A PETRI-NET BASED APPROACH FOR THE INTERDEPENDENCE ANALYSIS OF CRITICAL INFRASTRUCTURES IN TRANSPORTATION NETWORKS

Angela Di Febbraro, Nicola Sacco
DIMSET – University of Genoa
Via Montallegro 1, 16145 Genoa (Italy)
angela.difebbraro@unige.it, nicola.sacco@unige.it

ABSTRACT

The paper deals with the problem of estimating the indirect consequences of safety and security accidents in the so-called transportation Critical Infrastructures, i.e., those assets consisting of systems, resources, and/or processes whose total or partial destruction, or even temporary unavailability, has the effect of damaging or significantly weakening the efficiency and the normal functioning of a Country.
In this framework, the aim of this paper is to define a methodology for estimating the costs deriving from the "chain-effect" which characterizes many CIs, in terms of reachability/non-reachability of some network nodes.
In doing so, a modelling approach based on Petri Nets (PNs) is proposed, being them a suitable formalism to predict the behaviour of a whole transportation network as a consequence of particular events occurring in it.
In the paper, after introducing and describing the PN models of transportation CIs, a case study is presented and discussed.

Keywords: Transportation Networks, Critical Infrastructures, Interdependence and Performance Analysis

INTRODUCTION

Since September 11th, the interest of institutions, managers, enterprises, and researchers has been focused on improving the safety and security levels of Critical Infrastructures (CIs), i.e., those assets consisting of systems, resources, and/or processes whose total or partial destruction, or even temporary unavailability, has the effect of weakening the efficiency and the normal functioning of a Country, or of damaging its economical-financial and social systems. As a reference norm in this framework, it is suitable to look at the recent European

Union Directive 2008/114/CE, in which the basic principles for addressing the CIs safety and security problem are introduced, from a normative point of view.

In particular, as regards transportation systems, the interest about such a problem has grown due not only to the potentially very high number of people killed or injured when an incident or accident occurs (direct losses), but also to the high costs and the large amount of time needed in many cases to restore the regular working conditions (indirect losses).

Then, focusing on transportation infrastructures, the problem of reducing their risk from both accidental events (hereafter referred as “safety events”) and malicious attacks (hereafter referred as “security incidents”), is often complicated by the intrinsic characteristics of the networks themselves. In fact, such networks are:

- often highly geographically *distributed*, so that controlling them at any time is practically infeasible;
- very *heterogeneous*, from both the points of view of the constituting civil structures and technological devices;
- *critical*, because in most cases no redundancy is possible;
- *open*, because almost the whole infrastructure is easily reachable by anyone;
- highly *populated* in some locations, where a large number of vehicles and/or people are gathered together such as in railway stations.

Moreover, the main characteristic that makes CI safety and security a particularly important problem to tackle with, is their “mutual interdependence”, that is, the fact that the smooth operability of each one of them often depends on the effective functioning of the others.

It is such an interdependence that makes indirect costs difficult to estimate in large CI networks, as it has been put into evidence by many real world examples, such as, for instance, the arson in the “White Mount Tunnel” connecting Italy and France, where 39 people died in 1999. Then, apart from such huge “direct” costs, three years were required to fully restoring the tunnel functionality. During the restoring period, the connection between Italy and France was guaranteed by the Frejus Tunnel, which was often near to its capacity saturation, thus resulting in frequent traffic jams, environmental pollution, and so on. These were some indirect costs.

Note that, although in the above example indirect losses were quite easy to be forecast, since there are only two tunnels between Italy and France, in general it is not so easy in complex transportation networks.

Then, in such a framework, the aim of this paper is to define a methodology for estimating the costs of the whole damage deriving from the chain-effect caused by an incident/accident to a critical infrastructure, in terms of reachability/non-reachability of some network nodes and links.

In doing so, a modelling approach based on Discrete Event Systems (DES) theory and, in particular, on Petri Nets (PN) is proposed. In fact, such a modelling formalism is characterized by features and algorithms able to put into evidence the properties and the behaviours of the modelled systems, thus resulting to be a suitable tool to describe the dynamics of a whole complex network of CIs, after the occurrences of particular events.

Finally, it is worth noting that the classic traffic assignment methodologies, such as Deterministic User Equilibrium (DUE) or Stochastic User Equilibrium (SUE), which are indeed suitable when only transportation networks are considered, can not be applied when different kinds of CI are taken into account at a time. In fact, Petri Nets, due to their

generality, allow to model complex systems gathering different classes of CIs, such as, for instance, power distribution lines and railway lines. To conclude, the well established and "easy to use" analytical and simulation tools for PN analysis allows to concentrate the efforts in the modelling phase, so as to build a very representative model of the real complex system.
The paper is organized as follows: after a brief literature review, and a basic description of DES and PN, the proposed approach to CIs analysis will be described. Then, a case study will be presented and analyzed.

LITERATURE REVIEW

In this section, a brief non-exhaustive literature review is reported with the aim of introducing the reader to the considered problem. Then, while for specific literature relevant to security and safety of critical infrastructures, the reader may refer to (Lewis, 2006) and (Macaulay, 2008), the problem of assessing the criticality of infrastructures has been faced in (Arulselvan, et al., 2009), where an approach based on graph theory (Bondy and Murty, 1980) is proposed to detect the most critical nodes in large networks. In this framework, an important approach to the identification of criticalities consists of the detection of the so-called Minimal Cut Sets (MCS) representing the set of events whose occurrences imply the interruption of the infrastructure services, or at least a significant worsening of the relevant performances (Ballocco et al., 2009). Such events represent the vulnerabilities of the CI network, and identify the criticalities of the system. Nevertheless, transportation infrastructures, especially when road networks are considered, are seldom characterised by MCS, since a high degree of redundanc, is often guaranteed, even though by means of different kinds of roads, such as, for instance, ordinary roads instead of highway roads, and, consequently, with different network global performances. In this sense, such a consequence, which may be thought of as an "indirect" damage, has to be investigated by ad hoc dynamic models able to take into account, at a time, the possible unreachability of some destination of the considered network, as well as the Level of Service (LoS) decrease of the whole network. Although graph theory appears to be a suitable tool for such analyses, Petri Nets (PN) (Murata, 1989) may represent a better modelling formalism, being capable to model in a unique framework different kinds of dynamics, and in particular for their well-known characteristic to easily model concurrency and synchronism of different events, often in a modular way. In this framework, an interesting application of PN to infrastructure interdependence analysis is described in (Gursesli and Desrochers, 2003) where different kinds of critical infrastructures are modelled in a unique framework and some consideration about interdependence of CIs are provided by applying the analysis of PN structural properties (Murata, 1989). In addition, the "intrinsic modularity" of PN is useful whenever the large networks of different kinds of infrastructures have to be considered, such as, for instance, a electric power distribution network and a railway transportation network. Then, for what concerns the modelling capabilities of PN, especially with respect to transportation systems, they have been put into evidence by the relevant vast literature. Readers may refer, for instance, to (Tolba et al., 2005) and (Di Febbraro et al., 2001) for highway networks or urban transportation networks modelled by means of microscopic or macroscopic approaches, to (Di Febbraro and N. Sacco, 2004) for what concerns urban transportation networks modelled by means of Hybrid Petri Nets, and, finally, to (Kaakai, 2007) for what concerns railway systems.

