event.
The system is also able to acquire Meteorological/hydrological sensor networks to display water levels, temperature, wind data and so on.

4.2.3.1.2 Impact Reporting

This component allows the visualization through GIS maps of those CI components that are estimated to be affected by a natural hazard in the next future. The user management and permission role procedures will ensure that each end user will visualize the information he/she is allowed for. The visualization through GIS maps will provide decision-makers with a picture of the state of the CI networks in a specific area that may be affected by natural hazards.

4.2.3.1.3 Consequence Reporting

This component allows the visualization through GIS maps of the consequences on the society, the environment and the industrial sectors that may be caused by the estimated failures occurring in CIs. In addition, this component also integrates specific models that provide efficient strategies to cope with crisis scenarios (e.g., calculation of optimal paths to reach affected areas). Both features may support a decision-maker when implementing actions needed to mitigate crisis scenarios.

4.2.3.1.4 Events Timeline

This component will show a timeline to display past event as well natural hazards that have been forecasted by the DSS. The TimeLine will be constantly updated with the occurred events (on the “negative” time domain) and with predicted events (in the “positive” time domain). Positive and negative attributes are provided on the basis of the moving “time” (i.e., this instant) dividing the past from the future.

4.2.3.1.5 Admin Console

The Admin Console will be used to monitor the DSS platform performances, and to perform all administrative operations. The Admin Console will be used by experts to set triggering event security thresholds (e.g. the earthquake DSS workflow will be triggered if and only if there will be an earthquake of a fixed magnitude). The Admin Console will be used as well to load in the EISAC DB all need static data as for example the vulnerability information data related to the interested CI components (see 4.2.4.2 to better understand how the vulnerability data are used within the Risk Assessment Workflow).

4.2.3.2 Service Layer

This Layer contains all modules that realise the DSS business logic. A central component of the Risk Assessment Workflow Module that orchestrates all operations of the local DSS such as the management of the end users and admin requests, the execution of process monitoring and configuration tasks of the Earthquake and Weather Forecast Workflows, the implementation of GIS services to allow the visualization and the manipulation of GIS data.

The Information Sharing And Collaboration Module allows the access to a collaborative platform (see Annex 2) to exchange data with CI operators and crisis decision makers.

In section 4.2.4, further details about the realisation of the Risk Assessment Workflow Module will be described.

4.2.3.3 Middleware Layer

The Middleware Layer implements procedures to gather, on a 24/7 basis, data coming from external sources such as meteorological data needed to feed models and simulations enabling the prediction of future extreme natural hazards. It contains two modules that realize the HPC services and the data access logic. In particular:

- The Simulation Manager monitors the DSS cluster instances to execute simulation models and to perform load balancing and task migration procedures;
- The Data Access Manager performs all the operations needed to operate with the Persistence Layer and implements solutions to be compliant with the basic requirements for database and network security.
- The Security module implements the availability requirements to ensure that DSS services and data will be accessible to final end users even in case of equipment failures (in general, the availability requirements are specified through minimum acceptable thresholds percentage of the time the service is available). To this end, this component implements a replica of the database servers, and of the file system of the DSS server to obtain a redundant distributed geographically database server.

4.2.3.4 Persistence Layer

The Persistence Layer will contain all data to be used within a CIPRNet DSS cluster instance. Each DSS cluster may store and/or retrieve these data in different databases:

- a public **GIS-Data DB** storing the GIS layers (compliant to INSPIRE [25] and OGC standards [19]). The data stored within the persistence layer will belong to different pre-defined categories:
  - Territorial layer
  - Socio-economical layer
  - Technological Infrastructure layer
  - Historical events layer

  Each layer can be divided in 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.

- a private **Local-DSS DB** containing custom information specific for each DSS cluster (e.g. the GeoPlatform users and projects);
- an **EISAC DB** containing data information common to all DSS clusters;
- a set of **External DBs** to retrieve data that can be accessed outside the DSS-cluster via specific protocols and interoperability standards (e.g. OCG standards for GIS data).

For instance, the sources of GIS-data can be governmental repositories (e.g. the national GIS repositories as the Italian SINANET site [26], the Italian National Institute of Statistics – ISTAT [22]), infrastructure operators, data coming from simulation models as the weather forecasts data that need to be logged in order to allow different kinds of offline analysis (e.g. statistical analysis).

In general, the data stored within the persistence tier will require different frequency of update operations. For example, the number of people living in a specific area need to be updated once each a year whilst 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 requirement. In some case the data updating operations will depend on authorized data scraping automated procedures.

The persistence tier will, in general, store already available historical data (e.g. rainfall data) and will allow the development and the maintenance of historical series of data.

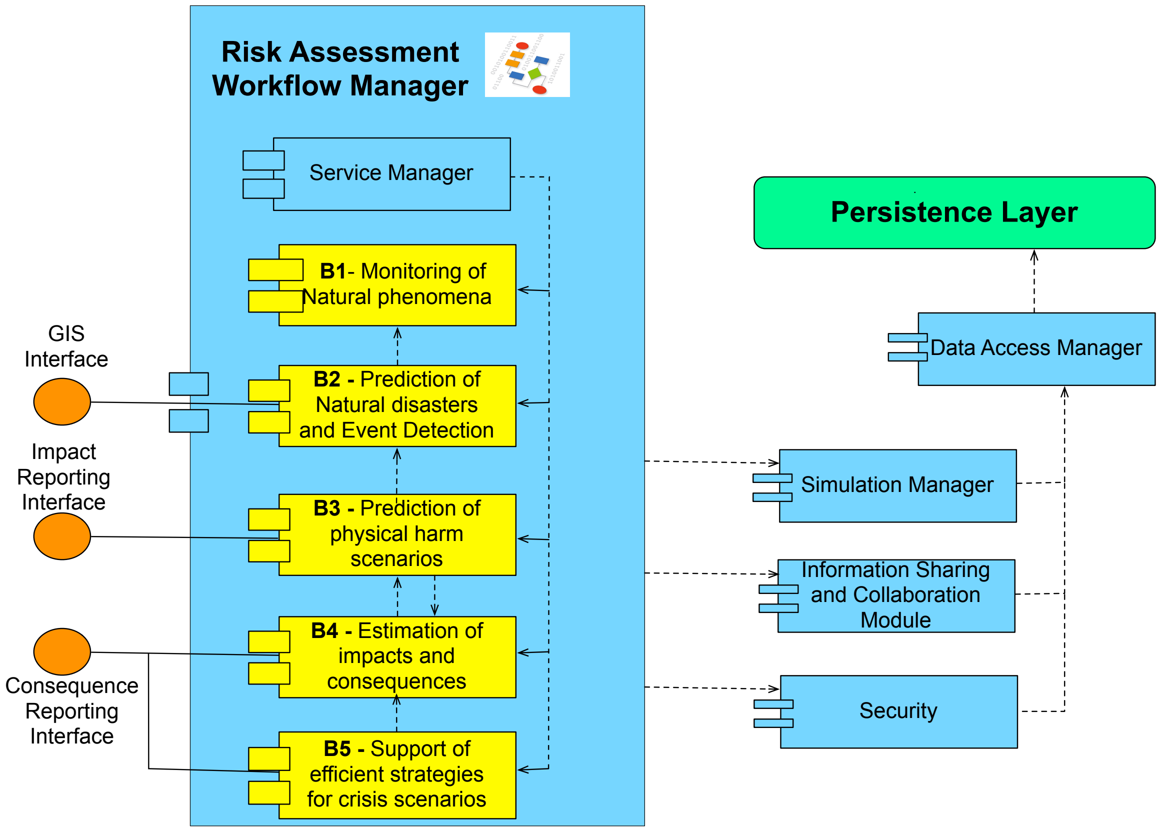

Figure 8: UML Components Diagram.

4.2.4 Realisation

In this section we describe how the key architectural concepts described in the previous section will be realised. In particular, we will focus on the realisation of the key functionalities of the DSS cluster architecture that is the *Risk Assessment Workflow Manager*. Figure 8 shows a

UML components diagram showing the *Risk Assessment Workflow Manager* consisting of five components or *functional bricks* ($\boldsymbol{B_n}$):

- ***B1: Monitoring of Natural phenomena***
- ***B2: Prediction of Natural disasters and Events Detection***
- ***B3: Prediction of physical harm scenarios***
- ***B4: Estimation of impacts and consequences***
- ***B5: Support of efficient strategies to cope with crisis scenarios***

The B_i will be inter-linked by the databases in the Persistence Tier (in the following we will refer to the Persistence Tier with CIPRNet DB) where new data will be stored together with historical data concerning with all types of geo-referenced information needed for the set up of the brick's functional actions.

The functional bricks presented in this section are related to the **Critical Infrastructure Risk Assessment** formula given in Equation (1). In particular:

- **B2** evaluates $\mathbf{Pr}(\boldsymbol{T_i})$ **-** probability of occurrence of the threat T_i by using all types of data provided by **B1**
- **B3** evaluates the product $\mathbf{Pr}(\boldsymbol{T})\ \boldsymbol{x}\ \boldsymbol{V}(\boldsymbol{CI_j^x}, \boldsymbol{T})$ – the expected physical damage D due to all possible threats on a CI element in a given area;
- **B4** evaluates $\boldsymbol{I}(\boldsymbol{CI_j^x})$ **-** is the sum of the impacts that the absence of the j-th CI component/service in produces upon failure in its network and in the other CI networks functionally related to it and the related consequences on the environment and on population affected by those failures.

The Risk Assessment Workflow can be triggered in two different ways:

- The Service Manager triggers and monitors in a prefixed scheduled way the DSS Risk Assessment Workflow for *predictable natural* hazards (as for example meteorological natural hazards). For instance, the Service Manager may trigger the risk assessment workflow twice a day, at 6.00 am and 6.00 pm.
- The Data Access Service implements procedures to gather, on a 24/7 basis, data coming from monitoring sensing networks as for example seismic monitoring network in order to acquire as soon as possible, the occurrence of *unpredictable natural hazards* (e.g. earthquakes).

Figure 9 shows the UML Deployment diagram that shows the interactions among the DSS server, the GIS server and the DB servers:

- the **DSS server** executes all the tasks needed for the Risk Assessment Workflow;

the **GIS server** is based on two servers: (i) *GeoServer* [28] to manage GIS data which can be provided to different kinds of clients such as web browsers and GIS desktops and (ii) *Geo-Platform* server (see Annex 3) runs on Linux machines only and allows to build advanced GIS interfaces;

- the **DB servers** consisting of the GIS-Data DB, the Local-DSS DB and the EISAC DB servers (the latters hosted in the ENEA UTMEA Computer Centre to provide higher physical security given by a locked room (where only authorized ENEA staff members can access the room) and a fire and UPS system. The GIS-Information DB will be based on PostGIS DBMS v.2.x to manage GIS data whereas the other DBs will be based on Postgres DBMS v.9.2.

Moreover, as shown in Figure 9, the ENEA UTMEA building is located inside the ENEA Casaccia Research Centre, a 24/7 access controlled Centre equipped with a system of doubled high security fence. Regarding the IT security, access control requirements is provided by two firewalls:

- the CIPRNet servers software-based firewalls;
- the ENEA Casaccia firewall and monitoring systems that constitutes the main barrier to ensure access control to CIPRNet data and systems.

Further details about the data security features implemented to secure the CIPRNet data, can be found in [5].

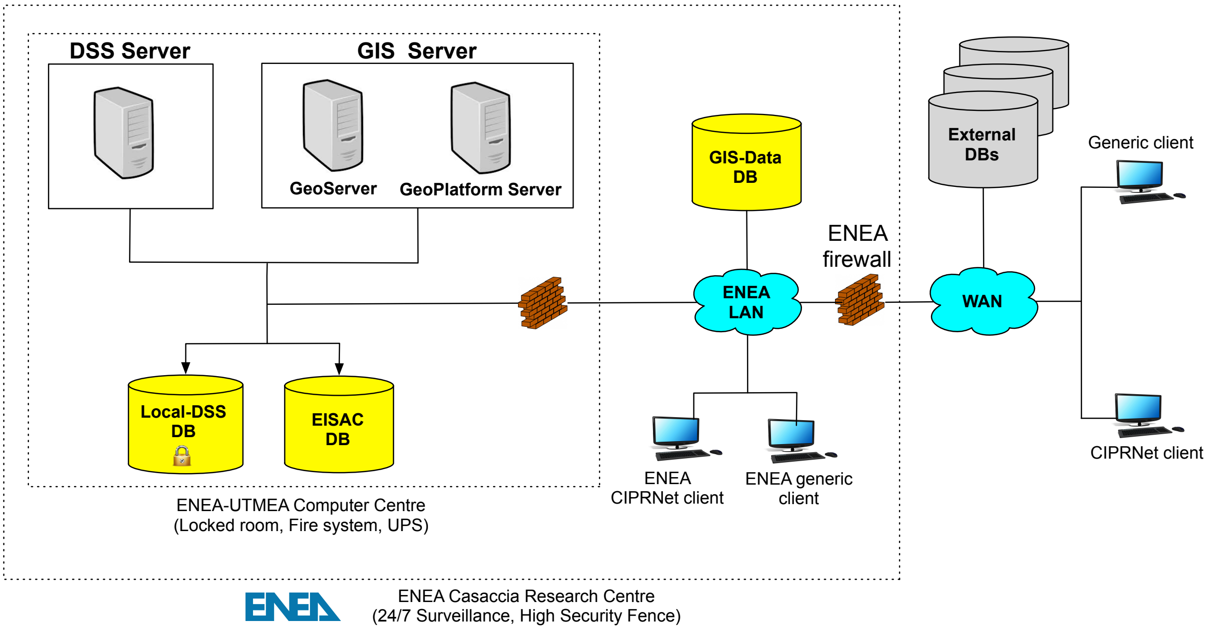

Figure 9: UML Deployment diagram.

4.2.4.1 B1: Monitoring of Natural phenomena

The functional brick **B1** implements all the actions needed to feed the DSS Risk Assessment Workflow with external data. These will encompass geo-seismic data, weather data and, in general, "raw" data, which the system should be able to handle, use for its purposes and store into the DB Persistence layer. There can be different sources of external data:

- *Seismic monitoring network to obtain data about earthquakes (localisation, magnitude)*
- *Meteorological satellites network*
- *Now-casting radar monitoring network*
- *Satellite SAR Images*

Figure 10 shows the workflow of B1. The Data Access Manager implements the procedure to import data from external data sources. Data acquisition can be *on demand* and *batch* procedures. The former may be used to import data on a scheduled way (the Service Manager component will activate the data acquisition procedure), whilst the latter can be used to continuously get data from external monitoring sensing networks, as for example earthquake data coming from the INGV (the Italian National Institute of Geophysics and Volcanology) database, for the I-EISAC node. The B1 functional block uses the Data Access Service to store the data within the CIPRNet DB.

