Minimality of Critical Scenarios in Petri Net Models

Nabil SADO and Hamid DEMMOU

Abstract—The aim of this paper is to define the concept of minimality of scenarios, considering that in our approach a scenario is defined as a partial order between events. For deriving feared scenario (ie: scenario that leads the system to critical situation) Petri nets are used for the modelling of systems. To avoid space state explosion, Petri net reachability is translated into provability of linear logic sequent. It is possible to determine a partial order of transition firings and extract feared scenarios which are represented by sequents.

By analogy with the concept of minimal cutsets for the fault trees, we define in this paper the concept of minimal scenario.

Key words — Petri nets, scenarios, linear logic, minimality, partial order

I. INTRODUCTION

Embedded systems run the computing devices hidden inside another larger system or a product (cars, trains, planes, cell phones etc.). Embedded mechatronic systems have the charge of controlling various types of sub-systems composed of mechanic and hydraulic parts; they are also in charge of the monitoring of the whole system and of the coordination with other systems. Considering mechatronic systems in the automobile domain and focusing on safety analysis, it is very important to help car designers to identify critical scenarios and define corrective actions to avoid them as early as possible in the design stage. This means that when some event, affecting the safety of the system occurs, a reconfiguration action is executed in order to maintain the vehicle in a safe degraded state. If the reconfiguration fails then the system will reach a feared (dangerous) state with dramatic consequences for the passengers. So it is important to understand how the system reaches such feared states at the early design stage of the system to set up the reconfiguration actions.

For static systems the most popular approach for reliability analysis is based on fault trees [1]. 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 [2] (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 [3]. For the dynamic reliability (system with reconfigurations) a method for deriving feared scenarios is developed in [4]. The analysis of the Petri net model of the system makes possible to determine a partial order of transition firings and thus to extract the feared scenarios. The method is based on linear logic [6] as a new representation of Petri net model. It is based on equivalence of reachability in the Petri net and provability of sequents in linear logic [7].

This formal framework allows us to focus the analysis on the interesting parts of the model for reliability studies [5]. Then we avoid exploration of the global system and the problem of state space explosion. This analysis aims at deriving feared scenarios by determining causality links between events [5]. The objective of our work is to determine minimal scenarios. 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 the final feared state. Such scenario is then not minimal. In this paper we give the formal definition of the notions related to our approach and then, as the concept of minimal cutsets was defined for the fault trees [2], we define a minimal scenario. This definition will be used in our algorithm to derive automatically critical scenarios but only minimal ones.

II. PRINCIPLES OF LINEAR LOGIC

A. Petri nets and linear logic

Linear logic proposed by J.Y.Girard [6] is a restriction of the classical propositional logic in order to introduce the notion of resource. By introducing new connectors, it clearly differentiates a unique copy of a resource $p$ (expressed by proposition $p$) from the presence of two copies of the same resource (proposition $p \& p$) [6]. The sequent calculus associated to this logic is based on a new set of connectors and rules: the main differences with classical logic are due to the absence of usual contraction and weakening rules. Theses 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 “$p$”. Descarding 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 \( \rightarrow \)). This implication permits to handle resource production and consuming. For example, formula \( a \rightarrow b \) states that resource \( a \) is consumed when resource \( b \) is produced. The translation of a Petri net to linear logic [6] has been presented in [7]. 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 \( \text{Pre}(\cdot) \) and post-condition \( \text{Post}(\cdot) \) of transition
- To each transition \( t \) of the net an implicational formula is defined as follows:

\[
\text{pre}(t) \otimes P_t \rightarrow \otimes P_o
\]

Each sequent of the form \( M, t_1, \ldots, t_p \rightarrow M' \) 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 [9]. Using the rule for introducing the \( \otimes \) connector on the left hand side \( \otimes \) allows changing the initial marking with a set of atomic formulas (tokens, not necessarily used at the same date). By applying the \( \rightarrow \) rule, it is now possible to extract the causal relations of the atomic formulas from marking \( M \) to \( M' \).

A marking \( M \) is a monomial, denoted \( A_1 \otimes A_2 \otimes \ldots \otimes A_k \), where \( A_i \) are place names: if any place \( A_i \) contains several tokens \( n \), for example, \( n \) instances of the proposition \( A_i \) appear.

