Afrique SCIENCE *02(2) (2006) 176 - 186* 176
ISSN 1813-548X

Etude de sûreté de fonctionnement d'un système électrique simple

Mébarek DJEBABRA

Laboratoire de prévention industrielle, Institut Universitaire d'Hygiène et Sécurité, Université Hadj-Lakhdar de Batna, Algérie.

(Reçu le 09 Janvier 2006, accepté le 19 Avril 2006)

* Correspondance, courriel : *djebabra.mebarek@lycos.com*

Résumé

L'objet de cette étude est de mettre en exergue le rôle que joue certaines méthodes de sûreté de fonctionnement pour mener à bien une étude de sécurité des systèmes techniques.
Pour illustrer nos propos, un exemple simplifié d'alimentation électrique des dispositifs de sécurité est également présenté.

Mots-clés : *Étude de sécurité, sûreté de fonctionnement, performances, systèmes électriques.*

Abstract

Dependability study of a simple electric system

The object of this study is to show the role, which plays dependability methods to carry out a safety study of technical systems.
To illustrate our remarks, a simplified example of safety devices is also presented.

Keywords : *Safety study, dependability, performances, electrical systems.*

1. Introduction

La sûreté de fonctionnement est la science de défaillances des systèmes. Elle inclut ainsi leur connaissance, leur évaluation, leur prévision, leur mesure et leur maîtrise [1]. Ses principaux concepts sont [2] : la fiabilité, la disponibilité, la sécurité et la maintenabilité.
La sûreté de fonctionnement n'est pas uniquement un ensemble de concepts mais également une discipline qui regroupe des méthodes permettant d'évaluer les concepts

précités de manière qualitative et quantitative.
Ces méthodes présentent les avantages suivants [3] :
- elles permettent d'envisager, de manière méthodique, les différents aspects liés aux systèmes étudiés et d'apporter des éléments techniques pour juger des performances de ces systèmes,
- la plupart de ces méthodes trouvent leur pleine efficacité lorsqu'elles sont pratiquées au sein d'un groupe de travail pluridisciplinaire [4]. A ce titre, ces méthodes constituent un support d'échange et de communication entre les différents acteurs,
- ces méthodes sont complémentaires ce qui permet d'assurer l'exhaustivité de l'étude de sûreté de fonctionnement des systèmes [5-7].

Ces avantages n'épargnent pourtant pas ces méthodes de certaines limites. Les plus importantes concernent les systèmes étudiés et l'exhaustivité de ces méthodes. En effet, malgré l'usage répandu de ces méthodes, l'ensemble de ces méthodes est dédié à l'identification des risques générés par des installations industrielles grâces à des analyses de leur bon fonctionnement et/ou de leurs dysfonctionnements [8]. De même et malgré le perfectionnement croissant de ces méthodes, le recours à une seule méthode ne garantit pas l'exhaustivité de la démarche de gestion des risques. En d'autres termes, l'utilisation d'une seule méthode ne permet pas de mener à bien une étude *systématique* de sûreté de fonctionnement des systèmes techniques [1,4,9].

L'objectif de cet article est double : surmonter les deux principales limites inhérentes aux méthodes de sûreté de fonctionnement évoquées ci-dessus et proposer une étude de sûreté de fonctionnement des systèmes techniques basée sur le formalisme des réseaux de Petri.
Afin de mettre en exergue, notre proposition, un exemple simple mais suffisamment représentatif fera l'objet de l'illustration de nos propos.

2. Etude de sûreté de fonctionnement proposée

L'étude de sûreté de fonctionnement préconisée a pour objectif de mettre en défaut le système étudié afin de dégager ses différents dysfonctionnements. La vision que nous adoptons est du type *pessimiste* et s'oppose à celle adoptée par les concepteurs des systèmes techniques. Nous justifions notre choix par le fait qu'il va dans le sens de la sécurité. En effet, l'étude de sûreté de fonctionnement que nous préconisons cherche à démontrer que le système ne répond pas au cahier de charge du point de vue de sécurité.
Rappelons que cette étude de sûreté de fonctionnement est une démarche composée d'un certain nombre d'étapes autour desquelles peuvent s'articuler des méthodes spécifiques. Ces principales étapes sont [6,7] :

