Failures propagation in critical interdependent infrastructures

Stefano Panzieri

Dipartimento Informatica e Automazione,
Università degli Studi "Roma TRE",
via della Vasca Navale 79, Roma 00146, Italy
E-mail: panzieri@uniroma3.it

Roberto Setola*

Complex Systems and Security Lab,
Università Campus Bio-Medico di Roma,
Via A. del Portillo 21, Roma 00128, Italy
E-mail: r.setola@unicampus.it
*Corresponding author

Abstract: Welfare in developed countries strongly relies on many heterogeneous infrastructures generically named as critical infrastructures. These infrastructures, designed as autonomous systems, are actually more and more mutually dependent. This introduces new and extremely dangerous vulnerabilities in the overall system because an accidental or a malicious fault (e.g. terroristic attack) could exploit these 'connections' to unpredictably spread, amplifying its negative consequences and affecting unforeseeable and haphazard sets of users. In this paper, we analyse performance degradation induced on this system of systems by the presence and spreading of failures in order to emphasise the most critical links existing among different phenomena. Due to uncertainties that characterise these systems, we use Fuzzy Numbers (FNs) to represent involved quantities. This allows a modelling approach that can be set up using also qualitative information that are easier to obtain from experts and stakeholders. Moreover, this choice brings to a better characterisation of the level of confidence of our results. Preliminary results on a simple case study illustrate the effectiveness of the proposed approach.

Keywords: interdependencies; critical infrastructures; complex systems; critical infrastructure protection; CIP; large-scale systems; heterogeneous complex networks; input-output inoperability.

Reference to this paper should be made as follows: Panzieri, S and Setola, R. (2008) 'Failures propagation in critical interdependent infrastructures', *Int. J. Modelling, Identification and Control*, Vol. 3, No. 1, pp.69–78.

Biographical notes: Stefano Panzieri received the 'Laurea' degree in Electronic Engineering in 1989 and a PhD in Systems Engineering in 1994, both from the University of Roma 'La Sapienza'. Since February 1996, he is with the 'Dipartimento di Informatica e Automazione' of University of 'Roma Tre', where currently is an Associate Professor. His research interests are in the field of industrial control systems, and in particular the study of iterative learning control applied to robots and the area of mobile robots with a special attention to the problem of localisation and sensor-based navigation.

Roberto Setola received his Laurea degree in Electronic Engineering (1992) and his PhD in Electronic Engineering and Computer Science (1996) from the University of Naples. From 1999 to 2004, he served at the Italian Prime Minister's Office, and presently he is Professor of Automatic Control at University CAMPUS Bio-Medico di Roma. He has been the Technical Responsible of the Italian Government Working Group on Critical Infrastructure Protection and Member of G8 Senior Experts' group for Critical Information Infrastructure Protection. He has written 3 books about simulation of dynamic systems and more than 100 scientific papers related with modelling, estimation and control of complex systems (electromechanical, biological and social) and about critical infrastructures.

1 Introduction

Developed countries rely on many technological infrastructures, such as: energy production, transportation and distribution; telecommunications networks; water management and supply networks; transportation (air, rail, marine and surface); healthcare and hospitals systems; banking and financial services (US Government, 2003a; Wigert and Dunn, 2006). Due to their relevance, they are generally referred as *critical infrastructures* because

'if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.' (EU Commission, 2005).

In the very last years, for a lot of economical, social, political and technological reasons, we observed a rapid change in the organisational, operational and technical structures of these infrastructures. Indeed, to reduce costs, to improve efficiency and to provide innovative services, infrastructures have become more and more interoperable and have extensively adopted Information and Communication Technologies (ICT). Moreover, to effectively and profitably operate in the global market in the absence of monopolistic privileges, infrastructures' stakeholders have started to focus on their core business and then to use outsourcing strategies.

Therefore, although designed as logically separated systems delivering different services, these infrastructures have become highly dependent and interdependent, each one relying (directly or indirectly) on the services provided by the others. Those connections contribute to create a very huge and complex system of systems which appears prone to cascade failures, as dramatically emphasised by the different black-outs that characterised the 2003 summer (PIC, 2004; US and Canada Power System Outage Task Force, 2004). Indeed, due to the presence of interdependencies, a failure in any subsystem may easily propagate to the others, with the result of affecting a large, unpredictable and geographically jeopardised set of users.

As an example, the failure in 1998 of the telecommunication satellite Galaxy IV in geo-stationary orbit on the US west cost (Rosenbush, 1998), beside creating communication problems (almost 90% of US pagers were affected), led to significant difficulties also in the transportation system: numerous flights were delayed due to the absence of high-quote weather information, while refueling on highways became difficult as gas stations could not process credit card transactions (for more information on interdependency related incidents see Bologna and Setola (2005)).

Another dramatically illustrative example happened at the beginning of 2004 in Rome (PIC, 2004). Here, the failure in the air conditioning system of an important telecom node caused a large blackout into land and wireless telecommunications (affecting almost all the service providers), the quitting of the financial transaction into 5000 banks and in 3000 postal offices, and also difficulties at the international airport, where about 70% of check-in desks were forced to use manual procedures.

In addition to vulnerability due to accidental and natural failures, critical infrastructures, for their increased relevance, are becoming targets for terrorist and criminal actions (OCIPEP, 2003). Indeed, attacks could be carried on against infrastructures to create damage, panic, mistrust or even to increase the effects of more traditional acts of terrorism, for example, slowing down emergency services and delaying rescue operations (US GAO, 2003).

Due to the relevance of the topic, different approaches have been proposed to estimate possible impacts of failures in this interacting scenario. However, as illustrated in Casalicchio et al. (2006) and Wigert and Dunn (2006), many of them are qualitative techniques mainly devoted to identify and to catalogue the different critical infrastructures.

These approaches, also because they are devoted to politicians and decision makers, appear highly abstract and only partially able to discover elements neglected by the experts.

An interesting approach is the Input-output Inoperability Model (IIM) developed by Haimes and Jiang (2001) that specialised the economic market equilibrium model of (Leontief, 1966). This model aims to capture inside to a 'simple' framework the overall consequences that a negative event may produce in an interdependent scenario. The model analyses how inoperability, that is, incapacity to correctly perform its own task, in one economic sector (e.g. electric industry) influences the other and how inoperability is propagated and amplified due to interdependencies. The authors describe the consequences of any failure in terms of percentage of inoperability expected for each component.

