Modeling cascading failures in "systems of systems" with uncertain behavior

Enrico Zio, Giovanni Sansavini

Modeling cascading failures in 'systems of systems' with uncertain behavior

E. Zio
Ecole Centrale Paris and Supelec, Paris, France
Energy Department, Politecnico di Milano. Milan, Italy

G. Sansavini
Energy Department, Politecnico di Milano, Milan, Italy

ABSTRACT: We model cascading failures in interdependent critical infrastructures (CIs). We adopt a modeling framework based on simulation, which accounts for the physical specialization of the components and their interdependencies. We analyze cascading failures triggered by the intentional removal of a single component in the CIs and study the influence of the systems operating safety margins and interdependency parameters on the consequences of the cascade. Uncertainties in the model parameters are propagated, within a probabilistic representation framework.

1 INTRODUCTION

We consider critical infrastructures (CIs); these are large scale, man-made networked systems, mostly spanning long distances, which grant the continuous production and distribution of goods (e.g. fluids, energy, data) and services (e.g. banking, health care) essential for the welfare and security of modern Society. Such infrastructures are named critical, as any incapacity or destruction would have a debilitating impact on the health, safety, security, economics and social well being (Kröger and Zio 2011).

To evaluate the vulnerability of CIs models must be built describing the flow of the physical quantities within the networks.

Functional models have been proposed to capture the basic features of CI networks within a weighted topological analysis framework which abstracts the representation of the dynamics of the CI elements (Motter and Lai 2002; Dobson, Carreras et al. 2007; Zio and Sansavini 2009). These models have been shown to shed light on the way complex networks react to faults and attacks (Kröger and Zio 2011).

A characteristic of CIs is that they are highly interconnected and mutually dependent in complex ways, both physically and through information and communication technologies used for data acquisition and control, leading to the concept of "systems of systems" (Rinaldi 2004). This adds the need of assessing the influences and limitations which interacting CIs impose on their operating conditions (Zimmerman 2001).

The functional modeling of interdependent CIs can be carried out in a simulation framework which abstracts the physical details of the individual infrastructures, but at the same time captures their essential operating features and interdependencies, and examines the emergent effects of cascading failures (Newman et al. 2005; Zio and Sansavini 2011). In such modeling framework, interdependencies are represented as links (edges) connecting nodes across the interdependent systems; these links are conceptually similar to those of the individual systems and can be bidirectional with respect to the interdependence.

In this paper, the modeling framework described above is extended to account for the physical nature of the components and their interdependencies. The propagation of cascading failures in a power transmission network is taken as reference example; its components are physically specialized in "generators" and "distributors"; the effects onto two other interdependent CIs (communication and transportation) are investigated, whereby the interdependencies are distinguished in "physical", "cyber", "geographic" and "logical" (Rinaldi et al. 2001). The analysis focuses on cascading failures triggered by the intentional removal of a single component, e.g. due to a malicious attack.

Inaccuracies in the values of the parameters of the cascading failure model may lead to erroneous estimations of the effects that a failure has on the CI system. Then, uncertainties in the model parameters are accounted for within a probabilistic framework.

The paper is organized as follows: the modeling of cascading failures in the power transmission CI with physical characterization of the components is presented in Section 2; in Section 3, the characterization of interdependencies is introduced; in Section 4, the functional model for interdependent CIs is de-

tailed; in Section 5, the proposed model is applied to three interdependent CIs whose topological structures are based on the 380 kV Italian power transmission network (TERNA 2002, Rosato, Bologna et al. 2007). Conclusions are drawn in Section 6.

2 A MODEL OF CASCADING FAILURES IN A POWER TRANSMISSION NETWORK

The model proposed represents the power grid as a network of N nodes (substations) and K edges (transmission lines). Two types of substations are distinguished: N_G generators are the sources of power and N_D distribution substations are at the outer edge of the transmission grid, as centers of local distribution grids.

While the connectedness of the power grid allows for the transmission of power over large distances, it also implies that local disturbances may propagate over the whole grid. The failure of a power line due to a lightning strike or a short-circuit leads to overloads in nearby lines. Power lines are guarded by automatic devices that take them out of service when the voltage is too high. Generating substations are designed to switch off if their power cannot be transmitted; this protective measure has the unwanted effect of diminishing power for all consumers. Another possible consequence of power line failure is the incapacitation of transmission substations, possibly causing the power from generators to not reach distribution substations and ultimately consumers.

In the unperturbed state, each distribution substation can receive power from any of the generators. As substations lose function, the number of generators, N_G^i, connected to (and able to feed) a certain distribution substation i decreases. The concept of connectivity loss, C_L, is used to quantify the average decrease in the number of generators connected to a distributing substation (Albert et al. 2004). The calculation of this parameter relies on the topological structure of the network and the available least-resistance pathways. Denoting by N_G the order of the generation subset at the unperturbed state of the network, and N_G^i the number of generation units able to supply flow to distribution node i after disruptions take place, C_L takes the following form:

$$C_L = 1 - \frac{1}{N_D}\sum_{i=1}^{N_D} N_G^i / N_G \qquad (1)$$

where the averaging is done over all distributing substations. In synthesis, C_L measures the decrease in the ability of distribution substations to receive power from the generators.

