A system-of-systems framework of Nuclear Power Plant Probabilistic Seismic Hazard Analysis by Fault Tree analysis and Monte Carlo simulation

Elisa Ferrario, Enrico Zio

A system-of-systems framework of Nuclear Power Plant Probabilistic Seismic Hazard Analysis by Fault Tree analysis and Monte Carlo simulation

Elisa Ferrario[a], Enrico 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 propose a quantitative safety analysis of a critical plant with respect to the occurrence of an earthquake, extending the envelope of the study to the interdependent infrastructures which are connected to it in a "system-of-systems" – like fashion. As a mock-up case study, 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 Probabilistic Seismic Hazard Analysis of such system of systems is carried out by Fault Tree analysis and Monte Carlo simulation. As outcome of the analysis, the probability that the nuclear power plant reaches an unsafe state is computed for different earthquake's epicentre distances and the contribution of the interdependent infrastructures to the safety of such critical plant is highlighted.

Keywords: System of systems, Probabilistic Seismic Hazard Analysis, Fault Tree Analysis, Monte Carlo simulation

1. INTRODUCTION

In the present paper, we consider the quantitative safety analysis of a nuclear power plant (NPP) with respect to the occurrence of an earthquake. We assume that internal emergency devices are available to provide safety for the plant upon such disturbances. However, accidental events in the industrial history, e.g., the recent Fukushima disaster (IAEA, 2011), have shown that the post-accident recovery of the full or partial safety of the plant may also depend on the infrastructures connected to it. In this view, the surrounding environment 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 must extend to the interdependent infrastructures connected to it, adopting a "system-of-systems" point of view. To this aim, both the intra-system and inter-systems dependencies, i.e., the dependencies between the components of a same infrastructure system and between the components of different infrastructure systems, respectively, are taken into account.

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

The assessment is performed by two main steps: first, a conceptual map is built to understand all the intra-system and inter-system dependencies among the components of the infrastructure systems connected to the nuclear power plant; then, a Fault Tree analysis is applied and the probability that the nuclear power plant enters in an unsafe state is computed by Monte Carlo simulation 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 Probabilistic Seismic Hazard Analysis are illustrated; in Section 3, the Fault Tree analysis by Monte Carlo simulation for Probabilistic Seismic Hazard Analysis is described; in Section 4, the case study and the results of the analysis are presented and discussed; in Section 5, conclusions are provided.

2. PROBABILISTIC SEISMIC HAZARD ANALYSIS

A Probabilistic Seismic Hazard Analysis (PSHA) consists of four procedural steps (EPRI, 2003; NUREG/CR-6372, 1997):

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 (EPRI, 2003; NUREG/CR-6372, 1997).

The major outputs of the seismic hazard analysis 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 (EPRI, 2003; NUREG/CR-6372, 1997).

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 greater than m and a and b are parameters obtained by regression data analysis (EPRI, 2003; NUREG/CR-6372, 1997). This relation implies that the magnitude is exponentially distributed:

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

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 (EPRI, 2003):

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

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 (Douglas, 2011). They usually assume this expression (EPRI, 2003):

$$\log z' = C_1 + C_2 m + C_3 m C_4 + C_5 \log\left[r + C_6 \exp(C_7 m)\right] + C_8 r + g(source) + g(site) \tag{3}$$

where z' is the mean ground motion parameter, C_i, $i = 1, \ldots, 8$, 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 (Ambraseys et al., 2005):

$$\log_{10} z' = C_1 + C_2 m + (C_3 + C_4 m) * \log_{10} \sqrt{r^2 + C_5^2} + C_6 S_S + C_7 S_A + C_8 F_N + C_9 F_T + C_{10} F_0 \tag{4}$$

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).

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 (EPRI, 2003):

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

where $i = 1,....,S$ 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.

A fragility evaluation is then 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) for the fragility model that assumes this expression (EPRI, 2003):

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

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'*.

