Reliability Engineering and System Safety 107 (2012) 214–223

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Investigation of the structure of a networked system

Stefano La Rovere [a,*], Paolo Vestrucci [b]

[a] NIER Ingegneria, via C. Bonazzi 2, 40013 Castel Maggiore (BO), Italy
[b] DIENCA, University of Bologna, via dei Colli 16, 40126 Bologna (BO), Italy

ARTICLE INFO

Article history:
Received 15 October 2010
Received in revised form
17 November 2011
Accepted 11 June 2012
Available online 27 June 2012

Keywords:
Network
Critical infrastructure
Importance
Sensitivity
Nuclear power plant

ABSTRACT

The information coming from the network topology, which does not depend on the failure and repair probabilities of its elements, is useful in the preliminary RAMS (Reliability, Availability, Maintainability, Safety) analysis and in the Security assessment of critical infrastructures. We propose an approach to investigate the network structure by ranking its elements through Importance and Sensitivity measures.

The System performances are referred to User nodes (Partial risks) and to the whole network (Global risk). The First order Differential Importance Measure and a so-called Hybrid measure allow the ranking of elements according to their Importance and to the Sensitivity of the model outputs. The ranking of Edges through the above measures super-imposes the ranking of the (unfaultable) User nodes.

The original proposals of the paper concern the use of the Total order Differential Importance Measures in order to consider the “interactions” among the independent input variables of the model (Edges unavailability) and the investigation of the system structure through the estimation of measures in the whole range of values [0;1]. The proposed approach is applied to a simple case study; the simplicity emphasizes the obtained results, allows judging them quantitatively and qualitatively and is not a limitation for real case applications.

1. Introduction

1.1. Networked system analysis

Several critical infrastructures—such as energy grids, communication systems, remote command-control system, auxiliary systems in complex (e.g. nuclear) power plants—are made up of components which are interconnected in a networked structure. The information coming from the topology of the network, which does not depend on the probabilities of failure and repair of its elements, is useful in the preliminary assessment of the RAMS (Reliability, Availability, Maintainability and Safety) performances and in the Security assessment of the infrastructure.

The limits of the available methods and the need of restricting the computational times for the analysis of networked system suggest the use of a framework that integrates different approaches in a problem-driven approach to solution; it may include elements of Complexity Science methods for the initial screening of the infrastructure vulnerabilities, Probabilistic Risk Analysis (PRA) methods for the quantitative scenario analysis and agent-based modeling for a deeper assessment of the screened scenario [1].

Graph-theoretical methods are widely used to infer the structural characteristics of large-scale network; their application allows the comparison among different network configurations and the identification of its critical elements. The focus is on network connectivity properties and not on the actual physical flow through it. Different “Centrality measures” can be used to obtain information about the network topology: Degree centrality [2,3], Closeness and Betweenness centrality [4], Information Centrality [5].

When looking at the safety, availability or vulnerability of a physical infrastructure, its elements are characterized by their reliability/availability and can be ranked through “Reliability centrality measures”; the network performances can be measured by the “Reliability efficiency” of the graph [6–8].

Sampling techniques can be used in order to investigate the change of the centrality measures or the change of the network “reliability efficiency” conditioned to the removal of one and more Edges [9,10]; this approach shows the interest in the assessment of the “interactions” introduced by the network structure, which manifest themselves for the simultaneous changes of the elements reliability/availability.

With reference to the above mentioned framework, Graph-theoretical methods are generally used for the initial screening of the infrastructure vulnerability. Because of their topological perspective, the use of the obtained results in the subsequent application of PRA methods could be not effective; indeed, PRA methods refer to

Abbreviations: DIM/^{II}DIM/^{T}D, First/Second/Total order Differential Importance Measure; MAUT, Multi-Attribute Utility Theory; MCS, Minimal Cut-set; MPS, Minimal Path-set; OAT, One At Time; PRA, Probabilistic Risk Analysis; RAMS, Reliability, Availability, Maintainability, Safety

* Corresponding author. Tel.: +390510391024.
E-mail address: s.larovere@niering.it (S. La Rovere).

0951-8320/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2012.06.013

risk figures, which are generally defined as the product between the probability of occurrence and the produced damage of the potential scenario. For instance, in several realistic applications the network has few source nodes that feed several user nodes; for the application of PRA methods, the system performance should be not referred to the existence/reliability of paths between each pair of nodes (as generally for Graph-theoretical methods), but to the damage produced in each degraded state of the system (i.e. configuration of the network after the failure of one or more Edges) by all the User nodes which are not more connected to a Source node.

The use of importance measures for the identification and ranking of the network vulnerabilities was suggested by different authors. "Traditional" importance measures (for instance, the Risk Achievement Worth) have been used, even though they are not additive [11,12]. A common value has been assumed for the reliability of elements subjected to failure and repair; it has been stated that the Importance ranking is the same even if the probability changes (keeping the same value for all component) [12]. Multi-Attribute Utility Theory (MAUT) has been used in order to quantify the damage produced by each scenario, according to the "values" of the decision-maker [12,15].

