Reliability Engineering and System Safety 105 (2012) 51–63

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures

P. Trucco*, E. Cagno, M. De Ambroggi

Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy

ARTICLE INFO

Article history:
Received 31 March 2011
Received in revised form
2 August 2011
Accepted 1 December 2011
Available online 9 December 2011

Keywords:
Critical Infrastructures
Interoperability
Vulnerability
Time-dependent
Functional model

ABSTRACT

The paper describes a new integrated formalism for the dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures at regional level. The model assesses the propagation of impacts in terms of disservice due to a wide set of threats. The disservice can be propagated within the same infrastructure or to other CIs by means of the interdependence model, which is able to represent physical, cybernetic, geographic as well as logical interdependencies and also the shift of the demand between two infrastructures that can provide the same or fully/partially replaceable service. The model is dynamic, since both the impact of the specific threat on a generic infrastructure node and the inoperability functions are time-dependent. A pilot study has been carried in the metropolitan area of the province of Milan, considering the Critical Infrastructures referred to the transportation system.

1. Introduction

Critical Infrastructures are those assets, systems or parts thereof, which is essential in the provision of services that are deemed to be vital for the functioning of society, "including the supply chain, health, safety, security and economic or social well-being of the people". Beside this definition reported in the EC Directive 114/08/EC [1] many other slightly different definitions of CIs may be found in literature (e.g., [2,3]). Whereas an infrastructure can be considered an integrated socio-technical system to deliver a certain service to society, the concept of criticality remains discussed. However, despite their criticality level, such infrastructures can be destroyed or disrupted by severe technical-organisational failures, natural disasters or deliberate acts of terrorism, resulting in possible significant impacts on society.

Existing approaches to vulnerability and interdependency analysis of complex CIs networks refer to different scientific fields, e.g. physical network modelling, network economics, etc. [2,3], yet each of them focuses only on one aspect of the problem and does not provide a complete representation of all the relevant factors involved. If on one hand specific modelling techniques may result particularly effective when applied to specific target problems and scopes (e.g. physical network modelling applied to system control and recovery procedures), on the other hand the same techniques are hardly useful when different system perspectives need to be integrated in the same approach. This is the case, for example, of the modelling and decision support needs of Critical Infrastructure Protection Programmes defined at regional or local level.

1.1. The PReSIC programme

In Italy, private and public operators of critical services are already committed with investments and procedures to guarantee system safety and service continuity. Under this point of view, when homeland security and defence are concerned, actions and responsibilities are established at a national level. Nevertheless, the Lombardy Region Administration realised that thanks to better information sharing processes among actors – concerning threats, vulnerabilities and crisis management – it would be possible to enhance the efficacy of invested resources and the safety of citizens as well. Indeed, the Lombardy Region is one of the most industrialised regions in Europe and its long range competitiveness and development rely on complex and sophisticated infrastructure systems.

Thus, the objective of the Lombardy Region Administration it is not to add a new level of control or decision-making in the context of national homeland security system. On the contrary, Lombardy Region is acting to promote extended and improved collaborative processes among actors (public and private), able to support operators of CIs in preventing and manage service disruptions deriving from events that by nature develop beyond the boundaries of a single infrastructure or require the joint intervention of more than one organisation.

Starting from this subsidiary approach the Lombardy Region Administration started a preliminary and explorative study

* Corresponding author.
E-mail address: paolo.trucco@polimi.it (P. Trucco).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.12.003

dealing with the definition and evaluation of an integrated system to set up the inter organisational collaborations within prevention, monitoring and emergency management processes for regional CIs. In line with the contents of the Directive 114/EC/2008, the action has been focused on energy and transport infrastructures. Nevertheless, the boundaries of the system might evolve in the near future to include new actors and offer new functions according to an evolving scenario of increasing collaboration, subjected to the demonstration of effectiveness and real benefits for all the actors involved. The programme, named PReSIC, is in charge to a composite team of industrial, professional and academic partners. To actually meet the needs of CIs operators and other stakeholders, the activities included in the first phase of PReSIC were

- inventory of CIs nodes and interdependency analysis, on a regional scale, due to potential accidents and service disruption events requiring synergic and coordinated responses;
- deployment of requirements for a Network Enabled Operations (NEO) model adopting NAF (NATO Architecture Framework) (NATO 2007);
- in depth analysis of juridical aspects and institutional constraints to guarantee the correct interaction and responsibility allocation among the actors of the system.

The first point of the PReSIC workplan required to identify the most appropriate modelling strategy for both the documentation of critical nodes and the development of thorough interdependency analyses.

Similar other regional or local initiatives have been already started in the recent years [4–8], and some others are trying to start, all sharing the same needs in terms of vulnerability and interdependency modelling and analysis of relevant infrastructure systems. In addition, until recently, network security and service continuity was a matter of concern mainly for the operators. As a consequence, policy-makers and public managers have to tackle infrastructure protection at a higher level and need accurate decision support tools to address an issue, which is not just technical but also societal. As it will be documented in the next paragraph, to our knowledge there is no documented interdisciplinary methodology that would enable this kind of analysis.

The paper proposes a new integrated formalism for the functional modelling of vulnerability and interoperability of Critical Infrastructures. The proposed model is dynamic, since both the impact of the specific threat on a generic infrastructure node and the inoperability functions are time-dependent. A pilot study has also been carried out in the metropolitan area of the province of Milan, considering the Critical Infrastructures referred to transportation and mobility services (road, rail, underground, and airport systems).

The paper is organised as follows: in Section 2 a state-of-the-art review on modelling techniques for CIs interdependency analysis is briefly presented and the need for a new functional modelling approach is highlighted. In Sections 3 and 4 the entities and mechanisms of the new proposed formalism are described in detail. Section 5 reports the description and discussion of a pilot application to transport infrastructures in the metropolitan area of Milan (Italy), whereas Section 6 summarises major findings and draws some conclusions.

2. State of art on modelling CI interdependencies—the need of a functional modelling

In the last decade, many approaches to CI Protection have been developed [9,10]. The focus of those works was directed towards

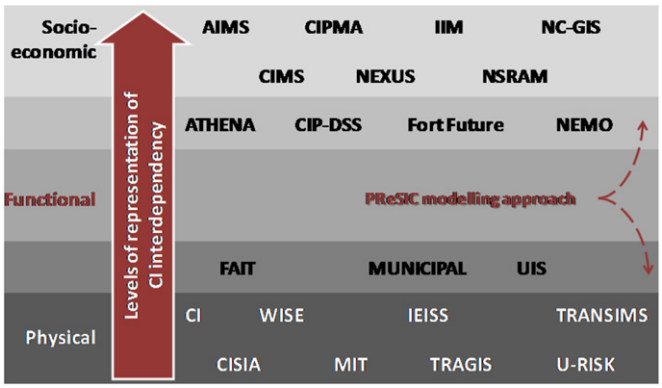

Fig. 1. Classification of models and methodologies for CI interdependency analysis.

three different classes of problems: identifying (e.g. [11]), characterizing (e.g. [12]), and modelling interdependencies between CIs (e.g. [4]). From the analysis of the state of the art comes out that all the documented approaches to interdependency modelling can be classified according to their intended level of analysis. To this end, three levels of description and analysis of interdependencies between CIs have been defined: physical, functional and socio-economic; Fig. 1, shows the corresponding clusters of the most well-known models, techniques and tools.

Considering the objectives and the extension of typical regional plans for Critical Infrastructure Protection (CIP), it is apparent that neither the physical nor the socio-economic levels of representation are adequate. The former, due to a very detailed description of the infrastructure systems, is not able to support the analysis o wide geographic areas and secondly is not suited to tackle logical interdependencies [13]. The latter, on the other hand, is not able to offer an adequate topological representation of the infrastructure systems to be matched with the geographical distribution of service demands. Actually, an application of the IIM model has been proposed for the analysis of underground infrastructures in a urban area [14,15], but this approach resulted to be limited in its scalability properties, and in any case is not able to account for demand variations.

Thus, to better identify the solution able to meet the needs of regional CIP programmes, such as PReSIC, at best, the modelling tools and techniques generally adopted to model interdependencies between CIs were also analysed and compared: Input–Output Model [14–16]; Dynamic Bayesian Networks [17–19]; Intelligent Agent [20,21]; Petri Nets [22,23]; Fuzzy cognitive maps [24]; Markov Chains [25,26]; Systems Dynamics [27].

The techniques have been evaluated considering basic modelling capabilities and particular aspects necessary to achieve the specific purposes of regional-scale CIs modelling:

- taking into account multi-attribute components of the system;
- representing the time dimension;
- incorporating time dependent parameters;
- leading diagnostic and prognostic analysis;
- modelling multi event analysis and the interaction among them;
- representing the effects of particular decision strategies;
- leading probabilistic analysis for the system represented;
- modelling the model the interaction between external events and infrastructure;
- modelling all the types of interdependencies [13];
- accounting for different types of impact over a wide set of targets (citizens, economic activities, CIs, natural and cultural heritages, etc. [28]).

