# Ontology-based Approach to Disruption Scenario Generation for Critical Infrastructure Systems

Paolo Trucco[1], Boris Petrenj[1], Sara Bouchon[2], Carmelo Di Mauro[2]

[1]Politecnico di Milano, Department of Management, Economics and Industrial Engineering, Piazza Leonardo da Vinci 32, 20133 Milano
[2]RGS – Risk Governance Solutions S.r.l., Italy
E-mails: paolo.trucco@polimi.it, boris.petrenj@polimi.it, sara.bouchon@riskgovernancesolutions.eu, carmelo.dimauro@riskgovernancesolutions.eu

**Abstract:**

The systematic and complete identification of relevant disruption scenarios for Critical Infrastructure (CI) systems is still one of the major challenges to achieve higher resilience performance. We assist Authorities and Operators in this endeavour through creating a comprehensive and multi-dimensional all-hazards catalogue for CI. It is implemented by developing two ontologies:

- *CI systems Ontology*, covering Energy, Transport, Water and Telecommunications sectors, each being described through two sub-ontologies (physical and functional) interconnected within the service delivery topology.;
- *Hazards & Threats Ontology*, characterising different typologies of events, their attributes, types and possible effects to CI systems.

The two ontologies are connected through vulnerability and (inter)dependency models. The main results achieved include: 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.

**Keywords: Critical Infrastructure, Scenario Analysis, Ontology, Vulnerability**

**Biographical notes:**

**Paolo Trucco** is Full Professor of Operations Risk Management and Director of the PhD Programme in Management, Economics and Industrial Engineering at the School of Management, Politecnico di Milano (Italy). His major area of research is Risk Analysis and Resilience Engineering of complex socio-technical systems and global supply chains, with expertise in the Oil&Gas, energy, transportation, healthcare and manufacturing sectors. Paolo Trucco is scientific advisor of the Lombardy Region Government (Italy) on Regional Programmes for Critical Infrastructure Resilience. He is author of more than 220 scientific publications and in the last four years he has been coordinating five research projects, at national and European level, on Critical Infrastructure Protection and Resilience.

## 1. Introduction

Critical Infrastructure (CI) 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 external to the infrastructure (e.g. flood, chemical explosion, terrorist attack) or internal (e.g. technical failure, sabotage, human error). As such, threat and vulnerability analysis is a key element within CIP strategies and CI risk assessment; for example, at European level, it is part of the CI identification process, since the EC Directive 2008/114/EC (EC, 2008) 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. Also at infrastructure level, vulnerability and risk assessment need to be applied to define appropriate protection 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*"; EC, 2008) and Business Continuity Plans (BCP).

However, it is difficult for Authorities or Operators to get comprehensive information of all potential disruption scenarios relevant for CIP planning, since:

- Hazard, threat and vulnerability analysis models or methods are often very specific in nature and strongly connected to narrow technical disciplines;
- 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 CI systems, encompassing all the plausible domino effects, is still one of the major challenges to achieve higher protection and effective allocation of resources.

The aim of the paper is to illustrate an ontology-based approach to disruption scenario generation for interdependent CI. An ontological view of the problem was assumed to assure the general value and the extended applicability of the method despite the wide spectrum of different infrastructure topologies, hazards and threats, vulnerabilities, interdependencies, and environmental conditions. Furthermore, an ontology-based approach provides the analyst with a standardised and comprehensive multi-dimensional all-hazards catalogue for CI that eventually offers a common platform to develop more homogeneous, comprehensible, and comparable assessments. More specifically, two interconnected ontologies were developed:

- An ontology of physical and functional topologies of Critical Infrastructure systems;
- An ontology of Hazards & Threats (H&T) affecting CIs.

They were then merged through specific vulnerability and dependency entities.
Finally, the coordinated set of ontologies was implemented into a dedicated software tool to support a consistent process for disruption scenario generation. The model and the tool are not intended to cover the entire Risk Assessment process requirements, but to strengthen a qualitative threat and vulnerability identification, that are the key elements to ground a reliable qualitative or quantitative Risk Analysis.

The paper is organised as follows. Section 2 explains the ontological approach to scenario generation. It shows the phases of ontology development and methodology used in the study and gives an overview of the relevant existing ontologies in the field. Section 3 presents the resulting ontologies for Critical Infrastructure systems (CI) and Hazards & Threats (H&T). In Section 4 we explain the modelling of Vulnerabilities and Interdependencies adopted to connect the main ontologies. Section 5 describes the ontologies validation process that was undertaken, including two pilot applications. Conclusions are given in the final section, covering the main contribution of the paper, study limitations and opportunities for future research.

# 2. Ontological Approach to Scenario Generation

An ontology can be defined as '*a formal description of entities and their properties, relationships, constraints, behaviours*' (Grüninger & Fox, 1995), or simpler as '*a specification of a conceptualization'* (Gruber, 1993).

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; hence, they are used to capture and share knowledge about some domain of interest. Ontologies range from taxonomies and classifications, database schemas, to fully axiomatized theories. An ontology together with a set of individual *instances* of classes constitutes a *knowledge base* (Noy & McGuinness, 2001).

Ontology is a structure that allows creating a conceptual map organizing elements within a domain, 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. 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 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. From the perspective of Lacy & Gerber (2004) ontologies are beneficial in simulation and modelling through the formalization of semantics, the ability to query and inference, and the sharing and reuse of developed models.

The ontology development process can be organised as presented in Figure 1; it is commonly implemented as an iterative process.

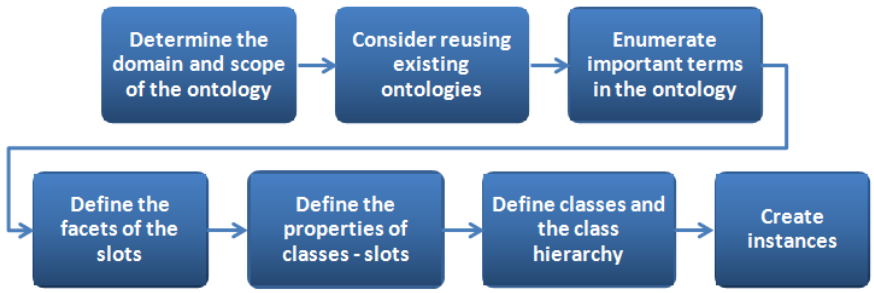


**Figure 1: Process of Ontology Development** (adapted from Noy & McGuinness, 2001)

To make sure that the concepts in the ontology reflect reality, that the ontology fits intended use, and that we have an adequate level of detail, we added a final validation phase to the process, as reported in Section 5.

**Overview of available ontologies for CI and Emergency Management**

Liu et al. (2013) conducted a thorough review of the ontologies in the field of crisis management (CM). They have identified a set of critical subject areas covering the information concepts dealt with within CM – Resources, Processes, People, Organisations, Damage, Disasters, Infrastructure, Geography, Hydrology, Meteorology, Topography and Other. Among these ontologies, originally designed for these areas of CM, very few are formally represented and publicly available, while most of them describe concepts in a single subject area. The same paper also indicated the lack of a common vocabulary or description standard.

