From Safety Analysis of Reconfigurable Systems to Design of Fault-Tolerant Control Strategies

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

From Safety Analysis of Reconfigurable Systems to Design of Fault-Tolerant Control Strategies

P.-Y. Piriou, J.-M. Faure, *Member, IEEE,* J.-J. Lesage, *Member, IEEE*

***Abstract*— The design of fault-tolerant control strategies requires a perfect knowledge of both the possible reconfigurations of the system and of the behavior of this system when failures occur. In this paper it is shown that the use of a model-based safety analysis (MBSA) framework, able to cope with repairable and reconfigurable phased-mission systems, is helpful for the choice of the best reconfiguration strategies to be implemented in the control system. The core of this approach is based on the integration of a model of the system structure (Fault Tree), a model of the dysfunctional behaviors of the components of the system (Switched Markov Processes) and a model of the reconfiguration mechanisms (Moore Machines). The syntax and semantics of the different models and their integration is first defined. The benefits of this approach for performance evaluation of fault-tolerant control strategies are afterwards illustrated through an application example.**

***Keywords*— Fault-tolerant control, reconfiguration strategies, model-based safety analysis (MBSA), Generalized Boolean logic Driven Markov Processes.**

I. Introduction

The design of fault-tolerant control strategies for automated industrial systems requires the precise knowledge of their dysfunctional behavior. The possible failures, their consequences in terms of functions loss or performance degradation, the reconfigurations that remain possible despite failures thanks to redundancies ... have to be studied in a step preliminary to the fault-tolerant control design [10].

Model-Based Safety Analysis (MBSA) technics are often used to perform this dysfunctional analysis but are classically limited to the analysis of dynamic failure mechanisms only ([5], [9]) without considering possible repairs of components. Including repairs in MBSA is nevertheless mandatory for lots of systems whose duration of the mission is over several years, like power plants and power distribution networks. Few modeling frameworks allow to model explicitly, in addition to the structure of the system, more or less complex dysfunctional behaviors of its components in terms of failures/repairs. To do that, Markov processes ([2]) or transition systems ([1], [6]) are well-suited.

Nevertheless, despite the benefits of these worthwhile contributions for a more accurate safety analysis, it remains difficult to model and analyze the impact of different reconfiguration strategies, e.g. to describe how the service is transferred from a main component (or subsystem) which has failed to one or several spare components (or subsystem(s)) and how the operation of the main component is resumed once it has been repaired. In fact, reconfiguration strategies can be complex when multi-state components are considered and deserve to be explicitly and formally described. Moreover, reconfiguration controls are performed by human operators or by automatic systems which may fail, and this failure can impact safety or performances [11]. However, up to now, explicit modeling of the reconfiguration strategies and of the failures of the control of these strategies has not been addressed in safety analysis.

The aim of this paper is to show how fault-tolerant control strategies can be designed, on the basis of the results of a dysfunctional analysis. To meet this objective, a new powerful MBSA formalism which allows to cope with dynamic repairable and reconfigurable systems is proposed.

The outline of the paper is the following. Section 2 presents briefly the syntax of Generalized Boolean logic Driven Markov Processes (GBDMP), the MBSA formalism we propose. The benefit of GBDMP for modeling repairable reconfigurable systems is illustrated on a case study at section 3. In section 4 we show how qualitative and quantitative safety analyses can be used for the design and the choice of reconfiguration strategies for fault-tolerant control. Finally, concluding remarks and perspectives are drawn up in section 5.

II. Generalized Boolean logic Driven Markov Processes (GBDMP)

A. Boolean logic Driven Markov Processes

Boolean logic Driven Markov Processes (BDMP) have been developed by EDF R&D [2] for safety analysis of systems whose components are repairable. To meet this objective, the structure of the system is modeled by a fault-tree that includes not only logical gates but also *triggers*. The triggers permit translating the redundancy mechanisms between main components and spare components (or subsystems). Moreover, the leaves of the tree are not basic events which can be represented by Boolean variables (like in classical fault trees) but a description of the failure/repair behavior of components in the form of Triggered Markov Processes (TMP) [2].

One may informally describe the dynamic behavior of a BDMP as follows: the state of each node of a BDMP (leaf or gate) n is characterized by two Boolean variables that represent its activation status M_n and its failure status F_n. The

P.-Y. Piriou is with Electricité de France, R&D, 78400 Chatou, France (e-mail : pierre-yves.piriou@edf.fr).

