Une méthode pour obtenir des scénarios critiques dans les systèmes mécatroniques

Sarhane KHALFAOUI[*,**] et Edwige GUILHEM[*]
* PSA Peugeot Citroën
Direction des Systèmes d'Information
18, rue des Fauvelles
F-92256 La Garenne Colombes cedex

Hamid DEMMOU[**] et Robert VALETTE[**]
** LAAS CNRS
7, avenue du Colonel Roche
F-31077 Toulouse cedex

Summary
This paper deals with safety in design of mechatronic systems. For this purpose, it is important to characterize feared behaviors (which are critical) in the early design stage. In order to help designers taking into account safety constraints, the feared behaviors have to be directly derived from a system model. A qualitative and quantitative analysis of these behaviors are necessary to select good architectures. The qualitative analysis points out all the behaviors leading to states in which the motorist and the passengers safety is no longer guaranteed. We are proposing a method based on a qualitative analysis of a Petri net model of the system. It allows to derive feared scenarios by determining the sequences of actions and state changes leading to the feared state. Finally we present a comparison between Fault trees and the results obtained by our approach.

Introduction

La part croissante de l'électronique dans le secteur automobile, bien qu'ayant considérablement amélioré et diversifié les services rendus par le véhicule, a complexifié la conception des systèmes mécatroniques sûrs, alliant mécanique, hydraulique et électronique ainsi qu'un calculateur. Ces systèmes sont hybrides, la dynamique continue étant associée à la partie énergétique et la dynamique discrète étant liée à la commande numérique, et à l'existence d'événements discrets (défaillances, dépassement de seuils…). Ce papier s'intéresse à la sécurité des systèmes mécatroniques. Pour cela, il est important de caractériser les scénarios redoutés au plus tôt dans la phase de conception.

La rareté de ces scénarios redoutés rend inefficaces les méthodes basées seulement sur la simulation [1]. Pour aider les concepteurs à prendre en compte les contraintes de sécurité, les scénarios redoutés doivent être directement déduits d'un modèle du système. Une analyse qualitative et quantitative de ces scénarios est nécessaires pour choisir les architectures les plus sûres. Comme le système est hybride, nous avons choisi une modélisation associant réseau de Petri et équations différentielles [2]. Le modèle réseau de Petri décrit le fonctionnement nominal, les défaillances et les mécanismes de reconfiguration.
Nous proposons une méthode basée sur l'analyse qualitative du modèle RdP permettant de déduire les scénarios redoutés, en particulier en déterminant la suite d'actions et d'états conduisant à l'état redouté.
Une comparaison des résultats obtenus avec les méthodes classiques de SdF (arbres de défaillances) est présentée à la fin de l'article.

Cas d'étude

Présentation

Le cas d'étude est basé sur un système de régulation du volume de deux réservoirs (cf figure 1). Il est constitué d'un calculateur, de deux pompes, de trois électrovannes (tout ou rien), de deux capteurs de volume et des deux réservoirs régulés (Réservoir 1, Réservoir 2) et d'un troisième réservoir de vidange. Les deux réservoirs régulés alimentent des utilisateurs selon un besoin prédéfini (fonction du temps).
Le volume dans chaque réservoir (1 ou 2) doit rester dans un intervalle donné [V_{imin}, V_{imax}]. Le contrôle s'opère à l'aide du calculateur qui décide, selon la valeur du volume (délivrée par le capteur), d'approvisionner (ou non) le réservoir en question en en alimentant (ou non) l'électrovanne concernée.
Pour chaque réservoir, on distingue donc deux phases de fonctionnement selon que l'électrovanne alimentant ce réservoir est ouverte ou fermée :

- Une phase de conjonction lorsque l'électrovanne est ouverte. Le volume dans le réservoir est croissant durant cette phase, et cela quelle que soit la valeur du débit de sortie vers l'utilisateur (le débit d'alimentation de l'électrovanne est bien supérieur, par hypothèse, au débit de sortie).
- Une phase de disjonction lorsque l'électrovanne est fermée. Le volume dans le réservoir est par conséquent décroissant.