In the CI domain, ontologies exist within simulators in specific sectors, used for observing and analysing the behaviours of a system, such as PSCAD – for conceptualising power system simulators and EPANET for representing water distribution simulators (Grolinger et al., 2011). These ontologies often include interdependencies enabling these domain simulators to be integrated in a federation. For example Tofani et al. (2010) use the ontology framework to model the interdependencies between CIs. Their Knowledge Based System (KBS) architecture consists of three ontologies: WONT (World ONTology) contains basic elements that are common across CI domains; IONT (Infrastructure ONTology) extends WONT to define specific CI and FONT (Federation ONTology) allows modelling dependencies among components of

different infrastructures. The DIESIS project (*Design of an Interoperable European federated Simulation network for Critical Infrastructures*) aimed to establish a basis for the modelling and simulation of CI based upon open standards (Rome et al., 2009). The DIESIS KBS design incorporates MKIONT (Meta-knowledge Infrastructure Ontology) which defines a general template for expressing the basic concepts and relationships of CI and their interconnections, but also IONTs, FONT and gateway components. MKIONT template essentially provides an object-oriented approach for defining the IONTs and FONT (Masucci et al., 2009). GenOM (Generic Object Model) represents and organizes the knowledge about CI interdependencies through a three-layered hierarchy of object classes (McNally et al., 2007; Lee & Yavagal, 2004). The Infrastructure Interdependency Simulator (I2Sim) uses a cell-channel model (based on the extension of Leontief input-output model) to represent the physical elements of CI and their interdependencies (Rahman et al., 2008), which enables the modelling of interdependencies without modelling the details of involved entities (Grolinger et al., 2011). Still, domain ontologies express concepts in a highly specialized manner and are often very detailed, making it difficult to merge ontologies into a general representation (Masucci et al., 2009). HLA (High Level Architecture) standard (by IEEE) and MSI (Multi-Simulator Interface) program (Rubin et al., 2006) focused on modelling of system interdependencies to enable federated simulations. However, environments based on these approaches are not suitable for simulating CI (Tofani et al., 2010; Masucci et al., 2009).
Other existing CI ontologies represent geographic information in infrastructure systems, such as OTN (Lorenz et al., 2005) – a formal description of the Geographic Data Files (GDF, that is an ISO standard for specifying how to store geographic information for intelligent transport systems).

SoKNOS system (Babitski et al., 2011) is a functional prototype for an integrated EM system that makes use of ontologies and semantic technologies for various purposes. The central ontology is a core domain ontology on EM, which defines the basic vocabulary of the EM domain. It is aligned to the foundational ontology DOLCE (Descriptive Ontology for Linguistic and Cognitive Engineering) which is a part of the WonderWeb Foundational Ontologies Library (Masolo et al., 2003). In SoKNOS specialised ontologies are developed for *Resources and Damages*, while *Deployment Regulations Ontology* defines the relations between the former two. For the definition of system components ontologies of *User Interfaces and Interactions* and *Ontology for Geo Sensors* were developed (Babitski et al., 2011).
The ENISA report on 'Gaps in standardisation related to resilience of communication networks' (ENISA, 2009) highlighted the lack of a consistent taxonomy for cyber security that identifies the role of resilience and defined basic risk and attack taxonomies. The subsequent ENISA report on 'Ontology and taxonomies of resilience' (Vlacheas et al., 2011) addressed this gap by defining an *Ontology of Cyber Resilience* based on a taxonomy of resilience, network and security threats at its core.
DISASTER project ('*Data Interoperability Solution at Stakeholder Emergency Reaction*', 2014) developed an integrative and modular ontology for establishing a common knowledge structure between all the first responders involved in an emergency. French ISyCri (*Interoperability of Systems in Crisis Situation*) project aimed at providing partners involved in crisis management with an agile Mediation Information System (MIS), not only to support the interoperability of the partners' information systems but to also coordinate their activities through a collaborative process (Bénaben et al., 2008). To this end, a *Crisis Ontology* (covering the studied system and the crisis characterisation) and a response ontology were built.

Dealing with interoperability issues, W3C Incubator Group presented Emergency Information Sharing Protocols among the CI operators and first responders – e.g. *Emergency Information Interoperability Frameworks (EIIF)* for EM, through which critical requirements and candidate ontology components are introduced (W3C, 2009). European Committee for Standardisation, with assistance of experts, specified a message structure to record a view of a situation as seen by a particular observer at a particular time (OASIS, 2009). This message structure in the frame of Disaster and Emergency Management is named the *Tactical Situation Object (TSO).*

According to Ouyang (2014), even though different databases have been proposed, there is no standardised data collection methodology for interdependent CI. At the best of authors' knowledge as well, a standardised and comprehensive ontology regarding CIs assets, functions and interdependencies is not documented in the extant literature.

**Overview of ontologies for Hazards and Threats**

The concept of "hazard" can be defined in many different ways, as diverse as the disciplines and sectors involved (for a review of existing definitions, see for instance Thywissen, 2006). The following can be considered as a good synthesis of all existing definitions: "*A potentially damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic disruption or environmental degradation. Hazards can include latent conditions that may represent future threats and can have different origins: natural (geological, hydro-meteorological and biological) or induced by human processes (environmental degradation and technological hazards). Hazards can be single, sequential or combined in their origin and effects. Each hazard is characterised by its location, intensity, frequency and probability*" (UN/ISDR, 2004).

Hazards and Threats were first time scientifically categorised in two classes: *Attack* - that required civil and military defences, and *Natural hazards* (Odén B., 2009 quoting Broberg, 2005). It happened after the Lisbon earthquake in 1755, which is believed to have caused a major outset in European risk thinking. Societies were shaped by fear of the threatening perils from wars, revolutions, fire, plague and famine" (Odén B., 2009 quoting Broberg and Nordin, 2000). Thus, the first class underline the intentional offense generated by social communities; the events of the second one are out of the human control. This categorisation reflected the social perception of risks.

The transition from a traditional to a modern society in Western Europe is usually described in terms of certain interrelated processes of change that involves a deep development of technologies. The hazard associated to dangerous materials and technologies and the social concern about the related risks allowed the sociologist Ulrich Beck defining the modern society as the society of risk, i.e. as "*a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself* " (Beck, 1992). Quarantelli (1984) wrote, "*To the category of natural hazards…has been added the relatively new category of technological accidents and mishaps. These are the disasters brought about by human error and the collective mistakes of groups.*" This led to a threefold hazard categorization:

- Attack;
- Natural;
- Technological.

Sometimes the term "man-made" hazard was used as synonymous of "technological" hazard to remark the responsibility and intentionality related to the generation of such risks (Smith, K. 1985). This highlights the fact that risks are also socially constructed and some risks are perceived as more dangerous because they are discussed in mass media more frequently, such as terrorism. Risk society leads to analysis of risks, causing prejudgment. As terrorism began to be more widely recognized as a hazard (or threat), the two terms "technological" and "man-made" began to be separated and less frequently used as synonyms. For many scientists and people it simply did not make sense to refer to terrorism as a technological hazard, mainly due to the distinction that can be made about the intentionality and the responsibilities related to the occurrence of such threats. Therefore, the class related to *Attack* was replaced with the *Man-made* (or *Human*).