- description du système (ses composants, sa raison d'être ainsi que sa délimitation),
- analyse des performances du système étudié afin de déterminer le niveau de sécurité souhaité (donc d'insécurité qui correspond à un événement non souhaité qu'il faut éviter),
- modélisation du système étudié par le formalisme réseaux de Petri, exploration qualitative du modèle :
- exploration du modèle en chaînage avant (simulation du modèle par injection des pannes simples et multiples dans le but d'examiner leur propagation ainsi que la réaction des protections en terme de basculement du système d'un mode de fonctionnement à un autre),
- exploration du modèle en chaînage arrière où l'on part d'un marquage indésirable pour explorer les chemins qui y conduisent. Cette exploration permet d'examiner les différentes situations causales,
- simulation des événements externes (pour faciliter l'exploitation et la simulation des configurations particulières),
- exploration quantitative du modèle par la simulation Monte-Carlo afin d'estimer les performances du système en terme de disponibilité, de fiabilité et MTTF,
- prise de décision grâce à la mise en œuvre des mesures de sécurité permettant de respecter le niveau de sécurité souhaité.

La suite de l'article, consiste en un détail des étapes de la démarche d'étude de sûreté de fonctionnement énumérées précédemment.

3. Résultats

3-1. Description du système étudié

La ***Figure 1*** représente, d'une manière volontairement simplifiée, ce que pourrait être un système d'alimentation électrique des dispositifs de sécurité des installations industrielles.

3-2. Analyse des performances du système étudié

Une première analyse du principe de fonctionnement du système montre l'existence de trois niveaux de performance du système :

• *Niveau de performance 1* qui correspond à un *mode de fonctionnement normal*. Ce niveau est caractérisé par l'alimentation des transformateurs T_1 et T_2 par la source principale et auxiliaire. Donc, T_1 et T_2 sont sous tension et le groupe diesel est à l'arrêt.

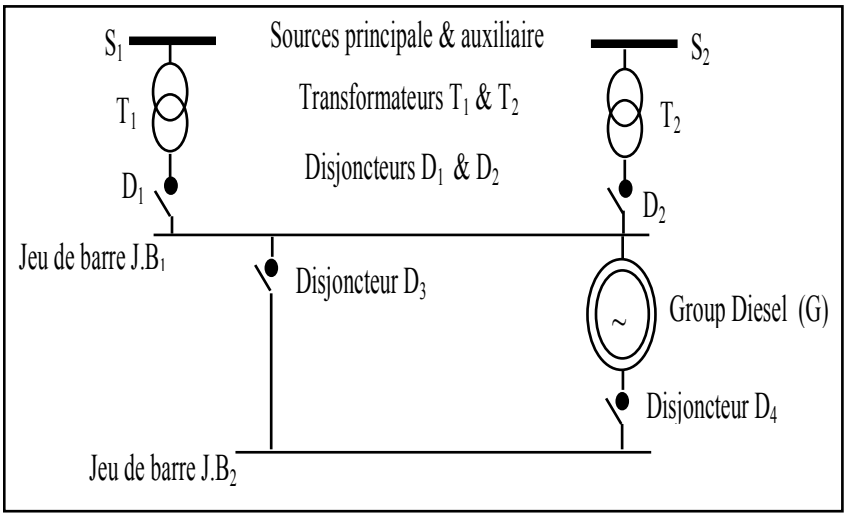

Figure 1 : *Schéma de principe du système électrique*

• *Niveau de performance 2* qui correspond à un *mode de fonctionnement dégradé* (mais non critique). En effet, en cas de défaillance de la source principale, le système fonctionne avec T_2.

• *Niveau de performance 3* caractérisé par la perte d'alimentation au niveau des deux sources. Ce cas correspond à un *mode de fonctionnement critique.*

L'analyse des différents niveaux de performance du système montre que le niveau de performance 3 correspond à une situation qu'il faut éviter car le fonctionnement du système en mode critique signifie que celui-ci a plus de chance de tomber en panne et par conséquent ce mode de fonctionnement risque de causer la perte d'alimentation des dispositifs de sécurité.

L'étape suivante d'une étude de sûreté de fonctionnement consiste à analyser les scénarios des dysfonctionnements conduisant à la perte d'alimentation des dispositifs de sécurité.