3. FAULT TREE ANALYSIS AND MONTE CARLO SIMULATION FOR THE PROBABILISTIC SEISMIC HAZARD ANALYSIS UNDER A SYSTEM-OF-SYSTEMS FRAMEWORK

Consider a critical plant *H* (in our case the nuclear power plant) connected to N_S interdependent systems S_i (in our case the power and water distribution networks and the transport network), with N_{S_i} components linked by $K_{S_{(i,l)}}$, $i,l = 1,...,N_S$, intra-system and inter-systems dependencies. The overall system is therefore composed by $N = \sum_{i=1}^{N_S} N_{S_i} + 1$ components, where the critical plant object of the analysis has been purposedly explicited.

We wish to comprehensively evaluate the safety of the critical plant *H* with respect to the occurrence of an earthquake. To do this, in addition to the direct effects of the earthquake on *H*, we evaluate also the structural and functional responses of the N_{S_i}, $i = 1,...,N_S$, components and their impacts on the systems S_i, $i = 1,...,N_S$, and on the critical plant *H*. The approach taken is based on Fault Tree (FT) analysis and Monte Carlo (MC) simulation for Probabilistic Seismic Hazard Analysis (PSHA), and consists of the following operative steps:

1. build the fault tree of the top event "unsafe state of critical plant *H*", within a system-of-systems viewpoint that accounts also for the infrastructure connected to *H*;
2. identify the minimal cut sets $M_1, M_2, ..., M_{mcs}$;
3. sample a magnitude value from the double truncated exponential distribution (2);
4. compute the ground motion value at each of the N_{S_i}, $i = 1,...,N_S$, components of the systems S_i, $i = 1,...,N_S$, and on the critical plant *H*, by equation 4;
5. compute the fragility, *f*, for all the components N_{S_i}, $i = 1,...,N_S$, of the systems S_i, $i = 1,...,N_S$, and for the critical plant *H* by equation 6; *f* is a vector of N values corresponding to the N components of the system;

6. sample a matrix $\{u_{j,k}\}$, $j=1,...,N_T$, $k=1,...,N$, where N_T is the number of simulations, of uniform random numbers in [0,1);
7. determine the fault state matrix $\{g_{j,k}\}$, by comparing the fragility, *f*, with the matrix $\{u_{j,k}\}$, $j=1,...,N_T$, $k=1,...,N$: if $f_k < u_{j,k}$, $g_{j,k}=1$; otherwise $g_{j,k}=0$. When $g_{j,k}$ assumes value 1, the *k-th* component is affected by the earthquake, i.e., it enters a faulty state; otherwise, it survives. Each row of the matrix $\{g_{j,k}\}$ represents the states of the N system components of the system, i.e., its configuration;
8. assess the state of *H* for each row *j* of the matrix $\{g_{j,k}\}$ determined at step 7., i.e., for each system configuration sampled, by evaluating the system structure function $X_{H_j}=\Phi(g_{j,1},...,g_{j,N})=1-(1-M_1)(1-M_2)...(1-M_{mcs})$, $j=1,...,N_T$. A vector $\{X_{H_j}\}$, is thus obtained, whose elements assume value 1 when the critical plant *H* is in an unsafe state and 0 otherwise;
9. estimate the probability of the critical plant *H* of being unsafe by computing the sample average of the values of the vector $\{X_{H_j}\}$, $j=1,...,N_T$.

The procedure above is repeated a large number of times for different values of earthquake magnitude.

4. CASE STUDY

We consider the evaluation of the safety of a fictitious nuclear power plant in response to earthquakes. We include in the analysis the responses of the interconnected systems that provide services which can aid keeping or restoring its safe state.

In Section 4.1, the description of the specific system studied is given; in Section 4.2, the results of its evaluation are provided, together with some critical considerations.