This model assumes that the percentage of inoperability of each infrastructure depends, by means of given correlation terms, called Leontief coefficients, on the level of inoperability of other infrastructures and on failures induced by an external cause:

$$x_i(k+1)=f_i\,(x_1(k),\ldots,x_{i-1}(k),\, x_{i+1}(k),\ldots,x_n(k),\, u_i) \quad (1)$$

where x_i is the percentage of inoperability of ith infrastructure and u_i represents the constant external causes. When the previous function can be approximated by a linear expression

$$\mathbf{x}(k+1) \approx \mathbf{A}\mathbf{x}(k) + \mathbf{B}\mathbf{u} \quad (2)$$

the final downstream consequences of a failure represents the equilibrium point of the system

$$\overline{x} = (\mathbf{I} - \mathbf{A})^{-1}\,\mathbf{B}\mathbf{u} \quad (3)$$

Even if this formulation is very simplified, it can emphasise some important phenomena and in particular the increase of consequences due to the presence of cascade and feedback mechanisms (i.e. interdependencies). A similar, but more general approach can be found in the *influence model* (Asavathiratham et al., 2001) where each infrastructure is modelled as a Markov chain whose evolution is influenced not only by its own state, but also by the states of the neighbouring sites.

In any case, the most challenging issue to set up these models are the evaluation of the Leontief coefficients. In the formulation proposed in Haimes and Jiang (2001) and Haimes et al. (2005), they are calculated using economic statistic data extracted from the Bureau of Economic Analysis (BEA) database related to *make* and *use* matrices. Specifically, they assume that exist a direct correlation among the economical value of the different resources *used* by a given sector and their relevance for the operability of other sectors. However, as stressed also by the authors, this represent a very crude approximation. A different approach has been recently proposed in Rosato et al. (2008) where these 'macroscopic' coefficient are calculated on the base of the correlation existing among each couple of infrastructures, these latter evaluated using topological-base simulations.

Considering each infrastructure as an unicum, represents a very crude simplification that does not take into account its geographical extension and its structure. Indeed, as noted in Rinaldi et al. (2001), interactions among different components produce the emergence of behaviours that are not predictable from the knowledge of any single-isolated part. This suggests to adopt a bottom-up approach for their modelling as Complex Adaptive Systems (CAS) that is largely used in bio-complexity researches and appears particularly useful for situations with sparse or non-existent macroscale information.

According to this bottom-up philosophy, in Setola and Ulivi (2003) the authors proposed an approach where each infrastructure is decomposed into its macrocomponents and the failure propagation among them is analysed. This requires a quantitative description of the partially unknown interdependency phenomenon. To manage these uncertainties, the level of inoperability associated with each macrocomponent is represented by fuzzy values.

A different aspect of the problem is connected with the topology of the networks and their robustness. The pioneer works done by Strogats and Watts (Watts and Strogatz, 1999) and by Barabasi (Albert et al., 2000), emphasised the *small world* and *scale-free* properties of many technological infrastructures. Specifically, the presence of hubs (i.e. nodes connected with a large number of other nodes) increases the robustness with respect to accidental failures, but makes the network prone to deliberate attacks (Albert and Barabasi, 2002).

Moreover, as shown in Motter and Lai (2002) and Crucitti et al. (2004), the 'destruction' (i.e. removal) of a node forces also a global redistribution of load all over the network, inducing subsequent cascading failures. The authors stressed how this is particularly dangerous in presence of networks which exhibit a highly heterogeneous distribution of loads, even if an adequate level of over-capacity may greatly attenuate the phenomenon.

A different analysis on the role played by hubs in network robustness has been conducted also by removing some nodes in descending order of betweennes (Holme et al., 2002), or edges in descending order of betweennes (Albert et al., 2004) or range (Motter and Lai, 2002). However, as stressed in Latora and Marchiori (2004), these indexes not always correspond to the most *critical components*, that is, nodes and links that are fundamental to the functioning of the network. On the other side, such elements are the targets to protect from terrorist attacks.

However, considering systems composed by different and heterogeneous infrastructures represent an harder and less investigated challenge. Indeed, in this case one cannot simply assume that the coupled system is just a new larger system but, due to the presence of heterogeneous elements, one have to carefully consider the role played by the different nodes and the meaning of each link. In Newman et al. (2005) where the authors studied a system composed by two connected networks (L and M). In details, they assumed that, a failure in one component of the system (say L) has the effect of producing a increasing load on the other components of system L, but also a redistribution of the load in the components of model M. The authors showed that this load increase induces a shift in the critical point or, in other terms, the coupling makes the system more susceptible to large failure.

These models are mainly focused on propagation of the negative consequences induced by a given failure. However, they do not consider that the failures by themselves might propagates and then induce further faults in other elements. The combined effect of inoperability and failure propagation may give rise to very catastrophic scenario.

In this paper, we generalise the *Input-output Inoperability* model proposed in Haimes and Jiang (2001) to explicitly consider both inoperability and failure propagation. Moreover, to better handle data ambiguity and to make easier the interaction with operators and stakeholders, we use Fuzzy Numbers (FNs) to describe the different quantities.

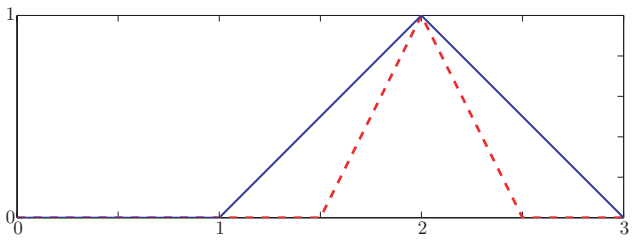
This research has been developed inside to the project Critical Infrastructure Simulation by Interdependent Agents (CISIA), promoted by the University CAMPUS Bio-Medico and the Univesity 'Roma Tre', to define a suitable methodology to analyse this class of systems.