To conclude, it is worth to introduce CI ranking criteria able to provide indications about the importance of each structure in the CI network, so as to assess the global risk of the considered system. Then, assuming to be able to compute direct and indirect losses by means of suitable models, an approach for ranking critical infrastructures from the point of view of criticality may be addressed by considering each element of the network, or at least the most important ones among them, as a potential "vulnerability", so as to compute the direct and indirect losses for the whole network, as a consequence of attacks to one or more of them. Hence, for what concerns the definition of a ranking criterion, consider the parameter PI_j proposed in (Apostolakis and Lemon, 2005) and defined, for any potential vulnerability j, $j = 1,2,\ldots,J$, as the weighted sum

$$PI_j = \sum_{i=1}^{K} \alpha_i d_{i,j}, \qquad j = 1,2,\ldots,J, \tag{1}$$

where $d_{i,j}$ is the estimated loss caused by the vulnerability (or, in terms of CI networks, by the unavailability of the service) with respect to a given performance index i, $i = 1,2,\ldots,K$, and w_i is a suitably chosen weighting term.

Then, the most critical infrastructures may be identified by sorting the computed performance indices, that is,

$$PI_1 < PI_2 < \ldots < PI_j < \ldots < PI_J. \tag{2}$$

Then, in the following sections, after defining the basic PN models of transportation infrastructures, a revised ranking index for transportation infrastructures derived from the general one in Eq. (1) will be defined.

BASICS OF DISCRETE EVENT SYSTEMS AND PETRI NETS

In this section, some basic definitions and remarks first about Discrete Event Systems (DES), in turn about Petri Nets, are given with the aim of introducing a formalism intended to accomplish structural analysis of CIs and the relevant performance evaluation.

Discrete Event Systems

DES can be intuitively defined as discrete-state, event-driven systems whose state evolution depends entirely on the occurrences of asynchronous events. In such a definition, an event can be, roughly speaking, thought of as something instantaneous, whose occurrence causes a transition from a state of the system to another one. In many DES, an event can be identified with a specific action taken, with a spontaneous occurrence dictated by Nature, or with a result of several conditions being all met at once. From a formal point of view, a DES is a dynamic system characterised by a set E of feasible events, a discrete (even not numeric) state space X, and an event-driven evolution, given by the relation

$$\underline{x}_{k+1} = \delta(\underline{x}_k, e_k), \qquad k = 0,1,2,\ldots, \tag{3}$$

where $\underline{x}_{k+1} \in X$, (resp., $\underline{x}_k \in X$) is the state vector after (resp., before) the occurrence of the event e_k, that is, after the k^{th} event occurred from the initial time instant, and δ is the so-called *state transition function*.

Coming back to the problem of modelling the behaviours and the interconnections of critical infrastructures, it is useful to write the state vector as $\underline{x}_k = \left[\underline{x}_k^1 \quad \underline{x}_k^2 \quad \ldots \quad \underline{x}_k^{H-1} \quad \underline{x}_k^H \quad \underline{x}_k^{\text{int}}\right]$, where:

1. the subvector $\underline{x}_k^h$, $h = 1,2,\ldots,H$, gathers the variables that describe the state of each single h^{th} critical infrastructure of a complex system, being H the total number of CI in the considered area;
2. the subvector $\underline{x}_k^{\text{int}}$ gathers the variables describing the state shared by two or more CIs.

Analogously, the state space may be rewritten as $X = X^1 \cup \ldots \cup X^h \cup \ldots \cup X^H \cup X^{\text{int}}$, where the superscripts distinguish the state subspaces of each single h^{th} critical infrastructures and the subspace of the shared states.

Then, as regards the event set E, it also may be divided into the subsets:

3. E^h, $h = 1,2,\ldots,H$, that is, the set of the events that determine the state evolution of the h^{th} critical infrastructure of a complex system, taking into account those driving the nominal dynamics, and those blocking or damaging it, such as security incidents, attacks, accidents, and so on;
4. E^{int}, that is, the set of the events that "interconnect" different CIs, for instance by changing the state of some variables of the vector $\underline{x}_k^{\text{int}}$.

As an example, consider a railway line and the transformer that gives power to the electric line along the railway. Then, apart from the variables describing the state of the railway line and of the transformer, it is easy to identify a state variable, say x_{up}^h, describing whether the h^{th} electric distribution line is powered by the transformer, or not. Such a variable also says whether trains are powered and can run, or not.

For a detailed introduction to DES, the reader may refer to (Cassandras and Lafortune, 2008).

Petri Nets

A Stochastic Timed Petri Net Structure (STPNS) is a bipartite oriented graph (see Murata, 1989, for more details) described by the 5-tuple

$$STPNS = (P, T, Pre, Post, \Theta), \tag{4}$$

where

- P is a set of n *places*, and T is a set of m *transitions*. The sets P and T are disjoint, that is, $P \cap T = \varnothing$;
- $Pre \in \mathrm{N}^{n,m}$, being $\mathrm{N}^{n,m}$ the set of the matrices gatherings non-negative integers, is the *pre-incidence matrix*, whose generic element $Pre(i, j)$ indicates the weight of the arc exiting from place $p_i \in P$ towards every output transition $t_j \in T$;

- $Post \in \mathrm{N}^{n,m}$ is the *post-incidence matrix* whose generic element $Post(i,j)$ indicates the weight of the arc exiting from transition $t_j \in T$ towards every output place $p_i \in P$;
- $\Theta = \{\Theta_j \mid \forall t_j \in T\}$ is the *clock structure*, where the element Θ_j may be a vector of a scalar. In particular, if Θ_j is a vector, its generic element $\theta_j(z) \in \mathrm{R}_+$, $z = 1,2,3\ldots$, gives the deterministic delay occurring between the z^{th} enabling and the z^{th} firing of transition t_j. In this case, t_j is said "deterministic transition". On the other hand, if $\Theta_j = 1/\lambda(t_j)$ is a scalar, then each firing delay of transition t_j is an extraction of an exponential stochastic variable with rate $\lambda(t_j)$, and then t_j is said "stochastic transition". Finally, if $\Theta_j = 0$, then t_j is an "immediate transition".

For what concerns the state of the system modelled by means of PN, it is represented by the marking vector

$$M(k) = [M_1(k) \quad M_2(k) \quad \ldots \quad M_n(k)]^T, \quad M_i(k) \geq 0, \forall i = 1,\ldots n, \quad k = 0,1,2,\ \ldots, \tag{5}$$

Which gathers n non-negative integers which represent the number of "tokens" in each place $p_i \in P$, after the k^{th} transition firing. In this representation, transitions are associated with the events whose occurrences cause the marking change.
Then, a Stochastic Timed PN (STPN) is defined by the couple

$$STPN = \{STPNS, M_0\}, \tag{6}$$

where $STPNS$ is a stochastic timed Petri net structure, and $M_0 = M(0)$ is the initial marking, that is, the initial state of the system.
Finally, from a graphical point of view, places are represented by circles, immediate and timed transitions by lines and boxes, respectively, arcs by arrows; finally, tokens are represented by black dots. An example of a simple PN is depicted in Figure 1.