A transition is a formula \( M_1 \rightarrow o M_2 \) where \( M_1 \) and \( M_2 \) are markings (in fact, \( \text{Pre} \) and \( \text{Post} \) functions of the transition). The expression \( M_1 \rightarrow o M_2 \) represents the transition firing and it will appear in a sequent as many times as this transition is fired.

A scenario can be represented by a sequent in linear logic. The initial marking and the considered multi-set of transition firing are the premises of the sequent, while the final marking is the conclusion. Proving the sequent is equivalent to establish the reachability of the final marking from the initial one. The sequent \( M, \sigma \rightarrow M' \) represents a scenario with \( \sigma = t_1, \ldots, t_n \) the ordered list of the different firing instances of the concerned transitions whereas \( M \) and \( M' \) are respectively initial and final marking.

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 from the proof tree of the sequent [9].

---

**B. Proof of a sequent and labeling the proof tree**

A reachability proof in a Petri net model is equivalent to the proof of the corresponding sequent. The objective is to derive a partial order on the set \( \lambda_0 \) of the fired transitions of the proof tree. A sequent proof tree is a syntactical proof. The canonical construction of the proof tree is based on an iterative step which consists in eliminating each transition firing of \( \lambda_0 \) after having verified that the required atoms have been produced. This step has to be executed once for each transition firing of \( \lambda_0 \). The precedence relations imposed by the structure and the markings of the Petri net are those which relate, for each atom, the application of the iterative step which produces it with the one which consumes it. These precedence relations are obtained by building labelled proof tree [9] and formally define one scenario.

Proving a sequent gives one proof tree for each firing sequence. By proving a sequent \( m \) proof trees can be derived. Labeling a proof tree can produce \( n \) precedence graphs. The figure 2 shows how a labelled proof tree is built for the sequent \( P_1 \otimes P_2, t_5 \otimes t_6 \otimes t_7 \rightarrow P_3 \otimes P_4 \) (Petri net of the figure 1). This proof tree corresponds to one particular firing order \((a, b, c)\), where the token used to fire transition \( c \) is the one produced by transition \( a \) firing. In the final marking the token in \( P_3 \) is the one produced by the firing of \( b \).
III. SETS OF EVENTS AND SCENARIOS

A. 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 \(e^i_j\) with \(j \in \{1..n\}\) and represent the set of events noted \(E_i\) it is potentially infinite, but it is built from the bounded set \(T\) of transitions. The events \(e^i_j\) for any \(j\) correspond to the different firings of the same transition \(t_i\). Any subset \(l \subset E\) is a set of events.

A set of events \(l\) can be considered as a mutil-set built on \(T\), or as a positive or null integer vector with a dimension equal to the number of transitions of the Petri net.

The multi-sets \(l\) can be represented by monomial in \(\otimes\) (this connector is commutative and not idempotent) of implicative linear logic formulas.

By analogy with the characteristic vector of a firing sequence in Petri net we will note \(l\) the vector mentioned above. In the multi-set vision, its components are the occurrence number of \(t\) in the multi-set \(l\). If \(l\) contains \(K\) elements \(e^i_j\) for fixed \(i\), then \(l(t_i) = K\).

Let the Petri net of figure 3. Two examples of set of events are:

\[
l_1 = \{e^1_2, e^2_3, e^3_4, e^4_1\} \quad \text{and} \quad l_2 = \{e^1_2, e^2_3, e^3_4, e^4_1, e^5_2\}
\]

These sets, considered as multi-sets in the form of monomial in \(\otimes\), give:

\[
l_1 = t_o \otimes t_3 \otimes t_6 \otimes t_\_
\]
\[
l_2 = t_o \otimes t_3 \otimes t_6 \otimes t_\_ \otimes t_9 \otimes t_\_
\]

\(t_o\) represents the formula: \(P_1 \otimes P_5 \rightarrow \sigma P_2 \otimes P_4\)

\(t_s\) represents the formula: \(P_2 \rightarrow \sigma P_1\)

\(t_c\) represents the formula: \(P_4 \otimes P_5 \rightarrow \sigma P_3 \otimes P_5 \otimes P_6\)

\(t_d\) represents the formula: \(P_6 \rightarrow \sigma P_5\)

When we consider vectors, we have:

\[
\bar{l}_1 = \begin{bmatrix} t_o & 1 \\ t_s & 1 \\ t_c & 1 \\ t_d & 1 \end{bmatrix}, \quad \bar{l}_2 = \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \end{bmatrix}
\]

Definition 2 (Concatenation of sets of events): Let two sets of events \(l_1\) and \(l_2\) considered as monomial in \(\otimes\) (multi-sets). The result of the concatenation of \(l_1\) and \(l_2\) gives \(l_3\) such that:

\[
l_3 = l_1 + l_2
\]

When we considerer sets, it is simply necessary to change all the suffixes of the events of \(l_2\) to have no event of \(l_2\) identical to an event of \(l_1\), before doing the union of the two sets. The suffixes are arbitrary integers used only to distinguish the different instances of firing of a same transition.

