Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

PERTINENT SCENARIOS IN TEMPORAL PETRI NETS FOR CRITICAL SYSTEM ANALYSIS

Nabil SADOU & Hamid DEMMOU

LAAS – CNRS, University of Toulouse
07 avenue du colonel Roche, F31077 Toulouse Cedex
{sadou, demmou }@laas.fr

Abstract: This paper deals with dynamic reliability of embedded systems. It is addressed by generating critical scenarios. This paper proposes a definition of the concepts of minimality and completeness, related to the notion of scenario. These two concepts guarantee the pertinence of scenarios. In Petri net model, a scenario is defined as a partial order between events leading from one partial state to another one. We use linear logic as a new representation of Petri net model. The definition of minimality and completeness is based on this new representation.

Keywords: Critical systems, reliability Petri net, linear logic, scenarios, minimality, completeness

1. INTRODUCTION

Reliability analysis of dynamic systems is based on dynamic models (Dufour and Dutuit, 2002) such as Markov graphs, Petri nets, or various simulation models which can be built from very general modelling languages. These models are interesting for quantitative analysis with Monte Carlo simulation. However, in some cases, the reliability data are not completely available. It is necessary to start with a qualitative study: proof of properties or listing of feared (critical) scenarios.

In our approach for reliability analysis of dynamic systems (Sadou and al, 2005), feared scenarios (which lead from normal states to feared ones) are derived from Petri net model. These scenarios help system designers to identify critical situations and to define corrective actions to avoid them as early as possible in the design stage. Based on linear logic (Girard, 1987) as new representation (using the causality relations) of Petri net model, a qualitative analysis allows to determine a partial order of transition firings and thus to extract feared scenarios (Sadou and al, 2005). The analysis is focalised on the parts of the model that are interesting for the reliability analysis (Sadou and al, 2005) avoiding exploration of the global system and the problem of the state space explosion. This formal framework is based on equivalence between accessibility in the Petri net and the provability of linear logic sequent (Sadou and al, 2005). The method extracts and identifies clearly the feared scenarios starting from a partial knowledge of the feared state.

The final objective is to determine all minimal scenarios (to guarantee minimality and completeness). Indeed, one scenario can lead to a feared state and contains events (that are the consequence of another events of the scenario), which are not strictly necessary to reach this feared state. Such scenario is not minimal. The completeness is also important. Indeed, the designer needs to have all feared scenarios to define appropriate architecture for safe systems. In this paper an overview of the notions related to linear logic is given. The approach for deriving feared scenarios is briefly presented. The formal definition of the minimality and completeness is then proposed. Finally, an industrial example based on the landing system of an airplane is presented.

2. PRINCIPLES OF LINEAR LOGIC

Linear logic proposed by J.Y.Girard (Girard, 1987) is a restriction of the classical propositional logic in order to introduce the notion of resource (Girard, 1987). The sequent calculus associated to this logic is based on a new set of connectors and rules: the main difference with classical logic is the absence of usual contraction and weakening rules. These rules are precisely the ones forbidding the correct handling of multiple copies because of the equivalence (in classical logic) between proposition "*p AND p*" and proposition "*p*". Discarding these rules leads to split each one of the classical *AND* and *OR* connectors into two different ones getting four different connectors. In this paper we will only use two linear logic connectors, the times connector $\otimes$ to represent resource accumulation (formula $a \otimes b \otimes b$ expresses that one copy of resource a and two copies of resource b are available) and the linear logic implication (represented by the symbol $\multimap$). This implication permits to handle resource production and consuming. For example, formula $a \multimap b$ states that resource a is consumed when resource b is produced. The translation of a Petri net to linear logic has been presented in (Pradin and al, 1999).

