Minimality of critical scenarios with linear logic and cutsets

Leila Boucerredj* & Nasr Eddine Debbache

Laboratory of Automatic and Signals - Annaba (LASA)
Department of electronics, Faculty of Engineering,
University Badji-Mokhtar Annaba – BP 12, 23000 Annaba, Algeria.

Soumis le : 26.06.2012 *Révisé le : 07.12.2013* *Accepté le : 14.05.2014*

ملخص
يقترح هذا العمل نهجا جديدا في مجال أمنية التشغيل للأنظمة الميكاترونيكية. هدفها هو استخراج كافة السيناريوهات الحرجة ذات الحد الأدنى التي تؤدي بالنظام إلى حالة الفشل، وذلك مباشرة من أشجار الدليل للمنطق الخطي لإقامة روابط سببية بين الأحداث غير المرغوب فيها والحالات الطبيعية. أشجار الدليل للمنطق الخطي تحتوي على أحداث التي هي نتيجة لحالة في السيناريو، ولكن ليس سببا ضروريا تماما للإنتاج النهائي للحالة الحرجة. وحجم شجرة الدليل يتناسب مع عدد من التحولات في معبر متتالي يمكن إثباته. لهذا يستند هذا النهج على مفهوم الحد الأدنى لطريقة شجرة الخطأ وتطبيقها على أشجار الدليل للمنطق الخطي لنموذج شبكات بيتري في سياق غير مألوف. الهدف منه هو تقليل حجم أشجار الدليل للمنطق الخطي وتوليد عدد أدنى من السيناريوهات الحرجة.

الكلمات المفتاحية: *أمنية التشغيل- أنظمة ميكاترونيكية- شبكات بيتري- المنطق الخطي- الحد الأدنى لسيناريوهات الحرجة- الحد الأدنى.*

Résumé
Ce travail propose une nouvelle approche d'analyse de la sûreté de fonctionnement des systèmes mécatroniques. Son objectif est d'extraire les scénarios redoutés minimaux qui conduisent un système vers un état de défaillance, à partir des arbres de preuves de la logique linéaire et établir les liens de causalité entre les événements redoutés et les fonctionnements normaux. Les arbres de preuves de la logique linéaire contiennent des événements qui sont la conséquence d'événement inclus dans le scénario, mais qui ne sont pas strictement nécessaires à l'obtention de l'état critique redouté final. La taille de l'arbre de preuve est proportionnelle au nombre de franchissement des transitions dans le séquent prouvable. L'approche proposée est basée sur la notion de coupe minimale de la méthode des arbres de défaillances appliquées aux arbres de preuves de la logique linéaire du modèle réseau de Pétri dans un contexte inconnu. L'objectif est de réduire la taille des arbres de preuves de la logique linéaire et de générer un nombre minimal de scénarios redoutés.

Mots clés: *Sûreté de fonctionnement - Systèmes Mécatroniques - Réseaux de Petri - Logique linéaire - Scénarios redoutés minimaux - Coupe minimales.*

Abstract
This work proposes a new approach for analyzing the dependability of mechatronic systems; its goal is to extract all minimal feared scenarios that lead a system in a state of failure, directly from the proof trees of linear logic to establish the causality between undesirable events and normal operations. The proof trees of linear logic contain events that are the result of event in the scenario, but not strictly necessary for the final production of the critical feared state. The size of the proof tree is proportional to the number of firing transitions in the sequent provable. The proposed approach is based on the concept of minimal cutsets of the fault tree method applied to the proof trees of linear logic of Petri net model in an unknown context. The aim is to reduce the size of the proof trees of linear logic and generate a minimum number of feared scenarios.

Keywords: *Dependability - Mechatronic systems -Petri net - Linear logic - Minimal Feared scenarios - Cutsets.*

**Auteur correspondant: chiraz_leila@yahoo.fr*

1. INTRODUCTION

The progressive integration of electronics in the car and avionic fields has lead to improvements in both functions and services. However, this has caused an increased complexity in the design of these systems, typically mechatronic systems [1 - 4], which makes the control of their reliability difficult [5]. Mechatronic systems (MS) merge electric, mechanic hydraulic and electric technologies and use a computer control and monitoring [6]. The benefit of such systems lies in the very large flexibility thanks to the software implementation of the control and monitoring functions. Consequently, functions improving safety can be easily added. However, at the industrial level, few efficient methods exist to evaluate the effects of MS on the security of these systems [6 - 10].

