Assessing nuclear power plant safety and recovery from earthquakes using a system-of-systems approach

Elisa Ferrario, Enrico Zio

ASSESSING NUCLEAR POWER PLANT SAFETY AND RECOVERY FROM EARTHQUAKES USING A SYSTEM-OF-SYSTEMS APPROACH

E. Ferrario[a] *and E. Zio*[a,b]

[a]*Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy - Electricité de France, at École Centrale Paris - Supelec, France*

enrico.zio@ecp.fr, enrico.zio@supelec.fr

[b]*Department of Energy, Politecnico di Milano, Italy*

enrico.zio@polimi.it

Abstract

We adopt a 'system-of-systems' framework of analysis, previously presented by the authors, to include the interdependent infrastructures which support a critical plant in the study of its safety with respect to the occurrence of an earthquake. We extend the framework to consider the recovery of the system of systems in which the plant is embedded. As a test system, we consider the impacts produced on a nuclear power plant (the critical plant) embedded in the connected power and water distribution, and transportation networks which support its operation. The Seismic Probabilistic Risk Assessment of such system of systems is carried out by Hierarchical modeling and Monte Carlo simulation. First, we perform a top-down analysis through a hierarchical model to identify the elements that at each level have most influence in restoring safety, adopting the criticality importance measure as a quantitative indicator. Then, we evaluate by Monte Carlo simulation the probability that the nuclear power plant enters in an unsafe state and the time needed to recover its safety. The results obtained allow the identification of those elements most critical for the safety and recovery of the nuclear power plant; this is relevant for determining improvements of their structural/functional responses and supporting the decision-making process on safety critical-issues. On the test system considered, under the given assumptions, the components of the external and internal water systems (i.e., pumps and pool) turn out to be the most critical for the safety and recovery of the plant.

Keywords: System of systems, Recovery, Seismic Probabilistic Risk Assessment, Hierarchical representation, Monte Carlo simulation.

1. INTRODUCTION

We consider a safety-critical plant, e.g., a nuclear power plant (NPP), exposed to an external hazard, e.g., an earthquake. Internal emergency devices have been designed to provide safety for the plant upon occurrence of the hazardous event, i.e., even if the infrastructure services are not available. However, the history of industrial accidents, including the recent Fukushima nuclear disaster [1], has shown us that the safety of a plant depends also on the infrastructures in which it is embedded, which may or may not provide "resilience" properties. Then, the analysis for the evaluation of the probability that a critical plant remains or not in a safe state, i.e., in a condition that does not cause health and/or environmental damages, upon occurrence of an external accident event, must extend to the interdependent infrastructures connected to it, adopting a "system-of-systems" point of view [2], [3], [4], [5], [6], [7], [8]. For this, we adopt the framework of analysis proposed by the authors in [9] and extend it to include the capacity of the system of recovering from an external aggression or shock, using as representative quantity the recovery time, i.e., the period necessary to restore a desired level of functionality of a system after the shock [10].

As a test system for the developments of our considerations and analyses, we consider the impacts of an earthquake on a nuclear power plant, extending the system boundaries to the power and water distribution, and the transportation networks (the interdependent infrastructure systems) that can provide services necessary for keeping or restoring its safety. The test system is fictitious and highly simplified, intended only to illustrate the way of analyzing the problem under a "system-of-systems" viewpoint, accounting for the effects of the interdependencies.

The systemic analysis is performed in two main steps. In the first step, a conceptual map previously built by the authors [9] to understand all the dependencies and interdependencies between the components of the infrastructure systems connected to the nuclear power plant is exploited to construct a hierarchical representation of the system of systems. Hierarchical modeling is here used for a top-down analysis of the elements that at each level have most influence in restoring safety. Indeed, the hierarchical representation facilitates the identification of the structure of the system of systems, allowing the determination of the

critical elements [11]. As a quantitative indicator of the contribution of the components to the recovery of safety, the criticality importance measure is used [12], [13].

In the second step, Monte Carlo simulation [14], [15], [16] is applied to compute 1) the probability that the nuclear power plant enters in an unsafe state and 2) the time of recovery of the safety of the nuclear power plant, accounting for the contributions of both the internal emergency devices and the connected infrastructures.

The reminder of the paper is organized as follows. In Section 2, the basic concepts of a Seismic Probabilistic Risk Assessment are introduced; in Section 3, the hierarchical modeling of a system of systems and Monte Carlo simulation framework for Seismic Probabilistic Risk Assessment are described; in Section 4, the test system and the results of the analysis are presented; in Section 5, conclusions are provided.

2. METHOD FOR SEISMIC PROBABILISTIC RISK ASSESSMENT

To estimate the probabilities of occurrence of different levels of earthquake ground motion that may affect an infrastructure and its response to such event, a Seismic Probabilistic Risk Assessment (SPRA) is typically applied. In a very short and schematic synthesis, it is based on three parts [17], [18]:

- Seismic Hazard Analysis: computes the probabilities of occurrence of different levels of earthquake ground motion at a site of interest.
- Seismic Fragility Evaluation: identifies the seismic capacity of a component in terms of its conditional probability of failure for any given ground motion level.
- System Analysis: integrates the outputs of the hazard and fragility analyses to evaluate the impact of an external event to the infrastructure of interest.

The first part is traditionally developed as a Probabilistic Seismic Hazard Analysis (PSHA) consisting of four procedural steps [17], [18], [19]:

1) Earthquake source zones identification and characterization
2) Earthquake recurrence relationship definition
3) Ground motion attenuation relationship formulation
4) Exceedance probability calculation

The first step concerns the identification and characterization of the seismic sources in the proximity of the site of interest. It involves geological, seismological, geophysical data and scientific interpretations; as a consequence it is a critical part of the analysis and it is

associated with considerable uncertainty [17], [18]. The major outputs of this step are the seismic map that defines the seismic zones (areas where the earthquake sources have common characteristics like geometry, earthquake activity, earthquake annual recurrence rate), the probability distribution of the source-to-site distance and the identification of the maximum earthquake magnitude, i.e., the largest magnitude that a source can generate [17], [18].

In the second step, the seismic earthquake recurrence relationship, i.e., the annual frequency of occurrence of a given magnitude event for each source, is defined. Typically, it is described by the Gutenberg-Richter law, $\log(n) = a - bm$ where n is the number of earthquakes with magnitude[1] greater than m and a and b are parameters obtained by regression data analysis [17], [18]. This relation implies that the magnitude is exponentially distributed [22], [23]:

$$F_M(m) = 1 - e^{-\beta m} \quad (1)$$

where $\beta = log_{10}b \cong 2{,}303b$ represents the relative frequency of smaller to larger events. Equation 1, however, is an unbounded probability distribution so that the magnitude can assume very high values, which are unrealistic and very low values, which are negligible. Therefore, the distribution is double-truncated by upper and lower bounds, m_{max} and m_{min}, respectively, and it is reformulated as follows [17]:

$$F_M(m) = \frac{1-e^{-\beta(m-m_{min})}}{1-e^{-\beta(m_{max}-m_{min})}} \quad (2)$$

The third step identifies the ground motion value at the site of interest, given the source-to-site distance and the magnitude. The higher the distance from the source, the lower is the ground motion value. Typical ground motion parameters are the peak ground acceleration and the spectral acceleration. Many ground motion equations have been defined on the basis of the earthquake and site characteristics [24]. They usually assume this expression [17]:

$$logz' = C_1 + C_2 m + C_3 m C_4 + C_5 \log[r + C_6 \exp(C_7 m)] + C_8 r + g(source) + g(site) \quad (3)$$

where *z'* is the mean ground motion parameter, C_i, i=1,…,8, are the regression coefficients, r is the source-to-site distance, m is the magnitude and *g(source)* and *g(site)* are terms that reflect the characteristics of the source and site, respectively.

For example, the peak ground acceleration is well described by [25]:

$$log_{10}z' = C_1 + C_2 m + (C_3 + C_4 m) * log_{10}\sqrt{r^2 + C_5^2} + C_6 S_s + C_7 S_A + C_8 F_N + C_9 F_T + C_{10} F_O \quad (4)$$

where S_S and S_A represent the types of soil (soft, stiff or rock, when both variables are set to zero) and F_N, F_T and F_O describe the faulting mechanism (normal, thrust or odd).

[1] The magnitude scale typically used is the moment magnitude defined by [20]. For medium size earthquakes it is similar to the Richter values [21].

In the fourth step, the probability of exceedance of ground motion in any time interval is computed by an analytical integration for each magnitude, distance and ground motion value by the following equation [17]:

$$\nu(z) = \sum_{i=1}^{S} \lambda_i\,(m_{min}) \int_{m_{min}}^{m_{max}} \int_{r_{min}}^{r_{max}} f_{R_i}(r|m) f_{M_i}(m) P(Z > z|m,r)\, dmdr \qquad (5)$$

where $i = 1, \dots, S$ represents the source zone, $f_{R_i}(r|m)$ and $f_{M_i}(m)$ are the probability density functions of the source to site distance and of the magnitude, respectively, $P(Z > z|m,r)$ is the probability of exceedance of the ground motion for each source zone, m_{min}, m_{max}, r_{min}, r_{max} are the lower and upper bounds of the magnitude and distance considered and $\lambda_i(m_{min})$ is a rate that removes the contribution of earthquakes with magnitude lower than m_{min} that is not significant.

In the second part of the SPRA, a fragility evaluation is carried out to provide the parameter values (i.e., the median acceleration capacity A_m and the logarithmic standard deviation due to randomness and to uncertainty in the median capacity β_r and β_u, respectively) of the component fragility model of the kind [17]:

$$f' = \Phi\left[\frac{\log\left(\frac{z'}{A_m}\right) + \beta_u \Phi^{-1}(Q)}{\beta_r}\right] \qquad (6)$$

where *f'* is the conditional probability of failure for any given ground motion level *z'* and *Q* is the subjective probability of not exceeding a fragility *f'*.

In the third part, an evaluation of the consequences of the seismic event to the infrastructure under analysis is traditionally performed by the development of event trees and logic models for each event tree top event [17]. In this work we adopt a hierarchical representation and a Monte Carlo simulation for this evaluation.

3. METHOD FOR SAFETY ASSESSMENT AND RECOVERY ANALYSIS

In this Section, the hierarchical representation of a system of systems (Section 3.1) and the operative steps of the Monte Carlo (MC) simulation method for its Seismic Probabilistic Risk Assessment (SPRA) (Section 3.2) are summarized.

3.1. Hierarchical representation of a system of systems

Let us denote a system i at the level L of the hierarchy as $S_i^{(L)}$ and by $N_S^{(L)}$ the number of systems at the level L. In the hierarchical representation of a system-of-systems view of a critical plant, H, at the top of the hierarchy there is only $N_S^{(1)} = 1$ system, the critical plant itself, and it is denoted as $S_1^{(1)}$. At the second level, $L = 2$, this is connected to $N_S^{(2)}$ systems, $S_i^{(2)}$, $i = 1, \dots, N_S^{(2)}$, inside and outside the plant, that provide it with the necessary inputs for its operation. The systems $S_i^{(2)}$, $i = 1, \dots, N_S^{(2)}$, at level $L = 2$, can, in turn, be broken down into subsystems $S_i^{(3)}$, $i = 1, \dots, N_S^{(3)}$ at the third level of the hierarchy, $L = 3$. The hierarchical modeling is built by identifying the elements (or groups) that are "part of" the parent objects, and continuing up to the desired level $L = N_L$, where N_L is the number of levels of the hierarchy. For the analysis of interest here, the hierarchy is continued down to the level of details of the individual components of the system of systems. However, following this procedure for building the hierarchical model, some components may not be considered. Actually, some elements of the system of systems i) may not provide the critical plant H with the inputs necessary for its operation, thus, they cannot be represented in the level-2 of the hierarchy, and ii) may not be part of any system $S_i^{(2)}$, $i = 1, \dots, N_S^{(2)}$, thus, they cannot be identified by the decomposition criteria. These components (hereafter called "recovery supporting elements") provide the components (or groups) of the systems $S_i^{(2)}$, $i = 1, \dots, N_S^{(2)}$, with the inputs necessary for their functioning or recovery and are here represented as a part of the systems (groups) they support.

