Simulation-Based Characterisation of Critical Infrastructure System Resilience

Boris Petrenj* and Paolo Trucco*

*Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy
Piazza Leonardo da Vinci 32, 20133 Milano
E-mails: boris.petrenj@polimi.it, paolo.trucco@polimi.it

Abstract: This paper presents a simulation-based approach to the resilience analysis of Critical Infrastructures systems, making possible the characterisation of the structural resilience features of the system and estimation of the benefits that are derived from improved resilience practices, i.e., preparedness or responsiveness, due to enhanced information-sharing processes among the actors. Resilience characterisation is composed of assessment of the node *vitality* (i.e., the Missed Service Demand (MSD) generated at the system level) and *agility* (i.e., the sensitivity of system performance to an improved response time in the node). Scenario analysis is subsequently used to simulate different strategies intended to minimise the impacts of large events. The transportation system in the metropolitan area of Milan is used for this purpose; more specifically, a reduction of disruption response times in agile nodes was simulated according to a real snowfall scenario.

Key words: Critical Infrastructure, Resilience Analysis, Simulation, Case Study

Biographical notes:

Boris Petrenj is currently a PhD candidate at Politecnico di Milano in the Department of Management, Economics and Industrial Engineering and is a member of the Risk Management and System Sustainability research group. His current research is in the field of Critical Infrastructure Protection and Resilience (CIP/R) with a focus on information-sharing and collaboration processes, public-private partnerships, risk/emergency management, infrastructure interdependencies and vulnerabilities. He received his MSc in Electrical and Computer Engineering with a specialisation in Electronics from the Faculty of Technical Sciences at University of Novi Sad, Serbia.

Paolo Trucco is Associate Professor of Industrial Operations and Risk Management. His primary research interests are risk analysis and resilience of complex socio-technical systems, human reliability and organisational risks analysis. He is a member of the Italian Association of Experts on Critical Infrastructures and contributes to OSN (National Observatory for Homeland Security and Defence) and is the Scientific Coordinator of PReSIC, the Public-Private Partnership of the Lombardy Region on CI Protection and Resilience. He received his MSc in Industrial Engineering (Politecnico di Milano) and PhD in Quality Engineering (University of Florence).

Acknowledgements:

The work presented in this paper was developed within MATRICS (www.matrics.it), a research project co-funded by the Italian Ministry of Research and Education (MIUR) and the Lombardy Region Government (Italy). This financial support is gratefully acknowledged.

1 Introduction

The increasing importance of Critical Infrastructure (CI) systems for societal and economic development and citizen well-being has attracted recent attention for reasons of protection and resilience. The resilience of CI systems has become one of the key elements required to assure the continuity of operations as well as the availability of vital functions in modern societies (Cohen, 2010; George, 2008).

Due to the intensive exchange of goods, services and information between infrastructures and their physical collocation and linkage via financial markets or human behaviour, CIs have become a highly interdependent system of systems that is prone to cascading disruptions. These interdependencies create opportunities as well as vulnerabilities by rendering the impacts longer in duration and more widespread (Zimmerman, 2004). Crisis scenarios involving critical infrastructures require diverse actors and intervention by multiple organisations. Because no single organisation contains all of the necessary resources or possesses all of the relevant information and expertise necessary to cope with complex inbound and outbound interdependencies under different accident scenarios (Petrenj et. al., 2012), organisations must work together before, during and after disasters to effectively respond and recover from an event.

Protection measures (i.e., physical protection of facilities, surveillance, cyber-protection of information and control (SCADA) systems, screening of people entering the site, etc.) are important but not sufficient to ensure full protection. Highly reliable protection efforts are also notably expensive. The variety of possible hazards ranging from natural disasters, terrorist attacks, and operator errors to elementary technical failures makes it impossible to completely avoid operational risk. Even under the hypothesis of knowledge of all threats, the complexity of interconnected systems makes it is impossible to know all of the possible behaviours of the system in advance and ensure protection from all sources of disruption.

Coping with inevitable events requires expanded efforts from the pre-event to during-event (and post-event) phases of emergency management. This shift of focus from prevention only to the inclusion of response and recovery activities offers more comprehensive risk management and an all-hazard approach (De Bruijne & Van Eeten, 2007; Pursiainen, 2009). This approach also can be described as the addition of resilience to protection. Although

vulnerability addresses only system protection, resilience also focuses on systems recovery following an adverse event (Haimes, 2009b).

The definition of resilience varies across different fields but generally implies the ability to recover from a shock, insult, or disturbance and the quality or state of flexibility (Bouchon, 2006). The disaster management domain considers it as *"the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organising itself to increase this capacity for learning from past disasters for better future protection* and *to improve risk reduction measures"* (UN, 2005; p. 9). The resilience definition used by the US Department of Homeland Security (DHS) is "*the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions*" (DHS, 2009; p. 111). More specifically, **infrastructure resilience** is "*the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event"* (NIAC, 2009; p. 8). Enhancement of system resilience at different levels (structure, network, community, etc.) could lead to massive savings via risk reduction and expeditious recovery (Ayyub, 2013).

The resilience of a community/region is a function of the resilience of its subsystems, including but not necessarily limited to its critical infrastructures, economy, civil society, governance (including emergency services), and supply chains/dependencies (ANL, 2012). **Technical resilience** aims to render an infrastructure capable of withstanding an impact and maintaining an acceptable level of functionality (e.g., through added redundancy/backups, geographical isolation, etc.). Of course, the concept of resilience is much broader than this description. The '*full spectrum resilience*' (Boone, 2012) approach includes **organisational resilience** (covering strategic, operational, and tactical levels of intra- and inter-organisational coordination and collaboration addressed across a range of potential impacts) and **societal resilience** (e.g., preparation of the authorities, population and economic system via emergency plans, business continuity plans, evacuation plans, alternative resources, etc.). Economic, environmental and ecological aspects are also often considered as relevant components of resilience.

In a time in which infrastructures are tightly connected, it is important to consider the contribution of information-sharing and collaboration as one of the main pillars and perhaps the most important factor within the mission of protection and resilience of CIs. Indeed, among researchers, infrastructure operators and governmental agencies, *information-sharing and collaboration* have been recognised as the key element for improving the effectiveness and efficiency of crisis response (Bharosa, 2009; DHS, 2013; Dilmaghani & Rao, 2008; Eckert, 2005; Federowicz et al., 2007; Gryszkiewicz & Chen, 2010; NIAC, 2012; Petrenj et al., 2012; Schooley & Horan, 2007). At the first level of collaborative activities between organisations, information-sharing offers better preparedness for events, anticipation of consequences and faster response to an incident. Cross-organisational collaboration and flow of information during emergencies are critical components of emergency response because the majority of crisis management activities rely on the efficient circulation of information among actors.

The aim of the paper is to develop a simulation-based methodology for characterisation of CI system resilience. The CI system and its nodes are first characterised according to their agility and vitality, which enables a focus on the nodes at which the applied efforts will have the most significant effect. The methodology is based on different simulation models as well as different KPIs (performance metrics).

Although the methodology is suitable for assessing the benefits of different resilience and protection efforts (e.g., structural, technical, etc.) on system performance, the primary aim of this work is to enable the assessment of organisational resilience capabilities, i.e., improved information-sharing during the emergency and intra- and inter-organisational coordination and collaboration (Taylor-Powell et al., 1998). Due to the use of a functional modelling approach, the proposed methodology does not depend on the technical specifications of specific resilience solutions (e.g., tools, standards, protocols, interoperability, technological and architectural solutions for information-sharing, etc).

The paper is organised as follows. Section 2 describes the state-of-the art approaches for resilience evaluation and the metrics used in this study. Section 3 explains the simulation approach and the adopted model in detail. Section 4 depicts the methodology implemented to carry out the analysis, describes the test case (a real snowfall event in a large European region) and illustrates the modelling of threat, impact and recovery processes. The main results of the resilience analysis and the scenario simulations are summarised and discussed in Section 5, and conclusions are presented in the final section.

2 Key attributes of system resilience: perspectives in the literature and the study approach

Resilience is a broad and multifaceted concept, and several researchers are currently working to capture its core elements and properties to arrive at a possible quantification and assessment approach (ANL, 2010; Fisher & Norman, 2010; Francis & Bekera, 2014; Hémond & Robert, 2012; Ouyang & Dueñas-Osorio, 2012; Rosenkrantz et al., 2009; Solano, 2010; Tierney & Bruneau, 2007). However, no common definition of resilience or a standardised method of measurement currently exists. Despite the various definitions, general agreement has been reached by the authors on three key elements of resilience, i.e., the ***absorptive***, ***adaptive*** and ***restorative*** capacities (Francis & Bekera, 2014; SNL, 2013). Improved protection implies mitigation of threats via improved resiliency to reduce risk primarily by reducing the vulnerability to and potential consequences of an event (Moteff, 2012).

Despite the also nonexistent complete consensus on the major factors that should be taken into consideration in modelling risk, the agreement is that at minimum, we need to understand the factors connected to evaluation of the likelihood of the threats (or hazards), the vulnerability of the system to these threats and the severity of possible consequences (Aven, 2011; Haimes, 2009a). In the current study, we adopt a subset of the most typical risk factors as a metric for ex-ante assessment of the expected effect of a certain level of resilience, specifically due to improved organisational resilience capabilities. In agreement with the major part studies on CI resilience reported in the

literature, we adopt an all-hazard approach to postulate the occurrence of a generic disruption event. As a consequence, the threat likelihood becomes irrelevant, and only system vulnerability and severity of consequences are taken into consideration.