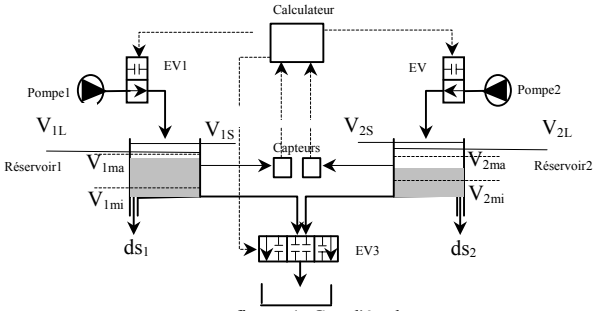


figure 1. Cas d'étude

La loi de contrôle du calculateur pour chaque réservoir est telle que lorsque le volume dépasse la limite supérieure de commande V_{imax} pendant la phase de conjonction, alors le calculateur commande la fermeture de l'électrovanne. Lorsque le volume devient inférieur à V_{imin} (limite inférieure de commande) durant la phase de disjonction alors le calculateur commande à l'électrovanne de s'ouvrir et on change par conséquent de phase de fonctionnement.
Ce système doit assurer l'approvisionnement des utilisateurs tout en évitant le débordement de l'un des réservoirs. Une troisième électrovanne de secours est prévue pour cet effet. Elle est partagée entre les deux réservoirs et assure leur vidange quand ils débordent. Elle ne peut être utilisée que par un seul réservoir à la fois. Quand le volume dans l'un des réservoirs dépasse la limite supérieure de sécurité (V_{iL}), alors le calculateur commande l'ouverture de cette électrovanne du côté du réservoir qui risque de déborder, et ce jusqu'à ce que le volume devient inférieur à V_{imin}.

Pour simplifier nous supposons que seules les électrovannes peuvent subir des défaillances. Les électrovannes 1 et 2 (prévues pour l'alimentation des

réservoirs) peuvent être bloquées en ouverture. En cas de défaillance de l'électrovanne 3 (de secours), celle ci est mise hors service.

Modélisation

Modèle du fonctionnement nominal

Le fonctionnement nominal du système des deux réservoirs consiste en une succession de phases de conjonction et de disjonction suite à des commandes d'ouverture et de fermeture des électrovannes. Le fonctionnement des deux réservoirs est identique en termes d'états et de succession d'états. En effet, les deux réservoirs possèdent la même loi de commande et les deux électrovannes possèdent les mêmes modes de défaillance. Une fois le modèle du réservoir 1 et de sa commande établi, il suffit de le dupliquer en adaptant tout simplement les seuils de commande et les paramètres de défaillances et de réparation à ceux du réservoir 2.

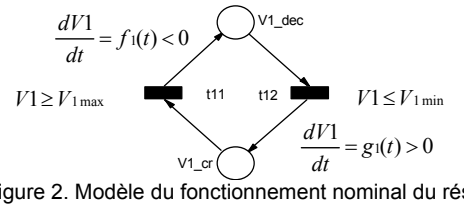


figure 2. Modèle du fonctionnement nominal du réservoir 1

La figure 2 illustre le modèle de fonctionnement nominal du réservoir 1. La place V1_dec représente la phase de disjonction (le volume décroît) tandis que la place V1_cr représente la phase de conjonction pendant laquelle le volume croit. La place EV1_OK modélise le bon fonctionnement de l'électrovanne 1. Les transitions t11 et t12 représentent respectivement la commande de fermeture de l'électrovanne 1 quand le volume dépasse V1max et la commande d'ouverture de la même électrovanne quand le volume devient inférieur à V1min.