Rappelons qu'en sûreté de fonctionnement, cette analyse est conduite habituellement par la méthode « *Arbre de défaillance* » qui est largement utilisée en sûreté de fonctionnement [10,11]. Cependant, cette méthode souffre de certaines limites dues essentiellement au comportement évolutif du système ainsi qu'à l'interdépendance entre ses composants. Pour cette raison, notre choix sera détourné vers les réseaux de Petri qui ne souffrent pas de ces limites et dont l'utilisation en sûreté de fonctionnement occupe une place de choix [12-14].

3-3. Modélisation des scénarios de dysfonctionnements par les réseaux de Petri

La figure 2 représente les réseaux de Petri relatifs au système étudié.

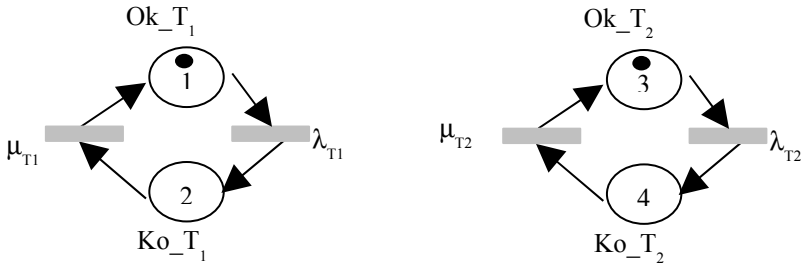

Figure 2.a *: Réseaux de Petri relatif au comportement de T_1 et T_2*

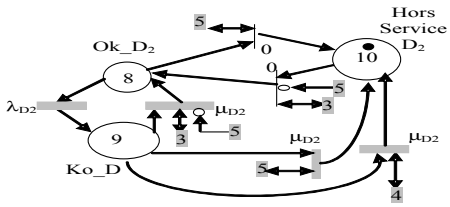

Figure 2.c : *Réseaux de Petri relatif au comportement de D_2*

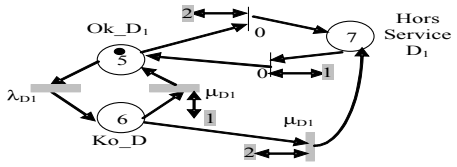

Figure 2.b : *Réseaux de Petri relatif au comportement de D_1*

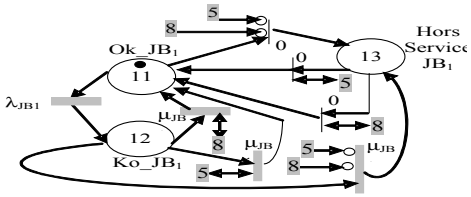

Figure 2.d : *Réseaux de Petri relatif au comportement de JB_1*

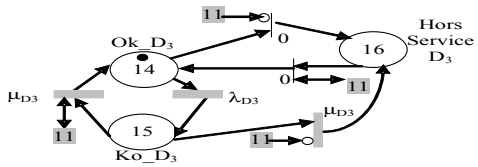

Figure 2.e : *Réseaux de Petri relatif au comportement de D_3*

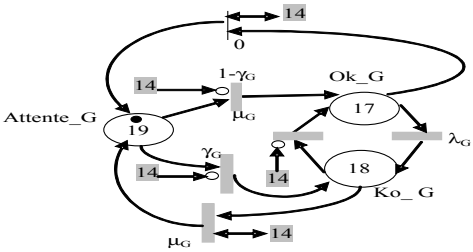

Figure 2.f : *Réseaux de Petri relatif au comportement du groupe diesel*

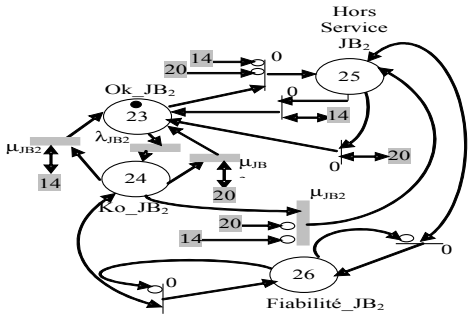

Figure 2.h : *Réseaux de Petri relatif au comportement de JB_2*

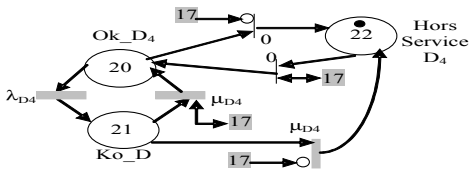

Figure 2.g : *Réseaux de Petri relatif au comportement de D_4*

Figure 2 : *Réseaux de Petri du système électrique étudié*

3-4. Exploration qualitative des réseaux de Petri

3-4-1. Exploration en chaînage avant

Cette exploration consiste en une *simulation des dysfonctionnements* dans les réseaux de Petri grâce à *l'injection* des pannes (déclencher le franchissement d'une ou plusieurs transitions) et d'en déduire les conséquences qui en résultent (mise à jour dans les autres réseaux). Chacune des conséquences déduites sera examinée selon les critères de sécurité retenus (ici, c'est la situation d'insécurité qui correspond à la perte d'alimentation des dispositifs de sécurité de l'installation).

A. Injection de pannes simples

Il s'agit, dans ce cas, d'injecter qu'une seule panne (ou défaillance) par composant. Par exemple, la défaillance du transformateur T_1 se traduit, dans le réseau de la ***Figure 2.a***, par le franchissement de la transition λ_{T1} et par conséquent par le passage du jeton de la place 1 à la place 2. La transition qui sépare les places 5 et 7 de la ***Figure 2.b*** devient alors sensibilisée. Le délai qui lui est associé étant nul. Elle est, donc, tirée instantanément et un jeton disparaît de la place 5 et un autre apparaît dans la place 7. La disparition du jeton de la place 5 engendre le tirage instantané de la transition liant les places 10 et 8 de la ***Figure 3.c***. D'où le démarquage de la place 10 et le marquage de la place 8. Donc, l'injection d'une panne au niveau de T_1 provoque une mise hors service de D_1 et mise en service de D_2.

