An Ontology-based Approach to Vulnerability and Interdependency modelling for Critical Infrastructure Systems

P. Trucco & B. Petrenj
Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy

ABSTRACT: The systematic and complete identification of meaningful accident scenarios for Critical Infrastructure is still one of the major challenges to achieve higher resilience performance. THREVI2 project has been designed to answer this need by developing a comprehensive and multi-dimensional all-hazards catalogue for CI. Specific objectives are: to develop and elaborate three coordinated ontologies (Hazards & Threats, CIs topologies, CIs Interdependencies); to merge them by existing vulnerability models; and to develop a dedicated software tool for scenarios generation to support different end-users (e.g. authorities and operators). 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.

1 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 then merged through specific vulnerability and dependency entities.

The preceding paper (Trucco et al., 2014) presented the ontology development process adopted in the project and described the main features of the final integrated set of ontologies. In this paper we will briefly recall on the main results regarding CI and H&T ontologies and build upon the previous work. The advancements include modelling of vulnerabilities and interdependencies and progress in the development of the supporting software tool (PATHFINDER).

The paper is organised as follows. The following section explains the ontological approach to CI risk assessment and gives an overview of the two main ontologies. Section 3 explains the approach to modelling vulnerabilities and different types of interdependencies. In Section 4 the PATHFINDER software tool is presented, including some examples. Section 5 summarises the most important findings and their practical implications, the remaining issues, and the path forward.

2 ONTOLOGICAL APPROACH TO SCENARIO GENERATION

2.1 *Methodology*

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

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.

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*. [5]

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.

2.2 *CI Ontology*

For the Critical Infrastructure System Ontology, the sectors covered include *Energy*, *Transport*, *Water* and *Telecommunications*, for a total of 11 different infrastructure subsectors (Figure 1).

The CI System 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 ontologies description. At the end 62 documents have been used to develop the final 22 sub-ontologies

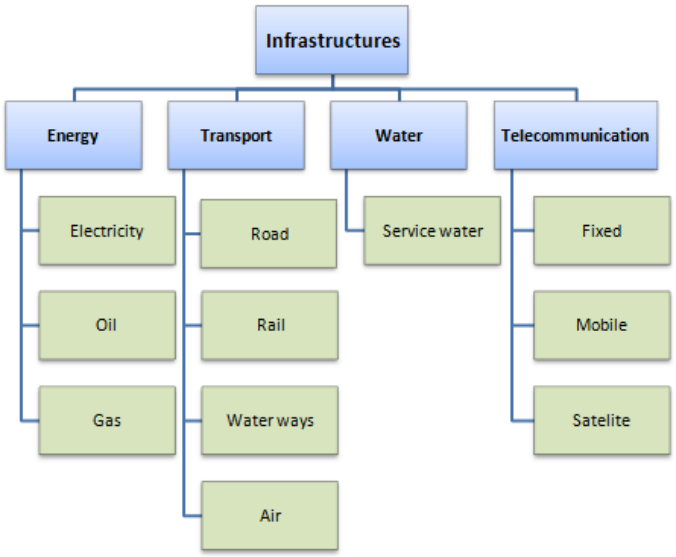

Figure 1. Covered infrastructure sectors and subsectors

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) which were subsequently linked within the service delivery process.

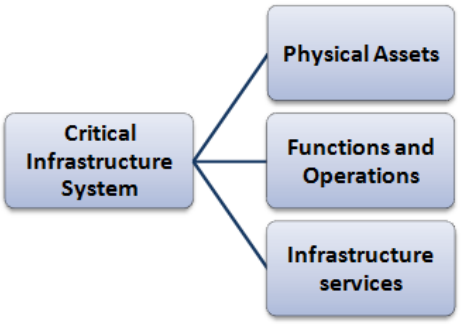

Figure 2. Critical Infrastructure ontology framework

2.3 *Hazards &Threats Ontology*

Hazard and Threats (H&T) Ontology aims to systematically characterise different typologies of events to be used for the development of the PATH-FINDER 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.

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 (RGS, 2013).

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), 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 defense or economic security. A threat may be an individual, an organization, or a "nation" (PCCIP, 1997) In publications on security of IT systems, threats are seen as the potential for a particular threat-source to successfully exploit a particular vulnerability, which means that 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 (RGS, 2013).

