Resilience of Critical Infrastructures: A Risk Assessment Methodology for Energy Corridors

Chapter

Resilience of Critical Infrastructures: A Risk Assessment Methodology for Energy Corridors

Andrea Carpignano, Daniele Grosso, Raffaella Gerboni and Andrea Bologna

Abstract

The need for scientific methodologies to assess quantitatively the resilience of critical infrastructures against natural hazards (like earthquakes, floods, storms, landslides and wildfires) during the last decade has become a relevant aspect for several countries and for the European Union. In fact, this quantification could allow setting and implementing effective measures to prevent or mitigate the negative socio-economic effects that a possible disruption of these infrastructures, caused by extreme natural events, could cause. This paper focuses, in particular, on energy corridors and proposes a new approach for evaluating their resilience, based on the definition of a criticality index able to estimate the economic damage associated to all the hazards by taking into account the spatial dimension of the infrastructure and by combining different interdependent parameters that could affect the criticality level. The procedure was tested by means of an application to a simplified case study. The obtained results highlighted the main advantages of the defined method, especially in ranking the critical sections of the infrastructure and prioritising the investments for reinforcing and protecting it or in identifying the further tests to be performed, especially in the case of a reassessment of the acceptable risk limit.

Keywords: critical infrastructures, risk acceptability, natural event, resilience, criticality index, energy corridors

1. Introduction

The reduction in the vulnerability to all the possible hazards (in many cases unpredictable) that could damage Critical Infrastructures (CIs) by improving the level of their protection and by increasing their resilience is one of the main goals of the European Union. The objective is to limit as much as possible the probability of widespread negative effects on EU's citizens and economy by ensuring services even in the case of significant disruptive events, coherently with the objectives of the Stockholm Programme [1] and of the EU Internal Security Strategy [2].

The United Nations International Strategy for Disaster Reduction (UNISDR) defined the resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration

of its essential basic structures and functions" [3]. This general statement applies also to the CIs.

According to the definition firstly given by the European Community in the 2004 Communication on "Critical Infrastructure Protection in the fight against terrorism" [4], the Critical Infrastructures are crucial systems, facilities, networks or assets which disruption would lead to relevant impacts on the socio-economic condition and development of a Member State (MS). For enhancing their protection not only against terrorism, but also against all the other hazards (thus including natural disasters), the European Programme for Critical Infrastructure Protections (EPCIP) was set [5, 6]. The aim of this programme was to define a general framework based on several principles including subsidiarity, sector-by-sector approach, complementarity, confidentiality, proportionality and stakeholder cooperation. It focused on the identification of the European Critical Infrastructures (ECI) defined as CIs located in EU's MS which disruption would significantly affect at least two MS [5]. It also addressed their possible interdependencies, the assessment of their risk by means of common approaches, the measures that could be set to improve their protection, the impacts that hazards and accidents external to EU's borders could have on the EU, the contingency plans to reduce or mitigate the negative effects of CI disruptions [5].

One of the most relevant documents for the implementation of the ECIP is the 2008 Directive on "the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" [7]. It represents the first approach to identify ECI and to evaluate the need for increasing their protection level, and it refers to only two specific sectors (energy and transport), pointing out the necessity of future reviews meant to include other sectors, like the information and communication technology (ICT) one. It also requires owners/operators of the identified ECI to produce Operator Security Plans (OSP), which define the options existing or being implemented for the ECI protection.

In 2013, a revision of the EPCIP was introduced [8], aiming at organising the implementation of the activities along three work streams (prevention, preparedness and response), at deepening the analysis of the interdependencies (both cross-sector and cross-border) and at taking into account critical ICT infrastructures and their relationship with other CIs (especially electricity generation and transmission infrastructures).

In 2017, an evaluation aiming at assessing the implementation of the 2008 Directive and focusing on its relevance, coherence, effectiveness, efficiency, EU added value and sustainability has been launched by the European Commission. The assessment process ended in 2019. It puts into evidence the need of revising the Directive, including further sectors besides the energy and transport ones and taking into account the interdependencies among sectors. Furthermore, it highlights the relevance that new threats – including those related to the artificial intelligence, the introduction of advanced ICT solutions that can create new vulnerabilities and the involvement of third countries in the ownership and operation of CIs – can assume [9, 10].

In order to effectively enhance the protection of CIs, quantitative methodologies, able to evaluate their resilience and to assess, in a holistic way, the different dimensions involved are needed. In particular, the approaches proposed in the scientific literature focus on some key aspects related to the concept of infrastructure resilience, namely: ad hoc risk assessment methodologies for quantifying the resilience of CIs, interlinks and interdependencies among CIs, analysis of the infrastructure vulnerability with respect to different kind of threats. Some of these approaches also try to assess the multi-dimensional (energy, social, environmental and economic) impacts due to disruptive events involving CIs.

With respect to these aspects, different reviews of the proposed studies are available in literature, as those carried out by Ouyang [11], Griot [12], Wang et al. [13] and Liu et al. [14].

Considering the quantitative methodologies for evaluating the resilience of CIs, two studies prepared by the JRC can be firstly mentioned. In particular, Galbusera et al. [15] proposed a feasibility study for the application of stress tests (like those adopted in the nuclear and economic sectors) to the evaluation of CI resilience against several hazards. Giannopoulos et al. [16] carried out an analysis of the state of the art related to the risk assessment methodologies that could be useful for the protection of CIs. A general approach to risk analysis and management of system-of systems can be found in the studies performed by Haimes et al. [17] and by Ariel Pinto et al. [18]. Eusgeld et al. [19] analysed instead the alternative modelling options (integrated and coupled models) for system-of-systems and proposed a specific High Level Architecture (HLA) for modelling Supervisory Control and Data Acquisition (SCADA) and "System under Control" (SuC, like gas supply system or power supply system). Labaka et al. [20, 21] suggested a holistic framework (based on the identification of resilience policies, on their influence and on the methodology for their implementation) aiming at increasing the resilience of CIs by identifying their resilience level, their weaknesses and the possible improvements to be implemented. Mao et al. [22] highlighted that different measures aiming at increasing the resilience of CIs can be coherent or conflicting among each other, due to a missing systemic approach. Consequently, they proposed a framework based on a quality function deployment (QFD) that takes into account the correlations between resilience improvement actions at different stages of the CIs lifecycle. Nan et al. [23] proposed a method for resilience estimation, which combines a hybrid multi-layer model (for capturing the interaction between different subsystems) and an integrated metric (for the quantification of the resilience, considering the different resilience capabilities). Ouyang et al. [24] focused on the CIs protection, starting from the actions that can be adopted to protect weak system components before a disruptive event happens and comparing the robustness-based approach (mainly related to the remaining functionality level of the system after the event and before the restoration) and the resilience-based approach (which includes the possible restoration path and the related rapidity).

The opportunity to model infrastructure networks as interconnected system-of-systems in order to properly describe the cascade effects due to their strong interdependencies has been underlined by several authors. Theocharidou et al. [25] suggested a new methodology – called CRitical Infrastructures & Systems Risk and Resilience Assessment Methodology (CRISRRAM) – developed in an all-hazard perspective and based on a system-of-systems approach (a definition of system-of-systems can be found in [26]), which introduces three layers (society, asset and system) and evaluates the direct or indirect effects on economy, environment and citizens caused by the hazards considered in each scenario. Another approach based on the system-of-systems concept, a Monte Carlo simulation and a Hierarchical Graph representation of the interdependent CIs is the one described by Ferrario et al. [27], which was applied to two case studies – concerning respectively small electric and gas grids (plus a SCADA system) and a large electrical distribution network – for the evaluation of their robustness. Kröger et al. [28] and Zio [29, 30] furtherly suggested an approach – helpful in CI protection – based on the risk and vulnerability concepts and able to allow the identification of possible vulnerabilities (both evident and hidden), thus avoiding the failures that could originate when the CIs are subject to hazards of multiple nature. Johansson et al. also focused on the opportunity to use vulnerability analyses to complete reliability studies of CIs [31] and demonstrated it by applying a Monte Carlo approach for reliability analyses and

a vulnerability analysis to an electric power system. Moreover, Johansson et al. [32] proposed a model that could be useful in the framework of vulnerability analyses of interdependent infrastructures that are described by both a network model (based on the graph theory) and a functional model. Stergiopoulos et al. [33] explored the interdependencies among CIs that cause cascading effects in the case of failure. For this purpose, the authors started from the dependency risk methodology proposed by Kotzanikolaou et al. [34, 35] and introduced graph centrality metrics in order to identify the nodes that mainly affect the risk paths and that can thus be controlled in order to improve risk mitigation. Furthermore, Stergiopoulos et al. [36] extended the studies performed by Kotzanikolaou et al. [34, 35, 37] by considering the time evolution of each dependency (using fuzzy models) and the concurrent common-cause cascading failures, developing a supporting tool for decision making (named CIDA, i.e. Critical Infrastructure Dependency Analysis). This tool can be useful in assessing the CI's resilience under different scenarios and the effectiveness of possible mitigation actions. Fu et al. [38] also focused on the opportunity of treating infrastructure networks as interdependent system-of-systems, while Utne et al. [39] proposed a methodological approach to model the interdependencies among CIs built starting from the use of relatively simple cascade diagrams. Furthermore, the JRC developed the Geospatial Risk and Resilience Assessment Platform (GRRASP), a graphical tool for analysing network systems that can be adopted to identify the critical elements of the network and to evaluate the cascading effects of CI disruptions, taking into account cross-sectoral and cross-border interdependencies [40].