By way of example, refer to Figure 1 in which the graph of the system (top), the grouping of its components (middle) and its hierarchical representation (bottom) are depicted. The intra-system dependencies (solid lines), the inter-system ones (dashed lines) and the connections to the critical plant H (bold lines) are identified (Figure 1, top). The increasing resolution in the four levels considered is illustrated (Figure 1, middle): in the first level (square shape), the critical plant H is represented; in the second level (dashed oval shape), the three interdependent systems, $S_i^{(2)}$, $i = 1, \dots, 3$ are reported; in the third and fourth levels (dotted and solid oval shapes, respectively), the grouping of the elements within the systems of level 2 are specified. In Figure 1, top, the recovery supporting elements are those not connected to the critical plant H but linked to other components by dashed lines (i.e., $S_1^{(4)}$ and $S_2^{(4)}$); in

Figure 1, middle, they are grouped in the systems to which they provide support, e.g., $S_1^{(4)}$ is both in the systems $S_1^{(2)}$ and $S_2^{(2)}$ and $S_2^{(4)}$ is in the system $S_3^{(2)}$; in Figure 1, bottom, they are represented in the last levels of the hierarchy according to the grouping of the Figure 1 in the middle. Notice that the recovery supporting elements can belong to more systems (or groups) since they can be a support to different components (or groups), whereas all the others components (or groups) are within just one system since they are built following the criteria "to be a part of". A final remark is in order with respect to the top-down approach adopted to build the hierarchical model. It is possible that, before reaching the bottom of the hierarchy, some components cannot be subdivided further (e.g., $S_2^{(3)}$ coincides with $S_1^{(4)}$) leading to an incomplete hierarchical representation. Therefore, in this circumstance, a copy of those elements is reported in the levels they are absent [26].

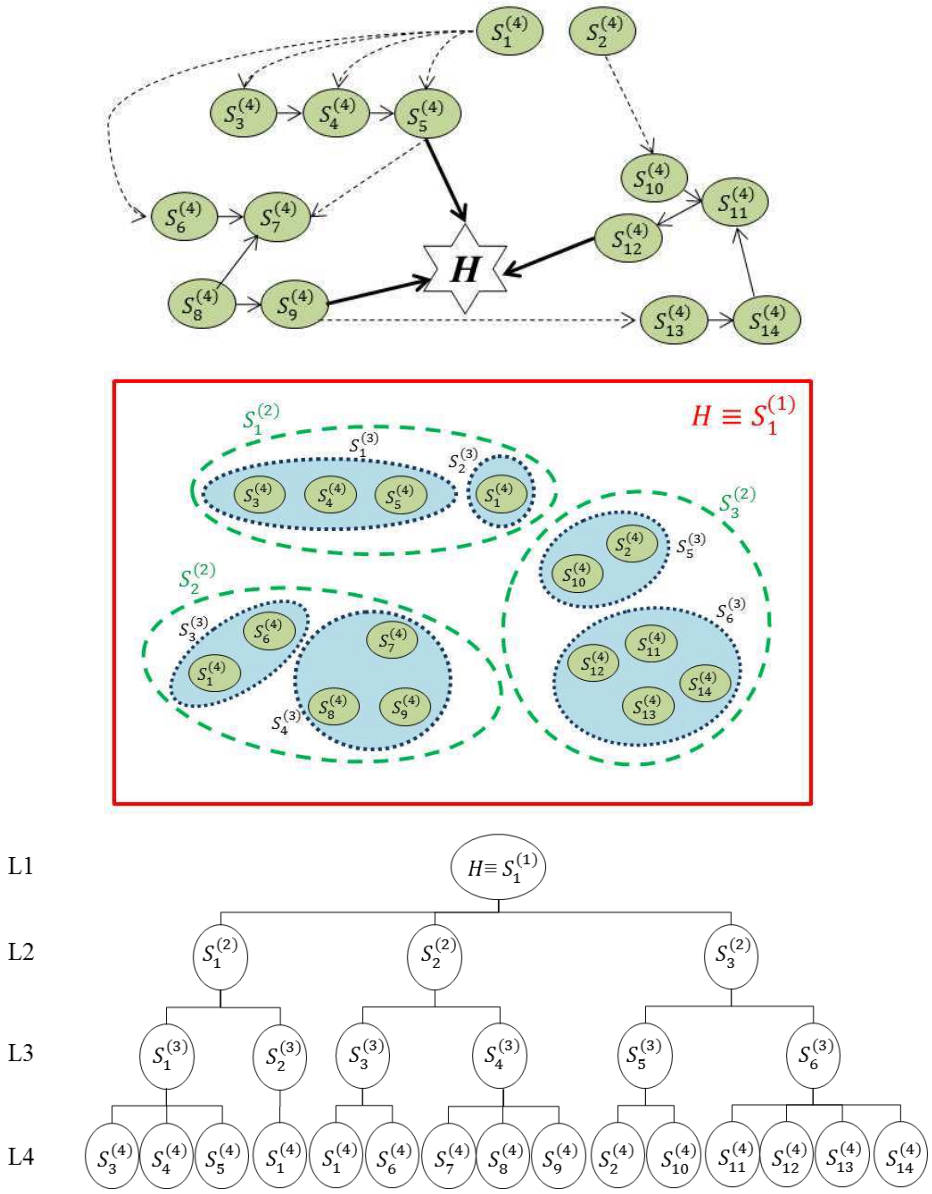


Figure 1: Top: dependencies among the components of the system of systems; the links represent the intra-systems dependencies (solid lines), the inter-systems dependencies (dashed lines) and the dependencies of the critical plant H on its interconnected systems (bold lines). Middle: graphical representation of their grouping; the rectangular, dashed, dotted and solid oval shapes represent the increasing resolution in the hierarchical level. Bottom: corresponding hierarchical representation; L: Level.

A system $S_i^{(L-1)}$, $i = 1, \dots, N_S^{(L-1)}$, at level $L-1$, $L = 2, \dots, N_L$, can be in an operational or in a failure state depending on the states of the systems at the level L, on their functionality and on their logic connections. A state (truth) matrix is associated to each system $S_i^{(L-1)}$, $i = 1, \dots, N_S^{(L-1)}$, $L = 2, \dots, N_L$, where the first columns represent the states of the systems $S_i^{(L)}$, $i = 1, \dots, N_S^{(L)}$, at level L and the last column represent the state of the system $S_i^{(L-1)}$,

$i = 1, \dots, N_S^{(L-1)}$, at level $L-1$. The entries $\{a_{ij}\}$ are equal to 1 or 0 according to whether the states are in a failure state or not.

By way of example, refer to Table 1 and Figure 2 where three state matrices and the corresponding fault trees are reported, with reference to the system $S_5^{(3)}$ at level $L = 3$ of Figure 1 (middle) composed by the systems $S_{10}^{(4)}$ and $S_2^{(4)}$ at level $L = 4$. The first two state matrices represent, respectively, the series and parallel configurations between the systems $S_{10}^{(4)}$ and $S_2^{(4)}$ (illustrated by the OR and the AND gate in the fault trees): in the first case, the state of $S_5^{(3)}$ can assume only one operational state, since the failure of $S_{10}^{(4)}$ or $S_2^{(4)}$ causes its failure; whereas, in the second case, $S_5^{(3)}$ is in a failure state when both $S_{10}^{(4)}$ and $S_2^{(4)}$ fail. The third matrix shows a case in which the state of $S_5^{(3)}$ depends only on the state of $S_{10}^{(4)}$. The fault tree of this last case is represented by an inhibit gate without condition on the system $S_2^{(4)}$.

Table 1: Three possible state matrices for the system $S_5^{(3)}$ of Figure 1 (middle) on the basis of the states of the systems $S_{10}^{(4)}$ and $S_2^{(4)}$. On the left: $S_{10}^{(4)}$ and $S_2^{(4)}$ are connected in series; in the middle: $S_{10}^{(4)}$ and $S_2^{(4)}$ are connected in parallel; on the right: $S_5^{(3)}$ depends only on $S_{10}^{(4)}$; 1 represents the failure state.

$S_{10}^{(4)}$	$S_2^{(4)}$	$S_5^{(3)}$
0	0	0
1	0	1
0	1	1
1	1	1

$S_{10}^{(4)}$	$S_2^{(4)}$	$S_5^{(3)}$
0	0	0
1	0	0
0	1	0
1	1	1

$S_{10}^{(4)}$	$S_2^{(4)}$	$S_5^{(3)}$
0	0	0
1	0	1
0	1	0
1	1	1

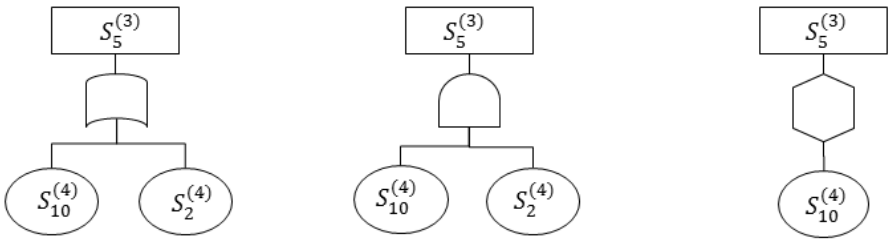


Figure 2: Corresponding fault tree representation of the state matrices reported in Table 1. On the left, $S_{10}^{(4)}$ and $S_2^{(4)}$ are connected in series (OR gate); in the middle, $S_{10}^{(4)}$ and $S_2^{(4)}$ are connected in parallel (AND gate); on the right, $S_5^{(3)}$ depends only on $S_{10}^{(4)}$ (INHIBIT gate without condition).

To define the appropriate state matrix for the systems $S_i^{(L-1)}$, $i = 1, \dots, N_S^{(L-1)}$, $L = 2, \dots, N_L$, a deep understanding of their functionality is necessary. The dependencies identified in Figure 1 (top) are a support for this analysis.