This paper is organised as follows. First of all a brief review of FNs is summarised in Section 2. Section 3 is devoted to illustrate our model, while Section 4 deals with a procedure to identify failure propagation links. In Section 5, some simulation results are presented, while Section 6 collects some conclusive remarks.

2 Fuzzy number

FNs can be seen as the most natural way to introduce model and data uncertainty in a technical talk. Consider the simple statement from an expert 'the energy supply will last for about two days'. According to a brief interview with an expert, we can represent the value 'about two days' with one of the diagrams in Figure 1. Here the so-called triangular FNs are assumed. In particular, the larger plot represents 'I am maximally confident that it can last two days and I am sure it cannot last less than one day or more than three', while the thinner one shows less uncertainty.

Figure 1 Triangular FNs representation



FNs can actually have any shape, the most common being triangular, trapezoidal and Gaussian. The big difference in their representation is that simpler shapes can be represented with a few parameters, while completely general shapes require to be sampled over the range of possible values. Therefore, their manipulation is much more intensive in terms of memory and computations.

Without lost of generality, here triangular FNs are considered. They can be memorised using the ordered triples representing the abscissa of the three vertices. The extension of the arithmetic operations is immediate for sum

and subtraction. Indeed, these are linear operations and the resulting FN is also triangular. For example, representing two triangular FNs A and B with the triples $[a_1, a_2, a_3]$ and $[b_1, b_2, b_3]$, their sum is simply obtained as $[a_1 + b_1, a_2 + b_2, a_3 + b_3]$.

On the contrary, multiplication of two triangular FN produces a FN whose sides are parabola segments. It is easy to see that multiplying two parabolic FN, the result is described in terms of fourth order polynomials and so on. So, exact computations can easily become unmanageable, in particular in iterative procedures like those required in simulations. Two strategies are typically used to solve this problem. The first consists in discretising the FN over the range of all the possible values. This means a huge consumption of both computational and memory resources and, in any case, introduces some errors due to the discretisation. The other solution is the approximation of the parabolic FN with a triangular one, avoiding the increase of complexity. In this case the product of FNs A and B is simply given by $[a_1 \times b_1, a_2 \times b_2, a_3 \times b_3]$. The case of division can be managed in the same way, once it is verified that the three values representing the divisor have all the same sign. A division by zero would imply a poor system modelling.

A different problem is posed moving to comparison. Typically, in fuzzy logic, the result of a comparison is a fuzzy quantity so that we can say that A is a little greater then B or is much greater than B. Even if there are some experimental tentatives to use this fuzzy information in programming, we have preferred to defuzzify the result before using it. To this aim, to compute $B > A$, the centre of gravity of $B - A$ is compared with zero.

For formal definitions and more details see Chiu and Wang (2002); Giachetti and Young (1997) and Ross (2004). In this paper, fuzzy numbers are used mainly as an extension of interval arithmetic. Actually, they represent our believe in a given assertion and are more flexible to use than the 'a priori' probability. A complete analysis of the relation between probability and fuzzy measures can be found in Dubois and Prade (1998) or in the Appendix A of Ross (2004).

3 Modelling failures' impacts

Any critical infrastructure is a complex, highly non-linear, geographically dispersed cluster of systems. Moreover, the presence of interdependencies, many of them hidden or poorly understood, greatly increases the complexity of the whole system.

However, in order to understand the most relevant macro phenomena, it is useful to consider the lumped model obtained decomposing the infrastructure into its macrocomponents, that is, objects with specific and easily recognisable role. In this way, global behaviour is figured out from their interaction.

Therefore, the ith infrastructure may be modelled as an oriented graph $\mathcal{G}_i = \mathcal{G}_i(n_i, l_i)$ composed by n_i nodes and l_i arches. Nodes are the macrocomponents and the presence of an arch between the two nodes represents a functional dependency between them, that is, an exchange of goods or services from the origin to the destination.

Then, we may model the system composed by N interdependent infrastructures via a global graph $\mathcal{G} = \mathcal{G}(n, l)$ where for n holds the following property

$$\dim(n) \leq \dim(n_1) + \cdots + \dim(n_N)$$

related to the fact that some nodes might belong to more than one infrastructure. On the other side

$$\dim(l) \gg \dim(l_1) + \cdots + \dim(l_N)$$

because we have to consider cross infrastructures' dependencies, that is, the functional relations that are referred as *interlinks* in Macdonald and Bologna (2001).

Notice that when we consider a single infrastructure, the quantities that flow along arches are homogenous. On the other side, in the overall scenario, flows along arches are heterogeneous quantities.

As mentioned before, the presence of these functional dependencies, in addition to make more complex the whole system, increases its fragility due to domino effects that might amplify consequences of negative events.

Moreover, interdependencies can increase also the exposition of each macrocomponent to natural and man-made failures. Indeed, failures or attacks may exploit these links (generally poor considered and supervised) to spread among infrastructures and then affect also remote sites (from logical or geographical point of view). Indeed, as stressed in Rinaldi et al. (2001), interactions can arise from physical connections, geographical proximity, cyber dependencies or other causes. These dependencies generally have not been specifically constructed nor planned, and sometimes they do not exist at all in normal operation, but they may be created due to a failure or can emerge from the modification of the area in which infrastructures operate.

Then, when a macrocomponent is affected by a failure this may propagate to neighbours nodes using a multitude of paths that we will refer as *Failure propagation* links. Notice that mechanisms for failure diffusion are strongly related to the types and the nature of the failure itself. Indeed, an explosion is generally propagated to spatial close elements, while a cyber-virus is propagated to elements connected to cyberspace in spite of their geographical location, and so on. Accordingly, for each class of failure (i.e. set of failures that spread with the same mechanisms) we have to consider different concepts of proximity that identify different and partially disjoined sets of neighbours.

Specifically, with respect to jth class of failure we introduce the graph $\mathcal{F}^j = \mathcal{F}^j(n, f^j)$ where the presence of an arch specify that the jth type of failure may directly spread between the connected nodes.

The $\mathcal{G}$ graph and those associated with failures, are oriented and generally not fully connected, but have a partially overlapping clusterised structure. In some cases, failure graphs may be decomposed into insulated sub-graphs, or even have unconnected nodes.