So we will have:

\[
l_3 = l_1 + l_2 = \{e^1_2, e^2_3, e^3_4, e^4_1\}
\]

\[
l_3 = t_o \otimes t_3 \otimes t_6 \otimes t_\_ \otimes t_9 \otimes t_\_ \otimes t_\_ \otimes t_\_
\]

B. Scenario

Let a Petri net \((P, T, Pre, Post)\) with an initial marking \(M_0\) and a final marking \(M_f\). Let \(l\) 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 \(M_f\) (one event by token).

Definitions 3 (Scenario): A scenario \(SC = (l, \prec_w)\) 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 \(\prec_w\) 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 \(E\).

Let us consider the Petri net of figure 3, with the markings \(M_0 = P_1 \otimes P_3 \otimes P_4 \otimes P_5 \otimes P_6\) and \(M_f\) such a set of events \(l \subset (E \cup I \cup F)\) is a strict partial order \(\prec_w\) defined on the set of events \(l\).

We introduce four initial events \(I \{11, 12, 13\}\) that correspond to the creation of a tokens in the place \(P1\), two tokens in the place \(P3\) and one token in the place \(P5\) and four final events (consumption of the tokens in the places \(P3, P4\) and \(P6\)).

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 \(t_i\) precedes \(t_j\) \((t_i, t_j\) are transition firings). In our representation of scenarios in the form of precedence graph, to each arc of \(A\), we associate an atom that represents the token produced by the firing of the transition \(t_i\) and costumed by the firing of the transition \(t_j\). The labelling of the arcs is
done with respect to the labelled proof tree [9].

The precedence graph of the fig 4 represents the scenario associated to the Petri net of the figure 3, and the markings $M_0 = P_1 \otimes P_2 \otimes P_3 \otimes P_4$ and $M_f = P_1 \otimes P_2 \otimes P_3 \otimes P_4 \otimes P_6$.

![Fig. 4. Precedence graph](image)

**Definition 4 (order Inclusion):** Let $\prec_1$ and $\prec_2$ be two partial orders defined in the same set of events $l$. The partial order $\prec_1$ is included in $\prec_2$ if:

$$\forall e_i, e_j \in l, \ (e_i \prec_1 e_j) \text{ implies } (e_i \prec_2 e_j).$$

It means that the linearizations of $\prec_2$ are linearizations of $\prec_1$. The inclusion term refers to the precedence constraints, the partial order $\prec_1$ has less precedence relations so it is less constrained and represents more possible sequences.

**Note:** The inclusion traduces the fact that if the partial order is expressed as a graph, and if the order $\prec_1$ is included in $\prec_2$ then all the arcs of $\prec_1$ are arcs of $\prec_2$. There is inclusion of the set of the arcs of $\prec_1$ in the $\prec_2$ one.

IV. SUFFICIENT CONDITION

**A. Sufficient sets**

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

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

Let $A_i, i=1, ..., n$ the set of the canonical proof trees of the sequent $M_0, l \vdash M_f$ and $S=\{A_i, j=1, ..., m\}$ the set of the partial orders of the elements of $l$ deduced from the labelled proof trees. Several canonical proof can give the same partial order (the same scenario), and one proof can also give different partial orders by different labelling [9].

In Petri net of figure 3 with the markings $M_0 = P_1 \otimes P_2 \otimes P_3 \otimes P_4$ and $M_f = P_1 \otimes P_2 \otimes P_3 \otimes P_4 \otimes P_6$, we can check that the set $\{e^1_1, e^2_1, e^3_1, e^4_1\}$ is sufficient. The sequent $P_1 \otimes P_2 \otimes P_3 \otimes P_4, t_1 \otimes t_2 \otimes t_3 \otimes t_4 \vdash P_1 \otimes P_2 \otimes P_3 \otimes P_4$ is provable. But the set $\{e^1_2, e^2_2\}$ is not sufficient because the sequent $(P_1 \otimes P_2 \otimes P_3 \otimes P_4, t_5 \otimes t_6 \otimes t_7 \otimes t_8 \vdash M_f = P_1 \otimes P_2 \otimes P_3 \otimes P_4 \otimes P_6)$ is not provable.