3.2. Monte Carlo simulation for Seismic Probabilistic Risk Assessment within a system-of-systems framework

Within the system-of-systems analysis framework here purported, we wish to evaluate the safety of the critical plant H exposed to the risk from earthquakes occurrence, accounting not only for the direct effects of the earthquake on H but also for the structural and functional responses of the connected systems $S_i^{(2)}$, $i = 1, \dots, N_S^{(2)}$, inside and outside the plant, through the analysis of the underlying dependency structure. In addition, we wish to determine the capacity of recovering of the system of systems, evaluating the period necessary to restore the safety of the critical plant. To do this, we adopt the hierarchical representation of the system of systems and Monte Carlo (MC) simulation for the quantitative SPRA evaluation [27]. The simulation procedure consists of the following operative steps:

1. choose a value of magnitude with respect to which the analysis is performed;
2. compute the ground acceleration value at each of the $S_i^{(L)}$, $i = 1, \dots, N_S^{(L)}$, $L = N_L$, elements of the system of systems, by equation 4; $N_S^{(N_L)}$ is the number of elements at the last level of the hierarchy, i.e., in our case, the number of individual components;
3. compute the fragility, f, for all the components $S_i^{(N_L)}$, $i = 1, \dots, N_S^{(N_L)}$, of the system of systems by equation 6; f is a vector of $N_S^{(N_L)}$ values, one for each individual component in the system;
4. sample a matrix of uniform random numbers in [0,1) $\{u_{j,k}\}$, $j = 1, \dots, N_T$, $k = 1, \dots, N_S^{(N_L)}$, where N_T is the number of simulations;
5. determine the fault state matrix $\{g_{j,k}\}$, $j = 1, \dots, N_T$, $k = 1, \dots, N_S^{(N_L)}$, by comparing the fragility, f, with the matrix $\{u_{j,k}\}$, $j = 1, \dots, N_T$, $k = 1, \dots, N_S^{(N_L)}$: if $u_{j,k} < f_k$, set $g_{j,k} = 1$; otherwise set $g_{j,k} = 0$ for $j = 1, \dots, N_T$ and $k = 1, \dots, N_S^{(N_L)}$. When $g_{j,k}$ assumes value 1, it means that in the *j*-th simulation the *k*-th component is hit by the earthquake, i.e., it enters a faulty state; otherwise, it survives. Each row of the matrix g represents the states of the $N_S^{(N_L)}$ system components in the *j*-th simulation;
6. determine the state of the critical plant H. This is done by propagating bottom-up through the hierarchy the faulty states of the components: the states of the $S_i^{(N_L)}$ components and the state matrix at the level $N_L - 1$ of the hierarchy are used to determine the states of the $S_i^{(N_L-1)}$ systems at the upper hierarchical level, $L = N_L - 1$,

and the evaluation is repeated for the states of the systems of the level $N_L - 2$ and so on until the top level of the hierarchy, $L = 1$.

In doing so, the state of H is evaluated for each row of the matrix $\{g_{j,k}\}$, i.e., for each configuration of the system sampled. A vector $\{h_j\}$ is then recorded, whose element h_j, $j = 1, \dots, N_T$, assumes value 1 when the critical plant H is in an unsafe state and 0 otherwise;

7. estimate the probability of the critical plant H of being unsafe by computing the sample average of the values of the elements of the N_T −dimensional vector $\{h_j\}$, $j = 1, \dots, N_T$.
8. for each configuration of the system sampled that turns the critical plant H in an unsafe state, evaluate the recovery time (RT) by the following steps:
    a. sample a matrix $\{R\_T_{r,k}\}$, $r = 1, \dots, N_{R\_T}$, $k = 1, \dots, N_S^{(N_L)}$, where N_{R_T} is the number of recovery time simulations of the $S_i^{(N_L)}$, $i = 1, \dots, N_S^{(N_L)}$, elements of the system of systems that are in a faulty state; for each element the sampling is done from the respective recovery time distribution;
    b. determine the recovery time of the critical plant H, computing the recovery times at each hierarchical level accounting for the configurations of the systems $S_i^{(L)}$, $i = 1, \dots, N_S^{(L)}$, $L = N_L, \dots, 1$, from bottom to top of the hierarchy. For example, if the systems at level L, are connected in series to the system at level $L - 1$, the recovery time of the latter is the maximum recovery time of the systems or components at the lower level L (Figure 3, left); if they are connected in parallel, the recovery time is the minimum (Figure 3, middle). In the other cases, specific evaluation should be performed. For example, if the failure of a given system $S_i^{(L)}$, $i = 1, \dots, N_S^{(L)}$, does not affect the state of another system $S_j^{(L)}$, $j = 1, \dots, N_S^{(L)}$, $j \neq i$, but plays a role in the operations of its recovery from failure it should be considered in the analysis like an increasing time for operations of recovery of the system at level $L - 1$ (Figure 3, right).

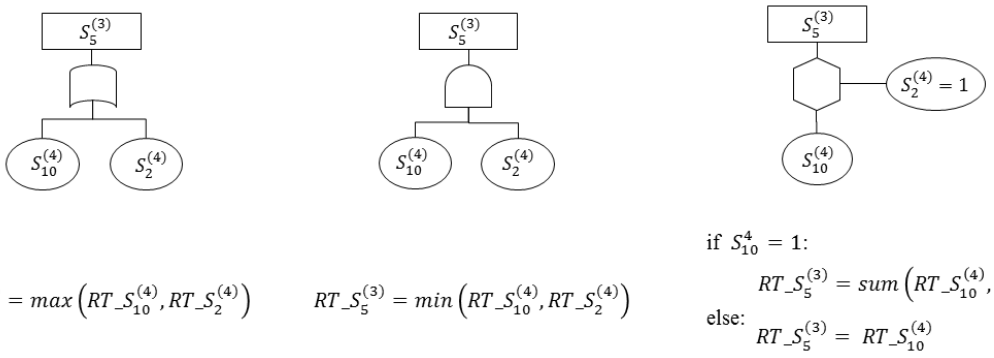


Figure 3: Computation of recovery time (RT) of the system $S_5^{(3)}$ with reference to three different configurations of the systems $S_{10}^{(4)}$ and $S_2^{(4)}$ represented in the fault tree. On the left: OR gate, the recovery time of $S_5^{(3)}$ is the maximum recovery time of $S_{10}^{(4)}$ and $S_2^{(4)}$. In the middle: AND gate, the recovery time of $S_5^{(3)}$ is the minimum recovery time of $S_{10}^{(4)}$ and $S_2^{(4)}$. On the right, INHIBIT gate: the recovery time of $S_5^{(3)}$ is the recovery time of $S_{10}^{(4)}$ but if the condition $S_2^{(4)} = 1$ is verified, the recovery time is the sum between the recovery times of $S_{10}^{(4)}$ and $S_2^{(4)}$. 1 represents the failure state.

Notice that it is assumed that infinite resources (e.g., repair teams and material) are available for the restoration process so that the recovery can be performed at the same time on all components in need. This assumption is made considering that in emergency situations all the possible means, resources and actions are deployed to keep or restore the critical plant safety. In any case, extension to the situation of limited resources does not pose significant difficulties in both the modelling and its quantification. Finally, the components are considered with binary states: fully operative or completely damaged and also the critical plant can assume only two states: fully operative or totally failed. This approximation is not realistic and leads to pessimistic results: multi-state modeling may be considered for a more realistic description, where different degrees of damage are contemplated.

4. EXEMPLIFICATION OF THE PROPOSED METHOD ON A TEST SYSTEM

We consider the mock-up problem of [9] concerning the safety of a nuclear power plant (the critical plant), provided with proper internal emergency devices, in response to an earthquake (the external hazardous event) in a system-of-systems framework, i.e., extending the boundaries of the analysis to the responses of the interconnected systems that could help keeping or restoring the plant safe state. The nuclear power plant is considered in a safe condition if it does not cause health and environmental damages, i.e., if it does not release radioactive material to the environment; to maintain this state it must be provided with electrical and water inputs to absorb the heat that it generates. We analyze the capacity of

recovering of the system of systems, in terms of the period necessary to restore the safe state of the plant.

When an earthquake occurs, the critical plant may not receive the input necessary to be kept in, or restored to, a safe state due to the direct impact on its emergency devices (safety systems) and to the damages to the interconnected infrastructures. Two quantities are used to characterize the loss of functionality of the various components of the system of systems embedding the critical plant, upon the occurrence of a damaging external event:

- from the safety viewpoint, the probability that the critical plant remains in safe state;
- from the recovery viewpoint, the time needed to restore the safe state of the critical plant.

Both quantities are here computed for two values of earthquake magnitude, 5.5 and 6, on the Richter scale.

In Section 4.1, the description of the system studied is given under a number of assumptions which simplify the problem to the level needed to convey the key aspects of the conceptual system-of-systems framework, while maintaining generality. In Section 4.2, the hierarchical representation of the system and some considerations about its capacity of recovering are given. In Section 4.3, we provide the results of the evaluation of the two quantities of interest above mentioned.

4.1. Description of the system

The system under analysis is composed by a critical plant, i.e., a nuclear power plant, a water system that provides coolant useful to absorb the heat generated in the nuclear power plant, a power system that provides electrical energy for the running of the nuclear power plant and the water system, and a road network relevant to the power and water systems for the transport of material and/or plant operators.

The water and power systems are subdivided into two independent parts, external and internal to the plant; the latter one represents the emergency system of the plant which needs to obviate at the absence of input from the main external system.

In Figure 4, the physical representation of the system is reported referring to a spatial plane (x, y) with origin in the river. Table 2 reports the fragility parameters A_m, β_r and β_u, adopted in this analysis, for illustration purposes. The values for the pump and the pipe components have been taken from [28] and [29], respectively, whereas the others fragility parameters have been assumed arbitrarily by the authors to perform the study with different values. Given the large-

scale system under analysis, two types of soil are considered, rock and soft. Figure 5 represents the spatial localization of the system shown in Figure 4 with reference to the reciprocal position of all the components (Figure 5, left) and to the position of the system with respect to the considered earthquake epicenter $A(70, 70)$ (Figure 5, right). The distances on the axes are expressed in kilometers.

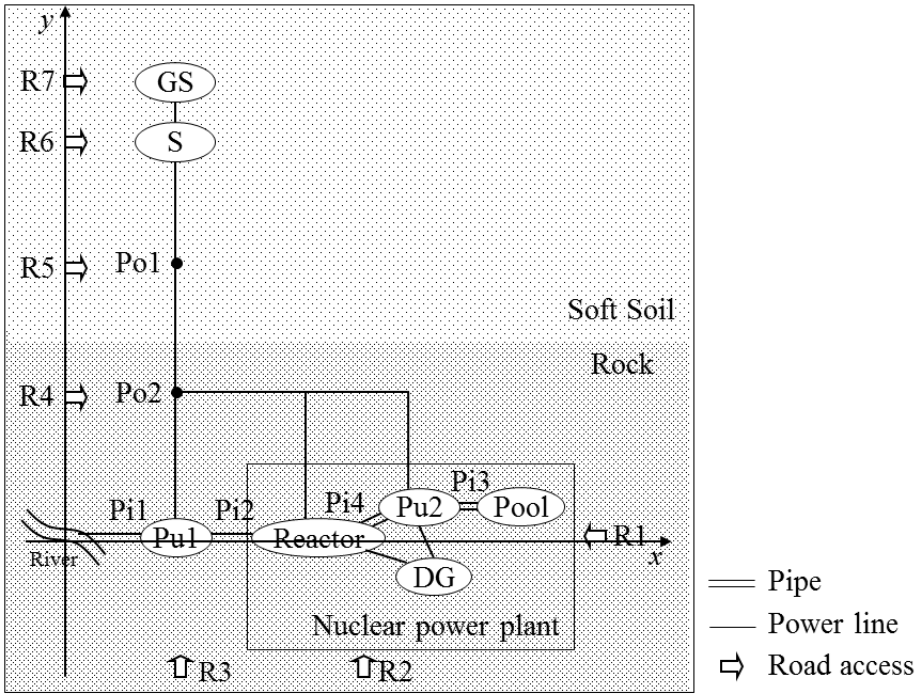


Figure 4: Physical representation of the system of systems. GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, DG: Diesel Generator, R: Road access.