The load on a transmission or distribution substation is modeled as dependent on the number of links transiting through it, when flow is sent from each available generation node to each distribution node. In this view, the maximum load or amount of flow passing through a node is related to the node betweenness (Sabidussi 1966; Nieminen 1974; Freeman 1978; Freeman, Borgatti et al. 1991; Little 2002), calculated as the number of shortest paths that pass through a node when flow is sent from each available generation node to each distribution node. The node with the highest value of betweenness is that through which the largest electric power flows within the system. Assuming that power is routed through the most direct path, the number of shortest paths that transit through a substation is a good approximation of how much power it is transmitting, i.e. its load (Albert et al. 2004).

In the proposed modeling framework, the load at a component is then the total number of shortest paths connecting every generator to every distributor passing through that component (Newman and Girvan 2004), (Batagelj 1994). At any instant of time, the load is to be compared with the component capacity, i.e., the maximum load that it can process. In man-made CI networks, the capacity of a component is limited by technological limitations and economic considerations. For modeling purposes, it can be assumed that the capacity C_j of component j is dimensioned proportionally to its nominal load L_j at which it is designed to operate initially,

$$C_j = (1+\alpha_j)\cdot L_j \quad j = 1, 2, ..., N \qquad (2)$$

where the parameter $\alpha_j > 0$ is called the tolerance parameter of the distributing substation j. This parameter can be regarded as an operating margin allowing safe operations of the component under possible load increments. When $\alpha_j = 0$, the system is working at its limit capacity, its operating margin being null: any further load added to a component would result in its failure and removal from the network and in the propagation of a cascading failure involving a large part of the system.

When all the components are working, the network operates without problems in so far as $\alpha_j > 0$. On the contrary, the occurrence of component failures leads to a redistribution of the shortest paths in the network and, consequently, to a change in the loads of the surviving components. If the load on a component increases beyond capacity, the component fails and a new redistribution of the shortest paths and loads follows, which, as a result, can lead to a cascading effect of subsequent failures.

When looking at the potential of a cascading process triggered by the removal of a single component, two situations are expected: if prior to its removal the component is operating at a relatively small load (i.e., if a small number of shortest paths go through it), its removal will not cause major changes in the balance of loads and subsequent overload failures are unlikely; however, when the load of

the component is relatively large, its removal is likely to affect significantly the loads of other components and possibly start a sequence of overload failures. Intuitively, the following behavior is expected (Motter and Lai 2002): global cascades occur if the network exhibits a highly heterogeneous distribution of loads and the removed component is among those with highest loads; otherwise, cascades are not expected.

However, any uncertainty in the tolerance parameter α_j can result in erroneous estimations of the operating margins that ensure safe operations with respect to the propagation of failures. To account for this, the tolerance α_j is assumed to be described by a normal distribution, i.e. $\alpha_j = N(\mu_\alpha, \sigma_\alpha)$.

3 MODELLING OF INTERDEPENDENCIES AMONG CRITICAL INFRASTRUCTURES

A framework for the characterization of interdependencies has been proposed in (Rinaldi et al. 2001). Interdependencies are characterized as either physical (an output from a system is required as an input to another system), cyber (the state of a system is dependent on information transmitted through an information infrastructure), geographic (two or more systems can be affected by the same local event, i.e. because they are spatially proximate), and logical (includes all other types of interdependencies, for example related to human behavior).

Operatively, from the modeling point of view, interdependencies between CIs can be represented as edges connecting nodes belonging to different infrastructures. If a CI is not able to supply the demanded service the outgoing dependency edge is removed, thus signaling the unavailability of the desired service to other CIs. The effect of a removed dependency edge is evaluated separately in the functional model of each of the dependent infrastructures. This means that each infrastructure only sees and acts upon local information regarding dependencies (Johansson and Jonsson 2009).

In the following, physically specialized interdependencies among three CIs, i.e. power transmission, communication and railway networks, are modeled and analyzed.

4 FUNCTIONAL MODEL OF INTERDEPENDENT SYSTEMS

Only the most essential functional properties of the CIs are modeled in order to provide a clear presentation of the developed methodology. More detailed functional models, embedding additional physical features, could be developed in case a more realistic characterization of the CIs is required.

The functional models of the railway and communication CIs are quantified by a connectedness evaluation algorithm which computes the shortest path lengths, d_{ij}, between node i and j in the two CIs. Upon failure, the variation in the systems performances is then evaluated as the relative decrease in the average global efficiency, ΔE_{glob}, with respect to the unperturbed systems. The average global efficiency of a network, E_{glob}, is defined as the average of the inverse shortest path lengths in the network, i.e. $E_{glob} = \left(\sum_{i \neq j \in G} 1/d_{ij} \right) \Big/ N(N-1)$ (Latora and Marchiori 2005).

A node of the railway network is in service as long as it has access to the telecommunication system and as long as the power transmission system is supplying electricity. Hence, each node of the railway network has a cyber dependency from the telecommunication system and a physical dependency from the power transmission network. If the interdependent node in the communication network fails, the node in the railway network may fail with probability p_{cr}, while if the interdependent node in the power transmission network fails, the node in the railway network is disconnected.

A node of the communication network is in operation as long as the power transmission system is able to supply electricity. Hence, each node of the communication network has a physical dependency from the power transmission network. If the interdependent node in the power transmission network fails, the node in the railway network is disconnected.