This means that when some event affecting the reliability of the system occurs, a reconfiguration action is executed in order to maintain the system in a safe degraded state. If the reconfiguration fails then the system will reach a feared (dangerous) state with dramatic consequences for users. So it is important to understand how the system reaches such feared states to set up the reconfiguration actions.

In our previous work [12], our approach for safety analysis of dynamic systems, feared scenarios are derived from Petri net model. Based on linear logic as new representation (using the causality relations) of the Petri net model and proof tree. The hybrid aspect of MS (both continuous and discrete features) leads us to choose a model that associates PN and Differential Predicate Transition (DPT) [11, 12]. The PN model describes the operation modes, the failures and the reconfiguration mechanisms. The differential equations represent the evolution of continuous variables of the energetic part of the system. A qualitative analysis allows to determine a partial order of transition firings and thus, to extract feared scenarios (but not minimal) [12].

In the work of Sadou and *al* [13], the definition of the minimal scenario in Petri net model by restricted precedence graph concerns the case where the context is completely know (the initial and final markings are fixed).

Within our new approach for deriving minimal feared scenario the context is only partially known, we don't know the initial marking, and about the final marking we only know a part that contains the partial feared state. We don't know which transitions have to be fired. The problem is to write the right sequent that will initiate the desired search. It is necessary to write the list of the transitions that have to be considered, without knowing how many times exactly they will be fired.

From this approach we construct the canonical proof tree and we integrate the concept of cutsets in the canonical proof tree for deriving minimal feared scenario (restricted proof tree).

2. PRINCIPLES OF THE APPROACH

2.1 Feared scenarios definition

We call feared scenario a set of events (transition firings for a Petri net model), verifying a partial order and leading from one partial state corresponding to normal behaviour (partial marking), to another one that represents a dangerous situation of the system. A partial state is the conjunction of a subset of the system components states [13].

2.2 Minimal Cutsets associated to the feared state

A cutsets is a combination or a subset of elements whose failure leads to system failure. A minimum cutsets is a section containing no other cut.

As an example, consider the fault tree shown in figure 1.

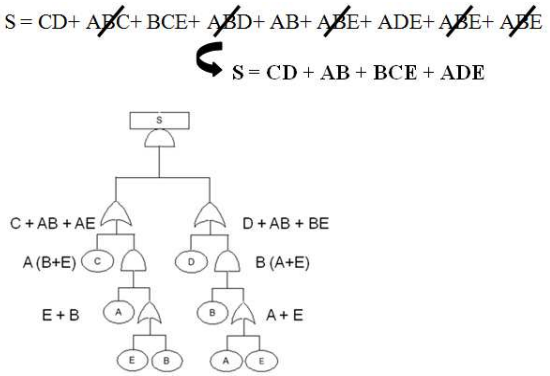

Figure 1. Concept of minimal cutsets.

2.3 Petri Nets and LL proof tree

The translation of a PN in LL [14, 15], has been presented in [12]. A logic formula is associated to every marking and to every transition firing instance. A marking M is a monomial in $\otimes$, denoted $P_1 \otimes P_2 \otimes ... \otimes P_k$, where P_i are place names: if any place P_k contains several tokens (n, for example), n instances of the proposition P_k appear. A transition is a formula $M_1 -o M_2$ where M_1 and M_2 are markings (in fact, Pre and Post functions of the transition). This expression represents the transition firing: it will appear in a sequent as many times as this transition is fired. A sequent is associated to a scenario: the initial marking and the considered multiset of transition firings are the premises; the final marking is the conclusion. This sequent is then proved by applying the rules of the sequent calculus. In our approach we only use a part of the MILL (Multiplicative Intuitionist Linear Logic) fragment [12, 15]; its provability is equivalent to the reachability of the final marking from the initial one, and the multiset of transition firings exhibits which transitions are fired.

