Critical scenarios for dynamic systems reliability

Nabil SADOU, Hamid DEMMOU

LAAS-CNRS, University of Toulouse
07, avenue du colonel Roche
F-31077 Toulouse Cedex 04
{sadou, demmou}@laas.fr

ABSTRACT. This paper deals with reliability of dynamic 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: Temporal Petri nets, linear logic, scenario, minimality, completeness

1. Introduction

Reliability analysis of dynamic systems is based on dynamic models [Dufour and al., 2002] such as Markov graphs, Petri nets, or various simulation models which can be built from very general modeling 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.

For static systems the most popular approach for reliability analysis is based on fault trees [Lee and al., 1995]. A fault tree provides a simple modelling framework to represent the interactions between components form the reliability point of view. Static fault trees use traditional Boolean Logic functions to represent the combination of components failures (events) that cause system failure. One interesting aspects of fault trees is that a set of minimal cutsets [Rauzy, 2001] (similar to the prime implicants of the Boolean function) can be derived. These minimal cutsets (as well as the prime implicants) are a combination of all the necessary failures of components that lead to system failure. To deal with the complexity of dynamic systems, fault trees, are not sufficient: safety analysis of such systems must include timing considerations and the order of the events [Chris and al., 1995].

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 contain events (that are the consequence of other events of the scenario), which are not strictly necessary to reach this feared state. Such scenario is not minimal. 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 is then proposed.

2. Petri net and 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 :

$$t : \bigotimes_{i \in \Pr e(pi,t)} P_i \multimap \bigotimes_{o \in Post(po,t)} P_o$$

Each sequent of the form M, t1,..,tp ⊢ M' expresses the reachability between the markings M and M', by indicating which are the fired transitions (t1,…,tp). 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 $\multimap \mathrm{L}$ 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 al., 2006].

3. Method for deriving feared scenarios

The method [Sadou and al., 2005] 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 linear logic. Indeed in linear logic any proof remains true if we enrich linearly the context (monotony in traditional logic).

4. Sets of events and scenarios

4.1. Events and sets of events

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 particular firing of a transition $t_i \in T$.

If t_i is fired *n* times then there will be n events corresponding to t_i. These events are noted e_j^i with $j \in [1..n]$ and represent the set of events noted *E*, it is potentially infinite, but it is built from the bounded set *T* of transitions. The events e_j^i for any j correspond to the different firings of the same transition t_i . Any subset $l \subset E$ is a set of events.

4.2. Scenario

4.2.1 Case of ordinary Petri net

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 M_0 (one event by token) and F a set of events that represent the consumption of tokens associated to the final marking M_f (one event by token).

Definition 2 (Scenario): A scenario $SC = (l, \prec_{sc})$, associated to the Petri net *P*, the markings M_0 , M_f and a set of events $l \subset (E \cup I \cup F)$ is a strict partial order $\prec_{sc}$ defined on the set of events *l* .

We note that the events are defined on a set greater than the initial one. We need the concept of initial and final events to compose complex scenarios from elementary scenarios. The firing sequence is the linearization of the restriction of the scenario on the events of *E*.

4.2.1 Case of temporal Petri net

Definition 3 (*temporal Petri net***):** a temporal Petri net is a pair N_{ti}=<*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.

Definition 4 (*Scenario*) A scenario $SC = (I, \prec_{sc})$, associated to the temporal Petri net N_{tl}, the markings M_0, M_f and a set of events $I \subset (E \cup I \cup F)$ is a strict partial order defined on the set of events *I*.

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 precedence relations 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.

Example:

If we consider the example of the figure 1, to the transition t_1 is associated the temporal thresholds $t = \tau 1$ and to the transition t_2 the threshold $t = \tau 2$ with $\tau 1 < \tau 2$. So, considering that *P1* and *P2* marked, if the place *P3* is marked then the transition t_1 will be fired before the transition t_2. Indeed the threshold associated to t1 is lower than the one of t_2. In this case we don't consider the scenario associated to the firing of the transition t_2. But, if t_3 is fired (place *P3 empty*) and if the places *P1* and *P2* are marked, only the transition t_2 can be fired.

The conclusion is. the firing of the transition t_3 is the cause of the firing of the transition t_2. We have a precedence relation between the firing of the transition t_3 which empties the place *P3* and lead to the firing of the transition t_2.

This precedence relation is a consequence of the continuous dynamic of the system modeled by the temporal thresholds associated to the transitions t_1 and t_2. In this case we have a non-direct precedence relation. The partial order $\prec_{tsc}$ contains the non-direct precedence relations. This situation is currently observed in the case of temporal watchdog see [SAD and al,. 2006c].