In order to understand downstream consequences induced by one or more 'initial' failures, we should consider performance degradation related with two different phenomena: the absence of resources and the presence of failures. Both these phenomena, due to interdependencies, may propagate their consequences and then impact on the overall behaviour of the system.

To analyse degradation induced in the macrocomponents, we introduce the concept of *inoperability* index x_i. This index measures the capability of the ith macrocomponent to correctly perform its own task. Specifically x_i is represented by a FN defined in the range $[0,\ 1]$: when the element is perfectly working $x_i = 0$, while $x_i = 1$ means that it is completely inoperable, that is, it does not supply any resources.

Notice that using inoperability to model the different macrocomponent behaviour allow us to homogenise the quantities that flow along all the arches of $\mathcal{G}$ graph.

Let us define $F_i^*(k)$ the overall failure affecting the ith macrocomponent

$$F_i^*(k) = \min\left\{\sum_{j=1}^{m} \alpha_i^j F_i^j(k),\ 1\right\} \tag{4}$$

where $F_i^j(k)$ is the level of severity of failure of type j that affects the ith element and α_i^j are suitable FN scale factors. F_i^* and F_i^j are FN normalised in the range $[0,\ 1]$ with 0 for absence of failure and 1 as maxima amplitude.

Even if each class of failure has its own specific dynamics, as a very first approximation, we may assume that the severity of the failure of type j, that will affect at the next sample time the ith macrocomponent, depends on the externally induced failure u_i^j and on the level of severity (of the same type of the failure) that affects its neighbours:

$$\begin{aligned} &F_i^j(k+1) \\ &= \min\left\{\max\left[u_i^j(k) + \textstyle\sum_{p\neq i} \delta_{pi}^j F_p^j(k),\ r_i^j F_i^j(k)\right],\ 1\right\} \end{aligned} \tag{5}$$

where the summation is extended to all nodes of the $\mathcal{F}^j$ graph that are directly connected to the ith node. The FN coefficient δ_{pi}^j represents the attenuation of failure severity along the path from p to i.

The max operators, when r_i^j is set to 1, guarantees that the failure level cannot decrease, or in other words that there is no reparation process. On the other side, when the *repairing coefficient* is less than 1 Equation (5) includes also the dynamic associated with the restoring activities for the ith macrocomponent.

The previous equation, neglecting for sake of brevity the presence of min and max operators, may be written in compact form as

$$\mathbf{F}^j(k+1) = \mathbf{u}^j + \mathbf{R}^j\mathbf{F}^j(k) \qquad \forall\ j \in (1,\ldots,m) \tag{6}$$

where for each failure of type j, the vector $\mathbf{F}^j$ is formed with the level of severity affecting the different macrocomponent, $\mathbf{u}^j$ is the vector of external induced failure, and $\mathbf{R}^j = \{\delta_{pi}^j\}$ is a weighted instance of the incidence matrix associated with the $\mathcal{F}^j$ graph.

Notice that failure propagation paths, as mentioned before, are generally poor understood and normally described by experts with ambiguous expression like: "there are a few possibilities that this failure is propagated from entity i to entity j with a limited reduction in its level of severity". The use of FNs allows us to take into account the great level of uncertainties that characterises these relations, and permits a better handling of linguistic expressions. In the next section, we will summarise a procedure to facilitate extrapolation of these matrices from available data.

The presence of a failure in the ith component directly induces a degradation in its inoperability index, but we have also to consider the consequences related with the absence of resources. This latter term can be assumed proportional to inoperability indices of upstream nodes, then

$$x_i(k+1) = \min\left\{\beta_i F_i^*(k) + \sum_{q\neq i} a_{iq}x_q(k),\ 1\right\} \tag{7}$$

where β_i is a suitable FN scale factor, and the summation is extended to all nodes of the $\mathcal{G}$ graph that are directly connected with the ith one. The coefficients a_{iq} are FNs that represent, similarly to Leontief coefficients (Haimes and Jiang, 2001), how the inoperability of node q affects the one of node i.

Notice that $a_{iq} = 1$ means that the complete inoperability of the qth macrocomponent induces a complete inoperability in the ith one. On the other side, $\sum_{q\neq i} a_{iq} < 1$ means that the ith macrocomponent preserves some working capabilities (e.g. thanks to the presence of buffers, UPS etc.) in spite of the level of inoperability of its neighbours. Moreover, $\beta_i \sum_{j=1}^{m} \alpha_i^j < 1$ means that the macrocomponent is provided with protection mechanisms able to limit the impacts of failures, that is, to avoid complete inoperability of the elements. Finally,

$$\beta_i \sum_{j=1}^{m} \alpha_i^j + \sum_{q\neq i} a_{iq} > 1$$

means that operability of the ith macrocomponent may be nullified due to some combinations of direct (first summation) and indirect (second summation) failures.

As before, neglecting the min operator, Equation (7) may be put in a compact form

$$\mathbf{x}(k+1) = \beta^T\mathbf{F}^*(k) + \mathbf{A}\mathbf{x}(k) \tag{8}$$

where the vectors $\mathbf{x}$ and $\mathbf{F}^*$ represent, respectively, the inoperability indexes and the overall failures associated with the different nodes. $\mathbf{A} = \{a_{iq}\}$ is a weighted instance of the incidence matrix associated with $\mathcal{G}$.