4.1. Description of the physical system and its view as a system of systems

The system under analysis is composed by a critical plant, i.e., a nuclear power plant, *H*, the power system, S_1, that provides electrical energy for the running of the nuclear power plant, the water system, S_2, that provides coolant useful to absorb the heat generated in the nuclear power plant, and the road network, S_3, relevant to the nuclear power plant for the transport of material and 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 1 the physical representation of the system is reported referring to a Cartesian plan (*x*, *y*) with origin in the river. Given the large scale system under analysis, two types of soil are considered, rock and soft soil. Figure 2 represents the spatial localization of the system shown in Figure 1 with reference to the reciprocal position of all the components (Figure 2, left) and to the position of the system, with respect to three earthquake's epicenters, *A*, *B*, *C*, (Figure 2, right). The distances on the axes are expressed in kilometers.

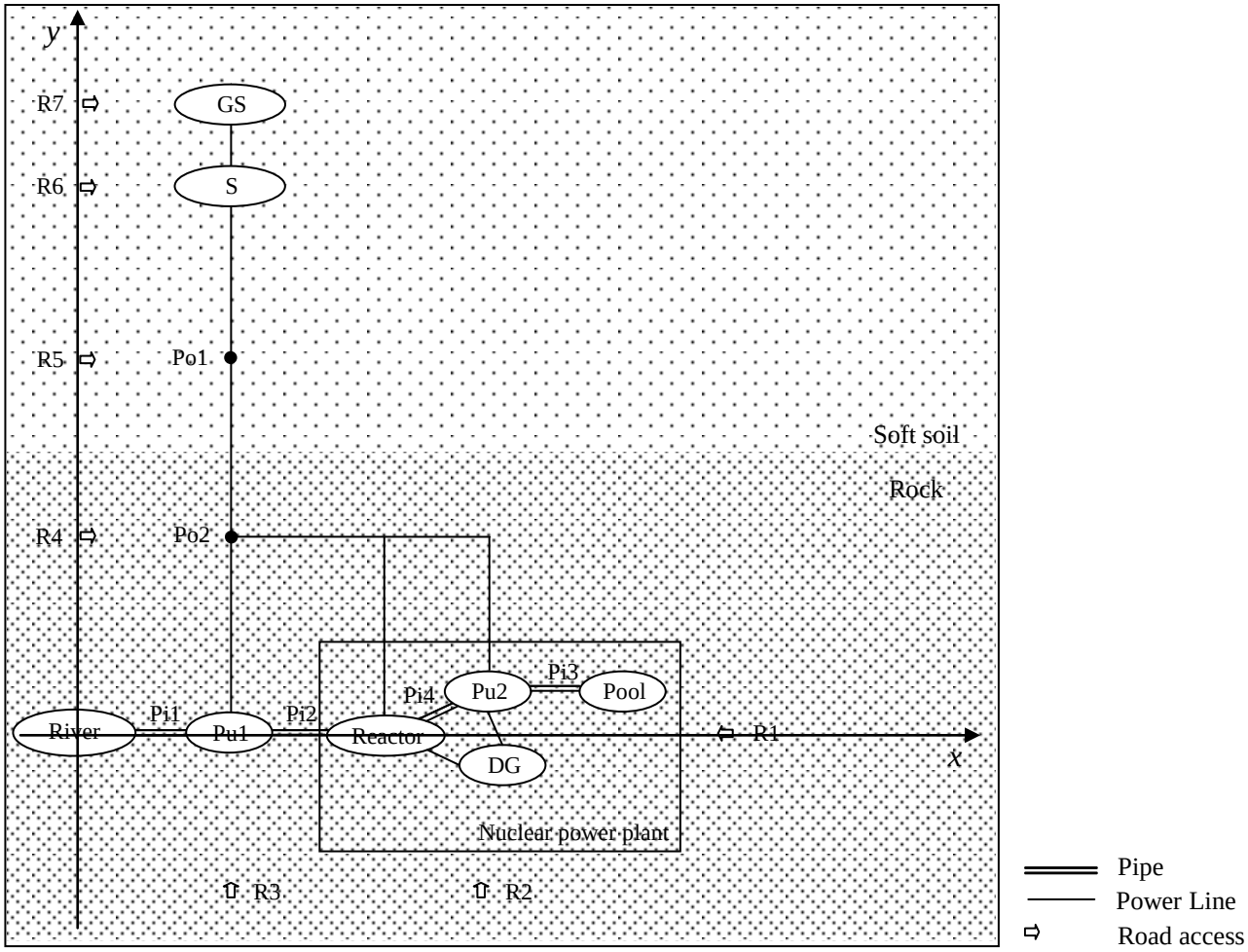

Figure 1. Physical representation of the system. GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, DG: Diesel Generator, R: Road access.

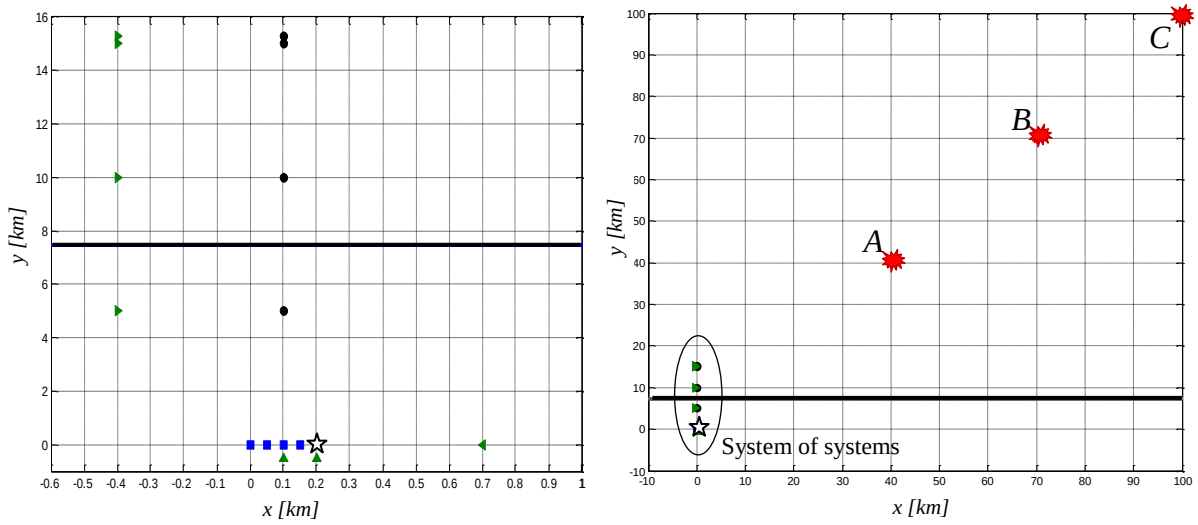

Figure 2. Left: spatial localization of the nuclear power plant (star) with respect to the components of the electric power system (circle, from top to bottom: Generation Station, Substation, Pole 1, Pole 2), water system (square, from left to right: River, Pipe 1, Pump 1, Pipe 2) and road transportation (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 three earthquake's epicenters A(40, 40), B(70, 70), C(100 , 100). The horizontal bold line in both Figures represents the division between soft soil (above the line) and rock (below the line).

In Figure 3, 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.

The external water distribution system (Figure 3, left) is formed by a source of water (e.g., a river), a pump and pipes that carry the water. The failure probability of these elements depends on the type of soil and on the design and materials of construction. Operators are in charge of the maintenance of the structural elements and mechanical components.

The external power distribution system (Figure 3, 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, power lines and poles to support them, the type of soil on which the infrastructures rest and the operators that run the generation station and provide the maintenance for all its elements and components.

The components of the emergency water and power distribution systems inside the plant are shown in Figure 3 on the right. The first system is composed by the same elements of the correspondent external system except for the source of water that is an artificial reservoir, whereas the power system includes only the emergency diesel generators.

The elements considered for the transportation system are the roads (Figure 3, 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.