De cette manière et en effectuant des simulations de fonctionnement des réseaux de Petri (injection de pannes simples), on obtient une liste de la propagation des pannes simples.

Remarquons que l'interprétation de l'injection des pannes simples correspond aux sensibilisations des différentes transitions des réseaux de Petri suite aux franchissements d'une transition quelconque dans l'un des réseaux de Petri. Cette injection engendre des conséquences qui provoquent le fonctionnement du système en mode dégradé à l'exception de la panne JB_2 qui provoque le fonctionnement du système en mode critique.

B. Injection de pannes multiples

Il s'agit, dans ce cas, d'injecter plusieurs pannes à la fois pour pouvoir déclencher d'autres transitions dans les réseaux de Petri et de déduire leur propagation. La structure du système retenu dans cette étude nous limite aux *pannes doubles*.

L'injection des pannes multiples (doubles dans notre cas) se traduit par le *franchissement conditionnel* des transitions (une transition T_x n'est franchie que si T_y l'est aussi). Dans notre cas, ces franchissements de transitions engendrent des conséquences

qui provoquent le passage du système en phase critique. Ainsi, la mise hors service de la barre JB_1 est conditionnée par les pannes (ou les mises hors services) simultanées de l'un des composants (T_1, D_1) avec l'un des composants (T_2, D_2).

C. Classification des effets de la propagation des pannes

Nous pouvons, à ce niveau de notre démarche, effectuer une classification de la propagation des pannes simples et multiples par niveau de performance du système. Dans notre cas, nous obtenons la classification suivante :

Niveau de performance 2	Propagation des pannes simples	Propagation des pannes doubles
	$T_1 \rightarrow D_1$; $T_2 \rightarrow D_2$; $JB_1 \rightarrow D_3$; $G \rightarrow D_4$	$T_1T_2 \rightarrow JB_1$; $T_1D_2 \rightarrow JB_1$; $D_1T_2 \rightarrow JB_1$; $D_1D_2 \rightarrow JB_1$
Niveau de performance 3		$JB_1G \rightarrow JB_2$; $JB_1D_4 \rightarrow JB_2$; $D_3G \rightarrow JB_2$; $D_3D_4 \rightarrow JB_2$

3-4-2. Exploration en chaînage arrière

La simulation des dysfonctionnements dans les réseaux de Petri, selon la technique d'injection de pannes appelée également « *chaînage avant* », a pour objectif d'en déduire les effets sur le système. Ces effets, une fois comparés avec le critère de sécurité retenu, vont nous permettre de déduire ceux qui contribuent à l'effet indésirable qu'est, rappelons-le, la perte d'alimentation des dispositifs de sécurité. Dans notre cas, il s'agit bien de la défaillance du jeu de barre JB_2 ou de sa mise hors service suite à des défaillances en amont du système ; ce qui correspond au démarquage de la place 23 de la ***Figure 2.h***.