**B. Sufficient scenarios**

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

**Definition 6 (weakly sufficient Scenario):** Let $l$ be a set of events, $l \subseteq (E \cup l \cap F)$ and $l' = l \cap E$ be the restriction of $l$ on $E$. The scenario $Sc = (l, \prec_{sc})$ is weakly sufficient to reach $M_f$ from $M_0$ if the sequent $l, M_0 \vdash M_f$ is provable and if there exist a partial order $\prec_{j}$ resulting from a proof tree $A_j$ such that $\prec_{j}$ is included in $\prec_{sc}$.

![Fig. 5. Elementary loop](image)

It means that any sequence that is a linearization of the scenario $Sc$ order will make possible to reach the final marking from the initial one since it is also a linearization of at least one partial order produced by at least one sequent proof. On the other hand if $\prec_{j} \neq \prec_{sc}$, then the precedence constraints of $Sc$ are not all necessary relations of causality. There are some parasite constraints of precedence in $Sc$ which is not imposed by the structure and markings of the Petri net.

![Fig. 6. Precedence graph obtained from a labelled proof tree](image)

**Definition 7 (sufficient Scenario):** Let $l$ be a set of events, $l \subseteq (E \cup l \cap F)$ 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 $l, M_0 \vdash M_f$ is provable and if there exist a partial order $\prec_{j}$ resulting from a proof tree $A_j$ such that $\prec_{j} = \prec_{sc}$.

It is not only necessary to have a set of events sufficient to reach $M_f$ from $M_0$, but in addition one of the partial orders deduced from the proof must be equal to $\prec_{sc}$.

Let us consider again the Petri net of figure 3 with the markings $M_0 = P_1 \otimes P_2 \otimes P_3 \otimes P_4$ and $M_f = P_1 \otimes P_2 \otimes P_3 \otimes P_4 \otimes P_6$. The proof tree of the sequent $M_0, t_1 \otimes t_2 \otimes t_3 \otimes t_4 \vdash M_f$
gives the partial order represented by figure 6. Hence the scenario $\mathcal{Sc}$ of figure 6 is sufficient.

V. NECESSARY CONDITION

A. Necessary set

Let $(P, T, \text{Pre}, \text{Post})$ be a Petri net with an initial marking $M_0$ and a final marking $M_f$.

**Definition 8 (necessary set):** Let $I_k \subseteq E$ be a sufficient set of event to reach $M_f$ from $M_0$. The set of events $I_k$ is necessary if:

$$\forall I_i \subseteq E \text{ sufficient to reach } M_f \text{ from } M_0 \exists I_i \subseteq E, \ I_i = I_i \otimes I_k$$

This concept expresses the fact that some events are necessary to reach an marking from another one. Any sufficient set of events includes these events.

If we consider the Petri net of figure 5 the set of events $I_k = t_a$ is necessary to reach the marking $M_f = P_2 \otimes P_3$ from the marking $M_0 = P_1 \otimes P_2$. We have also the sets $I_i = t_a \otimes (t_a \otimes t_a)^n$, but they include $I_k$.

VI. MINIMALITY

A. Minimal scenario and minimal set (for fixed initial and final markings)

Let us consider a Petri net $(P, T, \text{Pre}, \text{Post})$ with an initial marking $M_0$ and a final marking $M_f$.

**Definition 9 (minimal set):** Let $I_k \subseteq E$ be a sufficient set of events to reach $M_f$ from $M_0$. The set of events $I_k$ is minimal if and only if there is no set of events $I_i \subseteq E$ that is sufficient and that is a subset of $I_k$.

Note that the minimal set between to marking is not unique.

**Property 1** If a set of events is necessary to reach $M_f$ from $M_0$, it is minimal.

Indeed, if $I_k$ is necessary, all other set sufficient of events $I_i$ include necessarily all the events of $I_k$, so it can’t be a subset of $I_k$.

Let us again consider the Petri net of figure 5. The set of events $I_k = t_a$ is minimal to reach the marking $M_f = P_2 \otimes P_3$ from the marking $M_0 = P_1 \otimes P_2$. The sets $I_i = t_a \otimes (t_a \otimes t_a)^n$ are not minimal.

