GENERALISED TOPOLOGICAL AND FUNCTIONAL ONTOLOGIES FOR DISRUPTION SCENARIO DESCRIPTION IN CRITICAL INFRASTRUCTURE SYSTEMS

Paolo Trucco and Boris Petrenj
Department of Management, Economics and Industrial Engineering
Politecnico di Milano
Piazza Leonardo da Vinci 32
20133 Milan, Italy
paolo.trucco@polimi.it; boris.petrenj@polimi.it.

Abstract: The systematic and complete identification of relevant accident scenarios for Critical Infrastructure is still one of the major challenges to achieve higher resilience performance. THREVI2 project aims to answer to this Authorities' and Operators' important need. It is implemented by elaborating three coordinated ontologies (*CI systems*, *Hazards & Threats* affecting CI, *CI interdependencies*) and development of a dedicated software tool for system specification and scenario generation. THREVI2 ontologies have been developed by a joint implementation of different methodologies: literature review, experts' review, basic ontology development methodology, and a final pilot testing of the tool. The main results achieved are: i) a generalised and standardised specification framework for CIs and services; ii) a generalised and standardised all-hazards catalogue for CI; and iii) an improved scenario generation process to support CI risk assessment.

Key words: Infrastructure, Scenario Generation, Ontology, Disruption

INTRODUCTION

Critical Infrastructures (CIs) are exposed to a wide spectrum of hazards and threats which vary in nature (natural, technological, human-intentional or non-intentional) and, that can be internal (e.g. technical failure, sabotage, human error) or external to the infrastructure (e.g. flood, chemical explosion, terrorist attack). As such, hazard and threat assessment is a key element within CIP strategies and CI risk assessment. However, it is difficult for Authorities or Operators to get comprehensive information of all potential disruption scenarios relevant for CIP, since:

- hazard, threat and vulnerability assessments are often very specific in nature and related to different disciplinary fields;
- existing information most often focuses only on one type of hazard or on the vulnerability of one type of target (a single infrastructure or asset).

This is why the systematic and complete identification of meaningful accident scenarios for Critical Infrastructure is still one of the major challenges to achieve higher resilience performance. At **European/National level** it is a part of the CI identification process, since the EC Directive 2008/114/EC requires to develop "worst case scenarios", to simulate the failure of a

potential ECI, in order to assess the transboundary impacts on other Member States. At **infrastructure level**, vulnerability and risk assessment needs to be applied in order to define appropriate protection and resilience measures (e.g. European CI operators have to include in the Operator Security Plan "a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impacts").

THREVI2 project has been designed to answer to the Authorities' and Operators' need to get comprehensive information of all potential disruption scenarios relevant for CIP/R by developing a comprehensive and multi-dimensional all-hazards catalogue for critical infrastructures. Specific objectives are:

- to elaborate three coordinated ontologies (Hazards and Threats, CI topologies, CI Interdependencies);
- to merge them by existing vulnerability models; and
- to develop a dedicated software tool for scenarios generation to support different end-users in specifying the overall system of systems and generating a set of relevant disruption scenarios.

To this end, an ontology-based approach has been implemented and two interconnected ontologies have been developed:

- an ontology of Hazard & Threat affecting CI;
- an ontology of physical and functional topologies of Critical Infrastructure systems,

They have been merged through specific vulnerability and dependency entities.

ONTOLOGICAL APPROACH TO SCENARIO GENERATION

Methodology

An ontology can be defined as '*a formal description of entities and their properties, relationships, constraints, behaviours*' [1], or simpler as '*a specification of a conceptualization'* [2]. Ontologies are used to capture and share knowledge about some domain of interest. Ontology deals with questions concerning what entities exist or can be said to exist, and how such entities can be grouped, related within a hierarchy, and subdivided according to similarities and differences. It is used to describe the concepts and relationships that are important in a particular domain, providing a vocabulary for that domain as well as a computerized specification of the meaning of terms used in the vocabulary. Ontologies range from taxonomies and classifications, database schemas, to fully axiomatized theories. In recent years, ontologies have been adopted in many business and scientific communities as a way to share, reuse and process domain knowledge. Ontologies are now central to many applications such as scientific knowledge portals, information management and integration systems, electronic commerce, and semantic web services [3].