L'étape suivante de la simulation des dysfonctionnements dans les réseaux de Petri est de déclencher le « *chaînage arrière* » pour déduire les composants qui peuvent contribuer directement quant à l'occurrence de cet événement. Ainsi, nous obtenons les *coupes minimales* suivantes :

Insécurité d'alimentation électrique $= JB_2 \cup D_3D_4 \cup JB_1D_4 \cup D_1D_2D_4 \cup D_1T_2D_4 \cup T_1T_2D_4 \cup T_1D_2D_4 \cup GD_3 \cup GJB_1 \cup GD_1D_2 \cup GD_1T_2 \cup GT_1D_2 \cup GT_1T_2$.

3-5. Exploration quantitative des réseaux de Petri

L'exploitation quantitative des réseaux de Petri consiste à effectuer une simulation du type Monte-Carlo pour estimer les performances du système étudié. Dans notre cas, notre intérêt s'est porté sur les paramètres suivants : *disponibilité*, *fiabilité* et *MTTF* du

système. Les résultats de la simulation statistique du système sont fournis dans le tableau suivant.

Tableau 1 *: Résultats de la simulation*

Nb. histoires = 10^6	$\lambda_{Di} = 10^{-4}$; $\mu_{Di} = 10^{-1}$	$\lambda_{Ti} = 2.10^{-4}$; $\mu_{Ti} = 10^{-1}$
$\lambda_{JBi} = 3.10^{-4}$; $\mu_{JBi} = 10^{-1}$	$\lambda_G = 4.10^{-4}$; $\mu_G = 10^{-1}$	
Temps (en heures)	*Disponibilité (%)*	*Fiabilité (%)*
1	99.97	99.97
10	99.80	99.70
10^2	99.68	97.05
5.10^2	99.67	86.11
∞	99.67	0
MTTF $\approx 33.10^2$ heures		

3-6. Prise de décision

La maîtrise du risque «défaillance du jeu de barre JB_2 ou de sa mise hors service suite à des défaillances en amont du système» nous conduit, logiquement, à agir sur ces composantes qui sont bien sa fréquence et sa gravité d'occurrence. Cette action se concrétise en une utilisation des *techniques des barrières* couramment utilisée dans les études de sécurité et dont l'objectif consiste à faire face au risque grâce à un nombre suffisant de barrières (ce nombre est proportionnel à la gravité du risque qui est ici de 3). Rappelons qu'il existe deux types de barrières : les barrières techniques (matérielles ou immatérielles mais physiques) et les barrières d'utilisation (procédures, règles de l'art, formation, contrôles périodiques, tests, . . .).

L'allocation de l'objectif de sécurité en sous objectifs nous permet de répartir le nombre de barrières sur tous les composants qui contribuent à l'occurrence de l'insécurité d'alimentation électrique ***(Figure 3).*** Ce principe d'allocation, qui est du type descendant, s'effectue sur la base des simulations qualitatives des réseaux de Petri.