The evaluation of the candidate techniques made apparent that none is able to fully meet all the required capabilities. One alternative solution, suggested and adopted by some authors [29], would be to implement a hybrid modelling strategy (multiformalism), but the weakest point of this strategy is the paramount difficulty to harmonise a wide spectrum of information – coming from different sources, of different nature and level of detail, etc. – that must be processed by different models. The unique practical alternative to multiformalism is the development of an ad-hoc modelling formalism, directly implemented in a software code. It was decided to follow this option mainly because of

- the impossibility to use one of the models already proposed in literature (cf. Fig. 1) for PReSIC purposes and thus for other similar applications;
- the unmanageable complexity of adopting the multiformalism strategy (e.g., [29]) to model CIs interdependency on a regional basis;
- the opportunity to exploit proprietary databases and risk analyses – e.g. PRIM results [30] – through an ad-hoc formalism;
- finally, it has been also considered that the dimensions and perspectives of PReSIC justify the modelling effort.

3. Model definition and properties

The model allows to understand how disturbances or disruptions affecting some CIs spread to the whole network and impact on the society.

The CI network is described through the following conceptual entities: the vulnerable nodes, which represent the CIs in the model, the threat nodes, which introduce disturbances and disruption on the CIs (direct effect of threats on a vulnerable node), and the functional interdependencies (physical, geographical, cyber and logical), which spread the threats affecting a specific CI to the whole network (indirect effect of threats on a vulnerable node).

Fig. 2 shows the symbols used to describe the conceptual entities.

3.1. Vulnerable node

"Vulnerable node" is defined as a large functional part of a CI that assures the satisfaction of a considerable part of service demand at regional or local level (e.g. part of a pipeline network, a railway station, a portion of a highway, an underground line) and that does not need further disaggregation for the sake of the analysis. A vulnerable node has to be homogeneous (i.e. uniform in structure and function with respect to service demand), service self-providing (i.e. a system able to supply a value-added service through own means), and vulnerable (i.e. susceptible to threats that could decrease its functional integrity).

The definition of the k-th vulnerable node requires to specify the following main characteristics:

- name of the vulnerable node;
- name of the related infrastructure;

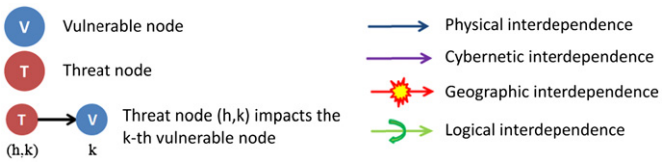

Fig. 2. Symbolism of the proposed formalism.

- type of the service supplied;
- maximum capacity $C_{max}(k)$, i.e. the maximum service the k-th node is able to supply under optimal conditions (the k-th node is undamaged, no threats neither disturbances from the network impact on it, so that it can work properly at its peak);
- standard demand $D_{std}(k,t)$, i.e. the service demand the k-th node is required to supply at time t under standard conditions (actual demand when no threats impact on the CIs network).

The state of the node is characterised by the following parameters:

- actual demand $D_{eff}(k,t)$, i.e. the actual service demand the k-th node is required to supply at time t in actual condition;
- maximum service $S_{max}(k,t)$, i.e. the maximum service the k-th node is able to supply at time t because of threats or disturbances coming from the network;
- actual service $S(k,t)$, i.e. the actual service level the k-th node supplies at time t;
- functional integrity $F(k,t)$: this parameter quantifies how the threats directly impacting on the k-th node reduce its maximum service level $S_{max}(k,t)$ at time t (the direct effect), and it is comprised between 0 (the k-th node is completely blocked) and 1 (optimal state);
- inoperability $I(k,t)$: this parameter quantifies how disturbances coming from the CIs network reduce the maximum service level $S_{max}(k,t)$ of the k-th node at time t (the indirect effect), and it is comprised between 0 (optimal state) and 1 (the k-th node is completely blocked by the disturbances coming from the network);
- disservice $\Delta(k,t)$: it quantifies the percentage inability of the k-th node to meet the actual demand at the time t and it is calculated through the following equation:

$$\Delta(k,t) = \frac{D_{eff}(k,t) - S(k,t)}{D_{eff}(k,t)} \quad (1)$$

It is comprised between 0 (the actual demand is fully satisfied) and 1 (the k-th node does not meet the actual demand at all).

3.2. Threat node

A threat is a generic entity with the potential to be the source of a disturbance or disruption for the considered vulnerable node of a generic CI. The origin of the threat can be whether internal (e.g. a fault) or external (e.g. a natural disaster) to the CI. Threats are modelled through "threat nodes" characterised by the couple (h,k) where h is the type of disturbance or disruption event (e.g. internal technical failure, earthquake) impacting on the k-th vulnerable node.

The model of the threat node is based on two assumptions: (1) the magnitude of the impact of the threat is independent from the specific state of the impacted node; (2) if more threats concurrently impact on one vulnerable node, the overall effect is assessed through the superposition principle (i.e. the sum of the impacts, which would have been caused by each threat independently). This assumption is reasonable since the impact is evaluated in functional (service level) terms and not in physical terms.

A complete definition of a threat node requires to specify the following main characteristics:

- name of the threat node;
- kind of disturbance/disruption (h);
- impacted vulnerable node (k);
- description of the impact;

- functional integrity modulation function $f_{FM(h,k)}(M(h,k))$, i.e. the form of modulation in which the functional integrity of a vulnerable node is varied depending on the percentage intensity $M(h,k)$ of the threat;
- propagation time $\Delta T_P(h,k)$, i.e. the measure of the loss rate of the functional integrity of the k-th node impacted by the h-th event;
- maximum time required for setting-up the intervention $\Delta T_{0max}(h,k)$, i.e. the maximum time required for setting-up a countermeasure after an integrity loss of the k-th node due to the h-th threat;
- maximum recovery time $\Delta T_{R\_max}(h,k)$, i.e. the maximum time window within which the k-th vulnerable node is restored to the level before the h-th event occurs;
- description of the recovery function of the functional integrity (e.g. smooth or step function).

In order to trigger a threat, two parameters have to be defined:

- percentage intensity $M(h,k)$ of the h-th threat impacting on the k-th node, it is comprised between 0 (negligible impact) and 1 (maximum impact);
- time $T_{M0}(h,k)$ at which the threat occurs.

3.3. Modelling of the cause-effect relationship between threats and vulnerable nodes

The threat h, impacting at time $T_{M0}(h,k)$ on the k-th vulnerable node, causes a reduction of its functional integrity $I(k,t)$ and consequently a reduction of the maximum service – $S_{max}(k,t)$ – the node is able to supply. The functional integrity of the k-th node at a generic time t is calculated through the following equation:

$$F(k,t) = F(k,0) - f_{F(h,k)}[M(h,k), T_{M0}(h,k), t] \tag{2}$$

where the reduction depends on the percentage intensity $M(h,k)$ of the threat, the instant $T_{M0}(h,k)$ at which the threat occurs, and the generic time t. The function $f_F(h,k)[M(h,k), T_{M0}(h,k), t]$ is assumed to be calculated as the product between a function of the solely intensity of the threat and a time-dependent function:

$$f_{F(h,k)}[M(h,k), T_{M0}(h,k), t] = f_{FM(h,k)}[M(h,k)] f_{Ft(h,k)}[T_{M0}(h,k), t] \tag{3}$$

$f_{FM(h,k)}$ is called functional integrity modulation function and it allows to define the functional integrity steady reduction after the impact, whereas the function $f_{Ft(h,k)}$ defines the dynamic through which the functional integrity reaches its new steady value. The forms of both the functions $f_{FM(h,k)}$ and $f_{Ft(h,k)}$ have to be properly defined through interviews and work sessions with the operators.

Fig. 3 shows some examples of the functional integrity modulation $f_{FM(h,k)}$ form.

Fig. 3(a) is an example of the $f_{FM(h,k)}$ form in case of a car crash on a three-lane highway: depending on the seriousness of the event, the rescuers may decide to close one lane, two lanes, or the whole carriageway, so that the modulation function has a step form. Fig. 3(b) shows an example of the functional integrity modulation form in case of a natural disaster, such as a flood: the CI does not suffer low-level inundations; when the magnitude crosses a threshold, the higher becomes the flood, the higher is the impact on the CI. Fig. 3(c) is an example of the $f_{FM(h,k)}$ form in case of a fire: for small size fire, the higher the magnitude, the higher the impact; for larger size, the CI is completely blocked.

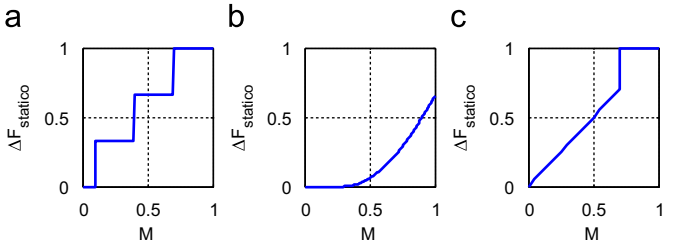

Fig. 3. Examples of the functional integrity modulation $f_{FM(h,k)}(M(h,k))$ form.

The time-dependent function $f_{Ft(h,k)}$ is assumed to be composed of standard functions (constant or exponential decay), so that it can be completely defined through the parameters of the threat node. Before time $T_{M0}(h,k)$, the threat does not influence the vulnerable node, thus the function is zero. The impact is modelled through an exponential decay. It is assumed that the duration of the impact does not depend on percentage intensity $M(h,k)$ of the threat, so that the exponential time constant $\tau_p(h,k)$ is approximately determined through:

$$\tau_P(h,k) \approx \frac{\Delta T_P(h,k)}{5} \tag{4}$$

The time $\Delta T_O(h,k)$ to setting-up countermeasures is assumed to be proportional to the percentage intensity of the threat:

$$\Delta T_O(h,k) = M(h,k)\Delta T_{O\_MAX}(h,k) \tag{5}$$

During time $\Delta T_O(h,k)$ the time-dependent function is constant (its value is obviously one).