Ontology is a structure that allows creating a conceptual map to organise elements within a domain by using *classes*, *properties* and *instances*. Any class can contain many subclasses

organized on different levels. An instance is an "object" within the ontology domain which is described using the relevant classes and properties. A property is a directed binary relation that specifies class characteristics; generally, they are attributes of instances and sometimes act as data values or as link to other instances. Properties may possess logical capabilities such as being transitive, symmetric, inverse and functional. Properties may also have domains and ranges. An ontology together with a set of individual *instances* of classes constitutes a *knowledge base* [4]. We use taxonomies to describe how different classes are related by organising them into groups and/or hierarchies (according to level of detail). Adopting a standardised description is also important for systematic connection between the taxonomies to the other parts of the ontology. In the first place we have to organise knowledge in specific domain, using scattered data and various sources. For the two main domains (Critical Infrastructures and Hazards & Threats) it is necessary to determine what concepts exist, and to describe and classify them within the domain in a systematic way.

THREVI2 ontologies have been developed by a joint implementation of different methodologies:

- literature review covering scientific, technical and regulatory documentation;
- experts review, to complement incomplete documentation, to validate and harmonise the proposed ontologies;
- basic ontology theory and development methodology;
- pilot testing of the SW tool in two different contexts, respectively at national and regional scale.

To make ontology development description clearer we describe typical steps in an ontology development process, as presented in Figure 1 [4].

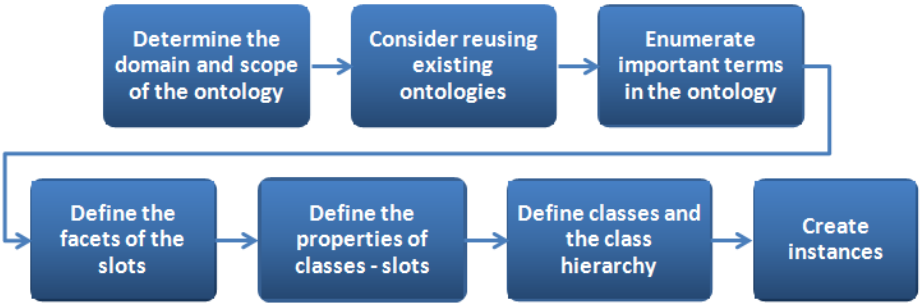

Figure 1: Process of Ontology Development (adapted from [4])

Critical Infrastructure Ontology

For the Critical Infrastructure System Ontology, the covered sectors include *Energy*, *Transport*, *Water* and *Telecommunications* for a total of 11 different infrastructure subsectors (Figure 2). Each CI is described by means of two interconnected sub-ontologies: one for the physical specification of CI topology, the other for the functional specification.

The overall infrastructure ontology framework is organized in three parts – assets, functions and services (Figure 3) which were subsequently linked with the service delivery process (Functional ontology).

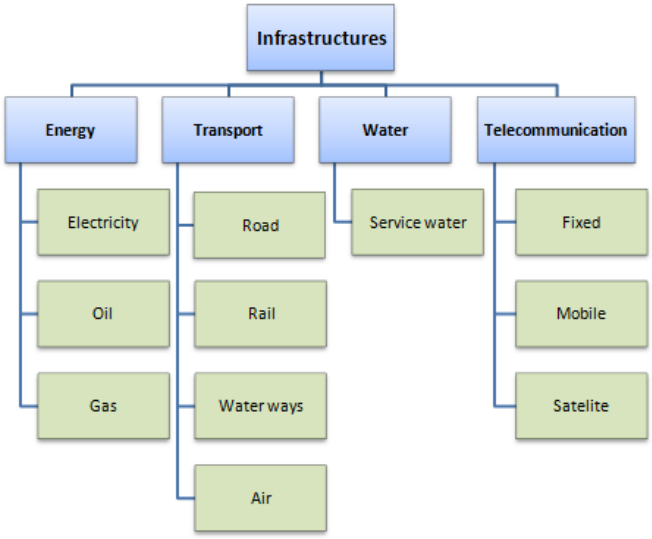

Figure 2: Covered infrastructure sectors and sub-sectors

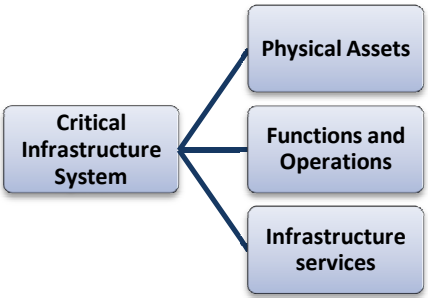

Figure 3: General CI ontology framework

The general concept of physical specification is to arrive at a complete and systematic physical description of the infrastructure thanks to a standardized nomenclature and definition of its most relevant elements. The goal for this effort was to deliver this capability by a mixed and harmonized used of international standards. More specifically, the Critical Infrastructure System ontology has been developed using different data sources:

- *Regulatory* – standards and codes adopted or required by government and public bodies
- *Technical/Professional* – standards and codes developed by industrial or professional associations, standardisation bodies, etc.
- *Scientific* – modelling and descriptive methods adopted in studies and tools reported in scientific literature

Globally, more than 100 references, of scientific, technical and regulatory nature, have been identified and systematically reviewed. After analysis, a portion of the sources turned out not to be useful for the ontologies description. At the end 62 documents have been used to develop the final 22 sub-ontologies (Table 1).

Through this literature review, for each type of infrastructure a list of physical assets and functions has been derived. All the assets and functions are classified according to a common classification scheme developed during the analysis, accompanied with a standardised description. The physical arrangement of a generic infrastructure has been specified using class hierarchy in OWL language and implemented in Protégé software (Figure 4).

Table 1: Summary of used references

Document type	Number of sources
Regulatory	**24**
National	(17)
International	(7)
Technical	**25**
National	(11)
International	(14)
Scientific	**13**
TOTAL	**62**

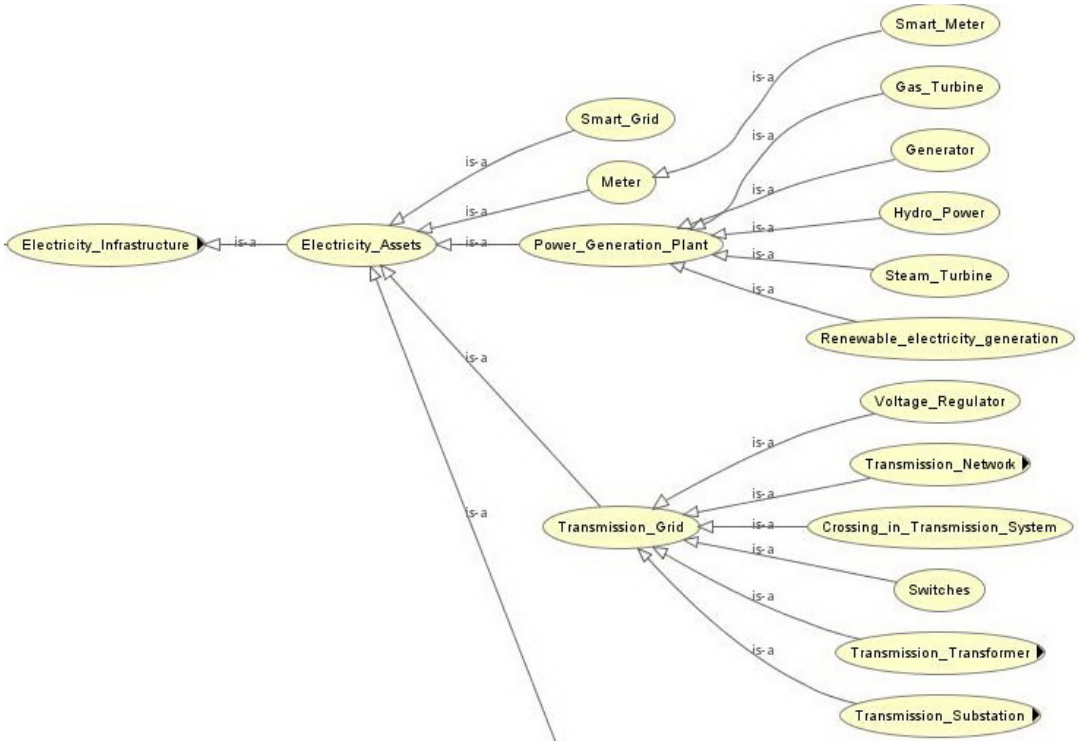

Figure 4: Portion of the Physical Asset sub-ontology for Electricity Infrastructure

As for the design of the Functional Ontology of CI, the aim was to cover all operations phases from the acquisition of resources (supply side) to the final service delivery to end users (demand side). Therefore, all the functional sub-ontologies have been organized with reference to a standardized functional representation of a general service delivery process (Figure 5). Accordingly, the highest level of the functional ontology has been organized into five main phases:

- sourcing;
- source stock;
- service generation;
- service stock;
- service delivery.