The sequent of equation (1), represents a scenario with $s = t_1,\ldots,t_n$ is the non ordered list of the different firing instances of the concerned transitions whereas M and M_f are respectively the initial and final markings.

$$M, s \vdash M_f \quad (1)$$

As usually within the sequent calculus framework, the proof is materialised by a tree which is read from bottom to up: the sequent to prove is written at the bottom of the tree. The proof stops when all the leaves of the tree are identity sequent ($P \vdash P$, for example). Several proof trees are possible but the proof is constructed in a canonical way [14, 15]. The rules that we use for this canonical proof are represented in [12]. An example of translation of a PN in LL is given in figure 2.

Initial marking:

$M = P_1 \otimes P_1 \otimes P_2$

Final marking final:

$M_f = P_1 \otimes P_3$

Transition:

$t_1 : P_1 \otimes P_2 - o P_3$

$t_2 : P_3 - o P_4 \otimes P_5$

$M, s \vdash M_f :$

$M \xrightarrow{t_1} M_f : (P_1 \otimes P_1 \otimes P_2), P_1 \otimes P_2 - o P_3 \vdash P_1 \otimes P_3$

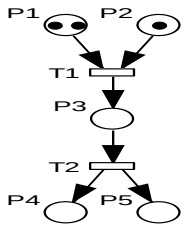

Figure 2. Translation of the PN in sequent.

It is necessary to write the list of the transitions that have to be considered, without knowing how many times exactly they will be fired. To express this kind of constraints in LL we use the exponential connector '*!*'. When we write *!t* in a sequent, it means that transition *t* can be fired zero, one or k times, depending on the needs and the progress of the proof.

3. A NEW METHOD FOR DERIVING MINIMAL CRITICAL SCENARIOS

The aim of a qualitative analysis is to point out the sequence of actions that leads to the feared states and to analyse more precisely what makes the system leave the normal behaviour and reach the feared state. Our method starts by a backward reasoning from the feared state in order to identify the causal chain of actions leading to that feared state. The backward reasoning is stopped when a nominal state is reached. A forward reasoning follows it in order to obtain all the possible evolutions from this partial nominal state. The bifurcation between the nominal behaviour and the feared one is identified and corresponds to a transition conflict in the PN [8, 12].

If M_d represents the partial feared state, the sequent that initiates the backward reasoning will be given by the equation (2):

$$M, !t_1, ..., !t_n \vdash M_d \wp \Gamma \quad (2)$$

Where Γ is a context that must be produced simultaneously with M_d; and $t_1,\ldots,t_n$ represent all the transitions of the PN (Fig. 3).

The formula of equation (3) can be used in the same way for the forward reasoning (Fig. 3).

$$M_n \otimes \Gamma, !t_1, ..., !t_n \vdash M \quad (3)$$

The reasoning in an unknown context is now illustrated in the following example (Fig. 3):

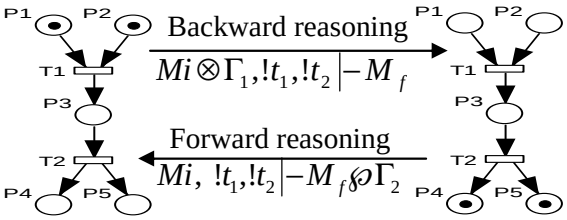

Figure 3. Petri net example.

• **Backward reasoning**:
At this stage, the translations of the PN are expressed as follows:

$M_i \otimes \Gamma_1, !t_1, !t_2 \vdash M_f$

$M_i \equiv P_1$; $\Gamma_1 \equiv P_2$; $M_f \equiv P_4 \otimes P_5$;

$t_1 \equiv P_1 \otimes P_2 - o\ P_3$; $t_2 \equiv P_3 - o\ P_4 \otimes P_5$.

• **Forward reasoning**:
The translations of the PN are now expressed as follows:

$M_i, !t_1, !t_2 \vdash M_f \wp \Gamma_2$

$M_i = P_1 \wp P_2$; $M_f \equiv P_4$; $\Gamma_2 \equiv P_5$;

$t_1 \equiv P_1 \wp P_2 - o\ P_3$; $t_2 \equiv P_3 - o\ P_5 \wp P_5$.