Actually, in view of the methodological character of this work, for the sake of simplicity, the influence of the design construction and materials, the supply of fuel and materials for plant operation, and the maintenance tasks are not included in the analysis. The power lines, being aerial elements and therefore being not directly affected by an earthquake, are also not considered. Finally, the assumption is made that the river is not perturbed by the earthquake so that it is a source of water always available.

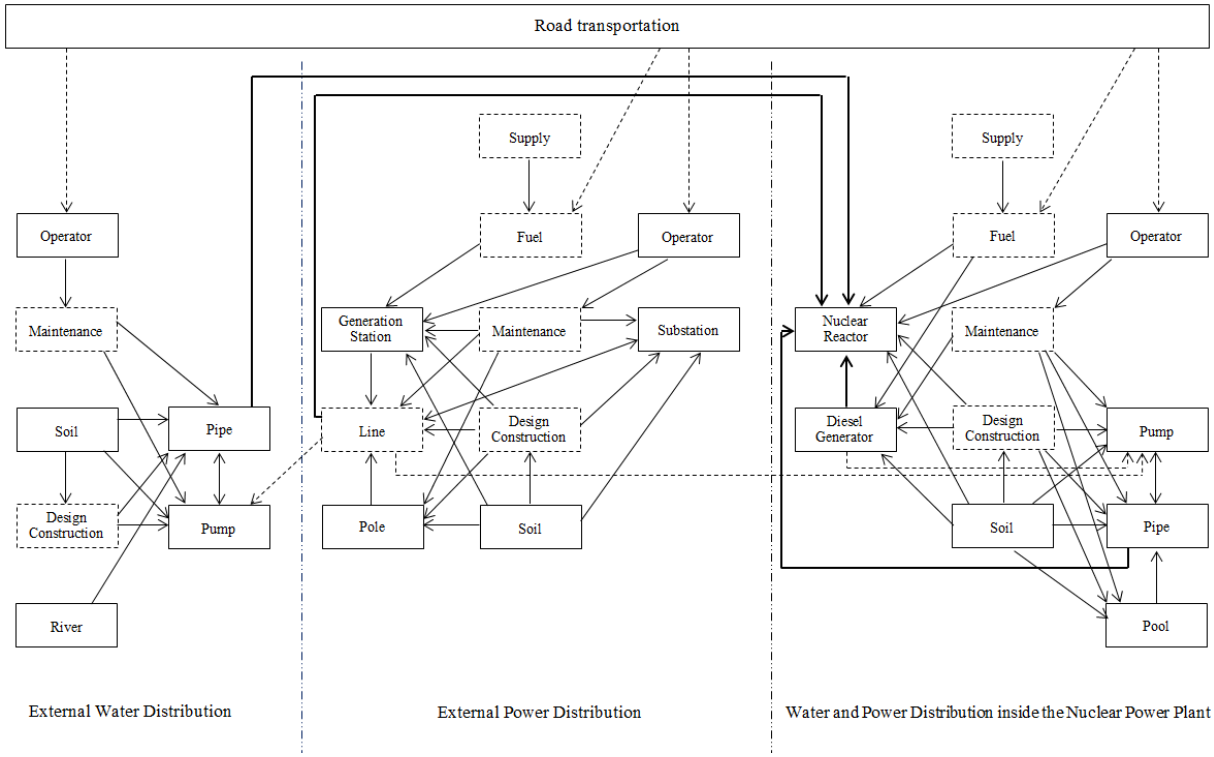

Figure 3. System of systems: the elements in the dashed box are not considered in the present study; the links represent the intra-systems dependencies (solid lines), the inter-systems dependencies (dashed lines) and the dependencies of the nuclear power plant on its interconnected systems (bold lines).

The inter-system dependencies are modeled as links connecting components of the three systems, S_i, i=1, 2, 3, (Figure 3, 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 water system depends on the power system as the pump needs electrical energy to work. This component receives the electrical energy from the external

power distribution network; on the contrary, it is assumed that the pump inside the nuclear power plant can obtain energy 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 operators for operation and/or maintenance.