"*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 (RGS, 2013).

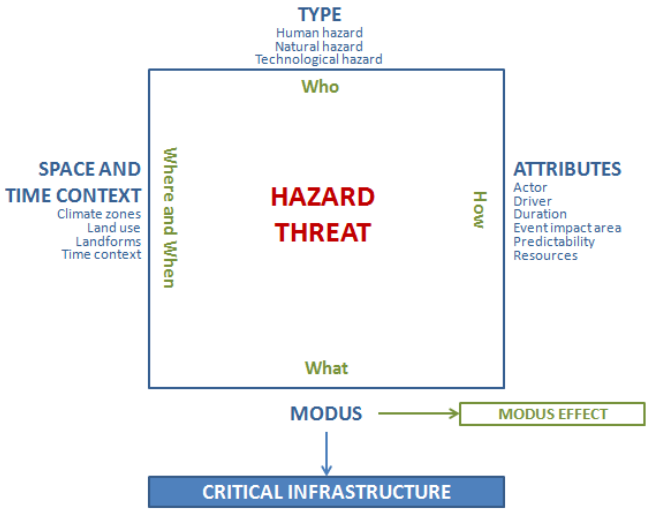

Figure 3. Hazard & Threat ontology

To be helpful in understanding hazards and threats in light of vulnerabilities and risk, need to be characterized in some detail (Figure 3). 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 has been used as the link between the ontologies of the CI and H&T, defining CI assets vulnerabilities.

3 MODELLING VULNERABILITIES & INTERDEPENDENCIES

3.1 *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 5), **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*).

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 (Annex A). 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.

3.2 *Interdependencies modelling*

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 (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 4).

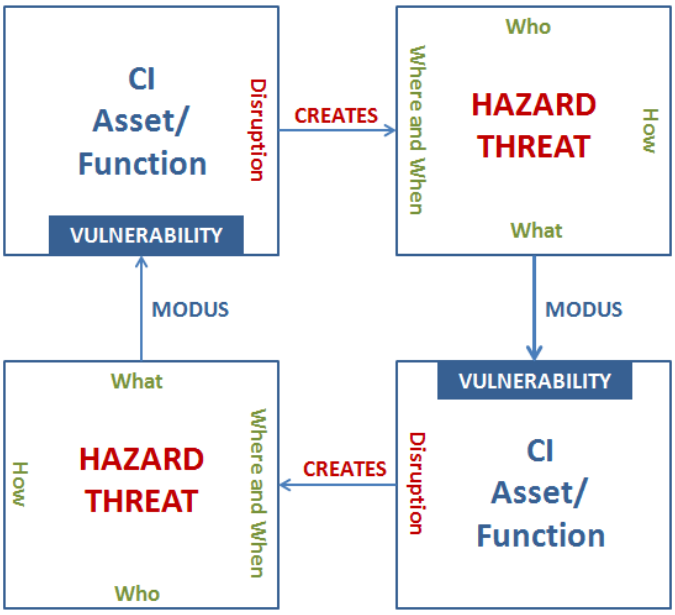

Figure 4. Modelling of geographical interdependency

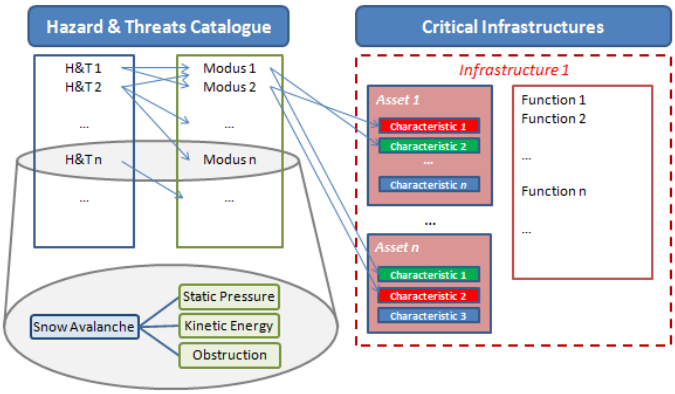

Figure 5. Impact/Vulnerability modelling (links between H&T and Infrastructure Assets)

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).

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.