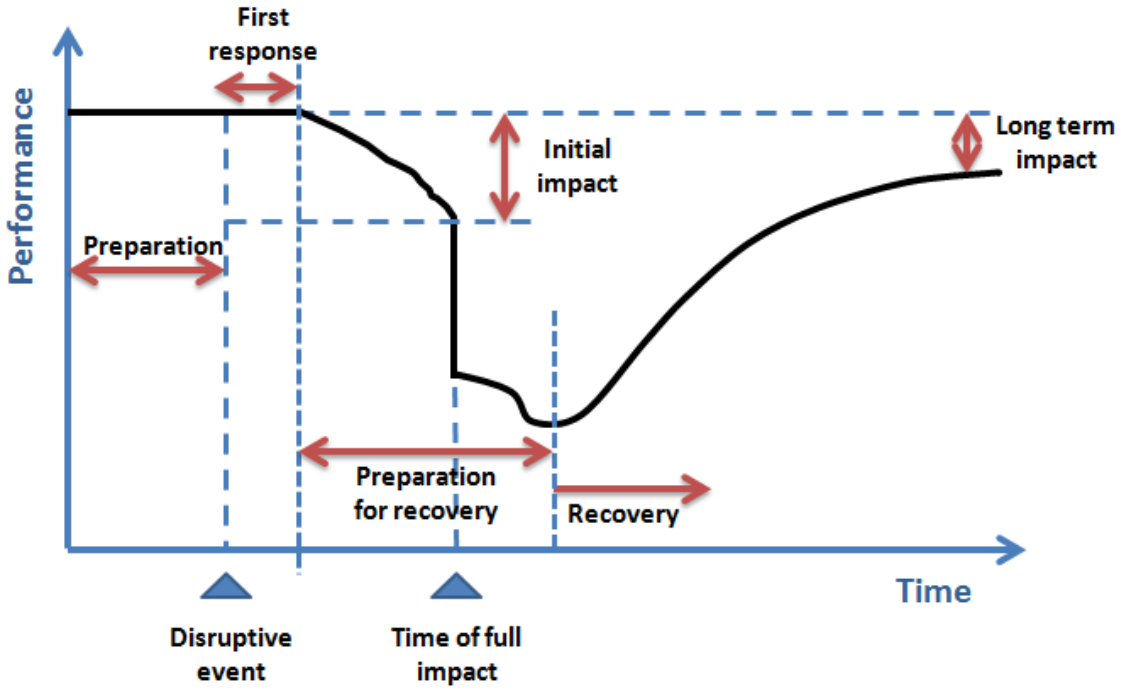

Figure 1: Generalised disruption profile and stages (adapted from Ayyub, 2013; Bruneau et al., 2003; Francis & Bekera, 2014; Kimmance, 2010; Ouyang & Dueñas-Osorio, 2012; Sheffi & Rice, 2005).

For the severity factor, one of the most common methods used to represent and measure the resilience of a CI system after an external shock (Ayyub, 2013; Kimmance, 2010) is its *degradation in quality* (Bruneau et al., 2003; Solano, 2010) or *loss of performance* (Francis & Bekera, 2014) in general. This type of approach has been used in numerous studies and includes the dynamics of the system after a perturbation (e.g., disruption shape and duration, response time/preparation for recovery, recovery shape and duration). The general disruption profile and its stages are presented in Figure 1.

Within the Enhanced Critical Infrastructure Protection (ECIP) Program, in 2010, the Argonne National Laboratory developed a measure of the resilience of critical infrastructures in collaboration with the DHS (ANL, 2010). The Resilience Index (RI) was based on the approach recommended by the National Infrastructure Advisory Council (NIAC), which argued for analysis of the resilience of an organisation or system by considering three major components (NIAC, 2010):

- **Robustness** is the ability to '*maintain critical operations and functions in the face of crisis*' (NIAC, 2010). This aspect is directly related to the ability of the system to absorb the impacts of a hazard and the ability of the asset to continue functioning in a degraded state (ANL, 2010), thus reflecting the *absorptive capacity* element of resilience.

- **Resourcefulness** is the ability to '*skilfully prepare for, respond to, and manage a crisis or disruption as it unfolds'* (NIAC, 2010). Resourcefulness includes elements of pre-event measures (e.g., training, planning) and post-event measures (application of training and planning, information-sharing, usage of resources) (ANL, 2010) and also represents the *adaptive capacity* element of resilience. Resourcefulness can be viewed as a complement to robustness that allows for a smooth and expedited transition from the response phase to the recovery phase (ANL, 2010), i.e., reducing the '*preparation for recovery*' phase (Figure 1).
- **Rapid recovery** is the ability to '*return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption'* (NIAC, 2010). Rapid recovery defines an asset's transition from a degraded functionality back to the full (or acceptable) operating level (ANL, 2010) and corresponds to the *restorative capacity* element of resilience.

Certain authors also consider *redundancy* as an additional property of resilience (Attoh-Okine et al., 2009; Bruneau et al., 2003) and define it as '*the extent to which elements, systems, or other measures of analysis exist that are substitutable*, i.e., *capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality*' (Bruneau et al., 2003). Redundancy is related to systems design and represents the availability of backup installations or spare capacity (UK CO, 2011). From our point of view, redundancy is a method for reducing vulnerability and is a component of robustness (together with reliability of infrastructures/components or prevention activities). However, on a higher level, *adaptability* (Figure 2) represents the means of absorbing new lessons drawn from an event (NIAC, 2010) and involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve all capabilities (*robustness*, *resourcefulness*, and *recovery*) before the next crisis (NIAC, 2010).

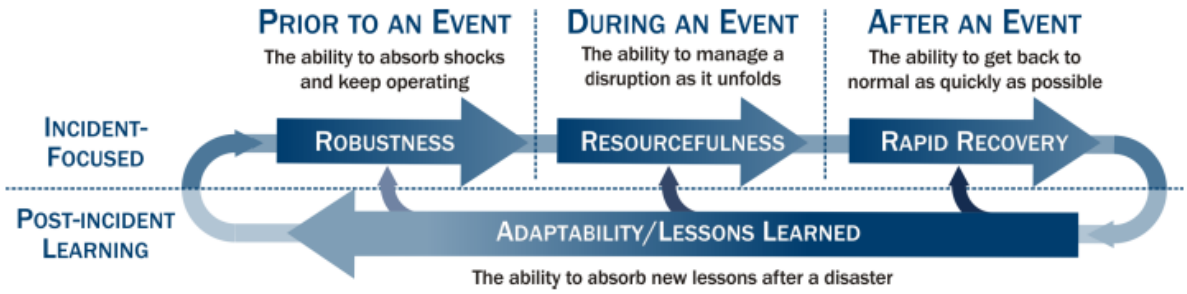

Figure 2: Elements and sequence of the resilience construct (NIAC, 2010)

The consequence-based approach to assessing system criticality is considered by several authors as adequate for evaluating and measuring the state of resilience for a CI operating in a context of interdependencies (Egan, 2007; Hémond & Robert, 2012; Robert et al., 2007). Criticality is related to the importance of the facility to a system and its environment if considering a generic disruption event and the impact of the loss of that facility (Fisher & Norman, 2010).

In our study, we measure the contribution of organisational capabilities to resilience by simulating their ability to reduce the loss of performance at the system-of-systems level. In this respect, performance disruption can be

measured in different ways, e.g., degradation in quality, degradation in functionality, reduction of service delivery, economic loss, etc. We use the service delivery of each single infrastructure system as its performance metric (Trucco et al., 2012), i.e., measurement of the *total* ***Missed Service Demand (MSD)*** generated in a scenario. We are aware that the consequences of an adverse event are multidimensional and not measurable by a single unit metric (Haimes, 2009b), but because our focus is on service delivery only (not considering socio-economic or physical effects), *total MSD* represents a valid measure. We will show that this limitation does not affect the generality of the proposed methodology that in the future might be enriched with a wider set of consequence dimensions and metrics.

We also define a simplified disruption profile based on empirical data, as depicted in Figure 3, thus overlooking possible long-term impacts on system functionality (e.g., due to severe physical effects). The shape reflects behaviour of a node during a real event in which performance is measured between 0 (the node is completely blocked) and 1 (nominal state). The marked area in Figure 3 is a function of the loss of nominal performance level, i.e., service level in our case. The size of the area is thus inversely proportional to system resilience, i.e., the smaller the area, the greater the system resilience (Kimmance, 2010).

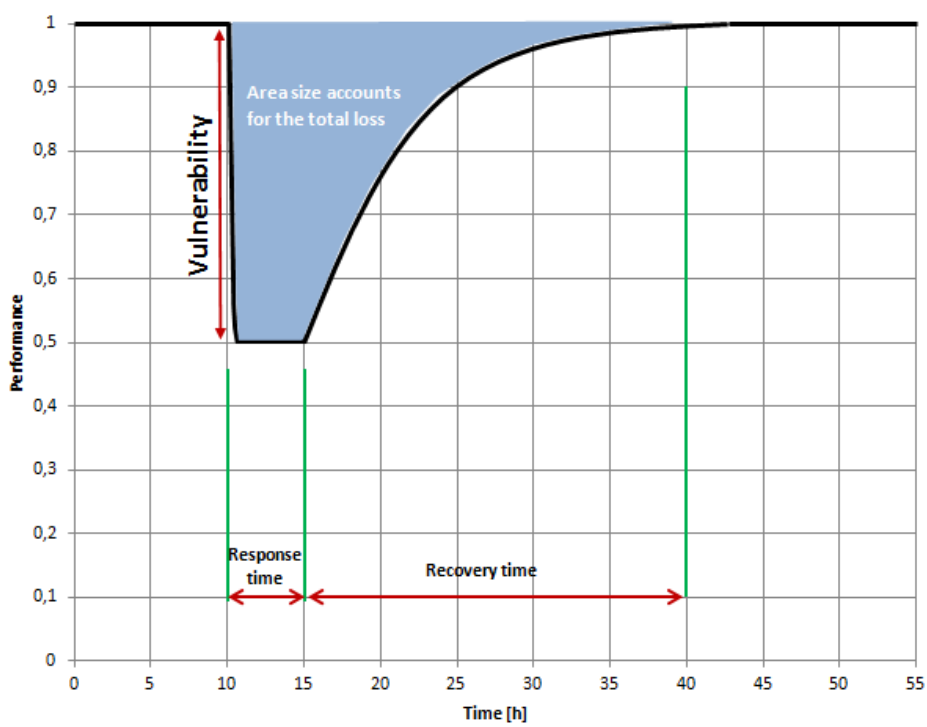

Figure 3: Sample of performance shape during a disruption and its main parameters.