PN dynamics

PN dynamics accomplishes the two following rules:

- **[Enabled transition]:** a transition t_j is enabled and may fire, that is, the relevant event may occur, if and only if

$$M_i(k) = \gamma Pre(i,j), \quad 1 < \gamma < \Gamma, \ \forall p_i \in P \tag{7}$$

  where the term γ indicates that transition t_j is enabled exactly γ times at the same time, and Γ indicates the maximum number of contemporary enabling of transitions;
- **[Transition firing]:** The k^{th} firing of a generic transition occurs when the associated event occurs for the k^{th} time. In a timed Petri net, the transition fire occurs after the mount of time given by the clock structure is elapsed from the transition enabling. A firing of a transition modifies the marking of the PN as expressed by the state equation

$$M(k+1) = M(k) + (Post - Pre)u, \qquad M(k) \geq 0, k = 0,1,2,\ldots, \tag{8}$$

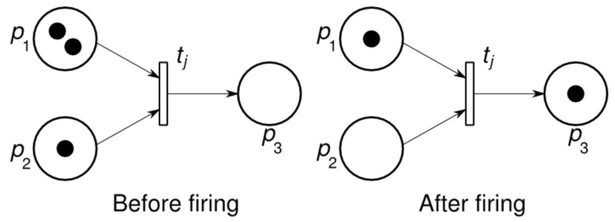

Figure 1 - Example of a generic PN firing.

where the generic marking $M(k+1)$ represents the PN state of the system after the k^{th} firing of the considered transition, and $u = \{0,1\}^m$ is a vector of all null elements but the one corresponding to the transition that fires, which is set to 1.

Note that Eq. (8) expresses, in an algebraic form, the following dynamics, also represented in Figure 1: the firing of a transition t_j removes as many tokens as the value of the element $Pre(i,j)$ from each place p_i of the net, and adds as many tokens as the value of the element $Post(i,j)$ to each place p_i of the net.

Structural Analysis of Petri Net models

For what concerns PN analysis, in the relevant literature there are many analytical tools for investigating any possible behaviour of the modelled system.
In order to recall the PN properties useful in interdependence analysis of CIs, consider the following definition:

- $\sigma[M(k)] = [M(k) \;\; t^{(k)} \;\; M(k+1) \;\; t^{(k+1)} \;\; M(k+2) \;\; \cdots]$ is the vector gathering a sequence of reached-marking/firing-transition, where $M(k)$ is the first marking of the sequence, and $t^{(k)}$ indicates the firing of a particular generic enabled transition; sometimes, for the sake of simplicity, and without loosing generality, the terms $M(k)$ in $\sigma[M(k)]$ are drop;
- $A[M(k)]$ is the set of all the enabled transitions at marking $M(k)$, i.e., the set of the transitions fulfilling the constraint expressed in Eq. (7);
- $L[M(k)]$ is the set of all the markings $M(h)$, $h \neq k$, which are reachable from $M(k)$, i.e., the set of all the markings in any possible sequence $\sigma[M(k)]$.

Liveness

For what concerns the PN properties, the most important one, for the purposes of the present paper, is the *liveness* property, which allows stating whether a generic transition t_j is:

- L0-live *(or dead)*, if it can never fire in any firing sequence $\sigma[M(k)]$;
- *L1-live (or potentially fireable)*, if it can fire at least once in some sequence $\sigma[M(k)]$;
- *L2-live,* if given any positive integer b it can fire at least b times in some firing sequence $\sigma[M(k)]$;
- *L3-live,* if it appears infinitely often in some firing sequence $\sigma[M(k)]$;
- *L4-live (or simply live*), if it is L3-live for every marking $M(h)$ in $L[M(k)]$.

Liveness property may put into evidence, in a large network of complex critical infrastructures, all the structures that can not work properly after the occurrence of particular events, as it will described in the following sections.

Reachability graph

Given a PN with initial marking M_0 and, at least, one non-dead transition, it is possible to reach, potentially, as many new markings as the number of the enabled transitions, provided that the firing of a transition does not make some of the others not enabled. Then, from each just reached marking, if there are other enabled transitions, it is possible to potentially reach more markings again. Finally, such an iterative process (see, for instance, Murata 1989), results into a collection of reachable markings which may be well represented as a graph, where nodes represent the reached markings and arcs represent the transitions whose firing transforms a marking into another one. In such a representation, with the aim of representing infinite possible markings into a graph with a finite number of nodes, let the element ω_i be the symbol indicating an indefinite positive number of tokens into the place p_i. Once built the so-called reachability graph, it results that any path originating in node $M(k)$ represents a firing sequence $\sigma[M(k)]$. Therefore, any node with no exiting arcs corresponds to a marking representing the deadlock condition, i.e., the condition where no system evolutions are possible.
To conclude, it is worth saying that many approaches for building the reachability graph may be found in the PN literature. The reader may refer to (Ye et., al, 2003) for a detailed description of different algorithms.

Petri Nets Performance Analysis

In this section, some considerations about the performance analysis of systems modelled by means of PN are discussed. Then, in order to accomplish a performance evaluation, the first step consists of defining the clock structure Θ.
Evidently, such a clock depends on the kinds of modelled infrastructures, for instance road or rail infrastructures, as well as on the traffic conditions. Then, in the following sections, for the sake of simplicity, the clock of the proposed PN models will be defined assuming to consider only railway networks and electric power distribution networks.

PETRI NET MODELS OF CRITICAL INFRASTRUCTURES

In this section, the PN basic models of single CIs and redundant CIs are described. In doing so, the relevant reachability graphs are built and discussed. Note that, in the following, for the sake of generality, the generic term “users” will be used when referring to those entities that are going to use a CI, such as vehicles, people, trains, or even electric power, etc.

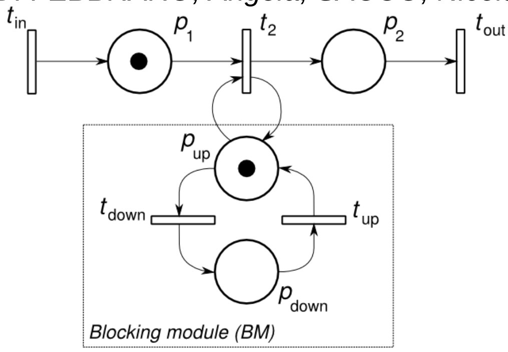

Figure 2 - Example of a single structure PN model.

Single structure model

Consider the PN depicted in Figure 2, whose places and transitions have the meanings reported in Table I and Table II. Such a net may represent a CI characterized by a single resource to provide the service. Examples of such structures are single-lane road sections between two intersections of an urban network, railway lines linking two stations, as well as bridges and tunnels. Analogously, such a model may represent a portion of the electric power distribution line.

Then, the service provided by the represented structure is modelled by transition t. Coming back to the above examples, t can model cars flowing along a road lane, a train departing from a station, or even the electric power flowing along a conductor. Analogously, transitions t_{in} and t_{out} represent cars or trains arriving at and departing from the considered structure, respectively.

Then, due to above firing rules, transition t may fire if the place p_{up} is marked. In such a condition the transition t is, in fact, L2-live, being the number of admissible firings limited only by the number of tokens in p_{in}.