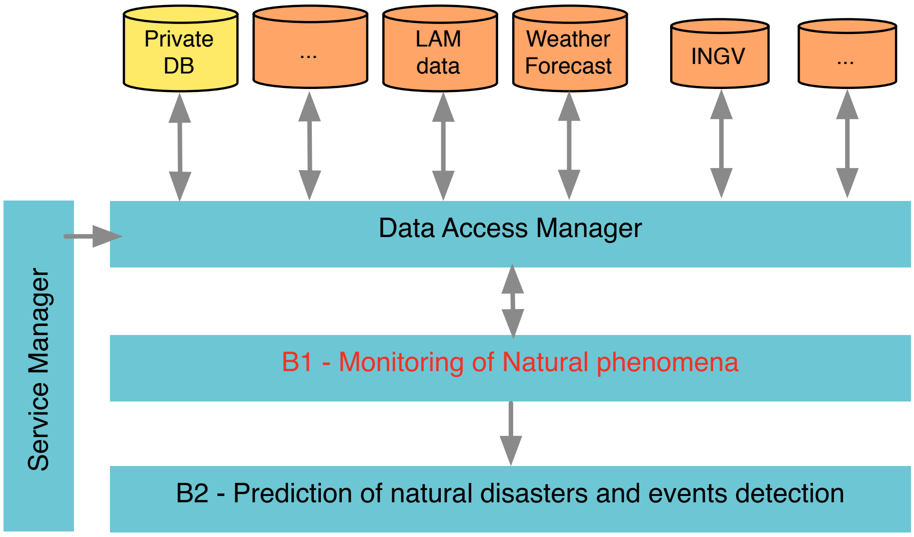

Figure 10: B1 Workflow Diagram: Monitoring of natural phenomena (LAM = Local Area Models, INGV = Italian National Institute for Geophysics and Volcanology, Weather Forecast will be provided by authorized sources like, e.g., the Servizio Meteorologico Aeronautica Militare).

4.2.4.2 B2: Prediction of natural disasters and events detection

Functional brick **B2**, as shown in Figure 11, will orchestrate a number of activities on the basis of incoming data: among others, the prediction of natural phenomena at the "appropriate scale" with indication of precipitation abundance, wind speed etc. "Appropriate scale" indicates that, in general, predictions will be made on the basis of the spatial resolution of the forecast released by appropriate sources (usually 5-10 km). However, for specific purposes (i.e. critical areas where higher resolution would be needed) the system could develop and/or use and rely on high-resolution local models (down to 1 km resolution). When downscaling through Local Area Model (LAM) is performed, the DSS will abandon the use of certified predictions (i.e. those, at larger scale, provided by authorized national authorities (like, e.g. in Italy the Air Force MetOffice) to use its own model that, although providing an high resolution forecast, will be possibly less prone to errors (as LAM models cannot have the same level of reliability of models that are officially used for releasing weather prediction nation wide). However, the accuracy of LAM will be carefully checked with a continuous assimilation of historical data in order to determine the range of confidence of its predictions. To the purpose of producing accurate and reliable forecasts, also sensors data, when available, will be used to provide forecast within a specified Risk Assessment Forecast Interval[1] (RAFI in the following) (e.g. 48 hours).

Let us further introduce the perturbation, by means of the indication of the manifestation of T_i the natural hazard. The natural hazard will be predicted with probability ***P*** together with its strength s_i. For all threat's manifestations, we will define a function that will project the effective strength (measured with the usual units of measure) into a phenomenological scale (***Grade Scale***) containing 5 levels (from 1 to 5) such as

$$F:(s_i) \rightarrow [1,5]$$

[1]The RAFI parameter represents the next temporal horizon (expressed in hours) of the risk assessment methodology. For example, for the EISAC IT configuration, the RAFI parameter would be 48 hours. In general, the RAFI parameter will depend on the meteorological forecast data (e.g. for the EISAC IT they are valid for the next 48 hours).

The ***strength transformation F*** will allow, for each threat manifestation s_i, the definition of a scale of phenomena manifestation. Let us imagine, for instance, that an earthquake will manifest, in a given area position r, a GPA (ground peak acceleration) equal to 0.20 g (GPA is measured as a fraction of the gravity acceleration g = 9.8 m/sec^2). According to the following Italian partitioning of seismic region [2]

- zone 1: $0.25g < GPA \leq 0.35g$
- zone 2: $0.15g < GPA \leq 0.25g$
- zone 3: $0.05g < GPA \leq 0.15g$
- zone 4: $GPA \leq 0.05g$

we will define the following **F** transformation:

F=1 if $s_i \leq 0.05g$

F=2 if $0.05g < s_i \leq 0.15g$

F=3 if $0.15g < s_i \leq 0.25g$

F=4 if $0.25g < s_i \leq 0.35g$

F=5 if $s_i > 0.35g$

Similar definition will be made with all other threat's manifestations, taking into account the specific characteristics of each natural phenomenon. Using for all threat's manifestations a similar transformation in the scale 1-5, a given environmental situation (or its prediction at a given time t) will be expressed to a "***threat strength matrix***" ***S*** (where the rows refer to the type of threat's manifestation and columns span in the interval [1-5]). In a case where at time t and at a considered site r, an earthquake is considered of GPA =0.20 g and a wind speed of 20 knots (corresponding, for instance, to ***F=2*** in the wind speed-grade scale), the associated ***threat strength matrix*** will be as follows (Table 3 represents the output of B2):

Table 3: Threat strength matrix.

	Threat grade				
Threat name	**1**	**2**	**3**	**4**	**5**
Earthquake (ground acceleration)	0	0	1	0	0
Strong Wind	0	1	0	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	0	0
Mud flows	0	0	0	0	0
Debris avalanches	0	0	0	0	0
Heavy Rain	0	0	0	0	0
Storm surge	0	0	0	0	0
…	0	0	0	0	0

[2] http://it.wikipedia.org/wiki/Classificazione_sismica_dell'Italia

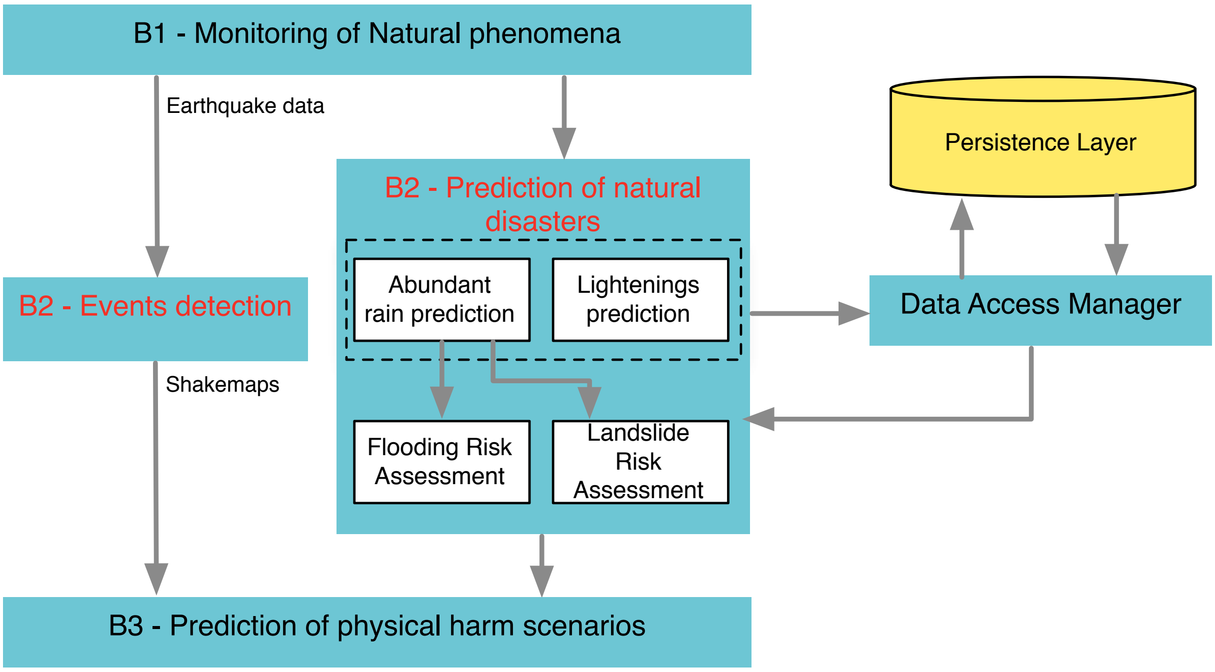

Figure 11: B2 Workflow Diagram: Prediction of Natural disasters and Events Detection.

4.2.4.3 B3: Prediction of physical harm scenarios

Functional brick **B3** is responsible for the prediction of harm (or physical damage) scenarios (Figure 12). Expected physical damage scenarios involving components of critical infrastructures on a hazardous area will be performed by computing the *Physical Damage Probability* of each CI component in the specified RAFI time frame (e.g. 48 hours). This phase will involve the evaluation of the harms that different CI are likely to undergo and the estimate of their specific losses (or reduction) of functionality. The B3 outcome will be a *Physical Harms Scenario (PHS)* describing the affected CI components and the extent of the physical damages. Estimates will be done either by using historical data and vulnerability assessment based on empirical functions. This is a relevant part of the whole DSS. This function correlates the predicted manifestations of a natural hazard to possible harms that the CI elements of the wounded geographical area can suffer. For example, using CI operators failure historical data and historical rain precipitation data on a specific area can be possible to find a correlation between these series of data and to find a valid precipitation rain vulnerability threshold of the different CI components. A deep CI components vulnerability analysis will be performed involving the CI operators and exploiting the literature on this subject. This is a central point as, to date, alerting systems of Civil Protections are related to the prediction of over-threshold intensity manifestations of natural hazards, lacking entirely a reliable (quantitative or even qualitative) assessment of the possible damage associated to them. Physical Damage Probability of different components can, indeed, depend on the specific hazards: damage of specific elements could be produced by some hazards and not by others. The results of this phase will be reported to the different CI operators.

Reporting of the PHS to one (or more) CI operators will be a confidential task as the information delivered may contain data regarding the degradation of infrastructural components and services of CIs. This information exchange will be carried out by using the Secure Information Sharing Platform that will be released by the project as a complementary (although relevant) part of the whole DSS. This platform (whose main objectives and technology will be described in Annex II) will be a web-based application allowing the secure exchange of information between CI operators and between the DSS management and the CI operators. Using such a platform, the PHS and the set of the impacts on the CI will be delivered by the DSS and CI operators respectively (see Section 3.2.3.4, on the other hand).

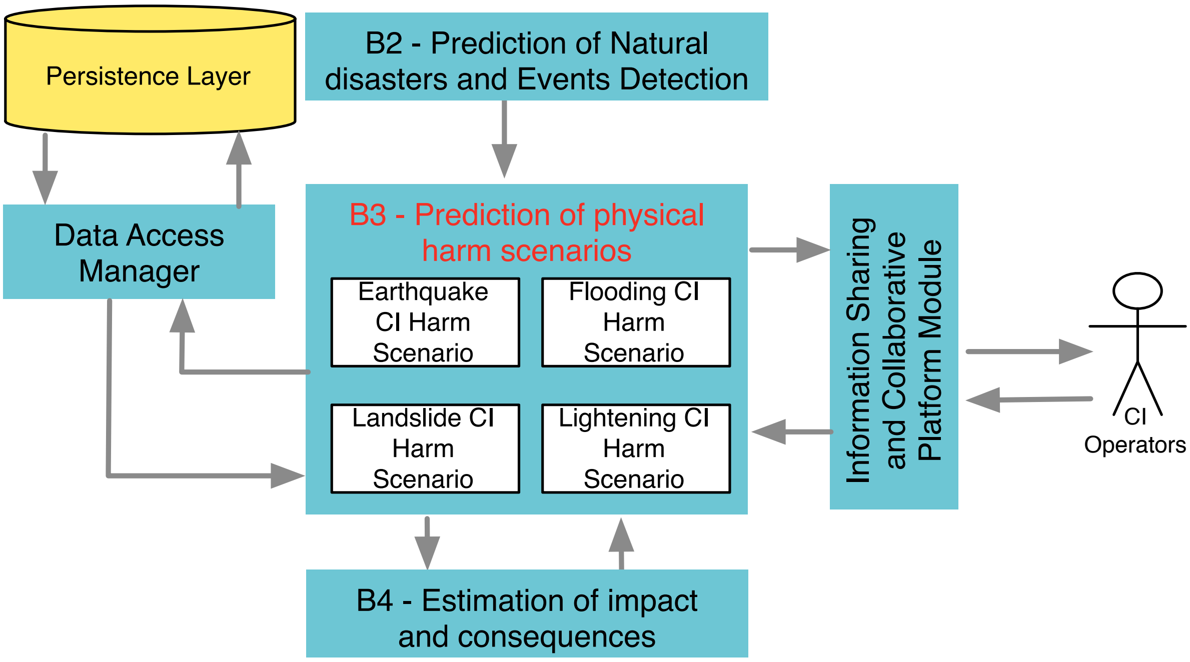

Figure 12: B3 Workflow Diagram: Prediction of Physical Harms Scenarios.

In the following, we will explain how the *PHS* will be obtained. From each CI element positioned in a given position area r, a ***"vulnerability matrix"*** V_{ij} will be loaded from the CIPRNet DB, which entries will be related to the maximum extent (strength) the element can sustain without being structurally (and thus functionally) perturbed. This matrix has the same rows and columns that the ***S*** matrix. The v_{ij} matrix element thus represents the extent of perturbation produced on the element by a threat manifestation ***i*** having a strength ***j***. In the example of Table 4, we report the case of a CI element which is perturbed at 50% for a grade 3 manifestation of earthquake (and completely, i.e. 1, for larger grades), completely by grade 2 (and above) winds, completely by grade 5 lightening, heavy snowfall and ice and completely by grade 4 (and above) flooding. The definition of Vulnerability Matrices of the different CI elements will be carried out by using element's technical data sheet and by elicitation with CI operators.

In general terms, the extent of physical damage ***D*** produced by a the threat manifestations $\boldsymbol{S_{ij}}$ on the CI element having a vulnerability matrix $\boldsymbol{V_{ij}}$ will be given by

$$D = max\{S_{ij}\ \boldsymbol{x}\ V_{ij}\}$$

where ***x*** indicates a scalar product between the elements ij of the two matrices.

The value of D will represent the extent of physical damage that is expected to affect the CI element depending on one (or more) of the threat manifestations that will strike it. From the computational point of view, given the definition of the two matrices, the value of D will be obtained by using the ***S*** matrix as a mask over the ***V*** matrix (when ***S*** matrix is null, this will cover the corresponding element of the ***V*** matrix which, in turn, will be disclosed when the ***S*** matrix is non vanishing) and by selecting the maximum among the disclosed ***V*** matrix values.

Table 4 Vulnerability matrix for a specific CI element.