The duration of the recovery process $\Delta T_R(h,k)$ is assumed to be proportional to the percentage intensity of the threat $M(h,k)$:

$$\Delta T_R(h,k) = M(h,k)\Delta T_{R\_MAX}(h,k) \tag{6}$$

In case of smooth recovery, the time-dependent function is an exponential decay and its time constant $\tau_R(h,k)$ is approximately determined thorough:

$$\tau_R(h,k) \approx \frac{\Delta T_R(h,k)}{5} \tag{7}$$

In case of step recovery, the function $f_{Ft(h,k)}$ is constant (its value is one) for the whole duration of the recovery process. After the recovery, the function is constant (its value is zero). For the sake of clarity the most relevant time instants are redefined as follows:

$$\begin{aligned} t_0(h,k) &= T_{M0}(h,k) \\ t_1(h,k) &= T_{M0}(h,k) + \Delta T_P(h,k) \\ t_2(h,k) &= T_{M0}(h,k) + \Delta T_P(h,k) + \Delta T_O(h,k) \\ t_3(h,k) &= T_{M0}(h,k) + \Delta T_P(h,k) + \Delta T_O(h,k) + \Delta T_R(h,k) \end{aligned} \tag{8}$$

so that the analytic expression of the time-dependent function is

$$f_{Ft(h,k)}[T_{M0}(h,k), t] = \begin{cases} 0 & t < t_0 \\ 1 - e^{-(t - t_0(h,k))/\tau_{P(h,k))}} & t_0 < t < t_1 \\ 1 & t_1 < t < t_2 \\ e^{-(t - t_2(h,k))/\tau_R(h,k))} & t_2 < t < t_3 \\ 0 & t > t_3 \end{cases} \tag{9}$$

Fig. 4 shows an example of the time-dependent function $f_{Ft(h,k)}$; while Fig. 5 describes an example of the time history of the functional integrity of a generic node under the impact of a generic threat.

If a number of n_h threats concurrently impact on a vulnerable node, the overlap effects are assessed through the superposition principle, therefore

$$F(k,t) = F(k,0) - \sum_{h=1}^{n_h} f_{FM(h,k)}(M(h,k)) f_{Ft(h,k)}(T_{M0}(h,k), t) \tag{10}$$

where $0 \le F(k,t) \le 1$.

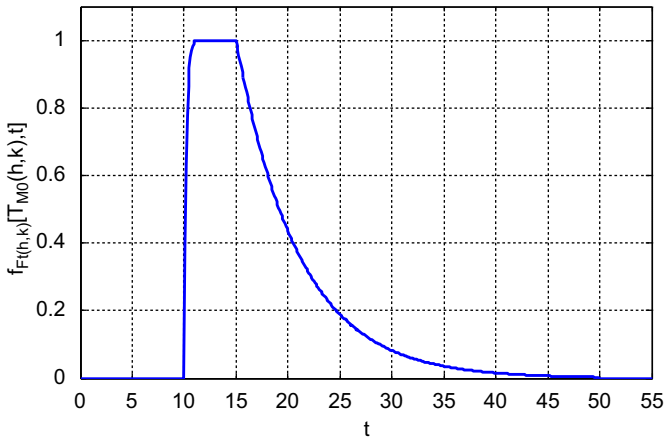

Fig. 4. Example of the time-dependent function $f_{Fi}(h,k)$(TM0 (h,k),t) form.

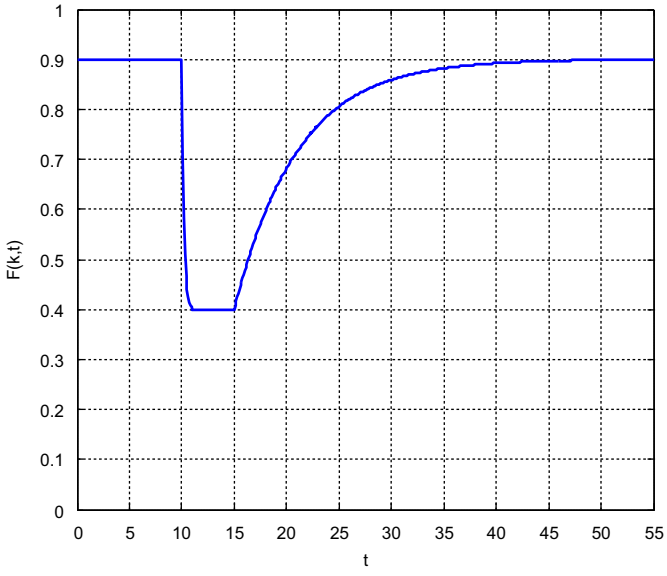

Fig. 5. Example of functional integrity $F(k,t)$ time history.

The maximum service that the k-th node is able to supply, taking into account the reduction of its functional integrity due to threats and assuming that the other nodes connected to it supply the service required, is

$$S_{max}(k,t) = F(k,t)C_{max}(k) \tag{11}$$

3.4. Modelling of functional interdependencies between vulnerable nodes

Disruptions and disturbances can be propagated within the same infrastructure or to other CIs by means of the interdependence model (indirect effect of threats on a vulnerable node). In general the node that propagates the disturbance is called "father", and "child" the node on which the disturbance has an impact. The way in which the disturbance propagates depends on the type of interdependence existing between the "father" and the "child". Two main categories of interdependences can be distinguished [28]:

- internal dependences: the service continuity of a specific infrastructure depends on the correct functioning of its own components and connections;
- external dependences: the service continuity of a specific infrastructure depends on the correct supply of the service of other infrastructures (or part of other infrastructures).

Furthermore, for both categories, four main types of interdependencies among CIs can be distinguished [13]:

- physical interdependencies are due to the exchanges of resources among the CIs (customer/supplier-type relations);
- cybernetic interdependencies are due to the transfers of information among CIs;
- geographic interdependencies are due to the geographic proximity or the physical intersection of two or more infrastructures;
- logical interdependencies are due to the overall economic and political context and also to the shift of the demand between two infrastructures that can provide the same or fully/partially replaceable services (e.g. in the transportation sector, it is possible to record a service demand shift from a railway to a highway in case of loss of service in the former).

The physical and cybernetic interdependencies become active when the generic "father" node j is not able to fully meet the actual demand ($\Delta(j,t) > 0$). The consequence is a reduction of the maximum service ($S_{max}(k,t)$) the generic "child" node k is able to supply. The reduction rate of the $S_{max}(k,t)$ is quantified through the inoperability – $I(k,t)$ – of the "child" node.

The effect of geographic interdependencies depends on the specific threat (h,j) impacting on the "father" node j. For instance, collapses or explosions can propagate between proximate infrastructures, while fault of a part of an infrastructure will not propagate to the proximate one. Therefore, the effect of the geographic interdependence is a reduction of functional integrity of the "child" node $I(k,t)$ and, consequently, a reduction of its maximum service $S_{max}(k,t)$.

The effect of logical interdependencies has to be assessed case-by-case. In general, a disservice of the "father" node j impacts on the demand of the "child" k (e.g. a strike of public transport services causes an increasing demand of road traffic).

3.5. Physical interdependencies

Physical interdependencies are due to the exchanges of resources among the CIs (customer/supplier-type relations). If a CI (or a part of it) does not work properly, the physically interdependent CIs are likely influenced, since its service demand contains also the service the connected CIs require for their actual functioning, too.

Consider the elementary case (Fig. 6), with only a father (j) and a son (k) vulnerable nodes.

The physical interdependence operates when the father node transfers a disservice ($\Delta(j,t) > 0$) to the child. A variation $d\Delta(j,t)$ of its disservice causes a variation $dI(k,t)$ of the k-th node inoperability.

Similarly to the vulnerability model, the variation $dI(k,t)$ is determined through a function $f_{I\Delta(k,j)}(\Delta_j)$ of the solely father node disservice $\Delta(j,t)$ and a time-dependent function $f_{It(k,j)}(dt)$.

$f_{I\Delta(k,j)}(\Delta_j)$ is called inoperability modulation function and it allows to define the steady variation of the inoperability as a consequence of a variation of the disservice of the father node,

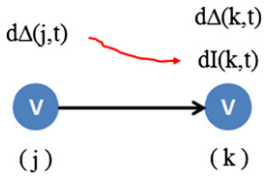

Fig. 6. Elementary case of physical interdependence: a single father node (j).

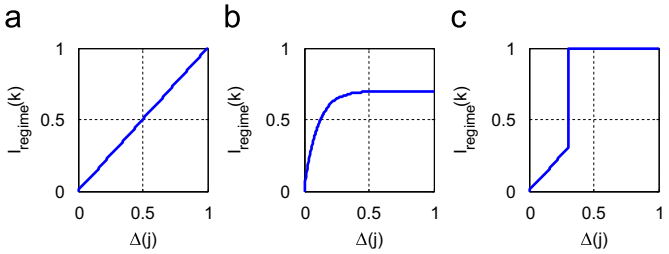

Fig. 7. Examples of the inoperability modulation function $f_{I\Delta}(k,j)(\Delta_j)$ form.

whereas the function $f_{It(k,j)}(dt)$ influences the dynamic through which the inoperability reaches its new steady value. The form of the functions $f_{I\Delta(k,j)}(\Delta_j)$ and $f_{It(k,j)}(dt)$ have to be properly defined through interviews and work sessions with the operators. Fig. 7 shows some examples of the inoperability modulation function $f_{I\Delta(k,j)}(\Delta_j)$ form.