Finally, with reference to the impact analysis of different threats on CIs, specific models have been developed in order to assess the physical security and the resilience of CIs themselves against single kinds of hazards. In particular, Khalil et al. [41] focused on the modelling of physical security of CIs under attack scenarios by using a Monte Carlo-based probabilistic dynamic approach. Urlainis et al. [42] implemented instead a supporting tool for decision making suitable to evaluate the risk related to oil & gas critical infrastructures after the occurrence of a seismic event. This tool adopts fault-trees, decision trees and fragility curves and allows the identification of the most critical sections of the analysed system based on the damage state of its components. Shakou et al. [43] proposed a framework for increasing the resilience of CIs with respect to climate change phenomena, based on different timescales and promoting flexibility, modularisation and diversification.

In comparison with the mentioned studies available in the scientific literature, the new methodological approach proposed in this paper mainly focuses on single large infrastructures (like energy corridors for oil and gas supply) and aims at taking into account their geographical dimension, allowing analyses characterised by a high spatial granularity. Furthermore, the proposed procedure is able to consider the most relevant interdependencies among the parameters that could impact on the criticality of an infrastructure with a simple mathematical formulation. Therefore, this work aims at being a supporting tool not only for infrastructures management companies and for the civil protection but also for public administrations.

The paper considers the energy CIs: according to the 2008 EU Directive, this category includes facilities and infrastructures for power generation and transmission, for oil and gas production, treatment, storage and transmission and LNG terminals [7]. In particular, it focuses on the energy corridors (oil and gas pipelines, power lines).

Its goal is to define a methodology for the evaluation of a criticality index, related to the failure of an energy infrastructure due to extreme natural hazards like earthquakes, floods, storms, landslides and wildfires. This criticality index is useful to assess the criticality level of each section of the infrastructure itself (taking into

account its spatial dimension) with respect to the socio-economic damage (measured in economic unit) caused by the failure. Furthermore, the possibility to estimate the distance from the criticality status even in case of non-critical scenarios and to compare the criticality condition with a risk acceptability criterion (identifying – for the most critical sections – the need for undergoing structural tests) could give a valuable support in prioritising investments and in defining suitable countermeasures and protective actions.

2. Methodology

The proposed approach starts from the concept of energy corridor. A corridor can be defined as an extensive infrastructure (like natural gas and oil pipelines and large power lines), characterised by a start point and an end point, that links production/refining facilities with distribution hubs. Energy corridors are usually strategic elements for the economy of the countries that are connected to them, and their influence spreads over a large area not limited to the geographical neighbourhood of the infrastructure. In a future world that is expected to be increasingly interconnected with large scale energy markets, the role of energy corridors could become crucial: the diversification of the sources and the possibility to ensure the functionality of the infrastructures could significantly impact on the security of energy supply and on the economic systems of several countries, especially those characterised by a high level of energy import dependency.

For these reasons, the quantitative evaluation of the resilience of the energy corridors against possible adverse events through the numerical estimation of their criticality level and the simultaneous identification of suitable criteria for risk acceptability are essential in order to identify the sections that require attention and investments for preventing potentially severe failures which could impact on the GDP (Gross Domestic Product) with losses at different scales.

According to the methodology described in the following sections, a set of parameters influencing the criticality status of the corridor and their interdependencies have been firstly defined (Section 2.1). A relationship linking these parameters has then been built to define a new Criticality Index (Section 2.2). A criterion for the risk acceptability (Section 2.3) and the application of the whole procedure to a simplified case study have been eventually discussed (Section 3).

2.1 Identification of the parameters and their interdependencies

The proposed methodology focuses on the quantitative assessment of the criticality of a single section of an energy corridor under an all-hazard perspective, i.e. with respect to all the possible extreme natural events.

For this purpose, the first step has been represented by the definition of a set of parameters that could affect the criticality level of an energy infrastructure, by their clustering into different groups and by the analysis of their interdependencies. Moreover, in order to take into account the spatial dimension of the energy corridors, the possible dependency of each parameter on the geographical position z_c (ranging between 0 and the corridor length l_c and measured in km) along the corridor itself has been explored. In fact, an infrastructure like a pipeline can typically run over long lengths and the natural environment surrounding it could significantly change along the route: consequently, certain natural hazards could be considered only for a limited set of branches and not for the overall length of the corridor. Eventually, the effects of a variation in the value of each parameter on the damage have been estimated. In particular, in this study 15 parameters and 4 groups

("Event related", "Corridor related", "Backup sources related" and "Users related") have been considered: the parameters taken into account are listed in **Table 1** and the dependency matrix is shown in **Table 2**. The interdependencies are identified assuming as increasing the value of each independent parameter and reporting the effect on the dependent parameter (decreasing or increasing when the independent parameter increases). The table reports also the effect of each parameter on damage.

Referring to Group 1, the seasonality s – that represents the variability of the considered natural event across the year – is the parameter that mainly affects the other ones. The probability p that the natural event could have an impact not only on the analysed corridor but also on other infrastructures supplying the same commodity (backup sources) is strictly related to the magnitude of the event itself and on the geographical context: it depends on the distance between the corridor (or corridor branch) and the considered backup source and on the potential damage area for the considered event, quantified through the damage distance λ. All the facilities located at a distance lower than or equal to λ are certainly involved by the event to such a degree that their functionality is lost.

In general, an increase in all the parameters related to the corridor (Group 2) causes an increase in the potential damage. It has to be highlighted that RT – which includes not only the time needed to repair the infrastructure but also the time for reaching the damaged section of the corridor and the time to get the requested spare parts – depends not only on the season but also on the temporal and spatial scale of

Group	Parameter	Description	Unit
1. Event related			
	p	Probability to involve more than a single facility	—
	λ	Damage distance (measure of the potential damage area of the event)	km
	τ	Time scale of the event (measure of its duration)	s
	s	Seasonal factor (influence of the season on the event)	—
2. Corridor related			
	l_c	Length of the corridor	km
	$c_{p,c}$	Peak capacity of the corridor	GJ/s
	RT	Repair time	s
3. Backup sources related			
	d_b	Distance between a single source and the corridor	km
	$c_{p,b}$	Peak capacity of the source	GJ/s
	$r_{m,b}$	Minimum available reserves for the single source	GJ
	α_b	Availability of the source	—
	α_{tec}	Technical availability of the source	—
4. Users related			
	i	Interruptible capacity	GJ/s
	α_i	Availability of interruptible capacity	—
	e	Energy intensity for the considered commodity	€/GJ

Table 1.
Considered parameters by group.

Parameter	Description	Dependency on the position z_c	Effects on damage		Inter-dependencies	
			↑	↓	↑ with	↓ with
p	Probability to involve more facilities	X	X		λ	d_b
λ	Damage distance		X			
τ	Event time scale		X		s	s
s	Season					
l_c	Corridor length	X	X			
$c_{p,c}$	Corridor peak capacity		X		s	s
RT	Repair time	X	X		τ, s	s
d_b	Distance source-corridor	X		X		
$c_{p,b}$	Source peak capacity			X	s	s
$r_{m,b}$	Minimum reserve of the source			X	s	s
α_b	Availability of the source	X		X	s, d_b	λ, s
α_{tec}	Technical availability			X	s	s
i	Interruptible capacity			X	s	s
α_i	Availability of i			X	s	s
e	Energy intensity		X			

Table 2.
Interdependencies and effects on damage.

the event: the greater the geographical extension of the natural event and its duration, the longer the time needed to reach the damaged section.