For a given Petri net, the translation is done as follows:

- An atomic proposition P is associated with each place P of the Petri net
- A monomial using the multiplicative conjunction $\otimes$ (TIMES), is associated with each marking, pre-condition *Pre( )* and post-condition *Post( )* of transition
- To each transition t of the net an implicative formula is defined as follows :

$$t : \underset{i \in Pre(pi,t)}{\otimes} P_i \multimap \underset{o \in Post(po,t)}{\otimes} P_o$$

Each sequent of the form $M, t_1, \ldots, t_p \vdash M'$ expresses the reachability between the markings M and M', by indicating which are the fired transitions ($t_1, \ldots, t_p$). The proof is derived in a canonical way. Using the rule for introducing the connector on the left hand side ($_L$) allows changing the initial marking with a set of atomic formulas (tokens, not necessarily used at the same date). By applying the $\multimap_L$ rule, it is possible to extract the causal relations of the atomic formulas from marking M to M'.

Building the proof generates a proof tree which begins by a sequent and finishes by the identity axiom. Moreover, it is possible to extract information about the firing order of transitions and temporal evaluation of scenarios in temporal Petri nets from the proof tree of the sequent (Sadou and Demmou, 2006).

3. METHOD FOR DERIVING FEARED SCENARIOS

3.1 General view of the scenario extraction method

The method is based on a qualitative analysis initiated from the Petri net model. The objective is to extract and clearly identify the feared scenarios starting from a model that contains the necessary knowledge to make the analysis. The initial partial knowledge of the feared state is progressively enriched by analyzing the components necessary to its occurrence. This method is made up of two steps: a backward and a forward reasoning. The backward reasoning starts from the partial feared state in order to determine the events that are necessary to reach it, and gives the last nominal states preceding the abnormal behavior. The forward reasoning starts from these nominal states, and determines the components that are implicated in the feared scenario. To determine the complete context in which the feared scenario occurs, the concept of context enrichment is introduced. Each time it is necessary the context is enriched by adding tokens to some places that can have an impact on the feared scenario. Linear logic transpose the problem of reachability into a problem of sequent proving which is more simple and efficient, and gives a formal and logical framework that ensures the coherence of the causality links and the partial orders. The problem of the partial context (partial marking of Petri net) can easily be addressed with Petri net associated to the linear logic. Indeed in a linear logic any proof remains true if we enrich linearly the context (monotony in traditional logic).

3.1 Principles of the scenario deriving algorithm

The backward and the forward reasoning are similar and it is why the procedures (algorithm) are the same for both of them (Demmou and al, 2002). The backward reasoning is done on the reversed Petri net with the target feared states as initial marking. Forward reasoning evolves in the initial Petri net with the conditioning (nominal) places as initial marking. In Petri net model, a transition is fireable if it is enabled (its input places are marked). In temporal Petri net, the transition must be enabled and the temporal constraints must be satisfied.

The backward reasoning evolves without taking into account the temporal constraints. If a transition is potentially enabled (some places are marked and other ones are empty) the empty places are enriched by adding tokens to make it fireable. The determination of the conditioning states is done by reachability analysis between the feared states and the normal sates; transitions are fired until a nominal marking (normal working of the system) is reached. In the forward reasoning both discrete and temporal evolution guide the scenarios deriving. It is done in the temporal Petri net. The conditions related to temporal constraints may be satisfied for transition firing.

4. SCENARIO AND MINIMALITY

4.1 Scenario

Definition 1 (*Event and set of events*)**:** Let a Petri net *(P, T, Pre, Post)* and M_0 its initial marking. An event is a distinct firing of a transition. The set of events is noted E. Any subset of E is a set of events.

Definition 2 (*temporal Petri net*)**:** a temporal Petri net is a pair N_{tl}=<N, D> where N is a Petri net <*P, T, Pre, Post* > and D is a function that associates to each t_i a static temporal interval *d(ti) = [dimin(ti), dimax(ti)]* that describes the enabling duration.

Let a Petri net (P, T, Pre, Post) with an initial marking M_0 and a final marking M_f. Let I a set of events that represent the creations of the tokens associated to the initial marking (one event by token) and F a set of events that represent the consumption of tokens associated to the final M_f (one event by token).