The service level can be reduced either by a threat impact on a node or by interdependencies (Figure 4). **Functional integrity** quantifies the direct impact of threats on the node service capability, i.e., the reduction of its maximum service capacity over time (the direct effect). **Inoperability** quantifies how disturbances originating from the CI network via interdependencies (physical, cyber, geographical, logical; Rinaldi et al., 2001) reduce the

maximum service level of a node starting from its actual service capacity. As a consequence, global service disruption is due to the combined effects of a loss of functional integrity on certain nodes and propagation of inoperability between nodes. At the system level, we are not sufficiently able to distinguish these two contributions, due to complexity.

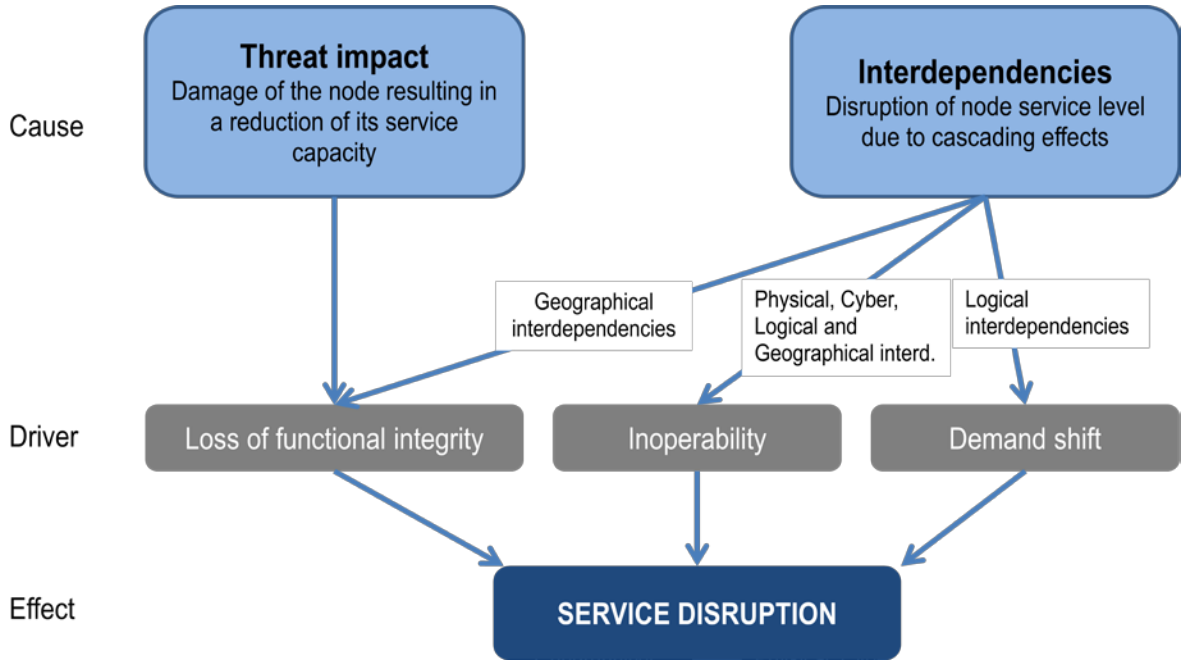

Figure 4: Causes of service disruption

Resilience can be enhanced (the area reduced) in several ways. The first approach might include enhancement of the node (or system) robustness (Figure 5a), which results in limited vulnerability and reduced initial impact of the threat. The robustness of a node can be increased not only by making it less vulnerable to external threats but also by reducing the number and intensity of interdependencies and thus reducing the propagation of inoperability.

The second option is to reduce the response time, i.e., the time required to set up and initiate the recovery process (Figure 5b). This improvement of resourcefulness can be achieved through better preparedness, i.e., enhanced anticipation and better situational awareness based on improved information sharing between the organisations involved in the incident response (ANL, 2010).

The third approach is to speed up the recovery process (Figure 5c), install a steeper recovery function and thus reduce the recovery time.

However, improved recovery and/or robustness require additional investments in the infrastructure itself or investments in equipment used during recovery. In the proposed application (Section 4.2), we focus our analysis on the assessment of benefits due to a reduced response time as the result of a more effective 'preparation for recovery' phase (Figure 1) due to enhanced information sharing and collaboration among operators.

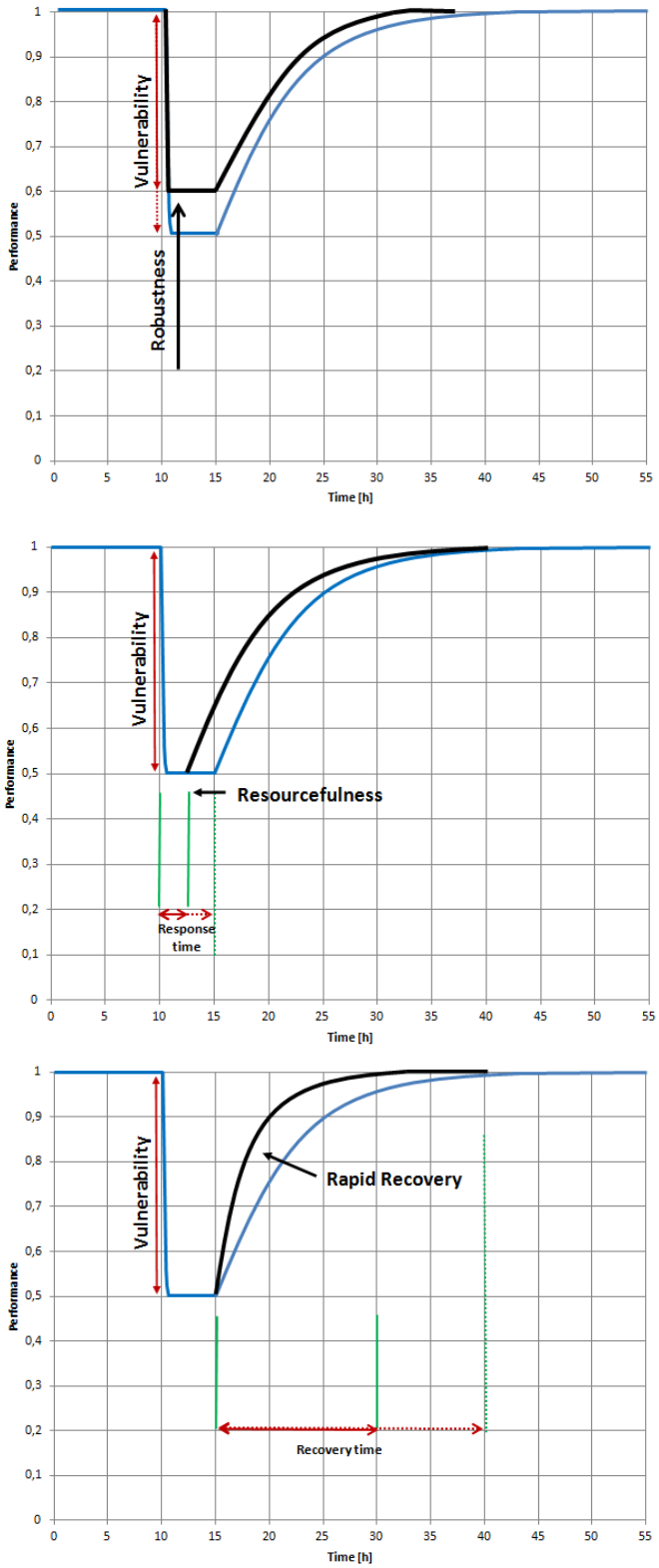

Figure 5: Different approaches for improving node resilience: a) reducing recovery time; b) improving robustness; c) reducing response time

3 Simulation-based resilience characterisation of CI systems

In characterising a CI system and the behaviour of its nodes, there are two types of possible scenario analysis, i.e., simple and complex, and each is suitable for examining specific features of the system.

A ***simple disruption scenario*** represents a disruption in a single node, whereas all of the other nodes retain full functionality. *Simple disruption scenario analysis* enables assessment of the effects of a single node disruption on the performance of the entire system, taking into account only the role of the different interdependencies present in the network. This approach enables characterisation of the nodes by means of their impact on the system as a whole.

A ***complex disruption scenario*** simulates the behaviour of the system after impact by several threats or a single threat that is able to affect more than one vulnerable node concurrently. By simulating a complex scenario, we are able to analyse the behaviour of the system and estimate the global and local effects of different resilience features and response strategies.

A simulation-based characterisation of a CI system can be obtained by combining adoption of simple and complex disruption scenario analyses to characterise system elements and to assess the benefits of improved capabilities and strategies relative to its resilience features within a consistent methodology. The phases and sub-steps of the proposed methodology are summarised in Figure 8.

In phase 1 (Figure 8), the CI system's nodes are analysed in terms of *vitality* and *agility*. Simple disruption scenarios are used to obtain the most essential or *'vital' nodes* (Luiijf et al., 2003) according to the level of MSD produced in the system by a complete disruption; the higher the level total MSD produced by a node disruption, the greater the node's vitality under the given circumstances. This approach also can be explained as node criticality because it estimates the consequences of node disruption (Fisher & Norman, 2010). In considering total system performance, we take into account both the direct (in the given node) and indirect (in other nodes) effects of node disruption.

Node agility indicates the sensitivity of the *total MSD* at the system level to improved node *resourcefulness* during an emergency. This measure can be estimated as the algebraic difference between the amount of MSD in the system with faster (-10%) and slower (+10%) responses during a specific period of the day and can be understood as a node's ability to anticipate the execution of those tasks deemed as crucial in preparation for the initial impact and commencement of recovery to normal conditions.

The first classification of nodes is carried out with respect to their average agility and vitality across the disruption hours (Figure 6).