The reciprocal is false, (i.e. a set of events can be minimal but not necessary). We can have many ways between two markings with different sets of events.

**Definition 10 (minimal Scenario)** Let $I$ be a set of events, $I \subseteq (E \cup I \cup F)$ and $I' = I \cap E$ be a restriction of $L$ on $E$. The scenario $\mathcal{Sc} = (I, \prec_w)$ is minimal to reach $M_f$ from $M_0$ if it is sufficient and if the set of events $I'$ is minimal.

It is necessary that one of the partial orders obtained by labelling one of the proof trees of sequent $M_0, I \vdash M_f$, be exactly $\prec_w$.

![Fig. 7. Petri net of a multi-components system](image)

B. Impact of the choice of 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 [5]. 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.

Let us consider the example of figure 7. It contains three components represented by three Petri nets. The feared state corresponds to the partial marking of the place $P_6$ or to simultaneous partial marking of the place $P_9$ and $P_{12}$.

The set of events $I_1 = t_{a} \otimes t_{a} \otimes t_{a} \otimes t_{a}$ is minimal to reach the final marking $M_f = P_2 \otimes P_3 \otimes P_5 \otimes P_6$ from the initial marking $M_0 = P_1 \otimes P_3 \otimes P_5 \otimes P_6$. Between the same markings, the set of events $I_4 = t_{a} \otimes t_{a} \otimes t_{a} \otimes t_{a}$ is not minimal because it is not sufficient. Indeed the sequent $P_1 \otimes P_3 \otimes P_5 \otimes P_6, I_4 \vdash P_2 \otimes P_3 \otimes P_5 \otimes P_6$ is not provable. But $I_4$ is sufficient and minimal to reach $M_f = P_2 \otimes P_3 \otimes P_5 \otimes P_6$ from $M_0 = P_1 \otimes P_3 \otimes P_5 \otimes P_6$.

If we consider, for example, the sequence $s = t_{a} \otimes t_{a} \otimes t_{a} \otimes t_{a}$,
it leads form an initial marking to a state that belongs to the class of the feared states (marking of the Petri net). From the causality point of view, we want to have only the events that directly cause the apparition of the feared state. The event \( t_e \) has not a causal relation with the feared state represented by the marking of the place \( P_0 \). So in the minimal scenario \( t_e \) may not appear for the first class of feared state (marking of the place \( P_6 \)) but if we have \( M_t = P_9 \otimes P_9 \otimes P_9 \otimes P_9 \otimes P_1 \) (marking of the place \( P_6 \)) as final marking \( t_e \) appears necessarily. On the other hand the event \( t_e \) has causal relation with the feared state that corresponds to the partial marking \( P_9 \otimes P_1 \) (i.e. for example the sequence \((t_e; t_f; t_h; t_i)\)).

As a conclusion we note that the characterization of the scenario is very dependent 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.

C. Minimal scenario (for minimal initial state and minimal feared state)

System is composed by a number of entities that interact. If the model of the system is a Petri net, the delimitation between the entities is not explicit, but at a given moment, for a given marking, we can assume that the tokens represent the number of the active entities. In the example of figure 7 if we note \( B(P_6) \) the Boolean associated to the place \( P_6 \), the marking associated to the feared state can be represented by a Boolean function:

\[
R = (B(P_9) \lor (B(P_9) \land B(P_{12})))
\]  

(1)

Note: when \( B(P_9) \) is “true” it traduces the presence of a token in the place \( P_9 \) and when \( B(P_9) \) is “false” there is no token in the place \( P_9 \).

1) Minimal Cutsets associated to the feared state: We assume that the monotonous function \( R \) is associated to the feared state and that \( C=\{C_i\} \) is a set of minimal cutsets of \( R \). For example for function (1) we have the cutsets

\[
C_1 = B(P_9) \\
C_2 = B(P_9) \land B(P_{12})
\]

Each minimal cutset represents a minimal marking associated to the feared state. Instead of considering any final marking \( M_t \) to derive minimal sets of events, we consider the markings associated to the minimal cutsets. In this case the context (marking of Petri net) is partially defined. With Petri net associated to the linear logic we can easily address this problem (partial marking). If an entity is not implicated it is not necessary to specify that it is in its initial state. Indeed in a linear logic any proof remains true if we enrich linearly the context (monotony in traditional logic).

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 certain places of the Petri net) consequence of the marking of the places corresponding to the minimal cutset.