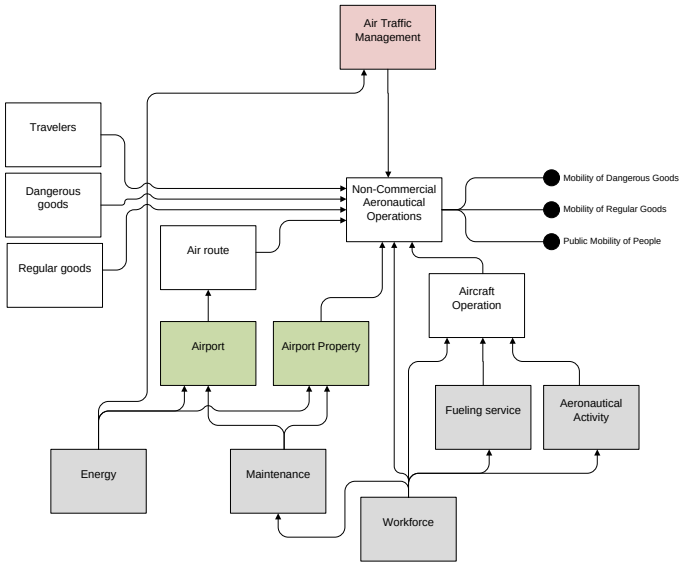

Figure 6. Service generation stage in Air transport sector

3.3 *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.

4 PATHFINDER SOFTWARE TOOL

The main output of the project is the PATHFINDER tool, principally planned for two types of users – *Critical Infrastructures managers/operators* and *National/Local Authorities* (*Civil Protection operators).* The general approach for identifying vulnerability paths is given in Figure 7, but may vary according to different users' needs.

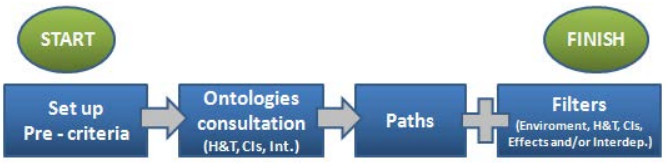

Figure 7. PATHFINDER Tool utilization process.

It will be possible to use the tool in two main modes (Figure 8):

– *WIZARD mode* – the order of setting the criteria (filters) necessary to delineate paths is defined. In this use mode a minimal cut set of selection criteria is defined. The user browses through the pages in an established order, that will be different according to the user type.
– *FREE mode* – the user can browse through the pages in free order without limitation (for expert users).

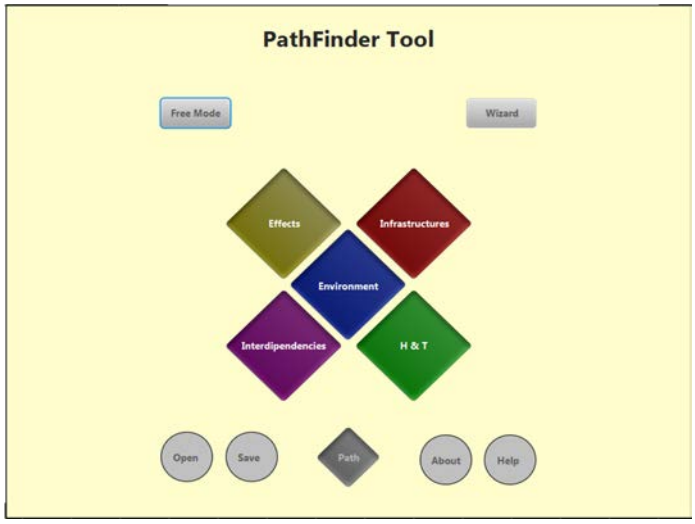

Figure 8. PATHFINDER Tool: main window

Other controls include (Figure 8):

– *Setup pages* (middle part of the screen) that contain all the set-up options.
– *Path Button* which launches the final query, and will remain disabled until a minimal set-up will be done. Effects are the impact modes through which the hazards hit the infrastructures. In Infrastructures page the user can set one or more infrastructure he is interested in. In Environments page the user can set one or more environments, which can be associated with infrastructure or

used for hazards screening. In Hazards and Threat page the user can define screening criteria for hazards and their attributes. (Figure 9)

– *Standard options* – enabling user to save on his computer the file containing the current set-up, open an existing file or use the guide.