The use of Importance and Sensitivity measures, to infer the structural characteristics of networked systems, is also the matter of two previous works of the authors [16,17]. In the first work [16] we introduced the system performances in terms of Global and Partial risks, by taking into account explicitly the damage produced in each degraded configuration of the network. With respect to Graph-theoretical methods, the use of the above risk figures (as well as MAUT) facilitates the integration between the preliminary topological evaluations and the subsequent Probabilistic Risk Analysis. In order to rank the Edges and User nodes of the network, in the same paper we proposed the use of the First order Differential Importance Measure because of its additive property. In the second work [17], in order to consider the correlations among Partial risks introduced by network structure, we proposed the use of a first order sensitivity measure (so-called Hybrid measure). These One-At-Time (OAT) measures provide "local" information, which is referred to the "nominal" value of the input variables of the model. In both works, according to the approach originally proposed by Birnbaum [18] and previously adopted for networked systems analysis [12], a common value equal to 0.5 is assumed for the unavailability of elements subjected to failure and repair. The following paragraphs introduce the first order Importance and Sensitivity measures, according to our previous works [16,17].

Section 2 completes the description of the strategy proposed for the investigation of the structural characteristics of networked systems. The original contributions of the paper concern

- The use of the Total order Differential Importance Measures in order to take into account the "interactions" among the input variables of the model (Edges unavailability);
- the investigation of the systems structure through the estimation of Importance and Sensitivity measures in the whole range of values [0;1] of the Edges unavailability.

Section 2 also provides some general information about the execution of the analysis for realistic systems.

Section 3 provides the results coming from the application of the proposed strategy to a case study; the graph simplicity emphasizes the obtained results and allows judging them quantitatively and qualitatively.

1.2. Networked systems performances

Let us consider a networked system made up of unfaultable N_s "Source" and N_n "User" nodes, connected by N_c directed Edges subjected to independent failure and repair events. The state of each Edge is described by a binary variable: $x_i=0$ if the Edge is available, 1 elsewhere (x_i^s is the state of the Edge "j" in the state s of the system).

The Unavailability of Edge "j" (U_j) is the result of the failure and repair events. The state of the each User node "i" is described by a binary variable: $x_i=0$ if the node is connected to at least one Source node through at least one path made up of available Edges, 1 elsewhere.

The unavailability of the User node "i" (U^i) is the probability that it is not connected to a Source node and strictly depends upon the Structure of the network.

The weight w_i represents the damage produced when the User node "i" is not connected to a Source node. For each state of the System (configuration of the network), the whole damage is the weight w_s, defined as the sum of the weights of the non-connected User nodes.

The performances of the networked system are specified in terms of Partial and Global risks. The Partial risks are referred to User nodes; for each node, the Partial risk is the product between the weight w_i and its unavailability ($R^i=w_i \cdot U^i$). The Global risk is referred to the whole network; it is the sum over the states of the System of the product between the weight w_s and the probability Pr_s that the System is in that state. It corresponds to the sum over the User nodes of the related Partial risks [16]

$$R=\sum_{s=1}^{2^{Nc}} Pr_s \cdot w_s=\sum_{i=1}^{Nn} R^i=\sum_{i=1}^{Nn} w_i U^i$$

$$\text{where } Pr_s=\prod_{j=1}^{Nc} (U_j)^{x_j^s}(1-U_j)^{(1-x_j^s)} \tag{1}$$

1.3. First order differential importance measures for networked systems

In order to rank the elements of the networked system—Edges and User nodes—with respect to their Importance, we proposed the use of an OAT measure, named Differential Importance Measure.

In order to operate with an "additive" measure and to refer it to the whole networked system, the Differential Importance Measure (DIM) is referred to the Global risk, according to the Eq. (1).

The First order Differential Importance Measure (DIM) can be expressed under the hypothesis of Uniform change or Uniform percentage changes of the input variables of the model [19]. Generally, the measure assumes different values under the two hypotheses; the ranking of the input variables can differ in the two cases. If a common value is assumed for the Edges unavailability (see section 2.3), as proposed for the system structure investigation, the DIM assumes the same value under the two hypotheses.

The DIM for the Edge "j" with respect to the User node "i" turns out to be [16]

$$DIM_j^i=\frac{w_i \frac{\partial U^i}{\partial U_j}}{\sum_{i=1}^{Nn}\left(w_i \sum_{j=1}^{Nc} \frac{\partial U^i}{\partial U_j}\right)} \tag{2}$$

Eq. (2) provides the fraction of the total change in the Global risk that is due to the change in the unavailability of the Edge "j" (while the others are kept at their initial value), through the User node "i".

The measure is additive with respect to User nodes, allowing the ranking of Edges with reference to the whole network. In this case, the measure for the Edge "j" with respect to the whole network provides the fraction of the total change in the Global risk that is due to the change in the unavailability of the