Control-in-the-loop Model Based Safety Analysis

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

Control-in-the-loop Model Based Safety Analysis

P.-Y. Piriou & J.-M. Faure & J.-J. Lesage
Automated Production Research Laboratory
Ecole Normale Superieure, Cachan, France

ABSTRACT

In most cases, Model Based Safety Analysis (MBSA) of critical systems focuses only on the process and not on the control system of this process. In this paper, we claim that, for complex controlled systems, not only the process but the whole closed-loop system Process/Control must be considered to perform a relevant MBSA. As one of the aim of the control system is to manage the numerous switching mechanisms that must be introduced in the process to ensure fault tolerance, mission phase changes, maintenance based on auto-test… The correct achievement of these mechanisms depends indeed on the state (faulty or faultless) of control system components. Hence, a qualitative or quantitative safety analysis which considers both the process and the control provides more realistic results by integrating the faults of the control system components that manage the above-mentioned switching mechanisms.

This claim is exemplified on an industrial case study issued from a power plant: the coolant feeding system. The considered process is very critical and includes numerous passive redundancies; moreover, since the lifespan of this system is equal to several decades, each component must be repairable. This process is controlled by a classical control system where some components are also redundant. First, the faulty behavior is modeled by a BDMP (Boolean logic Driven Markov Process) which is the unique formalism suitable to the modeling of systems with repairable components, as detailed in Bouissou & Bon (2003). The BDMPs obtained for the process in isolation and for the closed-loop Process/Control are then translated into finite state automata from which the Minimal Cut Sequences (MCS) are derived, as described in Chaux et al. (2012). The comparison of these two sets of minimal cut sequences shows the benefit of the control-in-the-loop approach. New sequences that combine failures of both process and control components are obtained in this case.

Figure 1 depicts the main steps of the comparative study performed in this paper.

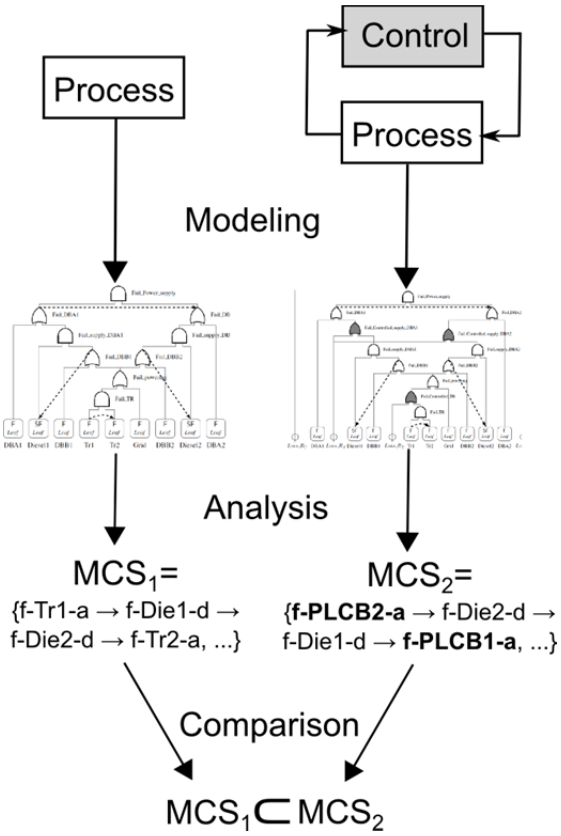

Figure 1. Main steps of the study.

REFERENCES

Bouissou, M. & Bon J.-L. 2003. A new formalism that combines advantages of fault trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering and Systems Safety* 82(2), pp. 149–163.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. June 2012. Systematic extraction of minimal cut sequences from a BDMP model. In *21th European Safety & Reliability Conference*, Helsinki (Finland). Session 16B, 8 pages.

Control-in-the-loop Model Based Safety Analysis

P.-Y. Piriou & J.-M. Faure & J.-J. Lesage
Automated Production Research Laboratory
Ecole Normale Superieure, Cachan, France

ABSTRACT: In most cases, Model Based Safety Analysis (MBSA) of critical systems focuses only on the process and not on the control system of this process. For instance, to assess the dependability attributes of power plants, only a model (Fault Tree, Markov chain...) of the physical components of the plant (pumps, steam generator, turbine, alternator...) is used. In this paper, we claim that for repairable and/or phased-mission systems, not only the process but the whole closed-loop system Process/Control must be considered to perform a relevant MBSA. Indeed, a part of the control functions aims to handle the dynamical mechanisms that change the mission phase as well as manage repairs and redundancies in the process. Therefore, the achievement of these mechanisms depends on the functional/dysfunctional status of the control components, on which these functions are implemented. A qualitative or quantitative analysis method which considers both the process and the control provides consequently more realistic results by integrating the failures of the control components that may lead to the non-achievement of these mechanisms. This claim is exemplified on an industrial study case issued from a power plant. The system is modeled by a BDMP (Boolean logic Driven Markov Process), assuming first that the control components are faultless, i.e. only the faults in the process are considered, and afterwards that they may fail. The minimal cut sequences of the system are computed in both cases. The comparison of these two sets of minimal cut sequences shows the benefit of the second approach.