On the contrary, when t_{down} fires, then t becomes not enabled. Note that, in this state, t is still L2-live because the sequence

$$\sigma = \begin{bmatrix} t_{up} & t & t & \cdots \end{bmatrix} \tag{9}$$

that contains as many firings of t as the number of tokens in p_{in}, is still admissible. Such a result is also pointed out by the relevant reachability graph depicted in Figure 3, where it is easy to note that there are no nodes (i.e., markings) without, at least, an exiting arrow (i.e., at least, an enabled transition).

Then, although single structures do not admit deadlocks, they are characterized by a high degree of criticality, since, after the firing of t_{down}, the marking of the net remains $M = [M_{p_{in}} \quad M_{p_{out}} \quad M_{p_{up}} \quad M_{p_{down}}] = [\omega_1 \quad \omega_2 \quad 0 \quad 1]$, where, as said above, the term ω_i indicates an indeterminate number of tokens in the relevant place p_i, until the transition t_{up} fires. In such a marking, $M_{p_{in}}$ may indefinitely increase (if a maximum capacity of the relevant place is not defined), whereas $M_{p_{out}}$ may only decrease until reaching zero tokens.

Table I - Meanings of places of the net in Figure 2.

Place	p_{in}	p_{out}	p_{up}	p_{down}
Meaning (when marked)	Users are going to use the CI	Users have left the CI	The modelled CI is available	The modelled CI is unavailable

Table II: Meanings of transitions of the net in Figure 2.

Transition	t_{in}	t_{out}	t	t_{down}	t_{up}
Meaning (when firing)	Users arrive at CI	Users depart from CI	Users use the CI	The modelled CI becomes unavailable	The modelled CI becomes available

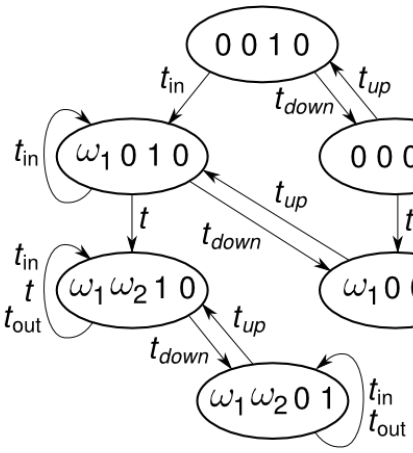

Figure 3 - Reachability graph of the single structure in Figure 2.

In other words, the modelled CI remains unavailable after a blocking event, until it is repaired and made operative again. Such a time interval does not only depend on the infrastructure itself, but also on the repairing time.

Note that such a configuration, although very simple, represents most real-world infrastructures; in effects, for instance, almost every railway line or power line can be thought of as a sequence of such a kind of modules. In addition, in such a model it is possible to take into account the stochastic occurrence of blocking events, which are modelled by means of the stochastic times associated with t_{down} and t_{up}.

To conclude, for the sake of compactness, let us introduce the Blocking Modules (BM) which represent the portion of the PN which models the enabling/disabling of the service provided by the considered CI.

Redundant structure model

Consider the PN representing a redundant CI depicted in Figure 4, whose places and transitions have the meanings reported in Table III and Table IV. Such a net represents all the CIs characterized by two parallel structures providing the same service. Valuable examples of such a configuration are given by highways or, in general, by two-lane roads for each direction. In these cases, it is intuitive that when only a lane is blocked, the other one may be still available. Then, the models representing CIs of such a class must take into account the described behaviour.

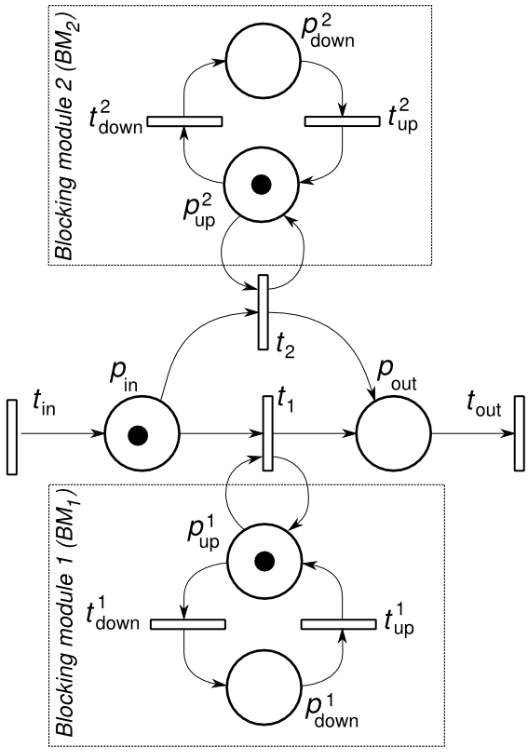

Figure 5 - Example of redundant infrastructures.

In doing so, consider again the model in Figure 4. In this case, the service provided by the CI is modelled by transitions t_1 and t_2. Indeed, whenever at least one of such transitions is enabled, the represented CI can provide its service, i.e., it is not blocked. In effects, as it is easy to note in the reachability graph reported in Figure 5, the only system condition in which both t_1 and t_2 are contemporarily disabled is the one characterized by the marking

$$M(k) = [M_{p_{in}} \quad M_{p_{out}} \quad M_{p^1_{up}} \quad M_{p^1_{down}} \quad M_{p^2_{up}} \quad M_{p^2_{down}}] = [\omega_1 \quad \omega_2 \quad 0 \quad 1 \quad 0 \quad 1], \tag{10}$$

where the term ω_i indicates an indeterminate number of tokens in the relevant place p_i. Such a marking, which is reached by means of both the firing sequences $\sigma = [\cdots \quad t^1_{down} \quad \hat{\sigma}_1 \quad t^2_{down} \quad \cdots]$ or $\sigma = [\cdots \quad t^2_{down} \quad \hat{\sigma}_2 \quad t^1_{down} \quad \cdots]$, where $\hat{\sigma}_1$ (resp., $\hat{\sigma}_2$) represents any sequence that not gathers t^1_{up} (resp., t^2_{up}), which also expresses the fact that, after the firing of t^1_{down} or t^2_{down}, the transition t_2 or t_1 may fire an indefinite number of times, respectively.

Evidently, such sequences are not much probable, especially when the repairing time, that is, the time elapsed between the firings of t^i_{down}, $i = 1,2$, and t^i_{up}, $i = 1,2$, is short. Then, since the probability that this infrastructure configuration becomes entirely blocked is less than that of the single infrastructure configuration, it is possible to conclude, intuitively, that the infrastructure in Figure 4 is more robust that the one in Figure 2. Such a conclusion may be reached also taking into account the relevant performances. Then, without losing generality, suppose that the CI in Figure 4 represents a two-lane highway stretch.