In literature, threat is sometimes used as a synonym of hazard, e.g. "threat: *a person or thing likely to cause damage or danger*" (Oxford Dictionary, 2012). Though, some definitions show a distinction between both concepts. The first difference between a hazard and a threat is related to the probability of occurrence and the magnitude of the potential event. A threat is a very low-probability but serious event – to which analysts may be unable to assign a probability in a risk assessment because it has never occurred. The difference is clearly illustrated by the precautionary principle, which seeks to reduce

potential threats to a set of well-defined risks before an action, project, innovation or experiment is allowed to proceed (European Commission, 2000). A threat is therefore associated with a high range of uncertainty.

The second difference is that a threat is the result of intent: "*a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not*" (Oxford Dictionary, 2012). The US Presidential Commission on Critical Infrastructure Protection (PCCIP, 1996), for example, defines "threat" as a "*foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defence or economic security*". A threat may be an individual, an organization, or a "nation" (PCCIP, 1997) but a threat-source does not present a risk when there is no vulnerability that can be exercised (Stoneburner et al., 2002). Threats do not necessarily need to originate from human sources, but can be natural, human, or environmental. "*Natural or technological threats*" is therefore used to define low-probability but serious events (compared to natural or technological hazards), while *Human threats* (e.g. cyber or terrorist threats) refer to the intent of creating harm or damage.

Thanks to a growing awareness of the complexity of hazards, vulnerabilities and risks, a number of different categorization schemes have been developed. (e.g Abbott, 1996; Alexander, 1993; Guha-Sapir; CATANAT; ADRC et al., 2008; Coburn et al., 2014; Coch, 1995; Eagleman,1983; Glade & Alexander, 2013; Lindell et al., 2006; Munich RE; Quarantelli, 1998; Smith, 2000; Swiss RE; Tobin & Montz, 1997; University of Cambridge). The specific classification criteria and the related level of break-down into sub-categories mainly rely on the specific scope and use of the scheme and the related information.

Among the different taxonomies and definitions, it is interesting to comment the UN definition of a specific class of hazards. The UN (2002) introduced the class "Environmental Degradation" which is defined as: "*Processes induced by human behaviour and activities (sometimes combined with natural hazards), that damage the natural resource base or adversely alter natural processes or ecosystems. Potential effects are varied and may contribute to an increase in vulnerability and the frequency and intensity of natural hazards*." It is an interesting approach because for the first time there was the evaluation of the combination of two or more processes that can create a risk. In other terms risks interpret according a number of classes, i.e. by defining taxonomy, but also tried to capture the representation of some risks, along with their properties and relations, according to a system of categories that, in other terms, can be defined as ontology. This classification is coherent with the statement of Burton that considers that "*natural and social systems interact to produce a hazard*" (Burton, 1993). This means that the events are originally neutral. They are recognized as hazards only when they intersect with human and societal systems (Burton, 1993). This further implies that in the fields of CI analysis and their relations with the societies such interactions still need to be accurately investigated. The classification of hazard cannot be simply made according to some criteria (e.g. phonological, geographical, likelihood, magnitude, etc.) but it requires the evaluation of the relationship with the society as target that depend on the services provided by the CI. That is the main reason why the classification of hazard has to go beyond the concept of taxonomy towards the definition of ontology.

## Study Methodology

We used 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 the systematic connection between the taxonomies to the other parts of the ontology.

The starting point, and main challenge, is the arrangement of a comprehensive and harmonised body of knowledge in each one of the specific domains, given scattered data collected from various sources. For the two main domains (*Critical Infrastructure Systems* and *Hazards & Threats*) we determined what concepts exist, and eventually described and classified them within the reference domain in a systematic way. This task was accomplished 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;

# 3. Ontology-Based Specification of CI Systems and Related Threats

**Critical Infrastructures Systems 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).

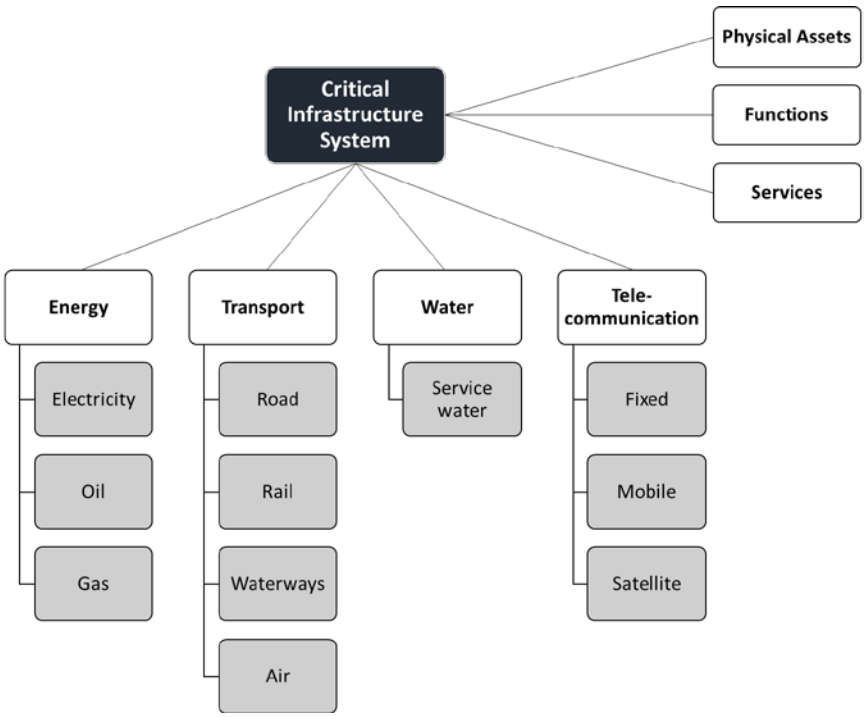


**Figure 2: Covered infrastructure sectors and sub-sectors**

Each CI is described by means of two interconnected sub-ontologies, one for the physical and the other for the functional specification. The overall infrastructure ontology framework is organized in three parts – assets, functions and services (Figure 2 that were subsequently linked within the service delivery process.

The ontology has been developed using various data sources. 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 ontology description. At the end 62 documents have been used to develop the final 22 sub-ontologies (reference list available inside the project deliverable).

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).

**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** |

Through this literature review, a complete list of physical assets and functions has been derived for each type of infrastructure. All the assets and functions are classified, according to a common classification scheme developed during the analysis, and accompanied with a standardised description (Table 2). Similarly, a list of functions with associated descriptions is given for each infrastructure sector (Table 3). The physical arrangement of a generic infrastructure (Figure 3) has been specified using class hierarchy in OWL language and implemented in Protégé software (Protégé, 2014).