The functional model of the power transmission network has been introduced in Section 2. An input from the communication system is required for the nodes of the power transmission network to operate. Hence, each node of the power transmission network has a cyber dependency from the communication network. If the interdependent node in the communication network fails, the node in the power transmission network may fail with probability p_{cp}.

The cyber dependencies from the communication network and the power transmission system, and from the communication network and the railway network imply different effects owing to different systems operating conditions. If communication is temporarily not required at a train station, then the effects of the unavailability of the dependent node in the communication network will not propagate to the railway network. The same argument holds for the cyber dependencies between the communication network and the power transmission system. This behavior is modeled assuming that p_{cr} and p_{cp} are described by a probability distribution, in particular two normal distributions are assumed, i.e. $p_{cr} = N(\mu_{cr}, \sigma_{cr})$ and $p_{cp} = N(\mu_{cp}, \sigma_{cp})$.

From the functional descriptions of the three CIs, it follows that cascading failures propagate in the power transmission network only due to the rerouting of the flows between generators and distributors, and their effects propagate to the communication and railway networks through the removal of the interdependency connections. Moreover, unlike the communication and the power transmission systems, which show mutual interdependencies, the operation of the transportation network are affected by the other two CIs but has no effect on them.

5 CASE STUDY

The model of cascading failure introduced in Section 2 has been applied to the topological network of the 380 kV Italian power transmission network (Figure 1). The network has N=127 nodes (N_G=30 generator and N_D=97 distributor nodes) connected by K=171 links (TERNA 2002, Rosato, Bologna et al. 2007). We simulate the propagation of cascading failures in the power transmission network and the effects on the communication and railway networks. Due to the lack of actual data, but with no loss of generality, the topological structure of the railway network has been taken identical to the structure of the power transmission network. Conversely, the base topological structure of the communication network has been taken from the power transmission network, but additional links have been added so that the neighborhood of each node forms a fully connected subgraph. For each node i, we identified the nodes k_i that are directly connected to it (forming the so called neighborhood of i), and connected k_i nodes by direct links. If node i malfunctions, information can still flow through this redundant wiring. This alteration accounts for the presence of alternative communication routes among nodes which are not 'too far' from one another.

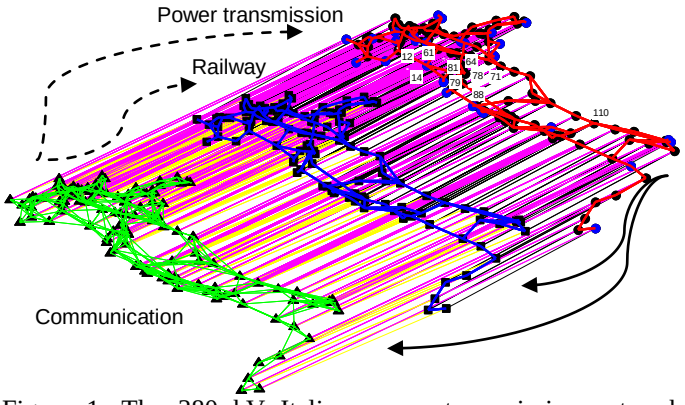

Figure 1. The 380 kV Italian power transmission network (TERNA 2002, Rosato, Bologna et al. 2007) and two interdependent CIs. Interdependencies are represented by links among the systems. Solid arrows symbolize "physical" dependencies on the power transmission infrastructure. Dashed arrows symbolize "cyber" dependencies on the communication infrastructure.

The effects of cascading failures triggered by the removal of substations in the power transmission system are first investigated. The scenario considered regards the malevolent targeted attack aiming at disconnecting node {88} (Figure 1), which handles the largest load in the system, i.e., through which pass the largest number of generator-distributor shortest paths. Previous studies have showed that power transmission networks can be very sensitive to this kind of attacks due to the difficulty of handling flow redistribution when the most congested elements fail, because neighboring elements are also working close to their full capacity and are incapable of handling significant additional flows (Duenas-Osorio & Vemuru 2009). Hence, the disconnection of a most congested node is regarded as a critical scenario of malicious attack. In addition to that, node {88} plays a strategic role in the system, bridging the northern and the southern branches of the Tyrrhenian backbone.

Once the triggering event occurs, flow redistribution takes place as a mechanism to equilibrate supply and demand constraints. The flow redistribution process is simulated at discrete time steps. At t_0 the network is intact; at t_1 a failure occurs; at t_i , $i \geq 2$ the cascading failure progresses as nodes overload and cause further failures in neighboring elements. The cascading process is followed until the response stabilizes; at this point, indicators of the severity of the cascade are computed, e.g. the connectivity loss, C_L (Section 2).

The analysis is made with respect to different values μ_α of the tolerance parameter α and fixed standard deviation, σ_α=0.3. The parameters μ_{cr} and μ_{cp} are taken equal to 0.5; σ_{cr}=0.3 and σ_{cp}=0.2. A sensitivity analysis with respect to μ_{cr} and μ_{cp} is presented in Section 5.1; on the contrary, the σ_α, σ_{cr} and σ_{cp} values have been heuristically set.