When an accident blocks only one of the two lanes, vehicles can still flow, although with a reduced flow. In equations, the mean section flow may be computed as

$$\bar{f} \cong \bar{f}_1 + \bar{f}_2 = \frac{1}{\frac{1}{H_1}\sum_{h=1,2,\ldots,H_1}\theta_1(h)} + \frac{1}{\frac{1}{H_2}\sum_{h=1,2,\ldots,H_2}\theta_2(h)}, \qquad (11)$$

where H_i , $i = 1,2$, is the number of firing of transition t_i , $i = 1,2$, during the considered time period. Then, when t_1 or t_2 is disabled, the mean flow becomes

$$\bar{f} \cong \bar{f}_2 = \frac{1}{\frac{1}{H_2}\sum_{h=1,2,\ldots,H_2}\theta_2(h)}, \qquad (12)$$

or

$$\bar{f} \cong \bar{f}_1 = \frac{1}{\frac{1}{H_1}\sum_{h=1,2,\ldots,H_1}\theta_1(h)}, \qquad (13)$$

respectively. Note that such mean flows may be computed by means or repeated simulations, so as to take into account the stochasticity represented by means of the stochastic transitions t^i_{down} , $i = 1,2$, and t^i_{up} , $i = 1,2$.

Summing up, it is also possible to note that the model described in this section may be generalized to represent CIs characterized by three or more parallel, independent services, by simply adding parallel transitions t_i , $i > 2$, and the relevant blocking modules BM_i , $i > 2$.

Table III - Meanings of places of the net in Figure 5.

Place	p_{in}	p_{out}	p^i_{up} , $i = 1,2$	p^i_{down} , $i = 1,2$
Meaning (when marked)	Users are going to use the CI	Users have left the CI	The service i , $i = 1,2$, of the modelled CI is available	The service i , $i = 1,2$, of the modelled CI is available

Table IV - Meanings of transitions of the net in Figure 5.

Transition	t_{in}	t_{out}	t_i , $i = 1,2$	t^i_{down} , $i = 1,2$	t^i_{up} , $i = 1,2$
Meaning (when firing)	Users arrive at the CI	Users depart from the CI	Users use the CI	The service i , $i = 1,2$, of the modelled CI becomes unavailable	The service i , $i = 1,2$, of the modelled CI becomes available

Combined infrastructures

In this section, the PN model representing the interaction of two different kinds of infrastructures is described. The main task is to show how PN may model different kinds of infrastructures and their interactions. Despite this, such a section simply gives a glimpse of the modelling approach, and then the PN model and the relevant reachability graph will not be described in details. Therefore, to this aim and without losing generality, the attention will be focused on the elementary model of railway line and the relevant electric power distribution line depicted in Figure 7.

Then, the service provided by the represented structure requires that, at the same time, both the power distribution line is on and the railway lines are not blocked. Then, the relevant PN model results to be the one reported in Figure 8, whereas the meanings of its places and transitions are reported in Table V and Table VI.

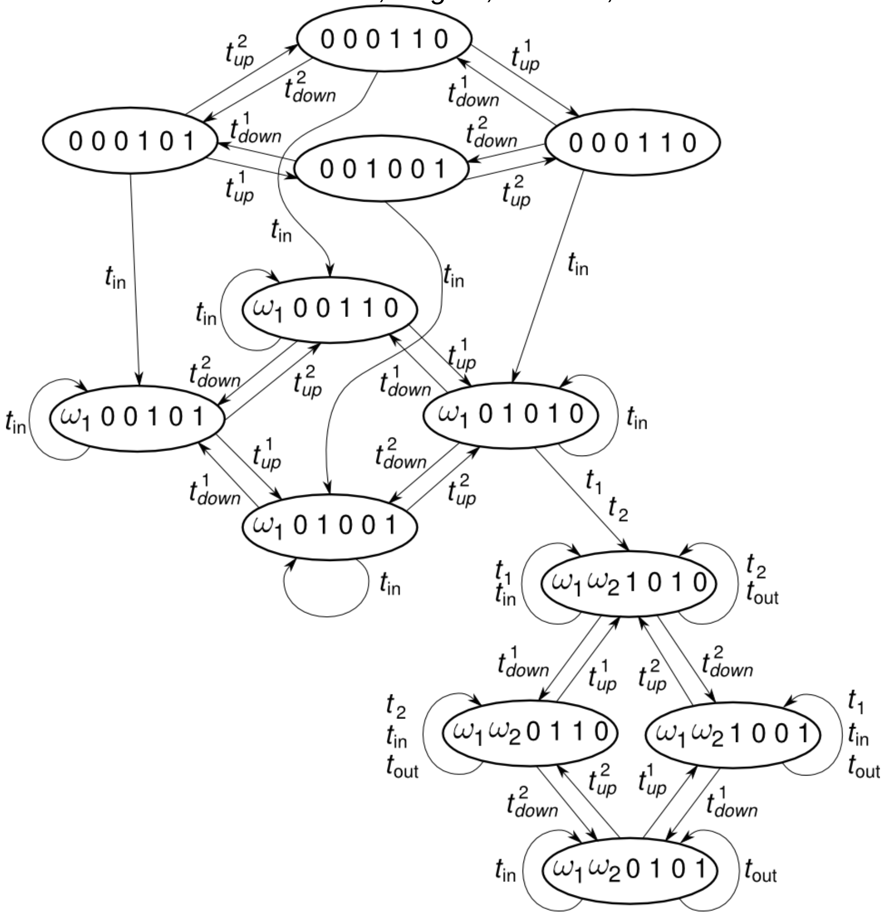

Figure 6 - Reachability graph of the single structure in Figure 5.

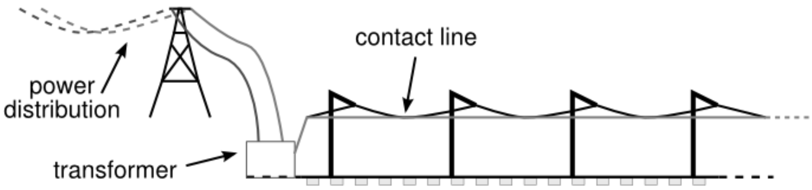

Figure 7 - Elementary model of railway line and the relevant electric power distribution line.

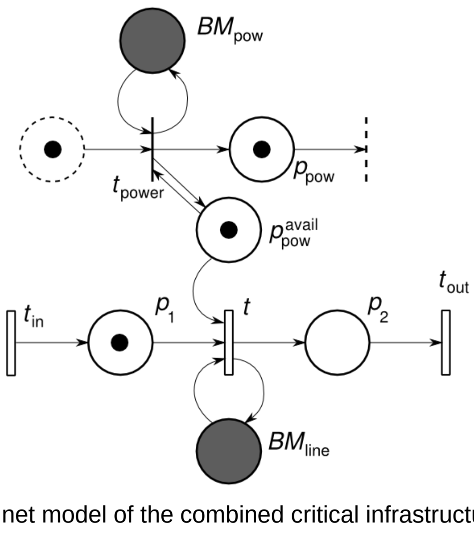

Figure 8 – Petri net model of the combined critical infrastructures in Figure 4.

Table V- Meanings of places of the net in Figure 8.

Place	p_{in}	p_{out}	p_{pow}
Meaning (when marked)	Trains are going to cross the rail stretch	Trains have left the rail stretch	Electric power is available for the rail stretch

Table VI - Meanings of transitions of the net in Figure 8.

Transition	t_{in}	t_{out}	t	t_{pow}	t_{pow}^{avail}
Meaning (when firing)	Trains arrive at the rail stretch	Trains depart from the rail stretch	Trains cross the rail stretch	Power becomes available for the rail stretch	Power becomes available for trains in the rail stretch

Note that in such a PN representation both the subnet modelling the train dynamics and the subnet modelling energy distribution are characterised by “blocking modules” as the one above presented. In particular, the model of the “train blocking module BM_{train} is equal to the one in Figure 3, and then it is not reported.

