Fiabilisation d'un système mécatronique dès la phase de conception

Amel Demri[*,], Abdérafi Charki[*], Fabrice Guerin[*], Mihaela Barreau[*] & Hervé Christofol[**]**

**LAboratoire en Sûreté de fonctionnement, QUalité et Organisation (LASQUO), **Laboratoire de Conception de Produits Nouveaux et Innovation (CPNI), ISTIA*
62, avenue Notre Dame du Lac
49000 Angers
amel.demri@univ-angers.fr

Résumé :

En phase de conception, une étude de sûreté de fonctionnement d'un système est généralement précédée d'une analyse fonctionnelle qui consiste à définir, avec précision, les limites matérielles du système étudié, les différentes fonctions et opérations réalisées par le système et les diverses configurations d'exploitation. Cette première étape permet de réaliser une décomposition hiérarchique du système en éléments matériels et/ou fonctionnels. Or celle-ci n'apporte pas d'informations sur les modes de défaillance, leurs effets, leur occurrence et leur criticité. Il est donc nécessaire de la compléter par une deuxième analyse prenant en compte les dysfonctionnements. Les deux types d'analyses qui sont complémentaires, peuvent permettre, si elles sont réalisées d'une manière pertinente, de modéliser plus finement un système complexe, grâce par exemple, aux Réseaux Bayésiens ou aux Réseaux de Petri. On propose dans cet article d'appliquer différentes méthodes classiques employées en sûreté de fonctionnement afin d'étudier un système mécatronique simple.

Abstract:

A study of reliability is generally preceded by a functional analysis, which consists in defining precisely, the material limits of a system, the various functions and operations realized by the operating system and various configurations. This first stage allows, making a hierarchical decomposition of the system in material and/or functional elements. However, this one does not bring information on the modes of failure, their effects, their occurrences and their criticality. It is necessary to complete this first stage by a second analysis taking into account the dysfunctions. These two complementary analyses allow us to model suitably a complex system thanks to the Bayesians and the Petri networks for instance. In this article, we propose to employ various classical methods to study a mechatronic system.

Mots-clefs :

Mécatronique ; Réseaux de Petri ; analyses qualitative et quantitative.

1 Introduction

La mécatronique est aujourd'hui en pleine expansion. Elle caractérise l'utilisation simultanée de la mécanique, de l'automatique, de l'électronique et du logiciel. L'analyse de la fiabilité d'un système mécatronique est extrêmement difficile.

Pour les domaines de la mécanique et de l'électronique, l'analyse de la fiabilité est basée sur des méthodes connues mais pour d'autres domaines tels que celui du logiciel, les outils actuels, permettant d'effectuer celle-ci, ne sont pas complètement maîtrisés.

La difficulté dans l'analyse de fiabilité d'un système mécatronique est due essentiellement à l'interaction entre les différents domaines.

Pendant la phase de conception des systèmes mécatroniques, les scénarios redoutés peuvent être mal identifiés du fait de la complexité inhérente à ces systèmes. Les études de sûreté de fonctionnement de ces systèmes sont basées, tout d'abord, sur une analyse qualitative ayant pour objectif de déterminer les différents événements possibles pouvant influencer leurs fonctionnements. Cette étape préliminaire permet de cibler les principaux événements redoutés, et de faciliter l'intégration d'une analyse quantitative (estimation de la probabilité de défaillance du système mécatronique) [Khalfaoui 2003].

La démarche que nous proposons consiste à traiter un système mécatronique en effectuant, dans un premier temps, une analyse fonctionnelle interne et externe et, dans un deuxième temps, une analyse dysfonctionnelle. Ces deux analyses constituent l'analyse qualitative. Enfin, dans un troisième temps, nous évaluerons la fiabilité du système par une analyse quantitative.

Dans cet article, nous nous intéresserons plus spécialement à l'analyse dysfonctionnelle d'un système mécatronique puisque l'analyse fonctionnelle de ce dernier est traitée dans l'article [Demri et al. 2007]. En ce qui concerne l'analyse dysfonctionnelle, notre choix s'est porté sur l'Analyse des Modes de Défaillance et de leurs Effets (AMDE), qui est une méthode utilisée plutôt dans le cas des composants mécanique et électronique. Un équivalent s'utilise pour les logiciels ; il s'agit de l'Analyse des Effets des Erreurs du Logiciel (AEEL). Mais le problème de ces méthodes réside dans le fait qu'elles ne prennent pas en considération les changements séquentiels d'état de fonctionnement du système. Pour remédier à cela, les réseaux de Petri [Girault et al. 2003; Ladet 1989; Moncelet 1998; Vidal-Naquet et al 1992]ont été utilisés afin de prédire quantitativement la probabilité d'apparition d'un événement redouté du système en fonction d'une expérience acquise sur l'évolution des états de fonctionnement des différents composants qui le composent.