The variables α_i, p_{cr} and p_{cp} can assume only non-negative values. To describe their uncertainties normal distributions have been assumed to constrain the values to be ≥ 0. The conditional sampling of such distributions is such that when $\mu_\alpha \sim 0$, the presence of more tolerant components is favored, i.e. $\alpha_i \geq 0$, and when $\mu_{cr} \sim 0$ and $\mu_{cp} \sim 0$, a stronger coupling among the interdependent CIs is favored, i.e. $p_{cr} \geq 0$ and $p_{cp} \geq 0$, respectively.

In Figure 2, the final value of the connectivity loss, C_L, obtained after the system has stabilized in response to the disconnection of node {88}, is plotted versus μ_α, the mean value of the probability distribution of the tolerance parameter, α.

Values of μ_α=200% of the design working load have been considered as further increments of μ_α do not improve C_L. Obviously, such a wide safety margin of μ_α=200% of the design working load would in most cases not be a reasonable situation in standard practice.

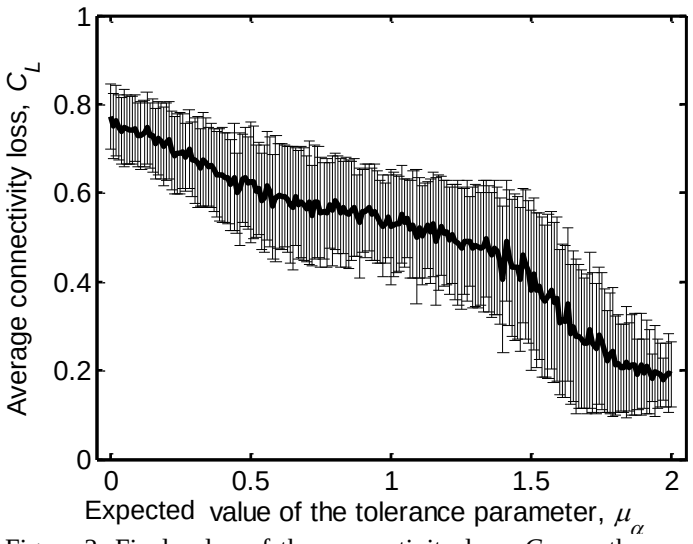

Figure 2. Final value of the connectivity loss, C_L, vs. the expected value of the tolerance parameter, μ_α, when the system response has stabilized. The cascades are triggered by the removal of the most congested node {88} in the power system. The error bars identify the standard error from 100 simulations for constant μ_α.

As expected, increasing the flow-carrying capacity of the network elements (i.e. increasing μ_α) reduces the extent of the cascades because flow redistribution can be handled at the local scale. The typical jumps to larger values of the connectivity loss, related to the so-called "islanding" effect (Zio and Sansavini 2010), are absorbed by the uncertainties on α.

The results shown in Figure 2 allow identifying an operating safety margin with respect to the transition between the cascade-safe region and the onset of disrupting cascades. For example, if one wants to reduce the average connectivity loss C_L below 60%, the power transmission network must be operated accounting for a safety margin $\mu_\alpha \geq 57\%$ beyond the design working load; the cascading failures occurring beyond this safety margin would result in connectivity losses lower than the selected value. Yet, such a wide safety margin might not be always available in real power transmission systems and component replacements might be required to comply with the prescribed safety margins.

Information concerning the benefits from possible system improvements can also be inferred. For example, the average connectivity loss is more sensitive to variations in the ranges $\mu_\alpha \in [0\%, 45\%]$ and $\mu_\alpha \in [140\%, 180\%]$. Hence, an increase in the tolerance within these ranges is more effective in improving the system vulnerability towards cascading failures.

We also analyzed the effects of the disconnection of the most congested node {88} in the power transmission CI on the communication and railway networks. Figure 3 shows the loss of service in these networks in terms of the relative decrease of the average global efficiency with respect to the unperturbed systems, ΔE_{glob}, versus μ_α. Due to the strong physical interdependencies between the power transmission system and the other two CIs, the loss of service trend is closely related to the connectivity loss, C_L, as it can be seen comparing Figure 2 and Figure 3. Due to the higher degree of redundancy in the communication network, the loss of service for this infrastructure is smaller than it is for the railway system. The curve in Figure 3 provides vulnerability information as the one in Figure 2. For example, if we aim at protecting the railway system by requiring a maximum loss of service, e.g. $\Delta E_{glob} \leq 0.5$, the interdependent power transmission network must be operated at $\mu_\alpha \geq 66\%$.

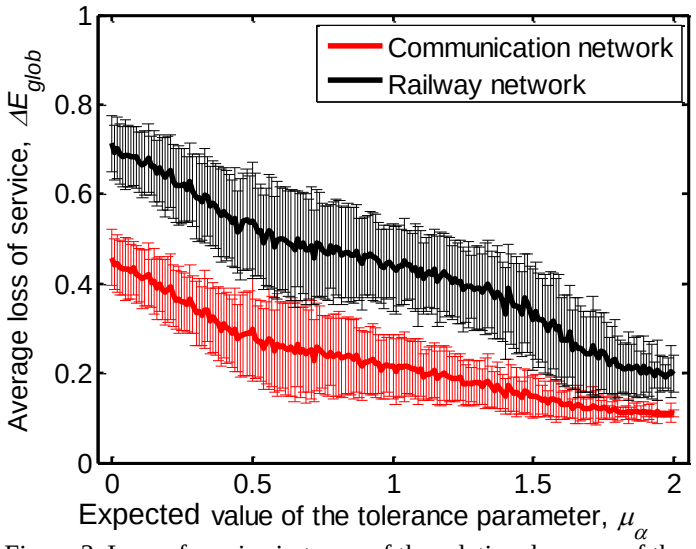

Figure 3. Loss of service in terms of the relative decrease of the average global efficiency with respect to the unperturbed systems vs. the expected value of the tolerance parameter, μ_α. The cascades are triggered by the removal of the most congested node {88} in the power transmission system. The error bars identify the standard error from 100 simulations for constant μ_α.