1 INTRODUCTION

Model-Based Safety Analysis (MBSA) can be defined as "an approach in which the system and safety engineers share a common system model created using a model-based development process" (Joshi et al. (2006)). MBSA performed for critical controlled systems are most often applied on a model of the process alone. This is the case for example in Chaux et al. (2012) and Sondermann-Woelke et al. (2012). In particular, the last publication highlights the role of control for the application of redundancies, but does not consider control failures. These approaches take into account mechanisms of reparations and redundancies in the plant but they omit that the functions which manage these mechanisms can fail, as well as the components which support them. Two kinds of control failures can then be distinguished: software and hardware based. This paper does not consider the software failures because they can be avoided (or at least limited) by using one of the numerous existing formal verification techniques, like for instance model checking (more details on this issue may be found in Berard et al. (2001)). But with the increase of the digital components in complex controlled systems, dependability studies performed for these systems cannot underestimate probable failures of the control components. Indeed, even if these components have a good reliability, their failures remain possible, especially when the concerned systems have a long lifespan. Moreover, new studies integrate more and more injuries whose causes are external (fire, flood, terrorist attacks...). These injuries concern the plant components as well as those of the controller without distinction between them. Hence control should be considered in the loop for MBSA practices, and this paper aims to show that this issue carries significant consequences on both the modeling and the results.

Indeed, the more complex the system is the more switching mechanisms appears in the controlled process (due to fault tolerance, mission phase changes, maintenance based on auto-test...). These switching mechanisms are handled by functions implemented into components of the control. Therefore, the achievement of these mechanisms depends on the ability of the control components to perform them. Hence, the failure of the control components may

lead to the non-achievement of these mechanisms, what may have a significant influence on the results of a qualitative MBSA. Moreover, the formalism for performing MBSA are generally not made for taking into account the loss of these switching mechanisms.

In order to illustrate this issue, the paper considers an industrial controlled system on which a comparison study is performed. First the system failure is represented by a model that complies with the BDMP formalism. Second, the minimal cut sequences are extracted from this model. Section 2 describes the case study and gives the definition of the BDMP formalism. Section 3 applies the MBSA stated above while considering only the process failures. Then a control architecture is described, and added to the model in section 4. For integrating these new failures in the model, three models are proposed and discussed. In the same section, the set of minimal cut sequences is updated, and compared with the previous one. This comparison shows that the control failures have a significant influence on the qualitative analysis of the system. Finally, the last section draws up concluding remarks and outlooks.

2 BACKGROUND

This section introduces the case study used in this paper and recalls the basics of the BDMP formalism.

2.1 *The coolant feeding system*

In order to exemplify our claim, we consider the case study presented in Chaux et al. (2012). It is a coolant feeding system issued from a power plant. Its purpose is to supply cooling fluid to the steam generator. It is composed of two redundant groups of pumps, and a strongly redundant power supply (Figure 1). The two groups of pumps are series-connected and the first one is powered by the power supply. The power supply of the second group of pump is not considered here.

Six kinds of components can be identified:

- The Grid (Grid) is the source of electricity supply.
- The electric Transformers (Tr1 and Tr2) decrease the voltage (from 400kV to 6.6kV).
- The Distribution Boards (DBA1, DBA2, DBB1 and DBB2) transfer the electricity from their inputs to their output.
- The Diesel generators (Diesel1 and Diesel2) are other possible sources of electricity supply.
- The Extraction pumps (Ex1, Ex2 and Ex3) provide a sufficient flow of cooling water.
- The Feeding Turbo Pumps (FTP1 and FTP2) pressurize the cooling water.

All the components may fail and be repaired. The diesel generators and the pumps may fail not only when they are active but also when they are dormant. The system fails when its supply function cannot be achieved. To avoid this general failure, several redundancies are defined:

- An active material redundancy is defined for the group of components (DBB1, DBB2).
- A passive functional redundancy is defined for the groups of components (DBB1, Diesel1) and (DBB2, Diesel2).
- A simple passive material redundancy is defined for the group of components (Tr1, Tr2), (DBA1, DBA2), (FTP1, FTP2).
- A 2 out of 3 passive material redundancy is defined for the group of components (Ex1, Ex2, Ex3). If one of the two primaries pumps fails, the third is activated.