In the example of figure 7, marking associated to \( C_1 \) is \( M_{j_1} = P_9 \otimes P_9 \) and the marking associated to \( C_2 \) is \( M_{j_2} = P_9 \otimes P_{12} \). If we want to take into account the preceding note we get \( M_{j_1} = P_9 \otimes Cont_1 \) and \( M_{j_2} = P_9 \otimes P_{12} \otimes Cont_2 \).

The initial marking to associate to each final marking is not given. We know that the initial marking of the Petri net is a multi-set of tokens. The initial state of the scenario will be a subset of the set \( M_{b_0} \) of the tokens corresponding to the set of all the components of the system assumed in their initial state \( (M_0 \subset M_{b_0}) \). It corresponds to the subset of the components really implied in the minimal scenario considered.

Note: to determine the minimum cutsets, 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).

2) Minimal scenario s associated Minimal Cutsets:

The definition of the minimal scenario associated to a minimum cutset is related to the notion of restricted graph. So we will define a restricted precedence graph to some of its elements. The restriction consists on deleting some events of the graph and completing it by the precedence relation induced by transitivity by the deleted elements.

Definition 11 (Restricted precedence graph): let a precedence graph \( G \) associated to a scenario \( sc \) be \((l_j, \prec_{sc})\) and the set of events \( l_j \) an subset of \( l_j \).

Let:

* \( C_m \) a connexe component of the precedence graph \( G \) composed by the event of the set \( (l_j \setminus l_i) \).

* \( e_i \) events of \( C_m \).

* \( e_i \) an event of \( l_j \) such as the event \( e_k \) precedes at least one event \( e_i \)

* \( e_i \) an event of \( l_j \) such that it exists at least one event \( e_i \) that precedes the event \( e_i \).

The Restricted precedence graph \( G_{rest} \) restriction of \( G \) to the elements of \( l_j \) is the precedence graph \( G \) where each connexe component is deleted and replaced by:
The precedence relation induced by the element of \( C_m \) in G with transitivity between the events \( e_i \) and \( e_j \).

- A final event when there is not event \( e_i \) that precedes event \( e_j \).
- An initial event when there is not event \( e_i \) that precedes event \( e_j \).

Example:

The precedence graph of the figure 8 corresponds to the scenario composed by the set of events \( l_1 = e_i^1 \otimes e_i^2 \otimes e_i^3 \otimes e_i^4 \otimes e_i^5 \). Its restriction to the subset of events \( l_2 = e_i^1 \otimes e_i^3 \otimes e_i^4 \otimes e_i^5 \) is done by deleting the connexe component (discontinuous arcs) and completing the graph by the arc for which the atom \( P_1 \) is associated (trading the transitivity) connecting the event \( e_i^1 \) and \( e_i^4 \).

Then we obtain the precedence graph of the figure 8.

Definition 12 (minimal scenario for a cutset):

Let consider a Petri net and a final marking \( M_\beta = C_i \otimes Cont_i \) associated to a minimal cutset \( C_i \), for feared state. \( M_{ai} \) is the initial marking of the Petri net. Let 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 \( M_{ai} = (M_{ai} \subset M_{ai}) \) a given initial marking. The scenario \( sc_i = \left( l_i, \lt_{w_i} \right) \) with \( G \) as precedence graph is minimal for cutset \( C_i \) to reach \( M_\beta \) from \( M_{ai} \) if it is sufficient between \( M_{ai} \) and \( M_\beta \), and if and only if there is no scenario \( sc_j = \left( l_j, \lt_{w_j} \right) \) with \( G' \) precedence graph such as:

- The scenario \( sc_j = \left( l_j, \lt_{w_j} \right) \) is sufficient to reach \( M_{\beta} \) from \( M_{ai} \) with \( M_{ai} \subset M_{ai} \) and \( M_{\beta} = C_i \otimes Cont_i \) (same minimal cutset)

ii) \( l_j \subset l_i \)

iii) There exists a marking \( M_{b} \) (partial marking) such as the sequent:

\[
\text{Cont} \ominus (\text{Cont} \cap Cont_i) \ominus (M_{ai} \ominus M_{ai}) \ominus M_b, \quad (l_i - l_j) \quad \text{is provable (the terms \text{Cont} are multi-sets and } \ominus \text{ represents the subtraction).}
\]

\[ iv) \text{the precedence graph } G' \text{ is identical to } G \text{ restriction of } G \text{ to the elements of the set } l_j \text{ completed by the precedence relations induced by the elements of } (l_i - l_j) \text{ in } G \text{ with transitivity.} \]