Fig. 7(a) is an example of the $f_{I\Delta(k,j)}(\Delta_j)$ form in case of two consecutive highway stretches (obviously modelled through two different nodes) without tollgates: a disruption which blocks the second stretch surely blocks the first one too (at the same manner with a delay), since no exit allows vehicles to take an alternative road. Fig. 7(b) shows an example of the $f_{I\Delta(k,j)}(\Delta_j)$ form in case of two consecutive highway stretches with tollgates: a block of the second stretch obviously causes problems to the first one, but its influence is lower, since vehicles can take an alternative way. Fig. 7(c) is an example of the $f_{I\Delta(k,j)}(\Delta_j)$ form in case of power supply: low disruptions cause a proportional power supply reduction to the whole interdependent CI; in case of relevant disruption, the energy provider may cut off the energy supply to some CIs in order to fully meet the demand of other most strategic ones.

The differential of the $f_{I\Delta(k,j)}(\Delta_j)$ is calculated through

$$df_{I\Delta(k,j)}[\Delta(j,t)] = f_{I\Delta(k,j)}[\Delta(j,t)] - f_{I\Delta(k,j)}[\Delta(j,t-dt)] \quad (12)$$

The time-dependent function $f_{It(k,j)}$ is assumed to be an exponential decay:

$$f_{It(j,k)}(dt) = 1 - e^{-(dt/\tau(k,j))} \quad (13)$$

where the time constant $\tau(k,j)$ influences the dynamic of the propagation.

The disservice variation $d\Delta(j,t)$ of the father node j causes an inoperability variation $dI(k,t)$ on the child node k:

$$dI(k,t) = df_{I\Delta(k,j)}[\Delta(j,t)] f_{It(k,j)}(dt) \quad (14)$$

As a consequence, the inoperability $I(k,t)$ of the child node is calculated through the integration of the previous:

$$I(k,t) = I(k,0) + \int_0^t \left[\left(\frac{\partial}{\partial \Delta_j} f_{I\Delta(k,j)}[\Delta(j,s)] \right) \left(\frac{\partial}{\partial t} \Delta(j,s) \right) (1 - e^{-(t-s/\tau(k,j))}) \right] ds \quad (15)$$

Moreover the model allows to consider a delay $T_I(k,j)$ in the propagation of the disservice. In this case the inoperability $I(k,t)$ is calculated through

$$I(k,t) = I(k,0) + \int_0^t \left[\mathbb{1}_{\{s < t - T_I(k,j)\}} \left(\frac{\partial}{\partial \Delta_j} f_{I\Delta(k,j)}[\Delta(j,s)] \right) \times \left(\frac{\partial}{\partial t} \Delta(j,s) \right) \cdot (1 - e^{-(t-s/\tau(k,j))}) \right] ds$$

where

$$\mathbb{1}_{\{s < t - T_I(k,j)\}} = \begin{cases} 0 & \text{per } s \geq t - T_I(k,j) \\ 1 & s < t - T_I(k,j) \end{cases} \quad (16)$$

Fig. 8 shows the effect of the father node disservice $\Delta(j,t)$ on the inoperability progress $I(k,t)$ of the child node.

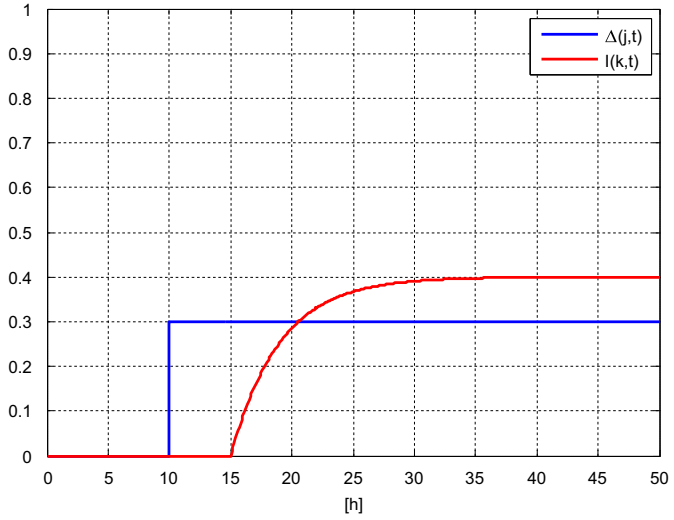

Fig. 8. Relation between the disservice $\Delta(j,t)$ of the father node and the inoperability $I(k,t)$ of the child node.

In case of more father nodes (i.e. $n-1$) concurrently contributing to the inoperability of a common child node, the inoperability $I(k,t)$ of the child node is a generic function of the $n-1$ disservices of the father nodes. Its form should be discussed for each particular case with the operators. However, since the proper functioning of the child node depends on the proper functioning of all father nodes, providing the required service mix, it can be assumed that the functioning of the child node at time t is solely influenced by the father node, which individually propagates the higher impact, i.e. the highest functional inoperability, at that time. This assumption is reasonable since the father node, which propagates the higher inoperability is seen as the operations bottleneck for the child node that does not receive the required service from one of its "suppliers".

The inoperability $I_j(k,t)$ that each father node j individually propagates on the child node k is

$$I_j(k,t) = I_j(k,0) + \int_0^t \left[\mathbb{1}_{\{s < t - T_I(k,j)\}} \left(\frac{\partial}{\partial \Delta_j} f_{I\Delta(k,j)}[\Delta(j,s)] \right) \times \left(\frac{\partial}{\partial t} \Delta(j,s) \right) \cdot (1 - e^{-(t-s/\tau(k,j))}) \right] ds \quad j = 1,\ldots,n; \quad j \neq k \quad (17)$$

According to the previous assumption, the inoperability $I(k,t)$ is calculated through

$$I(k,t) = max\{I_j(k,t)\} \quad con \quad j = 1,\ldots,n; \quad j \neq k \quad (18)$$

Fig. 9(a) describes the disservice progress for the father nodes. Fig. 9(b) shows the inoperability, which they individually propagate to the child node. Fig. 9(c) shows the inoperability of the child node, which is the maximum value between those individually propagated. Note that the child node is not influenced at every time by the disservice with the highest intensity or by the first emerging one.

Although the assumption of the highest propagated inoperability is quite reasonable, the formalism allows the user to model alternative mechanisms for each particular case.

The maximum service that the k-th node is able to supply, taking into account the physical interdependences with the other vulnerable nodes and assuming that no threats directly impact on it, is

$$S_{max}(k,t) = (1 - I(k,t)) C_{max}(k) \quad (19)$$

A complete definition of a physical interdependence requires to specify the following main characteristics:

- name of the physical interdependence;
- father node j;

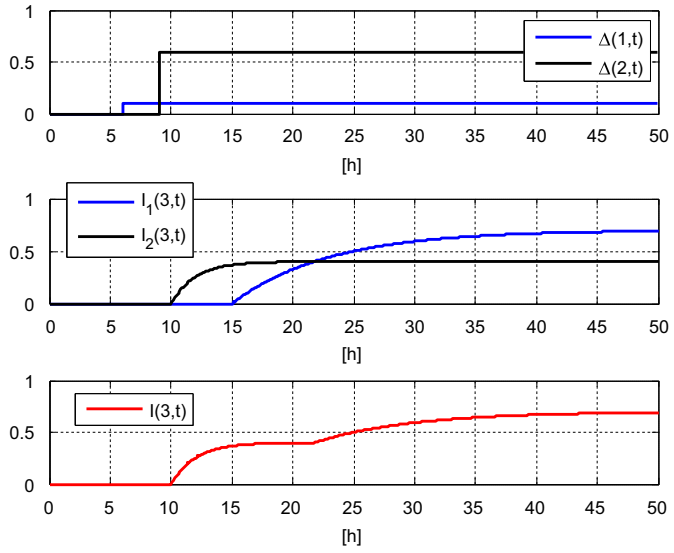

Fig. 9. Relationship between the disservices of the two father nodes and the inoperability of child one.

- child node k;
- description of the interdependence;
- inoperability modulation function $f_{\mathrm{FM}(h,k)}(M(h,k))$, i.e. the form of modulation by which the inoperability of a vulnerable node is varied depending on the disservice $\Delta(j,t)$ of the father node;
- delay time $T_I(k,j)$, i.e. the delay after which the father node disservice $\Delta(j,t)$ reaches the child node.
- time constant $\tau_I(k,j)$, i.e. the constant influencing the dynamic of the propagation.

3.6. Cybernetic interdependencies

Cybernetic interdependencies are due to the transfer of information among CIs: if a CI does not receive information from the interdependent one, it cannot work properly. Thus a lack of information causes a reduction of the maximum service the CI is able to supply. In particular, if the father node j does not send the whole information ($\Delta(j,t)>0$), its disservice causes an inoperability $I(k,t)$ on the child node k, which successively reduces its maximum service level $S_{max}(k,t)$. As a consequence, cybernetic interdependencies can be modelled in the same way of the physical ones.