The transport system is composed by seven interdependent road access points to the components of the power and water systems. One access is provided for the components outside the nuclear power plant, whereas two accesses are provided for the elements inside (Figure 1).

Note that, in the present study, the road assumes the function of "reserve component", since we assume that elements that fail can be immediately repaired/replaced if the access to it through the road system does not fail (recovery times are not considered).

Figure 4 shows the primary levels of the fault tree built for the analysis. It depicts the main causes of occurrence of the top event, i.e., critical plant *H* is in an unsafe state, which are the lack of energy and/or water supply by both the internal and external systems. For space limitation, the triangular elements in the tree are not detailed in the Figure. By way of example, the fault tree of the pump of the external water distribution is reported in Figure 5. This component is unable to provide its service if 1) the component itself fails and at the same time there is no road access to repair it or 2) it does not receive the necessary inputs of electrical energy and water. The external energy system fails if one or more of its elements fail, i.e., the generation station, the substation or the poles, whereas the external water system cannot provide water for the pump if a rupture of the pipe occurs.

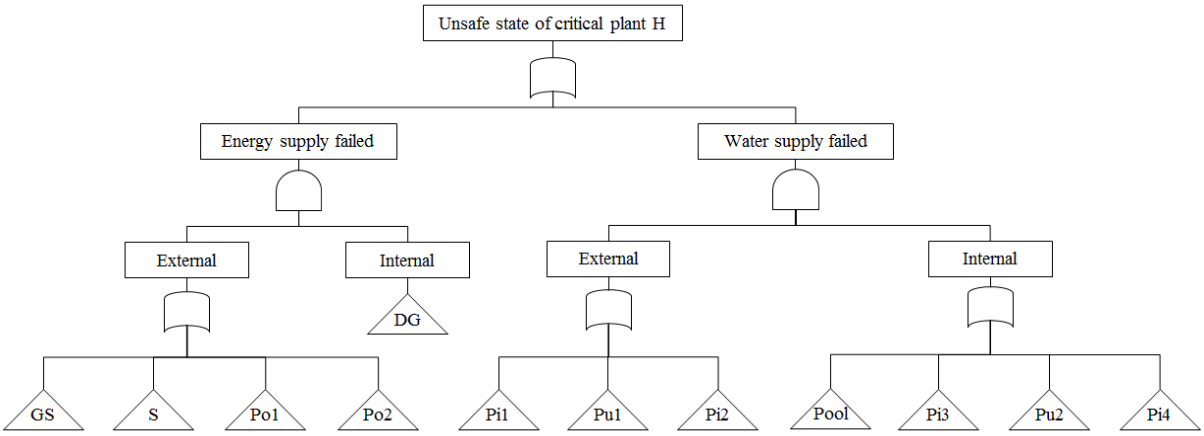

Figure 4. Fault tree of the system of systems: upper levels. The elements in the triangular shape are not detailed. NPP: Nuclear Power Plant, GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, DG: Diesel Generator.