Modèle de défaillance et de réparation de l'électrovanne 1

Ce modèle est le suivant :

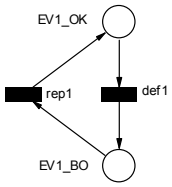


figure 3. Défaillance et réparation de l'électrovanne 1

Il représente le fait que l'électrovanne reste bloquée en ouverture après le tir de def1 et qu'elle peut reprendre un comportement normal après réparation (tir de rep1).

Modèle d'utilisation de l'électrovanne de secours

Cette électrovanne peut être utilisée de manière identique par les deux réservoirs 1 et 2.

Quand le volume dans le réservoir 1 dépasse la limite supérieure de sécurité (V_{1L}), et si l'électrovanne de secours est disponible (la place EV3_OK est marquée) alors t14 devient franchissable et on commence la procédure de vidange du réservoir 1 via l'électrovanne 3 en marquant la place EV3_oc1 . L'électrovanne n'est pas disponible pour une autre utilisation que celle en cours (place EV3_OK vide). Cette phase dure le temps que met le volume pour atteindre le seuil bas V1min. Ensuite, on libère l'électrovanne 3 (on marque de nouveau EV3_OK) et on recommence une phase de conjonction (on remet un jeton dans la place V1_cr) en tirant la transition t15.

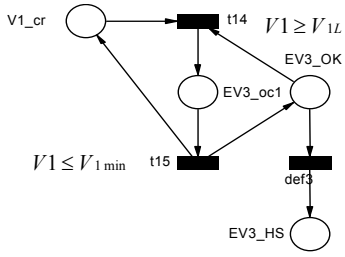


figure 4. Utilisation de l'électrovanne de secours

L'électrovanne peut subir une défaillance (tir de la transition def3). Dans ce cas, la place EV3_HS est marquée et l'électrovanne est mise hors service.

Modèle de système complet

Le modèle du système de régulation est le RdP de la figure suivante. Il regroupe les modèles de fonctionnement nominal des deux réservoirs, les modèles de défaillance et de réparation des électrovannes 1 et 2, les modèles d'utilisation de l'électrovanne de secours ainsi que les modèles d'occurrence des événements redoutés débordement des réservoirs 1 ou 2.

On déclare qu'il y a débordement d'un des deux réservoirs, par exemple le réservoir 1, quand le volume dans ce dernier dépasse V_{1S} (V_{1S} étant supérieur à V1max et à V_{1L}). Dans ce cas, on tire la transition t13 et on marque la place E_red1.

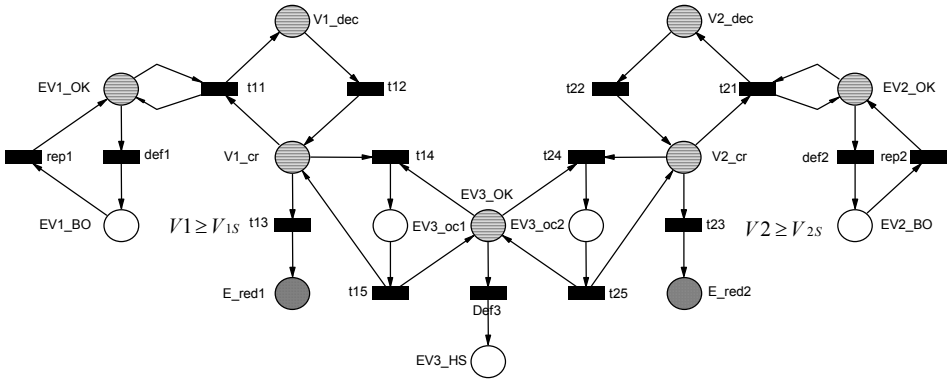


figure 5. Modèle RdP du cas d'étude

Méthode de recherche de scénarios critiques

Principe de la méthode

Le but de cette méthode est de mettre en évidence les suites d'actions et d'états qui conduisent aux états redoutés et d'analyser plus précisément ce qui fait que le système quitte le fonctionnement normal pour aller vers l'état redouté. La méthode que nous proposons est basée sur une analyse qualitative à partir d'un modèle Réseau de Petri. Ce modèle représente le fonctionnement nominal du système ainsi que son comportement en présence de défaillances. Il s'agit donc d'extraire et de rendre explicite les scénarios redoutés à partir d'un modèle agrégeant un ensemble de connaissances sur le fonctionnement du système.