Table 2: Fragility parameters used in the present work.

	A_m	β_r	β_u
Generation station	0.7	0.3	0.1
Substation	0.9	0.4	0.3
Power Pole	0.8	0.2	0.2
Diesel Generator	0.7	0.4	0.2
Pipe	1.88	0.43	0.48
Pump	0.2	0.2	0.3
Pool	0.2	0.1	0.1
Road	0.3	0.3	0.2

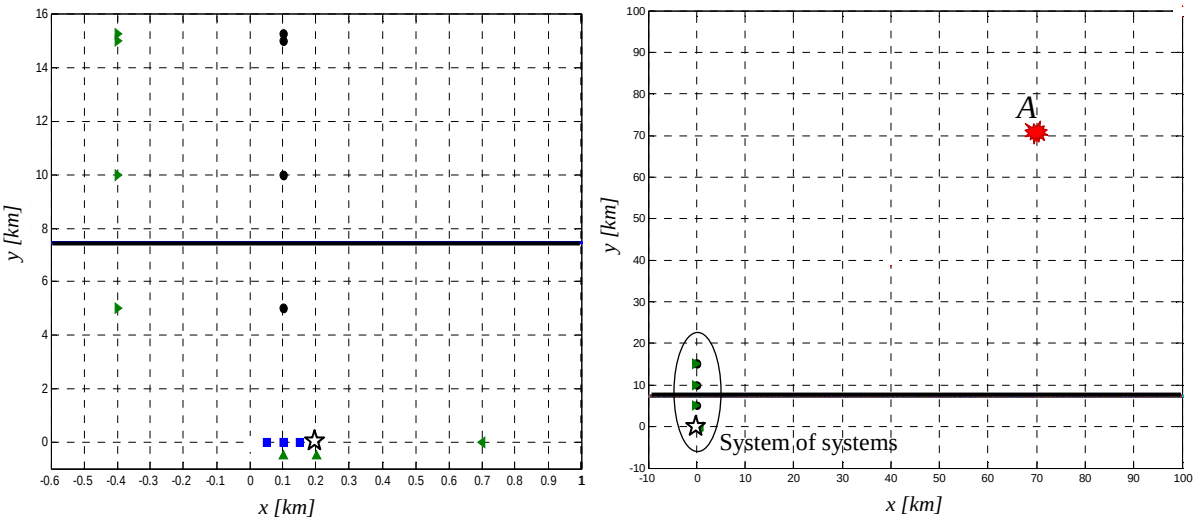


Figure 5: Left: spatial localization of the nuclear power plant (star) with respect to the components of the electric power system (circle, from top to bottom: Generation Station, Substation, Pole 1, Pole 2), water system (square, from left to right: Pipe 1, Pump 1, Pipe 2) and road transportation (triangle, from top to bottom and from left to right: R7, R6, R5, R4, R3, R2, R1). Right: spatial localization of the system of systems with respect to the earthquake's epicenter A(70, 70). The horizontal bold line in both Figures represents the division between soft soil (above the line) and rock (below the line).

In Figure 6, the system-of-systems representation is given by a conceptual map showing the components of the systems and their relationships, intra- and inter-systems. The intra-system dependencies are represented by the solid lines, the inter-system ones by dashed lines and those with the critical system by the bold lines. In addition, in the Figure the dependence of the system of systems on the type of soil on which the infrastructures rest is illustrated.

The external water distribution system (Figure 6, left) is formed by a pump and pipes that carry the water. The external power distribution system (Figure 6, center) is composed by the following elements: a generation station that produces the electrical energy, a substation that transforms the voltage from high to low, and poles that support power lines.

The components of the emergency water and power distribution systems inside the plant are shown in Figure 6 on the right. The first system is composed by the same elements of the corresponding external system considering in addition an artificial reservoir (i.e., the source of water), whereas the power system includes only the emergency diesel generators.

The elements considered for the transportation system are the roads (Figure 6, top). The state of this system is important for access of the materials and operators that are needed to restore the components required for the safe state of the critical plant. Given their role, they are considered as recovery supporting elements (see Section 3.1).

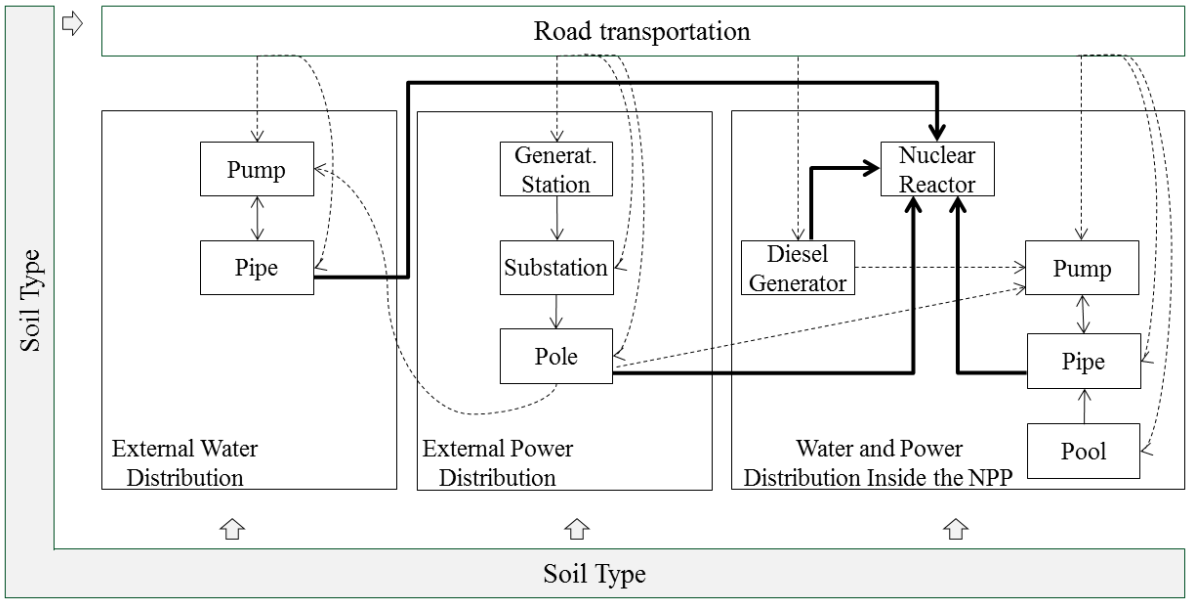


Figure 6: System of systems: conceptual map; the links represent the intra-systems dependencies (solid lines), the inter-systems dependencies (dashed lines) and the dependencies of the nuclear power plant on its interconnected systems (bold lines).

The inter-system dependencies are modeled as links connecting components of the power, water and road transportation systems (Figure 6, dashed lines); these links are conceptually similar to those linking components of the individual systems (intra-systems dependencies), and are considered bidirectional with respect to the "flow" of dependence between the connected systems. For example, the external water system depends on the external power system as the pump needs electrical energy to work. Notice that this relation is expressed by a link from the pole to the pump because the first one, supporting the power lines, is the closest element to the pump that carries the power (the same reason explains the connection of the pole to the nuclear reactor and to the pump inside the nuclear power plant). While the pump of the external water system can receive electrical energy only from the external power distribution network, it is assumed that the pump inside the nuclear power plant can obtain it from both the external and internal power systems.

The road transport network allows access to the components of the power and water systems for transporting material (e.g., fuel) and/or operators for operation and/or recovery.

The transport system is composed by seven interdependent road access points to the components of the power and water systems. They are distributed as follows: one road access is available for the components outside the nuclear power plant and two road accesses for those inside, i.e., the components outside the nuclear power plant can only be reached by one road access, whereas the ones inside by two road accesses (the same two accesses are provided for all the components inside) (Figure 4). In particular, the components of the

external power system are considered to have a different road access because they are far from each other (the minimum distance is 300 m between the generation station and the substation, Figure 5 left), the components of the external water system have the same road access, R3, because they are located close to each other (the total distance from the river to the nuclear power plant is 200 m, Figure 5 left) and the components of the power and water systems inside the nuclear power plant have the same two road accesses, R1 and R2, since they are contained in the same building.

Among these road access points, only the one connected to the generation station, R7 in Figure 4, has an impact on the state of the system of systems because it contributes to the running of the generation station, carrying materials and operators. On the contrary, the other road accesses have no direct impact on the state of the system of systems since they are used only to repair the elements that enter in a faulty state. Therefore, their contribution is not of interest for the evaluation of the safety of the critical plant, but they are relevant for the analysis of the capacity of recovering of the system of systems.

In this work we have not considered i) the power lines that, being aerial elements, are not directly affected by an earthquake and ii) the river, i.e., the source of water of the external water system, that it is assumed to be always available. Other aspects could be introduced in the analysis as i) the influence of the design, construction and materials of the infrastructures considered, ii) the supply of fuel and materials for plant operation, and iii) the maintenance tasks. However, in view of the methodological character of this work, for the sake of simplicity, we have not included them in the modelling.

4.2. Hierarchical representation of the system of systems and its capacity of recovering

From the conceptual map shown in Figure 6, the connections between the physical elements of the system of systems are presented in Figure 7. The solid, dashed and bold lines represent the intra-system dependencies, the inter-systems dependencies and the links to the nuclear power plant (NPP), respectively. The clusters taken into account in the analysis are identified in Figure 8, and they are structured hierarchically in Figure 9.

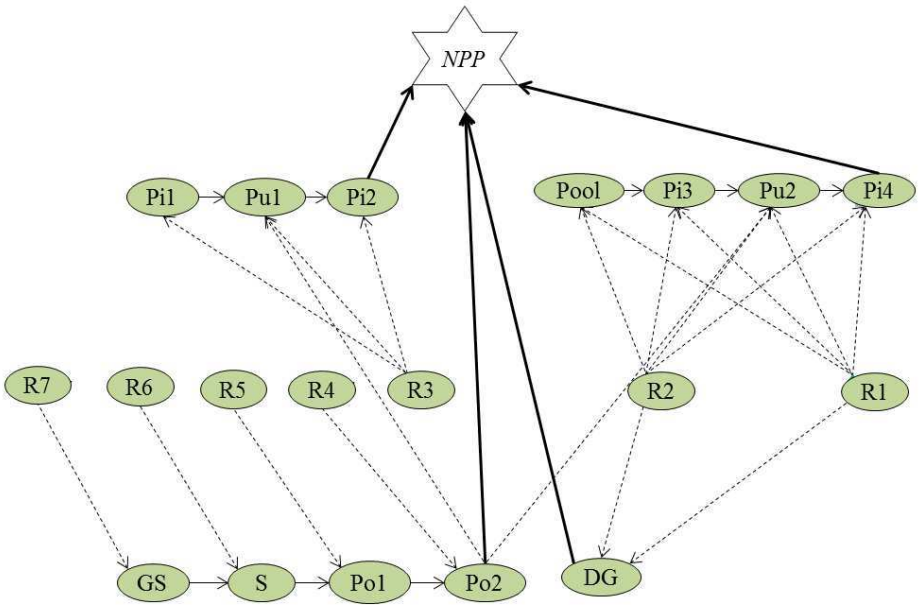


Figure 7: Dependencies among the components of the system of systems; the links represent the intra-systems dependencies (solid lines), the inter-systems dependencies (dashed lines) and the dependencies of the nuclear power plant (NPP) on its interconnected systems (bold lines). GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, DG: Diesel Generator, R: Road access.