J.-M. Faure is with LURPA, ENS Cachan, Univ. Paris-Sud, Supmeca, Université Paris-Saclay, 94235 Cachan, France (e-mail : faure@ens-cachan.fr).

J.-J. Lesage is with LURPA, ENS Cachan, Univ. Paris-Sud, Université Paris-Saclay, 94235 Cachan, France (corresponding author, e-mail: lesage@ens-cachan.fr).

activation statuses are controlled by the triggers; when the origin of a trigger is faulty (respectively not faulty), the destination is required (respectively not required). Hence, a node is activated (M_n becomes *true*) if and only if it is required and at least one of its fathers in the tree is activated, assuming that the top event is always active. The failure status of a gate is computed from the failure statuses of its sons like in classical fault tree analysis.

The concept of trigger that is introduced by the BDMP framework is a first attempt to model reconfiguration. Nevertheless, this modeling primitive presents three significant limitations:

- First, it is possible to model only one reconfiguration strategy: the destination of the trigger is activated as soon as the origin of the trigger fails and is deactived as soon as the origin is repaired. This strategy is not the only one which is used in practice, however [12].
- Second, the models of components (leaves of the fault tree) include only two operation modes: working and standby. Nonetheless, real components of critical systems may have more than two modes, for instance a standby mode, a normal mode and an overspeed mode, the latter one being a solution to perform the service during a limited time when the component is the only faultless one that remains.
- Last, possible failure of the trigger is not considered. It is assumed indeed that, when the origin of a trigger fails, the trigger always sends to its destination a request to go to the working operation mode. This is unfortunately not always true in practice, and especially when the trigger is implemented by an automatic system that comprises electronic boards, relays, etc. which may fail.

To overcome these limitations (restricted number of reconfiguration strategies, of operation modes, failure of the control of the reconfiguration not considered) a novel framework is defined in the next section.

B. Generalized BDMP (GBDMP) definition

Generalized BDMP have been defined from BDMP by replacing first the concept of trigger by that of switch whose behavior is described by a Moore machine [8]; complex reconfiguration strategies can then be modeled. Moreover, TMP are replaced by SMP (Switched Markov Processes) to model components with more than two operation modes. Last, control of the reconfiguration strategies is explicitly modeled by introducing the concerned control components in the modeling of the structure. These new components are connected to switch inputs; hence, the impact of their failures can be now considered.

The bases of the syntax and the semantics of GBDMP are now briefly given by using a simple example.

Definition 1. A Generalized Boolean logic Driven Markov Process is a 6-tuple $<V, E, \kappa, \upsilon, str, smp>$ where:

- $V = N \cup S = G \cup L \cup S$ *is a set of vertices partitioned into the nodes N (i.e. the gates G and the leaves L) and the switches S;*
- $E = E_F \cup E_S$ *is a set of oriented edges, such that* $E_F \subseteq G \times N$ *and* $E_S \subseteq (N \times S) \cup (S \times N)$*;*
- $\kappa: G \rightarrow \mathbb{N}^*$ *is a function that determines the gates kind. This function is the same as the one used in BDMP [2];*
- $\upsilon: E \rightarrow \mathbb{N}$ *is a function that associates an integer label to each edge;*
- $str: S \rightarrow \mathbb{M}$ *is a function that associates a Moore machine (which represents a reconfiguration strategy) to each switch.* $\mathbb{M}$ *designates the set of Moore machines;*
- $smp: C \rightarrow \mathbb{P}$ *is a function that associates a SMP to each component (a k-SMP for a component with k operation modes).* $\mathbb{P}$ *designates the set of Switched Markov Processes.*

A simple GBDMP is shown at Figure 1. The structure of the system is represented by a fault tree (part a of Figure 1). It is composed of 3 gates (*G1* is an AND gate, *G2* and *G3* are OR gates), 3 basic components (leaves *C1*, *C2* and *C3*) and a switch (*S1* depicted with a dashed rectangle). The solid (resp. dashed) arrows are the edges of E_F (resp. E_S), which connect the gates to the nodes (resp. the switches to the nodes and the nodes to the switches). The dysfunctional behavior of the leaves *C1*, *C2* and *C3* is depicted by the SMP "Pu" at part b of Figure 1. The component *C4* is in charge of the control of the switch, its dysfunctional behavior is depicted by the SMP "Co" at part b of Figure 1. The reconfiguration strategy implemented in switch *S1* is modelled by the Moore machine at part c of Figure 1. The label, calculated by function υ, of an edge of E_F (resp. E_S) permits to associate an edge to an operation mode of a leaf (resp. to associate a number of input or output of the Moore machine to a node).

