Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 48-21 (2015) 314–319

Modular Approach for Probabilistic Safety Assessment of Systems with Multiple Failure Modes

D. Ionescu [*,**] **N. Brînzei** [*,**] **J-F. Pétin** [*,**]

[*] *Université de Lorraine, CRAN, UMR 7039, Vandoeuvre-lès-Nancy, Cedex, 54518, France*
[**] *CNRS, CRAN, UMR 7039, Vandoeuvre-lès-Nancy, Cedex, 54518, France*
(e-mail: {dorina-romina.ionescu, nicolae.brinzei, jean-francois.petin}@univ-lorraine.fr)

Abstract: Probabilistic safety assessment (PSA) becomes quite difficult for the complex systems with different failure modes that are represented by Markov processes characterized by a large number of states and transitions. In order to overcome the complexity of this problem, we propose to build the Markov processes corresponding to each failure mode separately and to assess it's safety by the theory of p-languages. Further we can use the choice operator to model the system that incorporates multiple failure modes and to assess its safety performances.

Keywords: Probabilistic safety assessment, modular analysis and modeling, Markov models, p-languages, control systems, failure modes.

1 INTRODUCTION

The deterministic approach in the context of safety assessment was rapidly supplemented by the development of probabilistic studies, referred to more commonly as PSAs. The PSA is used to identify and to analyse every possible situation and sequence of events that might affect the systems performances. A typical PSA involves acquiring an in-depth understanding and collecting a large volume of related information, identifying the events (some may be stochastic) and the states of the system, modeling the systems, assessment of the relationships between events and human actions and development of a database on the systems and components reliability of a specific plant.

In this paper, the interest is to realize a PSA of systems with multiple failure modes assuming that the order relationship between events occurrence is taking into account because:

- event occurrence may depend on previous occurrence of other events; *e.g.* dynamic control systems may prohibit an event occurrence according to a previous occurrence (or not) of some other events,
- the impact of a sequence of events s on the system failure may be different according to the scheduling of the event occurrence within the events sequence; e.g. event e_1 followed by event e_2 leads to an undesired event while e_2 followed by e_1 has no impact.

Therefore these systems will be represented as state-transition models. Especially in the context of control systems or dynamic reparable systems it is necessary to take in consideration the changes between the different modes of failure or when the systems turns back into a functioning state after having passed in a failure state, and not only the events combination which bring the system in a failed state.

Analysis of such models can be based on two complementary reasoning: states-based reasoning and events-based reasoning. State-based reasoning involve the calculus of the probabilities associated to the system states and a classical approach that can be considered is the Markov and semi-Markov processes (Csenki (1995), Hawkes and Sykes (1990), Perman et al. (1997)). Regarding the event-based reasoning, the goal is to determine the events sequences. Some approaches have been recently developed to determine the critical events sequences and some basic properties such as minimality and consistency have been proposed for dynamic reparable system (Bouissou (2006), Chaux et al. (2013)). However, these approaches are based on deterministic language theory and focus on the identification of a set of events sequences but present some limitations and divergences for the probabilistic assessment due to modeling and sequence calculus assumptions. In order to overcome that, the probabilistic languages (Garg et al. (1999)) (which are the stochastic approach of the languages theory) can be used to evaluate the probability of events sequences.

In the PSA studies the fact of working with complex systems that are characterized by different failure modes and taking in consideration the occurrence order of the events that bring the system in one of this failure mode lead to large state-transition models (with combinatorial explosion of state number). These kind of models are difficult to build but also difficult to analyse. Thus a classical way to alleviate the complexity of large models are the modular approaches, by decomposition of complex systems in subsystems.

2405-8963 © 2015, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2015.09.546

Numerous works in modular approach field (Hermanns (2002), Delahaye et al. (2010), Maraninchi (1992), Grumberg and Long (1991)) are focused on analyzing the systems that have a complex behavior as multiple failure modes, nominal functionning, switching between different failure modes, etc. and these kind of systems are very often encountered in the real life (e.g. control systems). Most of these approaches use a state-based reasoning that is useful for systems where the events occurrence order it is not important. Also, in the mentioned works, the modular approaches are used for systems design or for qualitative analyze and system properties verification but not for quantitative assessment.