	Vulnerability grade				
Threat name	**1**	**2**	**3**	**4**	**5**
Earthquake (ground acceleration)	0	0	**0.5**	**1**	**1**
Strong Wind	0	**1**	**1**	**1**	**1**
Lightening	0	0	0	**1**	**1**
Heavy snowfall	0	0	0	0	**1**
Ice	0	0	0	0	**1**
Landslide	0	0	0	0	0
Flash flood	0	0	0	0	0
Flooding	0	0	0	**1**	**1**
Mud flows	0	0	0	0	0
Debris avalanches	0	0	0	0	0
Heavy Rain	0	0	0	0	0
Storm surge	0	0	0	0	0
…	0	0	0	0	0

4.2.4.4 B4: Estimation of impacts and consequences

Functional brick **B4** represents the most complex task as it performs a number of different evaluations and will be performed by a tight collaboration between CI operators. As far as its final output, it should provide both impacts on the Infrastructures (in terms of reduction or loss of functionality) and the corresponding impacts on society (citizens, goods, land etc.) (Figure 13). Through the use of the "collaborative platform" boosted by the Secure Information Sharing Platform, CI operators might provide to the DSS managers, in reply to the PHS, the extent of the reduction of functionality of their services as a consequence of the (predicted) physical damage(s) to one (or more) of their components that we define as the Impact Scenario (IS).

Also this matter should be treated confidentially as it contains information which could enhance operator's vulnerability. The CI operator response should be casted in a way that it could be properly inserted into the "system of systems" model available for Impact's evaluation. In this respect, DSS manager will provide a format, which the CI operator should fill in to communicate the extent of the reduction (or loss) of services. This format will be produced on the bases of the "granularity" of the "system of systems" model, which the DSS will be able to deal with. For "granularity" it is intended the level of description with which the dependent system model will be able to describe the regional scenario.

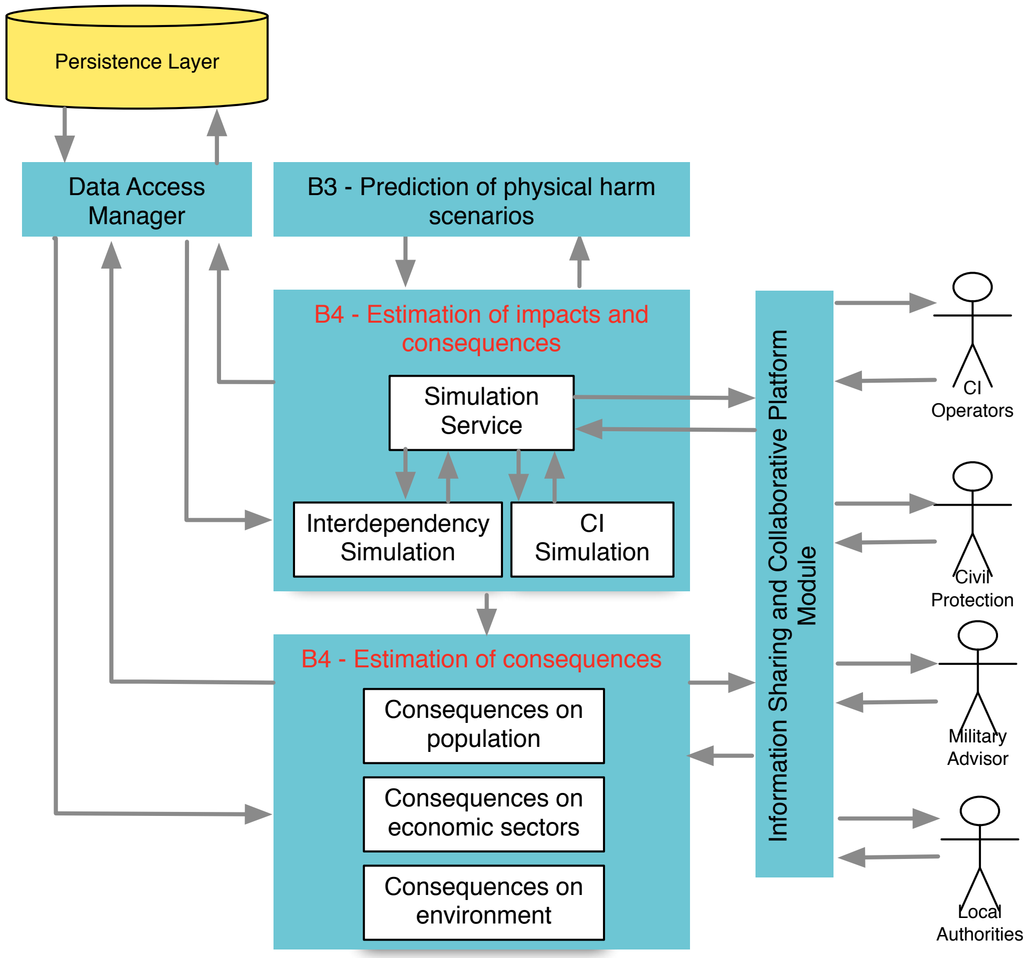

Figure 13: B4 Workflow Diagram: Estimation of impacts and consequences.

Impact on CI. The IS will predict the location and the extent of the harm suffered by the CI element(s) (on a single CI or on multiple CI) whose harm probability will be above a given threshold. This information is rapidly provided to operators of the involved CI. They will be asked to provide, as output of the system input, the reduction (or the loss) of functionality of their infrastructures as a consequence of the element fault. They will provide resulting data by using their simulators, fed with data representing the effective state of their infrastructure at the time when the fault could occur. The DSS should thus receive back, from the single CI operators, the estimated list of impacts. The DSS will thus sum up all the functional impacts on the different CI which will supply the input to an Interdependency *simulator* (e.g. I2Sim) which enables the DSS to provide an assessment of the consequences of multiple impacts on a system of *(inter)dependent* infrastructures. The Interdependency *simulator* will be enabled to perform self-consistent loops allowing the evaluation of the "equilibrium" state resulting from the sum of all impacts reported from the different infrastructures.

To conclude, the CIPRNet DSS will assess the impacts on CI based on two different sources of information:

- CI performance indicators that are related to the behaviour of CI taken individually (e.g. for a power grid, a performance indicator may take into account the overloaded lines against the total number of lines);
- CI service degradation indicators due to interdependency phenomena that are assessed by the Interdependency simulator.

Consequences on society, environment and industrial sectors. After having evaluated the impact scenario on CI, the DSS will evaluate the consequences that the predicted IS produces on different societal activities (industrial and welfare system) and the environment (whenever CI fault could imply environmental damage such as pollution etc.).

The result of this phase is the Consequences Estimate (CE) that will be estimated by crossing the resulting impact on the CI system with information layers of the DB (to estimate, for instance, economical and "welfare" losses etc.). In a sense, Consequences will measure the relevance of a predicted crisis scenario with respect to societal main assets. The four Sectors weighting the impacts of a CI crisis are:

- $\mathbf{S_1}$: Citizens in their daily life (measures: type of population affected by the reduction or loss of services, presence of old aged population and poverty in the affected areas etc.)
- $\mathbf{S_2}$: The industrial sector and its stress (in economic terms, loss of production etc.)
- $\mathbf{S_3}$: The environment and possible damages produced on it (in case of consequences on the environment induced by e.g. release of toxic material etc.).
- $\mathbf{S_4}$: The primary Services (subsequent reduction of services in hospitals, Public Offices, schools, public transportations etc.).

Functional brick **B4** is relevant not only for its technical contents but also as it represents a first practice of a "hybrid" (collaborative) strategy where CIP specialists will directly interact with CI operators, the latter being included in the CIPRNet DSS workflow. This represents a possible way-out for taking over the difficulties in realising, into external CIP "control rooms", accurate CI simulation models, properly fed with real domain data. The "hybrid" scheme should allow operators to comply with the confidentiality of their functional data and the DSS system to be input with impact assessments representative of the real field situation. Secure Information points will be provided to CI operators that could perform this collaborative action with a larger trust and confidence (to comply with industrial rules and needs).

Let us consider an example that shows how the CE is evaluated by the DSS. In Table 5 we listed the considered sectors with the associated factors and a the service delivered by a CI to each class of sector.

Table 5: An example of sectors and relative services provided to specific classes of sectors.

4.2.4.4.1.1 Sector 4.2.4.4.1.2 i	4.2.4.4.1.3 Factor 4.2.4.4.1.4 j	4.2.4.4.1.5 Service 4.2.4.4.1.6 k
4.2.4.4.1.7 Citizens	4.2.4.4.1.8 elderly people (>70)	4.2.4.4.1.9 electricity
4.2.4.4.1.10 Citizens	4.2.4.4.1.11 young people	4.2.4.4.1.12 electricity
4.2.4.4.1.13 Citizens	4.2.4.4.1.14 ill people	4.2.4.4.1.15 electricity
4.2.4.4.1.16 Primary sector	4.2.4.4.1.17 hospitals	4.2.4.4.1.18 telecommunication
4.2.4.4.1.19 Primary sector	4.2.4.4.1.20 hospitals	4.2.4.4.1.21 electricity
4.2.4.4.1.22 Primary sector	4.2.4.4.1.23 schools	4.2.4.4.1.24 electricity
Industrial	4.2.4.4.1.25 Large industrial plants	4.2.4.4.1.26 electricity

For example, let us consider the sector *citizens* and the relative factors. In order to define the CE, we need to define a function that may express the wealth/wellbeing of each specific factor **j** of each sector **i** w.r.t. a variation $\boldsymbol{\Delta Q_k}$ of a generic service **k**. This function depends on the specific sector and service.

We want to calculate the vulnerability of the citizens w.r.t the electricity service i.e. how them can successfully face the event of lack of energy supplied provided by a specific power grid serving a geographical area. We assume that the QoS of the electricity service, denoted with Q, is measured as the duration of an outage (in minutes) that can occur in a specific area that is usually covered by a specific electrical substation. Consequences will be summed up for all people present in that area. This means that we could estimate the total consequences density by evaluating the consequence for each single class of age (e.g. elderly or young people) living in a given.

We want to estimate the variation of wellbeing of the sector *citizens* (sector 1) living in that area due to the loss of electricity. We assume that the DSS has stored a **function of wellbeing** $\boldsymbol{W_{1,j}^{ele}}$ that expresses the variation of wellbeing of the citizens where the index j represents the class of people (grouped by age or people ill or healthy) w.r.t. loss of electricity occurring at time t=0.

Let us suppose that the IS estimates an electrical outage with a duration of $\Delta t^{out} = 60\ min$. and that we have the following figures for the numbers of the different classes of citizens:

$$N_i = 300, N_y = 500, N_e = 100,$$

Hence, we can estimate the variation of wellbeing of citizens considered due to the loss of electricity as:

$$C_1 = 1 - \frac{N_i W_{1,i}^{ele}(t^{out}) + N_y W_{1,y}^{ele}(t^{out}) + N_e W_{1,e}^{ele}(t^{out})}{(N_{ill} + N_{young} + N_{elderly}) W_1^{nominal}}$$

Equation 5: Consequences estimate on citizens due to the loss of electricity.

By looking at Figure 14, we know that: $W_{1,i}^{ele}(60) = 3.5, W_{1,y}^{ele}(60) = 6, W_{1,e}^{ele}(60) = 5$ so that: $C_1 \cong 49\%$. Such a data, provided to decision makers can be valuable to know the possible effects of damages and plans and thus to take appropriate countermeasures.

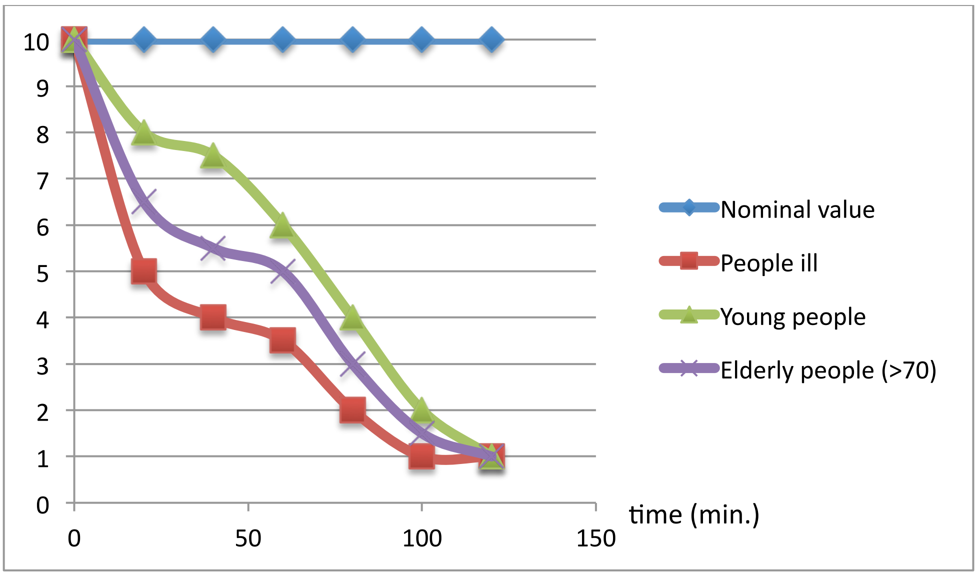

Figure 14: An example of function of wellbeing $\boldsymbol{W_{1,j}^{ele}}$ w.r.t. the loss of electricity.

The input data for this analysis are represented by various information layers (territorial, social-economic) stored within the CIPRNet DB. For example, the vulnerability vector may be defined using the different factors individuated by [34] for the social vulnerability assessment to environmental hazards. The positive/negative vulnerability factors will be reformulated to better represent the social vulnerability of a community with respect to the reduction of QoS Q of specific CI.

4.2.4.5 B5: Support of efficient strategies to cope with crisis scenarios

A system which is able to timely provide information on the probability that a certain course of events might produce damages and, as a consequence of these, loss of services, damage to environment, loss of relevant services for citizen's life and the industrial sectors, can be already ascribed to the class of "Decision Support Systems". These data, in fact, allow emergency responders, CI operators to extract relevant information from Crisis Scenarios on the bases of which they can develop wise and aware mitigation and healing strategies, and set up, even more importantly, prompt preparedness actions.

In the following, we present a possible scenario of use of the DSS in order to clarify how the different actors can rely on the DSS output to improve their crisis mitigation and preparedness strategies. In particular, the example is related to a crisis due to a flash flood event in the city of Rome that has impact on the electrical distribution grid, the telecommunication network, the public transport and the mobility infrastructure. In the scenario, special attention on the flow of data and communications with the electrical distribution grid operator will be paid.

Rome (12.00 am – 12/12/2016)

1. By using nowcasting data, B1 forecasts heavy rain precipitation on a large area of Rome starting from 1.00 pm
2. A Flash Flood is expected (B2) in a more specific area of Rome starting from 2.00 pm. Using the visualization feature of the GEOPlatform framework, it is possible to visualize the forecast on a geographical layer.
3. By using the expected rain precipitation values and the rain vulnerability data of the involved CI physical components, B3 builds the Physical Harms Scenario (PHS, see Figure 15) containing three electrical secondary substations, two telco BTS, and two metro stations that will be in failure with high probability due to the flood event.
4. B4 communicates the PHS to the electrical operator. An iterative procedure (steps a-f) is performed:
    a. The electrical operator emulates the application of the most suitable network reconfiguration procedure (with manual or automatic procedures) in order to mimic the isolation of the flooded substations for restoring the electrical network as much as possible;
    b. The electrical operator accesses the DSS to feed the expected switch off time of each electrical substation;
    c. The electrical operator alerts its personnel resources i.e., emergency crew teams to check on-situ the availability of the remote control in the substation (the alert will be useful for allowing, if the event will occur) the system restoration in the shortest possible time) and to provide and install service backup systems on the network, such as UPS, to feed the unavailable substations.;
    d. B4 using specific procedures (based on I2Sim) and the information coming from other operators may loop back to the electrical operator to communicate that some resources may be unavailable (e.g. a UPS can not be installed in 1 hour time, as estimated by the electrical operator, due to the traffic jam and the

unavailability of the remote control on some substations) and that the time to perform manual operations on the network will be significantly higher due to traffic jams;

e. The electrical operator uses this information to refine its network reconfiguration procedure and to compute the switch off time of the substations.