Le principe de notre méthode est d'enrichir progressivement le contexte dans lequel s'est produit l'événement conduisant à l'état redouté, en étudiant les conflits de comportements ayant un lien de causalité avec l'occurrence de l'événement redouté. Partant d'une connaissance très partielle des conditions d'occurrence de cet événement (par exemple le déclenchement d'une alarme suite au franchissement d'un seuil de sécurité), on s'intéresse aux comportements qui permettent d'éviter le chemin critique et qui correspondent à des bifurcations représentées par des conflits de transitions. L'étude des conditions de tirs de ces transitions de bifurcation nous informe de manière plus complète sur les conditions d'occurrence de l'événement redouté. Pour garantir la non occurrence de l'événement redouté (et donc une bifurcation du chemin critique), certaines conditions sont nécessaires, par exemple la disponibilité d'une ressource de reconfiguration ou la présence du système dans un état de fonctionnement bien déterminé. La non satisfaction de ces conditions nous conduit inévitablement vers l'état redouté. On a enrichi par conséquent nos connaissances sur l'événement redouté en faisant intervenir d'autres conditions (la non disponibilité d'une ressource, par exemple). L'étude des comportements qui sont en conflit avec ceux en conflit avec le comportement critique (et qui favorisent par conséquent l'occurrence de l'événement redouté) nous informe plus précisément sur le contexte dans lequel a eu lieu l'événement redouté. C'est pourquoi notre démarche se poursuit récursivement selon le même principe et pas à pas en analysant chaque état partiel intervenant dans un scénario redouté comme un état redouté et en se posant la question de savoir comment on peut y arriver. Nous avons élaboré une méthode générale basée sur 4 étapes qui a pour but de déterminer les conditions de marquages d'un ensemble de places donné (qu'on appelle état cible). Cela consiste à déterminer de manière systématique et formelle comment marquer et démarquer cet ensemble de places.

Cette méthode est composée de 4 étapes :

1. Détermination des états normaux (qualitativement ou quantitativement)
2. Détermination des états cibles (états partiels redoutés ou états à étudier)
3. Raisonnement arrière à partir de l'état cible (peut être un état redouté ou n'importe quel autre état partiel du modèle RdP)
4. Raisonnement avant à partir des états conditionneurs (mettre en évidence les ramifications : bifurcation entre fonctionnement normal et scénarios redoutés).

La première étape consiste à déterminer les places dont le marquage représente un état de fonctionnement normal. Ces places nominales seront utilisées comme critère d'arrêt du raisonnement arrière. Cette étape peut être réalisée de deux manières : soit en utilisant une connaissance a priori des états de bon fonctionnement du système soit en effectuant une simulation de Monte Carlo du modèle sur une courte fenêtre temporelle pour déterminer la probabilité de marquage des places du réseau. Celles qui auront une probabilité de marquage non négligeable seront assimilées à des places normales.

La deuxième étape détermine l'état cible à étudier. Cet état cible peut être soit un état partiel redouté soit un autre état partiel ayant un lien de causalité direct ou indirect avec cet état redouté (par exemple une place qui représente la disponibilité d'une ressource pour assurer un fonctionnement dégradé évitant l'occurrence de l'événement redouté).