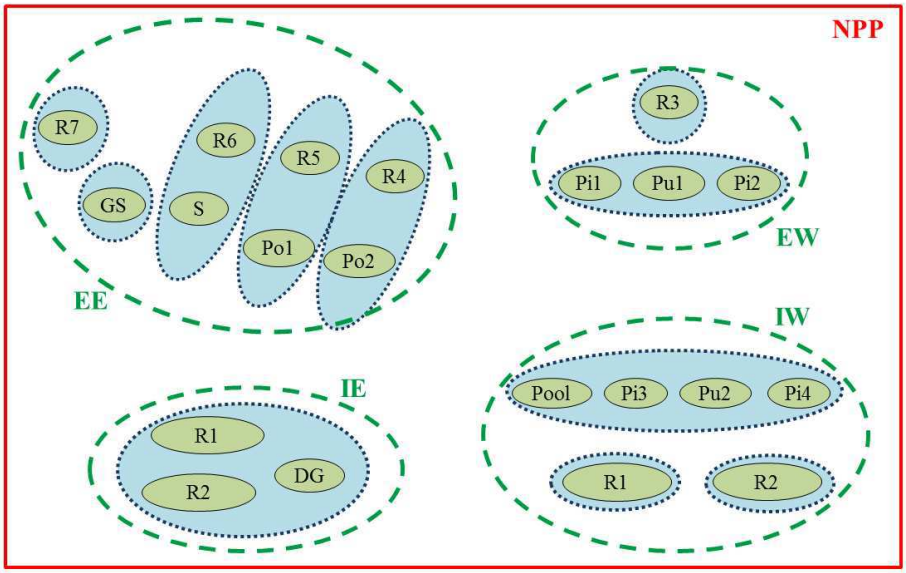


Figure 8: Representation of the system of systems highlighting its underlying structure of four hierarchical levels represented by the rectangular (level 1), the dashed (level 2), the dotted (level 3) and the solid (level 4) oval shapes. NPP: Nuclear Power Plant, EE: External Energy, EW: External Water, IE: Internal Energy, IW: Internal Water, GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, DG: Diesel Generator, R: Road access.

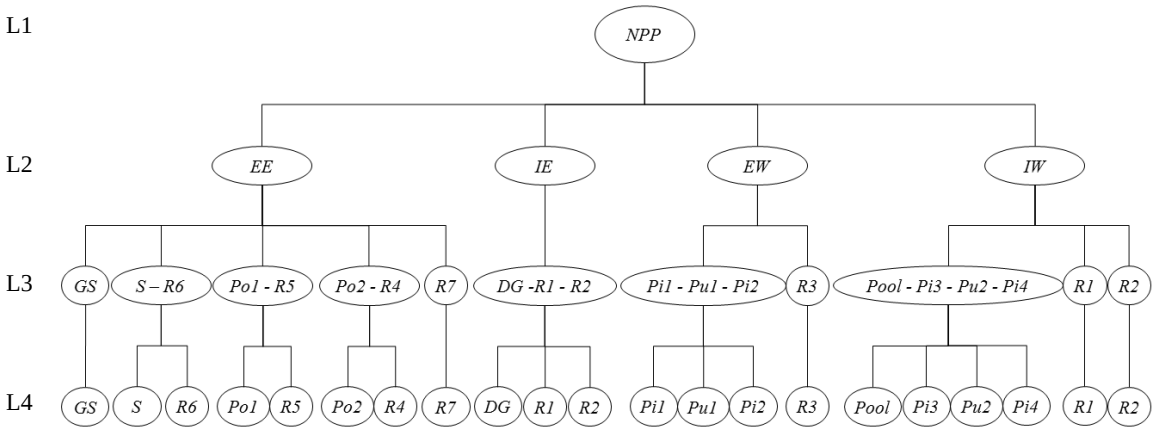


Figure 9: Hierarchical representation of the system of systems. NPP: Nuclear Power Plant, EE: External Energy system, EW: External Water system, IE: Internal Energy system, IW: Internal Water system, GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, DG: Diesel Generator, R: Road access, L: Level.

The nuclear power plant is at the top (level 1) of the hierarchy. Its safety is supported by the power and water systems that are partitioned, at the level 2, into external and internal parts: external energy (EE), internal energy (IE), external water (EW) and internal water (IW). The road accesses are the recovery supporting elements and, as explained in Section 3.1, they belong to the systems to which they provide support, i.e., in this test system they belong to the corresponding EE, IE, EW and IW systems. The level 3 is, then, composed by single individual components or road accesses or a combination of them, and the level 4, the most specified level, is formed by the individual elements (components and road accesses) of the system of systems. Notice that only the recovery supporting elements can belong to different systems (or groups), e.g., R1 and R2 are within both the IE and IW systems, whereas the other components appear in just one system, e.g., the pole Po2 belongs to the EE system.

The roads (elements R1, R2, R3, R4, R5, R6) are used only for the recovery task and, thus, do not influence the state of other parts of the system of systems, i.e., their failures do not cause the stop of the running of other components. On the contrary, they play a role for system recovery because if they are damaged they have to be recovered to allow reaching the system components that are failed for repairing them, and eventually restoring the safety of the critical plant. In other words, if a component fails, the road access to it has to be available for its recovery. For this reason, the components of the level 3 of the hierarchy are grouped together with the corresponding road, e.g., the substation (S) is grouped with the road R6, the diesel generator (DG) is grouped with the two roads R1 and R2, etc. Instead, when a road is connected with more than one component, the first grouping is among the components and, then, at the next higher level, the components are grouped with the road, e.g., the components

of the external water systems (pipes and pump) are grouped together at level 3 and then they are grouped with the road R3 at level 2. This grouping at level 3 allows highlighting the contribution of a road with respect to all the components (one or more) to which it provides access.

The road R7, plays a role in the external energy subsystem which goes beyond the access for recovery, as it provides the generation station with the access for the operators and materials necessary to its functioning. Therefore, the damage to this access road can cause the stop of the generation station and, as a consequence, the failure of the external energy subsystem. For this reason, it is not grouped with the generation station at the third hierarchical level.

The capacity of recovering of the system of systems is quantified in terms of the time needed to recover the safe state of the critical plant. To compute this, the evolution in time of the system of systems is included in the SPRA framework. For the sake of simplicity, damages from aftershocks are not considered in the time-dependent analysis.

As illustrated in the procedure of Section 3.2, the recovery time of the nuclear power plant is computed starting from the recovery time of the individual components at the bottom level of the hierarchy which is climbed from bottom to top through the configurations of the components or systems at each level.

To account for the uncertainty in the duration of the recovery, lognormal distributions have been associated to the recovery time of the individual components. Table 3 shows the means and the variances used in this study; these values have been taken on the basis of the following consideration. The time to recover a component depends on its size, its location, and the type of damage and the easiness to find the failure. It is assumed that, the components inside the nuclear power plant need more time for the recovery than the components outside. In particular, this happens when it is necessary to replace part of the component or the entire component given its huge dimensions and the difficulty to operate inside the plant.

For this reason, we have assumed that the mean of the time needed to recover the pump inside the nuclear power plant is larger than that needed for the pump outside. The large mean value of the time to recover the pool is due to its size, location inside the plant and difficulty in restoration. The time to repair a pipe could be very short (even few hours), but we have assumed a mean value equal to 4 days to account for the difficulty in locating the break. The diesel generator has a time of repair with a high uncertainty (variance equal to 5), because it may vary significantly depending on the type of damage. The components with lowest mean value of the recovery time are the power pole, the road, the generation station and the

substation that are outside the plant; the latter are affected by large uncertainty (variances of 5 and 10, respectively), because their recovery depends on the intensity of the damage, e.g., a generation station can be slightly perturbed by the earthquake and its repairing can last few hours but it can also be destroyed and in this case the time to build it again is obviously much higher.

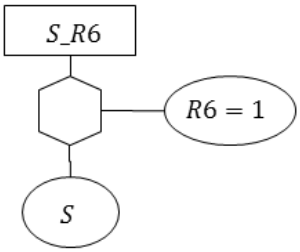
Table 3: Parameters of the lognormal distributions that describe the recovery time of the single components of the system of systems.

Components	**Mean [days]**	**Variance**
Pump (inside the plant)	75	3
Pump (outside the plant)	5	3
Pipe	4	3
Pool	75	3
Diesel Generator	30	5
Power pole	1.5	3
Generation Station	1	10
Substation	1	5
Road	2	3

By way of example, the explanation of the procedure for the evaluation of the time to recover power at the hierarchical level 3 and 2 for the test system under analysis is illustrated in the following, with reference to the Figures 10 – 11.

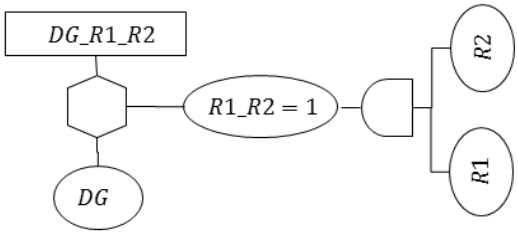
At level 3 of the hierarchy, there are five groups for the external energy (EE) system and one for the internal energy (IE) system. For the individual components of the EE system, i.e., generation station and road R7, the recovery times are described by lognormal distributions whose parameters are reported in Table 3, whereas for the groups made by the pairs of components and road access, e.g., substation and road R6 (S_R6), the recovery time is computed on the basis of the relations among them represented by the fault tree in Figure 10. For the group of the IE system, the fault tree of the recovery time of the triplet “DG_R1_R2” is reported in Figure 11.

As reported in the procedure of Section 3.2, given the assumption of unlimited resources for restoration, the recovery starts at the same time (i.e., immediately after the earthquake) on all the components in need. Actually, one exception is made for those components whose access is disrupted; in this case, the recovery is sequential: first, the access to them is restored and, then, components recovery starts.



$$\text{if } R6 = 1:$$
$$RT\_S\_R6 = sum(RT\_S, RT\_R6)$$
$$\text{else:}$$
$$RT\_S\_R6 = RT\_S$$

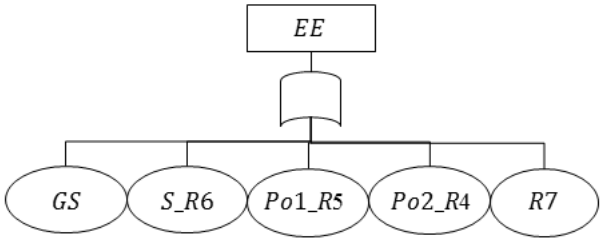
Figure 10: Fault tree representation for the computation of the recovery time (RT) of the pair "S_R6" at level 3 of the hierarchy; S: Substation, R: Road access. 1 represents the failure state.



$$\text{if } R1\_R2 = 1:$$
$$RT\_DG\_R1\_R2 = sum(RT\_DG, min(RT\_R1, RT\_R2))$$
$$\text{else:}$$
$$RT\_DG\_R1\_R2 = RT\_DG$$

Figure 11: Fault tree representation for the computation of the recovery time (RT) of the triplet "DG_R1_R2" at level 3 of the hierarchy; DG: Diesel Generator, R: Road access. 1 represents the failure state.

At level 2, the recovery time of the EE system is the maximum recovery time of the elements of level 3, since they are connected in series (Figure 12). The recovery time of the IE system is that of the triplet "DG – R1 – R2" computed at level 3.



$$RT\_EE = max(RT\_GS,\ RT\_S\_R6,\ RT\_Po1\_R5,\ RT\_Po2\_R4,\ RT\_R7)$$

Figure 12: Fault tree representation for the computation of the recovery time (RT) of the external energy system (EE) at level 2 of the hierarchy; GS: Generation Station, S: Substation, Po: Pole, R: Road access.