5. B4 applies the Consequence Analysis to the resulting Impact Scenario (IS). And produces a Consequence Estimate (CE).
6. B5 sends the Risk Assessment Report to all CI operators related to the Impact scenario. If the overall *risk value* associated to this crisis scenario is high (e.g., an hospital can be severely impacted by the loss of QoS of the different networks).
   a. *Mitigation action*: the electrical operator can use this information to mitigate the risk. For example, it can decide to dislocate emergency crew teams/UPS near the expected mostly impacted area.

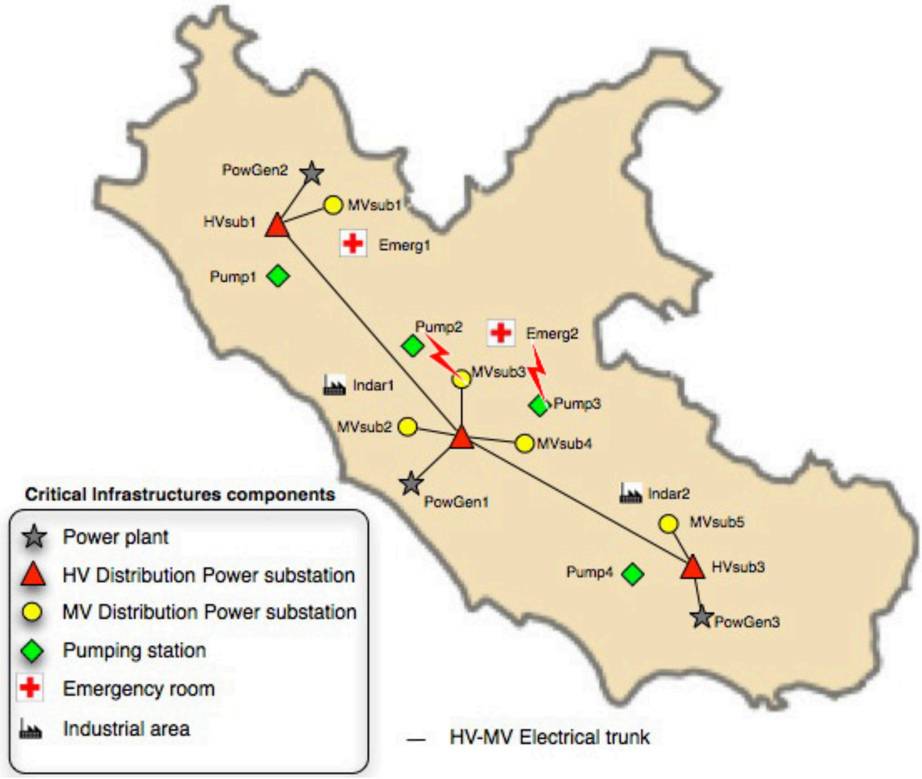

Figure 15: An example of an Physical Harms Scenario in the Lazio region (Italy).

Nevertheless, DSS could also, in principle, develop optimized strategies to solve critical situations; these strategies could be prompted to the operator's attention, serving as a basis to develop real actions, to take over critical situations. This task could encompass the following (explanatory i.e. incomplete) list of cases:

- sequences of actions to be performed to efficiently reactivate services after outages (i.e. electrical islanding, set up of viable communication channels for supporting reactivation of SCADA systems after telco outages etc.)
- optimal traffic diversion to bypass critically congested areas upon accidents or physical damages of the infrastructures (upon flooding, earthquakes etc.)

The possibility of designing such a powerful system, other than the complexity of the problems, which, in most cases, can be brought back to an optimization problem with an extended solution space, is inhibited by the fact that much information (needed to restrain the solution space of the optimization problem) is not available. A typical case for understanding this limitation is provided by the classical problem of load shedding: in case of needs, electrical operators can disconnect lines when demand becomes larger than the supply. To perform this strategy, electrical companies ensure to have a number of customers whose load could be occasionally disconnected. Thus, when a load shedding strategy must be designed, this information should be at hand. In many cases, however, the specific customers with a similar consumer profile are not known outside the electrical company, as this information is treated very confidentially, having a specific commercial value. For this reason, the design of an optimized load shedding activity by a third party (like the CIPRNET DSS manager) cannot be performed, due to the absence of required information.

To implement this strategy, we propose to install in the CIPRNET DSS only some "***Decision List of Actions***" which could be reasonably provided to crisis managers in the cases where the DSS contains all the essential information needed to envisage a possible crisis solution. In particular, we will refer to the case where communication infrastructures (roads and motorways, railways etc.) are involved. In case of accidents or natural hazards which serious damages on these infrastructures, the system will be able to redesign the traffic structures. Two cases will be considered:

(a) when a specific event like an earthquake or a landslide will affect the infrastructure. The DSS will acquire results from a specific traffic simulator of the involved area (at different traffic density values) and will indicate (for a general Origin/Destination O/D matrix) the optimized paths to be encouraged
(b) same as in the previous case but with specific constraints to the traffic induced by the presence of a nearby catastrophic event which, imposing a strong asymmetry to the displacement needs (asymmetry of the O/D matrices) will deserve different strategies to be re-optimized.

For these two cases, the DSS will provide operators with a detailed map of optimized paths for ensuring the fastest and most efficient displacements in crisis operations.

4.3 Simulators

Aside to the "real-time" DSS (i.e. the application which will run operationally and be fed with real-time data, the project foresees the activation of "off-line" DSS which will be usable for creating and solving **synthetic crisis scenarios**. A synthetic crisis scenario is produced by an "event simulator" which produces a synthetic event (i.e. an earthquake, an abundant precipitation, a strong wind or an heat wave etc.) in a way to stress some area to be analysed in terms of vulnerability of its asset, resilience of its infrastructures, efficacy of its preparedness and emergency procedures.
From the technical point of view, a synthetic event simulator replaces DSS B1; this application produces as output an information layer identical (in its technical form and format) to that coming from a "true" forecast or from a sensor system. Two simulators have been designed:

(1) an earthquake simulator. This system is able to produce a synthetic earthquake with user-defined characteristics (i.e. position of the epicentre and its magnitude); starting from the availability of these data from the user, the application elaborates the corresponding shake maps, in the same way the system would have elaborated starting from a true event detection. After this first task, the Simulator reconnects to the usual DSS workflow, producing the complete Risk Analysis predicted after the eventual occurrence of the described synthetic event.
(2) An abundant precipitation simulator. Also in this case, the application produces an information layer (similar to that coming out from the now-casting prediction) with characteristics, which can be user-defined: position of the precipitation, its extension (in terms of the area affected), and its abundance (in terms of expected mm of rain per hour). The system also provides the possibility of distributing the precipitation in the

given area with a abundance function position-dependent (i.e. not all the points of the selected area will be affected by the same rain intensity).

Simulators have been designed and will be set in place to answer to specific needs:

(a) the possibility of simulating "rare" events (i.e. earthquakes);
(b) starting from previous events, the simulator could implement similar, but stronger, events, enabling to determine eventual "critical" thresholds which might be then used as Alerting threshold when a similar event would be really predicted;
(c) Making stress test of existing infrastructures;
(d) As training systems for Emergency Managers and CI operators.

4.4 Implementation

In this section we will provide two scenarios that will allow introducing the technology development of the DSS. The two scenarios consider an instance of a local DSS Cluster allotted to the monitoring of the Lazio region (Italy). The following infrastructures will be considered within the scenarios:

- Three **water distribution networks,** three **hospitals;** three industrial **plants;**
- Three **Power plants**, three **HV Transmission Power grid** and three **MV Transmission Power grid** supply power to the water distribution networks, the hospitals the and industries;[3]

For each considered infrastructure, we will model only a limited subset consisting of the CI elements that are responsible for the delivery of services to other infrastructures.

In order to assess the impact of possible failures due to natural hazards and (inter)dependency phenomena, it is necessary to have the physical models of all the infrastructures and to analyse all the connections among them (Figure 16).

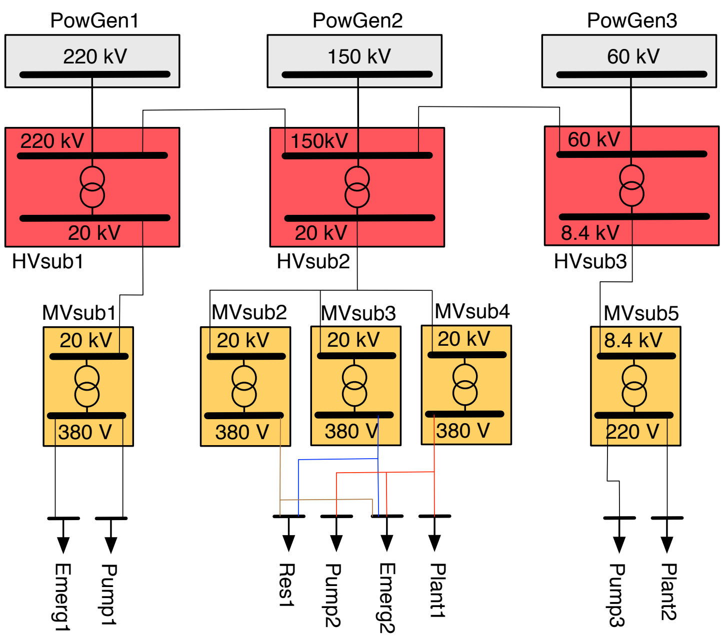

Figure 16: Power grid model.

[3]. In a realistic scenario, the three power sub-models here presented, should exhibit a connected topology i.e. the three sub-networks should be considered connected allowing for reconfiguration operations of the Power operators.

The latter task may be impracticable to fulfil for a big area (e.g. the Lazio region). That is the reason why the DSS will employ aggregated models of the CI of a specified area. In this scenario, we modelled the interdependencies between the CI through the I2Sim model (Figure 17).

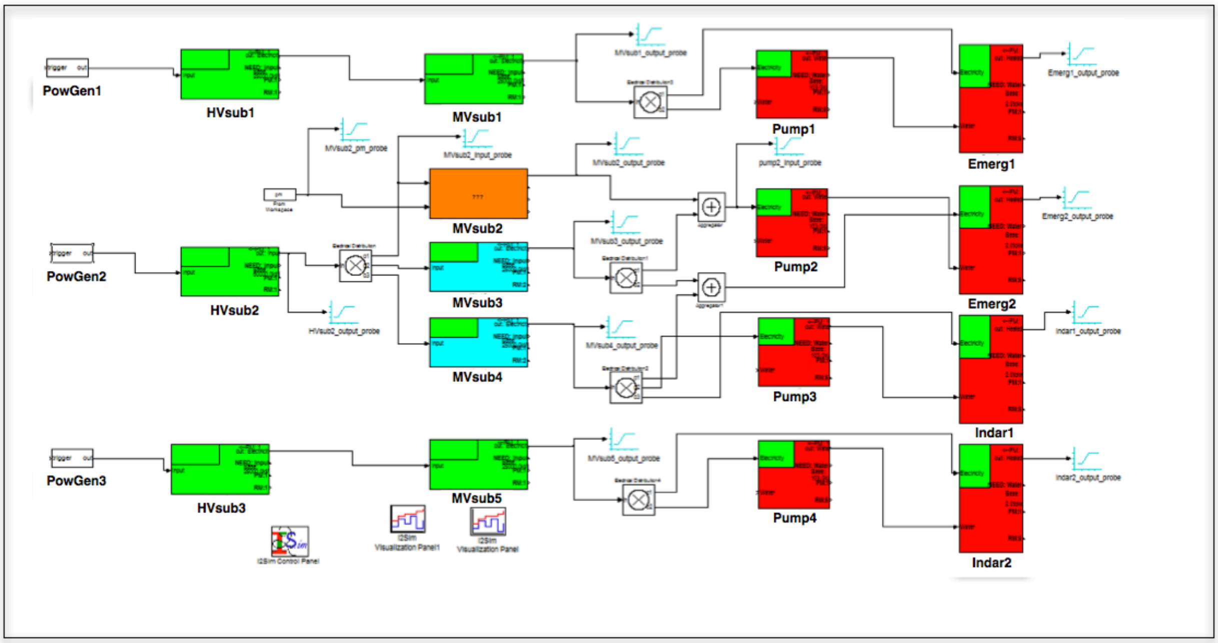

Figure 17: I2Sim model.

4.4.1 Unpredictable events: the Earthquake Workflow

Figure 18 shows the logical workflow implemented by the Risk Assessment Workflow Manager within the Italian DSS to assess the impact and the consequences of unpredictable events as earthquakes. The DSS acquires (each 5 minutes) INGV data representing earthquake data (i.e. epicentre coordinates and magnitude) coming from the INGV ISIDE sensor network. In this simple workflow, data are stored within the EISAC-DB as they are related to the entire Italian territory. However, the cluster and pluggable architecture of DSS allow the development of *ad-hoc* data acquisition procedures to acquire data directly from seismic monitoring sensor networks as in the case of a Local DSS Cluster allotted to a highly seismic risk area.

The Risk Map Viewer, which has been implemented using the GeoPlatform framework (see Annex 3), can be used to visualize the ISIDE data as shown in [36]. GeoPlatform allows the configuration of a parameter to establish the data refresh interval.