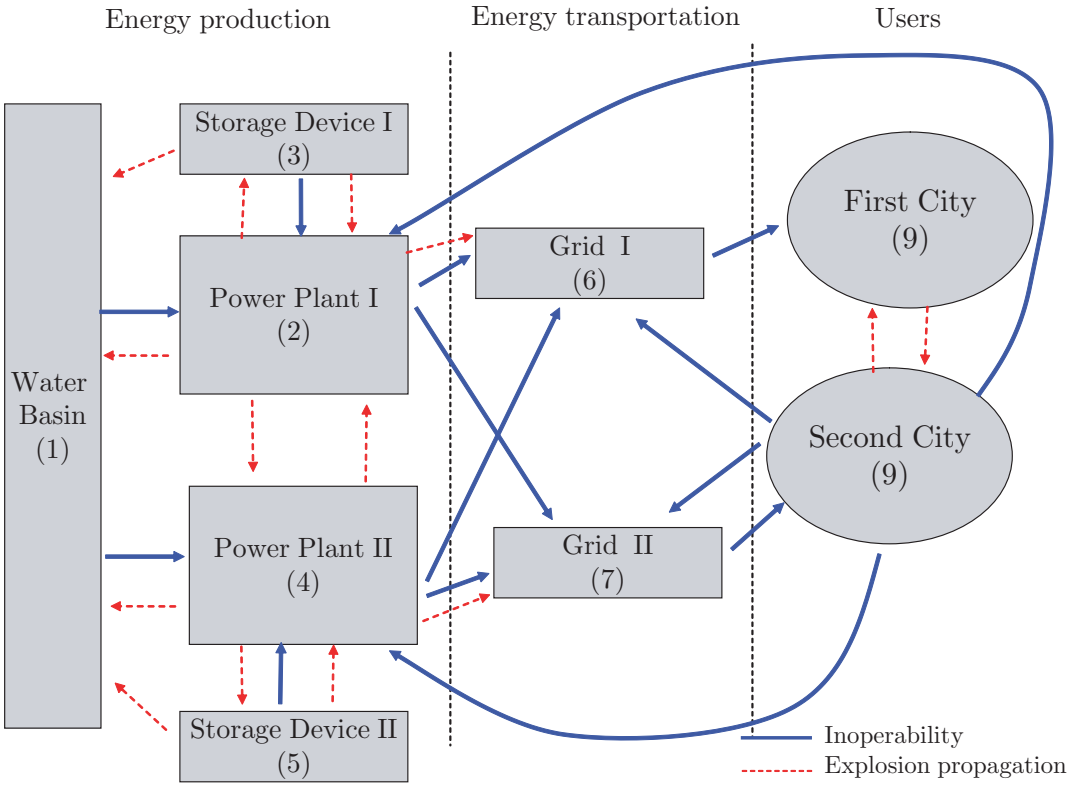
Notice that all entries in $\mathbf{A}$ and $\mathbf{R^j}$ matrices are FN normalised in the range $[0,\ 1]$, and their main diagonals are zero.

4 How evaluate failure propagation matrices

As mentioned before, failures may propagate via a multitude of mechanisms that exploit different propagation paths. Some of these, especially ones related to functional dependencies, are quite well understood by experts. On the other side, some are scarcely considered because they largely depend on interdependencies or other phenomena that are rarely considered when infrastructures are constructed.

To partially overcome these drawbacks, analysts have to adopt specific procedures able to support them in discovering and rating interdependencies and, more specifically, failure propagation links. In the following, we describe a possible strategy.

Figure 2 The case study scenario. Solid line represents functional dependencies, while dotted lines are explosion-based failure propagation links



First of all, with the help of experts, the analyst should identify the different classes of failures that might affects the scenario under the examination: explosion, flood, short-circuit, fire, PC-virus, etc. Then, for each one, he should identify how it spreads. The main mechanisms to be considered, extending the taxonomy proposed in Rinaldi et al. (2001), are:

- *Physical spreading*: failures may spread through physical linkages (i.e. related to exchange of physical quantities). Each time there is a material link among any two elements, we have to ask if the considered failure might propagate along it. These links are generally well-known to infrastructure's experts and could be read from functional schemes.
- *Geographical spreading*: possible among entities that are in close spatial proximity. In this case, the question to consider is: if this type of failure affects that macrocomponent, can it induce failures also in one or more near elements? Notice that these failure propagation links can be discovered quite easily comparing infrastructures' maps.
- *Cyber spreading*: spreading of faults associated with the cyberspace (e.g. virus, worm, etc.). Cyber interdependencies are generally less understood by experts even, for some aspects, they are the most important ones (US Government, 2003b). With a crude approximation, we can assume that cyber-dependency, due to its global characteristics (Rinaldi et al., 2001), induces the presence of a unicum giant fully connected cluster or, in other words, any system that uses the cyberspace is directly connected with any other system that uses the virtual space. If the granularity of the description is deep enough, we can have only a subset of the infrastructure affected by faults spread along this link, like computers and apparatus connected to the cyberspace. SCADA systems, for example, could continue to work even if the business network goes down.
- *Sociologic spreading*: related with behaviour of people during crisis. Modelling these relations is a very difficult task due to the huge quantities of factors to take into account, and also because humans may choose to follow or to disobey rules or stereotypic behaviours.

After aggregating these information, it is possible to identify the graph associated with the specific class of failure, that is, $\mathcal{F}^j$.

In order to obtain the corresponding incidence matrix, we need to associate to each arch the suitable value. Some of these value may be semi-automatically obtained starting from information about infrastructures, for example, *geographical spreading* may be evaluated on the base of macrocomponent's location. For the other, the help of some experts is needed. In this operation, the use of FNs allow a simplification due to their capability to handle statements like '*the failure is spread very easily*' or '*there is quite no spread of failure*' and so on.

5 Simulation results

In order to evaluate the importance of considering in an explicit form failures' propagation, we have analysed a

simple scenario composed by several infrastructures logically organised into three sectors:

- *Energy production*: this sector groups two power plants with associated fuel storage and a common water basin. These elements are geographically close.
- *Energy transportation network*: composed by two interconnected electrical grids.
- *Users*: two close urban areas. We assume that inside the second city is located the centre that supervises and controls the power plants and the grids.

In a very simplified manner, we assume that power plants need, in order to generate electricity, fuel from storage, water from the basin and control information from the second city. On the other side, the transportation network receives electricity from plants, control signals from the second city and supplies the urban areas. Finally, urban areas need electricity to provide different services to the populations.