Figure 10 displays an example of Human Hazards selection list (as a sub-ontology of H&T)

The PATHFINDER tool has been tested in two pilot applications in collaboration with one EU Member State and one relevant CI operator.

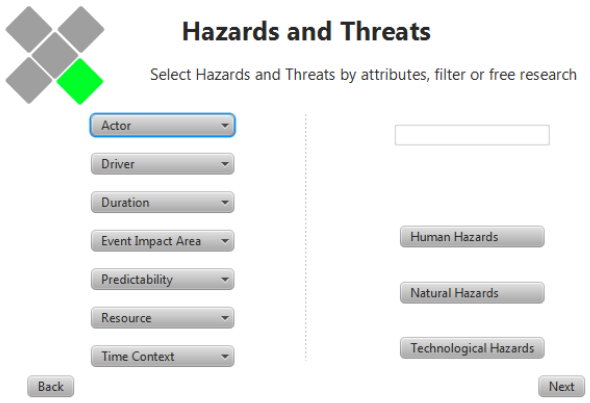

Figure 9. PATHFINDER Tool: Hazards & Threats main page

Figure 10. PATHFINDER Tool: Human Hazards selection list

5 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.

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 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.

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 (Rinaldi et al., 2001). 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.

REFERENCES

Trucco, P., Petrenj, B. & De Ambroggi, M. (2014) "Ontology-based Disruption Scenario Generation for Critical Infrastructure", Proceedings of *Probabilistic Safety Assessment and Management conference – PSAM12*, June 2014, Honolulu, Hawaii.

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

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

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

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

Risk Governance Solutions (RGS) 2013. THREVI2 Project – Deliverable 2.1. "*Hazard and Threat Taxonomy and Ontology*"

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

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

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.

ANNEX A: LINKS BETWEEN ASSETS AND MODUS

X - Modus affects Asset
C - Modus affects Asset conditionally (attribute required)

				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 diturbance	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	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							
		Oil	Oil plant and equipment	X	X			X	X						X	X	X	X	X	X	X	X					X	
			Oilholder station	X	X			X	X						X	X	X	X	X	X	X	X							
			Pressure Regulating Installation (PRI) station	X	X			X	X						X	X	X	X	X	X	X	X							
			Oil system	X	X			X	X						C	X	X	C	C	C	C	C							
		Gas	Gas plant and equipment	X	X			X	X						X	X	X	X	X	X	X	X					X	
			Gasholder station	X	X			X	X						X	X	X	X	X	X	X	X							
			Pressure Regulating Installation (PRI) station	X	X			X	X						X	X	X	X	X	X	X	X							
			Gas system	X	X			X	X						C	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	
		Rail	Rail Station					X	X																		X	
			Surface rail					X	X																		X	
			Rail bridge					X	X						C		C	C	X	X	X	X					X	
			Rail tunnel					X	X						X		X	X		X	X						X	
			Operating property					X	X						X		X	X		X	X	X					X	
			Non-operating property					X	X						X		X	X		X	X						X	
			Train														X		X	X	X	X					X	
		Air	Airport	X	X			X	X				X	X	X	X							X	X			X	
			Airport Property					X	X																		X	
			Aircraft														X		X	X	X	X					X	
		Water	Port					X	X						X	X			X	X	X	X					X	
			Ship														X		X	X	X	X					X	

(*continued*)

			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 diturbance	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	SERVICE WATER	Gaging station	X	X			X	X						X	X	X	X	X	X	X	X						
		Water abstraction and raw water transfer system	X	X			X	X						C	X	X	C	C	C	C	C					C	
		Water-Treatment system	X	X			X	X						X	X	X	X	X	X	X	X	X				X	
		Water main pipeline	X	X			X	X						C		X	C	C	C	C	C						
	COMMON ASSETS AND RESOURCES	SCADA	X	X								X			X												
		TRAVELERS							X	X	X																	X
		WORKFORCE							X	X	X																	X
		ENERGY																										X
		REGULAR GOODS												X								X						X
		DANGEROUS GOODS										X	X	X				X	X	X	X	X						X
		INFORMATION	X	X	X	X									X													X