Definition 3 (*Scenario*) A scenario $SC = (l, \prec_{sc})$, associated to the temporal Petri net N_{tl}, the markings M_0, M_f and a set of events $l \subset (E \cup I \cup F)$ is a strict partial order defined on the set of events l.

The partial order $\prec_{sc}$ is composed by the order relation deduced from the causalities present in the Petri net model noted $\prec_{PNsc}$ and the order relation generated from the temporal constraints, noted $\prec_{tsc}$.

In our representation of scenarios, partial order is defined by a directed graph (E, A) where the nodes E are a set of transition firings and the arcs A are pairs (t_i, t_j) such that ti precedes t_j (t_i and t_j are transition firings). To each arc A, we associate an atom that represents the token produced by the firing of the transition t_i and consumed by the firing of the transition t_j. The temporal constraints are represented by the discontinuous arrows.

In the Petri net of the figure 1 the precedence graph represents the scenario $P_1 \otimes P_2 \otimes P_3, t_2, t_3 \vdash P_5 \otimes P_7$ that leads from the marking $P_1 \otimes P_2 \otimes P_3$, to the marking $P_5 \otimes P_7$. The precedence relation between the firing of the transition t_2 and the transition t_3 imposed by the temporal constraints implicates that the transition t_2 is fired if and only if the transition t_3 is fired.

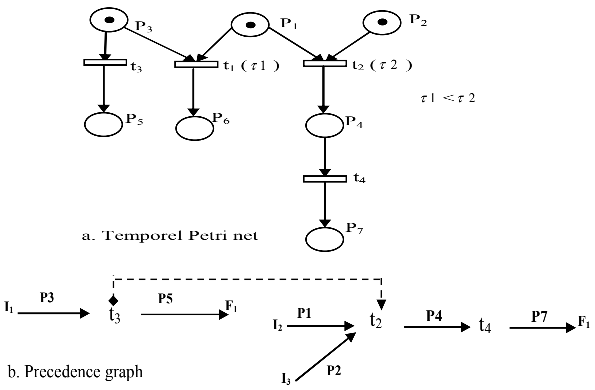

Fig. 1. Example of Petri net & precedence graph.

Definition 4 (*sufficient Scenario*): Let l be a set of events, $l \subset (E \cup I \cup F)$ and $l' = l \cap E$ be the restriction of l on E. The scenario $sc = (l, \prec_{sc})$ is *sufficient* to reach M_f from M_0 if the sequent $M_0, l \vdash M_f$ is provable and if there exist a partial order $\prec_j$ resulting from a proof tree such that $\prec_j = \prec_{PNsc}$ and another partial order $\prec_k = \prec_{tsc}$

4.2 Minimality (minimal scenario)

In a previous work (Sadou and Demmou, 2006) we defined the notion of minimal scenario. In this paper we give a short overview. To define a minimal scenario we need to define minimal marking. Indeed, in our deriving feared scenarios approach, the context (marking of Petri net) is only partially known. In (Sadou and Demmou, 2006) we proved that the characterization of the scenario depends on the final marking that represents the feared state. If this final state contains useless partial states (tokens in Petri net model), the scenarios will also contain useless events. It is thus necessary to define a minimal feared state (final state) and minimal initial state. Minimal marking corresponds to the minimal cutsets (Sadou and Demmou, 2006) associated to a Boolean expression that represents the marking associated to the feared state. Thus a minimal scenario is defined for a final and initial markings associated to each minimal cutset.

Example *(figure 2)*: The marking that represents the feared state can be represented by a Boolean function. We note B*(P)* the Boolean associated to the place *P*. If *B(P)* is true the place *P* is marked and if *B(P)* is false the place is empty. In the example (Figure 2), the function R associated to the feared state is: $R = B(KOs) \vee (B(KO1) \wedge B(KO2))$. Two minimal cutsets associated to the function *R* :

$C_1 = B(KOs)$ and $C_2 = B(KO1) \wedge B(KO2)$

We characterize the final marking associated to a cutset C_i by $C_i \otimes Cont_i$ where $Cont_i$ represents an unspecified context. The context $Cont_i$ is defined progressively with the construction of the scenario. It corresponds to edge effects (marking of some places of the Petri net) consequence of the marking of the places corresponding to the minimal cutset.