As it can be reasonably expected, an increase in the parameters related to the availability of backup sources causes a decrease in the damage. It can be underlined that the average distance between the backup sources provides information about the probability that a backup source could be involved in the considered extreme event: in fact, the higher the value of this parameter, the lower the probability. The availability of these sources depends not only on the seasonality, but also indirectly on the distance between the corridor and the source: in particular, it increases if the source is far from the epicentre of the event.

Considering Group 4, the parameters are related with the reference market: in case of a possible corridor failure, the market operator could decide a supply interruption for some selected users, in order to reduce the load of the considered infrastructure; the interruptible capacity could depend on the season. The energy intensity e (i.e. the amount of energy needed to produce a unit of GDP), instead, gives a measure of the importance of the commodity delivered by the considered corridor, allowing to quantify the economic damage deriving from the supply lost as a consequence of an extreme event.

It can be highlighted that the event related parameters can be evaluated on the basis of geological surveys and studies on natural hazards with respect to the specific site analysed. Among them, the probability of involving more facilities needs *ad hoc* formulations and cannot be generically expressed by means of a single mathematical relationship (as further discussed in Section 2.2). The majority of the corridor related and the backup sources related parameters are instead technical

data that are usually available for the specific infrastructures considered. Only the repair time should be estimated by means of suitable databases or specific investigations (Maintainability Analyses). Eventually, referring to the users related parameters, the interruptible capacity is an information that should be known as depending on already signed contracts and agreements, while the energy intensity for the commodity carried by the corridor can be obtained from statistical sources.

Furthermore, for the proposed method, the corridor can be assumed as one-dimensional, i.e. only characterised by the running coordinate z_c. This is because only the position along the corridor, the distance between the backup sources with respect to the corridor and the distance between the epicentre of the considered natural hazard and the corridor itself are relevant for the analysis.

2.2 Definition of the criticality index

Starting from the parameters and interdependencies identified in Section 2.1, in order to define a criticality index able to quantify the criticality of a single branch/corridor, a relationship expressing the socio-economic damage D due to a certain extreme natural hazard has been defined (Eq. (1)). It expresses the damage D in the section of the branch/corridor identified by the coordinate z_c (running over the corridor length, from 0 to l_c).

$$D(s,p,z_c,\tau) = \left\{ RT(s,z_c,\tau) \cdot \left[c_{p,c}(s) - \alpha_i(s) \cdot i(s) - \sum_b \alpha_b(s,p) \cdot c_{p,b}(s) \cdot \left(\frac{T_b}{RT(s,z_c,\tau)} \right) \right] \cdot \frac{1}{e} \right\} \tag{1}$$

where:

$$\begin{cases} T_b = T_b(s,z_c,\tau) = RT(s,z_c,\tau) & RT(s,z_c,\tau) \le \dfrac{r_{m,b}}{c_{p,b}} \\ T_b = T_b(s) = \dfrac{r_{m,b}(s)}{c_{p,b}(s)} & RT(s,z_c,\tau) > \dfrac{r_{m,b}}{c_{p,b}} \end{cases} \tag{2}$$

$$\alpha_b(s,p) = \alpha_{tec}(s) \cdot [1 - p(z_c)] \tag{3}$$

Eq. (1) defines the economic value of the share of the commodity carried by corridor c over the emergency time period (identified by RT) that cannot be directly delivered notwithstanding the contribution of interruptible users and the availability of backup sources. In fact, focusing on the square bracket in the equation:

- the term $c_{p,c}$ identifies the maximum amount of commodity that can be delivered per second in season s and that is lost due to the failure; as a consequence, the product between $c_{p,c}$ and RT defines the amount of energy unavailable during the repair time after the adverse event that caused the corridor failure
- the product between α_i, i and RT defines the part of this supply that can be avoided during the emergency due to the fact that some users are interruptible
- the product between α_b, $c_{p,b}$ and T_b corresponds to the amount of energy commodity that can be certainly supplied by the backup sources during the repair time.

Referring to the probability that the event could involve other facilities (in particular, the backup sources) than the considered corridor, this can be expressed

by several relationships or by more complex considerations that do not allow a simple mathematical formulation according to the different classes of natural events. For example, in the case of a river flood, p is a function not only of the distance between the corridor and the facility but also of the distance between the river and the facility. Furthermore, p is equal to 0 if the considered facility is outside the boundaries of the natural hazard, regardless of the distance between the source and the corridor. A possible relationship that can be adopted for some classes of events, like earthquakes, is the one expressed in Eq. (4) where the possible involved facilities are supposed to be the backup sources b. If the distance between the backup source and the corridor d_b is lower than the damage distance λ, the facility is assumed to be certainly involved by the event. If the distance d_b is higher than λ (i.e. the facility is located outside the potential damage area) the probability that the facility is involved by the event decreases in a proportional way with the increase of d_b.

$$p(z_c) = \begin{cases} \dfrac{\lambda}{d_b(z_c)} & d_b(z_c) \geq \lambda \\ 1 & d_b(z_c) < \lambda \end{cases} \tag{4}$$

Moreover, it has to be highlighted that Eq. (1) is defined if

$$c_{p,c}(s) - \alpha_i(s) \cdot i(s) - \sum_b \alpha_b(s,p) \cdot c_{p,b}(s) \cdot \left(\frac{T_b(s)}{RT(s,z_c,\tau)} \right) > 0$$

as, from the risk analysis point of view, the damage D has to be positively defined. A negative value of D means that the corresponding corridor section is not critical: negative values of this term could be obtained, for instance, in the case that no other facilities are involved by the natural event and the loss of corridor capacity is completely supplied by backup sources.

For this reason, the proposed relationship for defining the criticality index CI as a function of the socio-economic damage is the one reported in Eq. (5):

$$CI = \begin{cases} [1 + D(s,p,z_c,\tau)] \cdot \left[1 + e^{-D(s,p,z_c,\tau)}\right] - 1 & D(s,p,z_c,\tau) \geq 0 \\ \dfrac{1}{1 - D(s,p,z_c,\tau)} & D(s,p,z_c,\tau) < 0 \end{cases} \tag{5}$$

In this case, CI does not correspond to an economic value of the damage caused by the considered event (like D), but it allows to associate a numerical value also to the corridor sections that are not strictly critical (i.e. those for which D is negative) thus measuring their "proximity" to a real potential damage and ranking them according to a criticality perspective, as the safety margins progressively reduce when a negative value of D approximates to 0.

As it can be noticed, the CI relationship is built in order to have $\lim_{D \to \infty} CI = D$ and $CI = 1$ for $D = 0$ (i.e., when the infrastructure status changes from "non-critical" to "critical").

A graphical representation of CI as a function of D can be observed in **Figure 1**.

2.3 Criteria for risk acceptability

In the scientific literature, few studies are available to identify risk acceptability criteria for the socio-economic risk, and the differences among the economic

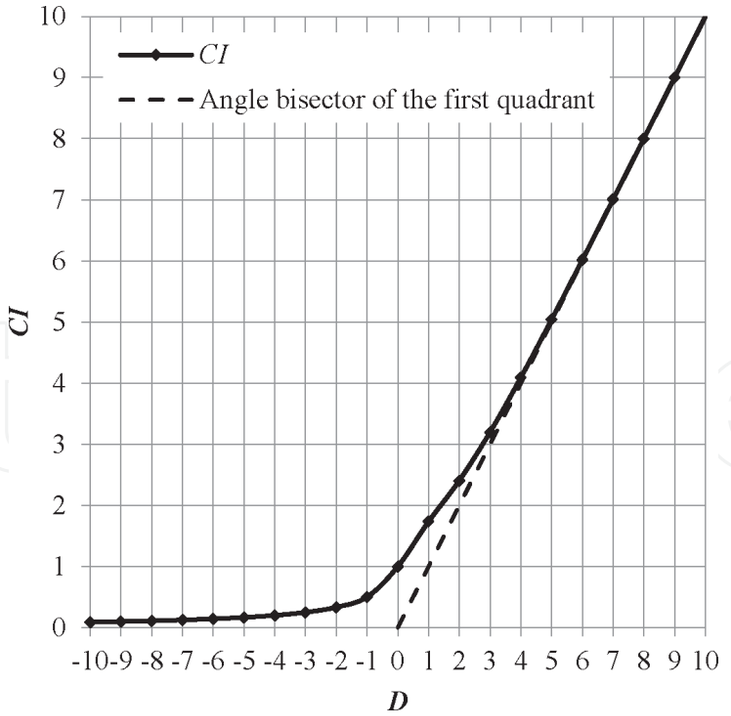

Figure 1.
Graphical representation of CI *as a function of* D.

systems do not allow to define easy procedures suitable to be applied to different contexts (like developed, developing and less developed countries).