With respect to the malicious targeted attack of single nodes, the components of the system can be ranked in view of the damage caused by the cascade of failures triggered by their individual removal. To this aim, in Figure 4 the histogram of the average connectivity loss, C_L, caused by the removal of each node in the power transmission system is presented for μ_α = 30% which is a reasonable assumption in standard practice. Surprisingly, the most congested node {88} is not among the most critical. Nodes {14, 79, 76, 71 and 12} are ranked as the most critical ones, being bottlenecks for many generator-distributor shortest paths due to their position in the network. Hence, an attacker aiming at disrupting the most 'active' node would not actually produce the maximum 'desirable' damage.

The ranking of the most critical components is dependent on the expected value of the tolerance parameter, μ_α, characteristic of the system; thus, it must be reevaluated in case the system undergoes modifications affecting its operating margins.

The analysis performed is limited to the removal of individual nodes, as removing groups of nodes constitutes a combinatorial problem which lies beyond the scope of the current work.

In Figure 5, the removal of each node in the power transmission system is associated with its consequences on the interdependent CIs. Similarities with Figure 4 appear, for the reasons explained above.

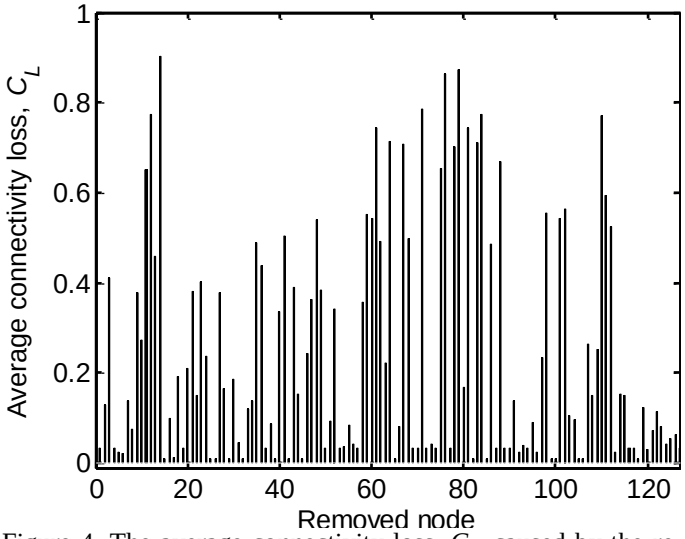

Figure 4. The average connectivity loss, C_L, caused by the removal of each node (abscissa) in the power transmission system. The expected value of the tolerance parameter is μ_α = 30%.

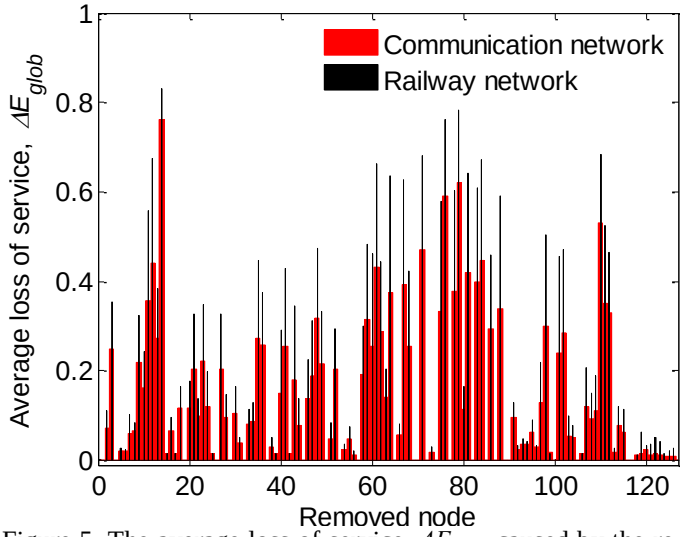

Figure 5. The average loss of service, ΔE_{glob}, caused by the removal of each node (abscissa) in the power transmission system. The expected value of the tolerance parameter is μ_α = 30%.

We performed an additional analysis focused on the intentional removal of the most connected node {64} of the communication system. The results are reported in Figures 6 and 7 for values of the interdependency strengths $\mu_{cr} = \mu_{cp} = 0.5$. Comparing Figures 6 and 7 with Figures 2 and 3, it appears that cyber dependencies are on the average less critical than physical dependencies with respect to the failure propagation, due to their assumed probabilistic nature. Yet, an attack on the communication network results in highly-variable consequences as it can be seen from the wide error bars in Figure 6 and 7. This renders more difficult any decision-making on CI protection.