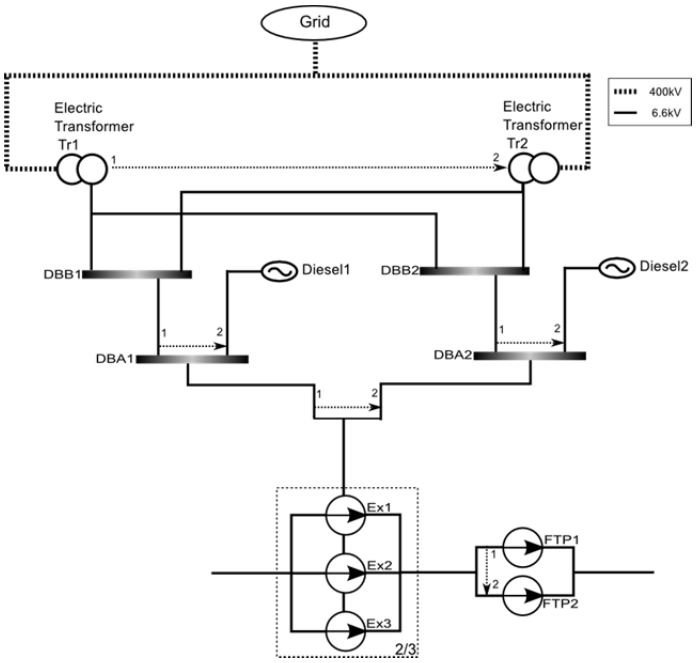

Figure 1. Schema of the coolant feeding system process

2.2 *Recall on the BDMP formalism*

The BDMP is a formalism defined by Bouissou & Bon (2003) to address the dynamic modeling issues while preserving the structure-expressiveness of tree based formalisms (fault tree approaches). Indeed, a static fault tree model aims to describe the system failure as a combinatorial expression on the failures of its leaves (a leaf model a component). The BDMP formalism keeps the same idea, but the Boolean basic leaves of the tree are replaced by dynamic ones specified by Markov Chains (MC). In particular, repairable components can be considered. Moreover,

these MC can consider non dysfunctional events to model switching between different operations modes (active, dormant ...). The occurrence of these non-dysfunctional events is managed by triggers. In particular, a passive redundancy mechanism can be modeled by such a trigger. Hence, a BDMP model can be implicitly defined as a multi-top coherent tree structure whose leafs are triggered MC. Since it is the unique formalism dedicated to the modeling of dynamic repairable systems, it is relevant to model the case study considered in this paper.

Most often, only two kinds of leaves are used and are called *F* and *SF*. The *F* leaves describe components fallible only in active mode, whereas *SF* leaves describe components fallible in both active and dormant modes ($L = L_F \cup L_{SF}$). The behavior of these leaves is specified by the models depicted on Figure 2. Since this paper addresses a qualitative analysis only, the labels of the arcs correspond to events. For performing a quantitative analysis, they should be considered as probability rates. In this figure: the events a-X, d-X, f-X-a, f-X-d and r-X, denote respectively the activation, the deactivation, the failure in active mode, the failure in dormant mode and the reparation of a component X. The two mainly used kinds of logic gates in a BDMP are *AND* and *OR*. But some works use an additional kind: the *PAND* gate. Such a gate expresses a dynamic logic: the failure status of a *PAND* gate is *True*, if and only if the failure status of all its children is *True* and have commuted from *False* to *True* in a predetermined order (generally from left to right in the tree).

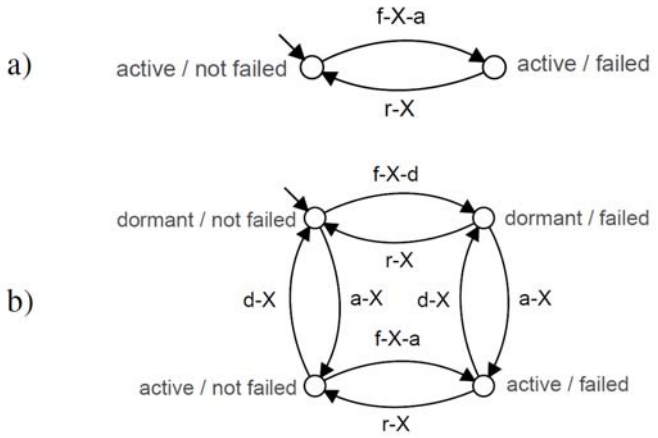

Figure 2. Behavior of the most used BDMP leaves: a) the *F* leaf; b) the *SF* leaf

Let us call the children of a given node (leaf or gate) the leaves of the sub-tree whose node is the root (if the node is a leaf then it has a single child: itself). Let T_i be a trigger, and ($Orig(T_i)$, $Dest(T_i)$) denoted respectively its origin and destination nodes. While $Orig(T_i)$ is not failed, the children of $Dest(T_i)$ stays in the dormant mode (the children of kind *SF* can still fail). When $Orig(T_i)$ fails, the MC of the children of $Dest(T_i)$ are triggered to the active mode, as soon as $Orig(T_i)$ is repaired. Then, they are put back in the dormant mode. For a better description of the BDMP semantics, see Chaux et al. (2011).