3.7. Geographic interdependencies

Geographic interdependencies are due to the geographic proximity of the infrastructures; their effect depends on the specific threat impacting on the interdependent CI. For instance, collapses or explosions can propagate between proximate infrastructures, while operational fault of a part of an infrastructure will not propagate to the proximate one.

Since geographic interdependences spread a threat impacting a CI on the proximate ones, their effect is a reduction of functional integrity of the proximate ones and, consequently, a reduction of their maximum service level. Accordingly, geographic interdependences can be modelled as threat nodes, which become active only when particular threats (i.e. an explosion) impact on the father node. Since these interdependences are threat nodes with conditional activation, their model is similar to that of a threat node.

A complete definition of the geographic interdependences requires to specify the following main characteristics:

- name of the geographic interdependence;
- father node (j);
- impacted vulnerable node (k);
- kind of disturbance/disruption (h) on the father node (j), which activates the interdependence;
- description of the impact;
- functional integrity modulation function $f_{FMP(h,k)}(M(h,j))$, i.e. the form of modulation in which the functional integrity of the child node k is varied depending on the percentage intensity $M(h,k)$ of the threat impacting on the father node j;
- propagation time $T_{PP}(h,k)$, i.e. the measure of the loss rate of the functional integrity of the child node k as a consequence of the threat h on the father node k;
- maximum time required for setting-up the intervention $\Delta T_{0maxP}(h,k)$, i.e. the maximum time required for setting-up a countermeasure after an integrity loss of the k-th node due to the h-th threat impacting on the j-th node;
- maximum recovery time $\Delta T_{\mathrm{R\_maxP}}(h,k)$, i.e. the maximum time window within which the k-th vulnerable node is restored to the level before the h-th event occurs;
- description of the recovery function of the functional integrity (e.g. smooth or step function).

3.8. Modelling of logical interdependencies

Logical interdependencies are due to the overall economic, political and social context, included the expected behaviour of citizens and other types of clients of the considered CIs. A particularly relevant phenomenon resulting in further CI interdependence during disruption or destruction events is the demand shift between two infrastructures that can provide the same service or fully/partially replaceable services. An example is a service demand shift in the transportation sector. If the rail transportation system registers a disservice, part of the demand will not be satisfied. The unsatisfied demand may behaves differently: some users will wait until the service will be recovered, other will give up to reach the destination, other will decide to use an alternative way to reach the destination (e.g. by car through the road transportation system). Therefore, part of the CI "road transportation system" bears an increasing demand depending on the disservice of the rail transportation system and the time in which the demand changes. Anyway the unsatisfied demand switches to the road transportation system only if the alternative way is able to match the surplus of demand.

In order to model this kind of logical interdependences, two parameters and a variable are introduced. The Demand Shift coefficient $DS(j,k)$ is defined as the percentage of demand of the father node j impacting on the child node k, and is assumed to be constant. The duration of the disservice $T_{\Delta}(j,t)$ determines how long the father node does a disservice and it is defined as

$$\text{if } \begin{array}{ll} \Delta(j,t)>0 \wedge \Delta(j,t-\mathrm{d}t)>0 & T_{\Delta}(j,t)=T_{\Delta}(j,t-\mathrm{d}t)+\mathrm{d}t \\ \text{otherwise} & T_{\Delta}(j,t)=0 \end{array} \tag{20}$$

The logical delay $T_{log}(j,k)$ is the time after which the demand of the father node begins to switch to the child node (e.g. the time after which the railway users decide to switch to the road transportation system).

The increase of demand $\Delta D_{log(j,k)}(t)$ for the child node k is

$$\begin{array}{l} \text{if } T_{\Delta}(j,t) \geq T_{log}(j,k) \wedge \Delta(k,t)=0 \\ \qquad D_{log(j,k)}(t)=DS(j,k)[D_{std}(j,t)-S_{MAX}(j,t)] \\ \text{otherwise} \\ \qquad \Delta D_{log(j,k)}(t)=0 \end{array} \tag{21}$$

In general, if there are n vulnerable nodes, the overall switches of the demand are calculated through the superposition principle.

The method is similar to the previous one, but $\Delta D_{log(j,k)}(t)$ is a square matrix (nxn). The sum of the elements in each column returns the increase of demand of the node (considered as child), whereas the sum of the elements in each row returns the reduction of demand on the node (considered as father). As a consequence, the overall switch of demand is

$$\Delta D_{log}(k,t) = \sum_{\substack{j=1 \\ j \neq k}}^{n} [\Delta D_{log(j,k)}(t) - \Delta D_{log(k,j)}(t)] \tag{22}$$

Finally, the actual demand on the k-th node is calculated through

$$D_{eff}(k,t) = D_{std}(k,l) + \Delta D_{log}(k,t) \tag{23}$$

A complete definition of the logical interdependences requires to specify the following main characteristics:

- name of the physical interdependence;
- father node j;
- child node k;
- description of the interdependence;
- demand Shift coefficient $DS(j,k)$: this parameter determines the maximum percentage of the father demand shifting to the child node;
- logical delay $T_{log}(j,k)$: the time after which the demand of the father node begins to switch to the son one.

3.9. Modelling of impacts

The impact model aims at evaluating the consequences of the disservice of the CIs due to specific threats either in terms of service disruption and damages to economic activities and people.

At this stage of the research project the model allows to estimate only the number of end users (e.g. citizens) affected by service disruption at each infrastructure node. The reason essentially stems from the kind of infrastructure analysed and the kind of information and data available from operators.

In order to calculate the number of users affected by service disruption, the parameter $u_{s0}(k,t)$ is introduced, which converts the service demand in number of end users. This parameter depends on the specific CI considered and it is generally time dependent. For instance, in case of the railway transportation system, this parameter determines the average number of passengers per train (which obviously depends on the hour of the day and on the season), so that it is possible to convert the service demand (i.e. train per hour) into the number of potential end users (i.e. passengers per hour). As a consequence the parameter $u_{s0}(k,t)$ has to be properly defined through interviews and work sessions with the operators.

Once defined this parameter, the number of user affected by a service disruption of node k at time t is simply calculated through the following equation:

$$u_s(k,t) = u_{s0}(k,t) D_{eff}(k,t) \Delta(k,t) \tag{24}$$

4. Overall model implementation

A generic CI system is modelled as shown in Fig. 10, where for the sake of clarity vulnerable nodes belonging to different CI are represented on different layers.

The model can be implemented in a generic programming language; in the present study Matlab™ has been used. This section aims at describing the logic followed by the recursive

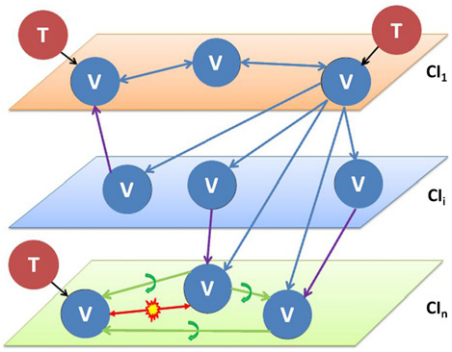

Fig. 10. Description of a generic CI system.

algorithm for calculating the state of the system at a generic time t (Fig. 11).

First of all, the input parameters – threats and standard demands – are generated: significant threats are selected to be studied and standard demand of considered nodes is characterised using experts' evaluations or reports and structured data provided by CI operators. To this end, a set of templates similar to FMECA worksheets has been prepared, where the experts listed internal and external threats for each node, along with a qualitative analysis of likelihood, consequences and severity (in terms of damages and service disruption). Then, the effect of each specific threat on the vulnerable nodes has been translated into a quantitative model through Eq. (25), taking also into account the geographic interdependencies:

$$F(k,t+\mathrm{d}t) = F(k,0) - \sum_{h=1}^{n_h} f_{FM(h,k)}(M(h,k)) f_{Ft(h,k)}(T_{M0}(h,k), t+\mathrm{d}t) - \sum_{\substack{j=1 \\ j \neq k}}^{n} \sum_{h=1}^{n_h} f_{FMP(h,k)}[M(h,j)] f_{FtP(h,k)}(T_{M0}(h,j), t+\mathrm{d}t)$$

$$0 \leq F(k,t+\mathrm{d}t) \leq 1 \tag{25}$$

Only after the definition of the impact of the threats, the effects of the other interdependences are evaluated. Since the disservice $\Delta(k,t+\mathrm{d}t)$, inoperability $I(k,t+\mathrm{d}t)$, and actual demand $D_{std}(k,t+\mathrm{d}t)$ parameters are mutual dependent, to avoid possible computational loops, the inoperability and the actual demand at the time $t+\mathrm{d}t$ are calculated using the disservice at the time (t). Shorter the discrete-time sampled, greater the accuracy of the approximation. Fig. 11 shows the simplified procedure.