The purpose of this paper is to provide an event-based modular compositional approach for the systems where the events occurrence order is important (and for which we are doing a probabilistic assessment). In order to take in consideration the events occurrences order we propose to use the events sequences that will be determined using the theory of probabilistic languages (p-languages).

The paper is organized as follows. In Section 2 we present our modular approach for the complex systems represented by multiple failure modes. This approach is illustrated in section 3 using a case study. Finally, section 4 presents the conclusions of this work and identifies some future research directions.

2 MODULAR APPROACH FOR PSA

The probabilistic safety assessment for a system with different failure modes becomes difficult to be realized when the system is represented by a large number of states and transitions. To overcome this inconvenient we propose a two step approach: firstly, to consider each failure mode separately and to realize a performance assessment for it and secondly, to integrate all failure modes in one model, using the choice operator (Garg et al. (1999)). The final outcome is the probabilistic assessment of events sequences belonging to the model that integrates all system failure modes.

2.1 Modelling and performance assessment for each Failure Mode

Firstly, each failure mode of the system is represented by a irreducible finite state automaton (FSA). Each FSA has only one equivalence class of states. Moreover this equivalence class is final, which means that it is not leading to any other class. In other words in the considered automata, there are no transient classes of states (in terms of graphs theory, the FSA is strongly connected). Given that the states of automaton are all accessible from any other state (they are positive recurrent), this property ensures that the stationary distribution of states' probabilities for the underlying stochastic process is unique. This stationary distribution of probabilities is obtained assuming that transition from current state to another state occurs at the end of the mean holding time in the current state. Thus considering only these times of jumps between states, an embedded discrete time Markov chain (DTMC) in a continuous time stochastic process is obtained. Consequently, the probability p_{ij} assigned to a transition (event) e_{ij} that starts from a given state x_i to another state x_j is given by the following relation:

$$\mathbb{P}(e_{ij}) = p_{ij} = \lambda_{ij}/\Sigma_{j\neq i}(\lambda_{ij}) \tag{1}$$

Therefore, according to Ionescu et al. (2014), the set of all events sequences that bring the system in a state x_i is called the sub-language L_i. This sub-language is defined on the alphabet of events Σ and it is a subset of the set of all possible events sequences Σ^* over Σ. It is determined using the lemma of Arden (Carton (2008)).

Arden Lemma 1. A sub-language L_i is the solution of the following equation:

$$L_i = L_i A + B \tag{2}$$

where A and B represent sub-sequences bringing the system in the state x_i (they are assumed to be known).

1. The only solution of the equation is $L_i = BA^*$ if $\varepsilon \notin A$, where ε is the empty sequence.
2. The solutions have the form $L_i = (B + C)A^*$ where $C \subseteq \Sigma^*$, if $\varepsilon \in A$.

For each state, x_i, of the system, the equation (2) can be written considering the sequences starting from all the other states $x_j \neq x_i$ and arriving in the state x_i by only one transition. The set of n equations (2) (where n is the number of system states) allow to obtain the analytic expression for the sublanguages L_i.

Calculating the probabilities for L_i we are able to analyse the probability that the system is in completely functional state, degraded state or failure state, in other words to assess the system safety.

Since the events probabilities and the sets of all events sequences $s = e_{12}e_{23}...e_{(n-1)n}$ that bring the subsystem in it's different states were determined we can use the p-languages theory (Garg et al. (1999)) in order to calculate the probabilities of the sequences (extracted from a sub-language L_i) that represent a specific interest for the PSA, by the following expression:

$$\mathbb{P}(se_{\Delta}) = \prod_{e_{ij}\in s} \mathbb{P}(e_{ij}), \forall s \in \Sigma^* \tag{3}$$

2.2 Integrate all the failure modes of the system using choice operator

As we have seen in the first part of our approach it is reachable to do a probabilistic safety assessment for a single failure mode. Because in the real life we are working with complex systems, the question is how to integrate different failure modes of a system in order to obtain a model that contains all of them.

Before seeing how the choice operator will contribute at the integration of different failure modes of a system, we will present some generalities about the p-languages theory within which the choice operator was defined.

2.2.1 Probabilistic languages

The theory of p-languages was developed by Garg et al. (1999) in order to model the stochastic discrete event systems (DES) behavior. A special event called "termination event", noted e_{Δ}, is used to represent the fact that the state of the system obtained after the occurrence of a