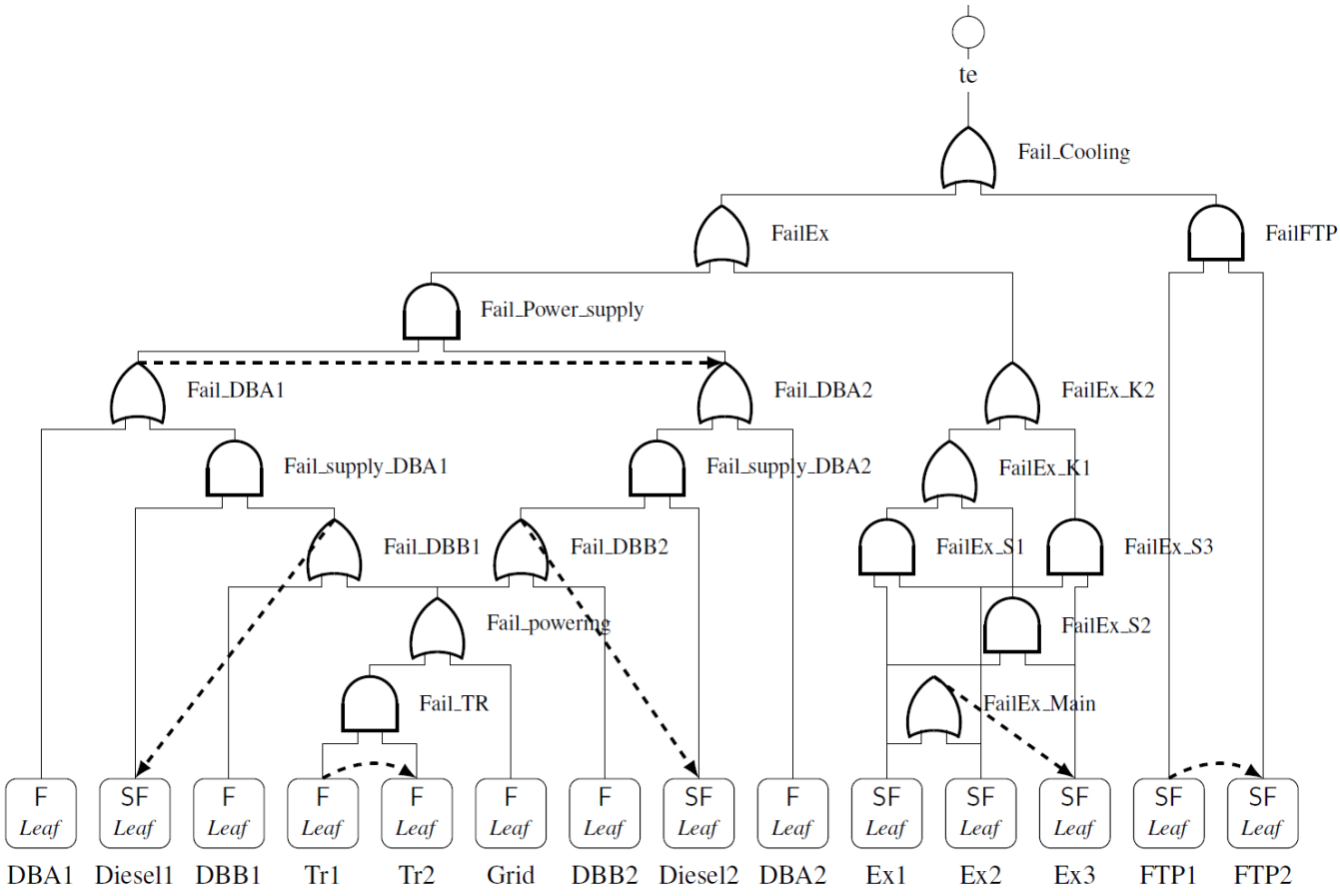

Figure 3. BDMP model of the coolant feeding system process

3 SAFETY ANALYSIS CONSIDERING ONLY THE PROCESS FAILURES

In this section, a BDMP model of the system is built considering only the failures of the process components. Then a qualitative analysis based on this model is performed.

3.1 *Building the BDMP model of the process*

Figure 3 shows the BDMP model of the coolant feeding system process.

The scenarios implicitly described by this BDMP model can be explicitly represented by the sequences of dysfunctional events that can occur. The next subsection aims to determine among them the shortest sequences which lead to the system failure.

3.2 *Extracting the Minimal Cut Sequences*

In the dependability scope, a qualitative study consists in determining the main weaknesses of a system. This knowledge can be used for easing the qualitative study, what become essential when complexity increases.

For static systems, these analyses consist in determining the *Cut,* which is defined by Birnbaum et al. (1961) as a set of failed components that leads to the system failure. A *Minimal Cut* of a static system has then been defined by Rauzy (2001) as a prime implicant of the related Boolean function which can be modeled using fault trees.

For dynamic systems, the system failure depends not only on the set of failed components but also on the order of occurrences of these components failure events. Then *Cut Sequences* and *Minimal Cut Sequences* have been defined by Tang and Dugan (2004), as respectively *Cuts* and *Minimal Cuts* whose component failures have been ordered.

But when the considered system contains repairable components, the failure events are not sufficient to describe all the possible way to fail. Then a *Cut Sequence* is redefined as a sequence leading to the first system failure. Chaux et al. (2013) proposes a framework to give a formal definition of *Minimal Cut Sequences*. Informally, the set of *Minimal Cut Sequences* (MCS) is the minimal set of sequences of minimal length that are necessary and sufficient to describe the whole set of cut sequences.

In order to extract these MCS, we use the algorithms defined in Chaux et al. (2011) and Chaux et al. (2012). The first one transforms a BDMP model into a finite state automaton and the second one extract the MCS of a finite state automaton. Several MCS limited to the length 5 (selected arbitrary among the 84 existing) extracted from the BDMP model described by the last sub-section (Figure 3) are sum up on Table 1.