Figure 2 depicts the scenario. Solid lines represent functional dependencies existing among the different macrocomponents, that is, the graph $\mathcal{G}$. The presence of a link means that the arrowhead component needs goods or services produced by the other element, or, in other terms, that the inoperability of this latter influences the arrowhead macrocomponent. These information, together with the corresponding scale factors, are collected into the incidence matrix $\mathbf{A}$ introduced in (8). For brevity, we report only the not zero entries:

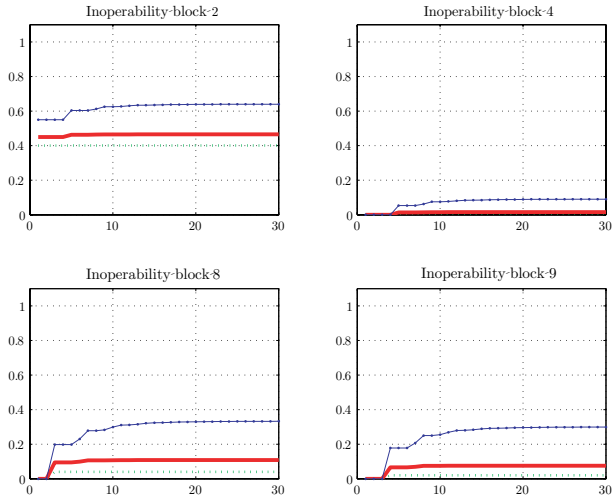
$$
\begin{aligned}
A(2,1) &= [0.05\ 0,\ 3\ 0.4] \\
A(2,3) &= [0.3\ 0,\ 4\ 0.5] \\
A(2,9) &= [0.05\ 0,\ 2\ 0.3] \\
A(4,1) &= [0.05\ 0,\ 3\ 0.4] \\
A(4,5) &= [0.35\ 0,\ 4\ 0.45] \\
A(4,9) &= [0.05\ 0,\ 2\ 0.3] \\
A(6,2) &= [0.4\ 0,\ 5\ 0.6] \\
A(6,4) &= [0.2\ 0,\ 3\ 0.4] \\
A(6,9) &= [0.01\ 0,\ 1\ 0.2] \\
A(7,2) &= [0.2\ 0,\ 3\ 0.4] \\
A(7,4) &= [0.3\ 0,\ 5\ 0.6] \\
A(7,9) &= [0.01\ 0,\ 1\ 0.2] \\
A(8,7) &= [0.5\ 0,\ 7\ 0.9] \\
A(9,8) &= [0.5\ 0,\ 7\ 0.9]
\end{aligned}
$$

Assume now that there is an explosion in the first power plant (block number 2) of medium severity ($u_2^e = [0, 40\ 0, 45\ 0, 50]$). Which are the downstream consequences of this failure?

Let us assume, for an instant, that the failure does not spread. In this hypothesis, we can consider the steady-state form of Equation (5), and then only Equation (7) has to be used to evaluate the overall consequences of the explosion. Without loss of generality in the following we will assume for simplicity $\beta = 1$.

Due to interdependencies, consequences are not limited to power plant but are spreaded along, as shown in Figure 3 where the inoperability of the two power plants and of the two cities are reported. However, looking to Figure 3, it is evident that inoperability of the faulted plant is further increased due to cascade effects. This can be explained analysing the schema of Figure 2: failure in power plant induces inoperability in the electric grid, this induces inoperability in urban areas and specifically in the second one (block number 9) where is located the control centre. This exacerbates problems in the second power plant (block number 4).

Figure 3 Inoperability, in the absence of failure propagation, of first power plant (block 2), second power plant (block 4), first city (block 8) and second city (block 9) (all values are FN)



As evident looking to the simulation results, because we have adopted a triangular FNs representation of the different quantities, the time histories of the latter are composed by three curves. The middle one (i.e. the solid line) represents the most 'believable' behaviour, while the other lines represent, respectively, an estimation of the best and worst case. Moreover, we are able to characterise the evolution of the uncertainties that, for each variable, is proportional to the difference between its maximum (line-dotted line) and minimum (dotted line) values.

If we consider that explosion by itself may spread, the scenario becomes more dramatic.

Indeed, an explosion may induce into elements in close geographic proximity further explosions and so on. This phenomena is illustrated in Figure 2 where dotted lines indicate links along which the explosion 'failure' propagates. The corresponding incidence matrix, reporting for brevity only the not zero entries, is

$$
\begin{aligned}
F^e(1,2) &= [0,\ 05\ 0,\ 2\ 0,\ 4] \\
F^e(1,3) &= [0,\ 2\ 0,\ 3\ 0,\ 5] \\
F^e(1,4) &= [0,\ 05\ 0,\ 2\ 0,\ 4] \\
F^e(1,5) &= [0,\ 2\ 0,\ 3\ 0,\ 5] \\
F^e(2,3) &= [0,\ 2\ 0,\ 3\ 0,\ 5] \\
F^e(2,4) &= [0,\ 1\ 0,\ 15\ 0,\ 2] \\
F^e(3,2) &= [0,\ 1\ 0,\ 3\ 0,\ 4] \\
F^e(4,2) &= [0,\ 1\ 0,\ 15\ 0,\ 2] \\
F^e(4,5) &= [0,\ 2\ 0,\ 4\ 0,\ 5] \\
F^e(5,4) &= [0,\ 1\ 0,\ 15\ 0,\ 3] \\
F^e(6,2) &= [0\ 0,\ 2\ 0,\ 4] \\
F^e(7,4) &= [0\ 0,\ 1\ 0,\ 25] \\
F^e(8,9) &= [0,\ 3\ 0,\ 5\ 0,\ 7] \\
F^e(1,3) &= [0,\ 2\ 0,\ 3\ 0,\ 6]
\end{aligned}
$$

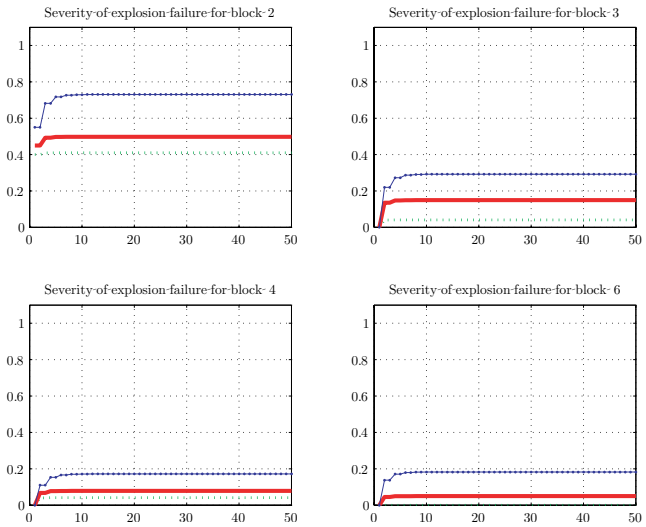
Notice that, as mentioned in the previous section, these quantities are generally characterised via a great level of uncertainties.