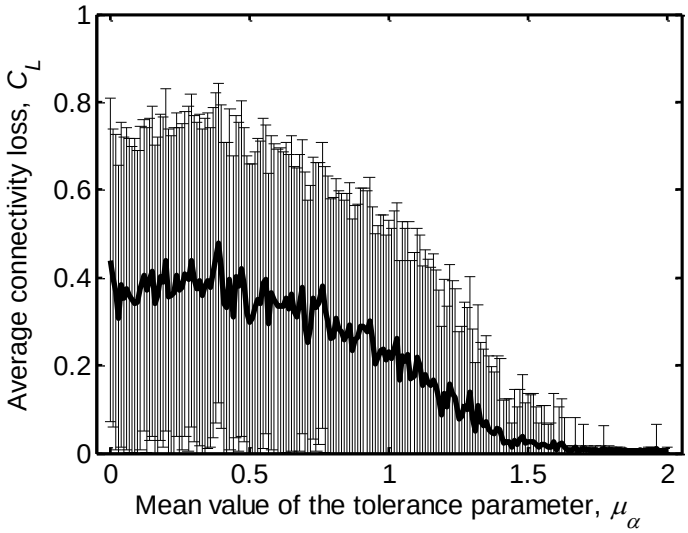

Figure 6. Final value of the connectivity loss, C_L, vs. the expected value of the tolerance parameter, μ_α. The results are averaged over 100 cascades triggered by the removal of the most connected node {64} in the communication system. $\mu_{cr} = \mu_{cp} = 0.5$.

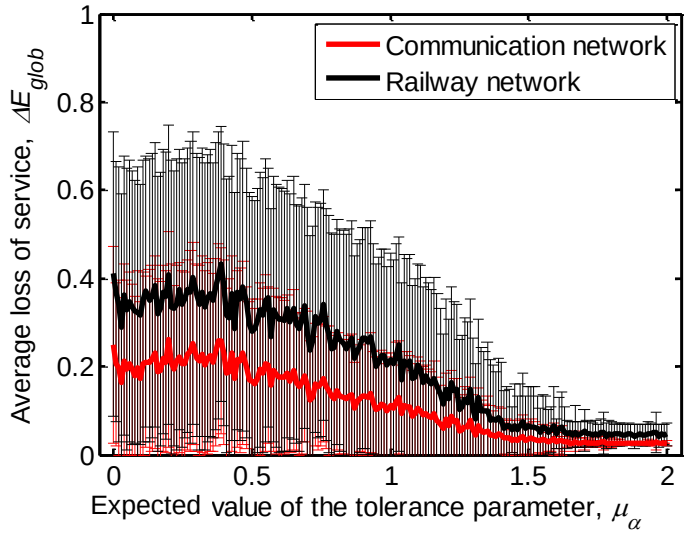

Figure 7. Loss of service, ΔE_{glob}, vs. the expected value of the tolerance parameter, μ_α. The results are averaged over 100 cascades triggered by the removal of the most connected node {64} in the communication system. $\mu_{cr} = \mu_{cp} = 0.5$.

5.1 *Sensitivity analysis with respect to μ_{cp} and μ_{cr}*

To look at the effects of the interdependency strengths on the failure propagation, we carried out a sensitivity study with respect to p_{cp} for two different μ_α values. Its results are reported in Figures 8 and 9, with $\mu_{cr} = 0.5$. A linear decrease in the effects of the cascading failure C_L and ΔE_{glob}, is shown when the interdependency strength, μ_{cp}, is reduced. The curves in Figures 8 and 9 convey information concerning the vulnerability of CIs with respect to the interdependency strength. As an example, if a maximum service loss is prescribed for the railway system, e.g. $\Delta E_{glob} \leq 40\%$, the interdependencies be-

tween the communication system and the power system must be operated so that $\mu_{cp} \leq 54\%$.

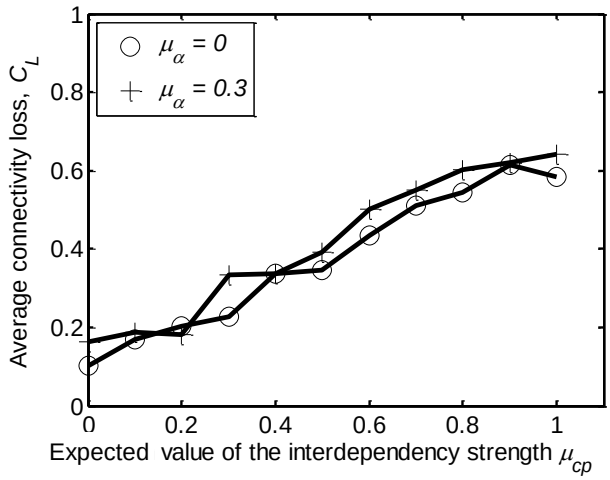

Figure 8. Average connectivity loss, C_L, vs. the interdependency strength, μ_{cp}. The results are averaged over 100 cascades triggered by the removal of the most connected node {64} in the communication system. $\mu_{cr} = 0.5$.