For this reason, in the present paper a specific criterion has been proposed, based on the overall economic estimation of damages due to natural events, which takes into account both direct (i.e. to houses, infrastructures, industrial facilities, etc.) and indirect (i.e. productive losses, lack of basic services to population) damages.

According to the Munich Re insurance company statistical data, related to the global natural loss events worldwide (including geographical, meteorological, hydrological and climatological events) over the period 1980–2015 [44], the 2015 overall losses accounted for about 0.14% of the global GDP (GDP data from World Bank statistics [45]). However, during previous years significantly higher percentage values have been reached, in particular in 2011 (mostly due to the Tōhoku earthquake and tsunami in Japan), when the losses peaked at about 380 billion US dollars, and in 2005, mainly related to the hurricane Katrina in the U.S.. These two events, in particular, highlight that extreme events involving developed countries generally lead to more relevant economic effects even at a global scale.

The proposed expression for the acceptable annual economic damage related to a certain corridor is evaluated as a fraction of the annual GDP, by taking into account the contribution of the energy sector to the GDP composition, the contribution of the analysed corridor to the overall energy supply of the country/area, the weight of the economic losses due to an extreme natural event.

In particular:

- The contribution of the energy sector to the GDP is expressed by the f_{en} factor, defined as:

$$f_{en} = \frac{VA_{en}}{GDP} \tag{6}$$

where:

VA_{en}: value added of the energy sector; it has to be noticed that the GDP at market prices is the sum of the gross value added at market prices for all the productive sectors [46, 47].

- The contribution of the analysed corridor to the regional energy supply is given by the economic value of the commodity carried by the corridor c per year; the factor f_c, is defined as:

$$f_c = \frac{EV_c}{VA_{en}} \tag{7}$$

where:

EV_c: economic value of energy commodity delivered by corridor c

- The annual value of economic losses and expenditures related to the failure of the corridor c due to the natural event ne is assumed as the maximum acceptable risk, and the factor f_{ne} is defined as:

$$f_{ne} = \frac{L_{ne}}{GDP} \tag{8}$$

where:

L_{ne}: total economic losses and expenditures due to the natural event ne.

As no statistical data is available to evaluate the expenditures and economic losses for a specific natural event ne causing the failure of corridor c, the average value f_{ne}, defined at regional/country scale, is used as equivalent of the "local" ratio between the annual economic losses and expenditures associated to the failure of corridor c and the economic value EV_c of the commodity carried by c per year.

The previously described steps can be summarised into a single relationship (Eq. (9)), which allows to quantify the current economic risk in terms of monetary losses as a consequence of the adverse natural event ne:

$$R_a = f_{ne} \cdot f_{en} \cdot f_c \cdot GDP \tag{9}$$

It has to be highlighted that specific estimations of the total economic losses and expenditures L_{ne} are not commonly available as public data and should be provided by insurance companies.

Once the current risk is defined, the maximum tolerable frequency (number of events per year) for a given damage in the corridor section identified by the coordinate z_c is assessed by adopting a graphical approach which starts from the previously defined Criticality Index (i.e. the economic value of the damage caused by the service disruption due to the analysed event) (**Figure 2**).

From the obtained maximum acceptable frequency, the corresponding event intensity can be evaluated using the frequency-intensity curve, which is characteristic for each class of events (**Figure 3**).

Several studies are available in literature regarding the relationship between the frequency and the intensity (or magnitude) of natural events. For example purpose, the ones performed by Hungr et al. [48], Jakob et al. [49, 50], Riley et al. [51] (related to the debris flow landslides), Hooke [52], Zhang et al. [53] (focusing on floods), and Papadakis [54] (considering earthquakes in Greece) can be mentioned.

In general terms, the intensity is associated to specific characteristics of the considered event (like the peak ground acceleration for the earthquakes, the maximum water level for floods, the maximum wind speed for storms and the heat flux

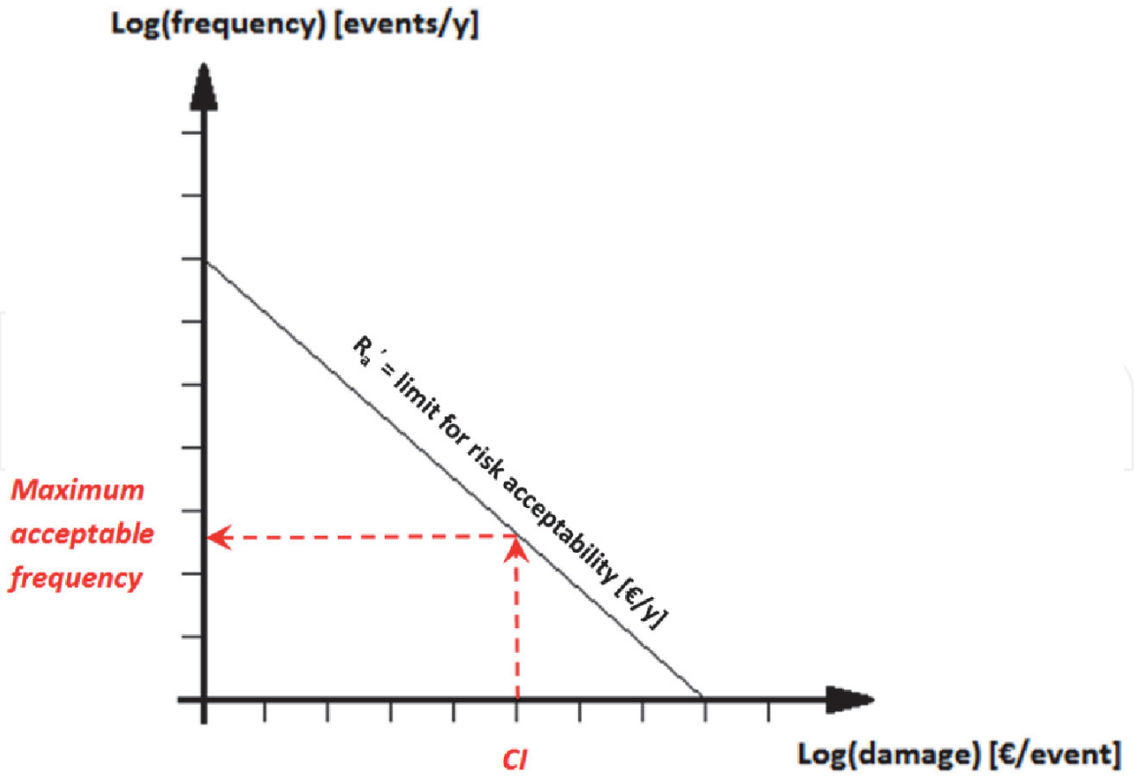

Figure 2.
Identification of the maximum tolerable frequency according to the CI *value.*

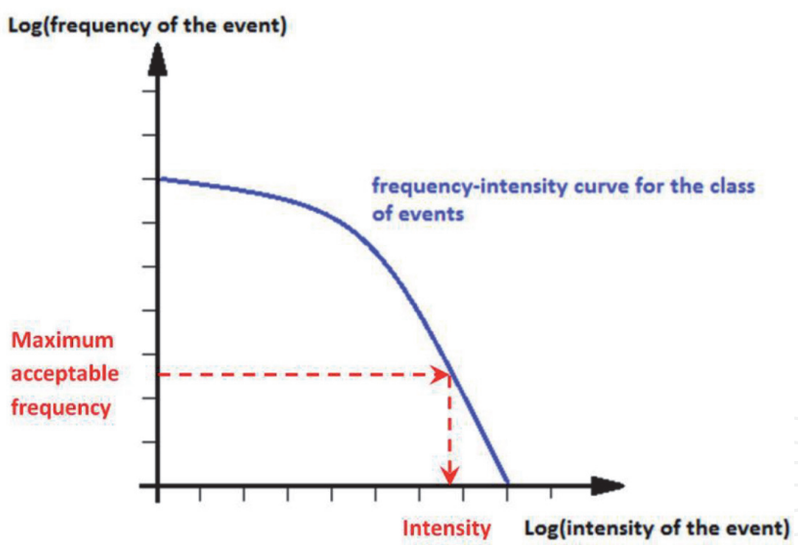

Figure 3.
Evaluation of the event intensity related to the maximum tolerable frequency according to frequency-intensity curve.

for fires) and the link between intensity and frequency is evaluated on the basis of historical data analyses.