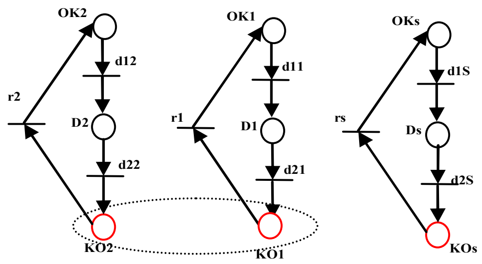

Fig.2. Minimal initial and final markings

Definition 5 (*minimal scenario for a cutset***):** Let us consider a Petri net and a final marking $M_{fi} = C_i \otimes Cont_i$ associated to a minimal cutset C_i for a given feared state. M_{0S} is the initial marking of the Petri net. Let us consider a set of events $l_i \subset (E \cup I \cup F)$ with $l_i' = l_i \cap E$ the restriction of l_i to E and M_{0i} $(M_{0i} \subset M_{0s})$ a given initial marking. The scenario $sc_i = (l_i, \prec_{sci})$ with G as precedence graph is minimal for cutset C_i to reach M_{fi} from M_{0i} if it is sufficient between M_{0i} *and* M_{fi}, and if and only it don't exist a scenario $sc_j = (l_j, \prec_{scj})$ with precedence graph G' such that:

i) The scenario $sc_j = (l_j, \prec_{sc_j})$ is sufficient to reach M_{fi} from M_{0j} with $(M_{0j} \subset M_{0s})$ and $M_{fj} = C_i \otimes Cont_j$ (same minimal cutset)

ii) $l_j \subset l_i$

iii) the precedence graph G'(see[1] for more information and some examples) is identical to *G _rest* restriction of *G* to the elements of the set l_j completed by the precedence relations induced by the elements of $(l_i\text{-}l_j)$ in *G* with transitivity.

When the condition ***(iii)*** is verified, it implies the presence of some events (events of the set $(l_i\text{-}l_j)$) that are not necessary. Indeed the suppression of these events does not modify the precedence relations between the other events (events of the set l_j) which are sufficient to reach the final marking associated to the corresponding minimal cutset.

5. COMPLETENESS

The definition of the completeness is related to minimality of scenarios. As for the minimality (Sadou and Demmou, 2006) we have two cases: the case when the markings are completely known and the case when the marking are partially known. In the first case, the definition is trivial, but in the second case (which is the case in our scenarios deriving approach), the definition is done for minimal initial and final marking.

5.1 Completeness (Fixed initial and final markings)

Definition 6 (*complete set of scenario*): Let a Petri net *P = (P, T, Pre, Post)*, initial marking M_0 and final marking M_f.

Let *SC, SC= {sc1, sc2,…, scn}* be a set of scenarios sufficient to reach M_f from M_0. The set *SC* is complete between the markings M_0 and M_f if there is no scenario *sci* minimal to reach M_f from M_0 such that $sci \notin SC$. (each minimal scenario belongs to *SC*).

In the example of the figure 3 between the markings $M_0=P1$ and $M_f=P4$, the set of scenarios *SC={sc1, sc2, sc3, sc4}* is complete between these two markings:

$$sc_1: \; P1, \; a,c \vdash P4 \,, \; sc_2: \; P1, \; b,d \vdash P4$$
$$sc_3: \; P1, \; a,e \vdash P4 \,, \; sc_4: \; P1, \; a,f,a,c \vdash P4$$

The definition 6 implicates that all minimal scenarios may belong to the set *SC*.