The inoperability due to physical and cybernetic interdependencies results from

$$I_j(k,t+\mathrm{d}t) = I_j(k,0) + \sum_{i=1}^{n_i} tsc_{(k,j,i)} \{ f_{I\Delta(k,j)}[\Delta(j,i\mathrm{d}t)] - f_{I\Delta(k,j)}[\Delta(j,(i-1)\mathrm{d}t)] \} (1 - e^{-(t+\mathrm{d}t-T(k,j)-i\mathrm{d}t/\tau(k,j))}) \tag{26}$$

where

$$n_i = \frac{t}{\mathrm{d}t}$$

$$tsc_{(k,j,i)} = \begin{cases} 0 & set+\mathrm{d}t-T(k,j)-i\mathrm{d}t < 0 \\ 1 & set+\mathrm{d}t-T(k,j)-i\mathrm{d}t \geq 0 \end{cases}$$

Thus the inoperability is calculated through

$$I(k,t+dt) = max\{I_j(k,t+dt)\} \quad con \quad j=1,\ldots,n; \quad j \neq k \tag{27}$$

Taking into account also the logical interdependencies, the demand variation is

if $T_{\Delta}(j,t) \geq T_{log}(j,k) \wedge \Delta(k,t) = 0$

$\Delta D_{log(j,k)}(t+\mathrm{d}t) = C\mathrm{d}T(j,k)[D_{std}(j,t) - S_{MAX}(j,t)]$

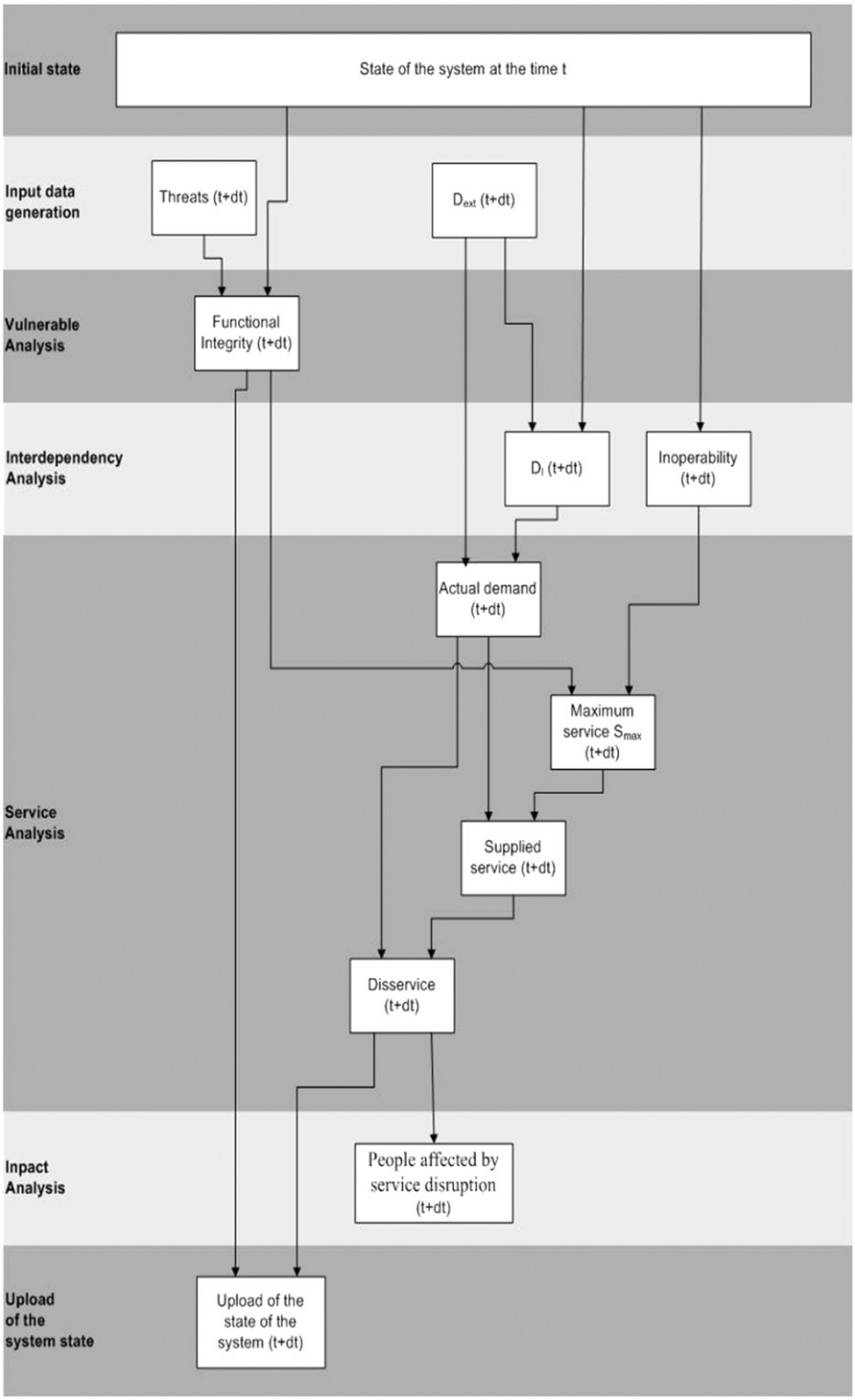

Fig. 11. Simplified algorithm for calculating the state of the system at a generic time t.

otherwise $\Delta D_{log(j,k)}(t+dt)=0$

$$\Delta D_{log}(k,t+dt)=\sum_{\substack{j=1\\ j\neq k}}^{n}[\Delta D_{log(j,k)}(t+dt)-\Delta D_{log(k,j)}(t+dt)] \quad (28)$$

Therefore, the actual demand of the k-th node is

$$D_{eff}(k,t+dt)=D_{std}(k,t+dt)+\Delta D_{log}(k,t+dt) \quad (29)$$

Then it is possible to calculate the maximum service level that the k-th node is able to supply, taking into consideration both the threats, which impact on it (through the functional integrity) and the effect of the functional interdependencies:

$$S_{MAX}(k,t+dt)=F(k,t+dt)[1-I(k,t+dt)]C_{max}(k) \quad (30)$$

and, consequently, the actual service level supplied $S(k,t+dt)$:

$$\begin{aligned} &\text{if } S_{MAX}(k,t+dt)\leq D_{eff}(k,t+dt)\Rightarrow S(k,t+dt)=S_{MAX}(k,t+dt)\\ &\text{if } S_{MAX}(k,t+dt)> D_{eff}(k,t+dt)\Rightarrow S(k,t+dt)=D_{eff}(k,t+dt)\end{aligned} \quad (31)$$

Finally, the disservice $\Delta(k,t+dt)$ of the k-th node at the time $(t+dt)$ is

$$\Delta(k,t+dt) = \frac{D_{eff}(k,t+dt) - S(k,t+dt)}{D_{eff}(k,t+dt)} \quad (32)$$

Fig. 12 illustrates the relationships between the several characteristics of the state of the vulnerable node from the functional integrity to the disservice passing through the computation of its inoperability, its demand variation, its actual demand and its maximum service level that the node is able to supply and, consequently, the actual service level delivered.

5. Pilot study

A preliminary pilot study has been carried out in the metropolitan area of the province of Milan. The aim of the pilot study was to demonstrate the applicability of the proposed model; test its capability to represent all the type of interdependencies; and give an overview of the possible outcome of the model.

The CIs considered referred to the transportation system (road, rail, underground, and airport systems). In particular, for the road system, it has been considered highways, beltways and the national roads. Fig. 13 shows all the infrastructure considered, while Table 1 summarises the CIs in terms of number and type of vulnerable nodes. A total of 169 vulnerable nodes have been modelled interacting through 420 functional interdependencies and 229 logic interdependencies. At this stage of the study Electric Power and Gas networks were considered as sets of threat nodes impacting on some vulnerable nodes of different transport systems (railway lines, airports, underground lines, depots, etc.). The characterisation of vulnerable nodes and threats was completed by means of public data, open theoretical models, data from the regional Civil Protection service, questionnaires and direct interviews to operators. Specific templates have been prepared and administered as described in Section 4. A total of 12 questionnaires were collected and 20 interviews were performed with different operators and functions within the same operator to better clarify or complete the information collected by the questionnaires.

Two different kinds of failure scenarios have been simulated:

- elementary failure scenario: triggered by the activation of multi-threats or a single threat able to impact on a vulnerable node at a time blocking it for the entire time-window considered;

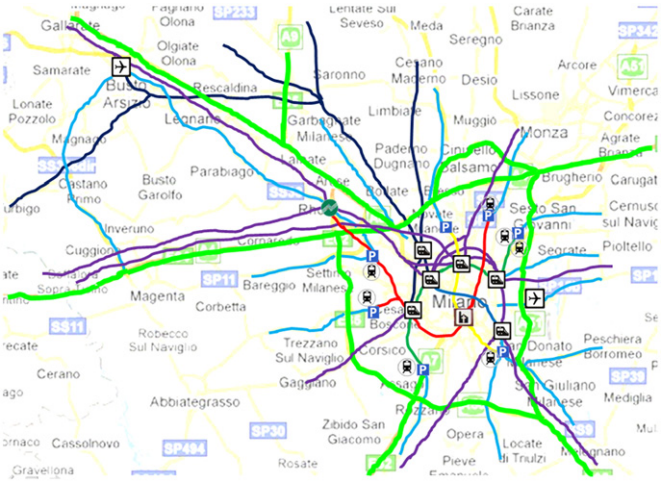

Fig. 13. Map of the CI network considered.