The obtained intensity has to be compared with the design limit value for the analysed infrastructure.

It has to be further underlined that R_a represents the current overall risk related to the event *ne*. If a lower limit for risk acceptability for that event is desired, a reassessment (i.e. a reduction) has to be performed, according to Eq. (10).

$$R_a' = \alpha_{ne} \cdot R_a \tag{10}$$

where:

R'_a: reassessed limit for risk acceptability (see **Figure 2**)

α_{ne}: reassessment factor for the definition of the limit for risk acceptability related to the class of natural events *ne*; $\alpha \in [0,1]$

In this case, the same *CI* value corresponds to a lower maximum acceptable frequency, which – in turn – corresponds to a higher intensity that could exceed the design conditions of the infrastructure. In such a situation, new structural analyses have to be performed in order to verify its resilience and the possible need for mitigation actions, such as structural reinforcement, redundancy or relocation.

3. Case study and results discussion

The methodological approach described in Section 2 has been tested by applying it to a simplified case study. The main assumptions adopted can be summarised as follows:

- an ideal corridor and related surrounding environment have been taken into account;
- only two classes of extreme natural events (river floods and earthquakes) have been considered;
- three backup sources are available, able to cover the load for the entire period of unavailability of the corridor; these alternative sources are independent from the corridor itself;
- there is no interruptible capacity;
- a reassessment of the limit for risk acceptability has been assumed, with a risk reduction of one order of magnitude.

The spatial layout of the corridor and of the backup sources is shown in **Figure 4**, while their characterisation and the values of the main parameters are reported in **Table 3**.

It has to be underlined that, in this simplified case study, the values of the parameters have been chosen in order to be realistic but they are not corresponding to a real case. In particular, all the parameters have been assumed to be seasonally

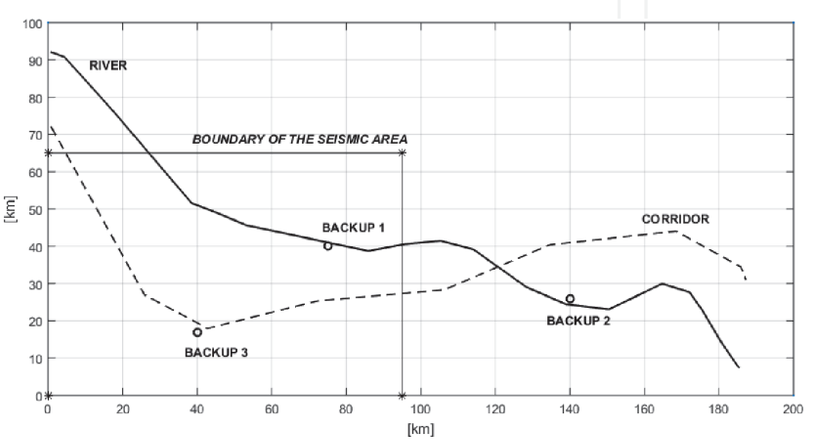

Figure 4.
Spatial layout of the corridor and of the backup sources.

Parameter	Description	Value	Unit
$p_{1,f}$	Probability to involve backup source 1 – flooding	0.5	—
$p_{2,f}$	Probability to involve backup source 2 – flooding	0.5	—
$p_{3,f}$	Probability to involve backup source 3 – flooding	0	—
λ_e	Earthquake damage distance	5	km
λ_f	Flooding damage distance	5	km
s	Seasonal factor (influence of the season on the event)	0	—
$c_{p,c}$	Peak capacity of the corridor	100	J/h
RT	Repair time	1	h
$c_{m,b1}$	Minimum operative margin in capacity – backup source 1	50	J/h
$c_{m,b2}$	Minimum operative margin in capacity – backup source 2	35	J/h
$c_{m,b3}$	Minimum operative margin in capacity – backup source 3	45	J/h
$\alpha_{t,b1}$	Technical availability of the backup source 1	0.95	—
$\alpha_{t,b2}$	Technical availability of the backup source 2	0.95	—
$\alpha_{t,b3}$	Technical availability of the backup source 3	0.95	—
i	Interruptible capacity	0	J/h
e	Energy intensity for the considered commodity	1	€/J
DBE	Magnitude of the design base earthquake	4.8	
DBF	Maximum discharge of the design base flood	2000	m^3/s
R_a	Current risk value	1	€/y
$R_a^{'}$	Reassessed limit for risk acceptability	0.1	€/y

Table 3.
Values of the main considered parameters.

independent. Furthermore, the values have been set in order to describe a realistic configuration from a physical point of view, while from the economic perspective a unitary value for current risk limit (1 €/y) has been selected mainly due to the unavailability of specific public data on the total economic losses and expenditures. In the reassessment of the limit for risk acceptability, the hypothesis of reducing it by an order of magnitude has been made. In general, if the proposed procedure is applied to a real system, the evaluation of the parameters should be performed according to the considerations expressed in Section 2.1.

The obtained CI (z_c) is shown in **Figure 5** for both earthquake (E) and flooding (F) events. In particular, it can be observed that the corridor sections characterised by the highest CI values are those close to the backup sources in the seismic area (in the case of earthquake event) and to the river (in the case of flooding event). The sections where $CI < 1$ are those corresponding to a damage $D < 0$, i.e. the capacity of the backup sources is more than the one requested to ensure the coverage of the load in the case of unavailability of the corridor.

However, it has to be remarked that all the sections characterised by CI value slightly lower than 1 have to be considered as they are close to a critical condition.

Referring to the evolution of the availability parameter α_b (s,p) for the three backup sources, it can be noticed (**Figure 6**) that the lower the distance between the corridor and the source, the lower the availability: this is because if the natural event involves an area in which the corridor and the backup are close to each other, the probability for the backup source to be damaged is higher, and so its availability is lower.

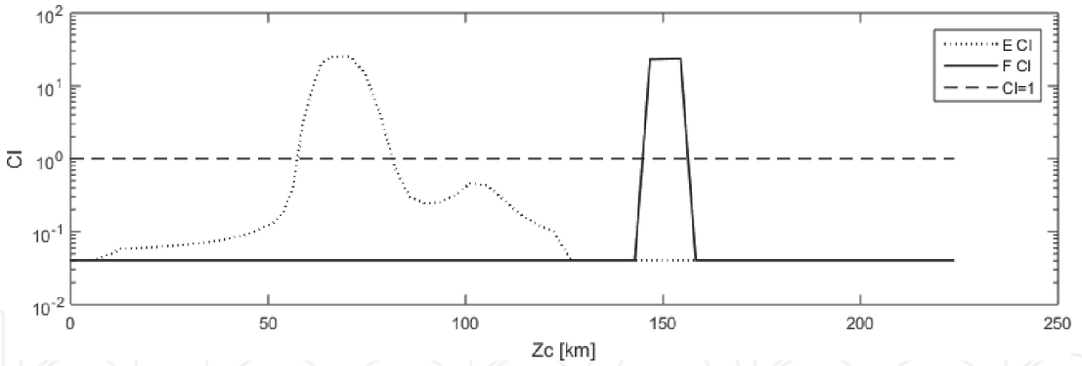

Figure 5.
CI *evolution with respect to the position along the corridor* z_c*; CI < 1 corresponds to D < 0.*