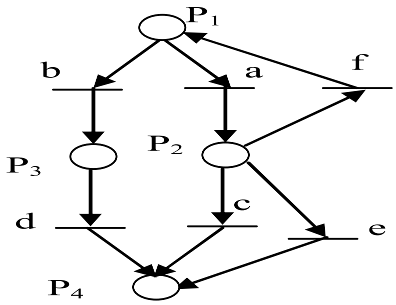

Fig.3. Petri net example

Definition 7 (*complete and minimal set of scenario*): Let a Petri net *P = (P, T, Pre, Post)*, initial marking M_0 and final marking M_f. Let *SC, SC= {sc1, sc2,…, scn}* a set of scenarios sufficient to reach M_f from M_0. The set SC is complete and minimal between the markings M_0 and M_f if:

- Each scenario of SC is minimal to reach M_f from M_0.

- There is no scenario *sci* that is minimal between M_0 and M_f such that $sci \notin SC$.

The set of scenarios is complete and minimal if it contains all the minimal scenarios but only the minimal ones.

In the example (figure 3) between the markings $M_0=P1$ and $M_f=P4$, the set *SC = {sc1, sc2, sc3}* is complete and minimal, while the set *SC' ={sc1, sc2, sc3, sc4}* is complete but not minimal.

5.2 Completeness (Minimal initial state and minimal feared state)

In this case the initial and final markings are partially known, the completeness may be defined for minimal final marking (associated to minimal cutsets) and set of minimal initial partial markings (determine by the backward reasoning). The determination of the minimal initial state is necessary. If we don't define these initial states, the completeness doesn't have sense. Indeed, the number of initial markings can be infinite. For each minimal cutset associated to the feared state, following the backward reasoning, we obtain some initial partial marking MP_j. The MP_j are the minimal initial markings that will be considered in the step of forward reasoning (conditioning states). The definition of the completeness is done between these initial markings and the final marking associated to the minimal cutset.

Backward reasoning: From each final marking associated to a minimal cutset ($Cont\_back_i$ is the unspecified context defined progressively with the backward reasoning). With the backward reasoning we obtain $M_{0j} = MP_j$ with *j= 1 to n* and *MP* an initial partial marking.

We obtain some scenarios expressed as follows: $C_i \otimes Cont\_Back_i, \; l_{back} \vdash MP_j$ *j=1 to n (*In the inverse Petri net).

Forward reasoning: From each initial marking MP_j determined in backward reasoning following the forward reasoning, we obtain some scenarios of the form:

$$MP_j \otimes Cont\_Forw_k, \; l_{av} \vdash C_i \otimes Cont\_Back_i \otimes Cont\_Forw_l$$

k =1 to m (In the initial Petri net).

Where $Cont\_Forw_k$ and $Cont\_Forw_l$ are the contexts that are necessary to reach the minimal cutest from the initial markings MP_j.

The complete set of scenarios may be defined for each minimal cutset considering all partial initial markings.

5.3 Complete set of scenarios associated to minimal cutsets

Definition 8 (*complete set associated to minimal cutset*): Let *P = (P, T, Pre, Post)* be a Petri net. Let *Ci* be a minimal cutset associated to a final marking. Let *SC* be the set of scenarios. The set SC is complete for the minimal cutest C_i if and only if each scenario sc_i minimal between the initial markings $MP_j \otimes Cont\_Forw_k$ and the final marking $C_i \otimes Cont\_Back_i \otimes Cont\_Forw_l$,belongs to SC

.**Definition 9** (*complete and minimal set of scenarios associated to minimal cutset*):

Let *P = (P, T, Pre, Post* be a Petri net*)*. Let C_i be a minimal cutset associated to a final marking

Let *SC* be a set of scenarios.

The set of scenarios SC is complete and minimal for the minimal cutset C_i if and only if *SC* contains only all minimal scenarios between the initial marking $MP_j \otimes Cont\_Forw_k$ and the final marking $C_i \otimes Cont\_Back_i \otimes Cont\_Forw_l$.

6. APPLICATION EXAMPLE

This case study concerns the landing system of a military airplane made by Dassault Aviation (Villani and al, 2003). The purpose is to characterize the feared scenarios that can affect the safe proprieties of its control software. Three landing sets containing each one a door and a landing gear compose the landing system. For landing, the following sequence must be performed: open the doors, retract the landing gears and close the doors. The scenario analysis will be focused on the feared events associated to the landing operation (extend of the landing gears). We have three feared events for each landing gear:

- Door stuck closed
- The landing gear doesn't extend
- Door stuck open after gear extension.