2 Etude de cas

Le cas que nous allons étudier, proposé par [Khalfaoui et al. 2002], concerne un système de régulation de volume de deux réservoirs comme montré sur la figure 1. Ces deux réservoirs alimentent des utilisateurs selon un besoin prédéfini.

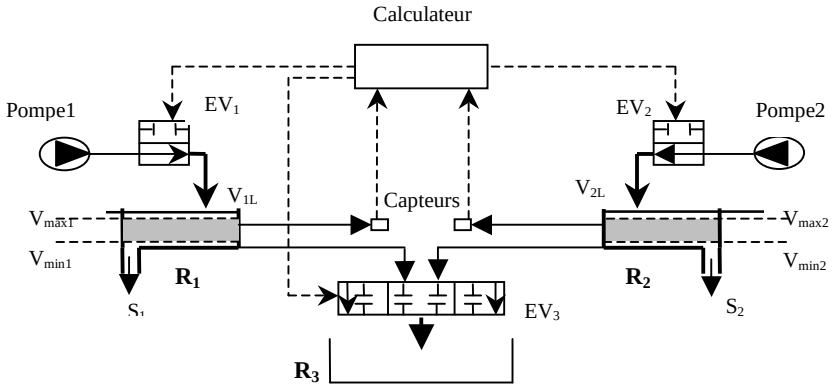


FIG. 1 – Système de régulation de volume.

Le système est constitué d'un calculateur, de trois électrovannes (EV_1, EV_2, EV_3), de deux pompes, de deux capteurs, de deux réservoirs régulés (R_1, R_2) et d'un réservoir de vidange (R_3). Le volume dans chaque réservoir doit rester compris dans l'intervalle [V_{min}, V_{max}]. Le contrôle se fait grâce au calculateur qui alimente (ou non) le réservoir concerné à travers l'électrovanne concernée. Si le volume de l'un des deux réservoirs régulés dépasse un certain volume limite V_L, le calculateur commande l'ouverture de l'électrovanne EV_3 pour vidanger les réservoirs. Les réservoirs alimentent les utilisateurs par les sorties S_1 et S_2.

3 Analyse qualitative

L'analyse qualitative a pour but de caractériser les scénarios redoutés provoqués par des changements d'états et des enchaînements d'événements. Les méthodes qualitatives sont fondées sur la nomenclature des dangers et des risques, de leurs origines et de leurs causes. Elles utilisent des tableaux standards permettant de classer les données et les événements.

Parmi les méthodes d'analyse qualitative nous avons choisi d'utiliser l'Analyse des Modes de Défaillances et de leurs Effets (AMDE), utilisée depuis les années 60. C'est une méthode d'analyse des risques dysfonctionnels basée sur l'établissement de relations de cause à effet [Villemeur 1988; Zwingelstein 1996]. Elle s'appuie sur l'identification des modes de défaillance des composants d'un système. Les dysfonctionnements identifiés sont tout simplement les effets perçus par le client. Pour une bonne analyse des modes de défaillance, il faut donc identifier les causes d'apparition.

Le tableau 4, qui représente l'AMDE effectuée sur le système présenté sur la figure 1, nous permet de conclure que les défaillances liées aux deux capteurs et au calculateur ont un effet très significatif sur le débordement des deux réservoirs R_1 et R_2.

En cas de défaillance des électrovannes EV_1 et EV_2, les effets peuvent être graves car on peut aussi avoir le débordement des réservoirs mais sous condition que l'électrovanne EV_3 soit défectueuse. Si l'électrovanne EV_3 reste bloquée fermée, les effets peuvent être graves car on peut avoir le débordement des réservoirs si les électrovannes EV_1 et EV_2 restent bloquées ouvertes.