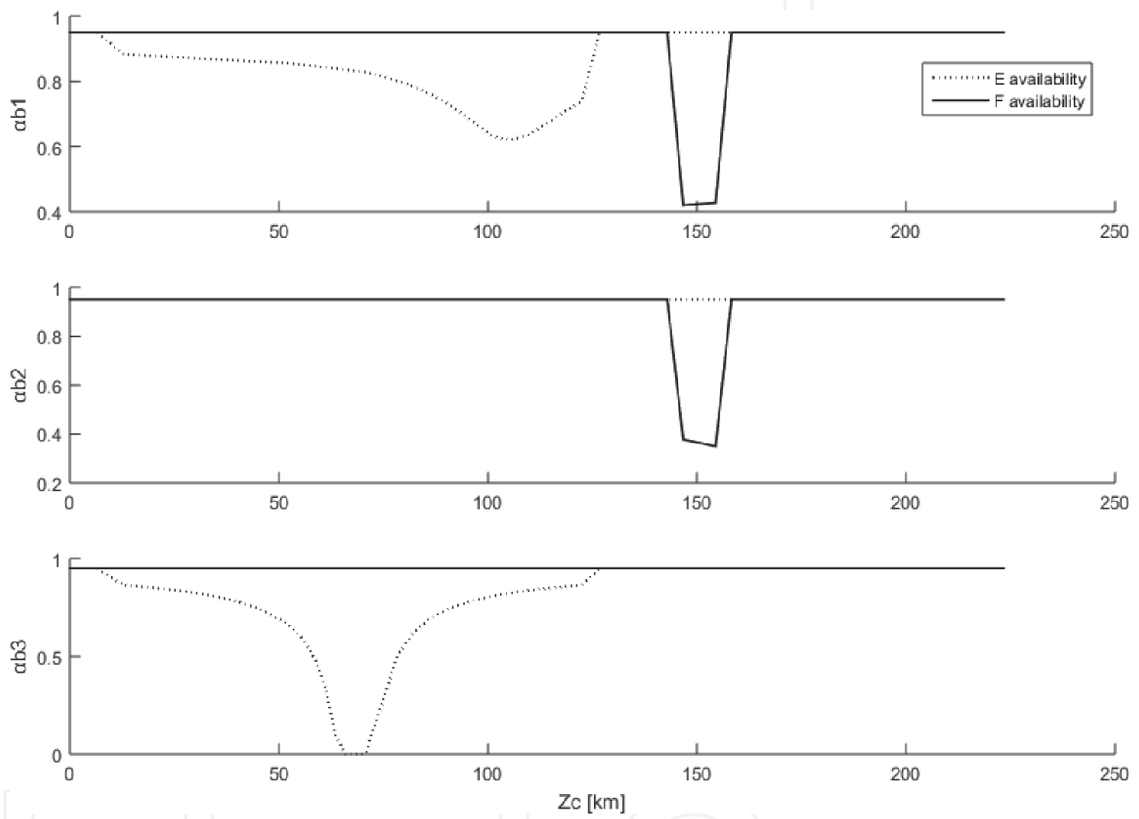

Figure 6.
Evolution of the availability of the backup sources with respect to the position along the corridor z_c*.*

Figure 7(a) shows the frequency-*CI* curves corresponding to the original limit for risk acceptability and to the reassessed one. **Figures 7(b)** and **(c)** represent the frequency-magnitude curves, which have been built by using two different approaches for the two considered classes of natural events:

- the Gutenberg-Richter law [55] in the case of earthquakes;
- a logarithmic relationship based on the one proposed by Wald et al. [56] in the case of flooding.

The vertical lines correspond to the design base earthquake magnitude (DBE) and flood (DBF) for the corridor.

Starting from these curves and from the previously defined *CI* evolution, the maximum acceptable frequencies and the related intensities for both earthquake

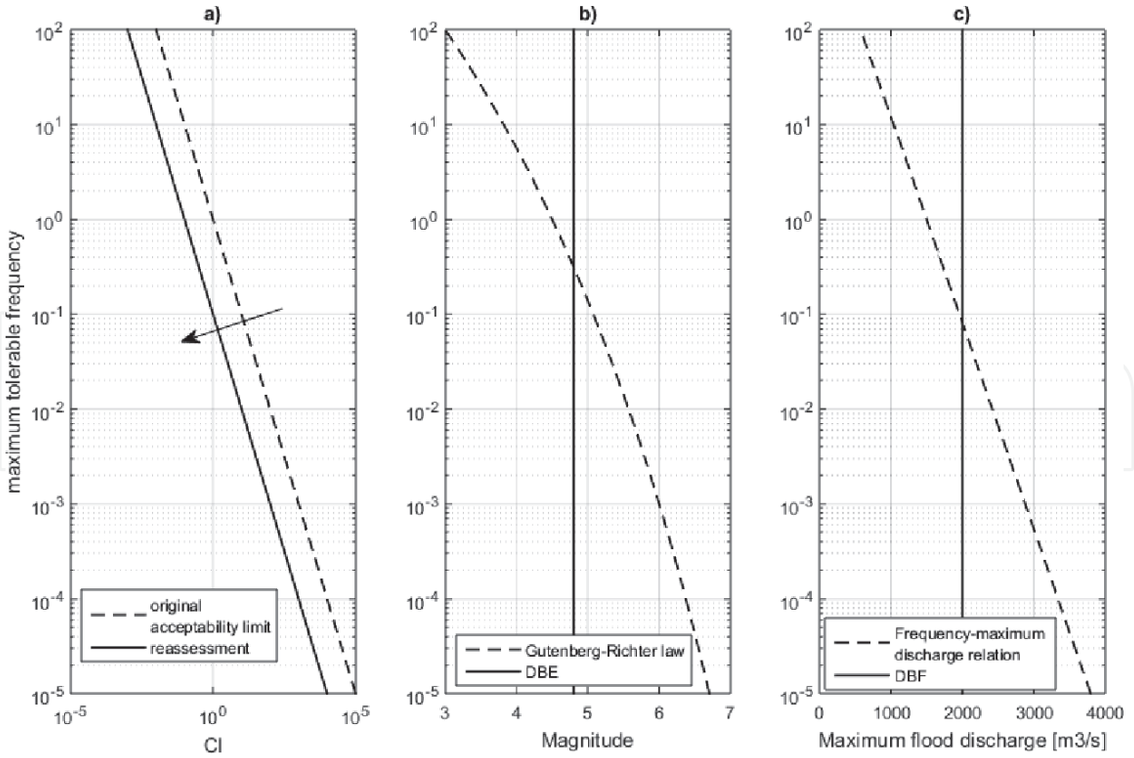

Figure 7.
*Frequency-*CI *(a) and frequency-magnitude curves (b, c) for the analysed case study.*

and flood events and for both the original (E/F old) and reassessed (E/F new) limit for risk acceptability have been estimated, as reported in **Figure 8**.

As it can be observed in **Figure 8a**, the maximum acceptable frequency for earthquakes reaches its minimum value (corresponding to the maximum intensity, visible in **Figure 8b**) in the section where the corridor and the backup source 3 are closest each other and are both affected by the natural event (p = 1 in Eq. (4)). Furthermore, it can be observed that in the case of reassessed risk limit the intensity is beyond the design condition (DBE, **Figure 8b**), thus leading to the need for performing tests in order to assess the robustness of the involved corridor section and to define suitable mitigation actions. The same considerations are valid for the flood (**Figure 8c** and **d**): the main difference is that – in this case – in the most critical corridor section the intensity overcomes the design value also for the original risk limit (DBF, **Figure 8d**), requiring further resilience tests also without hypothesising a reassessment of the limit for risk acceptability.

As mentioned before, the values of the considered parameters have been assumed without a specific reference to a real case, as the goal of the analysed case study is to show the functioning and the applicability of the proposed methodology through a theoretical example. For this reason, an analysis of the uncertainties has not been performed. Future works aiming at deeply exploring the criticality of existing infrastructures will include this aspect, especially regarding the event related parameters, with a particular attention devoted to the probability that different facilities are involved. As previously discussed, in fact, this probability needs detailed and complex considerations to be properly quantified with respect to the specific natural hazard and site studied.

This simplified case study, however, shows the potentiality of this approach in evaluating the possible critical sections of the infrastructures, prioritising the investments and the interventions in reinforcing them and in making them resilient to adverse extreme natural events.