6.1 System description

The system to be analyzed is composed of three computers controlling three landing gears and doors. The landing gears and doors movement is performed by a set of actuating cylinders. The cylinder position corresponds to the door or landing gear position (when a door is opened, the corresponding cylinder is extended). The cylinders (and the respective door and landing-gear) are considered as the controlled objects. The Rafale landing system has the following actuating cylinders:

- For each door, a cylinder opens and closes the door.
- For each right and left landing gear, a cylinder extends and retracts the landing gear and another cylinder blocks the landing gear in the extended position.

For the front landing gear, a cylinder retracts, extends and blocks the landing gear in the extended position. In order to improve the safety of the system four relief electro-valves are introduced, one for the opening, one for the closing, one for the extension and one for the retraction. Only one of the front, right or left landing gear system can use a relief electro-valve at a time. The computer sends the command E to extend the gears or R to retract the gears. An up/down handle is provided to the pilot. When the handle is set UP the extending landing-gear sequence is accomplished, when the handle is set DOWN the retracting landing-gear sequence is accomplished.

6.2 System modeling and application

When the place Ps0 of figure 4 is marked the door is close, if a command is send to open the door, the transition tn0 is fired but only if the elctro-valve ev1 is available: if it is not. a relief electro-valve is used and the transition tr0 is fired. In the case the relief electro-valve (that is shared with other components of the system) is used (firing of the transition t1), the transition red1 is fired and the system reaches the feared state (marking of the place E_red1). In the place P0 the opening starts. If the electro-valve is switched to off (firing of def_1) while the door is opening then the transition t_{d1} is fired. So the system is in sticking situation. If the relief electro-valve can be used (place *ev_relief_ok* marked) the transition tr1 is fired allowing the opening process until the door is completely open. If the relief electro-valve can't be used, the transition *red2* is fired and the feared state is reached.

In the Petri net of figure 4, the target place is *E_red1*. The minimal cutest associated to the feared state is $C = B(E\_red_1)$. It will be the initial minimal marking considered for the first backward reasoning (inversed Petri net). For the minimal cutset $R_1 = E\_red_{11}$ two initial partial markings are possible $MP_1 = Ps_0$ and $MP_2 = Ps_{12}$ (obtained from backward reasoning), which correspond respectively to the following scenarios (inverse Petri net)

Sc1: $E\_red_1,\ red_1 \vdash Ps_0$

Sc2: $E\_red_1 \otimes ev_1\_bo,\ red_2, td_1, def_1 \vdash P_0 \otimes ev_1\_ok$

These two partial markings ($MP_1 = Ps_0$ and $MP_2 = P_0 \otimes ev_1\_ok$) represent the initial markings that will be considered for the forward reasoning.

The complete set of scenario leading to the marking that represents the feared state (minimal cutest E_red_1) contains four scenarios which are:

Scenario 1:

$Ps_0 \otimes ev_1\_ok \otimes ev\_ok \quad , def_1, def, red_1 \vdash$

$E\_red_1 \otimes ev_1\_bo \otimes ev\_hs$

Where:

$Cont\_Forw_k = ev_1\_ok \otimes ev\_ok$ and

$Cont\_Forw_l = ev_1\_bo \otimes ev\_hs$

Scenario 2*:*

$Ps_0 \otimes ev_1\_ok \otimes ev\_ok \otimes P1 \quad , def_1, t_1, red_1 \vdash$

$E\_red_1 \otimes ev_1\_bo \otimes P_2$

Scenario 3:

$Ps_0 \otimes ev_1\_ok \otimes ev\_ok \otimes P1 \quad , def_1, t_1, red_1 \vdash$

$E\_red_1 \otimes ev_1\_bo \otimes P_2$.