Fonctions principales	**Modes de défaillance**	**Causes**	**Effets**
Garantir le remplissage de R_1 par EV_1	EV_1 bloquée ouverte	EV_1 défectueuse Capteur 1 HS Calculateur ne transmet pas l'information	Peut conduire au débordement de R_1 si l'EV_3 est défaillante
	EV_1 bloquée fermée	EV_1 défectueuse Capteur 1 HS Calculateur ne transmet pas l'information	Avoir un volume critique inférieur à V_{1min}
	Problèmes d'informations véhiculés par le capteur 1.	Calculateur HS Dérive du capteur 1	Débordement R_1 Avoir un volume critique inférieur à V_{1min}
	Mauvaises consignes données par le calculateur.	Calculateur HS Dérive du capteur 1 Erreur de programmation	Débordement R_1 Avoir un volume critique inférieur à V_{1min}
Vidanger R_1 par EV_3	EV_3 bloquée ouverte.	EV_1 défectueuse Capteur 1 HS Calculateur ne transmet pas l'information	Avoir un volume critique inférieur à V_{1min}
	EV_3 bloquée fermée.	EV_1 défectueuse Capteur 1 HS Calculateur ne transmet pas l'information	Peut conduire au débordement de R_1 si l'EV_1 est défaillante.
	Problèmes d'informations véhiculés par le capteur 1.	Calculateur HS Dérive du capteur 1	Débordement de R1 Avoir un volume critique inférieur à V_{1min}
	Mauvaises consignes données par le calculateur.	Calculateur HS Dérive du capteur 1 Erreur de programmation	Débordement de R1 Avoir un volume critique inférieur à V_{1min}

Tableau 1 – Tableau de l'AMDE

Après la réalisation de cette AMDE, différentes méthodes peuvent être appliquées pour estimer la probabilité d'apparition d'un événement redouté pour faire une analyse quantitative. Parmi les méthodes utilisées pour cette analyse on peut citer l'Arbre de défaillance, les réseaux Bayésien et les réseaux de Petri, etc. C'est cette dernière méthode que nous avons choisi pour faire notre analyse quantitative car il nous permet de modéliser l'aspect fonctionnel et l'aspect dysfonctionnel et de prendre en considération les changements séquentiels d'états de fonctionnement du système.

4 Analyse quantitative

Les réseaux de Petri ont été inventés en 1962 par Carl Adam Petri. Ils sont basés sur la théorie des automates. Ces réseaux permettent de représenter le comportement des systèmes dans les conditions de fonctionnement normal ainsi que leur comportement en cas de défaillance de leurs composants [Girault et al. 2003; Ladet 1989; Moncelet 1998; Vidal-Naquet et al 1992]. Les réseaux de Petri comportent deux types de nœuds : les places et les transitions. Une place est représentée par un cercle et une transition par un rectangle (ou un trait). Les places et les transitions sont reliées par des arcs orientés soit d'une place à une transition, soit d'une transition à une place. Afin de mieux expliquer le fonctionnement des réseaux de Petri, nous proposons un petit exemple illustré sur la figure 2.

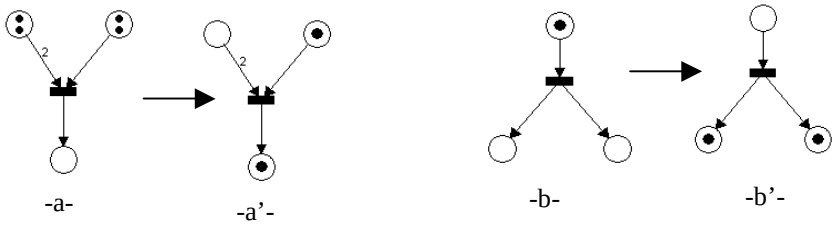


FIG. 2 – Exemple du fonctionnement d'un réseau de Petri.

La figure 2.a représente un réseau de Petri comportant trois places (deux places en entrée et une place en sortie), une transition, trois arcs orientés et quatre jetons. Autre exemple illustré en figure 2.b, montre un réseau de Petri comportant trois places (une place en entrée et deux places en sortie), une transition, trois arcs orientés et un jeton. Les franchissements des transitions nous donnent les réseaux présentés en figure 2.a' et 2.b'compte tenu du poids affecté à chaque arc.

L'utilisation des réseaux de Petri Stochastiques permet de prendre en compte l'occurrence des défaillances et leur influence sur le comportement du système Ces réseaux sont obtenus en injectant des durées de franchissement aléatoires aux transitions.