As regards the reachability, it is easily derived by some considerations on the one corresponding to the single infrastructure in Figure 3. However, although its structure is too complex for the purposes of the present paper, and then it will not be reported, it is possible to intuitively state that, according to the above configurations, also power distribution may lead the PN into a marking that disables transition t . Again, as soon as transition t_{pow}^{up} fires, transition t returns to be enabled. As regards the line blocking module, its dynamics is identical to the one above described for the single and the redundant infrastructure.

RANKING CRITERION FOR TRANSPORTATION NETWORK CRITICALITIES

In this section, a revised formulation of the ranking criterion for transportation critical infrastructure network in Eq. (1) will be given. To this end, consider a transportation CI network and consider the mobility demand among the Origin/Destination (O/D) pairs of the considered network. Evidently, the interruption of a link making up an O/D path used by many users causes a major disutility with respect to the interruption of an O/D path used by a few users. In addition, while on one hand the interruption of some links leads to an increase of the mean travel time, on the other hand it may lead to the unreachability of some nodes, or not.

Then, taking into account such considerations, the ranking parameter defined in Eq. (1) may be reformulated as the weighted sum

$$PI_j = \alpha_{nu} nu_j + \alpha_{\Delta T} \Delta T_j + \alpha_{Up} Up_j , \tag{14}$$

where:

- nu_j represents the number of users, expressed in million of users per day, which have to choose alternative paths with respect to the shortest one, due to the interruption of link j ;

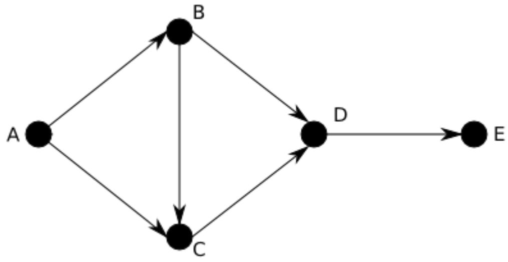

Figure 9 - Example of a complex transportation network.

- ΔT_j is the difference between the nominal Mean Travel Time (MTT) of users, computed over an a-priori fixed simulation time period, for the nominal "unblocked" network, and the MTT after the interruption of link j;
- Up_j is the number of O/D pairs which result to be unconnected due the interruption of link j;
- α_{nu}, $\alpha_{\Delta T}$, and α_{Up}, are suitable weights chosen in order to make the performance indices nu_j, ΔT_j, and Up_j comparable.

All the terms in Eq. (14) may be easily computed by means of the proposed PN model. In particular, Up_j is computed by means of the reachability tree, whereas ΔT_j may be computed by means of simulations.

CASE STUDY

In this section, a case study is described with the aim of putting into evidence the different phenomena that the proposed methodology is able to catch.
In doing so, consider the graph depicted in Figure 9 representing a railway network, where the arcs represent railway links, and nodes represent stations. For the sake of simplicity, without losing generality, in the following all the trains are assumed to depart from node A and to arrive to node E. Then, the relevant PN model is reported in Figure 10, whereas the meanings of places and transitions are summarized in Table V and Table VI, respectively.

Nominal behaviour

Consider the case in which all the arcs are available for transportation, namely the "nominal case". From the point of view of the PN model, this state is represented by the marking vectors in which the elements corresponding to the places p_{up}^i, $i = 1,2,3,4,5$, are always marked. Then, for the sake of compactness, in the following discussion, such fixed parts of the marking vectors are drop, together with the subscript in terms ω.
Then, only the markings of places p_i, $i = 1,2,3,4,5$, representing the nodes are reported. In other words, the marking after the k^{th} transition firing is defined as

$$M(k) = [M_1(k) \quad M_2(k) \quad M_3(k) \quad M_4(k) \quad M_5(k)]. \tag{15}$$

Table VII - Meanings of places of the net in Figure 10.

Place	p_1	p_2	p_3	p_4	p_5	BN_i
Meaning (when marked)	*A train is in station A*	*A train is in station B*	*A train is in station C*	*A train is in station D*	*A train is in station E*	*Blocking network of* t_i

Table VIII - Meanings of transitions of the net in Figure 10.

Transition	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
Meaning (when firing)	Trains enter the network	Trains travel along the link:						Trains leave the network
		A-B	B-D	B-C	A-C	C-D	D-E	

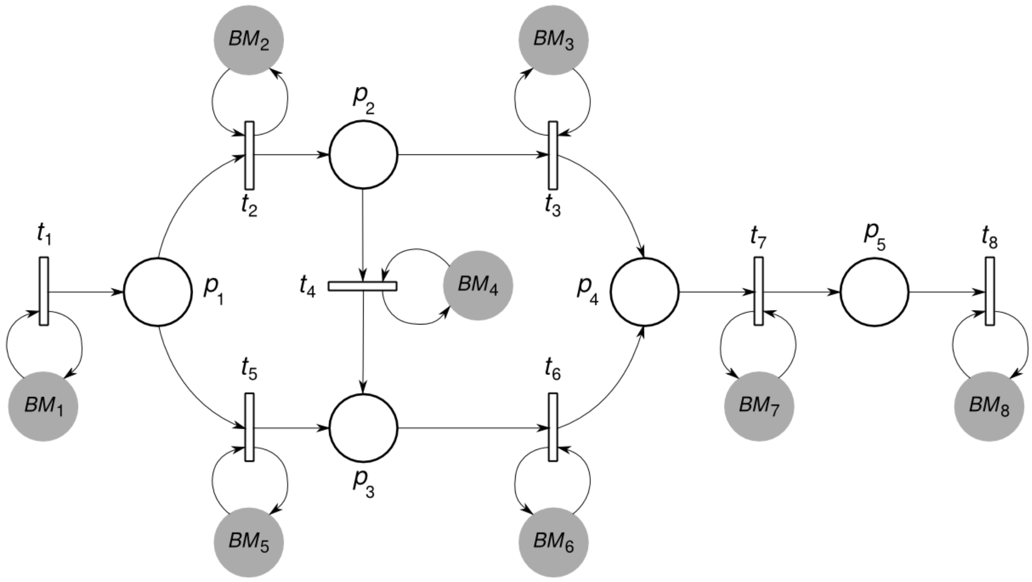

Figure 10 - Petri net model of the transportation network in Figure 9.

Therefore, consider the reachability graph of the PN in Figure 10, reported in Figure 11, where the initial marking $M_0 = [0 \quad 0 \quad 0 \quad 0 \quad 0]$ represents the condition of the railway network initially empty.

Then, as soon as trains flow throughout network links, the relevant transitions fire, thus leading the PN to the other states represented by the nodes of the reachability graph. Finally, after a while, all the links are crossed by an indefinite number of trains, thus leading to the condition represented by the marking $M(k) = [\omega \quad \omega \quad \omega \quad \omega \quad \omega]$. In this state, the most important piece of information to be pointed out is that all the transitions are enabled. In other words, trains can flow throughout all the network links. This is the nominal condition of the network.

Behaviour after blocking events

To the aim of assessing the criticality of the different links, consider the following two cases.