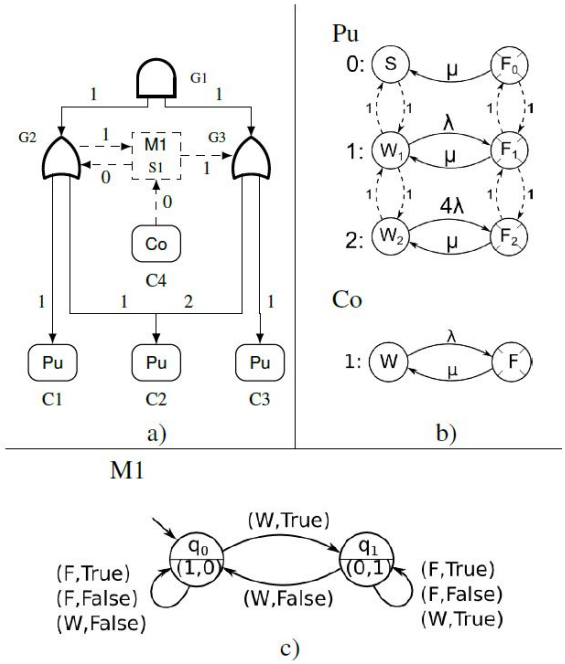


Figure 1: Example of GBDMP. a) Structure modelling; b) SMP *Pu* (associated with *C1*, *C2* and *C3*) and *Co* (associated with *C4*); c) Moore machine *M1* (associated with *S1*)

The behavior of a leaf is modeled by a k-SMP which is composed of k Markov chains. Each Markov chain corresponds to an operation mode and comprises faultless and faulty states; the transitions between these states are stochastic because they model failures and repairs. In the example of Figure 1 b, the 3-SMP associated with the leaves *C1*, *C2* and *C3* comprises three Markov chains (one for each line) to represent a component with two working modes and one standby mode; in this model, it is assumed that no failure occurs in the standby mode and that the failure rate in the second working mode is greater than the corresponding rate in the first working mode. $k(k-1)$ probabilistic transfer functions between the chains of a k-SMP must be defined. The value of the transfer function between two states of two different chains (in dashed arrows) is equal to 1 if no failure on-demand is considered (case of Figure 1 b) when the operation mode is changed and belongs to [0,1] otherwise.

The role of a switch is to set/reset the requirement statuses of the nodes that are connected to its outputs according to the values of its inputs and the reconfiguration strategy which is described by the associated Moore machine. In the Moore machine *M1* at Figure 1c, let q_0 be the current state. In this state, *C1* is activated in operation mode 1, *C2* is activated in operation mode 1 and *C3* is deactivated. The transition between state q_0 and state q_1 is fired if the associated condition "(W,*True*)" is true, i.e. if the SMP of *C4* (input #0 of *S1*) is in state W and if the output of Gate *G2* (input #1 of *S1*) is *True*. The firing of this transition implies the change of active state of *M1* (which becomes q_1) and the change of outputs values: the requirement status of *G2* (output #0 of *S1*) is reset and the requirement status of *G3* (output #1 of *S1*) is set. As a consequence, *C1* is deactivated, *C2* is activated in operation mode 2 and *C3* is activated in operation mode 1.

III. Dysfunctional Modelling of Reconfigurable Systems with GBDMP

A. A case study: coolant feeding system

In order to illustrate our approach, the system depicted in Figure 2 is used. It is a very simplified version, proposed by Company Electricité de France, of a part of the cooling system of nuclear power plants. Its main function is to feed a downstream system with a cooling fluid by using two groups of pumps. The first group of three pumps is powered by a heavily redundant electric power supply whose components are repairable. The system fails when fluid can no more be provided. Three stages of electric energy supply and two pumping stages can be identified:

- An electric transformer *Tr1* (A) connected to the grid, is used to provide low voltage electricity; if it fails, a second transformer *Tr2* is available thanks to a standby redundancy;
- A distribution board *TEb1* (B) powering a second distribution board *TEa1* (D) using one of the two transformers *Tr1* or *Tr2*. A diesel generator *Di1* (C) is in standby redundancy with subsystem *TEb1*;
- The lower level distribution board *TEa1* (D) powers the group of extraction pumps *Ex1*, *Ex2* and *Ex3* (E), using one of the two possible sources (*TEb1* or *Di1*);
- The fluid is extracted by the group of pumps *Ex1*, *Ex2* and *Ex3* (E). Only two pumps are used during operation, if one pump fails the third one is activated (standby redundancy 2 out of 3);
- Pumps *Pr1* and *Pr2* (F) pressurize the fluid; only one pump is used during operation, if the main pump *Pr1* fails the spare pump *Pr2* is activated (standby redundancy 1 out of 2).

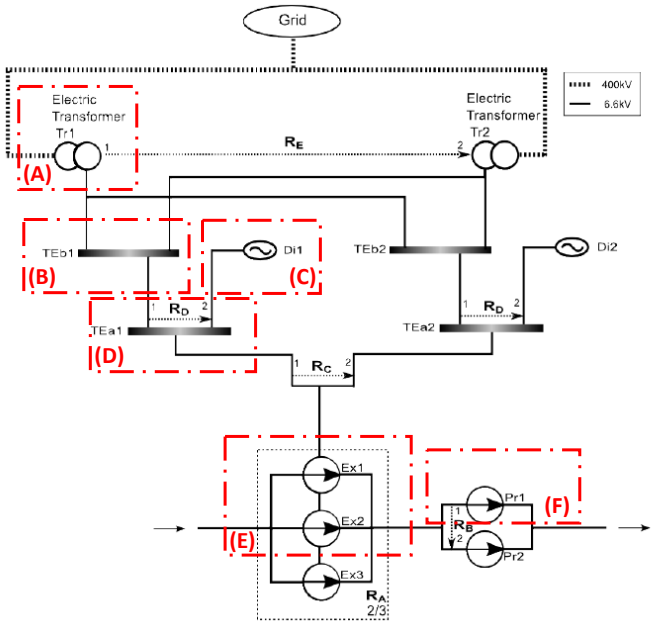


Figure 2: Physical architecture of the coolant feeding system

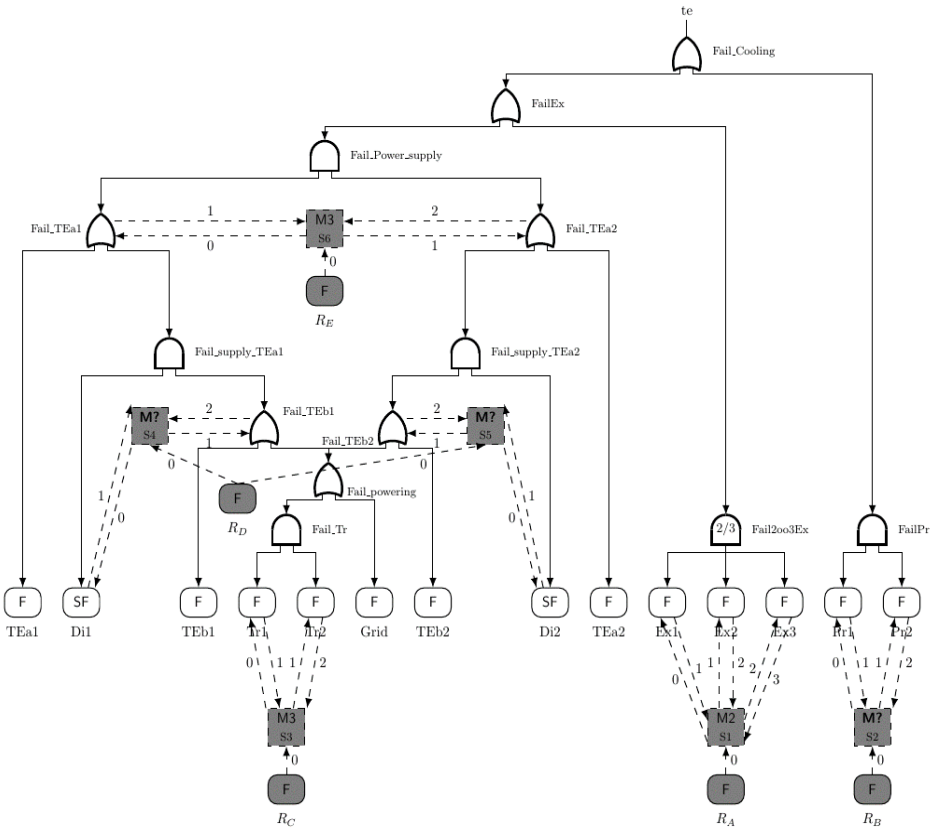
The subsystem {B, C, D} is duplicated in order to provide a standby redundancy for powering the extraction pumps. We consider that components can only fail when they are active, except diesel generators which may fail when they are in standby.