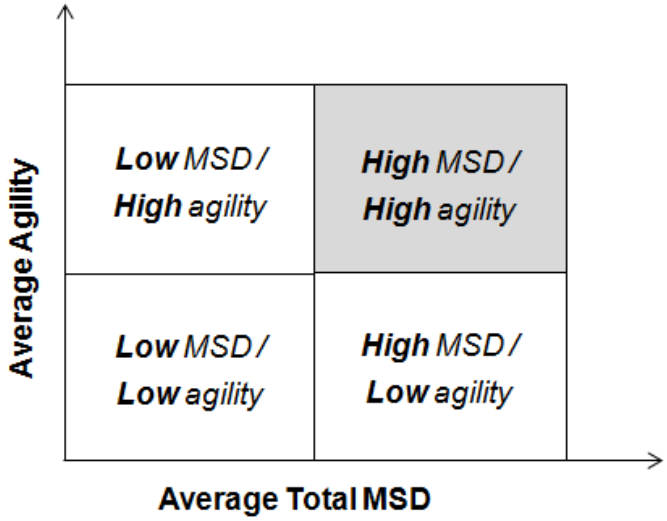

Figure 6: Classification of nodes in terms of vitality and agility

Each of the zones describes a specific relationship between the node behaviour and the corresponding effects at the system level and can be summarised as:

1. *Low MSD - Low Agility Zone*: This zone includes nodes whose disruption has a low impact on the system's performance and a reduced margin of improvement if a faster response is applied during an emergency.
2. *High MSD - Low Agility Zone*: The robustness of these nodes is important because the overall effects of a disruption are considerably high, and resourcefulness is not strongly related to the impact on the system.
3. *Low MSD - High Agility Zone*: Interdependencies are the main factor affecting the performance of the system because a reduction in response time has positive implications on the system, even though the total impact on the system is below the node average.
4. *High MSD - High Agility Zone*: High levels of MSD produced in the system by their disruption and a high variation of performance due to the response speed makes these nodes important in the system.

Characterising nodes by their agility and vitality enables us to distinguish nodes with the highest average values of agility and vitality and 'other nodes' that are not further considered (Figure 8). In the quest for nodes that would be the best targets for targeted response efforts, we characterise the selected group of nodes in greater detail in phase 2.

Due to the demand variation during the day, the MSD induced in the overall system by node disruption may also vary, and thus, node agility and vitality might differ according to disruption time. To account for this phenomenon, a second node classification process can be performed, this time using the variance of the nodes' agility and vitality across the daily hours instead of their average values. Therefore, it is possible to study how their total MSD and agility change over time in additional detail (Figure 7):

- High values of variance indicate unstable node behaviour over time, and thus, it is uncertain whether improvement in terms of response time reduction will result in benefits. These nodes are difficult to manage in emergencies;

- Nodes in the low-low zone have low MSD and agility variance, which makes them stable over time. This characterisation means that high agility will remain high (low variance), making it certain that an improvement in node survivability will benefit the system's resilience performance.

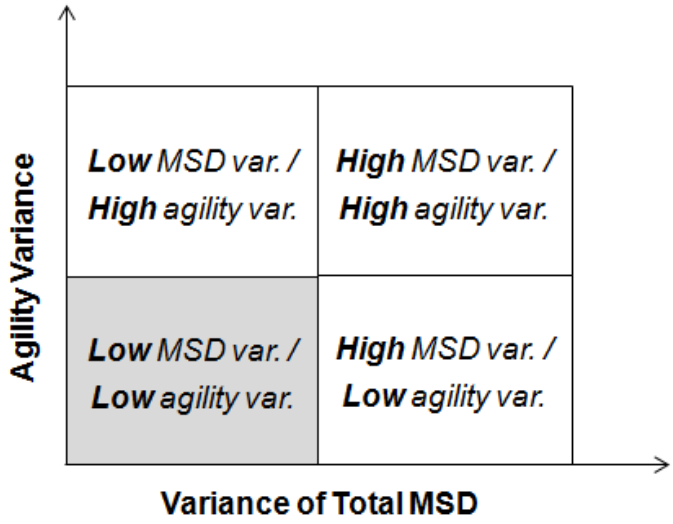

Figure 7: Further classification of high agility nodes in terms of MSD and agility variances

After identifying the most promising nodes for action, it is possible to move into a real case or plausible complex scenario to analyse the overall resilience of the CI system and compare different improvement options. The local and overall benefits in the system due to reduced response times in selected nodes can be assessed by considering three main response strategies:

a) Acting individually on one node at a time;
b) Acting simultaneously on a group of interdependent nodes (clusters);
c) Exploiting logical interdependencies (e.g., controlled migration of users from one heavily disrupted infrastructure to another) in addition to strategy b).

By simulating the proposed strategies, we investigate whether it is possible to benefit from exploiting the structural characteristics of an infrastructure system (targeted response) and/or exploiting logical interdependencies (controlled migration of a portion of users to other infrastructures offering the same service) in a complex scenario during an emergency response.

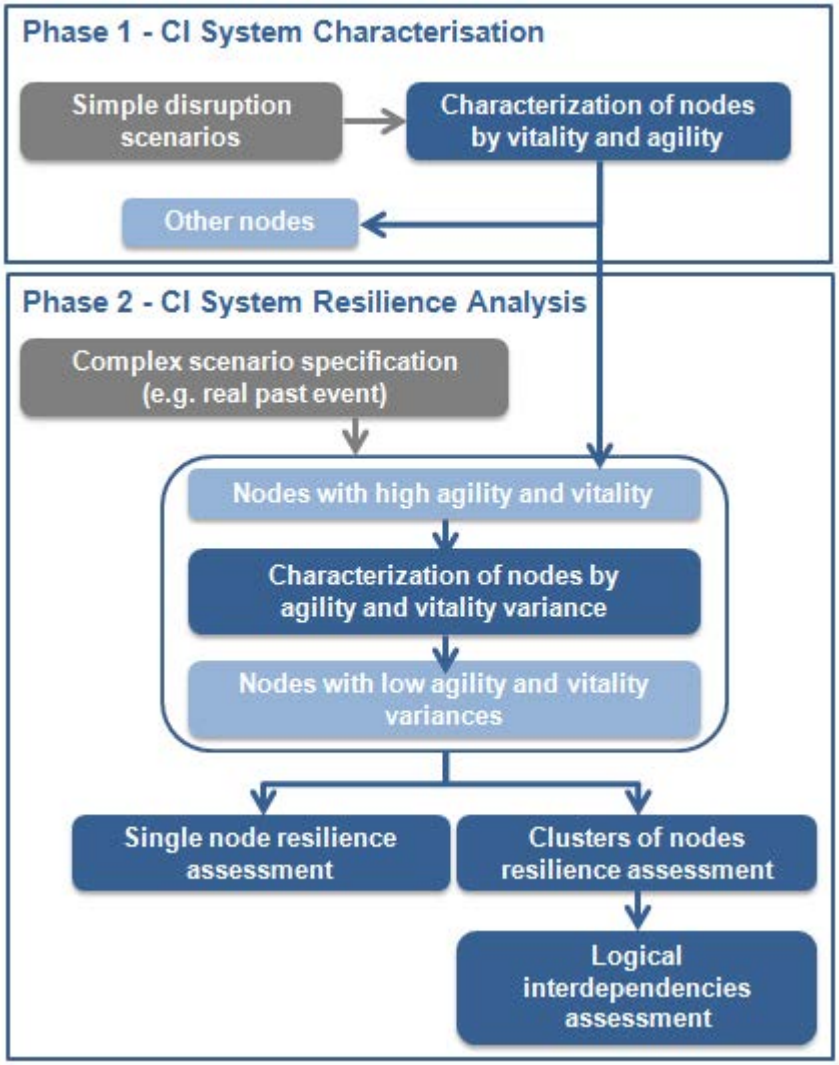

Figure 8: Flowchart of the steps of the analysis

4 Methodology implementation using the DMCI model

Considering the objectives of the study, a dynamic functional modelling approach was adopted according to the CI system description, which is the most adequate for use in this context (in contrast to physical and socio-economic levels of representation) (Trucco et al., 2012).

4.1 DMCI model features

Trucco et al., (2012) developed a newly integrated formalism for Dynamic Functional Modelling of vulnerability and interoperability of CIs (DMCI). The proposed modelling formalism is characterised by certain distinctive features:

- Specification of vulnerable nodes defined as *"a large functional part of a CI that assures the satisfaction of a considerable part of service demand at regional or local level (e.g., part of a pipeline network, a railway station, a portion of a highway, an underground line) and that does not need further disaggregation for the sake of the analysis."* A vulnerable node must be homogeneous (i.e., uniform in structure and function with respect to service demand), service self-providing (i.e., a system able to supply a value-added service through its own means), and vulnerable (i.e., susceptible to threats that could decrease its functional integrity) (Trucco et al., 2012). Vulnerable nodes are mutually connected to create intra- and inter-infrastructure interdependencies;
- Specification of threat nodes characterised by time-variant intensity and specific impact potential on different vulnerable nodes;
- Quantification of both functional and logic interdependencies due to the use of both service demand and service capacity for each node of the considered CIs;
- Time-dependent specification of the main parameters of the model, i.e., node functional integrity, interoperability, service demand and loss, etc.;
- Propagation of both inoperability and demand variations throughout the nodes of the same infrastructure and between interdependent CIs.

Figure 9 outlines the entities of the proposed formalism and their relationships. The model was first implemented in software code using Matlab® and is able to assess the propagation of impacts due to a wide set of threats. Therefore, the MSD can be propagated within the same infrastructure or to other CIs, thus exploiting the model's ability to represent functional, cybernetic, geographical, and physical as well as logical interdependencies (Trucco et al., 2012). Logical interdependencies are particularly relevant in both the transportation and electricity infrastructure systems. In the former system, logical interdependencies are primarily established by a shift of demand between two infrastructures that can provide the same or fully/partially replaceable mobility service (e.g., two different transportation means that connect the same towns); in the latter, logical interdependencies are established by the way in which different power generation sources or line sections are used to maintain the overall grid balance.

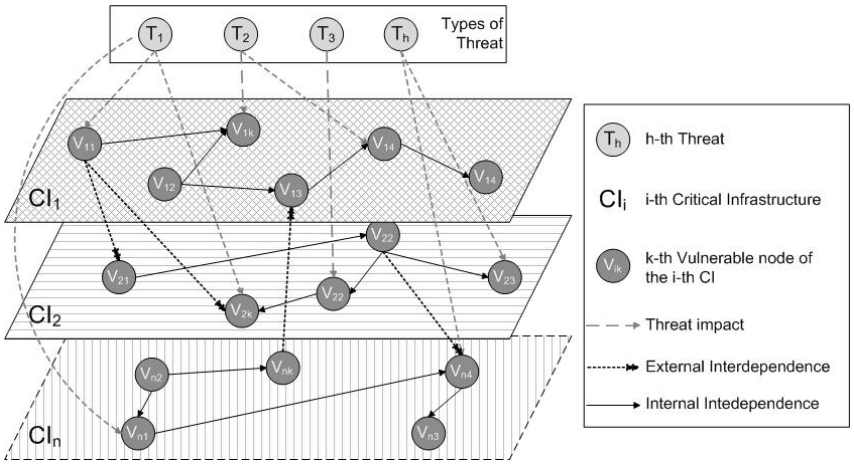

Figure 9: Entities and their relationships.