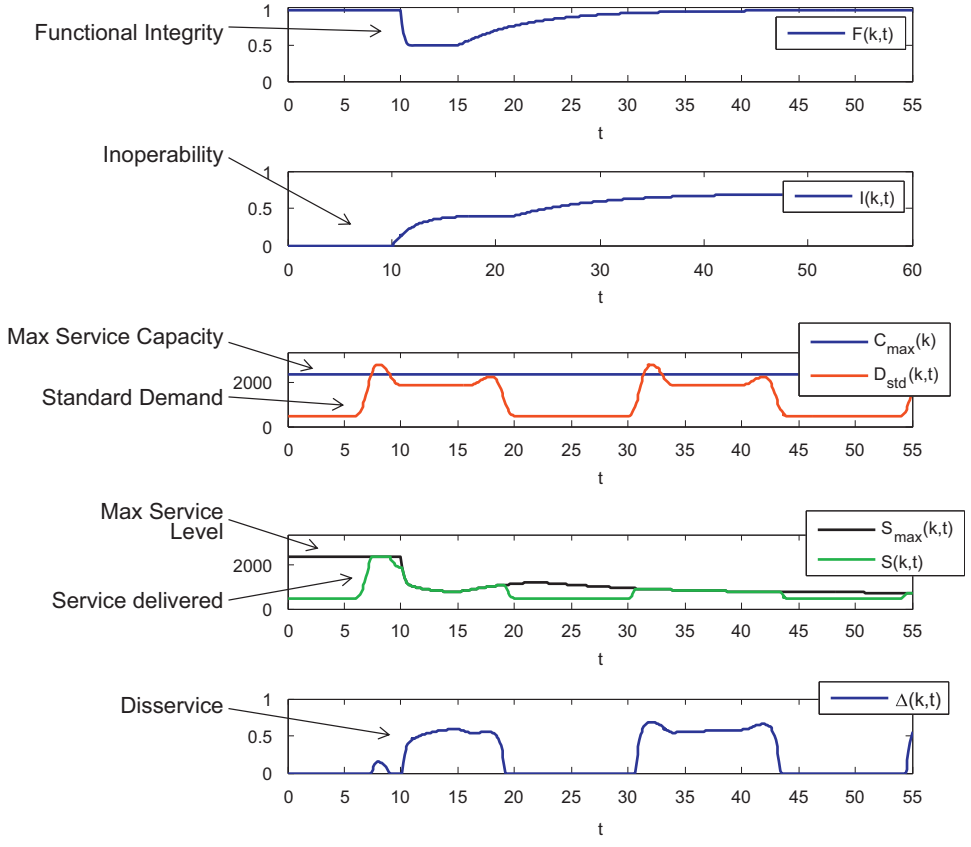

Fig. 12. Relationships between the several characteristics of the state of the vulnerable node from the functional integrity to the disservice.

– complex failure scenario: for example multi-threats or a single threat able to block more vulnerable nodes concurrently.

The time-window of the simulations is 36 h in order to completely register the transient associated to the threat.

On one hand the first approach allows to determine the characteristics of the system. Indeed, assuming that scenarios have equal likelihood to occur, the elementary failure scenario allows to assess the impact connected to each scenario. As shown in Table 2, nodes are arranged due to their impact on users in case of disruption in order to easily assess their criticality for society through the total number of people affected by service disruption per infrastructure node and for the infrastructural network. Another way to report the results of the simulation of elementary accident scenario is reported in Fig. 14, where each vulnerable node is plotted according to the frequency of its involvement (inoperability and/or functional integrity > 0) in the considered elementary scenarios (169 scenarios of 36 h of disruption of a single node) – the *x*-axis – and to the total registered disservice in the node adding up the single contribution of all the elementary accident scenarios. According to simulations, the most critical nodes of the Milan transportation system from an impact point of view are Centrale Station (Node #85), Garibaldi Station (84) and the Green Underground Line crossing the city centre (93). This is due to the high number of interdependencies existing among them and the whole system, and also to the great number of users involved in those nodes. Indeed, only a small percentage of the total estimated disservice is observed in the node directly impacted by the threat or in the node with the highest registered disservice in the considered scenario (Table 2). When a threat is considered able to completely disrupt the functional integrity of the Garibaldi Station (the triggered node; 84) for 36 consecutively hours, the registered disservice on the same node only account for the 2% of the total disservice in the overall system, and also the most critical node (the portion of the Green Underground Line crossing the city centre; 93) only accounts for the 6.6% of the total disservice.

On the other hand the complex failure scenario is useful to understand the inoperability dynamics in case of multi-threats or a single threat able to block more vulnerable nodes concurrently. The last row in Table 2 shows the results of the multi-event scenario

Table 1
Characterisation of the CIs considered.

CI	Number of vulnerable nodes	Notes
Road transportation system	82	Highways + beltways (30), national roads (52)
Rail transportation system	57	Railways (50), stations (7)
Airports	2	Linate and Malpensa
Local transportation system	28	Undergrounds (22), depots (6)

Table 2
Simulation results of some accident scenarios.

	Trigger node (#)	Total Disservice generated by the scenario (persons × CI nodes)	Disservice (%) in the trigger node	Node (#) with the highest registered disservice	Disservice (%) in the node with the highest disservice
Elementary failure scenario	85	4.2E06	7.5	85	7.5
	84	3.7E06	2.0	93	6.6
	93	3.0E06	7.7	93	7.7
Complex failure scenario	94–95 1–2	1.7E06	57.6	95	15.0

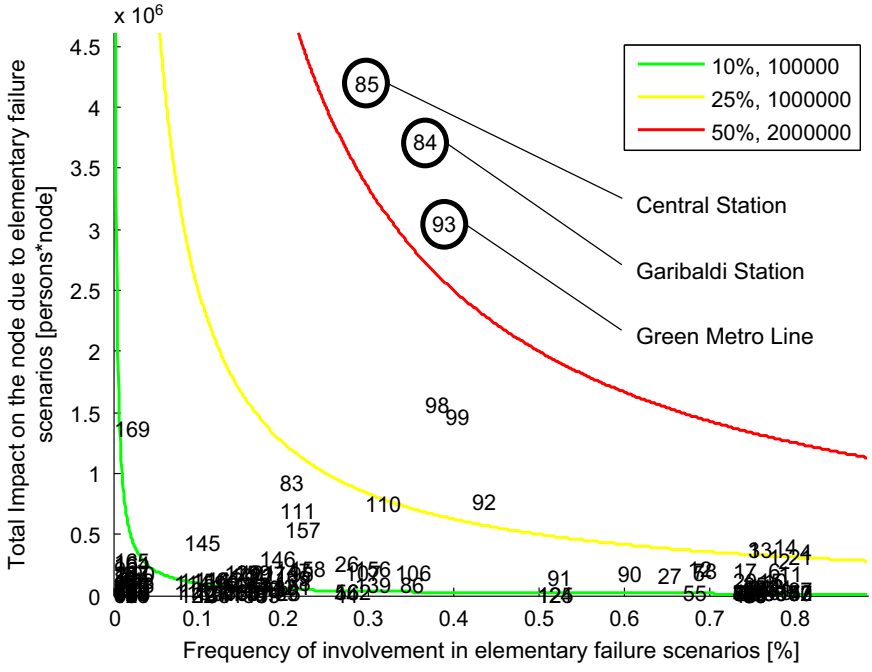

Fig. 14. Summary of the results of 169 elementary accident scenarios. Different clusters of vulnerable nodes can be appreciated.

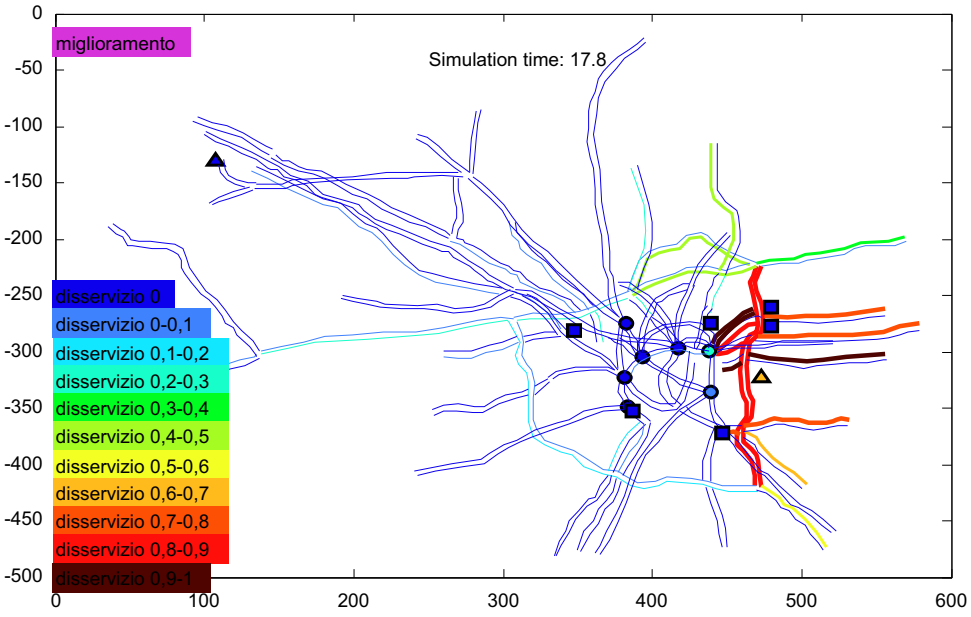

Fig. 15. Screenshot of the graphical interface showing the impact spread at simulation time 17.8 h.

involving at the same time crossing infrastructures (two highways and one underground line), modelled as three vulnerable nodes connected by physical and geographical interdependencies. According to results, the impact of a multi-threat scenario is higher than the sum of the impacts due to the corresponding single threat scenarios, showing an escalation factor of 1.86.