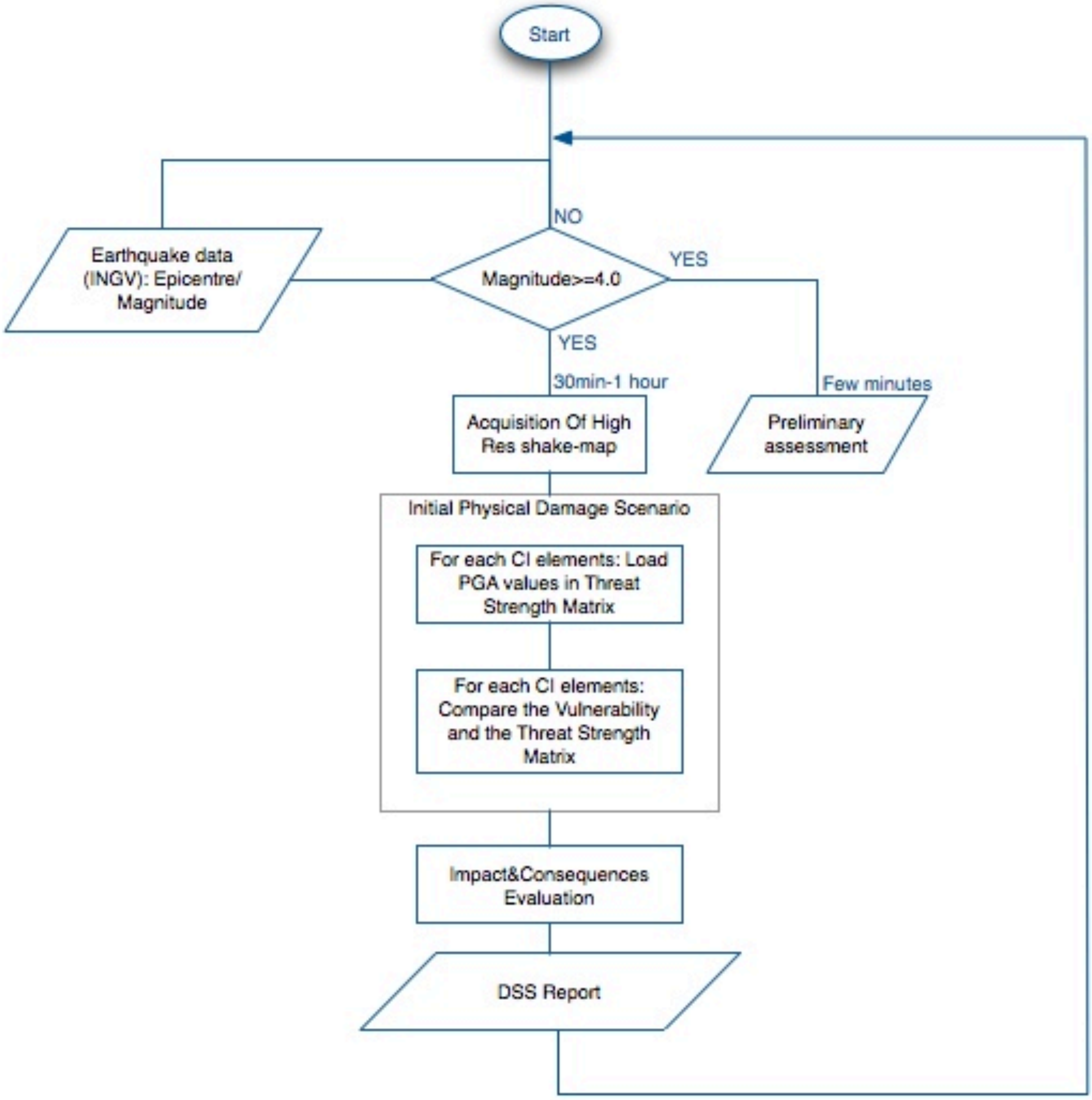

Figure 18: The Earthquake workflow

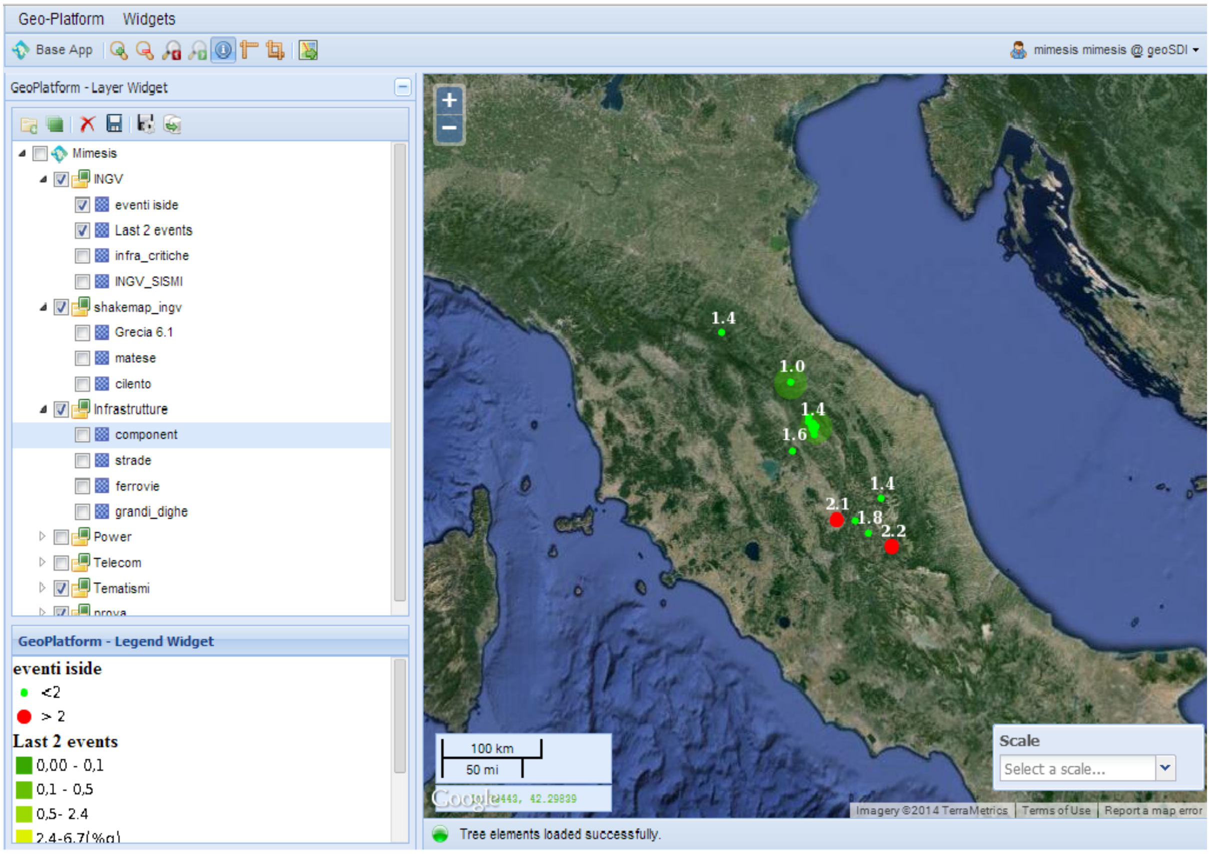

Figure 19: The DSS Risk Map Viewer displaying the ISIDE INGV data

Within the B2 functional brick the DSS exploits simplified models to compute the maps of ground shaking (the so called shake-maps) related to the two last reported events (these shake-maps are displayed as green filled circle around the points representing the seismic events, see Figure 19). In turn, these simplified shake-maps are used to have a preliminary assessment for events of a magnitude grater and or equal to 4 on the Richter scale. In parallel to the preliminary assessment the DSS waits for the detailed and high-resolution INGV shake-maps that, in general, are released 30min-1 hour after each seismic event. The DSS uses these shake-maps to run the complete Risk Assessment Workflow.

The Ground Peak Acceleration (GPA) values contained in the high resolution shake-maps are used to fill the rows related to the earthquake threat of the ***threat strength matrix*** of each CI components insisting on the area impacted by the seismic event. For instance, the threat strength matrix of a telecommunication router (R_{tlc}^{i}) placed on the top floor of a building can indicated that that component is impacted by a ground acceleration of a value between 0.05g and 0.15g (see 4.2.4.2):

Table 6: The threat strength matrix of a telecommunication router.

Threat	**1**	**2**	**3**	**4**	**5**
Earthquake (ground acceleration)	0	1	0	0	0
…	..	..	..	..	..

Within the B3 functional brick the DSS will build the PHS using the vulnerability matrix of each CI components. For example, for the telecommunication router (R_{tlc}^{i}) the Local DB may contain the vulnerability matrix as in **Table 7**.

Table 7: The vulnerability matrix of a telecommunication router.

Vulnerability	1	2	3	4	5
Earthquake (ground acceleration)	0	0	0.5	1	1
..	..	..	..	..	..

In the example the specific router component will not be affected by the seismic event. In general, there will be CI elements that will result in failure as the product of the threat strength matrix and the vulnerability matrix will be equal to 1.

For instance, let us suppose that the earthquake workflow is performed within the Local DSS Cluster related to the Lazio region (Italy) and that the ISIDE indicates a seismic event of magnitude 5 near Rome, the preliminary assessment (i.e. applying the simplified shake-map) can result in a *preliminary* PHS as in Figure 20. The preliminary PHS will be refined using the INGV detailed earthquake event shake-map.

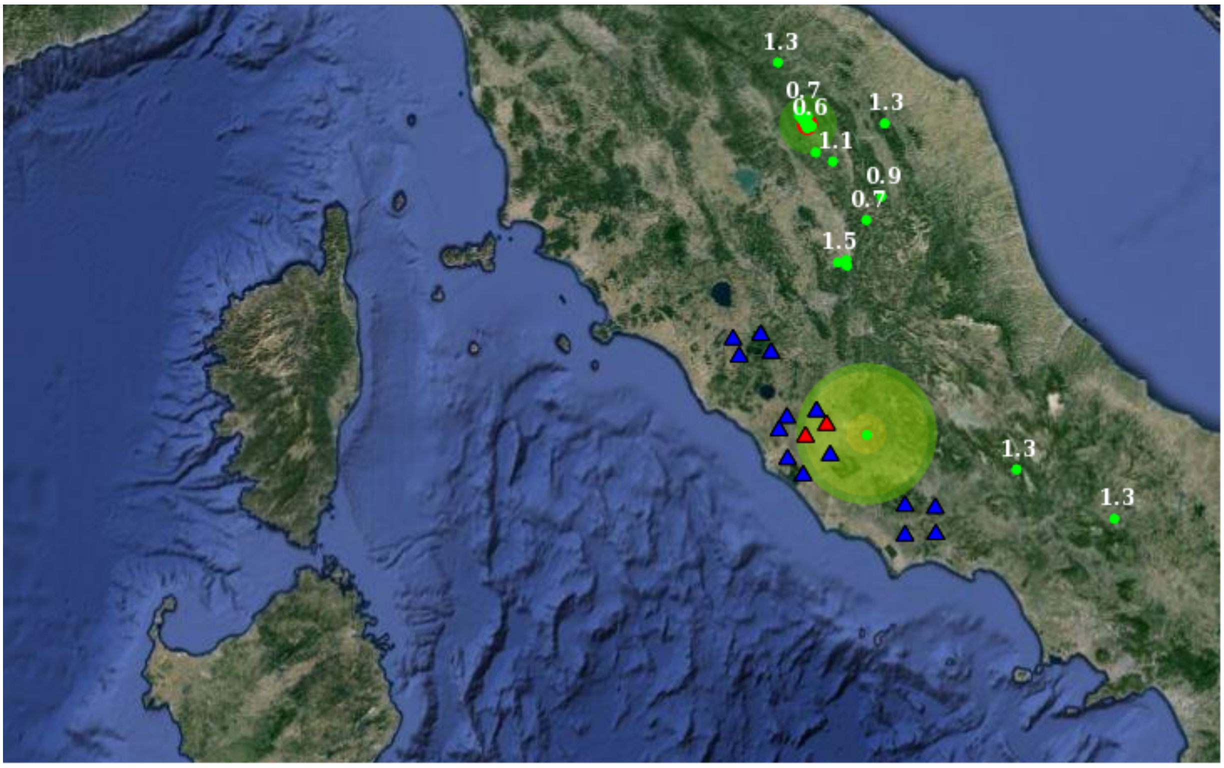

Figure 20: Rome earthquake preliminary Physical Harms Scenario.

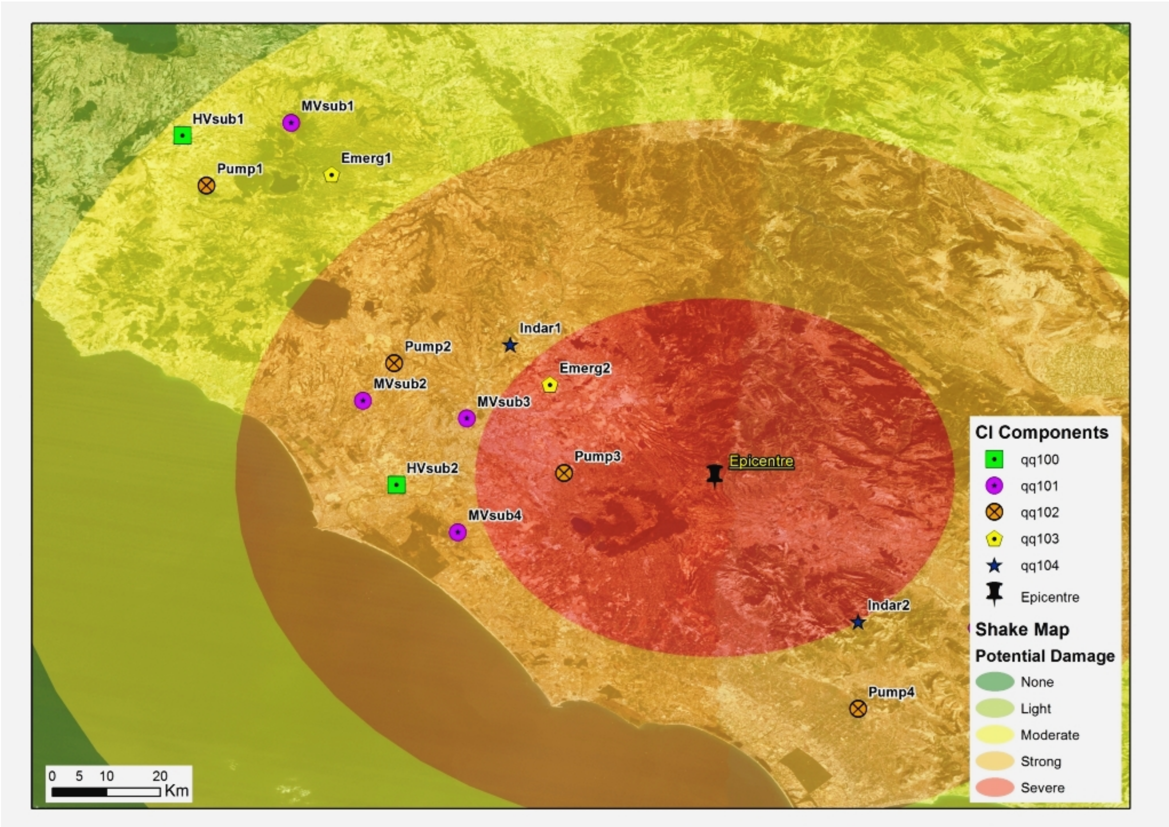

Figure 21: Rome earthquake event detailed shake-map.

The GPA values contained in the detailed shake-maps are used to configure the CI components ***threat strength matrix.*** Comparing the CI components threat strength matrix with their vulnerability matrix it will be possible to build the PHS as shown in Figure 15. In this example, the CI elements *Pump3* and *MVsub2* are considered to be in failure state.

The information about the possible loss of components **MVsub2** and **Pump3** (visible in Figure 15) is provided using a secure collaborative platform to all the CI operators. The CI operators will be required to provide the possible reduction of functionality of the components of their infrastructure due to the "possible" loss of MVsub2 component for the electrical and Pump3 for the water distribution network respectively. For example, the Power operator[4] will be required to provide the reduction of functionality of the following components: **MVsub1, MVsub2, MVsub3, MVsub4, MVsub5**.

Then, in order to provide an assessment of the consequences of multiple impacts on a system of *(inter)dependent* infrastructures, the CI operators information will be used to properly configure the I2Sim model (Figure 17), embedding all the dependencies (identified during the DSS design phase), will be executed to calculate the "equilibrium" state resulting from the sum of all impacts reported from the different infrastructures.