Thanks to the multiple redundancies, lots of reconfigurations are possible in this system for maintaining the production, even in case of multiple failures of components.

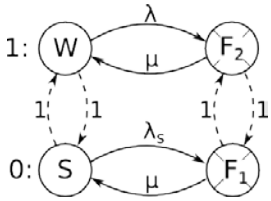
The first problem to solve before designing fault-tolerant control laws is therefore to determine the "best" reconfiguration strategies, in terms of productivity, safety or dependability for example. A method to search these best reconfiguration scenarios by performing a safety analysis of the system by using GBDMP is presented below.

B. GBDMP model of the case study

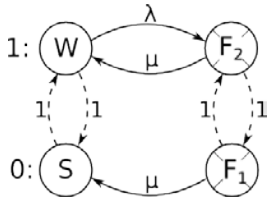
The GBDMP of Figure 3 models the possible dysfunctional behaviors of the coolant feeding system depicted at Figure 2. Each one of the 14 components (including the grid) is associated with a leaf of the GBDMP. Components that may fail in working mode and in standby mode are associated with a leaf of type SF ("Standby Failure", the corresponding SMP is given in Figure 3b); components



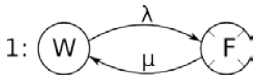
a) Fault tree of the GBDMP



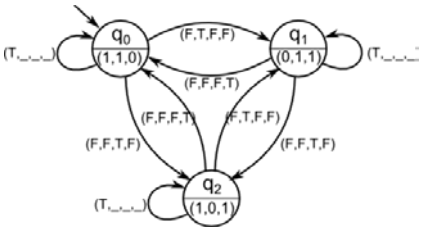
b) SMP associated with a leaf of type *SF*



c) SMP associated with a leaf of type *F*

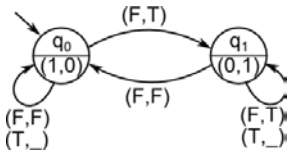


d) SMP associated with a leaf of type Co



e) Moore machine associated with switches type *M2* : "2 out of 3, latest replacement, latest resumption"

f) Moore machine associated with switches type *M3* : "1 out of 2, latest replacement, latest resumption"



g) Moore machine associated with switches type *M4* : "1 out of 2, earliest replacement, earliest resumption"

Figure 3: GBDMP of the coolant feeding system

that may fail only in working mode are associated with a leaf of type F (“simple Failure”, the corresponding SMP is given in Figure 3c). The structure of the system that makes that certain ordered combinations of fail and repair events of components lead to the global failure (*te*) is given by the fault tree Figure 3a.Each time a redundancy between several components has to be managed, a switch is introduced. The reconfiguration strategy which is chosen for each switch (and whose relevance has to be evaluated before designing a fault-tolerant control algorithm) is modeled by a Moore machine, associated with this switch. Three kinds of switches are used in this study case (an exhaustive study of the reconfiguration strategies has been proposed in [12]). Switches of type *M3* express a strategy "1 out of 2, latest replacement, latest resumption" (replacement occurs when the main component fails if the spare component is available, and resumption occurs when the spare fails if the main is available - the corresponding Moore machine is given in Figure 3f); switches of type *M4* express a strategy "1 out of 2, earliest replacement, earliest resumption" (resumption occurs as soon as the main component is available without waiting for a failure of the spare - the corresponding Moore machine is given in Figure 3g); switches of type *M2* express a strategy "2 out of 3, latest replacement, latest resumption" (the corresponding Moore machine is given in Figure 3e). Finally, a control equipment in charge of executing the reconfiguration is associated with each switch; it is considered that a control equipment has a unique working operation mode in which it may fail (type *Co* for the leaves R_A to R_E depicted by grey boxes at Figure 3a – the corresponding SMP is given in Figure 3d).