To obtain minimal scenario we have to consider this aspects [16]:
- the order relations between events must be effective relation of causality in the system;
- the list of event of the scenario must be minimal (without events of the loop of the system);
- the final marking corresponding to the feared state must be minimal.

This method based on four steps the goal of which aims at determining systematically and formally the conditions for the marking and the unmarking of some given set of places (called target state). The four steps of the method are the following:
- determining the normal states;
- determining the target states (partial feared states or states to be analyzed);
- backward reasoning starting from the target state (using the concept of cutsets in proof building);
- forward reasoning starting from the conditioning states (pointing out the bifurcations between normal working and feared scenarios and using the concept of cutsets in proof building).

This method uses LL for both backward and forward reasoning as described previously; this is why we develop a tool FSPMEDIT (Feared Scenarios PM Editor) [17], which makes it possible to extract the minimal critical scenarios from a Petri Net model.

3.1 Minimal scenarios in proof tree

The definition of the minimal scenario associated to a minimum cutest is related to the notion of restricted proof tree. So we will define a restricted proof tree to some of its elements (Fig. 4). The restriction consists in deleting some events of the proof tree and completing it by the precedence relation induced by transitivity by the deleted elements (rules of the MILL fragment (sequent identity)).
In figure 4, we can see that the initial sequent, $P_2, P_3, \Gamma_2, t_3, !T \vdash M_f$ of the proof tree, and the sequent obtained after the application of the *-oL* rule, are the same. We stop the process of building the proof and put $\Gamma_2 \equiv 1$(1 is the neutral element of the $\otimes$), and $M_f \equiv P_2 \otimes P_3$.
In this case the set of events which compose the scenario must be minimal and the precedence relations must be derived from a proof tree. It is the guaranty that there are not parasite precedence relations which are not present in the Petri net model.

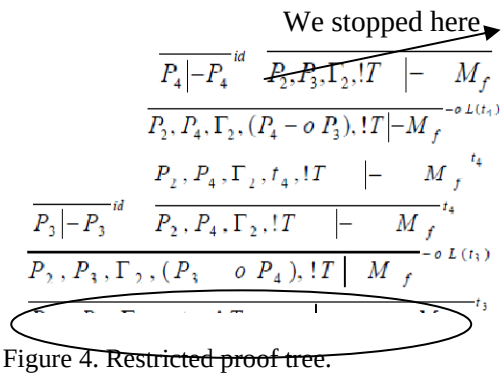

Figure 4. Restricted proof tree.

3.2 Case study

The case study is based on a volume regulation system of two tanks (Fig. 5). It is made of a computer, two pumps, ordered by a relay; two relay, ordered by a logical building block AND, two detectors of high level providing a signal as long as the level of the fluid did not reach it, thus authorizes the filling of tank, three electrovalves (EV1, EV2, EV3), two volume sensors, the two regulated tanks (tanks 1 and 2) and a third tank for draining (by the electrovalve 3). The two regulated tanks are used on demand of a user. This demand is described by a function of time flow rates (to the user (tanks 1 and 2) (t)). The volume of each tank(i) must be kept inside a given interval [V_{imin}, V_{imax}]. The volume is controlled by the computer, which decides, according to the values given by the volume sensors, to full (or not) the concerned tank by opening (or not) the concerned electrovalve (EV). The control law of the computer is such that the EV is closed when the volume of the controlled tank over crosses the high limit V_{imax}. On the other hand, the computer commands the opening of the EV each time the value of the volume in the controlled tank is lower than the limit V_{imin}. We distinguish two normal phases of the system, corresponding to the state of the EV:

- A conjunction phase when the EV is open. The volume in the tank is going up; no matter what is the value of the outgoing flowrate to the user (the pump flowrate is much higher than the outgoing flowrate);
- A disjunction phase when the EV is closed. The volume in the tank is decreasing;

If the volume of one tank exceeds the V_{iL}, the computer commands the relief electrovalve (EV3) of tank for draining, so that the volume becomes lower than V_{imin}, if the EV3 is out of order, the volume of the tank (tank 1 or 2) exceeds V_{iS}, then the overflow of the system.