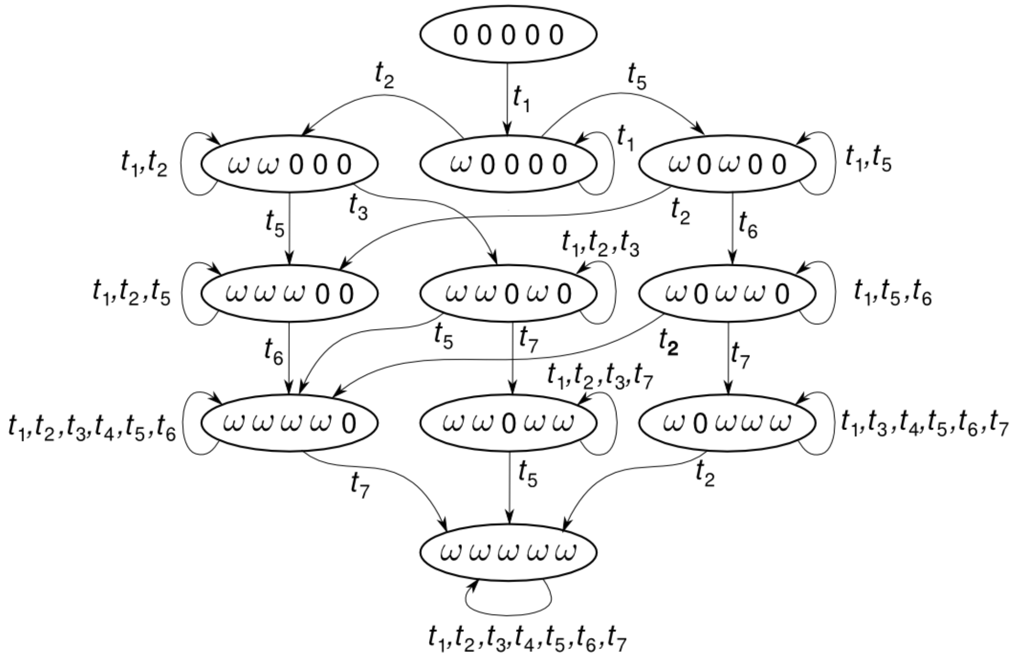

Figure 11 - Reachability graph of the Petri net in Figure 10.

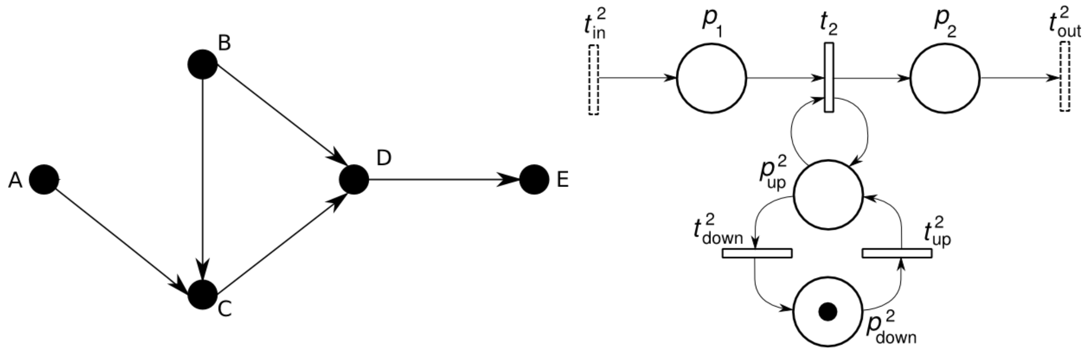

Figure 12 - Case study network configuration with link A-B blocked.

Case 1: link A-B blocked

Suppose that link A-B of the network in Figure 9 (represented by the transition t_2 in the PN model of Figure 10) becomes unavailable due to the occurrence of a blocking event. Such a condition is represented in Figure 12 where the portion of the relevant PN, modelling the considered link, is also reported. Again, with the aim of keeping the number of markings small, the marking of all the places of the blocking modules are dropped, although, the place p_{down}^2 is now assumed to be marked.

Then, looking at the relevant reachability graph reported in Figure 13, it is possible to note that the number of reachable states is now significantly reduced. In particular, the second element of the marking vector defined in Eq. (15) is always zero, thus indicating that the place p_2 (node B) is never marked (reached by trains). Moreover, looking at the labels of the arcs, it is easy to note that, in addition to transition t_2, which is directly blocked, also transitions t_3 and t_4 are never enabled nor can fire. This fact indicates that also link B-D and B-C, respectively, are never crossed by trains.

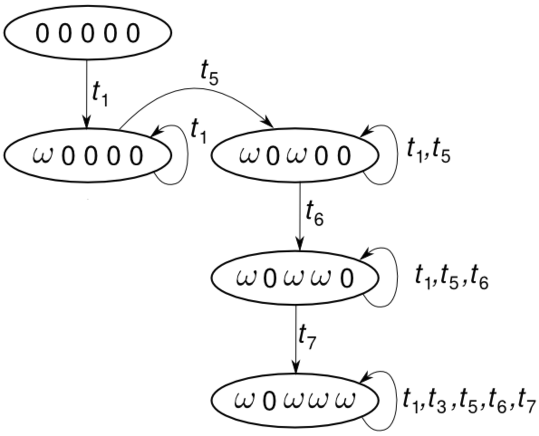

Figure 13 - Reachability graph of the PN representing the abnormal behaviour of the transportation network in Figure 10.

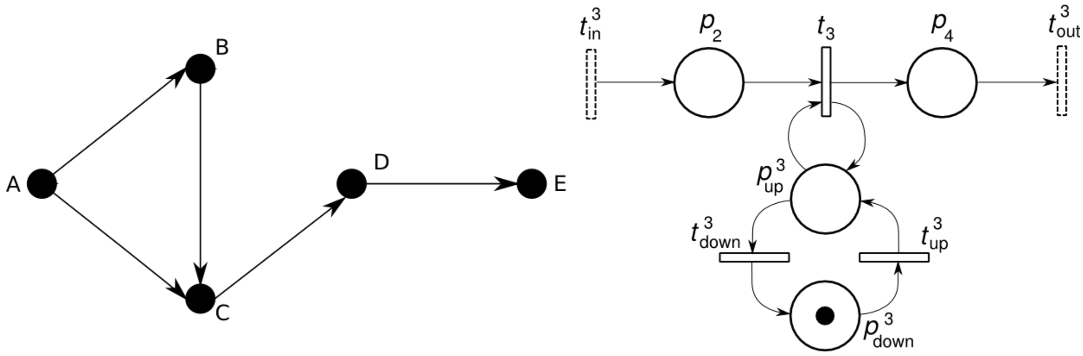

Figure 14 - Case study network configuration with link B-D blocked.