To demonstrate the applicability of the model, the authors presented a pilot study carried out in the metropolitan area of the province of Milan (Italy) in which the considered CIs refer to the transportation system (road, rail, underground, and airport system; Figure 10). In particular, for the road system, the pilot study considered highways, beltways and the national roads. The aim was to test the model's ability to represent all types of interdependencies and to provide an overview of the possible outcome of the model (Trucco et al., 2012). In the current study, we refer to the same case and simulation model.

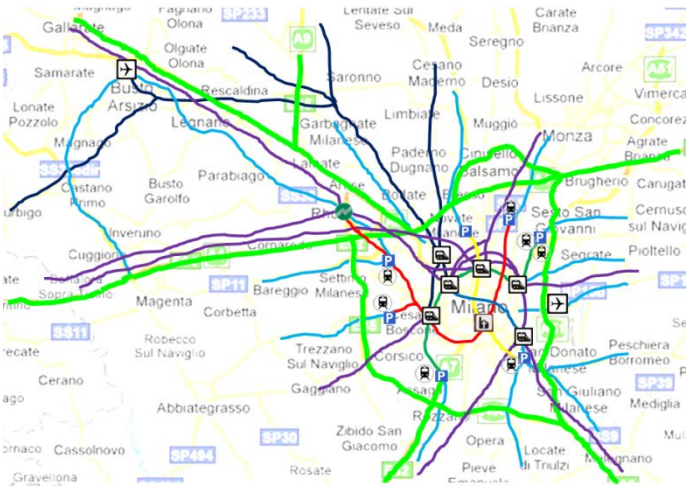

Figure 10: Milan metropolitan area transportation system

Afterwards, Cagno et al. (2011) applied DMCI to analyse a real scenario, i.e., the impact on the transportation system of a snowfall that took place in the north of Italy in December 2009. In the current study, we use the same data to characterise the system and the same scenario to assess the expected benefits on system resilience due to enhanced information-sharing and collaboration among CIs operators and first responders. Indeed, during an emergency, the ability to reduce the response time in all of the system nodes will naturally result in benefits. In cases

in which this is not possible (e.g., due to limited resources), it is necessary to prioritise nodes and attempt to achieve the best possible results by selectively acting on the most crucial nodes.

4.2 Pilot application in the Lombardy region (Italy)

Following the release of the EC Directive 2008/114/EC (EC, 2008), the Lombardy Region Administration decided to set up a preliminary study to investigate critical infrastructure vulnerabilities and to assess current emergency practices in the sector. It emerged that great potential exists for an increase in the flow of shared information with respect to criticality and accidents, which could increase the efficiency of the invested resources and also deliver improvements in the security level. The objective of the Lombardy region policy in CIP/R is therefore not to add new mechanisms or control processes but to **promote and advance collaborative processes**. In light of this logic, since 2010, the Lombardy Region has promoted a PPP aimed at defining a model of integrated and shared management that is capable of supporting a higher level of collaboration within the processes of prevention, risk monitoring and emergency management related to regional CIs. The preliminary study, carried out by a team of academics and consultants, provided a complete picture of the actual status of the vulnerability of regional infrastructural nodes and the corresponding emergency management processes adopted by the most important CI operators. More specifically, the study focused on:

- Carrying out a census of the critical nodes for major regional transportation (road, rail, air and underground) and energy (electricity, gas and fuels) infrastructures, and globally, more than 200 regional nodes have been identified and documented;
- Analysis of accidents that influence the regional CIs and creation of a series of historical cases;
- Mapping of the organisational models and operational processes of emergency management of the main CI operators active in the region.

Thematic Task Forces (TTFs) represent the backbone of the programme implementation. The TTFs thus far have focused on mapping of the information flows and communication channels among actors, developing collaborative procedures for coping with major meteorological events (e.g., heavy snowfall) and setting up collaborative activities in the case of large blackout events. The primary objective is to increase the effectiveness and operational efficiency using a greater standardisation of communication flows and channels among actors in the regional system. Additionally, operators are becoming more aware of the need to increase the quality of shared information, or at least improve communication effectiveness, to reach a common operational picture. An ongoing effort also exists to support the collaborative plans between CI operators via release of an information-sharing application.

4.3 Snowfall event and modelling

In the current study, we refer to the snowfall event that heavily impacted Northern Italy. On December 19th, 2009, the regional meteorological centre of Lombardy (ARPA-SMR) was alerted to the possibility of a significant and widespread snowfall over the entire region. Snow began to fall in the afternoon of December 21st (approximately 3 pm) and continued until the early morning of the following day (5 am), leaving an almost 30-cm layer of snow over the entire region. New precipitation fell in the early afternoon of December 22nd and lasted until the morning of December 23rd (8 am). Together with the snow, a second phenomenon of 'freezing rain' was present during this period, which was even more critical than the snow itself, considering its effects on the transportation system. The major problems that hamper proper functioning of the various considered infrastructures are summarised in the following sections. For a more detailed description, the reader may refer to Cagno et al. (2011).

Threat and impact modelling

A threat which impacts at time *t* on the CI or on a section of the CI (vulnerable node), causes a reduction of functional integrity and a consequent reduction in the maximum service level that the impacted node is able to supply. The same threat (i.e., the snowfall in the real scenario that is analysed) may impact different CIs in several different ways. This section explains how the reduction of functional integrity has been modelled for each CI of the considered transportation system.

With snow and freezing rain, the road surfaces become covered in ice. This phenomenon is particularly critical for motorways, where the draining asphalt facilitates the formation of ice on the road. Thus, the reduction in the services that can be supplied by the road system is primarily related to the reduction of vehicle speed and the increase of vehicle braking distance, which result in a considerable reduction of the flow of vehicles compared with the flow in normal meteorological conditions. Moreover, the probability of car accidents, small and large fender-benders and jack-knifing of trucks increases, which cause significant congestion on the roads. Next, another phenomenon that could be considered is related to snow-emergency operative procedures, i.e., roadblocks, truck filters, and measures imposed by CI operators to allow for minimal reduction of services to avoid traffic congestion and to reduce problems related to car accidents or jack-knifing accidents of heavy trucks.

In any of the abovementioned cases, because the impact could include partial or complete closure of the road, the reduction of functional integrity generated by the snowfall is similar to a step function (Figure 11).

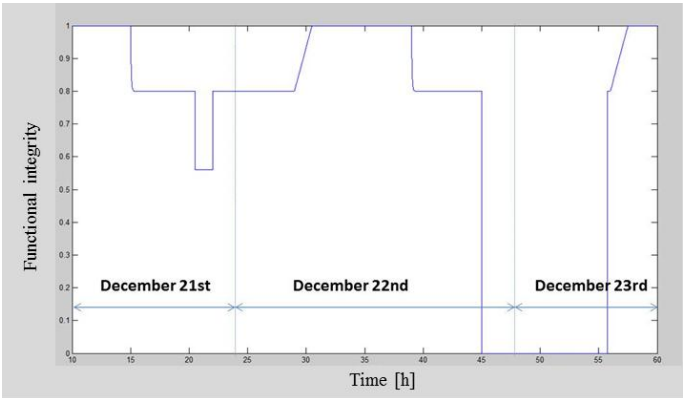

Figure 11: Functional integrity of highway A7 during the snowfall that took place in December 2009.

For railways, one of the major problems that usually occur during snowfalls is freezing of the railroad switches or formation of snowdrifts that prevent the proper functioning of the power system, which causes blockages of the railroad branches that depend on these systems. Furthermore, falling snow or landslide vegetation could add additional weight that may cause branches to break and fall onto the tracks or overhead wires.

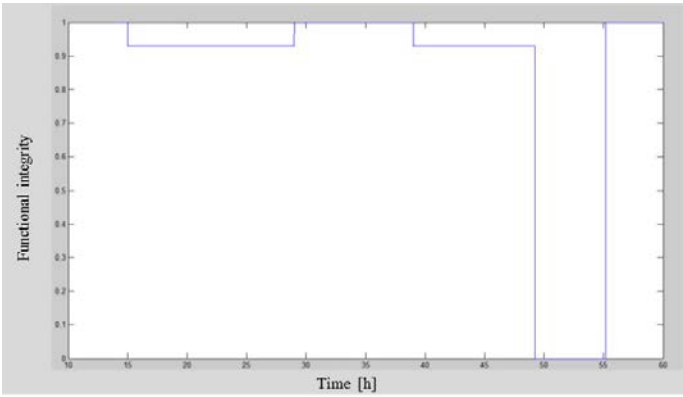

Figure 12: Functional integrity of the Milano-Como railway between 14.00 on December 21st and 12.00 on December 23rd.

The estimation of the reduction in the functional integrity of the railway network system was defined according to the number of trains cancelled over the total number of regional and local trains. Furthermore, the reduction rate was increased to account for the delays that occurred on the line and also caused MSD (Figure 12).

To model the loss of functional integrity at airports, specific data were collected directly from airport operators. The reduction rate was estimated as the ratio between the total number of movements (departures and arrivals) cancelled over the total movements in the period. Figure 13 shows the functional integrity of both airports (Malpensa and Linate) between 14.00 on December 21st and 12.00 on December 23rd.

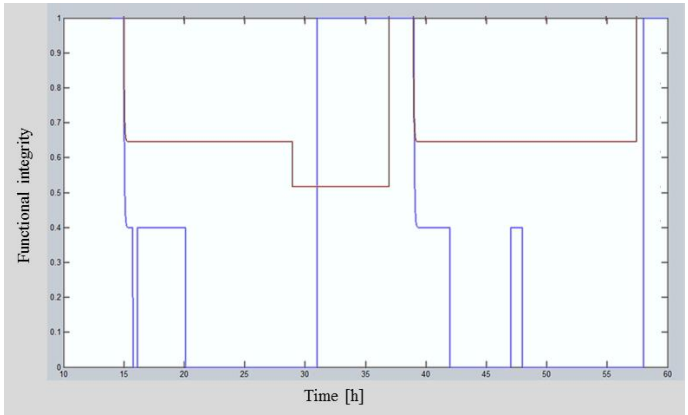

Figure 13: Functional integrity of the Milan Linate Airport (in red) and Malpensa International Airport (in blue) between 14.00 on December 21st and 12.00 on December 23rd.