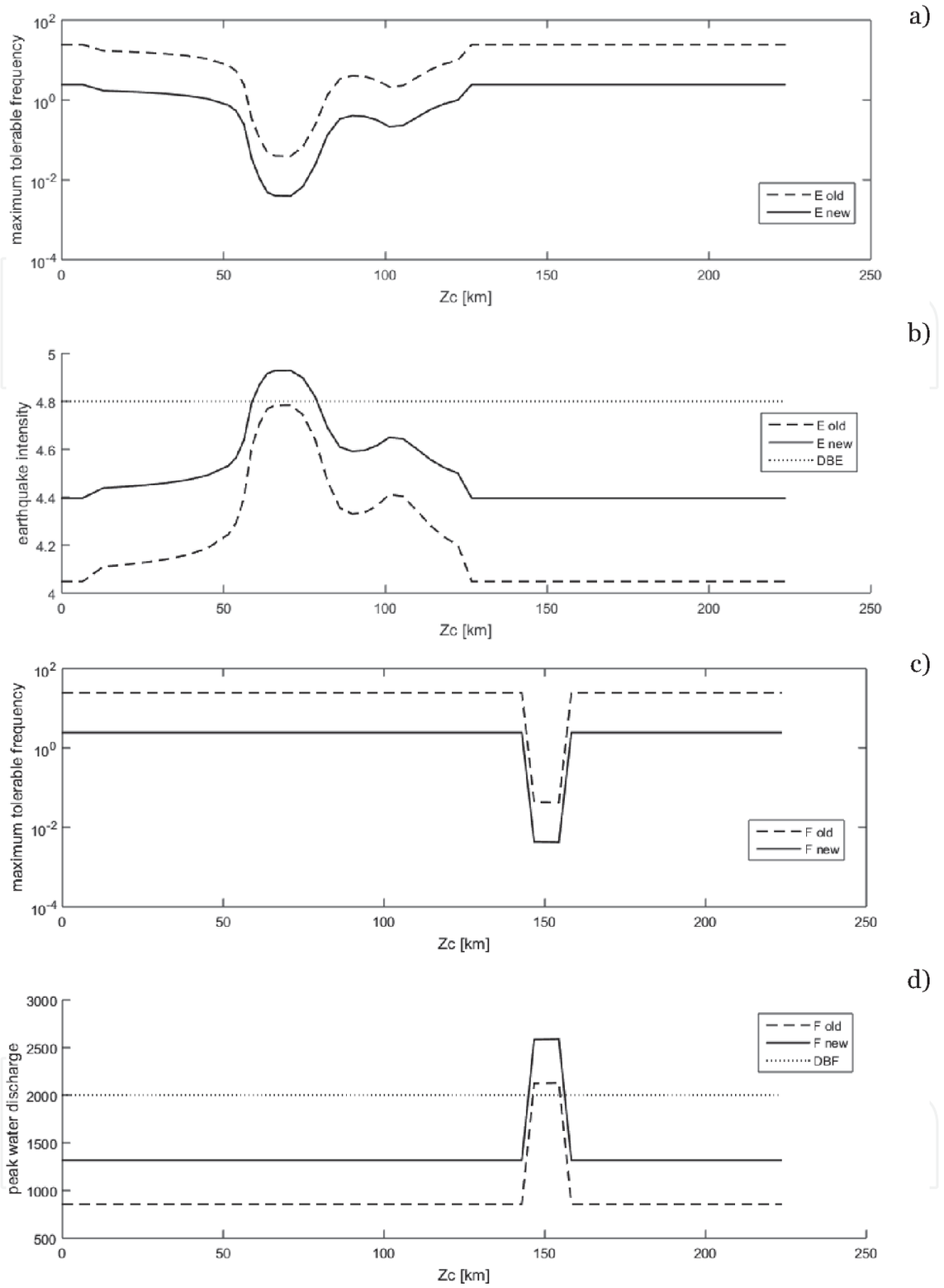

Figure 8.
Maximum tolerable frequencies and intensities of earthquakes (a-b) and floods (c-d) for the analysed cased study.

On the other hand, it also allows to identify some aspects that could be more deeply investigated in future studies in order to enhance the applicability to real cases and the effectiveness of the obtained results. In particular, among them, the unambiguous definition of the system boundaries can be mentioned. In fact, the identification of boundaries can be not easy in the case of meshed networks like natural gas distribution systems or power lines, for which it is difficult to define a single entry point and a single end point. Another relevant aspect is represented by

the availability of complete and uniform databases for both the technical characteristics of the analysed infrastructures/backup sources and the classes of natural events affecting the environment surrounding the infrastructure.

4. Conclusions

The protection of Critical Infrastructures against extreme natural hazards by evaluating and improving their resilience is one of the main goals for many countries or groups of countries (like the EU). For this reason, methodologies able to quantify the possible criticalities of these infrastructures are needed to better plan and implement actions, countermeasures and investments allowing to limit or avoid the negative energy, social and economic consequences deriving from natural hazards impacts.

With respect to other studies available in the scientific literature, the approach proposed in this paper focuses on energy corridors and aims at defining a criticality index, which is a function of the spatial position along the analysed corridor, and so it is useful to quantify the criticality level for each section of the considered infrastructure. This index is able to take into account a large variety of parameters (related to the natural event, to the corridor, to the availability of alternative sources and to the involved users) and their interdependencies. The developed methodology can be an effective supporting tool for decision makers and public administrations, for companies that have to manage crucial infrastructures for energy commodities transport and for the civil protection, as it allows – through a simple mathematical formulation – to identify the sections of an energy corridor that are critical with respect to a specific natural hazard or that are close to a criticality status, thus defining priority areas of intervention, preventive investments, mitigation actions and *ad hoc* countermeasures.

The introduced criticality index assesses in a numerical way the socio-economic damage (measured in monetary units) due to the effects of an extreme natural event on the selected infrastructure and can be used to evaluate the maximum acceptable frequency and the corresponding intensity of the event itself, allowing a comparison with the design condition of the corridor.

Furthermore, the possibility to evaluate the criticality index also for negative damage values (i.e. for not critical configurations) permits to measure the distance from the criticality, allowing to pay preventive attention to those sections that are closer to critical situations.

In general, the described approach gives the opportunity of ranking the single branches of a corridor according to their criticality and for all the different natural hazards, and, as a consequence, it gives the authorities in charge of protecting critical infrastructures the opportunity of prioritising the interventions.

The implementation of this methodology on real cases requires specialists from different fields and complex information. This can be deduced also from the application to a simplified case study (considering one corridor and two extreme events). However, the case study has underlined the advantages of the procedure, especially if a reassessment of risk acceptability limit is introduced, because it puts into evidence the safety margin with respect to the design conditions or the need for performing structural tests, quantifying the infrastructure resilience.

Additional aspects should be deeply analysed in the case of an extensive application of the proposed methodology, including – in particular – the availability of complete and homogenous technological and environmental databases and the proper definition of the system boundaries that could be not trivial in the case of meshed networks like the natural gas distribution ones.

Further studies could also be devoted to the analysis of multi-risk scenarios, i.e. to the concurrent occurrence of two or more extreme natural events, defining suitable strategies to allocate the acceptable risk (for instance by taking into account the safety margins of the infrastructure, if they are present), in order to test the infrastructure resilience in the worst (and low-frequency) conceivable conditions.

Author details

Andrea Carpignano[1], Daniele Grosso[2], Raffaella Gerboni[1*] and Andrea Bologna[1]

1 Politecnico di Torino, Torino, Italy

2 LINKS Foundation, EST@Energy Center – Politecnico di Torino, Torino, Italy

*Address all correspondence to: raffaella.gerboni@polito.it

References

[1] European Council. The Stockholm Programme – an open and secure Europe serving and protecting citizens, Official Journal of the European Union, 2010/C 115/01

[2] European Commission. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Communication from the Commission to the European Parliament and the Council, COM(2010) 673 final

[3] UNISDR. Terminology on Disaster Risk Reduction [Internet]. 2009. Available from: https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction [Accessed: 2020-09-23]

[4] European Commission. Critical Infrastructure Protection in the fight against terrorism, Communication from the Commission to the Council and the European Parliament, COM(2004) 702 final

[5] Commission of the European Communities. Green paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final

[6] Commission of the European Communities. Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final

[7] The Council of the European Union. Council Directive 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, 2008/114/EC

[8] European Commission. Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure, SWD (2013) 318 final

[9] European Commission. Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Final Report

[10] European Commission. Commission staff working document. Executive summary of the evaluation of council directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, SWD(2019) 308 final

[11] Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 2016;121: 43–60. DOI:10.1016/j.ress.2013.06.040

[12] Griot C. Modelling and simulation for critical infrastructure interdependency assessment: A meta-review for model characterization. International Journal of Critical Infrastructures, 2010;6:363–379. DOI: 10.1016/j.ress.2013.06.040

[13] Wang S, Hong L, Chen X, Zhang J, Yan Y. Review of interdependent infrastructure systems vulnerability analysis. In: Proceedings of the 2nd International Conference on Intelligent Control and Information Processes; 25–28 July 2011; Harbin, China: IEEE; 2011. p. 446–451

[14] Liu W, Song Z. Review of studies on the resilience of urban critical infrastructure networks, Reliability Engineering & System Safety. 2020;193: 1–16. DOI:10.1016/j.ress.2019.106617

[15] Galbusera L, Giannopoulos G, Ward D. Developing stress tests to

improve the resilience of critical infrastructures: a feasibility analysis, Luxembourg: Publications Office of the European Union; 2014. DOI:10.2788/954065