Analogous reasoning is used to define the recovery time for the water system at level 3 and 2.

To compute the recovery time at level 1, the logic relations (LR) between the external and internal energy and water systems at level 2 are given in Figure 13 and the corresponding state matrix of the nuclear power plant is reported in Table 4.

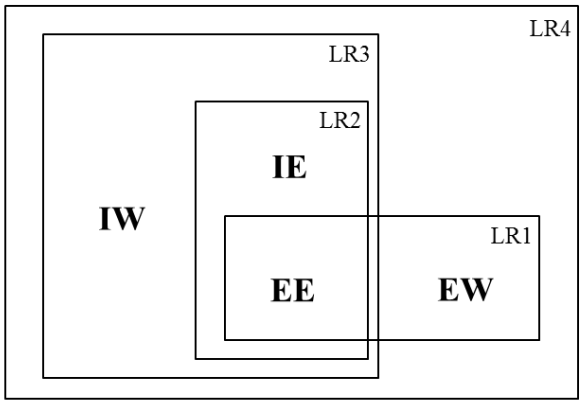


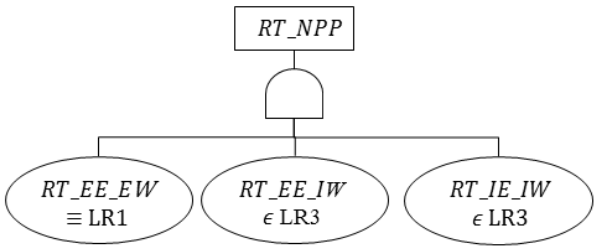
Figure 13: Schematic representation of the relations (LR) that exist between the external energy (EE) internal energy (IE), external water (EW) and internal water (IW) systems at the level 2 of the hierarchy.

Table 4: State matrix of the nuclear power plant (NPP) (level 1) on the basis of the states of the external energy (EE) internal energy (IE), external water (EW) and internal water (IW) systems (level 2); 1 represents the failure state.

EE	IE	EW	IW	NPP
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1
1	0	1	1	1
1	0	1	0	0
1	0	0	1	1
1	0	0	0	0
0	1	1	1	1
0	1	1	0	0
0	1	0	1	0
0	1	0	0	0
0	0	1	1	1
0	0	1	0	0
0	0	0	1	0
0	0	0	0	0

The EE and EW systems are grouped together in the relation LR1 because the EW system needs the EE system to work. The relation LR2 considers the IE and EE systems with respect to the relation LR3, since the IW system can receive electrical inputs both from the IE and EE systems and at least one of these two systems must work. The relation LR4 includes all the relations LR1, LR2 and LR3 and represents the nuclear power plant.

The recovery time of the nuclear power plant (Figure 14) is obtained by the minimum of the recovery time of the systems involved in the relations LR1 and LR3, since its safety is guaranteed when it is provided with both energy and water inputs. Therefore it is computed by the minimum recovery time of the pairs “EE – EW”, “EE – IW” and “IE – IW”.



$$RT\_NPP = min(RT\_EE\_EW,\ RT\_EE\_IW,\ RT\_IE\_IW)$$

Figure 14: Sketch of the computation of the recovery time (RT) of the nuclear power plant (NPP) at level 1 of the hierarchy on the basis of the recovery time of the external energy (EE) internal energy (IE), external water (EW) and internal water (IW) systems, grouped according the relations LR1 and LR3 identified in Figure 13.

For the sake of simplicity, the assumption has been made that the internal emergency devices will not stop functioning once successfully started. In fact, the diesel generator can be refueled in operation without causing an interruption of the production of the electrical energy and the pool of the internal water system has been assumed of infinite capacity.

4.3. Results

The Monte Carlo simulation for Seismic Probabilistic Risk Assessment illustrated in Section 3.2 has been applied to the test system of Section 4.1 for two values of earthquake magnitudes, M= 5.5 and M = 6 on the Richter scale at the epicenter of coordinates (x, y) = (70, 70) (Figure 4). The number of simulations (N_T) of the components configurations for each magnitude value is 2000 and the number of recovery time simulations (N_{R_T}) for each configuration that turns the nuclear power plant (NPP) in an unsafe state is 5000. These numbers have been arbitrarily chosen by the authors in such a way to reach a good trade-off between precision of the results and computational cost.

Figure 15 shows the estimated probabilities (under all assumptions made) that the nuclear power plant reaches an unsafe state upon the occurrence of an earthquake of magnitude equal to 5.5 (left) and 6 (right) on the Richter scale. The estimated conditional probabilities of failure of the external energy (EE), external water (EW), internal energy (IE) and internal water (IW) systems, given that the NPP has entered into an unsafe state, are also indicated.

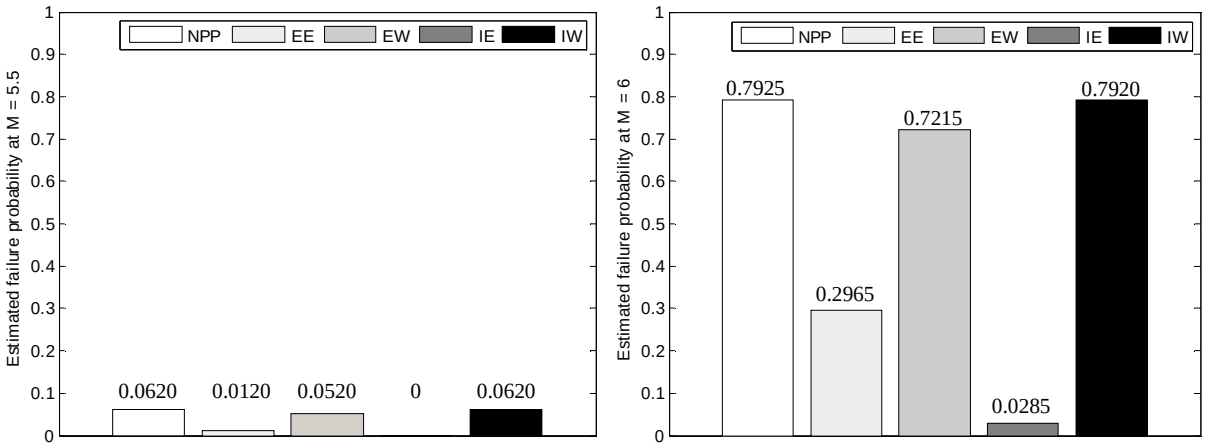


Figure 15: Estimate of the probability that the nuclear power plant (NPP) reaches an unsafe state upon occurrence of an earthquake of magnitude equal to 5.5 (left) and 6 (right) on the Richter scale, and the estimates of the conditional probability of failure of the external energy (EE), external water (EW), internal energy (IE) and internal water (IW) systems, given that the NPP has reached an unsafe state.

As expected, the higher the magnitude of the earthquake, the higher is the probability that the safety of the nuclear power plant cannot be assured.

The estimated probabilities of failure of the IW and EW systems are similar to that of the NPP at both magnitudes. This is because the two systems mostly contribute to the reaching of the NPP unsafe state. A qualitative analysis of the fragility values of the elements of the power and water systems, given in Table 5 in decreasing order for M = 5.5, on the left, and M = 6, on the right, shows that the first two components with higher fragility values are the pumps of the IW and EW systems. At magnitude 5.5 on the Richter scale, the third element in Table 5 is the road R7 that belongs to the EE system followed by the DG of the IE system that never fails in the simulation performed, due to its low fragility value ($2.52*10^{-3}$). At magnitude 6 on the Richter scale, the third element with higher fragility is represented by the pool that in the ranking at magnitude 5.5 is in the 10^{th} position; this represents a further weak element of the internal water system. The other components remain in the same ranking order both at magnitude 5.5 and 6 on the Richter scale, with increased fragility values for the higher magnitude.

Table 5: Conditional probability of failure of the components of the system of systems given an earthquake of magnitudes 5.5 (left) and 6 (right) on the Richter scale. The values are reported in decreasing order. GS: Generation Station; S: Substation; R: Road access; Po: Pole; Pi: Pipe; DG: Diesel Generator; Pu: Pump; M: Magnitude.

	M = 5.5
Pu2	3.78E-01
Pu1	1.27E-01
R7	3.66E-02
DG	2.52E-03
S	1.94E-03
Pi4	7.40E-04
Pi3	7.40E-04
Pi2	7.35E-04
Pi1	7.27E-04
Pool	4.57E-05
GS	7.05E-06
Po2	6.54E-10
Po1	1.01E-10

	M = 6
Pu2	9.32E-01
Pu1	7.46E-01
Pool	3.80E-01
R7	3.08E-01
DG	2.86E-02
S	2.74E-02
Pi4	9.64E-03
Pi3	9.64E-03
Pi2	9.61E-03
Pi1	9.53E-03
GS	1.13E-03
Po2	1.00E-05
Po1	5.28E-06

We now proceed with the evaluation of the capacity of recovering of the system of systems, starting from the top level of the hierarchy (recovery of the critical plant safety) and proceeding downward with the analysis of the lower levels to identify the causes and major contributors to the higher levels. The criticality importance measure [13], $I_i^{Cr,L}(t)$, of the component (or group) *i* at level *L*, $L = 2, ..., N_L$, of the hierarchy at time *t* is used to guide the analysis through the hierarchical model. It is defined as the probability that the component (or group) *i* at level *L*, $L = 2, ..., N_L$, of the hierarchy is critical for the system and failed at time *t*, given that the system is failed at time *t*:

$$I_i^{Cr,L}(t) = \frac{I_i^{B,L+1}(t)\cdot(1-r_i^{L+1}(t))}{1-R(\boldsymbol{r}^{L+1}(t))} \quad (7)$$

where $r_i^{L+1}(t)$ is the reliability of the component (or group) *i* at level *L*+1 of the hierarchy, $\boldsymbol{r}^{L+1}(t)$ is the vector of reliabilities of the components (or groups) at level *L*+1 of the hierarchy, $R(\boldsymbol{r}^{L+1}(t))$ is the system reliability, dependent on the reliabilities of the individual components (or groups) at level *L*+1 of the hierarchy and on the system configuration, $I_i^{B,L+1}(t)$ is the Birnbaum's measure of importance of the *i*-th component (or group) at level *L*+1 of the hierarchy and it is defined as $I_i^{B,L+1}(t) = \frac{\partial R(\boldsymbol{r}^{L+1}(t))}{\partial r_i^{L+1}(t)}$ [13].