Modelling of the recovery processes

Once the snowfall stopped, the CI operators attempted to restore services as soon as possible. The recovery time of each node in the road transportation system (i.e., highway, beltway, national road, or subsets of these) depends on the number of lanes in the road and the number of snowploughs employed. The increase in the functional integrity of the route is linear and reaches the value of 1 when the snowploughs terminate their work and the roads are completely cleared. The functional integrity was represented via a linear function (see Figure 11 as an example).

The recovery process of nodes in the railway network is achieved through the use of antifreeze liquids to thaw snow and ice from the sleeves that cover the overhead transmission wires. To account for the recovery of the railroad lines in the model, a step function (see Fig. 8 as an example) was used because the rail services concerned are not supplied until full recovery of the infrastructure is reached.

Recovery of the functional integrity of airport runways is achieved by scattering of chemical compounds (i.e., liquids consisting of sand and alcohol, gravel and/or rubble with a diameter less than or equal to 3.5 mm) that can improve the braking action of the aircrafts. To introduce this countermeasure into the model, it was not possible to resort to a linear function as in the model for the highway and road system, because the services supplied by the airstrip are not proportional to the number of meters of runway cleared of snow and ice. The services that can be supplied depend on the traction conditions of the entire runway because aircraft operation requires braking action along the entire length of the runway. For this reason, it was decided to resort to a step function to register the fact that this service is completely recovered only when the interventions carried out by the airport's personnel (staff) are completed.

5 Analysis and discussion of results

Phase 1: *Simple disruption scenario analysis*. This phase simulates the behaviour of the system by imposing a value of functional integrity equal to zero to a single node during a period of 15 h to evaluate the overall effect of the lack

of service in that node. Simulations of this type were run for each of the 169 nodes of the system. To ensure that both the demand cycle of the system and the recovery dynamics are fully covered, each simulation was run over a 36-hour window.

The demand in each node varies during the day, and therefore, in addition, the effects of 'shutting down' the node at a specific time of the day were considered via rolling simulation runs (i.e., each node disruption is started on the hour, e.g., 1 am, 2 am, 3 am, etc.) to better analyse the dynamic behaviour of the entire network. Thus, collection of data for each of the 169 nodes at 24 different periods of the day (one every hour) consisted of 4056 simulations. In this manner, the average total MSD (or *vitality*) was calculated for each node.

The second portion of the analysis consisted of running a new set of simulations for all 169 nodes within 24 different initial hours and over a 36-hour window as well as considering response time variations of ±10% in the disrupted node. The purpose of this set of simulations was to observe how the MSD values change with a faster response (reduced time) and a slower response (increased time) to a threat and thus obtain the nodes' average *agility* (across the disruption hours).

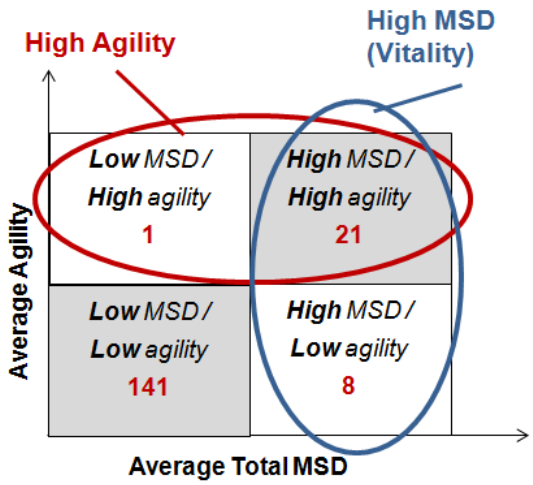

Figure 14: Classification of transportation system nodes in terms of MSD and agility.

Once the nodes are mapped into the matrix, two main groups are visible (highlighted in Figure 14), one including nodes that cause a high level of MSD in the system and other containing nodes with high agility. The former group includes nodes that have important effects on the system in terms of its overall performance. The latter group includes those nodes that induce great variation in system performance (total MSD) if the response time is reduced or increased (thus turning resourcefulness into benefits). Improvement of the system performance by acting on the vital nodes is feasible if their robustness is increased, either by improving node protection and/or preventing the propagation of MSD (through interdependencies) via node isolation. However, this approach may require structural changes in the system and additional investments. Improvements in the system's performance also can be achieved by acting on the agile nodes, primarily by developing strategies that enhance the response process. Because the proposed solution is focused more heavily on characterising resilience features than robustness, we focus on the nodes with high agility and assess the effects of improved organisational capabilities (resourcefulness/response time)

acting on this group. Resourcefulness is enhanced by the information-sharing processes among the actors, which is the focus of the current study.

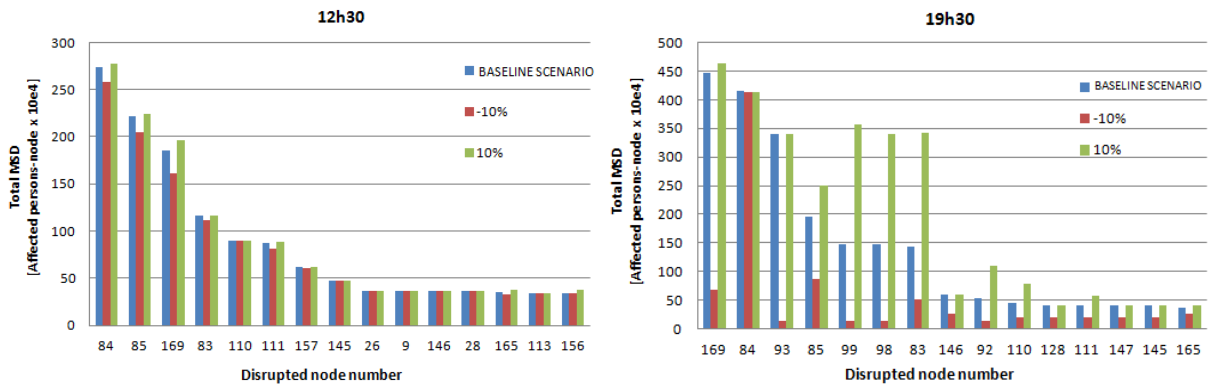

Figure 15: Vitality and agility dependence on disruption time: Total MSD vs. disrupted node for disruption at 12h30 (left) and 19h30 (right)

Figure 15 shows the nodes with the highest total MSD, according to the baseline scenario, as well as the ± 10% variation in response time due to disruption at two different hours, i.e., 12h30 and 19h30. This scenario is a good example of how the nodes' vitality and agility significantly vary with the disruption time due to the variation in demand during the day and also indicates that the variance of vitality and agility is an important factor that should be taken into consideration.

Focusing on the high-agility group (22 nodes), a second classification was carried out, this time using the variance of each indicator instead of its average value (Figure 16) to characterise 15 nodes as stable (making improvements certain) and 7 as nodes unstable (difficult to manage).

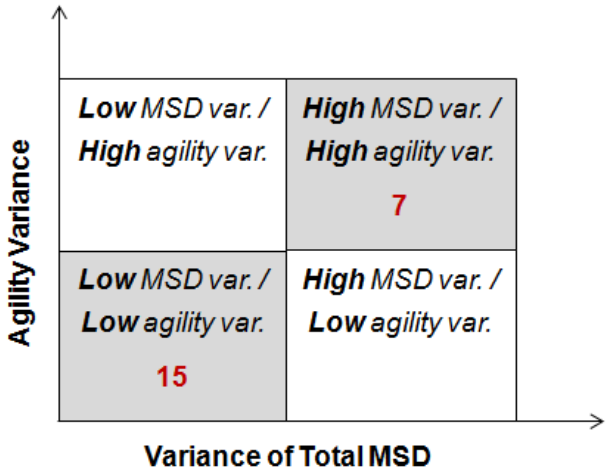

Figure 16: Classification of high-agility transportation system nodes in terms of MSD and agility variances

Phase 2: *Complex disruption scenario analysis*. Due to the amount of data collected, the simulation model was able to accurately replicate what occurred during the event. Starting from this "baseline" scenario, we further analysed the

expected effects of different response strategies that were defined based on the system characterisation explained in the previous section.

Not all of the nodes are vulnerable to a snowfall scenario, and thus, not all of the nodes located in the high-agility zone suffered a reduction in their functional integrity during the snowfall event. The nodes that are by far the most vital and agile and also show low variances of these values (i.e., the Centrale, Garibaldi and Cadorna train stations) did not experience any loss of functional integrity; therefore, we will focus on those that did, which include the following sections (all of them in the low-low variance zone):

- Nodes #1, 3, 4: Beltways;
- Nodes #13, 14: Highways;
- Node #113: Malpensa International Airport;
- Nodes #156, 157: Railways.

The first strategy consisted of acting on each of the nodes individually. The proposed action involved reducing the response time by 10%, 15%, 25% and 50% (with respect to the real situation) and observing the improvements in the system's performance. Improvements at railway nodes 156 and 157 resulted in a negligible reduction of the total MSD in the system (~0.01%), regardless of the improvement level. The global contribution of individual improvements in the road and highway nodes was low as well (~0.5% or ~16,000 MSD units), and this improvement saturated after a response time reduction of approximately 15%, i.e., any further improvement did not result in additional benefits on the global or local level.

We observed that local actions have rather limited impacts in absolute terms, whereas local improvements increase to 5% in the case of highways (~4,000 units) and by up to 40% for the Malpensa International Airport (~11,000 units). A reduction in the response time of the nodes corresponding to roads and highways of above 15% does not have additional effects on the system, because the behaviour of the system remains constant when further improvements are added.