As we focus our study on critical scenarios, and in order to simplify the problem, we consider that only the electrovalves can have failures. A typical failure of the electrovalves 1 and 2 (EV 1 and 2) corresponds to a blocked open state (stuck closed) in which the electrovalve does not react to a closure command of the computer, and EV3 out of order. These two electrovalves (EV 1 and 2) can be repaired after a failure occurrence.

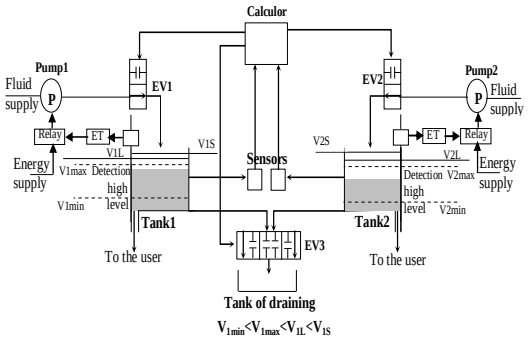

Figure 5. Case study

3.3 Stochastic Differential Predicate Transition (SDPT) Petri Net Model

Place P_1 of the net in figure 6 represents the disjunction phase (the volume is decreasing); place P_2 represents the conjunction phase in which the volume is increasing. Place P_4 corresponds to a state where the EV1 works. Transition t_1 represents the closing command of the EV 1 when the volume oversteps V_{1max}. Transition t_2 represents the opening command of the same electrovalve when the volume becomes lower than V_{1min}. Transitions t_4 and t_5 represent the fact that the electrovalve can stay blocked in an open state (t_4), and can be repaired (t_5). Tank 2 is modelled in the same way. When the volume in the tank 1 oversteps the high security limit (V_{1L}), and the backup electrovalve is available (place P_6 is marked) then t_7 becomes fireable and the draining process of tank 1 can start via the backup electrovalve by marking place

P_8. The EV3 can have failure (firing of transition t_6) in this case, the place P_7 is marked and the relief electrovalve is out of order.

The complete model of the case study includes the model of nominal operation of the two tanks (1 and 2), the models of failure and repair of electrovalves (1 and 2); the model for the use of relief electrovalve and the model of occurrence of the feared state of tanks 1 and 2 (overflow).

We say there is overflow on one of the tanks, for instance tank1, when the volume in this tank over crosses V_{1S} (V_{1S} is higher than V_{1max} and V_{1L}). In that case, transition t_3 is fired and place P_3 is marked.

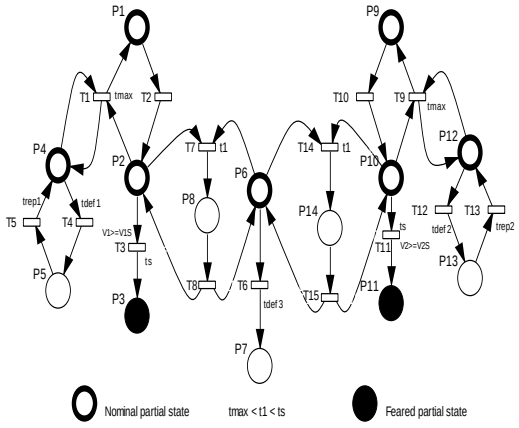

Figure 6. SDPT Petri net model of the case study.

3.4 Application and results

The new approach uses the concept of cutsets for deriving minimal FS in canonical proof tree (Backward and Forward reasoning) of a LL sequent.

For the sake of simplicity, we don't give the details of the application of LL rules and just explain the results in terms of transition firing in the PN.

To determine the minimal FS, we assume that the places associated to the feared state are safe (their marking cant exceeds one token). In the case of not safe places associated to the feared states a transformation of these places is necessary and can easily made but adding a new safe place, that consume the tokens of the no safe place to give only one token (weights are associated to the arcs of the Petri net).

Nominal and target states are represented in the model of complete system (Fig. 6). We are interested in the overflow of tank1. So the target state will be the partial feared state corresponding to the marking of place P_3.