With respect to the test system under analysis, the system reliability (level 1) depending on the reliabilities of the groups of level 2 and on their logic relations reported in Table 4, has been computed as follows:

$$R(\boldsymbol{r}^2(t)) = \left(1 - r_{EE}^2(t)\right)r_{IE}^2(t)\left(1 - r_{EW}^2(t)\right)r_{IW}^2(t) + \left(1 - r_{EE}^2(t)\right)r_{IE}^2(t)r_{EW}^2(t)r_{IW}^2(t) +$$
$$r_{EE}^2(t)\left(1 - r_{IE}^2(t)\right)\left(1 - r_{EW}^2(t)\right)r_{IW}^2(t) + r_{EE}^2(t)\left(1 - r_{IE}^2(t)\right)r_{EW}^2(t)\left(1 - r_{IW}^2(t)\right) +$$
$$r_{EE}^2(t)\left(1 - r_{IE}^2(t)\right)r_{EW}^2(t)r_{IW}^2(t) + r_{EE}^2(t)r_{IE}^2(t)\left(1 - r_{EW}^2(t)\right)r_{IW}^2(t) +$$
$$r_{EE}^2(t)r_{IE}^2(t)r_{EW}^2(t)\left(1 - r_{IW}^2(t)\right) + r_{EE}^2(t)r_{IE}^2(t)r_{EW}^2(t)r_{IW}^2(t) = r_{EE}^2(t)r_{EW}^2(t) +$$
$$r_{EE}^2(t)r_{IW}^2(t) + r_{IE}^2(t)r_{IW}^2(t) - r_{EE}^2(t)r_{EW}^2(t)r_{IW}^2(t) - r_{EE}^2(t)r_{IE}^2(t)r_{IW}^2(t)$$

The reliability $r_{EE}^2(t), r_{IE}^2, (t)r_{EW}^2(t)$ and $r_{IW}^2(t)$ of the EE, IE, EW and IW systems, respectively, at level 2 of the hierarchy, depend on the reliability of the groups at level 3, that in turns depend on the individual components at level 4. For example, the reliability $r_{EW}^2(t)$ at level 2 depends on the reliability of the groups Pi1-Pu1-Pi2 and R3 at level 3 (Figure 9); the first group is composed by three components, Pi1, Pu1 and Pi2, in series, thus, its reliability is the product of the single reliability of the corresponding elements at level 4 of the hierarchy ($r_{Pi1-Pu1-Pi2}^3(t) = r_{Pi1}^4(t)r_{Pu1}^4(t)r_{Pi2}^4(t)$), whereas the second group, having no impacts on the state of the system EW (as explained in Section 4.2) is not considered in the computation of the reliability $r_{EW}^2(t)$. The reliabilities of the individual components at level 4 are the complement to 1 of the corresponding conditional probabilities of failure, given a magnitude value, reported in Table 5.

Figure 16 shows the probability density functions (PDFs) (on the left) and the respective cumulative distribution functions (CDFs) (on the right) of the time it takes to restore the safety of the nuclear power plant when an earthquake of magnitude 5.5 (solid line) and 6 (dashed line) on the Richter scale occurs. The 95th percentile of the distributions is used as indicator of the time it takes to recover safety. As expected, at the lower magnitude the time for recovering safety is shorter.

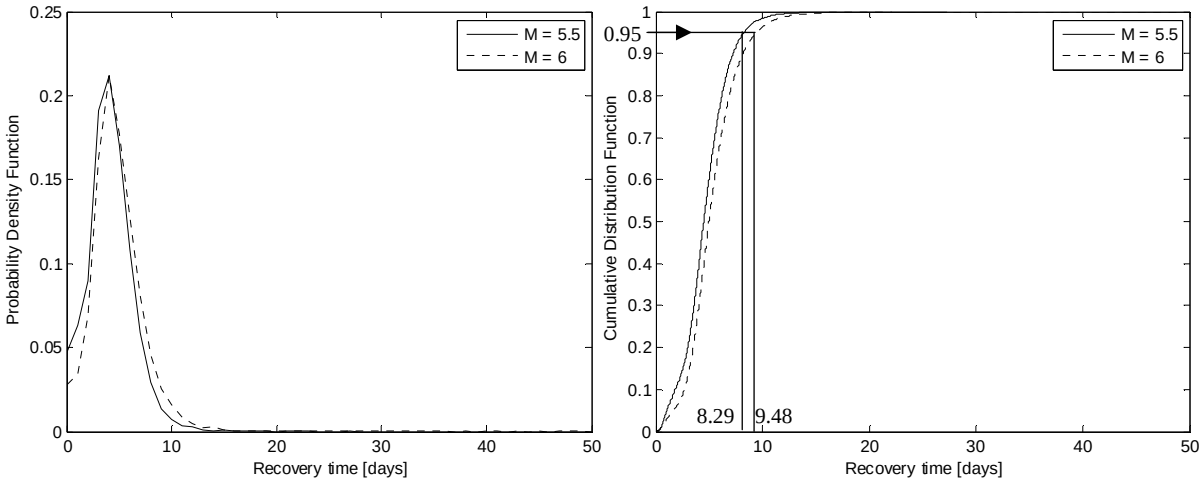


Figure 16: Left: probability density functions of the recovery time of the safety of the nuclear power plant when an earthquake of magnitude 6.5 (solid line) and 7 (dashed line) on the Richter scale occurs. Right: corresponding cumulative distribution functions.

In Table 6, the values of the criticality importance measure of the systems at level 2 (external and internal power and water systems) with respect to the level 1 of the hierarchy (critical plant) are reported. It can be seen that the EW and IW systems have a significantly higher impact than EE and IE systems both at lower and higher magnitudes.

Table 6: Criticality importance measures of the external (E) and internal (I) power (E) and water (W) systems for magnitudes equal to 5.5 and 6 on the Richter scale.

	M = 5.5	**M = 6**
$\boldsymbol{I_{EE}^{cr,2}}$	0.2081	0.0984
$\boldsymbol{I_{IE}^{cr,2}}$	9.8E-04	4.8E-04
$\boldsymbol{I_{EW}^{cr,2}}$	0.7614	0.6059
$\boldsymbol{I_{IW}^{cr,2}}$	0.9984	0.9883

Figures 17 and 18 show the probability density functions of the time it takes to recover the internal and external parts of the power and water systems (level 2 of the hierarchy) after the occurrence of an earthquake of magnitude equal to 5.5 and 6 on the Richter scale, respectively.

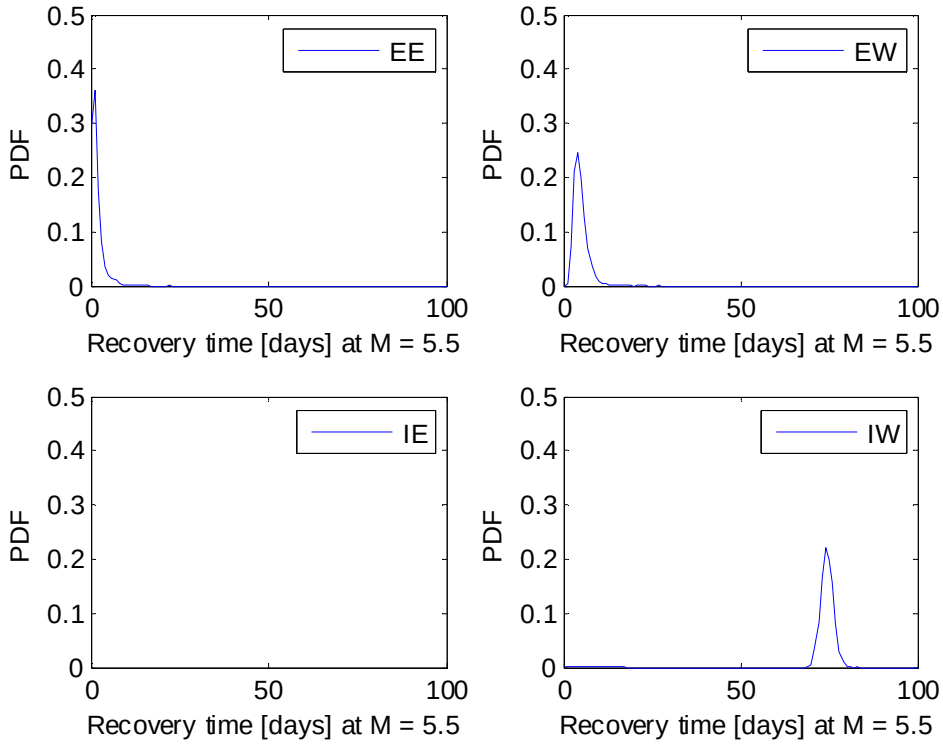


Figure 17: Probability density functions of the recovery time of the internal (I) and external (E) parts of the power (E) (left) and water (W) (right) systems, given the occurrence of an earthquake of magnitude (M) equal to 5.5 on the Richter scale.

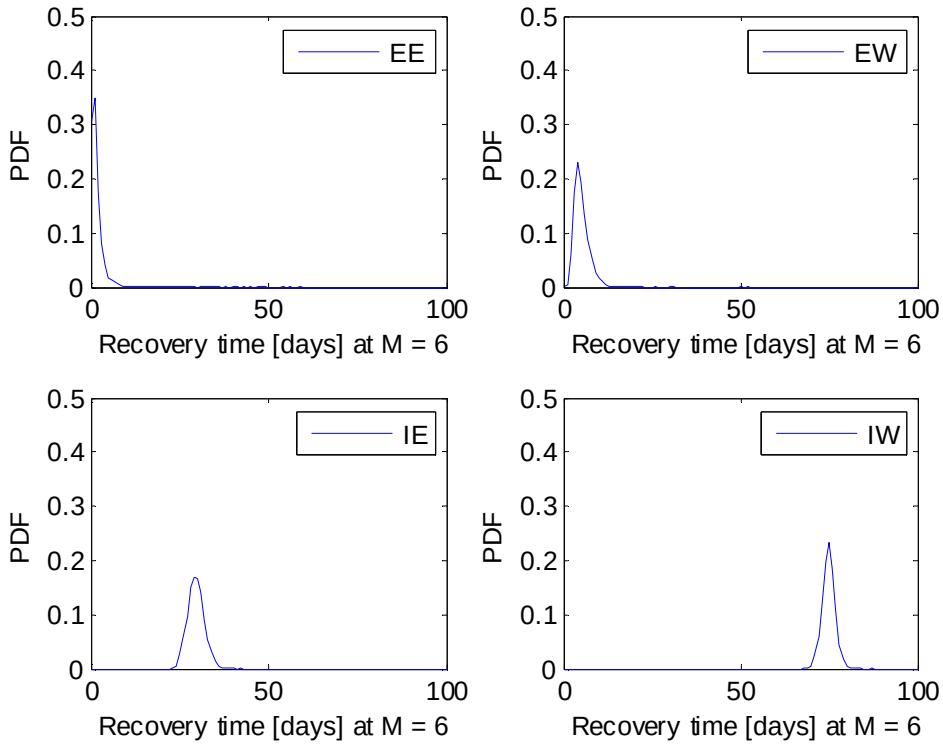


Figure 18: Probability density functions of the recovery time of the internal (I) and external (E) parts of the power (E) (left) and water (W) (right) systems, given the occurrence of an earthquake of magnitude (M) equal to 6 on the Richter scale.

At magnitude 5.5 on the Richter scale, the recovery time of the IE system is not present since this system has never failed in the simulation.
At magnitude 6, the recovery times of the external parts of the energy and water systems are concentrated at values lower than the recovery times of the internal parts, which means that the recovery times of the systems at level 2 depend on the recovery of the external parts.

Figure 19 shows the probability density functions of the time it takes to recover the groups of the external water system at the level 3 of the hierarchy, for an earthquake of magnitude 6 on the Richter scale.