Case 2: link B-D blocked

Suppose now that link C-D in the network of Figure 9, and represented by the transition t_3 in the PN model of Figure 10, becomes unavailable due to the occurrence of a blocking event. Such a condition is represented in Figure 14, where the portion of the relevant PN modelling the considered link is also reported. In this case, the place p_{down}^3 is assumed to be marked, although, in analogy with the above case, the marking vector depicted in the reachability graph only gathers the markings of places p_i, $i = 1,2,\ldots,5$. Then, looking at the relevant reachability graph, reported in Figure 15, it is possible to note that, with respect to the nominal case, also in this case the number of reachable states is reduced. By the way, in this case it is still possible to reach the marking $M(k) = [\omega \quad \omega \quad \omega \quad \omega \quad \omega]$, that is, the nodes of the network are reachable by trains. In addition, looking at the labels of the arcs, it is easy to note that only transition t_3, which is directly blocked, is never enabled nor can fire.

Simulation and ranking

In this section, some considerations about the network simulation are reported with the aim of evaluating a ranking for the links of the considered railway network. In doing so, it is worth

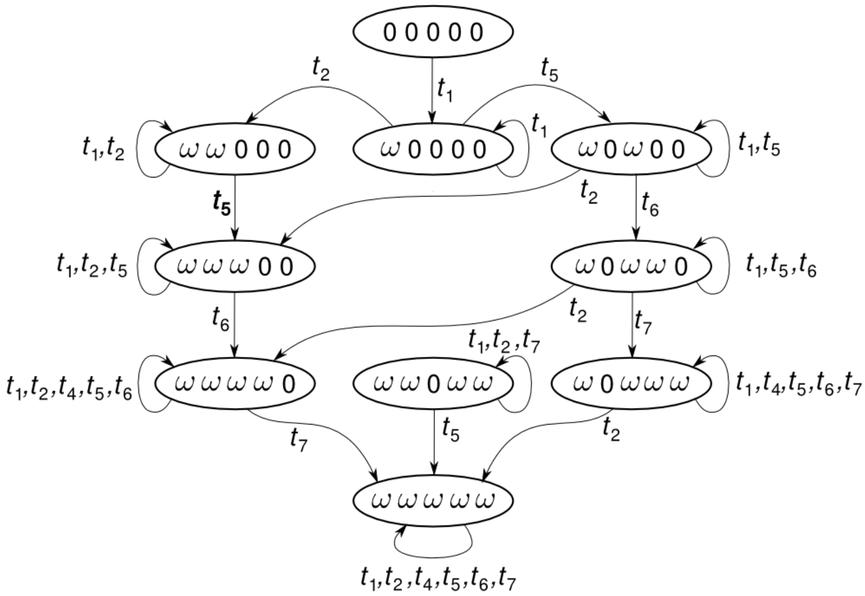

Figure 15 - Reachability graph of the PN representing the abnormal behaviour of the transportation network in Figure 14.

Table IX: Disutility and ranking parameters for the links of the network in Figure 9.

Link (transition)	nu_j	ΔT_j	Up_j	PI_j
A-B (t_2)	1	1h	0.005	1.305
B-D (t_3)	0	1h	0.005	0.505

underlining that such an analysis provide results significantly different to those achievable with methods based on graph theory, allowing, in practice, to compute also the amount of performance degrade after an event blocking.

Then, as regards the performance analysis, the following assumptions have been made:

- a one-day time horizon has been chosen;
- each link is used by 15 trains/day, with about 315 passengers on;
- the travelling times on the railway links are deterministic and equal to 1 hour;
- transitions t^i_{down} have been forced to fire manually.

Then, the results of the simulation trials in the two above considered cases are reported in Table IX. Finally, in order to compute the ranking parameter, the weights in Eq. (10) have been assumed to be $\alpha_{nu} = 0.8$, $\alpha_{\Delta T} = 0.5$, and $\alpha_{Up} = 1$, so as to make the different contributions comparable.

As regards the ranking results, link A-B represented by transition t_2 results to be the most critical one, mainly due to the disconnection between nodes A and B. On the other hand, the link represented by transition t_3 results to be the least critical one, because when it is unavailable all O/D pairs are still connected.

Considerations

The above examples show that the reachability graph analysis is able to put into evidence not only the links that are directly blocked, but also those network links and nodes which cannot be crossed or reached.
Then, when an economic evaluation of the non-reachability of some nodes, or of the interdependent unavailability of links, is available, it is possible to evaluate the indirect losses due to a blocking event occurring in the modelled complex CI network, for instance by assigning monetary costs to the parameters nu_j, ΔT_j, Up_j, and PI_j.

CONCLUSIONS

In this paper, a Petri Net analysis procedure has been developed to the end of estimating the indirect losses resulting, in networks of critical infrastructures, from safety and/or security events. In particular, the proposed model helps to individuate the most critical infrastructures in complex networks by providing the coefficients necessary to apply an easy-to-use ranking criterion.

REFERENCES

Amin, M. (2002), "Toward secure and resilient interdependent infrastructures", in Journal of Infrastructure Systems, Vol. 8, pp. 67–75.

Aposlakis, G., D. and Lemon (2005), "A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism", in Risk Analysis, vol. 25, n. 2, pp. 361-376.

Arulselvan, C. W. Commander, L. Elefteriadou, P. M. Pardalos (2009), "Detecting critical nodes in sparse graphs", in Computers & Operations Research, Volume 36, Issue 7, July 2009, pp. 2193-2200.

Ballocco, G., A. Carpignano, M. Gargiulo (2003), "Merging cut sets and reliability indexes for reliability and availability of highly meshed networks", in Proceedings of ESREL 2003, European Safety and Reliability Conference.

Bondy, J. A., U. S. R. Murty, (1980), "Graph Theory with Applications", New York: North-Holland.

Cassandras, C., S. Lafortune (2008), "Introduction to Discrete Event Systems", Springer Science.

Di Febbraro A., D. Giglio, N. Sacco (2001), "Modular representation of urban traffic systems based on hybrid Petri nets", in Proceedings of IEEE 4th International Conference on Intelligent Transportation Systems, IEEE ITSC, pp. 866-871.

Di Febbraro, A., D. Giglio, N. Sacco (2004), "On Modelling Urban Transportation Networks by means of Hybrid Petri Nets", in Control Engineering in Practice, vol. 12, n. 10, pp. 1225-1239.

EU Commission (2008), 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, in Official Journal of the European Union.

Gursesli, O., Desrochers, A. A., (2003), “Modeling infrastructure interdependencies using Petri nets”, in Proceedings of IEEE International Conference on Systems, Man and Cybernetics, Vol. 2, pp. 1506-1512.

Kaakai, F., S. Hayat, A. El Moudni (2007), “A hybrid Petri nets-based simulation model for evaluating the design of railway transit stations”, in Simulation Modelling Practice and Theory, Vol. 15, n. 8, pp. 935-969.

Lewis, T. G. (2006), “Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation”, Wiley – Interscience.

Macaulay, T. (2008). “Critical Infrastructure”, CRC Press.

Murata T., “Petri Nets: Properties, Analysis and Applications”, in Proceedings IEEE, Vol. 77, No. 4, pp. 541-580.

Tolba, C., D. Lefebvre, P. Thomas, A. El Moudni (2005), “Continuous and timed Petri nets for the macroscopic and microscopic traffic flow modelling”, in Simulation Modelling Practice and Theory, Vol. 13, n. 5, pp. 407-436.

Ye, X., Zhou, J., Song X., (2003), “On reachability graphs of Petri nets” in Computers & Electrical Engineering, Vol. 29, n. 2, pp. 263-272.