The result of the I2Sim simulation is stored in the Local database; in particular, the **output** table is filled with the possible evolution over time of the physical quantities assessed by I2Sim (e.g. the evolution over time of the water rate provided by **Pump1** or the power generated by **MVsub3**, the number of patients treated by **Emerg2**). Such information is then provided to the Civil Protection operators as a support for their emergency plans and to infrastructure operators who may refine their actions.

[4]We suppose that the same Power operator is responsible for all the MV components.

4.4.2 Predictable events: the Weather Forecast Workflow

The Weather Forecast Workflow shown in Figure 22 summarizes the steps that will be executed by the by the Risk Assessment Workflow Manager in order to *forecast* threats that can harm CI components. In particular, the presented workflow is valid for all threats that can be predicted using the weather forecast data. The workflow shown in Figure 22 is a simplification of the actual workflows that will be implemented for the different threats. For instance, a DSS cluster can implement an ad hoc workflow in order to forecast landslides. In this case we would need to *plugin* into our DSS cluster different models in order to be able to forecast the different typology of landslides that, in general, may be triggered by different processes (precipitation, earthquake, human induced) as well as different databases to correlate the different triggering natural hazards with the past landslide events. In general, the DSS pluggable architecture will allow to plugin in the workflow the already existent models and data proposed by the experts for the specific threats and in the specific area of interest in order to obtain DSS Cluster as effective as possible. In the following, a general DSS workflow will be showed. In particular we will refer to the DSS Cluster allotted for the Lazio Region.

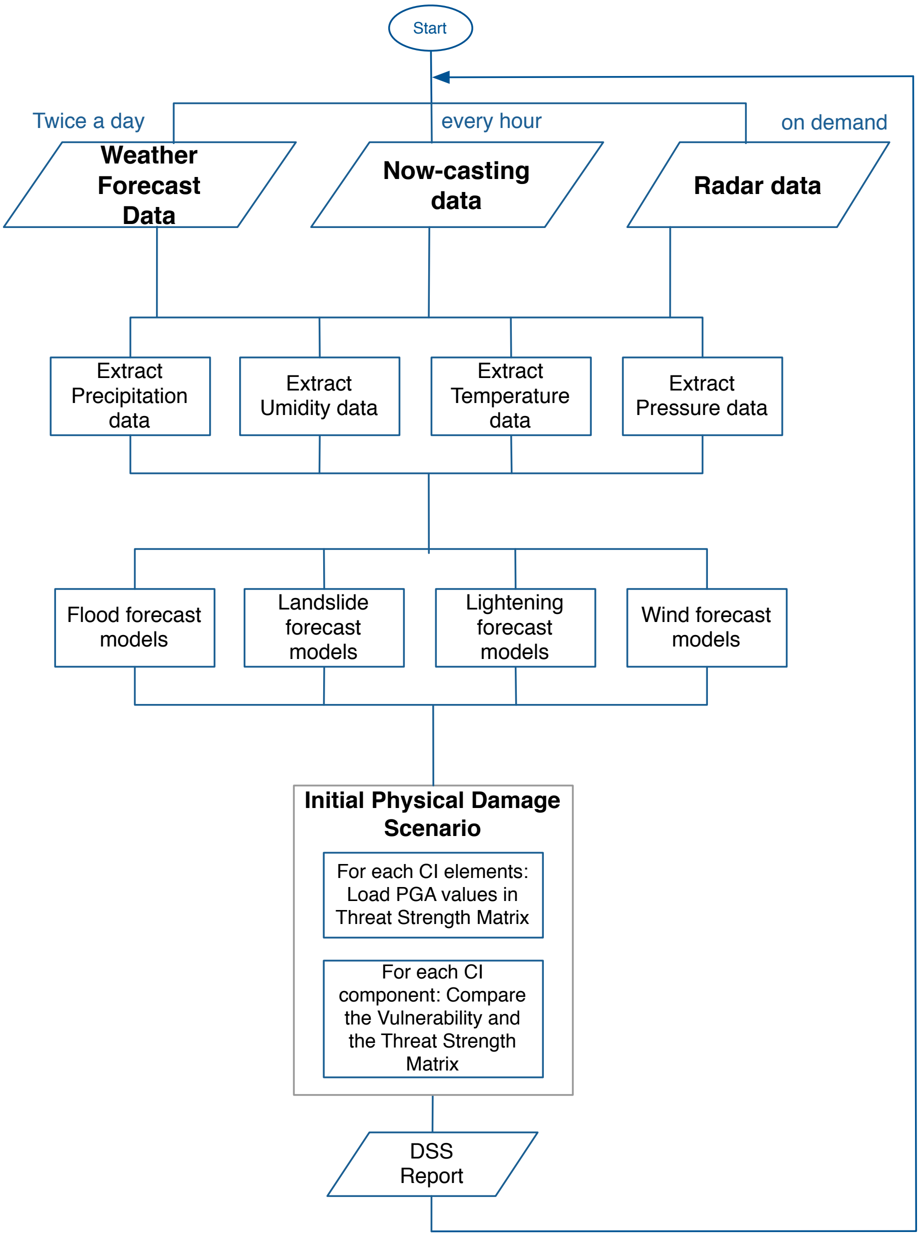

Figure 22: Weather Forecast Workflow diagram.

In order to describe the workflow of Figure 22 we will refer to the action timeline as showed in Figure 23.

Twice a day the DSS cluster acquires the weather forecast data from the national/regional agency responsible of this service (e.g., the Meteorological Service of Aeronautica Militare in Italy). Let's suppose that the DSS acquire the weather forecast data for the next 12 hours at 00:00 and 12:00 of each day, whilst the weather forecast data for the next 24 hours once a day at the 00:00. The DSS extract from the weather forecast data different information:

- Temperature
- Wind strength and direction
- Pressure
- Humidity
- Sea state
- Precipitation type

In some cases it will be possible to acquire high-resolution data related to specific area. In this case the prediction of threats will be more accurate.

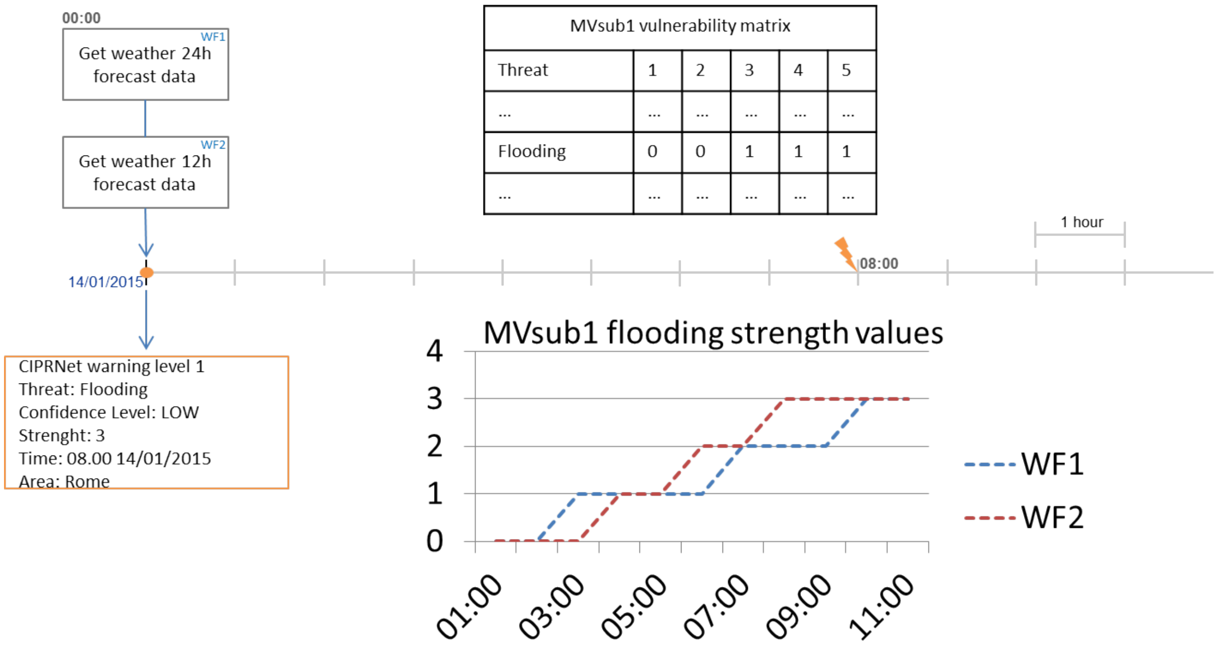

Figure 23: Forecasting a flooding from weather forecast data.

Using hydrological and hydraulic models of the Tiber river the DSS will produce values the flooding strength matrix of each CI components. For example, in Figure 23 we can see the evolution of the flooding strength values for a CI component of the electrical distribution network named MVsub1 and the related vulnerability matrix. Using this information and following the procedure described in section 4.2.4.3, the 12h weather forecast data allow the DSS to emanate a warning of level 1 related to a possible flooding event at 8:00 am. In general, the warnings that are emanated using weather forecast data (both 12 and 24 hours) are of level 1 that indicates that the confidence of the prediction is *low*. In order to increment the confidence in the prediction, the DSS acquires each hour now-casting data from local agencies and the values of monitoring sensor networks (as, for example, the pluviometric sensor network of the Tiber river). The Figure 24 shows how now-casting data and monitoring sensor network data are used to refine the forecast of a flooding event. For example, these data allow decreasing the warning level for the MVSub1 CI component. Vice versa, the DSS emanates a warning of level 2 (high level of confidence) for the MVSub2 CI component. The DSS may use earth observation data (e.g. using the Copernicus (previously GMES) Emergency Management Service data) to monitor an on-going extreme natural hazard as for example a flooding.

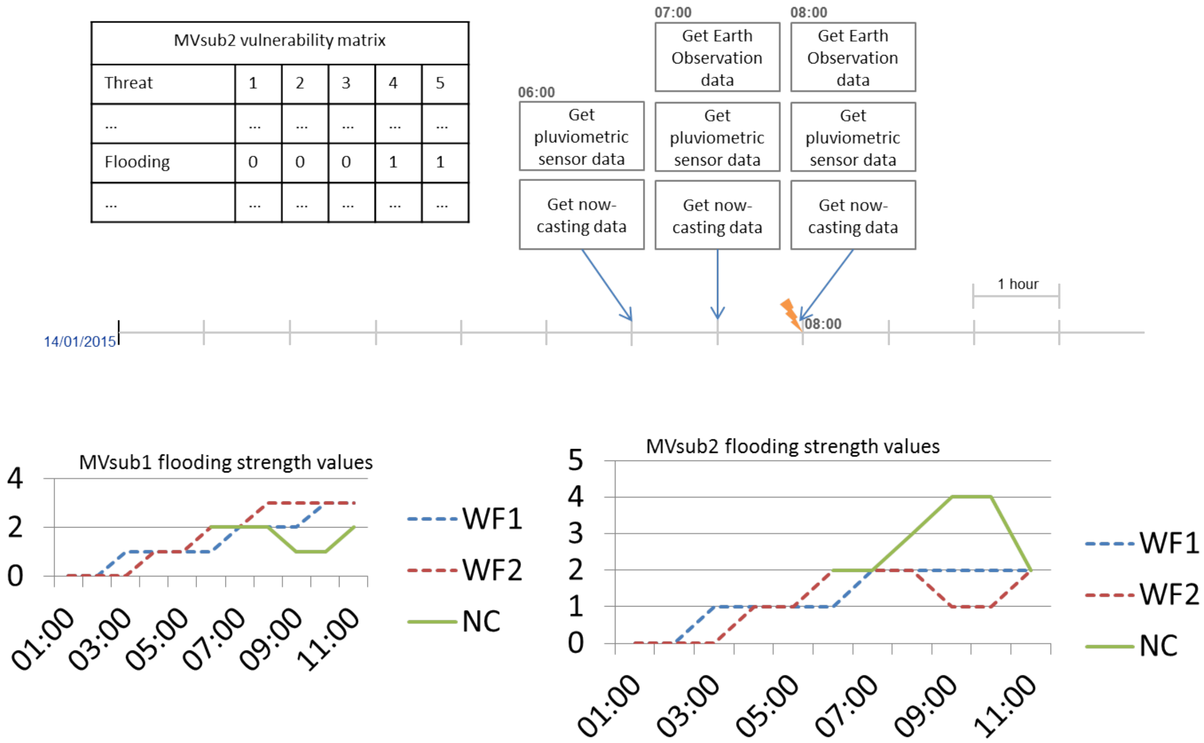

Figure 24: Flooding forecast refinement through now-casting data

5 Conclusion

This document describes the functional and non-functional requirements of the CIPRNet DSS platform, its architecture and the underlying Risk Assessment mathematical framework and workflow. The functional and non-functional requirements represent a further refinement and specification of the general requirement presented in [2]. The architectural principles presented in the document take under consideration both organizational and technological aspects of the DSS platform to be implemented. The main feature of the proposed architecture is the *pluggable architectural concept*. Indeed, the platform will need to plug-in different sources of data, models, simulators, algorithms to consider the specific needs and requirements of the different area of a national territory. In this way, in the future, for each EU member state it will be possible to run customized versions of the general DSS Risk Assessment workflow in order to provide the best risk assessment procedures that will consider all specificities of a member state region and/or area.

The Risk Assessment workflow consists of five functionalities or *functional bricks (Bi)* that are: B1) Monitoring of Natural phenomena, B2) Prediction of natural disasters and event detection, B3) Prediction of physical harms scenarios, B4) Estimation of impacts and consequences B5) Support of efficient strategies to cope with crisis scenarios. In section “Implementation” (4.4), two scenarios have been proposed on order to explain the different methodologies, procedures and technologies involved in each function brick Bi. The first scenario is related to the Risk Assessment workflow for *unpredictable events* (e.g., earthquakes) whilst the second describes the *weather forecast workflow* (i.e., valid for all threats that can be predicted using the weather forecast data).

The Simulator applications are integral parts of the DSS. They allow defining synthetic events that, analogously to real events, trigger the whole chain of Risk Analysis of the DSS. Synthetic events are built to allow the system to deal with rare events (i.e. earthquakes, unusually strong meteorological events etc.) that allow stressing the areas under analysis and providing a useful tool for training Emergency managers and CI operators. In addition, specific capabilities providing forecasts of meteo-climatological and flood events (described in [38]) will also be integrated in the DSS together with federated MS&A tools (described in [39]).

The DSS through the Threat forecasting, visualization and consequence analysis capabilities and implemented by the presented functional blocks, can improve the management options for mitigating the risks for emergency managers by estimating the consequences of specific contingency plans provided by the CI operators in order to find the actions that can reduce the risks on the specific assets.

6 References

[1] FP7 CIPRNet Project, Deliverable 4.7 “Detailed implementation plan of EISAC”.

[2] Hämmerli, B.M., Renda, A.: *Protecting Critical Infrastructure in the EU*, CEPS Task Force Report, Centre for European Policy Studies, Brussels, March 2011 (ISBN: 978-94-6138-070-8)

[3] FP7 CIPRNet Project, Deliverable 5.1 “Formal requirements specification”.