- Backward reasoning from the target state: at this stage, we use the reversed PN in which all the arcs are reversed.

The initial sequent expressing the reachability of the marking of P_3 is: $M_1, !T \vdash P_3 \wp M_2$. A token is then produced on place P_2 this place corresponds to a nominal state, therefore the backward reasoning is stopped (Fig. 7). The obtained sequent: $P_2, t_3 \vdash P_3$ represents the reachability of the partial feared state P_3 from the marking of place P_2 (state conditioner), after one firing of transition t_3, the backward reasoning is stopped (Fig. 7).

$$\frac{}{P_2 \vdash P_2}\,id \qquad \Gamma_1, !T \vdash \Gamma_2$$

$$\frac{}{P_2 \wp \Gamma_1, !T \vdash P_2, \Gamma_2}\,\wp_L$$

$$\frac{}{M_i, !T \vdash P_2, \Gamma_2} \qquad \frac{}{P_3 \vdash P_3}\,id$$

$$\frac{}{M_i, (P_2 - o\, P_3), !T \vdash P_3, \Gamma_2}\,-o\,L(t_3)$$

$$\frac{}{M_i, t_3, !T \vdash P_3 \wp \Gamma_2}\,\wp_R$$

$$\frac{}{M_i, !T \vdash P_3 \wp \Gamma_2}\,!L$$

Figure 7. Proof tree of sequent $(M_i, t_3, !T \vdash P_3 \wp \Gamma_2)$.

- Forward reasoning: thanks to the backward reasoning we have identified a scenario leading to the marking of place P_3, it represents the reachability of this marking from the marking of place P_2, therefore the initial sequent is: $P_2 \otimes \Gamma_1, !T \vdash M_f$. The place P_2 represents a conditioning state from which the system can either evolve to the feared state P_3. We can see that the transitions t_1, t_3, t_7 are in conflict. This step gives three possible behaviours, each one corresponding to the firing of t_3, t_1 or t_7:

The feared scenario previously found: $P_2, t_3 \vdash P_3$ corresponding to the firing of t_3 (tree 1).

The firing of transition t_1 from the initial marking a token in the place P_2 and P_4, leading to the marking of place P_1 and P_4 is shown by the following figures (Fig. 8 and Fig. 9).

$$\dfrac{\dfrac{\dfrac{}{P_2 \vdash P_2}^{id} \quad \dfrac{}{P_4 \vdash P_4}^{id}}{P_2, P_4 \vdash P_2 \otimes P_4}^{\otimes R} \quad \dfrac{\dfrac{}{P_1 \vdash P_1}^{id} \quad P_2, P_4, \Gamma_2, !T \vdash M_f}{P_1, P_4, \Gamma_2, (P_1 - o P_2), !T \vdash M_f}^{-oL(t_2)}}{P_1 \otimes P_4, \Gamma_2, t_2, !T \vdash M_f}^{\otimes_L}}{P_2, P_4, \Gamma_2, (P_2 \otimes P_4 - o P_1 \otimes P_4), !T \vdash M_f}^{-o\,L(t_1)}$$

$$\dfrac{P_2 \otimes (P_4 \otimes \Gamma_2), (P_2 \otimes P_4 - o P_1 \otimes P_4), !T \vdash M_f}{P_2 \otimes \Gamma_1, !T \vdash M_f}^{\otimes L,\, \otimes L}{}^{!L(t_1)}$$

Figure 8. Fragment 1 of the tree 2.

In figure 9, we can see that the initial sequent $P_2, P_4, \Gamma_2, !T \vdash M_f$ of the proof tree, and the sequent obtained after the application of the *-oL* rule, are the same. We stop the process of building the proof and put $M_f = P_2 \otimes P_4$ and $\Gamma_2 \equiv 1$.

We stopped here

$$\dfrac{\dfrac{\dfrac{}{P_5 \vdash P_5}^{id} \quad \dfrac{}{P_2, P_4, \Gamma_2, !T \vdash M_f}}{P_2, P_5, \Gamma_2, t_5, !T \vdash M_f}^{t_5} \quad \dfrac{}{P_4 \vdash P_4}^{id}}{P_2, P_5, \Gamma_2, !T \vdash M_f}^{!L(t_5)}}{P_2, P_4, \Gamma_2, (P_4 - o\ P_5), !T \vdash M_f}^{-o\,L(t_4)}$$

$$\dfrac{P_2, P_4, \Gamma_2, t_4\ !T \vdash M_f}{}^{t_4}$$

Figure 9. Fragment 2 of the tree 2.