**Table 2: List of assets - Electricity sector example (partial view)**

| Asset | Description |
|---|---|
| Meter | A device used to measure the amount of el electricity flowing through a point on the system |
| Smart Meter | An advanced electric meter that records consumption in intervals of an hour or less and communicates that information back to the utility for monitoring and billing purposes |
| Power Generation Plant | A power generation plant is a source of electricity. It is most likely fossil fuel–powered (coal, fuel oil, or natural gas) but could also be powered by nuclear, hydroelectric, a wind farm, or some other alternative power source |
| Generator | Technically, the generator is the part of the power plant that converts the mechanical power of a spinning shaft to electricity |
| Gas Turbine | High speed rotating machine in which fuel is burned continuously in a combustion chamber at high pressure and the combustion products are expanded through the turbine to produce shaft horsepower |
| Steam Turbine | Is a device that extracts thermal energy from pressurized steam and uses it to do mechanical work on a rotating output shaft |

**Table 3: List of functions - Electricity sector example (partial view)**

| Function | Description |
|---|---|
| Load/Demand [data forecast] | An amount of end-use demand./-The total amount of electricity used at any given moment in time usually measured m kW or MW |
| Demand activated governing | Form of pressure regulating installation (PRI) specifically designed to adjust automatically its set-point within pre-determined limits in sympathy with demand variations |
| Distribution Grid operations | One of the three parts that makes up the electric grid. The delivery of electricity over medium and low-voltage lines to end-use consumers. Distribution is owned and represented by the consumer's local distribution company (LDC), and is state regulated |
| Interruptible supply/load | Supply or load for which it has been contractually agreed that the consumer may be interrupted in accordance with specific terms and conditions |
| Input energy supply contract | The contract with Oil supply/supplier, Gas supply/supplier, Nuclear fuel supply/supplier, Water supply/supplier for delivery of the necessary input for the energy infrastructure systems |
| Metering and billing operations | Operations that a electricity supplier will conduct to meter and calculate the transmission cost, distribution cost, meter operation cost, data collection cost, tax etc, based on a contract between the consumer and the supplier. The supplier then adds in energy costs and the supplier's own charge. The terms and conditions for the contract must follow the European commission regulations although for each country of European union there may be some specific conditions |

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 4). 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.

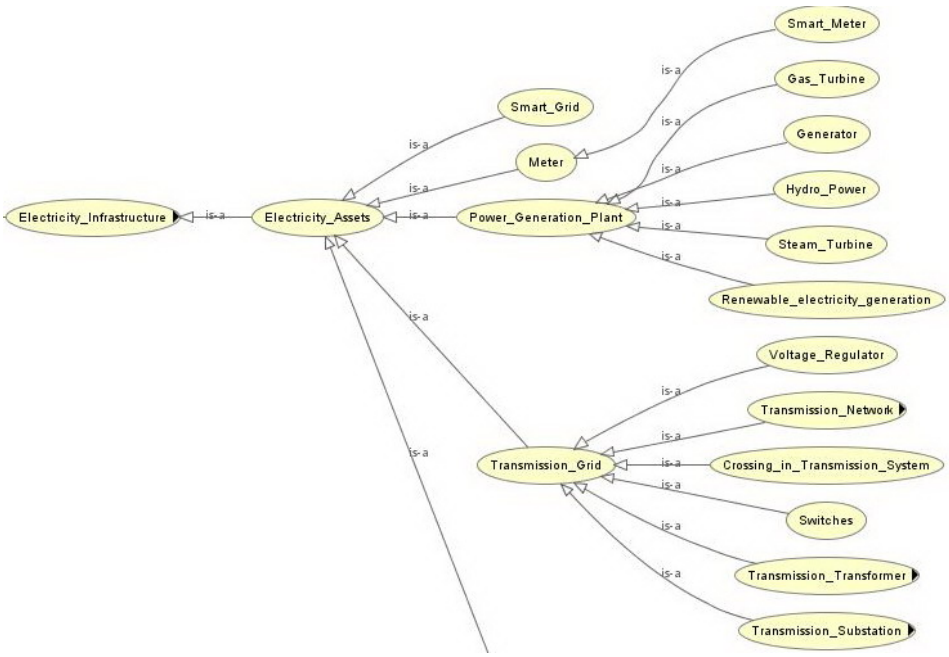


**Figure 3: Portion of the Physical Asset sub-ontology for Electricity Infrastructure**

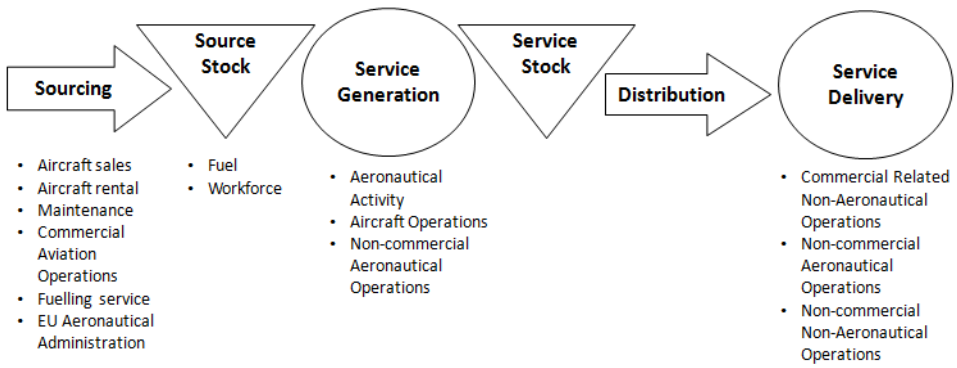


**Figure 4: General Service delivery process (Air transport functions used as an example)**

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 (Colquhoun & Baines, 1991). This formalism allows the construction of models comprising system functions (activities, actions, processes, and operations), functional relationships, and data (information or objects) that support systems integration (IDEF∅, 1993). More specifically, a 'function model' is a structured representation of the functions, activities or processes within the modelled system or subject area. It relates classes to its inputs (e.g. requirements, materials), mechanisms (e.g. resources, assets), controls (e.g. plans, legislations, monitoring) and outputs (e.g. functions, services).

In the context of this work, the IDEF∅ nomenclature is used to specify relations among classes, belonging to both the physical and functional ontologies, in terms of:

- input: entity X is *input to* entity Y (or, entity Y *has input* entity X), e.g. the output of a function or an operations activity is the input of another one;

- mechanism: entity X *is mechanism of* entity Y (or, entity Y *has mechanism* X);
- control: entity X *controls* entity Y (or, entity Y *is controlled by* entity X):
- output: entity X *delivers* entity Y (or, entity Y *is delivered by* entity X).

In our application IDEF∅ relates classes to its **inputs** (e.g. requirements, materials) and **outputs** (e.g. functions, services) – white boxes; **mechanisms** (e.g. resources, assets) – blue boxes; and **controls** (e.g. plans, legislations, monitoring) – red boxes. Bold circles represent connections between different phases of service delivery process. An example of links (relations) between Assets and/or Functions within the service delivery process in represented in Figure 5 where *Service Generation* stage within Air transport sector has been used as an example.