The impact that a failure of type *explosion* may induce on each macrocomponents is measured via α_i^e coefficients that represent the amount of failure induced by an explosion of maxima amplitude on the ith element. We assume, on the base of macrocomponents' characteristics, following coefficients:

$$\begin{aligned}
\alpha_1^e &= [0,05\ 0,1\ 0,3] \\
\alpha_2^e &= [1\ 1\ 1] \\
\alpha_3^e &= [0,7\ 0,8\ 1] \\
\alpha_4^e &= [1\ 1\ 1] \\
\alpha_5^e &= [0,7\ 0,8\ 1] \\
\alpha_6^e &= [0,1\ 0,2\ 0,3] \\
\alpha_7^e &= [0,1\ 0,2\ 0,3] \\
\alpha_8^e &= [0,2\ 0,3\ 0,5] \\
\alpha_9^e &= [0,2\ 0,3\ 0,5]
\end{aligned}$$

Using (5) can be seen that explosion is spread, with different level of severity, to all the neighbours of the power plant (see Figure 4). Now, as evident from Figure 5, this phenomena significantly contributes to augment degradations.

Figure 4 Level of severity of explosion failure for the first power plant (block 2), fuel storage of first power plant (block 3), second power plant (block 4), and first electric grid (block 6) (all values are FN)



Let us now consider that exogenous failure, that is the explosion of the first power plant (block 2) coded via u_2^e variable, last only for a short period of time, and that the first power plant could be progressively repaired with a repairing coefficient

$$r_2^e = [0,6\ 0,8\ 0,8]$$

we assume that no reparations is performed in the other macrocomponents, that is, $r_i^e = 1\ \forall\ i \neq 2$. Looking to Figures 6 and 7, it is evident that even in this case some residual 'explosion' failure is still present into the first power plant (block 2). This is due to propagation of explosion failures from the non-repaired neighbours. Moreover, as evident from the figures, the level of inoperability of the other elements remains high.

Figure 5 Inoperability of first power plant (block 2), second power plant (block 4), first city (block 8) and second city (block 9) (all values are FN)

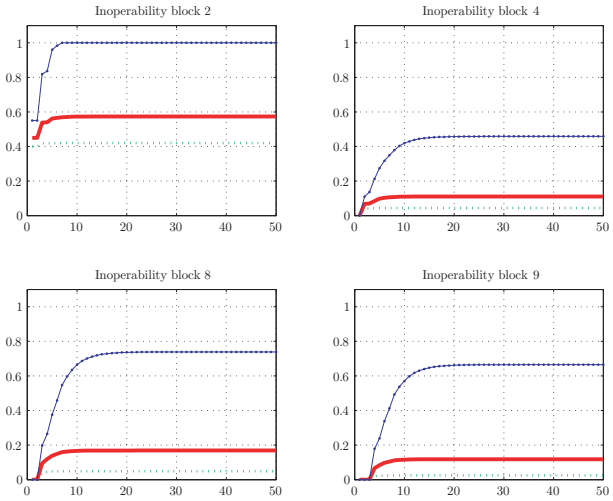
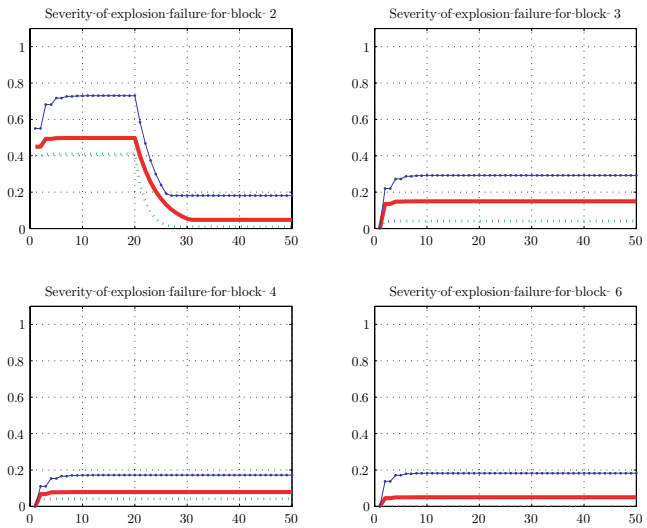


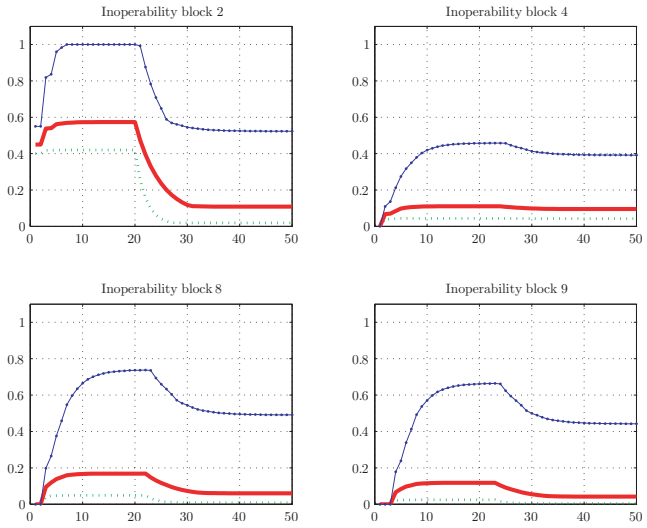
Figure 6 Inoperability, in the presence of repearing action, of first power plant (block 2), second power plant (block 4), first city (block 8) and second city (block 9) (all values are FN)



6 Conclusions

Actual socio-technological scenario is characterised by the increased importance of many and heterogeneous infrastructures. Due to their relevance, these systems are more and more considered as possible targets for terroristic or criminal attacks. For a lot of reasons, these infrastructures are becoming tightly coupled due to the presence of dependencies and interdependencies (many of them poorly known or completely hidden). This phenomena represents a very dangerous element because it increases the fragility of the whole system and makes it more prone to very large failure as dramatically shown in some recent episodes.