In what follows, the best strategies for *S2*, *S4* and *S5* are now going to be searched by performing a safety analysis on the GBDMP model. Once these reconfiguration strategies will be chosen, they will be important input data for fault-tolerant control design.

IV. FROM SAFETY ANALYSIS TO FAULT-TOLERANT CONTROL

Once a dysfunctional model of the system has been built, two kinds of safety analysis are classically performed. *Quantitative analysis* consists in calculating the probability of the global failure of the system (the probability of occurrence of the top event); *qualitative analysis* consists in calculating the set of Minimal Cut Sequences (MCS), i.e. the minimal set of sequences (composed of failure/repair events) of minimal length that are necessary and sufficient to describe the whole set of cut sequences [4]. These two kinds of analysis give complementary results and both are useful for choosing the most efficient reconfiguration strategies for fault-tolerant control purposes. For sake of clarity and due to the lack of space, the interest of qualitative analysis will be illustrated through the choice of the reconfiguration performed by switch *S2* and the benefits of quantitative analysis will be illustrated through the choice of the reconfiguration performed by switches *S4* and *S5*.

A. Qualitative analysis for switch S2

The calculus of MCS for dynamical repairable systems is a difficult problem leading to a combinatorial explosion of the state space to explore; nevertheless an efficient approach has been proposed for BDMPs in [3]. The corresponding algorithm has been extended to GBDMP and implemented in a prototype tool named SAGE (Safety Analysis in a GBDMP Environment). This tool includes also an interactive graphical interface for the simulation of GBDMP models. SAGE has been used for the qualitative and the quantitative analyzes of the different scenarios envisaged in the sequel of the paper.

The failure event (resp. the repair event) of a component "*comp*" is denoted f_{comp} (resp. r_{comp}). Thus: $f_{Pr1}f_{R_B}r_{Pr1}$ expresses the sequence of failure/repair events where the pump *Pr1* fails first, then the control equipment in charge of switch *S2* fails, then pump *Pr1* is repaired.

Pumps *Pr1* and *Pr2* are in standby redundancy 1 out of 2; the switch in charge of the management of this redundancy is *S2*, it is controlled by R_B. Even if a classical replacement strategy is chosen (the replacement occurs when the main component fails if the spare component is available) two strategies are possible for the resumption: "resumption at the latest" (resumption occurs when the spare fails if the main is available - see the corresponding Moore machine in Figure 3f) or "resumption at the earliest" (resumption occurs as soon as the main component is available - see the corresponding Moore machine in Figure 3e). The computed MCS of length 2 to 4 for both resumption strategies are given in table 1.

TABLE I. TWO RECONFIGURATION STRATEGIES FOR S2 AND THE CORRESPONDING MCS

Switch S2 type	***"resumption at the latest"***	***"resumption at the earliest"***
Corresponding MCS of length 2 to 4	$f_{Pr1}f_{Pr2}$ $f_{R_B}f_{Pr1}$ $f_{Pr1}f_{R_B}r_{Pr1}f_{Pr2}$ $f_{Pr1}r_{Pr1}f_{R_B}f_{Pr2}$	$f_{Pr1}f_{Pr2}$ $f_{R_B}f_{Pr1}$ $f_{Pr1}f_{R_B}r_{Pr1}f_{Pr2}$

Each one of the MCS expresses a possible failure scenario of the system. The shorter the MCS, the higher its impact on system dependability in terms of number of failure events that is sufficient for leading to the global failure. Of course the length of a MCS cannot be directly translated in a probability of failure, but the knowledge of the set of MCS brings to the engineers a very important feedback about the robustness of the system structure.

In table I, the first MCS of length 2, which is common to the two reconfiguration strategies, expresses the following scenario: the pump *Pr1* fails first (*S2* switches on pump *Pr2*) then the pump *Pr2* fails, what leads to the failure of *te*. The first MCS of length 4 is also common to the two strategies. Note that this MCS includes a repair event and can only be obtained if a model like GBDMP is used for performing a MBSA. This MCS expresses that pump *Pr1* fails first (*S2* switches on pump *Pr2*) then the controller R_B fails, so even if *Pr1* is repaired (r_{Pr1}) it is no more possible to switch on pump *Pr1* when *Pr2* fails (f_{Pr2}).