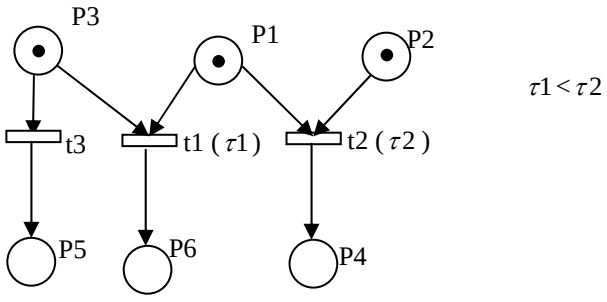


Figure 1. *Temporal Petri net*

Figure 2 shows the precedence graph of the scenario corresponding to the sequent $P1 \otimes P2 \otimes P3, t_2, t_3 \vdash P4 \otimes P5$ (firing of t_3 followed by the firing of t_2). The temporal constraints are represented by the discontinuous arrows.

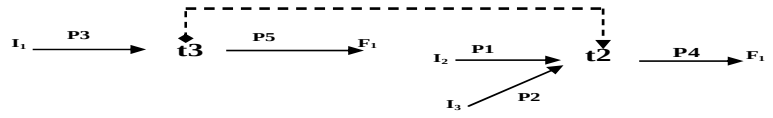


Figure 2. *Scenario generated from the Petri net of the figure 1*

5. Sufficient condition

5.1. Sufficient sets of events

Let us consider a Petri net (*P, T, Pre, Post*) with an initial marking M_0 and a final marking M_f. We remind tthat the proof of sequent in linear logic is equivalent to the accessibility in Petri net model.

Definition 5 (sufficient set): The set of events $l \subset E$ is sufficient to reach M_f from M_0 if the sequent $l, M_0 \vdash M_f$ is provable.

5.2. Sufficient scenarios

4.2.1 Case of ordinary Petri net

Let us consider a Petri net (*P, T, Pre, Post*), an initial marking M_0 and a final marking M_f

Definition 6 (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 $\prec_j = \prec_{sc}$ .The definition means that the set of events must be sufficient to reach M_f from M_0 and the partial order deduced from the proof is exactly the same as the partial order of the scenario.

5.2.2 Case of temporal Petri net

Definition 7 (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.

- There exists a partial order $\prec j$ that results from a proof tree A_i such that $\prec_j = \prec_{PNsc}$.

- There exists a partial order $\prec_T$ that results from temporal constraints associated to the Petri net transitions such that $\prec_T = \prec_{tsc}$.

Note that the partial order derived from a temporal Petri net is composed by a precedence relations derived from the proof tree and the temporal constraints.

6. Minimality

6.1. Minimal set of scenarios

Definition 8 (minimal set): Let $l_k \subset E$ be a sufficient set of events to reach M_f from M_0. The set of events l_k is minimal if and only if there is no set of events $l_i \subset E$ that is sufficient and that is a subset of l_k.

Note that the minimal set between two markings is not unique.

6.2. Minimal scenario

6.2.1 Case of ordinary Petri net

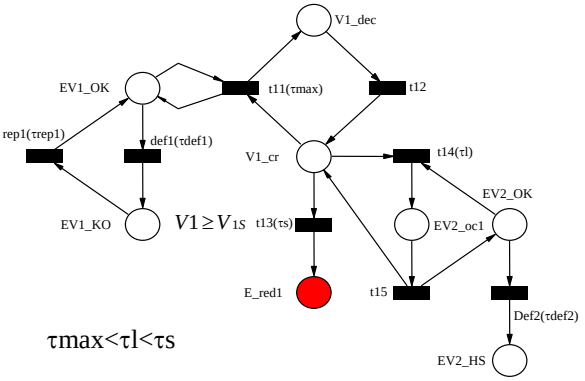
Definition 9 (minimal Scenario) Let *l* be a set of events, $l \subset (E \cup I \cup F)$ and $l' = l \cap E$ be a restriction of *L* on *E*. The scenario $sc = (l, \prec_{sc})$ is minimal to reach M_f from M_0 if it is sufficient and if the set of events l' is minimal.

It is necessary that one of the partial orders obtained by labelling one of the proof trees of sequent $M_0, l_i \vdash M_f$, be exactly $\prec_{sc}$.

