Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 48-7 (2015) 147–153

Modeling standby redundancies in repairable systems as guarded preemption mechanisms

Pierre-Yves Piriou, Jean-Marc Faure, Jean-Jacques Lesage

LURPA, ENS Cachan, Univ Paris-Sud, F-94235 Cachan, France
(e-mail: {pierre-yves.piriou; jean-marc.faure; jean-jacques.lesage}@lurpa.ens-cachan.fr).

Abstract: This paper proposes an extension of the BDMP (Boolean logic Driven Markov Processes) formalism for enriching its capabilities to model replacement and resumption mechanisms in repairable systems. The implicit assumptions made by the classical BDMP to describe these mechanisms are first highlighted. An analogy between standby redundancies management in critical systems and preemption mechanisms in concurrent systems is then proposed. This permits to formally define an extension of BDMP that allows several replacement and resumption mechanisms be specified. A case study illustrates the benefits of this proposal.

Keywords: Model Based Safety Analysis, Repairable component, Standby redundancy policies, Preemption, Boolean logic Driven Markov Process

1. INTRODUCTION

Component redundancy is a widely used design concept to improve safety of critical systems. It consists in duplicating a set of components of the system in order to increase the probability to achieve the aimed functions. For a standby redundancy, all the redundant components do not work simultaneously. The so called spare components are activated only if the so called main components are not able to perform their functions. When components are repairable, such a standby redundancy carries out two switching mechanisms: the replacement and the resumption. The triggering condition of these two mechanisms depend on a dysfunctional context. Hence, several redundancy policies may be defined for a given set of redundant components.

Safety analysis of a dynamic system basically consists in determining its most critical failure scenarios and assessing their probability of occurrence. These analyses are based on a model of the possible dysfunctional behavior. Boolean logic Driven Markov Processes (BDMP), defined in Bouissou and Bon (2003), is a promising modeling formalism with regard to its ability to capture the dynamic aspects that arise with complex systems. Indeed, it is well suited for dealing with repairable components, and one of its primitives (the trigger) allows to model standby redundancies (Carer et al. (2002)). Nonetheless, a unique redundancy policy can be translated through a BDMP trigger: the replacement occurs as soon as the main components fail, and the resumption occurs as soon as they are repaired. Moreover, the components which trigger these switching mechanisms are not represented in the model, and are then considered faultless.

This paper proposes an extension of the BDMP formalism for enriching its modeling capabilities. The extension aims to allow a modeling of standby redundancies more accurate than with the BDMP formalism. It mainly impacts the definition of the trigger primitive, in order to capture several redundancy policies, that can be specified as preemption mechanisms. Indeed, for concurrent systems, preemption consists in the interruption of a process, in a particular context, generally in order to trigger another process. Given that components can be seen as processes, a switching mechanism is similar to a preemption mechanism that occurs in a particular dysfunctional context.

What is above mentioned about BDMP formalism is developed and illustrated on a case study in section 2. Preemption in concurrent systems is next defined in section 3. This section also proposes an analogy with standby redundancies in critical systems. Section 4 introduces Guarded BDMP (GBDMP) as an extension of BDMP and illustrates its benefits on the case study introduced in section 2. Finally, concluding remarks are given in section 5.

2. PROBLEM STATEMENT

This section introduces first the case study illustrating the work. Secondly, it provides a recall on BDMP formalism and its benefits for performing Model Based Safety Analysis (MBSA). Finally, the modeling of standby redundancies by triggers is discussed, and illustrated on the case study.

2.1 Motivating example

The Coolant Feeding Water System (CFWS) is a crucial system of every nuclear power plant. It aims to supply cool water to the steam generator. Figure 1 provides a simplified view of this system that performs two subfunctions. First, three extraction pumps ($Ex1$, $Ex2$ and $Ex3$) provide a sufficient flow of cool water. Two out of the three must be available to fulfill the service requirements.

10.1016/j.ifacol.2015.06.486

Second, two redundant Feeding Turbo Pumps ($FTP1$ and $FTP2$) pressurize the cool water. At least one of these pumps must be faultless.

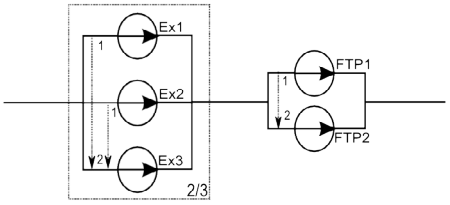

Fig. 1. A simplified view of the CFWS

Each component of this system can fail and be repaired, either in active or inactive mode. Furthermore, two different redundancy policies have been defined:

- When the main component ($Ex1$ or $Ex2$ for extraction pumps, and $FTP1$ for turbo pumps) is faulty and the spare component ($Ex3$ for the extraction pumps and $FTP2$ for the turbo pumps) is faultless, the main is replaced by the spare in both cases.
- The resumption conditions of the main component are not the same however. When an extraction pump is activated, it remains active until it fails; this implies that a main extraction pump is reactivated only if it has been repaired and the spare pump has failed. On the other hand, as $FTP1$ has better performances than $FTP2$, it is reactivated after a failure as soon as it has been repaired, even if $FTP2$ has not failed.