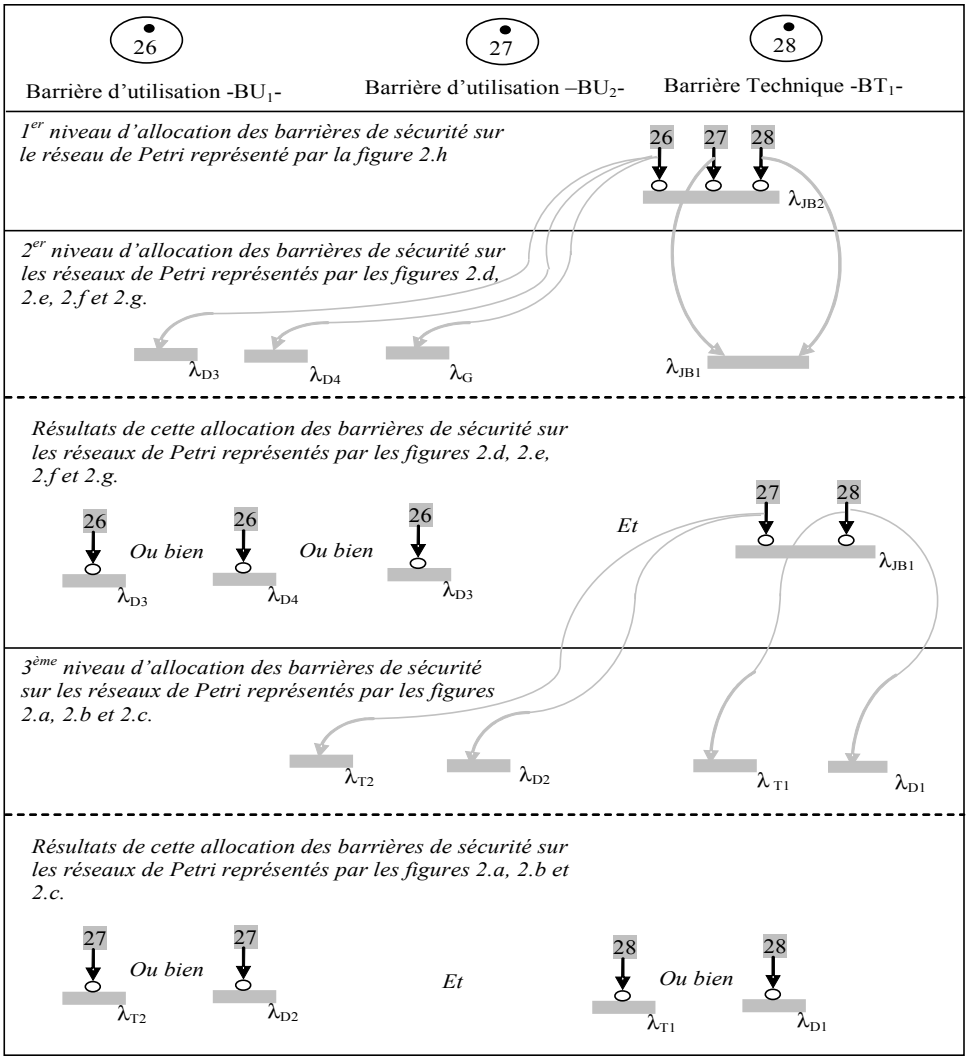

Figure 3 *: Principe d'allocation de barrières*

4. Discussion

Rappelons que les réseaux de Petri utilisés dans cette étude de sûreté de fonctionnement des systèmes techniques sont du type stochastique. L'utilisation de l'option réseaux de Petri séparés (c'est-à-dire réseau de Petri par composant du système étudié) permet d'assurer une extrême simplicité de leur élaboration ainsi qu'une bonne lisibilité de ces réseaux.

Les trois exploitations des réseaux de Petri présentés dans cet article méritent d'être commentés :

D'abord, le principe de la simulation qualitative des réseaux de Petri qu'est facilité par l'utilisation des logiciels professionnels dédiés pour ce type de modèles. Pour rappel, la finalité de ce type de simulations étant la déduction du graphe de marquage associé aux réseaux de Petri ainsi élaborés.
Puis, le principe de la simulation quantitative qui consiste en un couplage de la simulation statistique et les réseaux de Petri. Le principe de la simulation statistique des réseaux de Petri consiste à effectuer des tirages aléatoires suivant la loi uniforme continue sur [0-1] afin de déduire l'occurrence des prochains événements. Par exemple, le délai relatif à l'occurrence de l'événement caractérisé par la transition λ_{D1} est simulé par la relation suivante :

$$T_{D1} = -(1/\lambda_{D1}).\text{Log (Random)}$$

Avec : - T_{D1} est le délai de la prochaine défaillance du disjoncteur D_1
- λ_{D1} est le taux de défaillance du disjoncteur D_1 qui suit la loi exponentielle
- Random est une fonction prédéfinie qui génère des variables pseudo aléatoires sur [0-1].