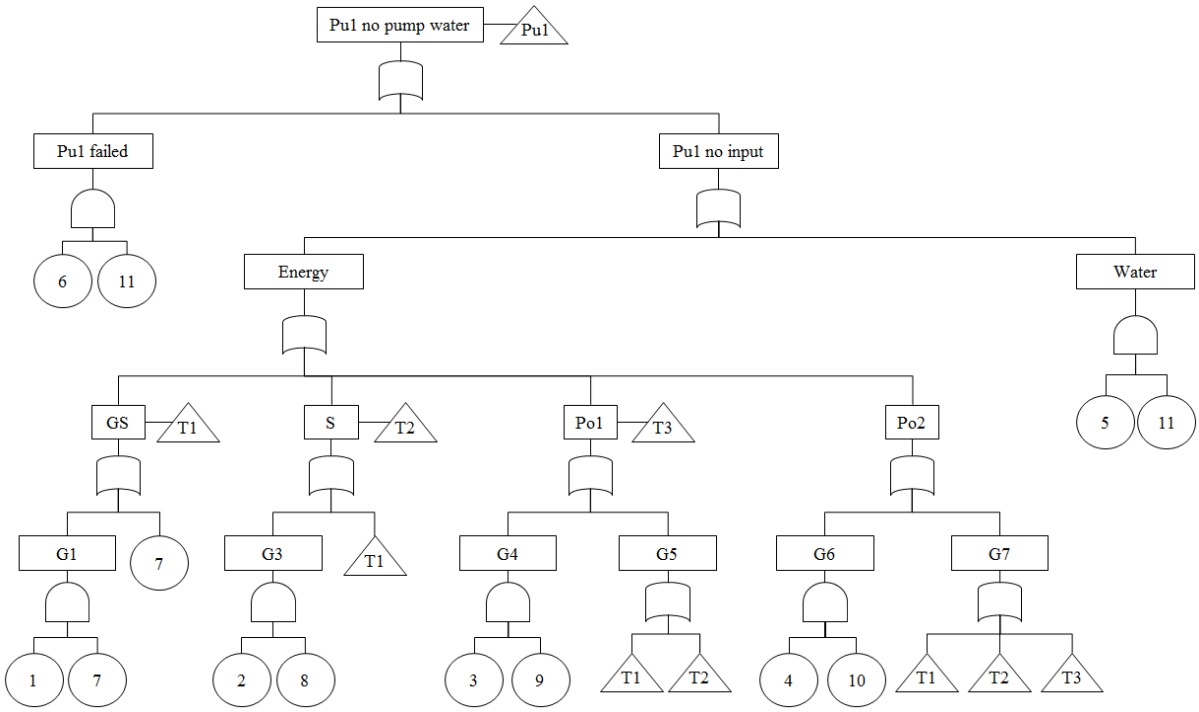

Figure 5. Fault tree details for the failure event of the component "pump" of the external water distribution system. GS: Generation Station, S: Substation, Po: Pole, Pi: Pipe, Pu: Pump, R: Road access. The numbers in the circles are referred to the failure of the components: 1→ GS, 2→ S, 3→ Po1, 4→ Po2, 5→ Pi1, 6→ Pu1, 7→ R7, 8→ R6, 9→ R5, 10→ R4, 11→ R3.

4.2. Results and limitations

Figure 6 shows the results of the evaluation by Monte Carlo simulation of the fault tree presented in the previous Section, within the Probabilistic Seismic Hazard Analysis procedure introduced in Section 3. For each magnitude level sampled from a truncated exponential probability distribution (2) with lower threshold m_{min}=5 and upper bound m_{max}=7, the estimate of the probability of the nuclear power plant to reach an unsafe condition, is computed.

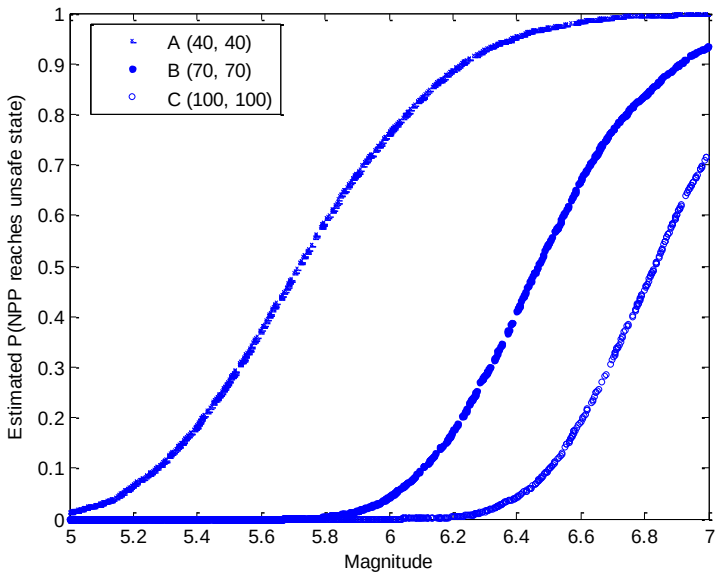

Figure 6. Estimate of the probability that the nuclear power plant reaches an unsafe state upon occurrence of an earthquake of a given magnitude, on the basis of different source-to-site distances. With reference to the map of Figure 2, the coordinates of the earthquake's epicenters considered are A(40, 40), B(70, 70), C(100, 100), expressed in kilometers.