Table 1. Examples of MCS of length from 2 to 5 considering only the failures of process components

Length	Sequences
2	f-DBA1-a,f-DBA2-a f-Ex1-a,f-Ex3-a f-FTP2-d,f-FTP1-a ...(6 others)
3	f-Die1-d,f-Die2-d,f-Grid-a f-DBA1-a,f-Die2-d,f-DBB2-a f-Grid-a,f-Die1-a,f-DBA2-a ...(16 others)
4	f-DBB1-a,f-Die1-a,f-Die2-d,f-DBB2-a f-Tr1-a,f-Die1-d,f-Die2-d,f-Tr2-a ... (36 others)
5	f-Tr1-a,f-DBB1-a,f-Die2-d, f-Die1-a,f-Tr2-a f-DBA1-a,f-DBB2-a,r-DBA1, f-Die2-d,f-DBA1-a ... (15 others)

Let us remark that from length 5, the MCS may contain repair events. For instance, the sequence f-DBA1-a → f-DBB2-a → r-DBA1 → f-Diesel2-d → f-DBA1-a, is minimal because the failure in dormant mode of the component Diesel2 may not occur without the previous reparation of the component DBA1. Then there exists no shorter cut sequence to fail by this way.

4 SAFETY ANALYSIS CONSIDERING THE CONTROL IN THE LOOP

In this section, the control system which manages the process components, and in particular the mechanisms of redundancies, is introduced. The modification of a BDMP model containing triggers is discussed. Then the control system failures and reparations are integrated to the BDMP model given in the last section. Finally, the MCS of the complete system are extracted and compared with the previous ones.

4.1 *Description of the control architecture*

A control architecture can be defined as the allocation of the control functions on the control components. In this paper, we focus on the control functions which manage the redundancies defined for the process. Moreover, only the passive redundancies require a switching management. Then among the redundancies defined in the subsection 2.1, only six

are concerned. Let R_A, R_B, R_C, R_D and R_E be the functions which manage the switching between respectively (DBB1, Diesel1), (Tr1, Tr2), (DBA1, DBA2), (FTP1, FTP2), (Ex1, Ex2, Ex3). Since the switching between (DBB2, Diesel2) is of the same kind that the one between (DB1, Diesel1), it is also managed by R_A.

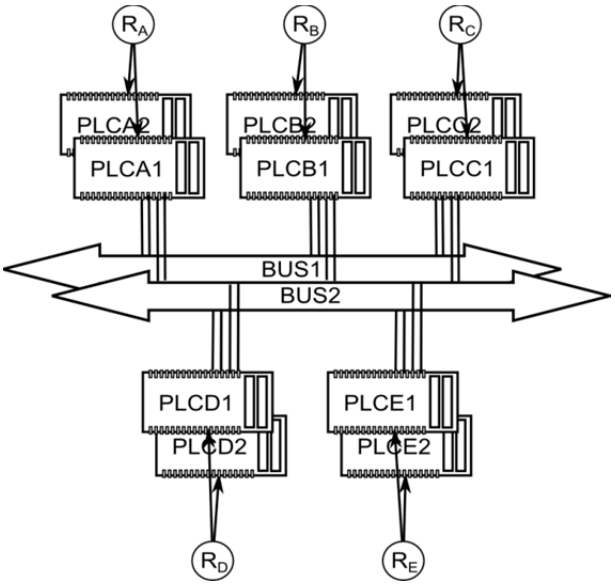

Figure 4. Schema of the control architecture

Each function R_X (for $X \in \{A, B, C, D, E\}$) is implemented on a couple of redundant PLC (Programmable Logic Controller): (PLCX1, PLCX2). The PLCs are connected to the process via two redundant buses (BUS1, BUS2). These redundancies are active, that is mean all the components are working, and the information must be treated and carried by at least respectively one PLC and one BUS. The control architecture of the coolant feeding system is depicted on Figure 4.

The loss of a switching function R_X (for $X \in \{A, B, C, D, E\}$) allocated to the components PLCX1 and PLCX2 can be represented by the BDMP model reported in Figure 5.

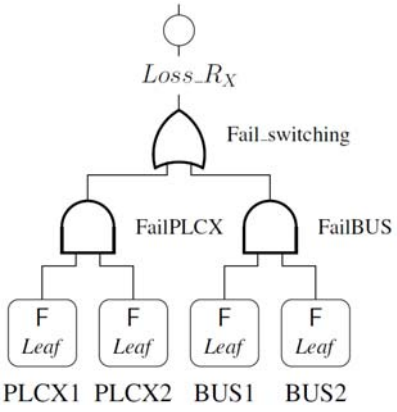

Figure 5. BDMP model representing the loss of a switching

4.2 *Modeling a switching function in a BDMP model*

In this work, a switching mechanism consists in the transfer of the service achievement from a component (or sub-system) to another. The expected behavior of a passive redundancy can then be defined with two conditional switching mechanisms ("component" can be replaced by "sub-system" below):

- *Replacement switching*: if the main component fails then a switching must occur from the main component to the spare one.
- *Withdrawal switching*: if the main component is repaired then a switching must occur from the spare component to the main one.

Thereby, if the function which manages the redundancy is lost, these switching cannot occur when they should do. In particular, if this function is lost after the failure of the main component but before its reparation, the withdrawal switching cannot occur.

Since the semantics of a BDMP trigger complies with this definition (cf. sub-section 2.2), a passive redundancy can be correctly modeled by such a trigger. Then the loss of the function which manages a redundancy corresponds to the loss of the corresponding trigger in the BDMP model. Figures 6, 7 and 8 show three possible models of the loss of the switching function R_D for the sub-tree corresponding to the feeding turbo pumps (gate FailFTP and leaves FTP1 and FTP2).