Ce principe de simulation, très simple est très efficace, nécessite des durées de simulation trop grandes. C'est pourquoi, ce type de simulation requiert également l'utilisation des logiciels de simulation. Dans notre cas, les résultats fournis par le ***Tableau 1*** ont été obtenus grâce à l'utilisation d'un programme informatique que nous avons dénommé PetriFiab [15].
Enfin, signalons que le principe d'allocation des barrières de sécurité sur les transitions des différents réseaux de Petri est assuré par à l'utilisation des transitions inhibitrices ***(Figure 3).***

4. Conclusion

Dans cet article, nous avons mis en exergue le rôle que peuvent jouer les réseaux de Petri dans une étude de sûreté de fonctionnement des systèmes techniques.
Les avantages que présente notre choix sont multiples. Les plus importants résident aux niveaux de : la richesse du modèle retenu - l'analyse qualitative du modèle grâce à l'élaboration des scénarios agressifs - l'analyse quantitative du modèle grâce à la simulation statistique qui offre la possibilité de prendre en considération l'interdépendance entre les événements caractérisant le système et son environnement.

Notons enfin, comme pour toute étude de sûreté de fonctionnement, que les étapes de la démarche présentée dans cet article ne sont pas figées puisqu'elles sont fortement liées aux objectifs de l'étude de sûreté de fonctionnement. Néanmoins, notre proposition peut être appliquée à des systèmes en conception ou en cours d'utilisation.

Références

[1] - A. Pages et M. Gondron « *Fiabilité des systèmes* ». Ed. Eyrolles Paris, France (1983)

[2] - S. Logiaco « *Etude de sûreté des installations électriques* ». Cahier technique n° 184. Collection Shneider Technique. Edition janvier (1999), Site Internet : *http://www.schneider-electric.com*

[3] - Desmas et C. Ancelin « *Les méthodes de fiabilité et la sûreté de fonctionnement* ». Note Electricité de France (EDF) N° 93NB00062 – France (1992)

[4] - G. Alain – Maurin « *Méthodologie d'intervention pour les études de sûreté de fonctionnement* ». Note Electricité de France (EDF). N° 93NB00059 – France (1992)

[5] - Y. Dutuit, Y. Chatelet, J. Dos-Santos et T. Bouhoufani « *Les diagrammes blocs fonctionnels : une aide à la construction des arbres de défaillances* ». Revue Européenne de diagnostic et de sûreté de fonctionnement. Vol.5, N°2 (1995) 181-200

[6] - M. Djebabra et S. Saadi « *Méthodologie d'étude de sûreté de fonctionnement des systèmes : analyse fonctionnelle* ». Phoebus la revue de sûreté de fonctionnement. N° 10 (1999) 27-34

[7] - M. Djebabra et S. Saadi « *Méthodologie d'étude de sûreté de fonctionnement des systèmes : analyse des défaillances* ». Phoebus la revue de sûreté de fonctionnement. N 12 (1999) 24-32

[8] - A. Villemeur « *Sûreté de fonctionnement des systèmes industriels* ». Ed. Eyrolles Paris, France (1988)

[9] - C. Lievens « *Sécurité des systèmes* ». CEPADUES –Editions, France (1996).

[10] - N. Limnios « *Arbre de défaillances* ». Editions Hermès. Traité des nouvelles technologies. Paris, France (1990)

[11] - Y. Dutuit et A. Rauzy « *Approche analytique événementielle : l'arbre de défaillance* », *in « Maîtrise des risques et sûreté de fonctionnement des systèmes de production »* (coordonnateurs : E. Niel & E. Craye). Ed. Hermès-Lavoisier, Paris, (2002) 197-235

[12] - M. Djebabra, L. Bendada et T. Bentarcia « *A reliability-based study for a flexible manufacturing system* ». The Journal of the System Reliability Center (2005). 1-6. Site Internet : *http://src.alioscience.com*

[13] - Y. Dutuit, Y. Chatelet, J-P. Signoret et P. Thomas « *Dependability modelling and evaluation by using stochastic Petri nets: Application to two test cases* ». Reliability Engineering and System Safety. Vol. 51 (1996) 1-8

[14] - J-P. Signoret « *Approche par simulation, chapitre 9 de l'ouvrage Maîtrise des risques et sûreté de fonctionnement des systèmes de production* », (coordonnateurs : E. Niel & E. Craye). Editions Hermès – Lavoisier. Paris, France (2002) 271-319

[15] - M. Djebabra « *Contribution à la modélisation, à la simulation et à l'analyse des dysfonctionnements des systèmes techniques* ». Thèse de Doctorat présentée à l'Université Bordeaux I, France, N° d'ordre 845 (1993).