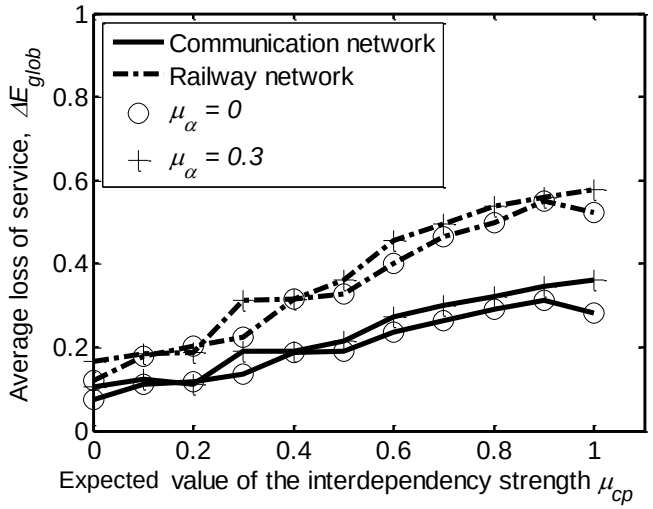

Figure 9. Average loss of service, ΔE_{glob}, vs. the interdependency strength, μ_{cp}. The results are averaged over 100 cascades triggered by the removal of the most connected node {64} in the communication system. $\mu_{cr} = 0.5$.

The interdependent CIs are not sensitive to variations of μ_{cr}, which do not influence the cascade triggering in the power system.

Finally, the removal of each node in the communication system is associated with its consequences on the interdependent CIs (Figures 10 and 11). The most connected node {64} in the communication system is the most critical with respect to failure propagation in the power system and in the railway network. Other critical nodes are {81, 78, 79, 61, 14, 110}. Nodes {14, 79, 110, 76, 81, 78, 61 and 64} are ranked as most critical for the communication infrastructure. Compared to the removal of the power stations, the relative ranking of some node originally present has changed and other nodes (i.e., node {12}) are not among the most critical. It turns out that the nodes {81, 78, 79, 61, 12, 14 and 64} linking the northern and the Tyrrhenian sections of the networks are the most critical. Moreover, node {110} that links the Adriatic and the Tyrrhenian sections of the networks is also ranked as critical.

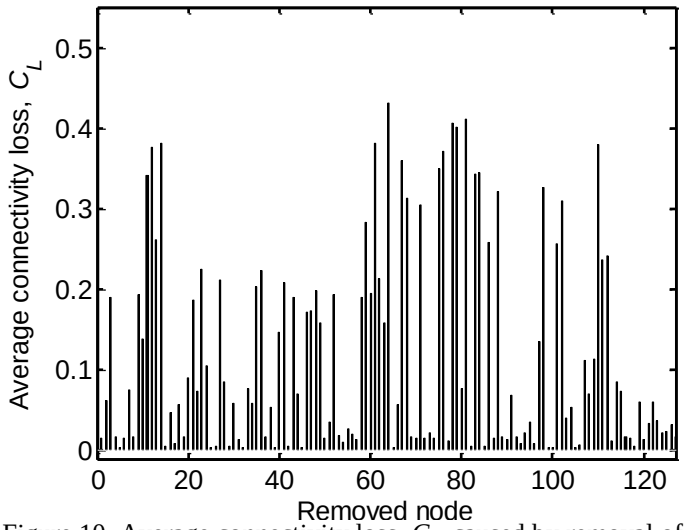

Figure 10. Average connectivity loss, C_L, caused by removal of each node (abscissa) in the communication system (100 simulations for each node). $\mu_\alpha = 30\%$, $\mu_{cr} = \mu_{cp} = 0.5$.

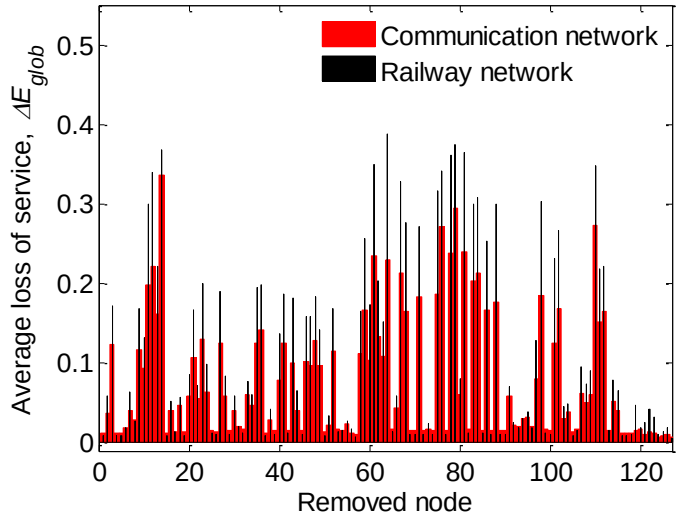

Figure 11. Average loss of service, ΔE_{glob}, caused by removal of each node (abscissa) in the communication system (100 simulations for each node). $\mu_\alpha = 30\%$, $\mu_{cr} = \mu_{cp} = 0.5$.

6 CONCLUSIONS

To improve the modeling of cascading failures propagation based on network theory, we have introduced the physical characterization of the components and of the interdependencies among CIs. The model has been applied to assess the cascade propagation process triggered by a defined node-removal scenario. Three interdependent CIs have been considered, namely the power transmission, the communication and the railway networks. We have accounted for uncertainties in the model parameters by a classic probabilistic framework of representation.