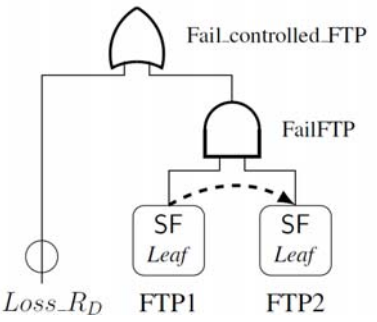

Figure 6. First solution to model the loss of a trigger in a BDMP model

The first proposition (Figure 6) expresses that while the switching function is loss, the group of pumps cannot perform its service even if none of them has failed. This model is very pessimistic because the main pump does not need the switching function for working alone. However in the case of a material redundancy, the function that manages a redundancy and the function that control the process components involved in this redundancy, are allocated on the same control components. Indeed, there is no need to be able to switch between two components if it is not possible to control them. In this

case, the loss of the switching function occurs as the same manner as the loss of the control function. And this model expresses that when the switching function is loss, the control function is also loss; then the group of pumps can actually not perform its service.

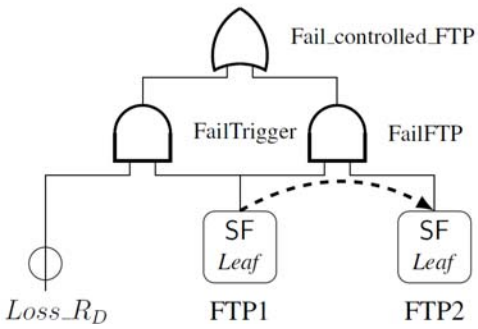

Figure 7. Second solution to model the loss of a trigger in a BDMP model

The second proposition (Figure 7) expresses that while the switching function is loss and the main pump failed, the group of pumps cannot perform its service.

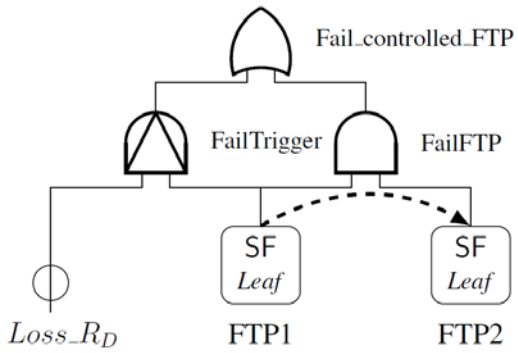

Figure 8. Third solution to model the loss of a trigger in a BDMP model

The third proposition (Figure 8) expresses that if the main pump fails after the loss of the switching function, then the group of pumps cannot perform its service (the gate FailTrigger is a PAND).

In order to choose between these three propositions, let us consider the critical sequence: f-FTP1-a → f-Loss RD-a → r-FTP1 → f-FTP2-a. The expected behavior described by this sequence is informally reported below:

1. Initially, the service is provided by FTP1.
2. After the failure of FTP1, the replacement switching occurs (from FTP1 to FTP2) by means of the function R_D.
3. After the loss of R_D, the service is still provided by FTP2.
4. After the reparation of FTP1, the withdrawal switching (from FTP2 to FTP1) cannot occur because of the loss of R_D; then the service is still provided by FTP2.
5. After the failure of FTP2, the service is not provided anymore (even if FTP1 had been repaired).

Let us remark that since this sequence leads to the first failure of this sub-system, it is a cut sequence for this sub-system. The Table 2 compares the accuracy of the three models proposed for this sequence. The accuracy criterion is here the conformance between the expected and the modeled behavior. The cells show the pump which provides the service, if any and the symbol Ø otherwise. Let us remark, than the last event is called f-FTP2, because it corresponds to f-FTP-d in the BDMP models, but should be f-FTP2-a in the reality.

Table 2. Confrontation of the behavior described by the three models to the expected one on a critical sequence

sequence	$1 \xrightarrow{f-FTP1-a} 2 \xrightarrow{f-Loss\_R_D-a} 3 \xrightarrow{r-FTP1} 4 \xrightarrow{f-FTP1} 5$				
expected	FTP1	FTP2	FTP2	FTP2	Ø
1st model	FTP1	FTP2	Ø	Ø	Ø
2nd model	FTP1	FTP2	Ø	FTP1	FTP1
3rd model	FTP1	FTP2	FTP2	FTP1	FTP1

The Table 2 shows first that none of the models is perfectly accurate. Indeed, a perfectly accurate model would specify exactly the same behavior as the expected one for any sequence. Moreover, the third model is the closest of the reality, but it is not conservative. Indeed, it misses at least the cut sequence considered above. It is also the case for the second model. We are then constrained to choose the first model, because despite its bad accuracy, it is the only one which is conservative. This discussion shows that the BDMP formalism (the unique one which is dedicated to model the repairable dynamic system) has not the semantics required for correctly model the loss of a trigger. More generally, the gates of a BDMP are focused on the failure events and not the repair events. Then the consequences of the reparation of the trigger's origin are fixed by the semantics of a trigger, and cannot be changed by modifying the structure.