The use of a reconfiguration strategy "resumption at the latest" for switch *S2* introduces an additional MCS of length 4: $f_{Pr1}r_{Pr1}f_{R_B}f_{Pr2}$, that expresses the following scenario: pump *Pr1* fails first (*S2* switches on pump *Pr2*) then *Pr1* is repaired (but *S2* doesn't switch on pump *Pr1*), then the controller R_B fails, so when *Pr2* fails (f_{Pr2}) it is no more possible to switch on pump *Pr1*.

This qualitative safety analysis shows that a "resumption at the latest" strategy introduces an additional scenario of possible failure. Nevertheless, as mentioned before, the knowledge of MCS only cannot be directly translated in terms of availability or reliability of the system. Before choosing the best reconfiguration strategies it is therefore necessary to additionally perform a quantitative analysis.

B. Quantitative analysis for switches S4 and S5

For studying the relevance of quantitative safety analysis for choosing efficient reconfiguration strategies, the case of switches *S4* and *S5* is studied. The specificity of the two diesel groups *Di1* and *Di2* is that they may fail both in working mode (failure rate λ) and in standby mode (failure rate λ_S), as described in Figure 3b.

A simulation of the unavailability rate of the coolant feeding system is given in Figure 4. In this simulation, the evolution of the probability of *te* is calculated for a mission time of 2000 hours by exploring two scenarios:

- A resumption strategy "at the latest" (resumption occurs when the spare fails if the main is available – switch type *M3* in Figure 3f) is chosen for *S4* and *S5*;
- A resumption strategy "at the earliest" (resumption occurs as soon as the main component is available – switch type *M4* in Figure 3g) is chosen for *S4* and *S5*;

For sake of confidentiality, unrealistic values have been chosen for failure/repair rates for the processing of these two scenarios: λ = 1 E-3 h^{-1}, λ_S = 1 E-4 h^{-1} and μ = 1 E-1 h^{-1}. If a resumption strategy "at the latest" is chosen for *S4* and *S5*, the resulting asymptotic unavailability is U_{M3} = 5.42 E-4 (solid curve at Figure 4). If a resumption strategy "at the earliest" is chosen for *S4* and *S5*, the resulting asymptotic unavailability is U_{M4} = 5.82 E-4 (dashed curve at Figure 4).

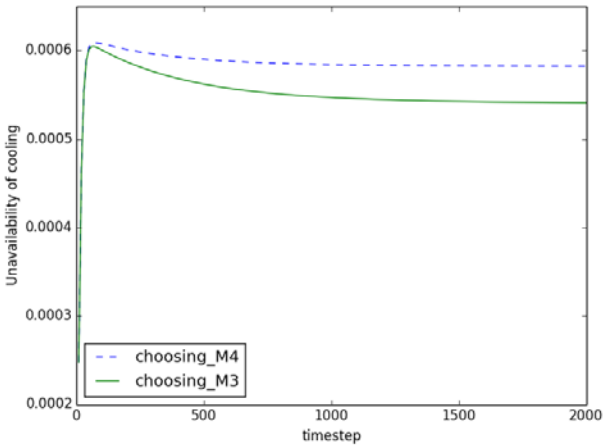


Figure 4: Influence of the choice of the resumption strategy for *S4* and *S5* on the unavailability of the coolant feeding system

The presence of peaks at the beginning of both curves can be explained as follows. As long as the electric supply by the grid works, the diesel groups are inactive but they may fail in their standby mode since they are associated to SMP of type SF (Fig. 3b). When the electric supply by the grid fails, diesel generators are switched on the working mode and the components connected to the grid (TEij, Trk, ..., see Fig. 2) are switched on the standby mode, but these components cannot fail since they are associated to SMP of type F (Fig. 3c). Consequently, the impact of the lack of failures of the components in standby mode onto the unavailability rate of the cooling system is larger when mission time increases (because diesels can be switched on) than at the beginning of the simulation (because diesels are assumed to be switched off). The decreasing of the unavailability rate of the system due to this phenomenon is even larger for a resumption strategy "at the latest" (switches type M3) because after switching, diesels remain in working mode as long as they are available.

By performing such a qualitative or/and quantitative safety analysis for the whole system, it is therefore possible to find the best reconfiguration strategy for each one of the switches, and consequently to exploit as better as possible the redundancies that make possible the system operation despite failures. Based on the reconfiguration strategy fixed for each switch, fault-tolerant control laws can then be designed as proposed in [7], [13] for example.