The objective of this work is to perform a MBSA of this system, that takes into account these two redundancy policies.

2.2 Recall on BDMP formalism

BDMP is a formalism defined in Bouissou and Bon (2003) to perform safety analysis of complex systems, and in particular repairable systems. A BDMP model can be implicitly defined as a multi-top coherent tree structure whose leaves are triggered Markov Processes. It is used to capture the failure scenarios of a critical system. To build such a model, the dysfunctional behavior of each component has first to be specified. It must be modeled by a trigger Markov process, that is defined as two Markov chains and two transfer matrices. One Markov chain specifies the dysfunctional behavior of the component in the active mode, and the other specifies its dysfunctional behavior in the inactive mode. A component can be activated or deactivated through the transfer matrices which give a probability distribution from the states of one chain to the states of the other. Figure 2 shows a representation (adapted from Bouissou and Bon (2003)) of a trigger Markov Process that specifies the behavior of a standard BDMP leaf (called SF leaf). λ_S, λ are failure rates and μ is a repair rate. It has been assumed that the failure rates are different in the two modes, and the repair rates are similar.

The system architecture is then translated into a fault tree. Activation and deactivation of a component are provoked by triggers that are defined from an origin node (leaf or logic gate output) to a destination one:

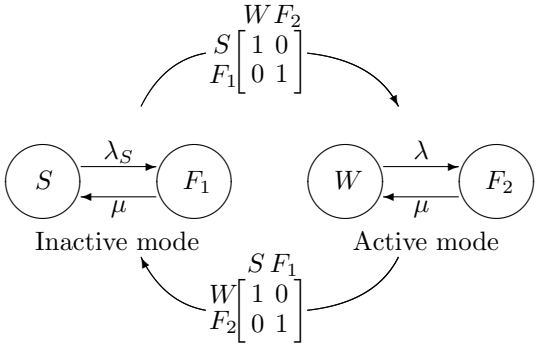

Fig. 2. Trigger Markov Process of the SF leaf

the destination is activated when the origin fails, and deactivated when the origin is repaired. A trigger is mainly used to model standby redundancies from the origin node to the destination one (cf. Carer et al. (2002)). The fault tree structure and the triggers determine the mode of each leaf, and the corresponding trigger Markov process determines its faulty status. Finally, the faulty status of each component is propagated through the fault tree to determine the occurrence of the top event.

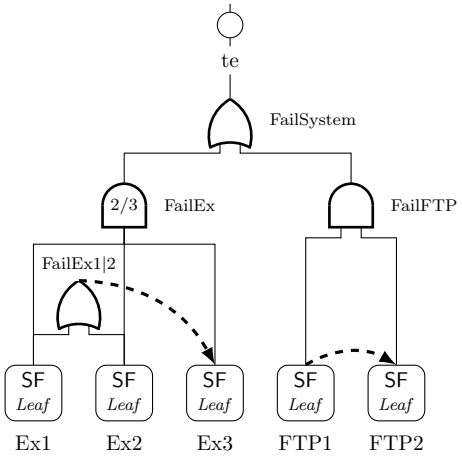

Fig. 3. BDMP model of the CFWS

The BDMP model of the CFWS is shown in Figure 3. It expresses that the system fails if 2 out of 3 extraction pumps or the 2 turbo pumps fail. The dysfunctional behavior of each pump is modeled by a SF leaf. The standby redundancies are modeled by the triggers:

- $Ex3$ is activated when $Ex1$ or $Ex2$ fails and is deactivated when the failed pump is repaired.
- $FTP2$ is activated when $FTP1$ fails and is deactivated when it is repaired.

BDMP has many benefits to perform MBSA. It is a tree-oriented formalism, easy to understand through its graphical representation. Moreover, trigger is an appropriate primitive to model standby redundancies.

BDMP formalism was initially developed for power plant applications, but is also used in other domains like computer security (Pietre-Cambacedes and Bouissou (2010), Kriaa et al. (2012)). Moreover Chaux et al. (2012) proposes a formalization of the BDMP semantics using finite state automata, in order to extract minimal cut sequences.