The knowledge gained from the type of analysis performed can help setting the value of the operating safety margin, μ_α, so as to limit the consequences of cascading failures, e.g. measured by C_L or ΔE_{glob}.

Ranking of the nodes according to the disruptions triggered by their individual removal has shown that nodes which could be thought of as most critical because of their high congestion or connectivity are not always associated with the largest consequences following their removal. This points to the fact that the physical characterization of the components and interdependencies and the introduction of the uncertainties add a further level of complexity to the cascade propagation, so that the system bottlenecks cannot be identified simply by the static topological analysis alone.

The proposed modeling framework allows also to look at the extent to which the interdependency parameters affect the cascade propagation, for different operating safety margins, μ_α. For example, given an operating safety margin value, the systems can be designed and operated, tweaking the interdependency strength, μ_{cr}, so as to limit the maximum average connectivity loss, C_L or service loss, ΔE_{glob}.

Future developments of this work will be the modeling of active safety systems for preventing and mitigating cascading failures propagations and the analysis of interdependent CIs having their own individual cascade dynamics.

ACKNOWLEDGMENTS

This work has been partially funded by the Foundation pour une Culture de Securite Industrielle of Toulouse, France, under the research contract AO2006-01.

REFERENCES

Albert et al. 2004. Structural vulnerability of the North American power grid, *Physical Review E* 69, 025103.

Batagelj, V. 1994. Semirings for social networks analysis. *Journal of Mathematical Sociology* 19(1): 53-68.

Dobson, I., B. A. Carreras, et al. 2007. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 17(2): 026103.

Duenas-Osorio & Vemuru 2009. Cascading failures in complex infrastructures systems. *Structural safety* 31: 157-167.

Freeman, L. C. 1978. Centrality in social networks conceptual clarification. *Social Networks* 1(3): 215-239.

Freeman, L. C., S. P. Borgatti, et al. 1991. Centrality in valued graphs: A measure of betweenness based on network flow. *Social Networks* 13(2): 141-154.

Johansson and Jonsson 2009. A model for vulnerability analysis of interdependent infrastructure networks. *Safety, Reliability and Risk Analysis: Theory, Methods and Applications* – Martorell et al. (eds), Proceedings of ESREL 2008 and 17th SRA Europe Annual Conference, 22-25 September 2008, Valencia, Spain, Taylor & Francis Group, London, 2009.

Kröger and Zio 2011. *Vulnerable Systems*. Springer London Ltd, London, 2011.

Latora and Marchiori 2005. Vulnerability and protection of infrastructure networks. *Physical Review E* 71, 015103.

Little, R. G. 2002. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. *Journal of Urban Technology* 9(1): 109 - 123.

Motter, A. E. and Y.-C. Lai 2002. Cascade-based attacks on complex networks. *Physical Review E* 66(6): 065102.

Newman, M. E. J. and M. Girvan 2004. Finding and evaluating community structure in networks. *Physical Review E* 69(2): 026113.

Newman D. E. et al. 2005. Risk Assessment in Complex Interacting Infrastructure Systems, *Proceedings of the Thirty-Eight Annual Hawaii International Conference on System Sciences*, January 3-6, 2005, Computer Society Press.

Nieminen, J. 1974. On the centrality in a graph. *Scandinavian Journal of Psychology* 15(1): 332-336.

Rinaldi, S.M. et al. 2001. Identifying, understanding and analyzing critical infrastructures interdependencies, *IEEE Control System Magazine*, 21(6), 11-25.

Rinaldi, S.M. 2004. Modeling and simulating critical infrastructures and their interdependencies, *Proceedings of the Thirty-Seventh Annual Hawaii International Conference on System Sciences*, January 5-8, 2004, Computer Society Press.

Rosato, V., Bologna, et al. 2007. Topological properties of high-voltage electrical transmission networks. *Electric Power Systems Research* 77: 99-105.

Sabidussi, G. 1966. The centrality index of graphs. *Psychometrika* 31(4): 581-603.

TERNA. 2002. Dati statistici sull'energia elettrica in Italia. Techical Report. *Terna S.p.A. - Rete Elettrica Nazionale*. (in Italian) http://www.terna.it/LinkClick.aspx?fileticket=PUvAU57MlBY%3d&tabid=418&mid=2501

Zimmerman, R. 2001. Social Implications of Infrastructure Network Interactions, *Journal of Urban Technology*, 8(3): 97-119.

Zio, E. and Sansavini G. 2009. Modeling failure cascade in network systems due to distributed random disturbances. *Proceedings ESREL 2008. Martorell et al. (eds): Safety, Reliability and Risk Analysis: Theory, Methods and Applications.* CRC Press, Taylor & Francis Group, London.

Zio, E. and Sansavini G. 2010. Modeling failure cascades in critical infrastructures with physically-characterized components and interdependencies. *Proceedings ESREL 2010. Ale et al. (eds): Reliability, Risk and Safety.* CRC Press, Taylor & Francis Group, London.

Zio, E. and Sansavini, G. 2011. Modeling interdependent network systems for identifying cascade-safe operating margins, *IEEE Transactions on Reliability*, 60(1):94-101.