4.3 *Integrating the control failures in the BDMP model*

Figure 9 shows the BDMP model of the entire controlled coolant feeding system. This model had been constructed by applying the model chosen in the last subsection for each passive redundancy. The new gates are darkened. The intermediate events of kind

$Loss\_R_X$ (for $X \in \{A, B, C, D, E\}$) should be replaced by the corresponding sub-tree (see Figure 5).

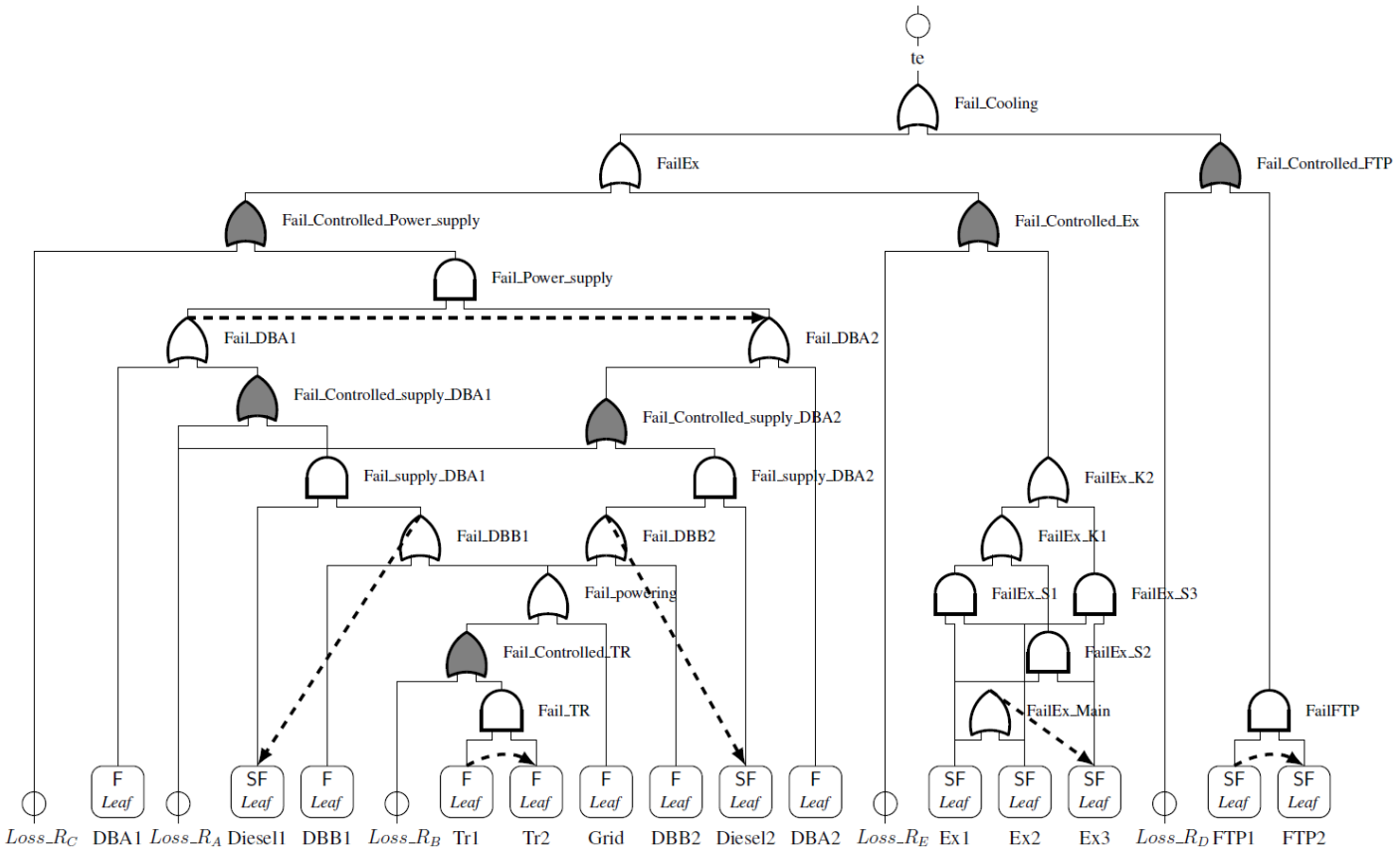

Figure 9. BDMP model of the controlled coolant feeding system

4.4 *Comparing the new MCS with the previous one*

Table 3. Examples of MCS of length from 2 to 5 considering the failures of both process and control components

Length	Sequences
2	**f-PLCA1-a,f-PLCA2-a** **f-BUS1-a,f-BUS2-a** f-Ex1-a,f-Ex3-a ...(16 others)
3	f-Die1-d,f-Die2-d,f-Grid-a f-DBA1-a,f-Die2-d,f-DBB2-a f-Grid-a,f-Die1-a,f-DBA2-a ...(16 others)
4	**f-PLCB2-a,f-Die1-d,** **f-Die2-d,f-PLCB1-a** **f-PLCB2-a,f-Die2-d,** **f-PLCB1-a,f-DBA1-a** f-Tr1-a,f-Die1-d,f-Die2-d,f-Tr2-a ... (90 others)
5	**f-Die2-d,f-PLCB1-a,f-DBB1-a,** **f-Die1-a,f-PLCB2-a** f-DBA1-a,f-DBB2-a,r-DBA1, f-Die2-d,f-DBA1-a ...(45 others)