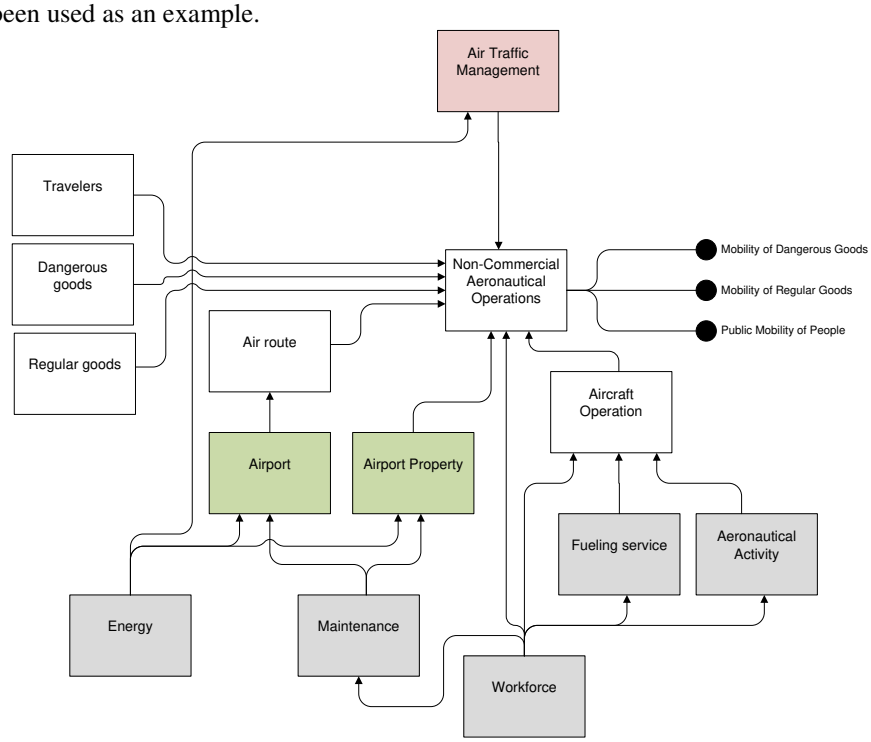


**Figure 5: Service generation stage in Air transport sector**

**Hazards & Threats Ontology**

Hazard and Threats (H&T) Ontology aims at characterising different typologies of events, in a systematic way, to be merged in a federation of ontologies enabling a first-order recognition of all the possible hazards and threats that can affect or destroy a generic CI; and all the possible infrastructure that can be affected by a specific hazard or threat.
As for the Hazards and Threats (H&T) Ontology, there is no standardized form of data collection. However, countries have collected a lot of information on hazards in various databases at international, country, regional and local levels.

The H&T 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 6):

- **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 7.
- **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
- **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 CI can be impacted and the relevant effects.
- **When and Where** the hazard can occur? *Spatial and temporal attributes sub-ontology*.

To be useful for understanding vulnerabilities, hazards and threats need to be characterised in some detail. In addition to the common attributes, "Modus" has been introduced as a feature to define and simplify in which way a given event occurs and can affect the CI. 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 origins). "Modus" has been used as the link between the ontologies of the CI and H&T, defining CI assets vulnerabilities. Each modus, in turn, can create one or more effects on infrastructure, that is the "Modus effect".

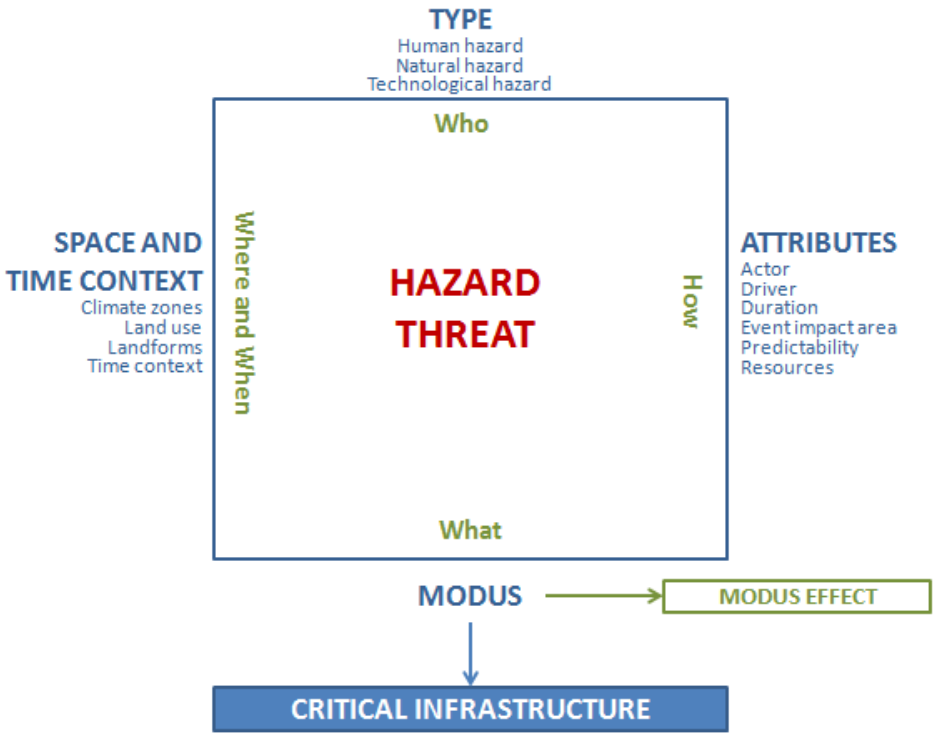

**Figure 6: Conceptual framework of the Hazard & Threat ontology**

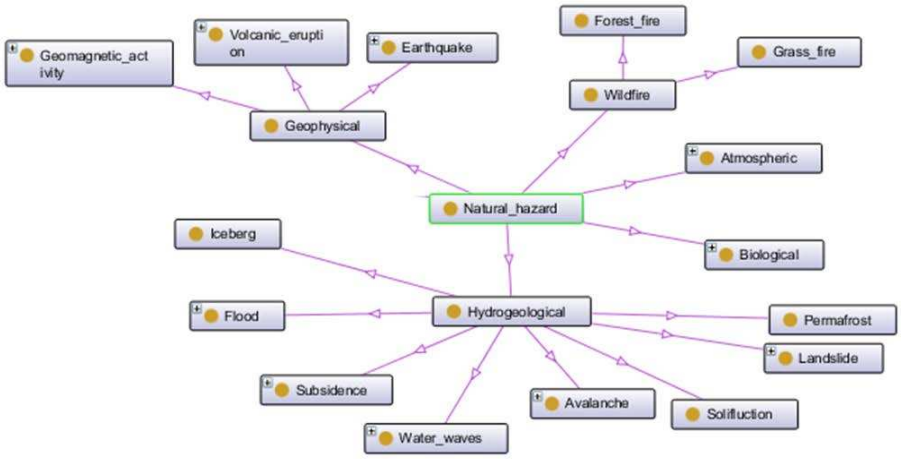


**Figure 7: Partial view of Natural hazards Ontology (first and second levels)**

# 4. Modelling Vulnerabilities and Interdependencies

### Vulnerability Modelling

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*' (Ezell, 2007).