When the conditions (iii) and (iv) are 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 2

In the example of the figure 9, if we consider the minimal cutset \( C_i = P_9 \) between the markings \( M_{o_1} = P_1 \otimes P_3 \otimes P_5 \otimes P_7 \otimes P_6 \) and \( M_{f_1} = P_2 \otimes P_3 \otimes P_5 \otimes P_7 \otimes P_6 \), the scenario \( sc_1 \) (figure 8) composed by the set of events \( l_1 = t_a \otimes t_b \otimes t_a \otimes t_b \otimes t_c \otimes t_c \) is sufficient but not minimal.

Indeed there exist a scenario \( sc_2 \) composed by events of the set \( l_2 = t_a \otimes t_b \otimes t_c \otimes t_c \) between the markings \( M_{o_2} = P_1 \otimes P_3 \otimes P_5 \otimes P_7 \) and \( M_{f_2} = P_2 \otimes P_3 \otimes P_5 \otimes P_7 \), with \( l_2 \subset l_1 \), and the sequent \( P_2 \otimes M_{b}, \quad a, b \mid P_2 \otimes M_{b} \) is provable (condition iii, \( M_{b} = P_1 \)).

The restricted graph associated to the scenario \( sc_1 \) to the element of \( l_2 \) is the graph of the figure 6 that corresponds to the precedence graph of the scenario \( sc_2 \) (condition iv).

Example 2

In the example of the figure 9, if we consider the minimal cutset \( C_i = P_9 \), between the markings \( M_{o_1} = P_1 \otimes P_3 \otimes P_5 \otimes P_7 \) and \( M_{f_1} = P_2 \otimes P_4 \otimes P_4 \otimes P_9 \), the scenario \( sc_1 \) of the figure 10 composed by the set of events \( l_1 = t_a \otimes t_b \otimes t_b \otimes t_d \otimes t_c \) is minimal. We note that the scenario \( sc_2 \) (also minimal) (figure 11) that corresponds
to the sequent:
\[ P_1 \otimes P_2 \otimes P_3 \otimes P_4 \otimes P_5 \otimes t_a \otimes t_b \otimes t_c \otimes t_d \otimes t_e \cdot P_2 \otimes P_4 \otimes P_5 \otimes P_9 \]
satisfies the conditions (i) to (iii) but the condition (v) is not satisfied. The firing of the sequence \((t_a, t_b, t_e)\) in the scenario \(s_{c_1}\) makes possible the parallel firing of the transitions \(t_c\) and \(t_d\) that is not case in the scenario \(s_{c_2}\).

The restricted graph of the scenario \(s_{c_1}\) is different from the precedence graph of the scenario \(s_{c_2}\). So the two scenarios are different.

*Fig. 10. Precedence Graph associated to the scenario \(s_{c_2}\) Example of the figure 9*

*Fig. 11. Precedence Graph associated to the scenario \(s_{c_1}\) Example of the figure 9*

**VII. CONCLUSION**

In this paper we addressed the minimality of critical scenarios (that lead to feared states) in Petri net model. Indeed, a scenario can leads to the feared state without being minimal \(i.e.\) it contains events which are not strictly necessary to reach the final feared state). The new representation of Petri net with formulas of linear logic allows us to define formally the notion of scenario.

To obtain minimal scenario we have to consider three aspects: (i) the order relations between events must be effective relation of causality in the system, (ii) the list of event of the scenario must be minimal (without events of the loop of the system) (iii) the final marking corresponding to the feared state must be minimal.

In the first time the definition of the minimal scenario concerns the case where the context is completely know (the initial and final markings are fixed). 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.

Within our method for deriving feared scenario [4] the context is only partially known, so the choise of the markings has an impact on the minimality of the derived scenarios. A minimal final marking is defined. It corresponds to the minimal cutsets 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.

This notion of minimality will be integrated in the approach of deriving feared scenarios in order to generate only minimal scenario.

We are currently working on the notion of completeness of the scenarios. A set of scenario \(S\) associated to minimal cutset \(C_i\) is complete if all minimal scenarios belong to \(S\). It is clear that the two notions completeness and minimality are related, for example if the set of event are necessary between two markings we can conclude that the complete set of scenario contains only the necessary scenario. So from the minimality we can define the notion of completeness.

**VIII. REFERENCES**