A second type of analysis consisted of three simulation campaigns in which concurrent and simultaneous improvements in clusters of targeted nodes were applied:

a) Roads and highways (nodes 1, 3, 4, 13, 14);
b) Malpensa airport (node 113) in combination with its direct road and highway connections;
c) Combined action on both local highways/roads and the Malpensa airport and its connections;

Figure 17 displays the total MSD after the improvements of response time in each of the three clusters of nodes. Option a) increased the overall resilience of the transportation system by 2.8% before reaching saturation (at a 15% response time reduction). Option b) delivered an overall improvement in the system of almost 8% when the recovery time was reduced to half of the original value. Option c), the best case, resulted in an increase of 11% (~270,000 units) in the overall benefit.

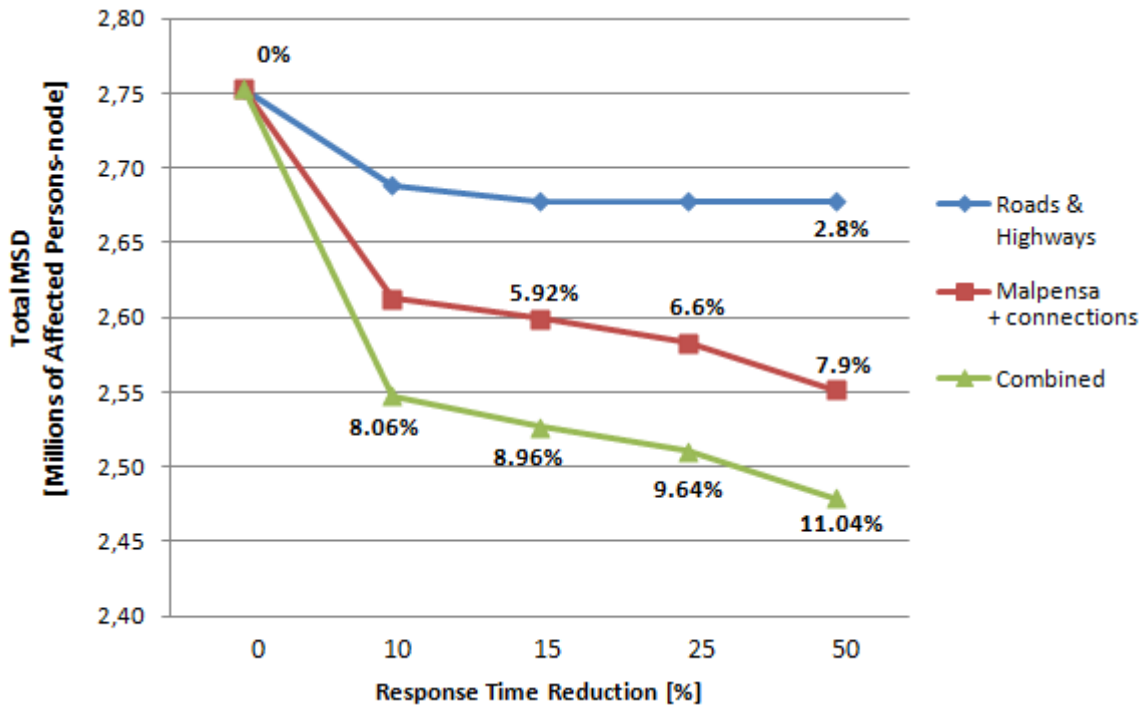

Figure 17: Overall improvements due to various reductions in response time for groups of high-agility nodes

Subsequently, in addition to the first proposed action, we consider a controlled migration of users from heavily disrupted infrastructure (roads, highways and beltways) to another, more robust option, i.e., railways and underground. This analysis is justified given that the *Significativity index*, as defined by Cagno et al. (2011), which quantifies the percentage importance of the impact of a threat on a given type of infrastructure with respect to the global impact of the threat on the CI system in the scenario, clearly indicated a major impact on highways (0.834) compared with railways (0.045) in the snowfall scenario considered.

The demand shift builds upon the logical interdependencies and simulates the decisions by people to switch to other infrastructures that offer the same service. However, the migration must be controlled because the train transportation system does not have an unlimited capacity and is able to absorb the increasing demand originating from the road system until it reaches its maximum capacity; after reaching that threshold, the system would suffer from saturation and generate additional MSD. Keeping this scenario in mind and considering the results from earlier simulation campaigns (Cagno et al., 2011), it was assumed that the shift of demand could range between 0% and 10%. Accordingly, simulations were run for six levels of demand shift (0%, 2%, 4%, 6%, 8% and 10%).

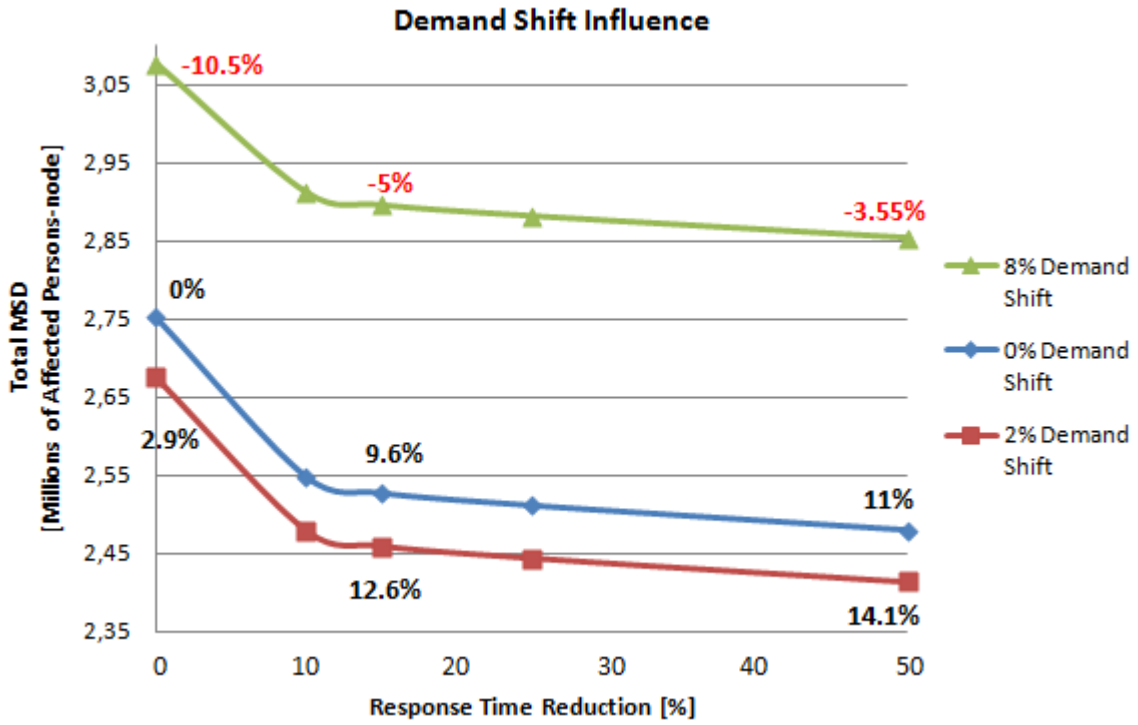

Figure 18: Overall improvements due to a combination of response time reduction and demand shift

Figure 18 shows the simulation outcomes for a combination of response time reductions (only in the high-agility nodes) and demand shifts (for 0%, 2% and 8%). This strategy results in a global reduction of MSD of up to 14% if the proposed 50% improvements in response time are reached and combined with the 2% demand shift. The simulations also showed that local reductions in MSD with the same improvements reach as high as 22% for roads and highways and up to 60% for the Malpensa International Airport.

6 Conclusions

This study provides useful results and original contributions at the methodological and practical levels. For the methodological aspect, the proposed approach to CI system resilience characterisation was applied in combination with a flow-based network simulation model (Trucco et al., 2012). However, this model is suitable for implementation in combination with other simulation models and/or other resilience performance measures or indices. With reference to Ouyang's (2014) classification and comparison, modelling and simulation approaches that consider functional performance are able to capture the system dynamics and cover all types of interdependencies (e.g., flow-based or agent-based methods) and are compatible with the defined methodology, unlike methods based on topology or economic theory. With respect to system resilience measures, different metrics (KPIs) are applicable for resilience quantification within the methodology (see e.g., Ayyub, 2013; Francis & Bekera, 2014; Henry & Ramirez-Marquez, 2012) according to different definitions of resilience and the specific needs of a particular infrastructure sector.

Building upon *Node vitality* (Luiijf et al., 2003), a.k.a. *Criticality* (Fisher & Norman, 2010), which estimates the overall consequences of node disruption, we introduced the concept of *Node agility*, which indicates the sensitivity of those consequences on the system level (or *total MSD*, in our case) for improved node performance during an emergency (improved *resourcefulness*, in our case). When deploying the resilience characteristics of complex system, the value of considering agility lies in the fact that it is crucial to target efforts to the components of the system in which they are guaranteed to materialise in improvements. In this way, the benefits are maximised, and emergency actions will have the highest value.

For practical implementation of the methodology to select the most effective resilience strategies under a given emergency scenario, the application to a large transportation infrastructure system subjected to a severe snowfall event returned selected general properties of the CI system response. For widespread disruption events in which a significant number of nodes are concurrently impacted, the rigidity of the system makes it impossible to provide significant global improvements by acting only on a few nodes, even the most vital or agile ones. However, efforts should be focused locally to create adequate improvements in the corresponding components of the network. The scattered resilience capabilities of such systems confirm the appropriateness of the proposed two-phase methodology.

Evidence returned by the application case suggests that an effective strategy for improving CI system resilience in response to large and widespread disruptions may consist of:

- *Node clustering* – To create benefits, each action must be supported by similar efforts in the interdependent transportation nodes. Response actions must be executed concurrently because isolated improvements usually do not provide any benefit. Therefore, in aiming to improve the system resilience on the global level, a promising approach involves identifying clusters of interdependent nodes on which to implement resilient measures concurrently. To maximise resilience, it is necessary to find the best combination of resilience options and node clusters, which is feasible through simulations.
- *Prioritisation* – Due to the infrastructure system size and limited available resources, it is not feasible to apply measures to the entire system, and therefore, it is necessary to prioritise activities, carefully target response efforts and act on selected (clusters of) nodes.
- *Allocate additional resources* – Civil protection or other public agencies normally house resources for use during emergencies. These additional resources are at the disposal of all of the involved actors but are not sufficient to fulfil all response needs. Therefore, resources must be allocated intelligently so that they can be utilised in the most efficient and beneficial manner. These mechanisms are generally defined, agreed upon and implemented within the PPPs.