Figure 7 Inoperability, in the presence of repearing action, of first power plant (block 2), second power plant (block 4), first city (block 8) and second city (block 9) (all values are FN)



In this scenario, it is important to understand the overall consequences of a given failure in order to focalise security initiatives. In this paper, we have illustrated a model able to characterise both failures and performance degradation propagation. Indeed, it is mandatory to consider these two phenomena tied together because, from their interaction, can emerge a more realistic crisis scenario.

Specifically, our result emphasises how it is important to define strategies devoted both to reduce the level of coupling existing among infrastructures, and to increase capabilities of each single element to prevent cascade effect, that is, to reduce the possibility that a given failure is transmitted to other elements.

The proposed model is focused mainly on network properties, and to obtain more significant results, we need to match it with the dynamic modelling of each single macrocomponent. In this way, we can better understand how a given failure is propagated through the elements and, at the same time, which are the consequences that can be induced on each element. One of the next goals of the CISIA project will be to understand if this propagation can induce failures of *different* nature.

As a second aspect, future work will concern topological properties of the network. Our attention will be focused on the identification of parameters able to help the analysts to identify the most *critical* components, that is, the elements which need to be more (and urgently) protected.

References

Albert, R., Albert, I. and Nakarado, G. (2004) 'Structural vulnerability of the North American power grid', *Physical Review E*, Vol. 69.

Albert, R. and Barabasi, A. (2002) 'Statistical mechanics of complex networks', *Reviews of Modern Physics*, Vol. 74, pp.48–97.

Albert, R., Jeong, H. and Barabasi, A. (2000) 'Error and attack tolerance of complex networks', *Nature*, Vol. 406, pp.378–382.

Asavathiratham, S., Leiseutre, B. and Verghese, G. (2001) 'The Influence Model', *IEEE Control System Magazine*, pp.52–64.

Bologna, S. and Setola, R. (2005) 'The need to improve local self-awareness in CIP/CIIP', *Procedings of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005)*, Darmstadt, Germany, pp.84–89.

Casalicchio, E., Donzelli, P., Setola, R. and Tucci, S. (2006) 'Modelling and simulation of interdependent critical infrastructure: the road ahead', *Modelling to Computer Systems and Networks*, London, UK Imperial College Press.

Chiu, C. and Wang, W. (2002) 'A simple computation of max and min operations for fuzzy numbers', *Fuzzy Sets and Systems*, Vol. 126, pp.273–276.

Crucitti, P., Latora, V. and Marchiori, M. (2004) 'Model for cascading failures in complex networks', *Physical Review E*, pp.69.

Dubois, D. and Prade, H. (1998) *Possibility Theory: an Approach to Computerized Processing of Uncertainty*. New York, Plenum Publishing Corporation.

E.U. Commission (2005) *Green Paper on a European Programme for Critical Infrastructure Protection COM(2005)576*, Brussels.

Giachetti, R.E. and Young, R.E. (1997) 'A parametric representation of fuzzy numbers and their arithmetic operators', *Fuzzy Sets and Systems*, Vol. 91, pp.185–202.

Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2003) *Threats to Canada's Critical Infrastructure*, TA03-001.

Haimes, Y., Horowitz, B.M., Lambert, J.H., Satos, J.R., Lian, C. and Crowther, G. (2005) 'Inoperability input-output model for interdependent infrastructure sector I: theory and methodology', *Journal of Infrastructure Systems*, pp.67–79.

Haimes, Y. and Jiang, P. (2001) 'Leontief-based model of risk in complex interconnected infrastructures', *Journal of Infrastructure Systems*, pp.1–12.

Holme, P., Kim, B., Yoon, C.N. and Han, S. (2002) 'Attack vulnerability of complex networks', *Physics Review E*, pp.65.

Italian Government Working Group on Critical Information Infrastructure Protection (PIC)(2004) *La Protezione delle Infrastrutture Critiche Informatizzate – La Realtá Italiana*, (in Italian).

Latora, V. and Marchiori, M. (2004) 'Vulnerabilty and protection of critical infrastructures', *cond-mat/0407491*.

Leontief, W.W. (1966) *Input-Output Economies*, New York, Oxford University Press.

Macdonald, R. and Bologna, S. (2001) 'Advanced modelling and simulation methods and tools for critical infrastructure protection', *Technical Report*, ACIP Project Report.

Motter, A. and Lai, Y. (2002) 'Cascade-based atacks on complex networks', *Physics Review E*, Vol. 66.

Newman, D., Nkei, B., Carreras, B., Dobson, I., Lynch, V. and Gradney, P. (2005) 'Risk assesment in complex interacting infrastructure systems', *Proceedings of 38th Hawaii International Conference on System Science*, Hawaii, Big Island.

Rinaldi, S., Peerenboom, J. and Kelly, T. (2001) 'Identifying understanding and analyzing critical infrastructure interdependencies', *IEEE Control System Magazine*, pp.11–25.

Rosato, V., Tiriticco, F., Issacharoff, L., Meloni, S., De Porcellinis, S. and Setola, R. (2008) 'Modelling interdependent infrastructures using interacting dynamical networks', *International Journal Critical Infrastructures*, pp.110–128.

Rosenbush, S. (1998) 'Satellite's death puts millions out of touch', *USA Today*.

Ross, T. (2004) *Fuzzy Logic With Engineering Applications*, Chapter 12. J. Wiley and Sons Ltd.

Setola, R. and Ulivi, G. (2003) 'Modelling interdependent critical infrastructure', in N.E. Mastorakis (Ed). *Recent Advances in Intelligent Systems and Signal Processing*, *Electrical and Computer Engineering Series*, WSEAS Press, pp.366–372.

US and Canada Power System Outage Task Force (2004) *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*.

US GAO - General Accounting Office (2003) *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233.

US Government (2003a) *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, USA, The White House.

US Government (2003b) *The National Strategy to Secure Cyberspace*, Washington, USA, The White House.

Watts, D. and Strogatz, S. (1999) 'Collective dynamics of 'small-world' networks', *Nature*, Vol. 393, pp.440–424.

Wigert, I. and Dunn, M. (2006) *International CIIP Handbook 2006*, ETH, The Swiss Federal Institute of Technology, Zurich.