The firing of transition t_7 from the marking of places P_2 and P_6 leads to the marking of place P_8 ($P_2 \otimes P_6, t_7 \vdash P_8$); this scenario corresponds to the start of the draining of tank 1 with the use of the relief electrovalve EV3 (when EV3 is available).
It becomes necessary to analyse the firing conditions of the transition t_1 by the marking of places P_2 and P_4, and the firing of transition t_7 by the marking of places P_2 and P_6. The analysis is to show how P_4 and / or P_6 are marked, takes into account the threshold values of continuous variables associated with transitions, to analysis the conflict of the transition t_3 with t_1 or t_7.

During the proof building (tree3), we obtain the two following sequent:

$$P_6, t_6 \vdash P_7,$$
$$P_6 \otimes P_{10}, t_{14} \vdash P_{14}.$$

After analysing the results we can conclude that there are two minimal FS:
The first feared scenario is given by equation (4):

$$P_4, t_4 \vdash P_5; P_2, t_3 \vdash P_3; P_6, t_6 \vdash P_7, \qquad (4)$$

And the second feared scenario is given by equation (5):

$$P_4, t_4 \vdash P_5; P_2, t_3 \vdash P_3; P_6, t_6 \vdash P_7; P_6 \otimes P_{10}, t_{14} \vdash P_{14}. \qquad (5)$$

So we find the two feared situations represented by equation (6):

$$S = \{EV1\_HS \vee (EV3\_HS \wedge EV2\_HS \wedge EV3\_OK)\} \quad (6)$$

The feared state ***S*** can be represented by a boolean function: EV 1 and 3 out of order, expresses that the EV 1 and 3 are in failure states (EV1_HS and EV3_HS); or EV 1 and 2 out of order (EV1_HS and EV2_HS) and EV 3 used to drain tank 2 (EV3 used).

By simulation with FSPMEDIT (Fig. 10) to extract the minimal critical scenarios from a Petri Net model, we obtain the same results (result with restricted proof tree).

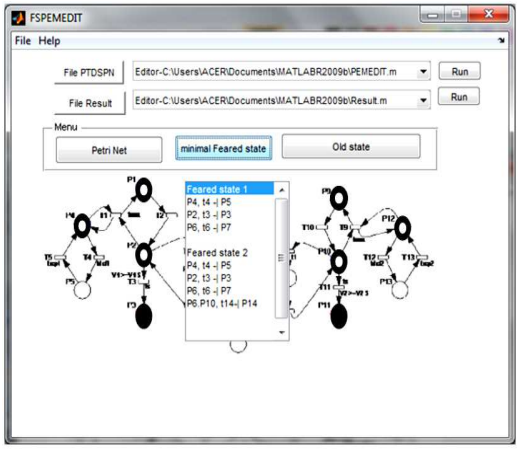

Figure 10. Minimal feared scenario by FSPEMIT.

3.5 DISCUSSION

Our objective is to identify all the minimal feared scenarios leading to the marking of place P_3. We started from a sequent expressing the reachability marking of place P_3, from an unknown initial marking. By applying a backward reasoning on this sequent and then a forward reasoning, we obtain the final sequent $P_2 \otimes \Gamma_1, !T \vdash M_f$ that contains all the possible scenarios leading to the marking of place P_3. From the restricted proof tree we deduce two results:
EV 1 and 3 out of order (it expresses the EV 1 and 3 are in failure states),
Or EV 1 and 2 out of order and EV 3 used to drain tank 2 (EV3 used).