Considering the control failures brings many new sequences as can be seen on the Table 3 that sums up several MCS selected arbitrary. Since the process has not been changed, it can still fail as presented in the last section. Then the new MCS includes the previous one. But 94 new sequences are added to the 84 previous ones (for the sequences of length lower than 5). Among them, 10 new sequences of length 2 show that the buses and the PLC which host the function R_A, R_C, R_D and R_E are very critical. Indeed, the achievement of the system function depends directly on the success of these groups of redundant component. Moreover, 54 new sequences of length 4 and 30 new sequences of length 5 that mix failures of both process and control components appear.

For instance, the sequence f-PLCB2-a → f-Die2-d → f-PLCB1-a → f-DBA1-a describes the behavior informally reported below:

1. Initially, the power supply is performed by the first line (Grid, Tr1, DBB1, DBA1) and the pumping services by Ex1, Ex2 and FTP1.
2. After the failure of PLCB2, nothing happens because it is in active redundancy with PLCB1.
3. After the dormant failure of Diesel2, nothing happens because the power supply is still performed by the first line.

4. After the failure of PLCB1, the controlled transformers are considered unavailable; then DBB1 and DBB2 either. The switching function R_A is not lost then the replacement switching from DBB1 to Diesel1 occurs. The power supply is performed by Diesel1 and DBA1.
5. After the failure of DBA1, the first line cannot supply the power anymore. The switching function R_C is not lost then the replacement switching from the first line to the second one occurs. But DBB2 does not transfer the power supply (because of the failure of the controlled transformers). The switching function R_A is still not lost then the replacement switching from DBB2 to Diesel2 occurs. But Diesel 2 has already failed in dormant mode. Then there is no other way for performing the power supply. Hence the coolant feeding system fails.

This set of MCS is a pessimistic representation of the weaknesses of the system considering both the process and the control. The number of MCS extracted is more than twice bigger when the control is considered. This observation confirms that the control should be taken into account in the MBSA studies for systems that bring many switching mechanisms. Let us remark that the results depend on the architecture choice for the control as well as the process. Then another choice of allocation of the control functions on the control components would lead to different results.

5 CONCLUSIONS

This paper claims that the failures of control components should not be omitted in the MBSA. A comparative study is performed on an industrial example. The system is modeled by a BDMP considering first only the process failures, and then considering also the control failures. The failures of control components may lead to a loss of the switching functions which handle the redundancy mechanisms between the process components. Hence we propose a modification of the model for considering the loss of these switching functions in a BDMP model. The study shows first that the set of MCS extracted is twice bigger from the model of the controlled process than from the model of the process (without taking into account the control). Furthermore, it shows that BDMP formalism is not fully adapted to deal with this issue.

Since this formalism does not allow us to describe correctly the loss of a switching function, ongoing works are aiming to define an extension of this formalism which offers that possibility. Furthermore, the consideration of failures in a closed loop system raises a failure propagation in-the-loop issue that cannot be addressed by a method based on tree formalism like BDMP. Hence, developing a qualitative analysis that deals with this issue is also under investigation.

6 ACKNOWLEDGEMENT

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

REFERENCES

Berard, B., M. Bidoit, F. A., Laroussinie F., Petit A., Petrucci L., & Schnoebelen P. 2001. *Systems and Software Verification. Model-Checking Techniques and Tools*. Springer. LSV.

Birnbaum, Z., Esary, J. & Saunders S. 1961. Multi-component systems and structures and their reliability. *Technometrics* 3(1), pp. 55–77.

Bouissou, M. & Bon J.-L. 2003. A new formalism that combines advantages of fault trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering and Systems Safety* 82(2), pp. 149–163.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. September 2011. Qualitative analysis of a BDMP by finite automaton. In *20th European Safety & Reliability Conference,* Troyes (France), pp. 2055–2057.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. June 2012. Systematic extraction of minimal cut sequences from a BDMP model. In *21th European Safety & Reliability Conference*, Helsinki (Finland). Session 16B, 8 pages.

Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou M. September 2013. Towards a unified definition of minimal cut sequences. In *4th IFAC DCDS*, Volume 4, York (UK). 6 pages.

Joshi, A., Heimdahl, M. P., Miller, S. P., & Whalen, M. W. February 2006. Model-Based Safety Analysis. Technical Report *NASA/CR-2006-213953*

Rauzy, A. (2001). Mathematical foundations of minimal cutsets. In *IEEE Transactions on Reliability* 50(4), pp. 389–396.

Sondermann-Woelke, C., Meyer, T., Dorociak, R., Gausemeyer, J., & Sextro W. June 2012. Conceptual design of advanced condition monitoring for a self-optimizing system based on its principle solution. In *21th European Safety & Reliability Conference*, Helsinki (Finland). session 28, 10 pages.

Tang, Z. & Dugan, J. 2004. Minimal cut set/Sequence generation for dynamic fault trees. In *Reliability and Maintainability, 2004 Annual Symposium-RAMS*, Los Angeles (USA), pp.207–213.