6.2.2 Case of temporal Petri net

The definition of minimal scenario is the same as the case of ordinary Petri net. In the case of temporal Petri net the definition is based on the definition of sufficient scenario which contains direct (derived from proof tree) precedence and non-direct precedence relations. (derived from temporal constraints)

The scenario of figure 3 is not minimal. Indeed the precedence relation between the events *def1* and *def2* does not correspond to any temporal constraints in the Petri net.



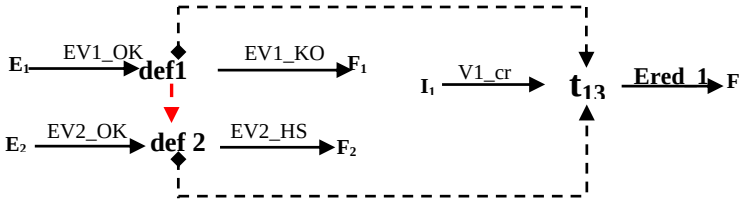


Figure 3. *Example*

6.3 minimal initial and final markings

As said in the introduction, the research of the feared scenarios is focused on the interesting parts of the model from reliability point of view [Sadou and al., 2006b]. We analyse only the parts that can be concerned by the feared state. So we have only a partial knowledge about the initial marking, and about the final marking we know only the part corresponding to the dangerous partial state. The choice of initial and final partial markings has an impact on the minimality of the scenarios [Sadou & al., 2006a].

To define a minimal scenario we need to define a minimal marking. Indeed, in our deriving feared scenarios approach, the context (marking of Petri net) is only partially known. In [Sadou and al., 2006a] 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 al., 2006a) 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 4): 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 4), the function R associated to the feared state is: $R = B(KOs) \vee (B(KO1) \wedge B(KO2))$. Two minimal cutsets are 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.

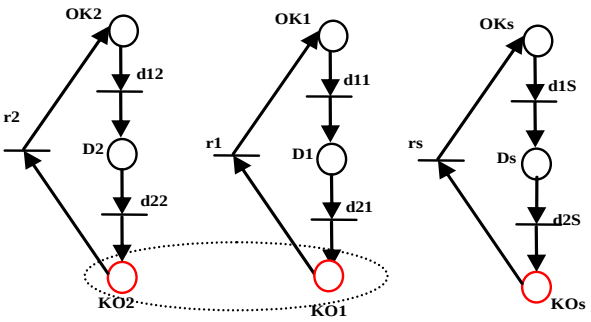


Figure 4. *Minimal initial and final markings*

Definition 10 (Restricted precedence graph): let a precedence graph *G* associated to a scenario $sc_i = (l_i, \prec_{sci})$ and the set of events l_j an subset of l_i.

Let:

- C_m a connex component of the precedence graph *G* composed by the event of the set $(l_i - l_j)$.
- e_i events of C_m.
- e_k an event of l_j such that the event e_k precedes at least one event e_i
- e_l an event of l_j such that it exists at least one event e_i that precedes the event e_l.

The Restricted precedence graph *G_rest*, restriction of *G* to the elements of l_j is the precedence graph *G* where each connex component is deleted and replaced by:

- The precedence relation induced by the element of C_m in G with transitivity between the events e_k and e_l.
- A final event when there is not event e_i that precedes event e_l
- An initial event when there is not event e_k that precedes event e_i.

Definition 11 (*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 Ci 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 $(l_i - l_j)$ in *G* with transitivity.

When the condition *(iii)* is verified, it implies the presence of some events (events of the set $(l_i - l_j)$) 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.

Example

In the example of the figure 3 [Sadou and al. 2006b], if we consider the minimal cutset $C_1 = E\_red1$, between the markings $M_{01} = EV1\_OK \otimes V1\_cr \otimes EV2\_OK$ and $M_{f1} = EV1\_KO \otimes EV2\_HS \otimes E\_red1$, the scenario sc*1* corresponding to M_{01}, $l_1 \vdash M_{f1}$ composed by the set of events $l_1 = def1^1 \otimes def1^2 \otimes rep1 \otimes def2 \otimes t13$ is not minimal. Indeed, there exits the scenario sc2 sufficient between the markings $M_{02} = EV1\_OK \otimes V1\_cr \otimes EV2\_OK$ and $M_{f2} = EV1\_KO \otimes EV2\_HS \otimes E\_red1$. This scenario corresponds to M_{02}, $l_2 \vdash M_{f2}$ composed by the set of events $l_2 = def1^1 \otimes def2 \otimes t13$ with $l_2 \subset l_1$. The sequent :

$Cont_j - (Cont_i \cap Cont_j) \otimes (M_{0i} - M_{0j}) \otimes M_b,\ (l_i - l_j) \vdash\ Cont_i - (Cont_i \cap Cont_j) \otimes M_b$

which corresponds in the Example to M_b, $def1 \vdash M_b$ (elementary loop) is provable with $M_b = EV1\_OK$. The graph of the figure 5 corresponds to precedence graph of the scenario sc1. We can notice that the completed graph with precedence relations induced by the elements of $(l_1 - l_2) = def1$ by transitivity is identical to the graph of the figure 3 which corresponds to the precedence graph of the minimal scenario sc_2.