[4] FP7 CIPRNet Project, Deliverable 6.4 “Implementation of the integrated CIP MS&A based ‘what if’ analysis”.

[5] FP7 CIPRNet Project, Deliverable 7.2 “Database of the DSS with consequence analysis”.

[6] FP7 CIPRNet Project, Deliverable 5.3 “Realisation of “ask the expert” function”.

[7] FP7 CIPRNet Project, Deliverable 8.4 “Publicly announced CIPedia”.

[8] J. R. Marti, J. A. Hollman, C. Ventura, and J. Jatskevich, “Dynamic recovery of critical infrastructures: real-time temporal coordination,” International Journal of Critical Infrastructures, vol. 4, no. 1, pp. 17– 31, 2008.

[9] FP7 CIPRNet Project, Deliverable 6.3 “Federate CI models”.

[10] EU FP7 Project DIESIS Fraunhofer, Deliverable D4.2a “Proof of concept” (2010).

[11] S. L. Cutter, “Vulnerability to environmental hazards”, *Progress in Human Geography* 20,4 (1996) pp.529-539.

[12] M. Khouj, C. Lopez, S. Sarkaria, and J. R. Martí, Disaster management in real time simulation using machine learning. CCECE, pp. 1507-1510. IEEE, (2011).

[13] Andrienko, N., Andrienko, G.: Intelligent Visualization and Information Presentation for Civil Crisis Management. Transaction in GIS, 11, 889-909 (2007).

[14] Charvat, K., Kubicek, P., Talhofer, V., Konecny M., Jezek, J. Spatial Data Infrastructure and geo-visualization in emergency management. Resilience of Cities to Terrorist and other Threats, pp. 443- 473. Springer Science + Business Media B.V. (2008).

[15] Pollino, M., Fattoruso, G., Della Rocca, A.B., La Porta, L., Lo Curzio, S., Arolchi, A., James, V., Pascale, C. An Open Source GIS System for Earthquake Early Warning and Post-Event Emergency Management. Lecture Notes in Computer Science, Vol. 6783, pp. 376-391. Springer, Berlin/Heidelberg (2011).

[16] SIT_MEW (Italian acronym for: Sistema integrato di telecomunicazioni a larga banda per la gestione del territorio e delle emergenze in caso di calamità naturali comprensivo di Metodologie di Early Warning) is a R&D project co-funded by Italian Ministry of Education, Universities and Research (MIUR) in the framework of the “GrandiProgettiStrategici” (GPS) national program.

[17] Pollino, M., Fattoruso, G., La Porta, L., Della Rocca, A.B, James, V.: Collaborative Open Source Geospatial Tools and Maps Supporting the Response Planning to Disastrous Earthquake Events. Future Internet, 4, 451-468 (2012).

[18] INGV, Italian National Institute of Geophysics and Volcanology. http://www.ingv.it, Last accessed 04.07.2014

[19] OGC: the Open Geospatial Consortium, http://www.opengeospatial.org, Last accessed 06.03.2014

[20] SPEE, http://www.spee.it, Last accessed 04.07.2014

[21] Lagomarsino, S., Giovinazzi, S. Macroseismic and mechanical models for the vulnerability and damage assessment of current buildings. Bull. Earthq. Eng., 4, 415-443 (2006).

[22] ISTAT, Italian National Institute of Statistics. http://www.istat.it, Last accessed 04.07.2014

[23] CNR IMAA, http://www.imaa.cnr.it/index.php?lang=en, Last accessed 04.07.2014

[24] GeoSDI, http://www.geosdi.org/index.php/en, Last accessed 04.07.2014

[25] INSPIRE, http://inspire.ec.europa.eu, Last accessed 04.07.2014

[26] ISPRA, Italian Institute for Environmental Protection and Research. SINANET is the ISPRA environmental and territorial data repository, http://www.sinanet.isprambiente.it/it, Last accessed 04.07.2014

[27] EU FP7 DIESIS Project, Deliverable D4.1b, http://www.diesis-project.eu/include/Documents/DIESIS_Final_Architectural_Design.pdf, Last accessed 04.07.2014

[28] GeoServer, http://geoserver.org/display/GEOS/Welcome, Last accessed 04.07.2014

[29] D. Power. Decision Support Systems: concepts and resources. Westport, USA. Quorum Books, 2002.

[30] Power, D.J. A Brief History of Decision Support Systems. DSSResources.COM, available online at http://dssresources.com/history/dsshistoryv28.html, Last accessed 12.08.2013

[31] FP7 CIPRNet Project, Deliverable 7.1 FINAL version "Decision Support System with consequence analysis".

[32] Sutton, D., Cappelli M., Das-Purkayastha A., Bologna S., De Nicola A., Rosato V., Garwood A., Harrison J., Pollard D., Skellorn W. (2011). NEISAS Dissemination – Final Report.

[33] Sutton, D., Harrison, J., Bologna, S., & Rosato, V. (2013). *The Contribution of NEISAS to EP3R*. In Critical I

[34] The GEOSDI platform, http://www.geosdi.org, Last accessed 06.03.2014

[35] The Geo-Platform, http://code.google.com/p/geo-platform, Last accessed 06.03.2014

[36] ISIDE - Italian Seismic Instrumental and parametric DatabasE, http://iside.rm.ingv.it, Last accessed 04.07.2014

[37] Cutter, S. L., Boruff, B. J. and Shirley, W. L. (2003), Social Vulnerability to Environmental Hazards. Social Science Quarterly, 84: 242–261. doi: 10.1111/1540-6237.8402002.

[38] FP7 CIPRNet Project, Deliverable 7.5 "Integration of meteo-climatological simulators, flood forecasts, earthquakes data and analysis tool".

[39] FP7 CIPRNet Project, Deliverable 7.6 "Interface to the technical demonstrator for federated CIP MS&A".

7 Annex 1 – A possible implementation of I-EISAC

In this Annex, we present EISAC and in particular we will discuss a possible organisation and management organisation of the **Italian node (I-EISAC) of the** pan-European networked organisation named EISAC (Figure 25)**.** In particular, we will see how the DSS will be contextualised within the Italian national emergency and crisis management systems.

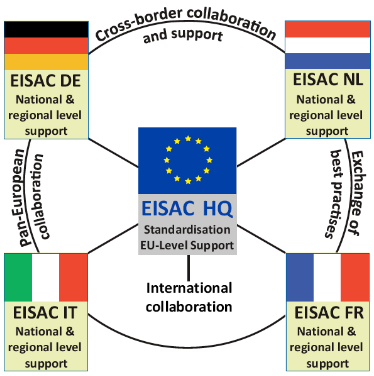

Figure 25: Vision of EISAC virtual centre of competence and expertise in CIP.

As described in Figure 26, the **CIPRNet DSS** may be connected to the **Italian Dept. of Civil Protection** (which is under the control of the **Presidency of the Council of Ministers**) and to **Regional Civil Protection** centres to provide:

- **Assessment of risk of CI** (24 hours a day during both **alert** and **non-alert** conditions) to assess the dynamic risk which they are subject in relation to weather-climatological and geophysical forecast (through the use of high resolution forecast (<1 km), nowcasting and Remote Sensing);
- **Assessment of impacts on the population and the environment** induced by the loss of components/services of one (or more) dependent CI;
- **Assessment of risk of CI in "what-if" scenarios** in order to verify (through synthetic stress tests) the components/services of CI with high vulnerability;
- **Support** during the preparation of strategies for mitigation of impacts also during the event handling of the crisis;
- **Support to regional and other local authorities** in the preparation of risk plans relative to specific high risk or high vulnerability areas.

The CIPRNet DSS may employ a communication channel with CI operators to get information about the state of each CI. Such information will be needed to produce an assessment of the risk of failure for CI components threatened by natural hazards.

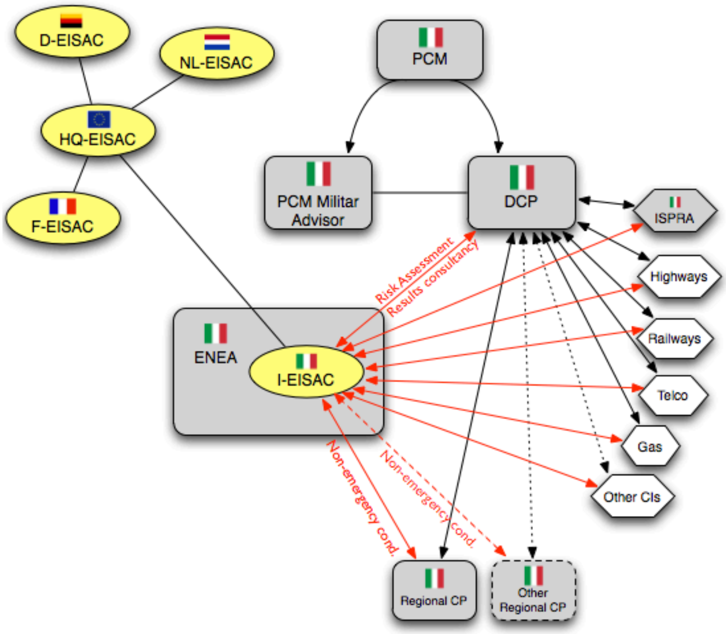

Figure 26: Italian governance for Emergency Management: the role of EISAC. CP: Civil Protection; PCM: Presidency of the Council of Ministers; DCP: Dept. of Civil Protection operating centre.

8 Annex 2 – A Secure Information and Exchange platform

This Annex describes the Secure Information Exchange platform named NEISAS (National and European Information Sharing and Alerting System), that is, the result of ENEA collaboration within a previous EU DG-HOME project. The NEISAS platform may be used within the DSS collaborative platform as a means to share sensitive information among CI operators and decision makers to avoid malicious attacks. The decision on the product that will be used to this aim will be discussed with the partners and taken at a later stage of the project. This Annex, and the description of the NEISAS platform, should be intended as being the setting of the technological requirement that the solution that will be adopted should display.

To the aim of realizing a web-based platform enabling secure information sharing among groups of CI operators (concerning CI attacks, vulnerability of technological elements, Quality of their Services etc.), ENEA has developed, within the NEISAS project [28] with the objective of increasing security in the information sharing critical information infrastructure security and resilience in order to support healing and mitigation strategies upon faults and to reduce risks of large cascading effects. To such purpose, NEISAS developed a framework consisting of a model and a platform for information sharing. In particular, the framework ensures data integrity, confidentiality (anonymity), security and service availability.

The NEISAS Framework is based on a National and EU information-sharing model (Figure 27). In particular, the NEISAS Platform for Trusted Information Sharing interprets EU requirements from certain (UK, NE) member states. It is compliant to IEC 27010 standards. It allows national and cross-border information sharing built upon robust, state-of-the-art technology. It is flexible and adaptable to several Critical Infrastructure domains.

NEISAS has been built starting from the idea that CI operators, and society in general, have more to lose if they do not share information than if they do. Furthermore, they have an added value in gaining access to information that CI players would otherwise not have access to; in being alerted to threats and potential vulnerabilities experienced by others and therefore being better prepared themselves; in learning from others and adopting best practices; and, finally, in tackling security issues collectively so as to generate a ‘public good’ rather than handling risks privately.

The NEISAS information-sharing model guarantees information sharing by means of “Trust Circles”. A “Trust Circle” consists in a group of people exchanging information using the NEISAS platform. Users with trustmaster and member roles compose it. The former role has management functionalities, as the ability to define advanced sharing rules between different trust circles, which are not enabled to the latter. The trustmaster is seen as a trusted coordinator and manager of a trusted information-sharing group. She/he is a member of a government agency or a trusted member elected as a representative of the group.

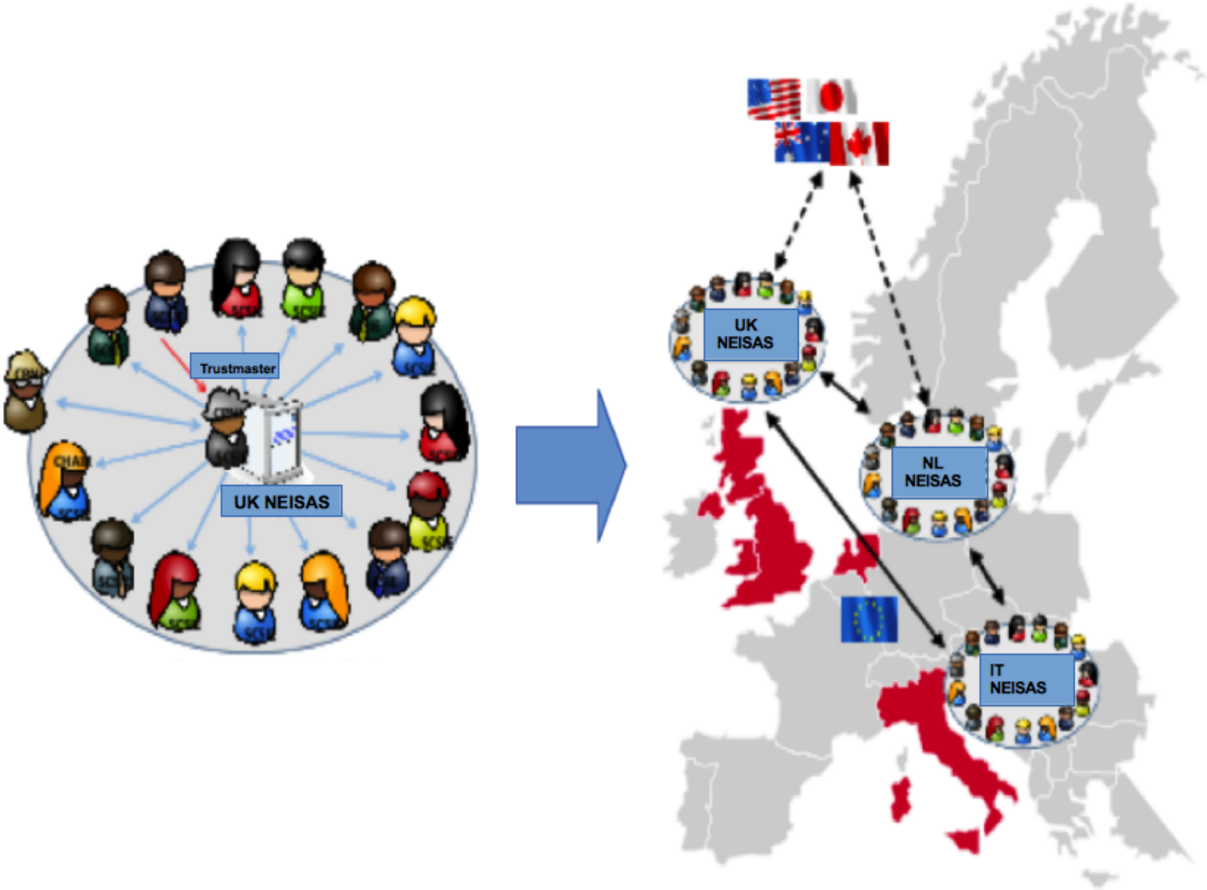

Figure 27: The NEISAS information sharing model.