Scenario 4:

$P_0 \otimes ev_1\_ok \otimes ev\_ok \otimes P1 \quad , td_1, def_1, t_1, red_2 \vdash$

$E\_red_1 \otimes ev_1\_bo \otimes P_2$

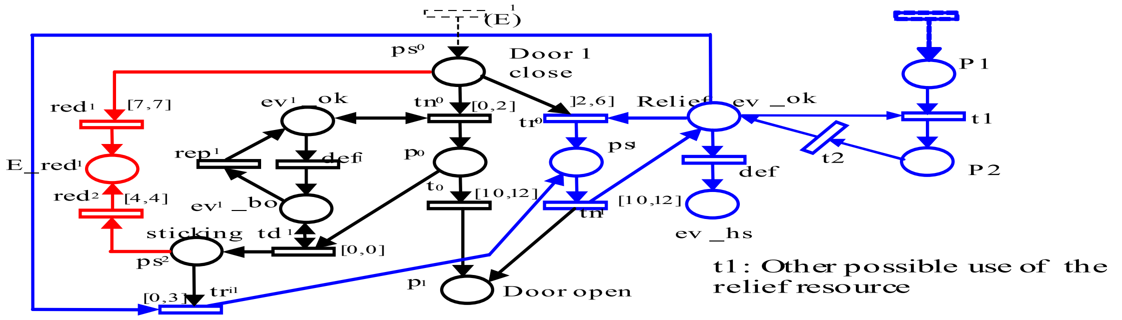

Fig. 4. Opening Petri net model of the three doors

7. CONCLUSION

In this paper the definition of minimality and completeness of critical scenarios (scenarios that lead to feared state) generated from temporal Petri nets model are defined. The new representation of a Petri net with formulas of linear logic allows us to define them formally. A minimal scenario represents a class of scenarios, and it contains only the events that are necessary. In minimal scenario the order relations between events must be effective relation of causality in the system and the list of event of the scenario must be minimal (without loop events of the system). The minimal scenario is defined between minimal final marking corresponding to the feared state and minimal initial marking. From the definition of minimal scenario, the completeness is defined in two cases. The first case is trivial and concerns the case where the initial and final markings are completely known. In the second case from the minimal final marking (characterized by minimal cutest) a minimal initial state is defined. If we don't define these initial states, the completeness doesn't have sense. Indeed, the number of initial markings can be infinite. Between these two markings, the complete set of scenarios is defined. It guaranties that all scenarios are derived.

The algorithm has been implemented in Java and the notions of minimality and completeness was integrated. The presented results of the application example have been obtained with this implementation.

REFERENCES

Sadou. N, H. Demmou. Minimality of critical scenarios in Petri net model. 2006 IEEE International Conference on Systems Man and Cybernetics (SMC'06), Taipei (Taiwan), 8-11 October 2006, 8p.

Dufour. F, Y. Dutuit, "Dynamic Reliability: A new model", λμ13-ESREL2002 European Conference, Lyon - France - 18 au 21 Mars 2002.

Girard. J.Y, " Linear Logic ", Theoretical Computer Science, 50, 1987, p.1-102.

Sadou. N, H. Demmou, J.C. Pascal, R. Valette. Object oriented approach for deriving feared scenarios in hybrid system. 2005 European Simulation and Modelling Conference, Porto (Portugal), 24-26 Octobre 2005, pp.572-578.

Pradin-Chézalviel. B, R. Valette, L.A. Künzle: "Scenario duration characterization of t-timed Petri nets using linear logic", IEEE PNPM'99, 8th International Workshop on Petri Nets and Performance Models, Zaragoza, Spain, September 6-10, 1999, p.208-217.

Demmou. H, S. Khalfaoui, N. Rivière, E. Guilhem, « A method forderiving critical scenarios from mechatronic systems », Journal Européen des Systèmes Automatisés, volume 36 – n°7/2002, pages 987 à 999.

E. Villani , F. Junqueir, P.E. Miyagi, R. Valette Petri net and OO for the modular analysis of an aircraft landing system.17th International Congress of Mechanical Engineering (COBEM'2003), Sao Paulo (Brésil), 10-14 Novembre 2003, 10p.