The lower layers of each functional sub-ontology contain more detailed functions specific for each CI sector and sub-sector.

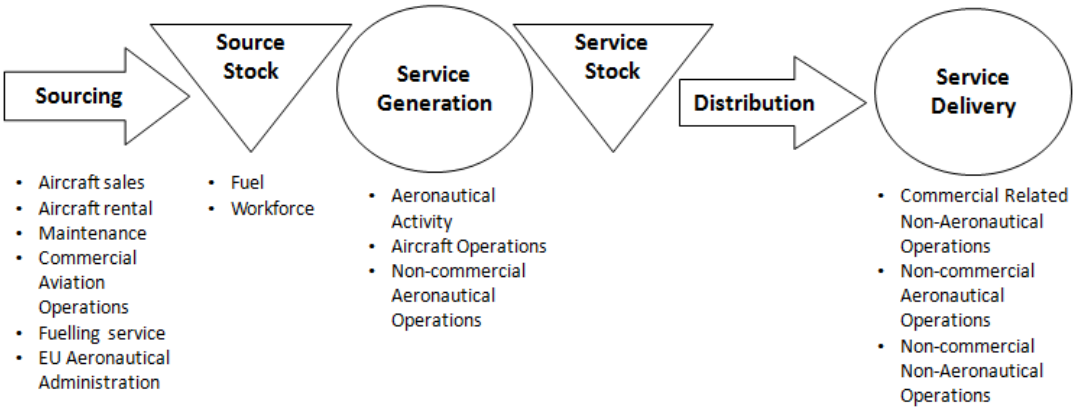

Figure 5: General Service delivery process (Air transport functions used as an example)

The relations (links) between Assets and/or Functions have been defined adopting the Integration Definition Function Modeling (IDEF∅) standard, generally used for developing structured representations of a system or enterprise. Figure 6 represents an example of links (relations) between Assets and/or Functions within the service delivery process, where *Service Generation* stage within Air transport sector has been used as an example.