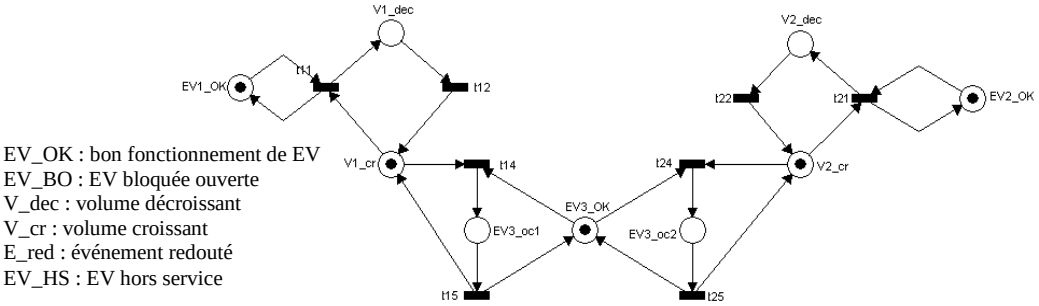


FIG. 3 – Modèle fonctionnel de réseau de Petri du cas étudié.

La figure 3 représente le réseau de Petri qui illustre le système étudié (figure 1). Ce réseau représente uniquement la partie fonctionnelle de notre système. Après l'application de l'analyse

dysfonctionnelle grâce à l'AMDE, nous avons repéré les défaillances jugées graves et nous les avons introduites dans le modèle fonctionnel comme le montre la figure 4.

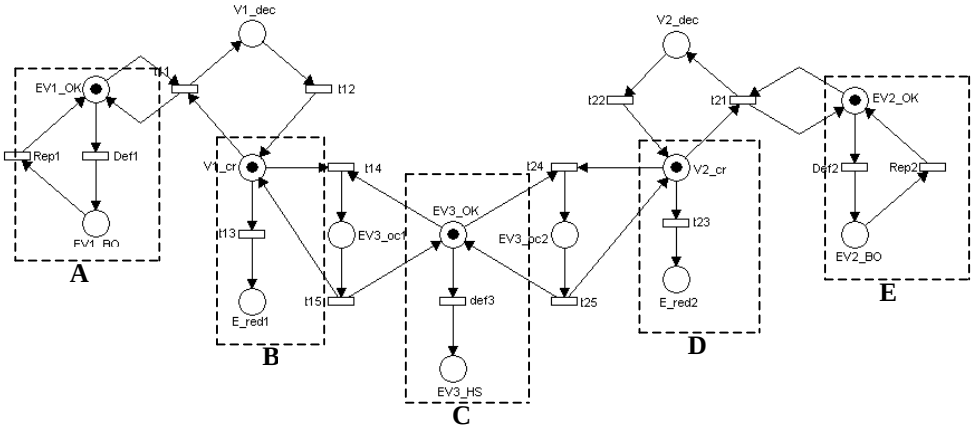
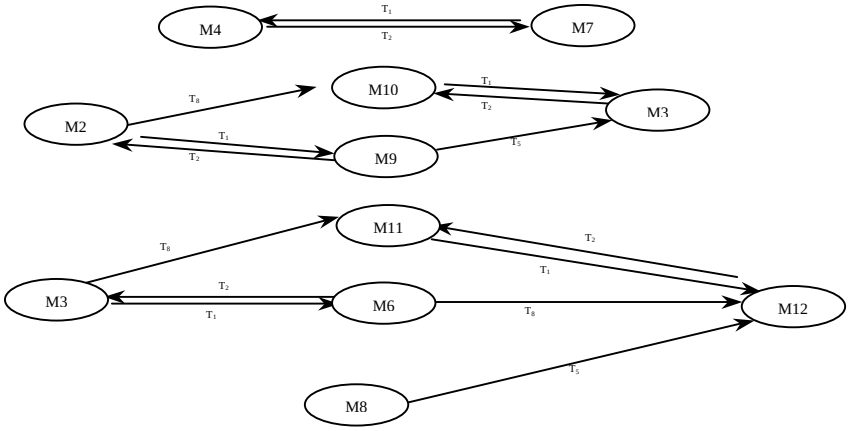


FIG. 4 – Modèle fonctionnel et dysfonctionnel de réseau de Petri du cas étudié.

Les blocs A et E représentent la défaillance et la réparation des électrovannes EV_1 et EV_2. Les blocs B et D représentent les événements redoutés (débordement de R_1 et R_2). Enfin le bloc C représente la défaillance, mais sans réparation, de l'électrovanne EV_3. On peut déduire de ce réseau de Petri, la matrice d'incidence avant $Pre(P_i,T_j)$, la matrice d'incidence arrière $Post(P_i,T_j)$ et la matrice d'incidence W [Barreau et al 2004]. Afin de simplifier le travail et de faciliter l'élaboration du graphe de marquage, nous nous sommes intéressés à la moitié du réseau en considérant la symétrie. Et nous avons obtenu le graphe de marquage comme illustré sur la figure3.