V. Conclusion

In this paper it has been shown the interest to perform model-based safety analysis of repairable and reconfigurable systems before designing a fault-tolerant control. The GBDMP model we propose allows to formally represent the redundancies and reconfiguration strategies in the system that can be exploited by fault-tolerant control. By performing a qualitative and/or a quantitative safety analysis based on this model, it is possible to choose the best replacement strategies of failed components and the best resumption strategies when components are repaired. Doing so, reconfiguration strategies to be implemented in the control system can be selected after being evaluated in terms of safety impact.

Other possible benefits of the presented approach have not yet been exploited. For example, the choice of replacement/ resumption strategies has been performed on the basis of possible critical scenarios of failures (the MCS). These failures have therefore to be monitored during operation of the system thanks to an online diagnosis. From the other hand, the Moore machines associated with the switches in charge of the reconfigurations in the system are part of the control and have to be integrated in the fault-tolerant control laws.

The integration between the MBSA approach we presented in this paper, the design of fault diagnosis and the design of fault-tolerant control laws are on-going works.

Acknowledgment

This work is funded by the French Investment of Future Program: Generic Components of Embedded Software as part of the CONNEXION project.

References

[1] M. Batteux, T. Prosvirnova, A. Rauzy, L. Kloul, *The altarica 3.0 project for model-based safety assessment*, in: Proc. 11th IEEE International Conference on Industrial Informatics (INDIN'2013), Bochum (Germany), July 2013, pp. 741–746.

[2] M. Bouissou, J.-L. Bon, *A new formalism that combines advantages of fault trees and markov models: Boolean logic Driven Markov Processes*, Reliability Engineering & System Safety, 2003(2), pp.149–163.

[3] P.-Y. Chaux, J.-M. Roussel, J.-J. Lesage, G. Deleuze, M. Bouissou, *Systematic extraction of Minimal Cut Sequences from a BDMP model*, in: Proc. 21th European Safety & Reliability Conf. (ESREL'12), Helsinki (Finland), June 2012, 8 pages.

[4] P.-Y. Chaux, J.-M. Roussel, J.-J. Lesage, G. Deleuze, M. Bouissou, *Towards an unified definition of minimal cut sequences*, in: Proc. 4th International Workshop on Dependable Control of Discrete Systems (DCDS 2013), York (UK), September 2013, 6 pages.

[5] J.-B. Dugan, S.-J. Bavuso, M.-A. Boyd, *Dynamic fault-tree models for fault-tolerant computer systems*, IEEE Transactions on Reliability, 1992 41(3), pp. 363-377.

[6] M. Gudemann, F. Ortmeier, *A Framework for Qualitative and Quantitative Formal Model-Based Safety Analysis*, in: Proc. IEEE 12th International Symposium on High-Assurance Systems Engineering (HASE 2010), San Jose (California - USA), 2010, pp. 132-141.

[7] J. Lunze, J.H. Richter, *Reconfigurable Fault-tolerant Control: A Tutorial Introduction*, European Journal of Control, 2008(5), pp. 359-386.

[8] E.-F. Moore, *Gedanken-experiments on sequential machines*, Annals of Mathematical Studies, 1956(34), pp. 129-153.

[9] Y. Papadopoulos, M. Walker, D. Parker, E. Rde, R. Hamann, A. Uhlig, U. Grtz, R. Lien, *Engineering failure analysis and design optimisation with HiP-HOPS*, Engineering Failure Analysis, 2011, 18(2), pp. 590-608.

[10] R. Patton, *Fault-tolerant control*, Encyclopedia of Systems and Control, 2015, pp. 422-428.

[11] P.-Y. Piriou, J.-M. Faure, J.-J. Lesage, *Control-in-the-loop Model Based Safety Analysis*, in: Proc. 24th European Safety & Reliability Conference (ESREL'14), Wroclaw (Poland), 2014, pp. 655-662.

[12] P.-Y. Piriou, J.-M. Faure, J.-J. Lesage, *Modeling standby redundancies in repairable systems as guarded preemption mechanisms*, in: Proc. 5th International Workshop on Dependable Control of Discrete Systems (DCDS 2015), Cancun (Mexico), May 2015, pp. 147-153.

[13] S. Shu, F. Lin, *Fault-Tolerant Control for Safety of Discrete-Event Systems*, IEEE Trans. On Automation Science and Engineering, 2014, 11(1), pp. 445-463.