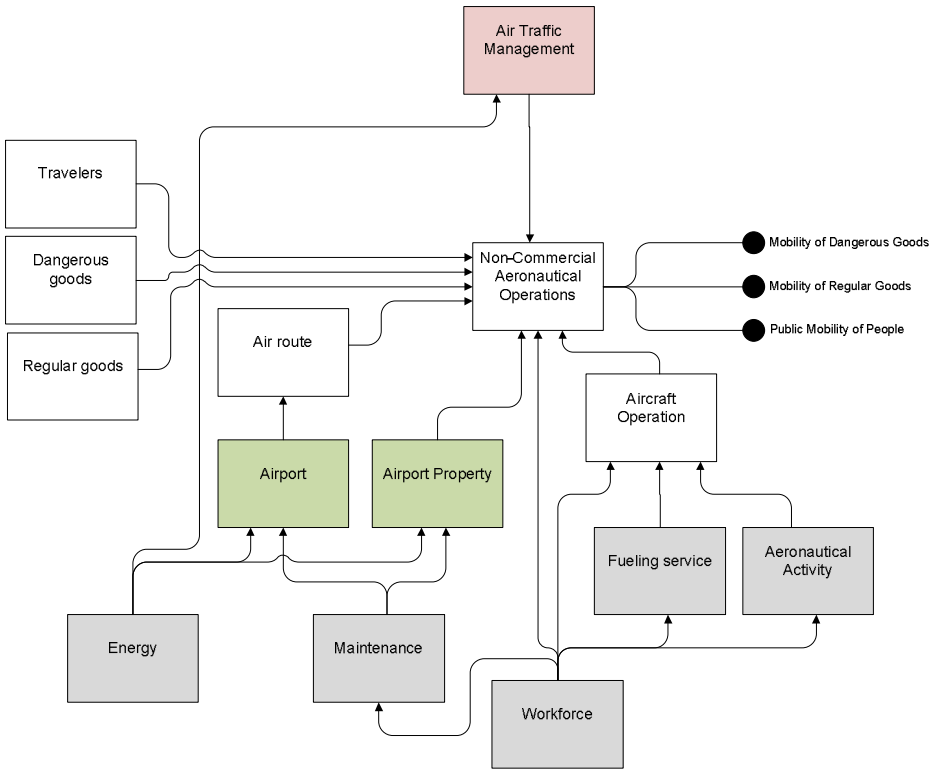

Figure 6: Service generation in Air transport sector

Hazard & Threat Ontology

Hazard and Threats (H&T) Ontology aims to systematically characterise different typologies of events to be used for the development of the Pathfinder tool that allows first-order recognition of:

- all possible threats that can affect or destroy a generic CI;
- all possible infrastructure that can be affected or destroyed by a specific threat.

The ontology is based on a hierarchical structure (classes and sub-classes), and is developed considering the possibility to reuse available literature on threat classification. For each class, a set of features (duration, impacted area, etc.) is assigned to better characterize the classes and to allow flexible navigation of the user within the ontology.

The overall Hazards & Threats Ontology framework is organized in four interconnected sub-ontologies, each one responding to a simple question (Figure 7):

1. **Who** is the hazard? *Events Type sub-ontology*. Potential events sub-ontology is created in the form of a hierarchical taxonomy. At the first level of this hierarchical taxonomy identifies the considered hazards have been classified as *Natural* (e.g. flood, landslide, etc.), *Technological* (e.g. dysfunction of equipment or system components) and *Human* (e.g. malicious act). Partial view of Natural hazards taxonomy is given as an example in Figure 8.
2. **How** the hazard can occur? *Hazard attributes sub-ontology*. A sub-ontology of hazard attributes is specified. Hazard attributes sub-ontology includes *Duration, Resource, Event impact area, Actor, Driver and Predictability*
3. **What** action are (can be) triggered by the hazard? "*Modus*" and "*Modus effect*" concepts are introduced in order to describe the actions/processes (impact mechanism) through which the Critical infrastructures can be impacted and the relevant effects.
4. **When and Where** the hazard can occur? *Spatial and temporal attributes sub-ontology*.

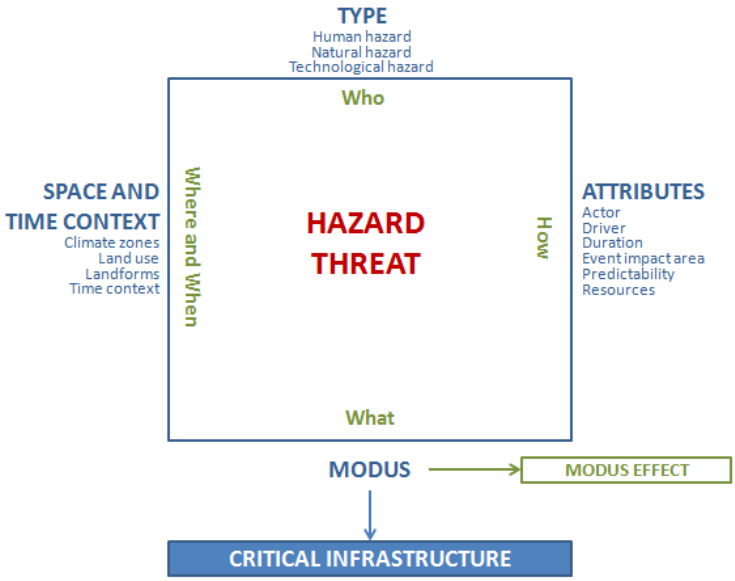

Figure 7. Hazard & Threat ontology

In addition to the common attribute it was decided to introduce a new feature to define how a given event, classifiable in terms of threat or hazard, occurs and can affect the CI. At this attribute has been given the name of **Modus**. Modus is useful because it allows simplifying the complexity of the ways in which an event can occur because, by approximation, events with different origins (natural, technological and human) may have the same modus (E.g.: both a landslide and a manifestation can create a road obstruction. In this case "Obstruction" is the one of the possible modus that characterised two hazards with different origin). Each modus, in turn, can create one or more effects on infrastructure (**Modus effect**). According to our description level, Modus is used as the link with the ontology of the CI Assets.