[16] Giannopoulos G, Filippini R, Schimmer M. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, Luxembourg: Publications Office of the European Union; 2012. DOI: 10.2788/22260

[17] Haimes YY. Models for risk management of systems of systems. International Journal of System of Systems Engineering. 2008;1:222–236. DOI:10.1504/ijsse.2008.018138

[18] Ariel Pinto C, McShane MK, Bozkurt I. System of systems perspective on risk: towards a unified concept. International Journal of System of Systems Engineering. 2012;3:33.46. DOI: 10.1504/ijsse.2012.046558

[19] Eusgeld I, Nan C, Dietz S. System of systems approach for interdependent critical infrastructures. Reliability Engineering & System Safety. 2011;96:6: 679–686. DOI: 10.1016/j.ress.2010.12.010

[20] Labaka L, Hernantes J, Sarriegi JM. Resilience framework for critical infrastructures: An empirical study in a nuclear plant. Reliability Engineering & System Safety. 2015;141:92–105. DOI: 10.1016/j.ress.2015.03.009

[21] Labaka L, Hernantes J, Sarriegi JM. A holistic framework for building critical infrastructure resilience. Technological Forecasting and Social Change. 2016;103:21–33. DOI: 10.1016/j.techfore.2015.11.005

[22] Mao Q, Li N, Peña-Mora F. Quality function deployment-based framework for improving the resilience of critical infrastructure systems. International Journal of Critical Infrastructure Protection. 2019;26:100304. DOI: 10.1016/j.ijcip.2019.100304

[23] Nan C, Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering & System Safety. 2017;157:35–53. DOI: 10.1016/j.ress.2016.08.013

[24] Ouyang M, Liu C, Xu M. Value of resilience-based solutions on critical infrastructure protection: Comparing with robustness-based solutions. Reliability Engineering and System Safety. 2019;190:106506. DOI: 10.1016/j.ress.2019.106506

[25] Theocharidou M, Giannopoulos G. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, Luxembourg: Publications Office of the European Union; 2015. DOI:10.2788/621843

[26] DeLaurentis D. Role of humans in complexity of a system-of-systems. In: Duffy VG, editor. Digital Human Modeling. Berlin-Heidelberg: Springer; 2007. p. 363–371. DOI: 10.1007/978-3-540-73321-8

[27] Ferrario E, Pedroni N, Zio E. Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation. Reliability Engineering & System Safety. 2016;155: 78–96. DOI: 10.1016/j.ress.2016.06.007

[28] Kröger W, Zio E. Vulnerable Systems. London: Springer; 2011. DOI: 10.1007/978-0-85729-655-9

[29] Zio E. Critical Infrastructures Vulnerability and Risk Analysis. European Journal for Security Research. 2016;1:97–114. DOI: 10.1007/s41125-016-0004-2

[30] Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering

& System Safety. 2016;152:137–150. DOI: 10.1016/j.ress.2016.02.009

[31] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliability Engineering & System Safety. 2013;120, pp. 27–38. DOI: 10.1016/j.ress.2013.02.027

[32] Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety. 2010;95: 1335–1344. DOI: 10.1016/j.ress.2010.06.010

[33] Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Gritzalis D. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. International Journal of Critical Infrastructure Protection. 2015;10:34–44. DOI: 10.1016/j.ijcip.2015.05.003

[34] Kotzanikolaou P, Theoharidou M, Gritzalis D. Assessing n^{th}-order dependencies between critical infrastructures. International Journal of Critical Infrastructures. 2013;9:93–110. DOI: 10.1504/ijcis.2013.051606

[35] Kotzanikolaou P, Theoharidou M, Gritzalis D. Cascading effects of common-cause failures in critical infrastructures. In: Butts J, Shenoi S editors. Critical Infrastructure Protection VII. Heidelberg: Springer; 2013. 171–182. DOI: 10.1007/978-3-642-45330-4

[36] Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Lykou G, Gritzalis D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. International Journal of Critical Infrastructure Protection. 2016;12:46–60. DOI: 10.1016/j.ijcip.2015.12.002

[37] Kotzanikolaou P, Theoharidou M, Gritzalis D. Interdependencies between critical infrastructures: Analyzing the risk of cascading effects. In: Bologna S, Hammerli B, Gritzalis D, Wolthusen S. editors. Critical Information Infrastructure Security. Berlin-Heidelberg: Springer-Verlag; 2013. 104–115. DOI: 10.1007/978-3-642-41476-3

[38] Fu G, Khoury M, Dawson R, Bullock S. Vulnerability Analysis of Interdependent Infrastructure Systems. In: Proceedings of the European Conference on Complex Systems (ECCS'12); September 2012; Brussels. Springer; 2012. p. 317–323

[39] Utne IB, Hokstad P, Vatn J. A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering & System Safety. 2011;96:671–678. DOI: 10.1016/j.ress.2010.12.006

[40] Azzini I, Dido M. GRRASP version 3.1 User Manual. In: Giannopoulos G, Galbusera L, editors. Luxembourg: Publications Office of the European Union; 2016. DOI: 10.2760/999066

[41] Khalil YF. A novel probabilistic timed dynamic model for physical security attack scenarios on critical infrastructures. Process Safety and Environmental Protection. 2016;102: 473–484. DOI: 10.1016/j.psep.2016.05.001

[42] Urlainis A, Shohet IM, Levy R. Probabilistic Risk assessment of Oil and Gas infrastructures for Seismic Extreme Events. Procedia Engineering. 2015;123: 590–598. DOI: 10.1016/j.proeng.2015.10.112

[43] Shakou LM, Wybo J, Reniers G, Boustras G. Developing an innovative framework for enhancing the resilience of critical infrastructure to climate change. Safety Science. 2019;118, 364–378. DOI: 10.1016/j.ssci.2019.05.019

[44] Munich Re. Loss events worldwide 1980–2015 [Internet]. 2016. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/Loss_events_worldwide_1980-2015.pdf [Accessed: 2020-09-24].

[45] World Bank. World Bank statistical database [Internet]. 2020. Available at: http://data.worldbank.org/ [Accessed 2020-09-24]

[46] Agarwala SK. Principles of Economics. New Delhi; Excel Books India; 2009. p. 324.

[47] Bhattacharyya SC. Energy Economics. Concepts, Issues, Markets and Governance. London: Springer-Verlag; 2011. p. 721. DOI: 10.1007/978-0-85729-268-1

[48] Hungr O, McDougall S, Wise M, Cullen M. Magnitude–frequency relationships of debris flows and debris avalanches in relation to slope relief. Geomorphology. 2008;96:355–365. DOI: 10.1016/j.geomorph.2007.03.020

[49] Jakob M, Friele P. Frequency and magnitude of debris flows on Cheekye River, British Columbia. Geomorphology. 2010;114:382–395. DOI: 10.1016/j.geomorph.2009.08.013

[50] Jakob M, Holm K, McDougall S. Debris-Flow Risk Assessment, Oxford Research Encyclopedia of Natural Hazard Science. Oxford University Press; 2016. DOI: 10.1093/acrefore/9780199389407.013.37

[51] Riley KL, Bendick R, Hyde KD, Gabet EJ. Frequency–magnitude distribution of debris flows compiled from global data, and comparison with post-fire debris flows in the western U.S. Geomorphology. 2013:191;118–128. DOI: 10.1016/j.geomorph.2013.03.008

[52] Hooke JM. Variations in flood magnitude–effect relations and the implications for flood risk assessment and river management. Geomorphology. 2015;251:91–107. DOI: 10.1016/j.geomorph.2015.05.014

[53] Zhang Q, Gu X, Singh VP, Sun P, Chen X, Kong D. Magnitude, frequency and timing of floods in the Tarim River basin, China: Changes, causes and implications. Global and Planetary Change. 2016;139:44–55. DOI: 10.1016/j.gloplacha.2015.10.005

[54] Papadakis G, Vallianatos F, Sammonds P. Non-extensive statistical physics applied to heat flow and the earthquake frequency–magnitude distribution in Greece. Physica A. 2016; 456:135–144. DOI: 10.1016/j.physa.2016.03.022

[55] Gutenberg B, Richter CF. Magnitude and Energy of Earthquakes, Annali di Geofisica, 1956;9:pp. 1–15. DOI: 10.4401/ag-4588

[56] Wald DJ, Jaiswal KS, Marano KD, Bausch D. Earthquake Impact Scale. Natural Hazards Review. 2011;125–139. DOI: 10.1061/(ASCE)NH.1527-6996.0000040