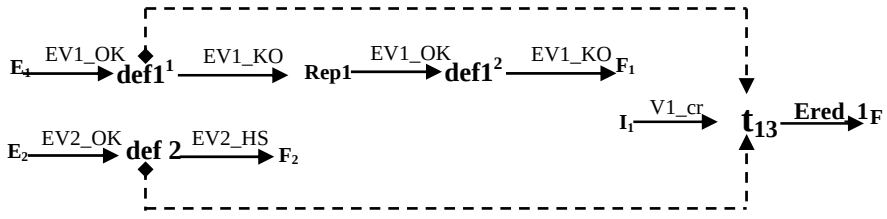


Figure 5. *Precedence graph associated to the scenario SC1*

7. Completeness

The definition of the completeness is related to minimality of scenarios. As for the minimality 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.

7.1 Completeness (Fixed initial and final markings)

Definition 12 (*complete set of scenario***)**: Let a Petri net *P = (P, T, Pre, Post)*, the initial marking M_0 and the 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 minimal scenario *sci* 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 12 implicates that all minimal scenarios may belong to the set *SC*.

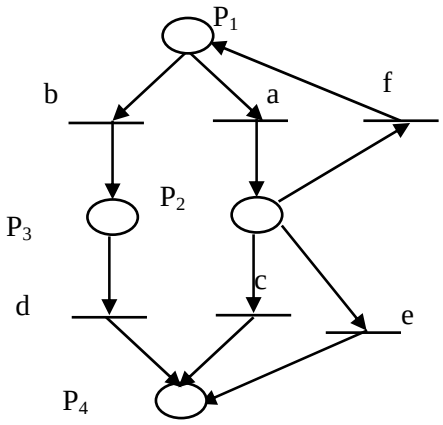


Figure 6. *Completeness example*

Definition 13 (*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.

7.2. 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 (determined 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.

Definition 14 (*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 minimal scenario sc_i 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 15 (*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 $C_i \otimes Cont\_Back_i \otimes Cont\_Forw_l$.

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 made it possible to introduce a formal definition of these two concepts. A minimal scenario represents a class of scenarios, and it contains only the events that are necessary. In a 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 corresponding algorithm has been implemented in Java and the notions of minimality and completeness was integrated into the tool ESA-PetriNet. This tool has been used to derive the different scenarios presented in the paper.

References:

Chris J. GARRET, Sergio B. Guarro, George E. APOSTOLAKIS, "The Dynamic Flowgraph Methodology for Assessing the Dependability of Embedded Software Systems", IEEE Transactions On Systems, Man, and Cybernetics, Vol. 25, No. 5, May 1995.

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

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

Lee. W.S, Grosh. D.L, Tillman. F.A, Lie. C.H. "Fault tree analysis, methods, and applications – A review", *IEEE Transactions on Reliability*, August 1, 1985; ISSN 0018-9529; r-34, page 194-203.

Medjoudj. M, Khalfaoui. S, Demmou. H, Valette. R. "A method for deriving feared scenarios in hybrid systems". *In Probabilistic safety assessment and management (PSAM 7 – ESREL 04)*. Berlin, Germany, 14-18 June.

Pradin-Chézalviel. B, Valette. R, Künzle. L.A. "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.

Rauzy. A. Mathematical Foundation of Minimal Cutsets. *IEEE Transactions on Reliability*, 50(4):389-396, december 2001.

Rivière. N, "Modélisation et analyse temporelle par réseaux de Petri et logique linéaire", thèse de l'INSA de Toulouse, le 26 novembre 2003.

Sadou. N, Demmou. H, 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.

Sadou. N, Demmou. H. 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.

Sadou. N, Demmou. H. Hybrid simulation for critical scenarios derivation. *2006 European Simulation and Modeling Conference (ESM'2006)*, Toulouse (France), 23-25 October 2006, pp.361-366.

Sadou. N, Demmou. D, Pascal. P, Valette. R. Continuous dynamic abstraction for reliability and safety analysis of hybrid systems. *6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*. August 29-September 1 ,2006, Beijing, P.R. China, 6p.