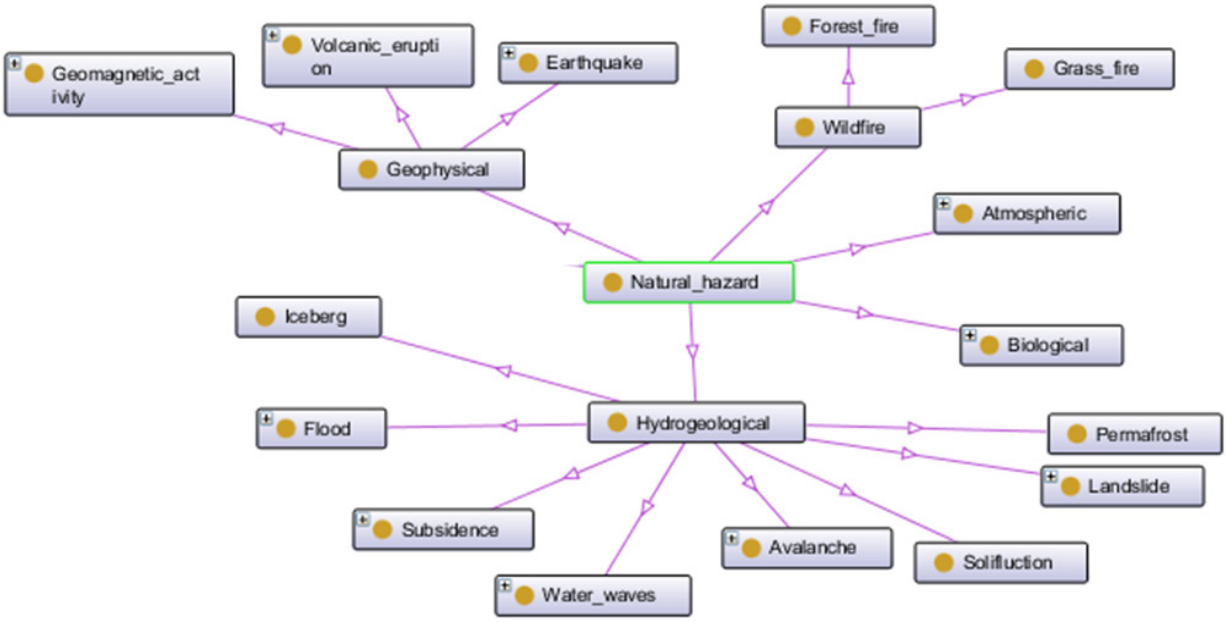

Figure 8: Partial view of Natural hazards (first and second levels)

MODELLING VULNERABILITIES & INTERDEPENDENCIES

Vulnerability modeling

Having developed CI assets and H&T ontologies, the following step consisted of connecting the two ontologies. It was done by assessment of actual and potential vulnerabilities of CI assets to specific hazards and threats. Vulnerability can be understood as '*the susceptibility of the infrastructure to threat scenarios*' [6].

For instance (Figure 9), **Snow Avalanche** can affect an infrastructure in different ways – either through direct impact on it, the subsequent static pressure and/or because by producing an obstruction (so it has *Static Pressure*, *Kinetic Energy* and *Obstruction Modus*).

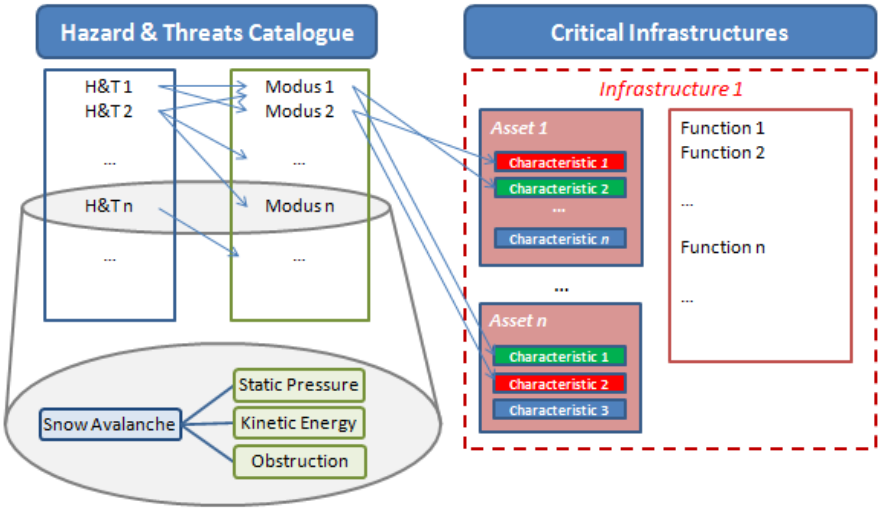

Figure 9. Impact/Vulnerability modelling (links between H&T and Infrastructure Assets)