Finally, a very simple graphical interface (Fig. 15) has been developed to easily understand the time propagation of disservice through the whole network.

6. Conclusions

Since the adequate functioning of infrastructures is crucially sustaining societal and economic development, their protection becomes more and more an important issue. Therefore a research project, named PReSIC, to investigate the role of CIs and to assess the related vulnerabilities, has been launched by the Lombardy Region Administration. The first point of the project required to identify the most appropriate modelling strategy for both the documentation of critical nodes and the development of thorough interdependency analyses.

The challenge of modelling and simulating CIs interdependence at regional scale had to cope with some specific critical issues:

- infrastructures had to be described at a functional level but assuring a geographical reference (GIS);
- several different types of interdependences and impacts had to be taken into consideration;
- dynamic phenomena had to be reproduced on both service level (inoperability) and demand (behaviour of citizens and organisations).

A new integrated formalism for the functional modelling of vulnerability and interoperability of Critical Infrastructures at regional level has been developed with the aim of embracing and quantifying all the major aspects – in particular infrastructural nodes and interdependencies – related to the specific level of investigation and trying to offer a positive answer to the actual need to mediate between the economical-organisational level and the physical one when the CIP problem is addressed at regional level. In that it is not possible neither to have the level of detail of the latter nor the easiness for the former.

The model is able to assess the propagation of impacts due to a wide set of threats. Therefore, the disservice can be propagated within the same infrastructure or to other CIs by means of the interdependence model which is able to model physical, cybernetic, geographic as well as logical interdependencies due to the shift of the demand between two infrastructures that can provide the same or fully/partially replaceable service.

Furthermore, the proposed model is dynamic, since both the impact of the specific threat on a generic infrastructure node and the inoperability functions are time-dependent. A recursive algorithm for the interoperability propagation is also proposed.

The modelling framework of interdependencies (and related threats and nodes) have been initially derived and developed on the basis of the observation of the normal functioning of the infrastructure system. Those data and info had been gathered from operators and available databases. In a second step the framework has been enhanced through the considerations of all those particular mechanisms that singularly might take place in rare events, as documented by past experience of operators (when available) or "what if" analyses based on experts' judgements applied to specific scenarios. Also all those characteristics have been entered into the model (both in the structure and in the parameterisation).

On the other side, the formalism and the model adopted in the pilot study are not able to identify unpredictable and rare interdependencies and vulnerability of the considered infrastructures; thus they cannot be used to replace the analysis of historical events and experts' judgements as primary sources for the identification of specific vulnerability and interdependency mechanisms. This is a clear limitation in the scope of the proposed modelling formalism; however, since the consideration of rare major disruptions and the identification of unpredictable domino effects are relevant issues in Critical Infrastructure protection, one of the next research activities will be to analyse some real "unlucky" events, for which a large amount of detailed information are available, to deeply test the capabilities of the proposed approach to simulate extreme accident scenarios.

To demonstrate the applicability of the proposed model a pilot study has been carried out in the metropolitan area of the

province of Milan. The CIs considered referred to the transportation system (road, rail, underground, and airport system). The scope was to test its capability to represent all the type of interdependencies and to give an overview of the possible outcome of the model. Indeed, the model is suitable for studying both elementary and complex failure scenarios providing a prioritisation of the vulnerable nodes of the CI system based on the expected global impact. At this preliminary level of the analysis the model returned a clear clustering of infrastructural nodes, in terms of relative vulnerability and global impact associated to the entire spectrum of accident scenarios in which each specific node might be involved. Also in this respect further research is needed to develop a set of indexes for measuring domino effects and system's resilience in order to better direct CI operators' efforts to a more effective and efficient management of the system (evaluated in terms of both global impact and mobilised resources).

Finally, there is the need to further test and verify the extent and flexibility of the formalism when a larger number of heterogeneous infrastructures (different from energy and transport) need to be included in the analysis.

Acknowledgement

The work presented in this paper has been partially funded by Eupolis Lombardia the Research Agency of the Lombardy Region. In addition the DG Civil Protection and Security had an important role in granting the willingness of CI operators to provide data and information.

References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. L 345/75. Official Journal of the European Union; Published 23.12.2008.
[2] Bouchon S. The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state-of-the-art. Ispra: IPSC. Joint Research Centre; 2006.
[3] Metzger J. An overview of Critical Infrastructure Protection (CIP): a critical appraisal of a concept. Critical Infrastructure Protection and Civil Emergency; 2004.
[4] Robert B, Morabito L. The operational tools for managing physical interdependencies among Critical Infrastructures. International Journal of Critical Infrastructures 2008;4:353–67.
[5] Robert B, De Calan R, Morabito L, Quenneville O. The preventive approach to risks related to interdependent infrastructures. International Journal of Emergency Management 2007;42:166–82.
[6] Robert B, De Calan R, Morabito L. Modelling interdependencies among critical infrastructures. International Journal of Critical Infrastructures 2008;4: 392–408.
[7] The Infrastructure Security Partnership. Regional disaster resilience: a guide to developing an action plan. Reston, Virginia: American Society of Civil Engineers; 2006.
[8] Cziner K, Mutafungwa E, Lucenius J, Järvinen R. Critical Information Infrastructure Protection in the Baltic Sea Area: the case of TETRA. University of Helsinki; 2007.
[9] Pederson P, Dudenhoeffer D, Hartley S, Permann M. Critical Infrastructure Interdependency Modeling: a Survey of U.S. and international research; 2006.
[10] Bagheri E, Ghorbani A. The state of the art in Critical Infrastructure Protection: a framework for convergence. International Journal of Critical Infrastructure 2007.
[11] Svendsen NC, Wolthusen SD. An analysis of cyclical interdependencies in Critical Infrastructures. Proceedings of the 2nd International Workshop on Critical Information Infrastructures Security 2007.
[12] Setola R, De Porcellinis S, Sforna M. Critical Infrastructure dependency assessment using the input–output inoperability model. International Journal of Critical Infrastructure Protection 2009.
[13] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine 2001.
[14] Haimes YY, Horowitz BM, Lambert JH, Santos JR, Lian C, Crowther Kenneth G. Inoperability input–output model for interdependent infrastructure sectors. I: theory and methodology. Journal of Infrastructure Systems 2005;11.
[15] Cagno E, De Ambroggi M, Grande O, Trucco P. Risk analysis of underground infrastructures in urban areas. Reliability Engineering and System Safety 2011;96:139–48.
[16] Crowther KG, Haimes YY, Taub G. Systemic valuation of strategic preparedness through application of the inoperability input–output model with lessons learned from Hurricane Katrina. Risk Analysis 2007:27.
[17] Bigham J, Jin X, Gamez D, Phillips C. Hybrid workflow and bayesian networks to correlate information in the protection of large scale critical infrastructures. Science Direct 2005.
[18] Skanata D, Byrd DM. Computational models of risks to infrastructure. NATO Science for Peace and Security Series: Information and Communication Security; 2007. p. 13.
[19] Jha MK. Applying Bayesian networks to assess vulnerability of Critical Transportation Infrastructure. Applications of Advanced Technology in Transportation ASCE 2008.
[20] Barton DC, San KL. An agent-based microsimulation of Critical Infrastructure systems. Sandia National Laboratory; 2000.
[21] Gadze JD, Pissinou N, Makki K. Intelligent agent approach to the control of Critical Infrastructure networks. World Academy of Science, Engineering and Technology; 2006.
[22] Pye G, Warren MJ. Conceptual modelling: choosing a Critical Infrastructure modelling methodology. School of Information Systems, Faculty of Business and Law, Deakin University; 2006.
[23] Krings A, Oman PA. Simple GSPN for modeling common mode failures in Critical Infrastructures. University of Idaho, Computer Science Department; 2005.
[24] Kosko B. Fuzzy cognitive maps. International Journal Man–Machine Studies 1986;24:65–75.
[25] DePoy J, Phelan J, Sholander P, Smith B, Varnado GB, Wyss GD, Darby J, Walter A. Critical Infrastructure systems of systems assessment methodology. Sandia National Laboratory; 2006.
[26] Jones DA, Davis CE, Turnquist MA, Nozick LK. Physical security and vulnerability modeling for infrastructure facilities. In: Proceedings of the 39th Hawaii international conference on system sciences; 2006.
[27] Conrad SH, LeClaire RJ, O'Reilly GP, Uzunalioglu H. Critical national infrastructure reliability modeling and analysis. Bell Labs Technical Journal 2007;11: 57–71.
[28] Cagno E, Grande O, Sala G. Underground infrastructures societal risk evaluation and intervention planning guidelines definition; 2008.
[29] Flammini F, Vittorini V, Mazzocca N, Pragliola CA. Study on multiformalism modeling of critical. In: Setola R, Geretshuber S, editors. CRITIS. Berlin Heidelberg: Springer-Verlag; 2008.
[30] Regione Lombardia, DG Protezione Civile, Prevenzione e Polizia Locale. PRIM 2007–2010. Programma regionale Integrato di Mitigazione dei Rischi. Studi Preparatori—Incidenza ad elevata rilevanza sociale in Lombardia; 2010.