The analysis is carried out for the three earthquake's epicenters, *A*, *B*, *C*, shown in Figure 2. As expected, the higher the distance, the lower is the probability that the safety of the nuclear power plant is not guaranteed.

Figure 7 shows the comparison between the probabilities that the nuclear power plant turns into an unsafe condition after the occurrence of an earthquake at epicenter A(40, 40) considering it both as an isolated component provided with its emergency devices (case of independence) and as a part of the system of systems, with the supporting infrastructures (case of dependence).

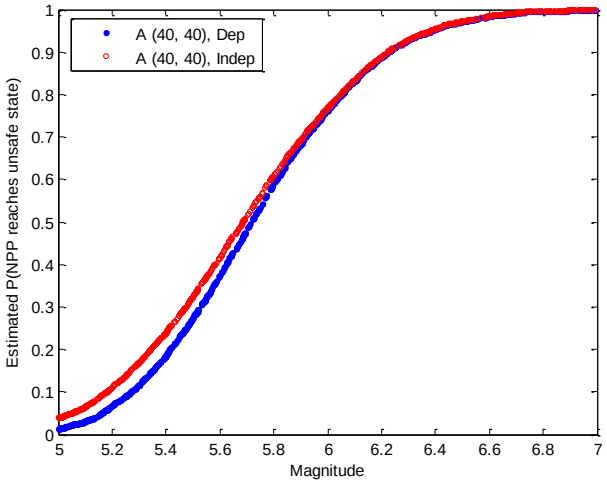

Figure 7. Comparison between the results of the MC simulation in the case of dependence of the nuclear power plant on the connected infrastructure systems, and in the case of independence, for earthquake's epicenter A(40, 40).

It can be seen that with the given assumptions and data, the probabilities to reach an unsafe state computed in case of dependence are slightly lower than those computed in case of independence, particularly at low earthquake magnitudes. This result shows that in principle the infrastructures in the surrounding of the critical plant can contribute to its resilience, offering additional possibilities for maintaining (or restoring) a safe condition, particularly when the earthquake magnitude is small.

5. CONCLUSIONS

We have used Fault Tree analysis and Monte Carlo simulation to perform a quantitative safety analysis of a nuclear power plant under the risk of occurrence of an earthquake, extending the area of study to its interconnected infrastructure systems (water and power distribution, and transportation networks) within a system-of-systems analysis framework.

The results obtained highlight that the interdependent infrastructure systems may play a role by providing additional support to the safety of a nuclear power plant, and it thus seems advisable to include them in the safety analysis.

More generally, the modeling framework proposed can be used to analyze the contribution to the safety of any critical plant, provided by the interdependent infrastructure systems connected to it.

Future work will concern the inclusion of the time for recovery of a failed component and the duration of emergency service supply.

References

Ambraseys, N.N., Douglas, J., SARMA, S.K. and Smit, P.M. (2005) 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*, 3, 1-53.

Douglas, J. (2011) Ground-motion prediction equations 1964-2010, *Pacific Earthquake Engineering Research Center*, Final Report BRGM/RP-59356-FR.

EPRI (2003) *Seismic Probabilistic Risk Assessment Implementation Guide*, EPRI TR-1002989.

Harary, F. (1995) *Graph Theory*. Perseus, Cambridge, MA

IAEA (2011) *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.

NUREG/CR-6372 (1997) *Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts*, UCRL-ID- 122160 Vol. 1.