4. CONCLUSION

In this paper we addressed the minimality of critical scenarios (that lead to feared states) in proof tree of Petri net model in unknown context (using LL). Indeed, a scenario can lead to the feared state without being minimal (*i.e*. it contains events which are not strictly necessary to reach the final feared state in proof tree) [12]. In our new approach for deriving minimal feared state the context is only partially known, it corresponds to the minimal cutsets associated to a boolean expression that represents the marking and firing transition associated to the feared state. This notion of minimality will be integrated in our method for deriving feared scenarios in order to generate only minimal scenario in proof tree (restricted proof tree). The quantitative analysis by the Markov graphs can lead to the fast explosion of the number of states. Moreover, the Markovian assumption remains very restrictive [18, 19]; the next objective is to complement our new approach by a quantitative analysis to estimate the occurrence probability of feared scenarios given by the qualitative analysis.

REFERENCES

[1] Zaytoon J., 2001. Systèmes dynamiques hybrides. *Ouvrage collectif sous la direction de collection Hermes Science*, 378p.

[2] Cazals F. & Meizel D., 2005. Projects in the pedagogy of mechatronics in engineering education, In the 6th International Workshop on Research and Education in Mechatronics, France, 453–458.

[3] Isermann R., 2007. Mechatronic systems - innovative products with embedded control, Control Engineering Practice, 10-16.

[4] Demri A., 2010. Contribution à l'évaluation de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle, Thesis at Angers University, 186p.

[5] Kececioglu D., 1991. Reliability Engineering Handbook. *Prentice Hall*, Inc., New Jersey, Vol. 2.

[6] Moncelet G., 1998. Dependability evaluation of mechatronic automotive systems using Petri nets, Thesis at Paul Sabatier University, Toulouse, CNRS. 158p.

[7] Dufour F. & Dutuit Y., 2002. Dynamic Reliability: A new model, Proceedings of ESREL 2002 Lambda-Mu 13 Conference, Lyon-France, 350–353.

[8] Demmou H., Khalfaoui S., Rivière N. & Guilhem E., 2002. A method for deriving critical scenarios from mechatronic systems, *Journal European of the Automated Systems*, vol. 36, (7), 987-999.

[9] Chalé H. G., Taofifenua O., Gaudré T., Topa A., Lévy N. & Boulanger J. L., 2011. Reducing the Gap Between Formal and Informal Worlds in Automotive Safety Critical Systems, 21st Annual INCOSE International Symposium. Denver, USA.

[10] Batteux M., 2011. Développement d'une chaîne de conception outillée d'un système de diagnostic appliquée aux systèmes technologiques pilotés, Thesis, Paris-Sud 11 University.

[11] Hochon J. C., Champagnat R. & Valette R., 1998. Modeling and simulation of hybrid system through Differential Predicate Transition Petri net, Actes of 4e Colloque African of the Informatique Recherche, DaKar, 737-749.

[12] Boucerredj L. & Debbache NE., 2007. Modelling of a hybrid system through differential predicate transition Petri nets model and proof tree, *International Journal of Aircraft Engineering and Aerospace Technology*, Vol. 79, (3), 261-267.

[13] Sadou N. & Demmou H., 2006. Minimality of critical scenarios in Petri net model, IEEE International Conference on Systems Man and Cybernetcs, Taipei (Taiwan), 3422-3429.

[14] Girard J.Y., 1987. Linear Logic, *Theoretical Computer Science*, 50, 1-102.

[15] Girault F., 1997. Linear Logic formalisation of Petri nets token game, Thesis at Paul Sabatier University, Toulous, CNRS, 178p.

[16] Boucerredj L. & Debbache N. E., 2011. Evaluation de la SdF des systèmes mécatroniques en utilisant la notion de coupe minimale et la logique linéaire, International Conference on Systems and Information Processing. 8 mai 45 University, Guelma, Algeria, 30-36.

[17] Matlab toolbox for Petri nets, Matlab – 2009 - www.mathworks.com.

[18] Boucerredj L. & Debbache NE., 2005. Dependability in the mechatronic systems from a Petri net model, *International Journal on Automatic Control and System Engineering*, Vol. 5, (3), 71-77.

[19] Dabrowski C. & Hunt F., 2011. Using Markov chain and graph theory concepts to analyze behavior in complex distributed systems, Proceedings of the 23rd European Modeling and Simulation Symposium, Rome, Italy, 659-668.