Moduses affect (are linked to) exclusively CI assets, while impact of modus on CI functions is taken into account through possible unavailability of asset needed to execute the function. The links have been mapped within a matrix indicating connections where modus affects an asset (Figure 10). In cases where modus affects an assets conditionally (e.g. depending on the asset material or position), asset has been characterised by additional attributes which define if the modus will affect the specific asset type. The typical examples of attributes are ***position*** of an asset (buried/ superficial/ above ground) for different types of pipelines, or asset ***material*** (steel/ concrete) in case of a bridge.

				MODUS																									
				Data alteration				Ground deformation		Contamination			Energy variation				Mechanical action						Environmental variation						
																	Wearing		Pressure										
				Data corruption	Data destruction	Data breach	Data theft	Transient ground deformation	Permanent ground deformation	Air contamination	Water contamination	Food contamination	Electrical discharge	Ionizing radiation	Thermal energy	Electromagnetical disturbance	Corrosion	Abrasion	Static pressure	Overpressure peak	Kinetic energy	Dynamic pressure	Temperature variation	Degradation of visibility	Degradation of air quality	Degradation of soil quality	Obstruction/ occupation	Unavailability of resources
ASSET	ENERGY	Electricity	Power Generation Plant	X	X			X	X						X	X	X	X	X	X	X								
			Transmission Grid	X	X			X	X				X				X	C	C	C	C	C								
			Distribution System	X	X			X	X				C			X	X	C	C	C	C	C								
			Smart Grid	X	X											X														
			Meter	X	X								X		X	X	X	C	C	C	C	C								
	TRANSPORT	Road	Surface Road					X	X						X		X	X			X							X	
			Road Bridge					X	X						C		C	C		X	X	X						X	
			Road Tunnel					X	X						X		X	X		X	X							X	
			Toll Booth					X	X				X		X	X	X	X		X	X							X	

Figure 10. Links between Modus and Assets (partial view)

Interdependencies modeling

In order to comprehensively cover possible vulnerabilities and risks it is needed to model all types of interdependencies.

Geographic interdependency occurs if a local environmental event creates state changes in infrastructures [7]. For example, a disrupted asset (impacted by a hazard and/or threat) can behave as a source of a new hazard causing cascading effects through different interdependency mechanisms (Figure 11).

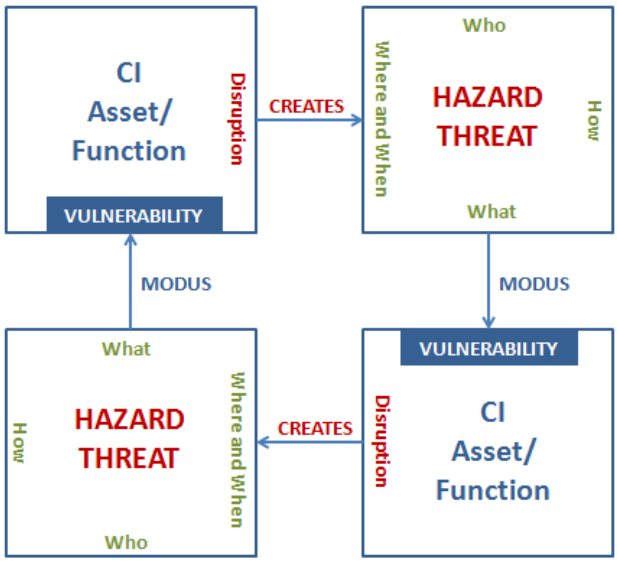

Figure 11. Modelling of geographical interdependency

Functional (or Physical) interdependency is a physical reliance on material flow from one infrastructure to another [7]. Within CI topologies (service delivery process) mechanism, control and material/resource inputs have been defined for each single function, as well as material flow between related functions – covering both dependencies within and between infrastructure sectors (e.g. see Figure 6).