Shared information concerns critical infrastructures. In particular, it concerns potential and actual attacks and vulnerabilities; best practices, incident responses, and relevant standards; research and analysis on threats, vulnerabilities, emerging trends and technologies; other information that supports in managing risks, protecting their assets and ensuring compliance and resilience.

The NEISAS platform provides basic functionalities allowing to issue posts and messages, to notify events and to contribute to forum discussions.

Furthermore it provides the following advanced functionalities:

- *traffic-light protocol for alerts* [29]. It is a policy used to categorise information as white (unrestricted information), green (community-wide, but not released outside the community); amber (limited distribution on a need-to-know basis), and red (personal, for named recipients only);
- *information sharing* on a one-to-one basis or with a specific group of members or other trust-circles;
- *anonymous posts* [29]. If sensitive information to be shared could potentially cause embarrassment to the originator's organization from a business perspective, the trustmaster could play a key role. The originator of the information may ask the trustmaster to advise other members about a specific topic, but to conceal her/his identity;
- *Information Rights Management*. It offers a further level of security, as the content of an IRM protected alert cannot be copied or printed.

Users of the NEISAS platform are individuals and organisations in the domain of Critical Infrastructures, as owners and operators of critical infrastructure in the following sectors (Figure 28):

- ICT/Telecommunications;

- Mass transportation;
- Energy (SCADA).

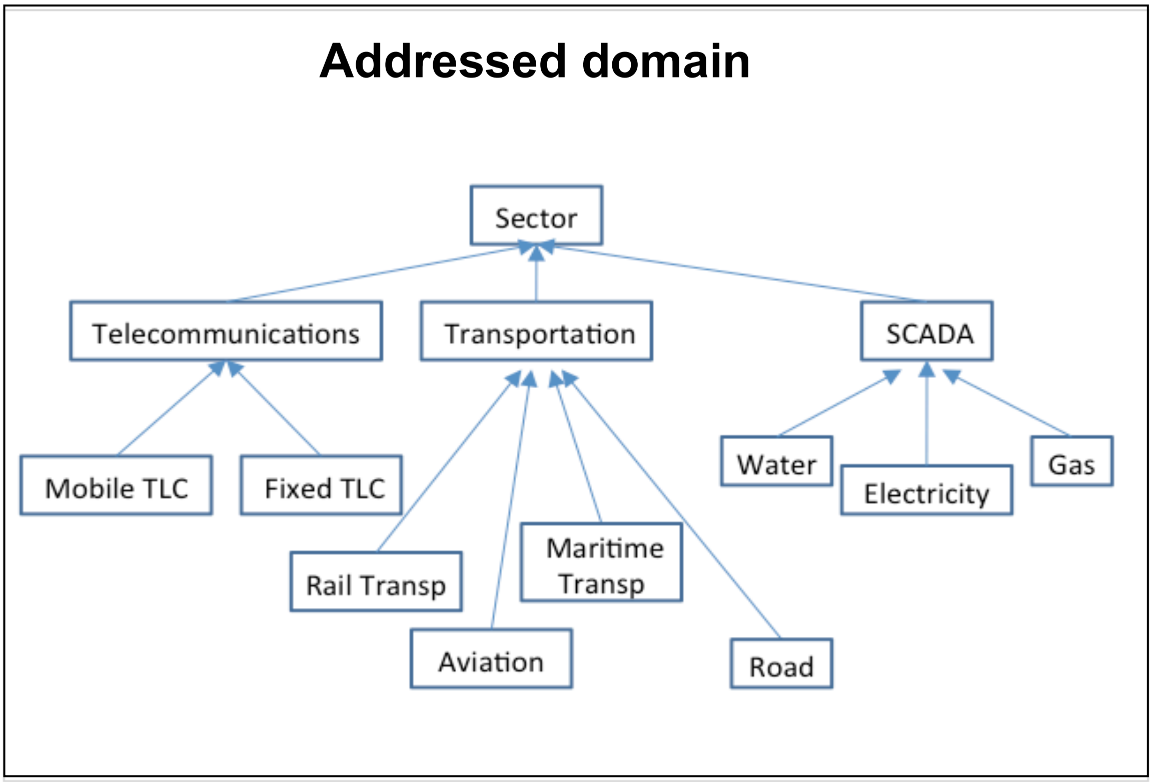

Figure 28: Critical infrastructures sectors.

The main features of the platform are the following:

- Social collaboration (Web 2.0) in the Critical Infrastructures domain;
- Access control;
- Identity Management;
- Microsoft Information Rights Management (IRM);
- Data protection;
- Resource discovery;
- Metadata Management;
- Content and Data Management;
- Interoperability.

The NEISAS graphical user interface is presented in Figure 29.

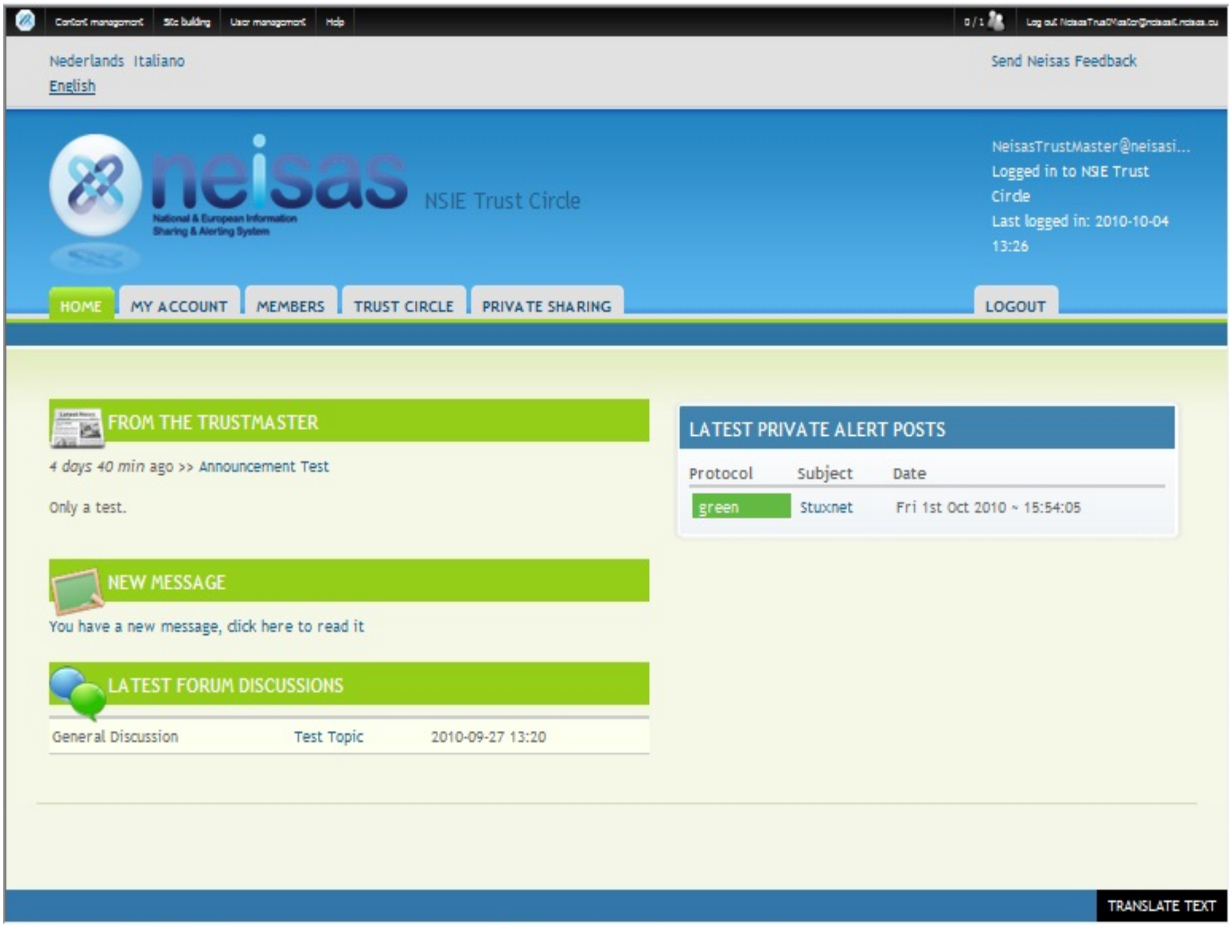

Figure 29: The NEISAS graphical user interface.

Finally, the functional architecture of NEISAS is presented in Figure 30.

The NEISAS platform may be customised for hosting the activities expected for CIPRNet. In particular, other than offering a "private" trusted platform for information exchange and sharing among operators and stakeholders, the same platform could host the collaborative information sharing among CIPRNet DSS managers and CI operators. The former may use the platform for sending to CI operators the Physical Harm Scenario; the latter may be committed to send back information on the impact of the predicted damage(s) on their Infrastructure by communicating a number of information (which will be expressly requested by the CIPRNet DSS manager) needed to feed, as input, the System of Systems model (e.g. based on I2Sim) in order to estimate the impact of the service reduction on one CI on the dependent others.

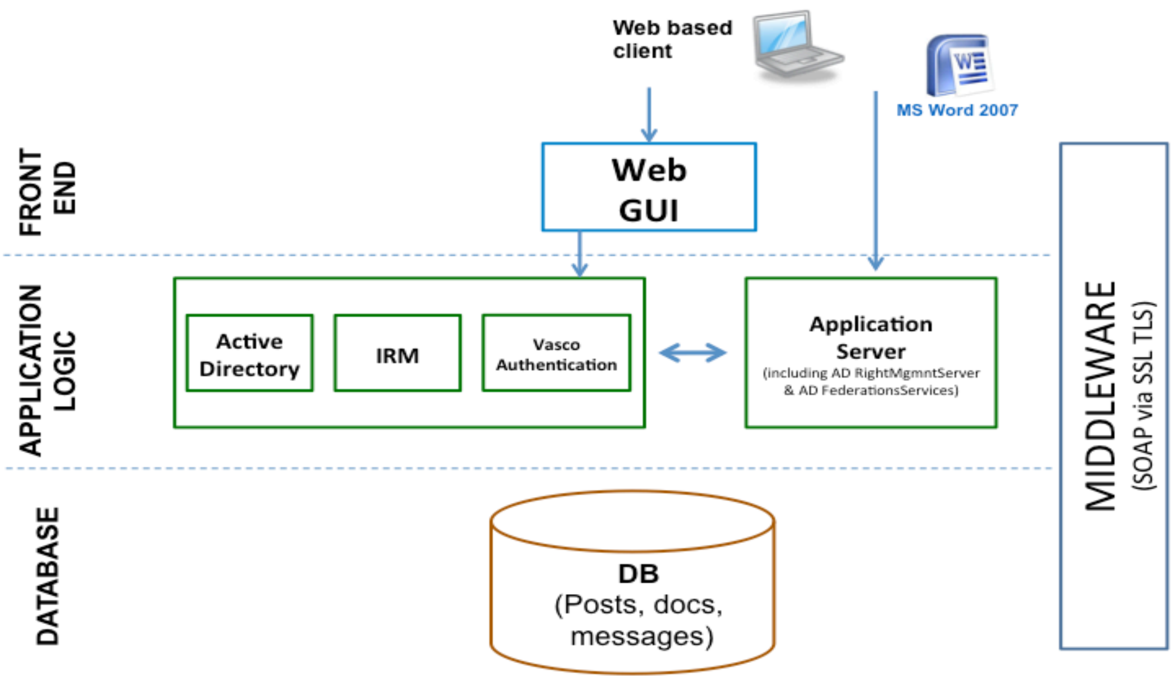

Figure 30: The NEISAS functional architecture.[5]

[5] VASCO authentication is an authentication server allowing to add a further level of security by means of an authentication device generating passwords (http://www.vasco.com).

9 Annex 3 – GeoPlatform

GeoPlatform [31] is an Open Source Framework developed by GEOSDI [30] for creating Rich Web GIS Applications based on geospatial web-based software and using an open source approach. GEOSDI is a research group of the Institute of Methodologies for Environmental Analysis of the National Council of Research (CNR IMAA), which designs, manufactures and distributes geospatial web-based software systems, using an open source approach. GEOSDI is also configured as a consultant for the Italian Civil Protection Department of the Prime Minister Office For implementing the Civil Protection National Spatial Data Infrastructure, according to the provisions of the INSPIRE Directive (2006) using Open Source software applications.

The objective of GEOSDI Programme is to provide a platform that would allow people to easily develop application to share their geo-based application and geographical information, taking advantage of the EU INSPIRE directive to share data (relative to the environment etc.) among different actors. For example, when an emergency occurs (e.g. emergency caused by earthquake, landslide, flood) the Civil Protection needs to manage and coordinate the emergency intervention, with the help of maps using: (i) Spatial Data; (ii) Infrastructures Data; (iii) Resource Data. These data can be provided through OGC standards [19] i.e. WMS that can easily be integrated in the GEOSDI solutions.

In the following the main features of the Geo-Platform are described:

- The framework is based on GWT (Google Web Toolkit) technology. The Web GIS application is developed using JAVA code that using GWT will be transformed in Javascript code optimized for any browser.
- The framework can be extended using Widgets (e.g. Map feature, Layer tree, Layer properties) that perform functional needs of the end user. For example, the CIPRNet DSS Risk Map Viewer component uses a particular widget to refresh automatically the geographical layer or map displayed on the current view every x seconds/minutes etc. This widget is used to refresh the earthquakes data layer. Another interesting component is the widget that can be used to send emails whenever specific events happen. This may be useful to issue alarms to CI operators.
- Geo-Platform can be installed locally on a Linux[6] machine (using a downloadable ISO DVD); such an installation allows to set up different users with roles and every user can have one or more projects associated. Data can reside locally or on different remote servers (via OGC-compliant services).

In the scenarios presented in 4.4 the Geo-Platform has been used to display ISIDE information [33], that is a system developed by INGV (Italian National Institute for Geophysics and Volcanology) to gather and store data from the Italian Seismic network and provides real-time information about seismic events (i.e. magnitude and epicentre) in Italy. Thanks to the specific feature developed and integrated in geo-platform framework it is possible to retrieve such seismic data in geospatial format (via WMS service provided through OGC standards). This feature may be easily imported into the CIPRNet Decision Support Systems (DSS) to perform impact assessment on buildings, roads etc.

In order to use Geo-Platform, there is currently no need to develop new Geo-Platform components to implement the DSS functionalities (at least, in the way in which these are conceived), but only to configure the data infrastructure hosting the different data sources (e.g. CI networks, weather forecast) that need to be imported/acquired into Geo-Platform. GeoPlat-

[6] The installation of GeoPlatform on a Windows machine has not been currently tested by ENEA.

form allows three different user profiles: “viewer” (only visualization allowed), “user” (the user can display and add WMS data) and “admin” (full privileges). The DSS layout can be edited group-wise by DSS team spread across different locations.

The use of Geo-Platform is compliant with the objectives of the CIPRNet DSS and that adopting such a platform would give the following advantages:

- use of the platform via browser;
- easy integration/exploitation of OGC-based spatial data;
- use of already built widget that allow high usability to the DSS users (e.g. CI operators to update the operability level of each CI).