For instance (Figure 8), **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*).

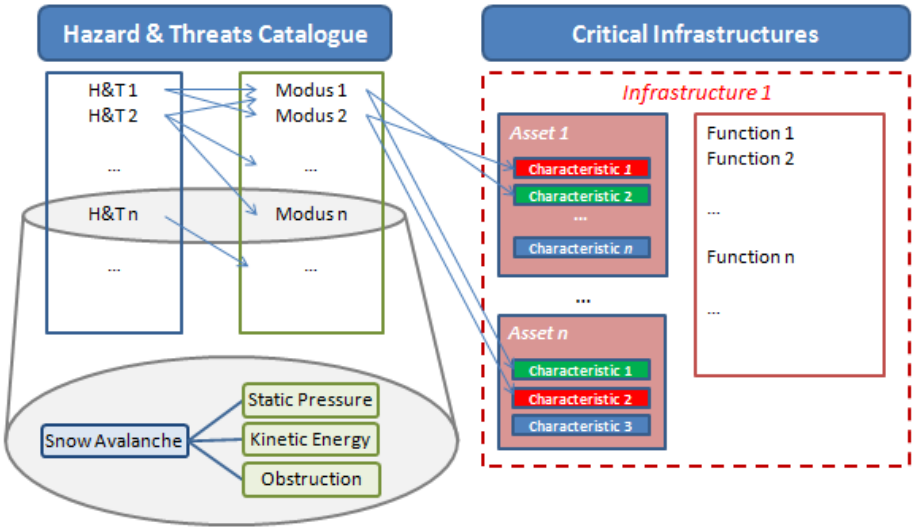


**Figure 8: Impact/Vulnerability modelling (links between H&T and Infrastructure Assets)**

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 (Table 4). 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.

**Table 4: Links between Modus and Assets (partial view)**

| | | | ASSET | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ENERGY | | | | | TRANSPORT | | | |
| | | | Electricity | | | | | Road | | | |
| | | | Power Gen. Plant | Transmission Grid | Distribution System | Smart Grid | Meter | Surface Road | Road Bridge | Road Tunnel | Toll Booth |
| MODUS | Data alteration | Data corruption | X | X | X | X | X | | | | |
| | | Data destruction | X | X | X | X | X | | | | |
| | | Data breach | | | | | | | | | |
| | | Data theft | | | | | | | | | |
| | Ground def. | Transient ground deformation | X | X | X | | | X | X | X | X |
| | | Permanent ground deformation | X | X | X | | | X | X | X | X |
| | Cont amin ation | Air contamination | | | | | | | | | |
| | | Water contamination | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Food contamination | | | | | | | | | |
| | Energy variation | Electrical discharge | | X | C | | X | | | | X |
| | | Ionizing radiation | | | | | | | | | |
| | | Thermal energy | X | | | | X | X | C | X | X |
| | | Electromagnetical disturbance | X | | X | X | X | | | | X |
| | Mechanical action – Wear. | Corrosion | X | X | X | | X | X | C | X | X |
| | | Abrasion | X | C | C | | C | X | C | X | X |
| | Mechanical action – Pressure | Static pressure | X | C | C | | C | | | | |
| | | Overpressure peak | X | C | C | | C | | X | X | X |
| | | Kinetic energy | X | C | C | | C | X | X | X | X |
| | | Dynamic pressure | X | C | C | | C | | X | | |
| | Env. variation | Temperature variation | | | | | | | | | |
| | | Degradation of visibility | | | | | | | | | |
| | | Degradation of air quality | | | | | | | | | |
| | | Degradation of soil quality | | | | | | | | | |
| | | Obstruction/ occupation | | | | | | X | X | X | X |
| | | Unavailability of resources | | | | | | | | | |

**X - Modus affects Asset**
**C - Modus affects Asset conditionally (attribute are required for full specification)**

**Interdependency Modelling**

The main concepts and definitions related to critical infrastructure interdependencies are widely accepted (see, e.g., Rinaldi et al., 2001). A proper modelling of all types of interdependencies is needed to comprehensively cover all the possible vulnerabilities and risks affecting CI.

**Geographic interdependency** occurs if a local environmental event creates state changes in infrastructures (Rinaldi et al., 2001). 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 9).

**Functional (or Physical) interdependency** is a physical reliance on material flow from one infrastructure to another (Rinaldi et al., 2001). 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).

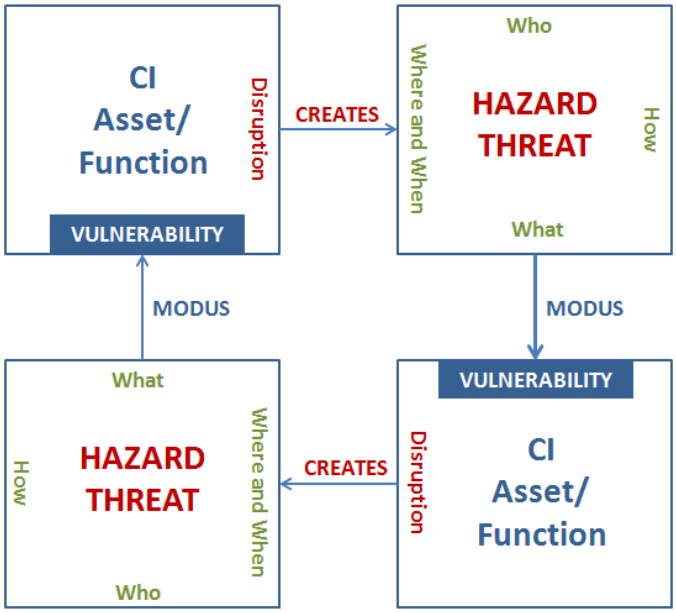


**Figure 9: Conceptual modelling of geographical interdependency**

**Cyber interdependency** occurs if the state of an infrastructure depends on information transfer between infrastructures (e.g. SCADA, communications, monitoring, controlling) (Rinaldi et al., 2001). 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.

# 5. Validation process

**Validation of ontologies**

In the first phase, 30 experts (summary in Table 5) were invited to review the Critical Infrastructure ontologies on assets and functions, including their topology within the service delivery process. Experts have been provided with an evaluation template (available on request) to systematically collect their comments, revisions and recommendations, such as:

- Doubts on the clarity of, or different nomenclature and description for assets and functions;
- Missing relevant asset and/or function items;
- Not relevant asset and/or function items (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. Each expert validated one or two sub-ontologies in her/his area of expertise.