The application case also revealed that *Exploiting logical interdependencies* (e.g., a demand shift from roads to rails) can improve performance, but in our scenario, it contributes to performance by a rather moderate amount (2-4%).

However, all of the above strategies can be achieved only by simultaneous and harmonised local actions based on situational awareness built upon deep collaboration and efficient information sharing. Planning should begin with

inter-organisational interactions during periods of normal operation during which contingency plans and emergency management processes can be jointly improved for future use. Of course, an in-depth investigation on how these processes can be effectively designed and implemented is beyond the scope of the current study. However, the possibility of accounting for these dimensions within the proposed methodology, e.g., the capacity of those in charge to take rapid action, largely depends on the simulation model used. The DMCI model, which was applied in this work, uses performance shapes (disruption, response time and recovery) according to the real technical and organisational capabilities of operators and public agencies, thus accounting for all relevant internal and external factors. In this respect, one limitation of our study is that possible real-time decisions and real-time changes in organisation and strategies are not covered in the simulation model. A further limitation of the simulation model is its inability to cover all of the resilience capabilities because it is limited to resourcefulness (cfr. Section 2). Still, depending on the power of the adopted simulation model, the proposed methodology contains sufficient general properties to be used for estimating benefits in the other two main resilience dimensions, i.e., improved system robustness or improved recovery process. Such analyses could support better decision-making on specific actions and strategic investments (e.g., infrastructure structural changes and location/allocation of available recovery resources).

REFERENCES

Argonne National Laboratory (ANL), Decision and Information Sciences Division, (2012) ‘Resilience: Theory and Application’, January 2012.

Argonne National Laboratory (ANL), Decision and Information Sciences Division (2010) ‘Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program’, August 2010.

Attoh-Okine, N.O., Cooper, A.T. and Mensah, S.A. (2009) "Formulation of Resilience Index of Urban Infrastructure Using Belief Functions," *Systems Journal, IEEE* , vol.3, no.2, pp.147,153.

Aven T. (2011) On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Analysis*, Vol. 31, No. 4, pp. 515–22.

Ayyub, B. M. (2013), Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making. Risk Analysis. doi: 10.1111/risa.12093

Bharosa, N., Lee, J. and Janssen, M. (2009) “Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises”, *Information Systems Frontiers* 12 (1), pp. 1-7.

Boone, W. (2012) ‘Full Spectrum Resilience: An Executive Summary’, *CIP report* June 2012, Center for Infrastructure Protection and Homeland Security, George Mason University, VA (USA)

Bouchon, S. (2006) *The Vulnerability of interdependent. Critical Infrastructures Systems*: Epistemological and Conceptual State-of-the-Art. Institute for the Protection and Security of the Citizen, EC JRC, 2006.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and von Winterfeldt, D. (2003) A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra* 19 (4), pp. 733–752.

Cagno, E. De Ambroggi, M. and Trucco, P. (2011) Interdependency analysis of CIs in real scenarios, Proceedings of ESREL 2011 - Advances in Safety, Reliability and Risk Management, Bérenguer, Grall & Guedes Soares (eds), pp. 2508-2514, Taylor & Francis Group, London, ISBN 978-0-415-68379-1.

Cohen, F. (2010) What makes critical infrastructures Critical?, *International Journal of Critical Infrastructure Protection*, Volume 3, Issue 2, pp. 53-54.

De Bruijne, M. and Van Eeten, M. (2007) Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management*, Volume 15, Issue 1, pp. 18–29.

Department of Homeland Security – DHS (2011), National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency.

Department of Homeland Security (DHS) website, Critical Infrastructure Protection Partnerships and Information Sharing (http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing), visited on 10/04/2013.

Dilmaghani, R. B. and Rao, R. R. (2008) "An Ad Hoc Network Infrastructure: Communication and Information Sharing for Emergency Response", *IEEE International Conference on Wireless & Mobile Computing, Networking & Communication* (WIMOB '08), pp. 442-447, October 2008, Avignon, France.

Eckert, S. E. (2005) Protecting Critical Infrastructure: The Role of the Private Sector in Guns and Butter. *The Political Economy of International Security*, Peter Dombrowski, ed. Boulder, Colo.: Lynne Rienner Publishers, 2005.

Egan, M. J. (2007), Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Journal of Contingencies and Crisis Management*, 15, pp. 4–17.

European 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, Official Journal of the European Union

Fedorowicz, J., Gogan, J. L. and Williams, C. B. (2007) "A collaborative network for first responders: Lessons from the CapWIN case", *Government Information Quarterly*, Vol. 24, No. 4, pp. 785–807.

Fisher, R. E. and Norman, M. (2010) 'Developing measurement indices to enhance protection and resilience of critical infrastructure and key resources', *Journal of Business Continuity & Emergency Planning*, Vol. 4, No. 3, pp. 191-206, Henry Stewart Publications

Francis, R. and Bekera, B. (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliability Engineering & System Safety, Volume 121, pp. 90-103.

George, R. (2008) Critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, Volume 1, pp 4-5.

Gryszkiewicz, A. And Chen, F. (2010) "Design Requirements for information sharing in crisis management command and control centre", Proceedings of the 7th Intrenational ISCRAM Conference, May 2010, Seattle, USA.

Haimes Y. (2009a) On the complex definition of risk: A systems-based approach. Risk Analysis, 29:1647–1654.

Haimes Y. (2009b) On the definition of resilience in systems. *Risk Analysis* 29:498–501.

Hémond, Y. and Robert, B. (2012) "Evaluation of state of resilience for a critical infrastructure in a context of interdependencies" *International Journal of Critical Infrastructures* – Special Issue on Next Generation Critical Infrastructure Systems: Challenges, Solutions and Research, Vol. 8 No. 2/3, pp.95-106.

Henry, D. and Ramirez-Marquez, J. E. (2012) Generic metrics and quantitative approaches for system resilience as a function of time, *Reliability Engineering & System Safety*, Volume 99, pp. 114-122.

Kimmance, J. (2010) Infrastructure Risk & Resilience. Assessing Infrastructure Vulnerability, Diversity and Resilience. Presentation at Business Continuity Institute (BCI) Workshop, Bristol 2010

Luiijf, H.A.M. Burger, H. & Klaver M. (2003) Critical Infrastructure Protection in Netherlands: A Quick-scan. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (ISBN: 87-987271-2-5). Copenhagen: EICAR.

Moteff, J. D. (2012) 'Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress', Congressional Research Service, CRS Report for Congress, August 23, 2012.

National Infrastructure Advisory Council – NIAC (2009) '*Critical Infrastructure Resilience – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

National Infrastructure Advisory Council – NIAC (2010) 'A Framework for Establishing Critical Infrastructure Resilience Goals - Final Report and Recommendations by the Council', U.S. Department of Homeland Security, Washington, D.C., 2010.

National Infrastructure Advisory Council – NIAC (2012), '*Intelligence information sharing – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering & System Safety*, Volume 121, pp. 43-60.

Ouyang, M. and Dueñas-Osorio, L. (2012) Time-dependent resilience assessment and improvement of urban infrastructure systems, *Chaos: An Interdisciplinary Journal of Nonlinear Science*, Volume 22, Issue 3, American Institute of Physics.

Petrenj, B., Lettieri, E. and Trucco, P. (2012) Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities, *International Journal of Critical Infrastructures* – Special Issue on Next Generation Critical Infrastructure Systems: Challenges, Solutions and Research, Vol. 8 No. 2/3 (2012), pp.107-120.

Pursiainen, C. (2009) 'The Challenges for European Critical Infrastructure Protection', *Journal of European Integration*, Volume 31, Issue 6, pp. 721-739.

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

Robert, B., Morabito L. and Quenneville, O. (2007) "The preventive approach to risks related to interdependent infrastructures", *International journal of emergency management*, Vol. 4, No. 2, pp.166–182.

Rosenkrantz, D. J., Goel, S., Ravi, S.S., and Gangolly, J. (2009) "Resilience Metrics for Service-Oriented Networks: A Service Allocation Approach," IEEE Transactions on Services Computing, vol. 2, no. 3, pp. 183-196.

Sandia National Laboratories, Complex Adaptive Systems of Systems (CASoS) Engineering (2013). A Resilience Assessment Framework for Infrastructure Systems, website visited on August 1st, 2013, available at: http://www.sandia.gov/CasosEngineering/resilience_assess_framework.html

Schooley, B. and Horan, T. (2007) "Towards end-to-end government performance management: Case study of interorganizational information integration in emergency medical services (EMS)", *Government Information Quarterly*, Vol. 24, No. 4, pp. 755–784.

Sheffi, Y. and Rice, J. (2005) A Supply Chain View of the Resilient Enterprise, *MIT Sloan Management Review*, 47 (1), pp. 41-48.

Solano, E. (2010) 'Theoretical Framework for the Vulnerability and Resilience Assessments of Infrastructures', Presented at the IHSS Reseach Summit 2010, Research Tiangle Park, NC.

Taylor-Powell, E., Rossing, B., & Geran, J. (1998). Evaluating collaboratives: Reaching the potential. Madison, WI: University of Wisconsin-Extension.

Tierney, K. and Bruneau, M. (2007) Conceptualized and Measuring Resilience, TR News 250, pp. 14–17.

Trucco, P. Cagno, E. & De Ambroggi, M. (2012) Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures, *Reliability Engineering & System Safety*, Volume 105, September 2012, Pages 51-63, doi:10.1016/j.ress.2011.12.003.

UK Cabinet Office, Civil Contingencies Secretariat (2011) Keeping the Country Running: Natural Hazards and Infrastructure: A Guide to improving the resilience of critical infrastructure and essential services.

United Nations (2005), Report of the World Conference on disaster prevention, Kobe (Hyogo, Japon), 18-22 January 2005.

Zimmerman, R. (2004) Decision-Making and the Vulnerability of Interdependent Critical Infrastructure. CREATE report, Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, Los Angeles (CA), USA.