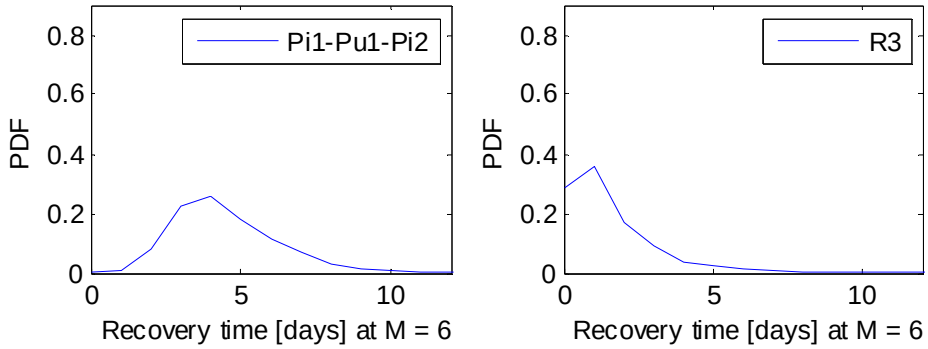


Figure 19: Probability density functions (PDFs) of the recovery time of the groups at level 3 of the hierarchy for the external water system, given the occurrence of an earthquake of magnitude (M) equal to 6 on the Richter scale.

The group of components Pi1-Pu1-Pi2 contributes mostly to the recovery time of the EW system since the state of the road R3 has no impact in the state of the EW system, as explained in Section 4.2; then, the criticality importance measure of Pi1-Pu1-Pi2 is 0.6059, i.e., it is equal to $I_{EW}^{cr,2}$ as shown in Table 6.

Figure 20 illustrates the recovery time distributions of the components Pu1, Pi1 and Pi2 at level 4 of the hierarchy, and Table 7 reports the corresponding criticality importance measure values: at level 4, the major contributor to the recovery time is the component Pu1 that has the highest importance measure value equal to 0.5906.

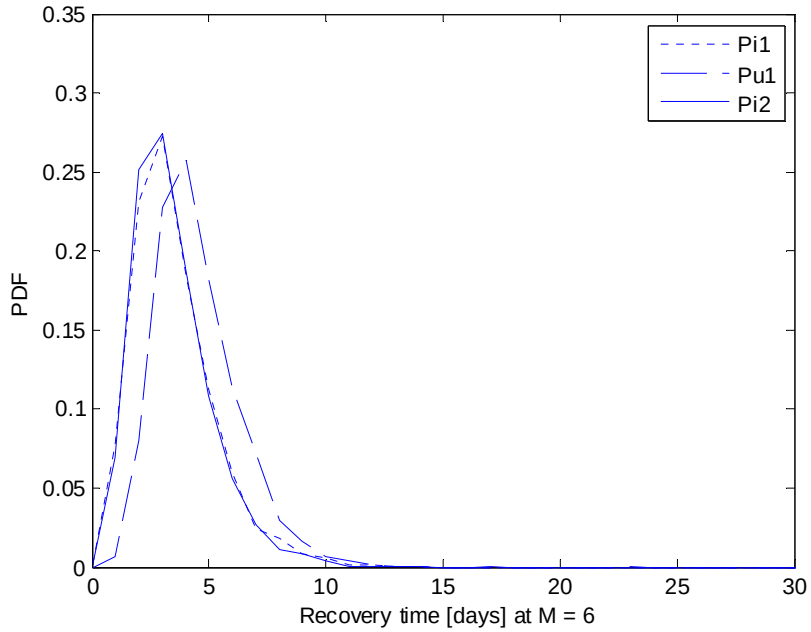


Figure 20: Probability density functions (PDFs) of the recovery time of the components Pi1, Pu1 and Pi2 given the occurrence of an earthquake of magnitude (M) equal to 6 on the Richter scale.

Table 7: Criticality importance measures of the groups at the level 4 of the hierarchy, for an earthquake of magnitude (M) equal to 6 on the Richter scale.

	M = 6
$\boldsymbol{I_{Pi1}^{cr,4}}$	1.93E-03
$\boldsymbol{I_{Pu1}^{cr,4}}$	5.91E-01
$\boldsymbol{I_{Pi2}^{cr,4}}$	1.95E-03

A similar analysis on the internal water system (here not reported, for brevity), leads to the conclusion that the pump and the pool are the most relevant components for the time of recovery of such system.

5. CONCLUSIONS

We have adopted a system-of-systems framework previously proposed by the authors for the analysis of the risk of a critical plant (a nuclear power plant in the example worked out) exposed to hazardous external events (earthquakes in the example worked out), so as to account for the influence of the interdependent infrastructures in which the plant is embedded. We have represented the system of systems with a hierarchical model and used Monte Carlo simulation for its probabilistic evaluation in terms of the safety of the nuclear power plant and its capacity of recovering, measured in terms of the time needed to restore safety.

The plus of this framework is that it allows performing a systematic analysis through the hierarchical levels of the model, and identifying the contribution to the safety recovery time of the system-of-systems individual elements (here measured by the criticality importance measure). The results which are obtained by such type of analysis can be useful to point out which systems are recovered early and which take more time to be recovered. These findings can help identifying margins for improvement of the structural/functional responses of the critical elements, for improving the global recovery of the system of systems so as to increase the safety of the critical plant. In the end, they can inform decision makers in their planning choices of actions for increasing the safety of critical plants.

Future work will be devoted to explore other system modeling and analysis approaches for comparison, like for example Multilevel Flow Modelling (MFM) [30], Stocastic Flowgraphs [31], Goal Tree Success Tree – Master Logic Diagram (GTST – MLD) [32], with the aim of pointing out limitations and benefits with respect to their application.

REFERENCES

[1] International Atomic Energy Agency. The great east Japan earthquake expert mission – IAEA international fact finding expert mission of the Fukushima Dai-ichi NPP accident following the great east Japan earthquake and Tsunami. Mission Report 24 May – 2 Jun 2011. 162 p.

[2] Adachi T, Ellingwood BR. Serviceability of earthquake-damaged water systems: Effects of electrical power availability and power backup systems on system vulnerability. Reliability Engineering & System Safety. 2008; 93(1):78‑88.

[3] Aven T. On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. Risk Analysis. 2011; 31(4):515–522.

[4] Eusgeld I, Nan C, Dietz S. “System-of-systems” approach for interdependent critical infrastructures. Reliability Engineering & System Safety. 2011; 96(6):679-686.

[5] Haimes YY. On the Complex Definition of Risk: A Systems-Based Approach. Risk Analysis. 2009; 29(12):1647-1654.

[6] Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety. 2010; 95(12):1335-1344.

[7] Kröger W, Zio E. Vulnerable systems. London: Springer; 2011. 63 p.

[8] Wang S, Hong L, Chen X. Vulnerability analysis of interdependent infrastructure systems: a methodological framework. Physica A: Statistical Mechanics and its Applications. 2012; 391(11): 3323-3335.

[9] Ferrario E, Zio E. A system-of-systems framework of Nuclear Power Plant Probabilistic Seismic Hazard Analysis by Fault Tree analysis and Monte Carlo simulation. Proceedings of the joint 2012 International Conference on Probabilistic Safety Assessment and Management (PSAM 11) & European Safety and RELiability Conference (ESREL 2012), Helsinki, Finland, June 2012.

[10] Cimellaro, GP. Reinhorn, AM. Bruneau, M. 2010. Framework for analytical quantification of disaster resilience. Engineering Structures 32: 3639-3649.

[11] Gomez C, Sanchez-Silva M, Duenas-Osorio L, Rosowsky D. Hierarchical infrastructure network representation methods for risk-based decision-making. Structure and Infrastructure Engineering: Maintenance, Management, Life-Cycle Design and Performance. 2011. http://dx.doi.org/10.1080/15732479.2010.546415

[12] Cheok MC, Parry GW, Sherry RR. Use of importance measures in risk informed applications. Reliability Engineering and System Safety. 1998; 60: 213-226.

[13] Zio E. Computational methods for reliability and risk analysis, Chapter 2, Series on Quality, Reliability and Engineering Statistics, Vol 14, World Scientific Publishing Co. Pte. Ltd., 2009.

[14] Kalos MH, Whitlock PA. Monte Carlo methods. Vol. 1, Basics. New York: Wiley; 1986. 186 p.

[15] Zio E. Computational methods for reliability and risk analysis. Series on Quality, Reliability and Engineering Statistics, Vol 14. Singapore: World Scientific Publishing Co. Pte. Ltd.; 2009. Chapter 2, Monte Carlo simulations for reliability and availability analysis; p. 59-69.

[16] Zio E. The Monte Carlo Simulation Method for System Reliability and Risk Analysis. London: Springer Series in Reliability Engineering. 2012.

[17] Seismic Probabilistic Risk Assessment Implementation Guide, EPRI, Palo Alto, CA: 2003. TR-1002989.

[18] Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Expert. Main Report, Vol. 1. 1997, NUREG/CR-6372 UCRL-ID- 122160. Supported by U.S. Nuclear Regulatory Commission (NRC), the U.S. Department of Energy (DOE); and the Electric Power Research Institute (EPRI).

[19] Sen TK. Fundamentals of seismic loading and structures. Singapore: John Wiley & Sons, Ltd; 2009. Chapter 7, Probabilistic Seismic Hazard Analysis; p. 181-218.

[20] Kanamori H. The energy release in great earthquakes. Journal of Geophysical Research. 1977; 82(20): 2981–2987.

[21] Kanamori H. Magnitude scale and quantification of earthquakes. In: SJ. Duda and K. Aki Editors. Quantification of Earthquakes. Tectonophysics, 1983; 93: 185-199.

[22] Kramer SL. Geotechnical Earthquake Engineering, Prentice Hall, New Jersey. 1996.

[23] Weatherill GA, Burton PW. The application of multiple random earthquake simulations to probabilistic seismic hazard assessment in the Aegean region. First European Conference on Earthquake Engineering and Seismology. Geneva, Switzerland. 2006.

[24] Douglas J (Bureau de Recherches Géologiques et Minières). Ground-motion prediction equations 1964-2010. Berkeley (California): Pacific Earthquake Engineering Research Center: 2011. 455 p.

[25] Ambraseys NN, Douglas J, SARMA SK, Smit PM. Equations for the estimation of strong ground motions from shallow crustal earthquakes using data from Europe and the Middle East: horizontal peak ground acceleration and spectral acceleration. Bulletin of Earthquake Engineering. 2005; 3:1-53.

[26] Gomez C, Sanchez-Silva M, Dueñas-Osorio L. Clustering methods for risk assessment of infrastructure network systems. Applications of statistics and probability in civil engineering – Faber, Koler and Nishijima (eds). Taylor and Francis Group, London. 2011: 1389-1397.

[27] Huang YN, Whittaker AS, Luco N. A probabilistic seismic risk assessment procedure for nuclear power plants: (I) Methodology, Nuclear Engineering and Design. 2011; 241: 3996– 4003.

[28] Varpasuo P. Seismic fragility analysis of selected heavy components in LNNP unit1 reactor building. Transactions of the 17th International Conference on Structural Mechanics in Reactor Technology (SMiRT). Prague, Czech Republic, August 17-22, 2003.

[29] Basu PC. Seismic fragility of nuclear installations. Atomic Energy Regulatory Board. Mumbay, India. 2008. Presentation: http://civil.iisc.ernet.in/basu.pdf

[30] Lind M. An introduction to multilevel flow modeling. Nuclear safety and simulation. 2011; 2(1): 22-32.

[31] Huzurbazar, A. V, Williams B. J. Flowgraph models for complex multistate system reliability. Modern statistical and mathematical methods in reliability. 2005; 10: 247-262.

[32] Modarres M, Cheon SW. Function-centered modeling of engineering systems using the goal tree–success tree technique and functional primitives, Reliability Engineering & System Safety. 1999; 64(2): 181-200.