**Table 5: Review from international experts**

| Infrastructure | CI Operator | Government | Research/ | Total |
|---|---|---|---|---|

| | | | Consultancy | |
|---|---|---|---|---|
| Energy | 9 | | 1 | **10** |
| Telecom | 3 | | 1 | **4** |
| Transport | 5 | 5 | 4 | **14** |
| Water | 2 | | | **2** |
| **Total** | **19** | **5** | **6** | **30** |

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 that 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 model.

**Implementation of the model into a software tool**

After validation, the full set of ontologies with related vulnerability and interdependency models have been implemented into a software, as the final usable tool intended to support the analyst in consulting the ontologies and generating a set of relevant disruption scenarios. The software allows selecting a combination of different types of infrastructures (and their assets) as targets, different environments and interdependencies, in order to characterize the types of potential Hazard and Threat impacts to be considered in a scenario.
It is principally intended for two types of users – *Critical Infrastructures managers/operators* and *National/Local Authorities* (*Civil Protection operators).* The former are generally more interested in evaluating vulnerabilities – and related disruption scenarios – of their own infrastructure when put in certain environment and coupled with other infrastructure with specific characteristics; the latter are more interested in creating cases to analyse the spectrum of relevant disruption scenarios for all the vital infrastructures serving a certain geographical area.

# 6. Conclusions

Classification of hazard evolves along with the social progress and at the same time highly depends on interaction of different systems – natural, social, technical. As for the dealing with CI, relationships between entities (assets and functions) matter as much as their properties. Therefore we need to improve by moving from a taxonomy-based approach (classification) to an ontology-based approach which is able to capture complex relationships between concepts (and taxonomies). The advantage of an ontological approach to disruption scenario generation for CI goes beyond 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. Indirect benefits are also expected, in terms of quality of shared information among actors, thanks to a standardised nomenclature and modelling of CI assets, functions and vulnerabilities.

The present study aimed at assisting Authorities and CI Operators to get comprehensive information of all potential disruption scenarios relevant for CIP-R. It was achieved through the development of:

- A generalised and standardised specification framework for CI systems and services (CI Ontology);

- A generalised and standardised all-hazards catalogue for CI (Hazard & Treat Ontology); and,
- An improved scenario generation process where main vulnerabilities and interdependencies are taken into consideration.

The proposed model offers a systematic and exhaustive analysis of threats and vulnerabilities, and a more consistent way for the generation of plausible and relevant disruption scenarios. Starting from a comprehensive Hazard & Threat list and assets selected by the analyst, the software tool can also automatically perform Vulnerability Analysis (i.e. Asset vs. Threat applicability). Furthermore, the tool also allows the deployment of cause-effect mechanisms based on vulnerability and interdependency modelling and subsequent mapping of critical functions and processes (enabled by built-in topologies).The final validation of the software tool should include pilot testing of the scenario generation process in two different application contexts – single infrastructure/organisation operations and heterogeneous dependent CI systems within a regional area. Its contribution to current practices on Risk Identification and Analysis process and comprehensive preparedness planning should be empirically confirmed.

The contribution of the study to the general body of knowledge consists of publicly available integrated ontologies covering relevant domains when it comes to scenario identification. It enables an easy description of CI systems and their behaviour in face of H&T and under influence of interdependencies. Integration of this work with ontologies for inter-organisational information sharing presents a good opportunity for the development of a comprehensive Emergency Management ontology for CI.

However, the proposed integrated ontology suffers from some limitations. The main one is a detailed modelling of 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 (Rinaldi et al., 2001). This category may contain policy, legal or regulatory regimes, economic systems and trends, social and human factors etc., making it very complex and uneasy to be properly addressed via ontology development. Another limitation is manifested though weak abilities in geo specification and description of CI (partial modelling of geo interdependencies). Future planned activities include integration of Geographic Information System (GIS) that will enable visualisation as well as spatial representation of assets, systems and threats. We also have to consider that the level of detail that the model does not take into account is the probability of a threat occurrence.

## Acknowledgment

The present work summarizes the theoretical and methodological developments carried out under the THREVI2 research project (www.threvi2.eu), which has been co-funded by DG Home Affairs of the European Commission, under CIPS/ISEC Work Programme. The financial support is gratefully acknowledged.

## References

Abbott, Patrick L., 1996, *Natural Disasters*. Wm. C. Brown Publishing Co., 438 pp.

ADRC, CRED, GRIP, LA RED, MUNICH RE, UNDP (2008), Disaster Loss Database Standards Prepared by the Working Group on Disaster Data, September 2008, Global Risk Identification Programme (GRIP) Bureau for Crisis Prevention and Recovery (BCPR) United Nations Development Programme (UNDP) 11-13, chemin des Anémones, Châtelaine, CH-1219 Geneva, Switzerland, http://www.gripweb.org

Alexander, D.E. 1993. *Natural Disasters*. University College London Press, London, and Kluwer Academic Publishers, Dordrecht and Boston, 632 pp.

Babitski, G., Bergweiler, S., Grebner, O., Oberle, D., Paulheim, H., & Probst, F. (2011). SoKNOS–Using Semantic Technologies in Disaster Management Software. In *The Semanic Web: Research and Applications* (pp. 183-197). Springer Berlin Heidelberg.

Beck, U., (1992) *Risk Society: Towards a New Modernity*. New Delhi: Sage. (Translated from the German Risikogesellschaft) 1986.

Bénaben, F., Hanachi, C., Lauras, M., Couget, P., & Chapurlat, V. (2008, May). A metamodel and its ontology to guide crisis characterization and its collaborative management. In *Proc. 5th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2008)*.

Broberg G (2005) Tsunamin i Lissabon (The Tsunami in Lisbon) (in Swedish). Bokförlaget Atlantis AB, Stockholm

Broberg G, Nordin S (eds.) (2000) Risk och historia. Sex uppsatser om katastrofer och livets vanskligheter (Risk and history. Six essays about catastrophes and the risks in life) (in Swedish). Ugglan 14, Avdelningen för idé- och lärdomshistoria, Lund university, Lund

Burton, I., Kates, R.W., White, G.F., 1993. *The Environment as Hazard*. 2nd Edition. Guilford Press, New York and London, 290pp.

CATANAT Observatoire permanent des catastrophes naturelles et des risques naturels, http://www.catnat.net

Coburn, A.W.; Bowman, G.; Ruffle, S.J.; Foulser-Piggott, R.; Ralph, D.; Tuveson, M.; 2014, A Taxonomy of Threats for Complex Risk Management, Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

Coch, N.E., 1995. Geohards: Natural and Human. Prentice-Hall, Englewood Cliffs, 481pp.

Colquhoun, G. J. & Baines, R. W. (1991). A generic IDEFO model of process planning. *The International Journal of Production Research*, *29*(11), 2239-2257.

DISASTER project website (2014) http://disaster-fp7.eu/node/21

Eagleman, J. (1983) *Severe and Unusual Weather.* Van Nostrand Reinhold.

ENISA (2009) "*Gaps in standardisation related to resilience of communication networks*"

European Commission (2000). *Communication from the Commission on the precautionary principle* (COM/2000/0001).

European Council (2008), Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union.

Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, *27*(3), 571-583.

Glade, T. & D.E. Alexander (2013), *Classification of Natural Disasters*, Encyclopedia of Natural Hazards, Encyclopedia of Earth Sciences Series 2013, pp 78-82

Grolinger, K., Capretz, M.A.M., Shypanski, A. & Gill, G.S. (2011) Federated critical infrastructure simulators: Towards ontologies for support of collaboration, *2011 24th CCECE conference*, Niagara Falls, ON, 001503-001506.

Gruber. T. R. (1993) "*A translation approach to portable ontologies*" Knowledge Acquisition, 5(2):199-220. http://www-ksl.stanford.edu/kst/what-is-an-ontology.html

Grüninger, M. & Fox. M. S. (1995) "*Methodology for the design and evaluation of ontologies*", Technical Report, University of Toronto, Toronto, Canada.

Guha-Sapir, D., R. Below, Ph. Hoyois - EM-DAT: International Disaster Database – www.emdat.be – Université Catholique de Louvain – Brussels – Belgium. http://www.emdat.be/new-classification

*Integration Definition for Function Modeling (IDEF∅) Standard* (1993), Draft Federal Information Processing Standards Publication 183.

ISyCri Project Website http://www.irit.fr/isycri/eng/presentation.html

Lacy, L., & Gerber, W. (2004, December). Potential modeling and simulation applications of the web ontology language-OWL. In *Proceedings of the 2004 Winter Simulation Conference,* (Vol. 1). IEEE.

Lee, S.W. & Yavagal, D., "GenOM User's Guide," Technical Report TR-SIS-NISE-04-01, Knowledge Intensive Software Engineering Research Group, Dept. of Software and Information Systems, UNC Charlotte, 2004.

Lindell, M. K., Prater, C. S., and Perry, R. W. 2006. Fundamentals of Emergency Management - Chapter 5 Principal hazards in the united states, Emmitsburg, MD: Federal Emergency Management Agency Emergency Management Institute. Available at www.training.fema.gov/EMIWeb/edu/fem.asp

Liu, S., Shaw, D. & Brewster, C. (2013, May). Ontologies for Crisis Management: A Review of State of the Art in Ontology Design and Usability. In *Proceedings of the ISCRAM 2013 conference, 12-15 May, 2013*.

Lorenz, B., Ohlbach, H. J., & Yang, L. (2005). Ontology of transportation networks.

Masolo, C., Borgo, S., Gangemi, A., Guarino, N., Oltramari, A. (2003): WonderWeb Deliverable D18: Ontology Library (final)

Masucci, V., Adinolfi, F., Servillo, P., Dipoppa, G., & Tofani, A. (2009). Ontology-based critical infrastructure modeling and simulation. In *Critical Infrastructure Protection III* (pp. 229-242). Springer Berlin Heidelberg.

McNally, R. K., Lee, S. W., Yavagal, D., & Xiang, W. N. (2007). Learning the critical infrastructure interdependencies through an ontology-based information system. *ENVIRONMENT AND PLANNING B PLANNING AND DESIGN*, *34*(6), 1103.

Munich RE, https://www.munichre.com/touch/portal/en/touch_login/index.html

Noy, N. F., & McGuinness, D. L. (2001). *Ontology development 101: A guide to creating your first ontology,* Stanford University, Stanford (CA), USA

OASIS (2009). Disaster and emergency management - Shared situation awareness. www.oasis-open.org

Odén B., (2009), Risks in the Past and Present, Book chapter in the *Risks in Technological Systems*, Göran Grimvall, Åke J. Holmgren Per Jacobsson, Torbjörn Thedéen Editors, Springer-Verlag London.

Oxford Dictionary (2012). *Oxford dictionary of English*. Online version.

Ouyang, M. (2014) 'Review on modeling and simulation of interdependent critical infrastructure systems', *Reliability Engineering & System Safety*, January, Vol. 121, pp.43–60.

PCCIP (1996) The US Presidential Commission on Critical Infrastructure Protection (PCCIP), July, 15, 1996 President Clinton Executive Order 13010 establishing the President's Commission on Critical Infrastructures Protection.

PCCIP (1997) President's Commission on Critical Infrastructure Protection – PCCIP (1997), *Critical Foundations: Protecting America's Infrastructure*.

Protégé official website: http://protege.stanford.edu/

Quarantelli, E.L. (1984). Perceptions and reactions to emergency warnings of sudden hazards. Ekestics, 309, 511–515

Quarantelli, E.L. (ed.). 1998. What Is A Disaster? Perspectives on the Question. London and NY: Routledge.

Rahman, H. A., Armstrong, M., Mao, D., & Marti, J. R. (2008, October). I2Sim: a matrix-partition based framework for critical infrastructure interdependencies simulation. In *Electric Power Conference, 2008.* Canada (pp. 1-8). IEEE

Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.K. (2001). *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*. IEEE Control Systems Mag. 21: 11-25.

Rome, E., Bologna, S., Gelenbe, E., Luiijf, E. H., & Masucci, V. (2009, July). DIESIS: an interoperable European federated simulation network for critical infrastructures. In *Proceedings of the 2009 SISO European Simulation Interoperability Workshop* (pp. 139-146). Society for Modeling & Simulation International.

Rubin, A., Hein, C., & Prasad, G. (2006). Multi-Simulation Interface (MSI) for Complex Simulations.

Smith, K. (2000). *Environmental Hazards-Assessing Risk and Reducing Disasters*, Routledge, 3rd Edition, 381 p.

Smith, K., (1985), *"Environmental issues",* Progress in Physical Geography March 1985 9: 82-88,

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30).

Swiss RE, http://www.swissre.com

Thywissen, K. (2006), *Components of Risk a Comparative Glossary, United Nations University* – Institute of Environment and Human Security

Tobin, G.A. and Montz, B.E. 1997. *Natural Hazards, Explanation and Integration.* New York, London: Guildford Press.

Tofani, A., Castorini, E., Palazzari, P., Usov, A., Beyel, C., Rome, E., & Servillo, P. (2010). An ontological approach to simulate critical infrastructures. *Journal of computational science*, 1(4), 221-228.

UN/ISDR (2002). Living with Risk – A Global Review of Disaster Reduction Initiatives (Preliminary Version). Geneva, Switzerland: United Nations ISDR. Downloaded from: http://wwwunisdr.org.

UN/ISDR (2004). Glossary. Basic Terms of Disaster Risk Reduction. http://www.unisdr.org/eng/library/lib-terminology-eng.htm

University of Cambridge, THREAT OBSERVATORY - Taxonomy of Macro-Threats: A framework for categorising socio-economic threats and collecting structured data, http://cambridgeriskframework.com/taxonomy

Vlacheas, P. T., Stavroulaki, V., Demestichas, P., Cadzowm S., Gorniak, S. & Ikonomou, D. (2011, December). *Ontology and taxonomies of resilience.* The European Network and Information Security Agency (ENISA).

W3C (2009). http://www.w3.org/2005/Incubator/eiif/XGR-Framework-20090806/