Cyber interdependency occurs if the state of an infrastructure depends on information transfer between infrastructures (e.g. SCADA, communications, monitoring, controlling) [7]. The information is normally transmitted through the information infrastructure. Cyber interdependencies have been modelled by connecting information (a common resource that has been identified as an input to functions) and telecommunication assets.

VALIDATION

In the first phase, about 25 experts have been invited to review the Critical Infrastructure ontologies on assets and functions. Experts have been provided with an evaluation template (available on request) where they have been able to propose:

- doubts on the clarity of, or different nomenclature and description for assets/functions;
- missing relevant assets and/or functions;
- not relevant assets and/or functions (candidates to be removed);

They have also reviewed the service delivery process and validated connections (and their types) between assets and/or functions, indicating missing or wrong links.

Based on the comments and recommendations received by the experts, some of the assets and functions have not been used in the final integration of CI sub-ontologies. It is either due to a high level of detail – assumed not to be relevant to describe the effects of threats to service delivery process -, or to an activity that is not being carried out on regular bases (and thus not relevant in the standard service delivery process). However, we decided to keep these assets/functions inside the catalogue in order to assure the completeness of the ontology and a comprehensive description of CI.

In the subsequent phase experts are requested to validate the integration of CIs and H&T ontologies which are connected through different types of interdependencies. This part of the validation has been carried out through face-to-face interviews with technical managers and experts along with the pilot application of the PATHFINDER tool.

CONCLUSIONS

By developing of a multidimensional ontology-based model it is possible to generate and document a larger set of plausible accident scenarios, fully exploiting the generalised existing knowledge on CIP as well as all the specific knowledge on the system under analysis and its external environment. The advantage of an ontological approach to disruption scenario generation for CI is a systematic specification and classification of concepts in the domains of interest. It embraces all hazard approach, allowing detection of complex cascading effect mechanisms difficult to be identified and directly elicited by experts.

The main results achieved are generalised and standardised specification framework for CIs and services, generalised and standardised all-hazards catalogue for CI, and improved scenario generation process to support CI risk assessment. Indirect benefits are also expected, in term of quality of shared information among actors thank to a standardised nomenclature and modelling of CI vulnerabilities. By integrating CI, Hazards & Threats and vulnerabilities, the PATHFINDER tool enables effective risk assessment and prioritisation of activities and resources in order to reduce those risks.

The main limitation of the approach is manifested though weak abilities in geo specification and description of CI (partial modeling of geo interdependencies). Further limitation, or extreme challenge, will be integration of soft and organisational factors involved in interdependencies (i.e. difficulties in modeling logical interdependencies).

An open issue remains on how to model logical interdependencies as a further level of integration between CI sub-ontologies. Two or more infrastructures are logically interdependent if the state

of each depends upon the state of the other via some mechanism that is not a physical, cyber, or geographic connection [7]. This category can contain policy, legal or regulatory regimes; economic systems and trends; social and human factors, etc. – making it very complex and uneasy to properly cover.
Future planned activities include integration of Geographic Information System (GIS) which would enable visualisation as well as spatial representation of assets, systems and threats.

Acknowledgment

THREVI2 research project has been co-funded by DG Home Affairs of the European Commission, under CIPS/ISEC Work Programme. The financial support is gratefully acknowledged.

REFERENCES

[1] M. Grüninger and M. S. Fox. "*Methodology for the design and evaluation of ontologies*", Technical Report, University of Toronto, Toronto, Canada (1995).
[2] T. R. Gruber. "*A translation approach to portable ontologies*" Knowledge Acquisition, 5(2):199-220, 1993. http://www-ksl.stanford.edu/kst/what-is-an-ontology.html
[3] Protégé official website: http://protege.stanford.edu/
[4] N. F. Noy and D. L. McGuinness, "*Ontology Development 101: A Guide to Creating Your First Ontology*", Stanford University, Stanford (CA), USA
[5] *Integration Definition for Function Modeling (IDEF∅) Standard*, Draft Federal Information Processing Standards Publication 183, 1993.
[6] Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, *27*(3), 571-583.
[7] S.M. Rinaldi, J.P. Peerenboom and T.K. Kelly. "*Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*" IEEE Control Systems Mag. 21: 11-25. (2001).