M_2=(10100010) M_3=(10001010) M_4=(10000100) M_6=(01001010) M_7=(01000100) M_8=(01010001) M_9=(01100010) M_{10}=(10100001) M_{11}=(10001001) M_{12}=(01001001) M_{13}=(01100001)

FIG. 5 – Graphe de marquage du réseau de Petri.

M_2, M_3, M_4, M_6, M_7, M_8, M_9, M_{10}, M_{11}, M_{12}, M_{13} représentent les marquages intermédiaires que peut prendre le réseau de Petri. A partir de ce graphe de marquage, on peut déduire la matrice des taux de transition Q. Pour les premiers résultats obtenus, nous avons utilisé des lois exponentielles pour les transitions def_1, t_{13}, def_3 et rep_1 qui sont définies en fonction des moyennes des temps MTBF et MTTR $\left(\lambda = \frac{1}{MTBF},\ \mu = \frac{1}{MTTR}\right)$. Avec $\lambda_1 = \lambda_8 = 2.10^{-3}$, $\lambda_5 = 10^{-3}$, $\mu_2 = 2.10^{-2}$. $\lambda_1, \lambda_5, \lambda_8$ représentent les taux de défaillance (pour respectivement def_1, t_{13} def_3 voir figure 4). μ_2 correspond au taux de réparation (pour rep_1 voir figure 4).

La probabilité d'apparition (en régime stationnaire) est obtenue grâce à la résolution de l'équation matricielle suivante : $\Pi.Q = 0$ avec $\sum_i \pi_i = 1$ (1)

Pour des taux de défaillance et de réparation choisis, la probabilité d'apparition de l'événement redouté correspondant au débordement est égale à :

$$\Pr[M(P_5) = 1] = \pi_3 + \pi_6 + \pi_{11} + \pi_{12} = 0.1781$$

La probabilité d'apparition d'un événement redouté d'un système mécatronique ainsi calculée, ne pourra pas être évaluée correctement, que si l'on définit justement les lois de transition du réseau de Petri. Ceci dépendra beaucoup d'un retour d'expérience sur les états de fonctionnement des différents composants du système.

5 Conclusion et perspectives

L'article présente l'enchaînement et l'utilisation, pour un système mécatronique simple, de différentes méthodes qui sont classiquement utilisées en Sûreté de Fonctionnement. Nous avons effectué une analyse qualitative en utilisant l'AMDE qui nous a permis d'identifier les principales causes de défaillance. Cette analyse a été complétée par une analyse quantitative grâce aux réseaux de Petri stochastiques afin de représenter le comportement dynamique du système. De ce réseau, on en a déduit la matrice des taux de transitions ainsi que les probabilités des régimes stationnaires pour pouvoir calculer la probabilité d'apparition de l'événement le plus redouté identifié grâce l'AMDE.

Les perspectives que nous envisageons pour ce travail porteront sur la partie logiciel, sur une comparaison de résultats quantitatifs obtenus à partir d'autres méthodes (réseaux Bayésiens par exemple).

Références

Barreau M., Todoskoff A., Mihalache A., Guerin F., & Dumon B. 2004. Dependability assessment for mechatronic systems: electronic stability program (ESP) analysis. *IFAC AVCS International Conference on Advances in Vehicle Control and Safety*, Gênes Italia.

Girault C., & Valk R. 2003. Petri Nets for systems Engineering. A guide to modelling, Verification, and Application. *Springer*. Germany.

Khalfaoui S. 2003. Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile. *Institut national polytechnique*. Toulouse.

Khalfaoui S., Guilhem E., Demmou H., & Valette R. 2002. Une méthodologie pour obtenir des scénarios critiques dans les systèmes mécatroniques. *ESREL, European Conference*.

Ladet P. 1989. Réseaux de Petri. *Techniques de l'ingénieur, S1*.

Moncelet G. 1998. Application des Réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile. *Université Paul Sabatier*. Toulouse.

Vidal-Naquet G., & Choquet-Geniet A. 1992. *Réseaux de Petri et Systèmes Parallèles*. Paris: Armand Colin.

Villemeur A. 1988. Sûreté de fonctionnement des systèmes industriels. *Eyrolles*.

Zwingelstein G. 1996. La maintenance basée sur la fiabilité. Guide pratique d'application de la RCM. *Hermes*. Paris

Demri A., Charki A., Guerin F., & Christofol H. Analyses Fonctionnelle et Dysfonctionnelle d'un Système Mécatronique. *Qualita*, Tanger, Maroc.