La troisième étape génère l'ensemble des chemins qui mènent vers l'état partiel redouté. On effectue un raisonnement sur le modèle RdP inversé, c'est pour cette raison qu'on l'appelle étape de raisonnement arrière. Dans ce réseau inversé, on prend comme marquage initial le seul état redouté et l'on cherche de façon exhaustive tous les scénarios [3] minimaux (aucun franchissement de transition non nécessaire n'est effectuée) permettant de consommer le marquage initial et aboutissant à un marquage final uniquement formé de places associées au fonctionnement normal. Au cours de cette étape, on est en général amené à enrichir le marquage initial (ajouter des jetons dans certaines places). Cela se fera chaque fois que pour consommer un jeton dans une place non associée à un fonctionnement normal il faut franchir une transition non sensibilisée par un marquage accessible à partir du marquage initial non enrichi. Les jetons ajoutés lors du processus d'enrichissement du marquage correspondant à des états partiels qui sont des conséquences logiques des scénarios redoutés et qui seront donc nécessairement observés lors de l'évolution du système vers l'état redouté. En inversant les scénarios obtenus lors de cette étape, nous aurons les suites d'actions possibles menant d'un état normal à l'état redouté. Cet état normal est nommé état conditionneur.

La dernière étape de la méthode consiste à construire un raisonnement à partir du modèle RdP initial en partant de chaque état conditionneur déterminé à l'étape précédente. C'est l'étape de raisonnement avant. Cela a pour objectif de localiser les bifurcations entre le comportement redouté et le fonctionnement normal du système ainsi que les conditions (de marquage de certaines places du réseau) impliquées dans ces bifurcations.

Afin de mieux comprendre cette méthode de recherche de scénarios, nous allons la mettre en œuvre en s'appuyant sur le modèle du système de régulation des réservoirs.

Application au cas d'étude

Première itération

Appliquons maintenant la méthode décrite précédemment au cas d'étude.

1. Etats normaux : Ce sont les places rayées dans le modèle du système complet.
2. Etat cible : On s'intéresse au débordement du réservoir 1. L'état cible sera donc l'état partiel redouté E_red1 (place grisée dans le RdP).
3. Raisonnement arrière à partir de l'état cible : Cette étape donne la liste des scénarios menant à l'état partiel redouté. La seule transition en aval de la place E_red1 est la transition t13. Un jeton est alors produit dans la place V1_cr. Cette dernière représentant un état de fonctionnement normal, le raisonnement arrière s'arrête. On obtient donc le scénario qui représente l'accessibilité de l'état partiel redouté E_red1 à partir du marquage de la place V1_cr (qu'on appelle état conditionneur) en tirant une fois la transition t13.

4. Raisonnement avant à partir de la place V1_cr :
   Le but de cette étape est de mettre en évidence les bifurcations entre le fonctionnement normal et les scénarios redoutés. La place V1_cr représente un état conditionneur à partir duquel on pourrait évoluer soit vers l'état redouté en question (marquage de E_red1 par le tir de la transition t13) soit vers d'autres fonctionnements. Cela se traduit par le conflit entre les trois transitions en aval de la place V1_cr : t13, t11 et t14.
   Cette étape donne trois fonctionnements possibles selon que l'une ou l'autre des transitions est tirée :
   - le scénario redouté trouvé dans l'étape précédente (à partir du marquage de V1_cr, tirer une fois la transition t13 pour marquer E_red1).
   - le tir de t11 à partir du marquage initial (un jeton dans chacune des places V1_cr et EV1_OK) conduisant au marquage des places V1_dec et EV1_OK. Ce scénario représente la fermeture de l'électrovanne EV1 quand elle n'est pas bloquée en ouverture et quand le volume dans le réservoir 1 dépasse la limite de contrôle supérieure ($V>V_{1max}$).
   - le tir de la transition t14 à partir du marquage de V1_cr et de EV3_OK. Cela conduit au marquage de la place EV3_oc1. Ce scénario correspond au début de la procédure de vidange de secours du réservoir 1 quand l'électrovanne 3 (appelée EV3) est disponible.

Suite à l'application de notre méthode à l'état partiel redouté débordement du réservoir 1 (correspondant au marquage de la place E_red1) on obtient les résultats suivants :

- L'occurrence de l'événement redouté (tir de t13 et/ou marquage de E_red1) est provoqué par le non franchissement des transitions t11 et t14 qui sont en conflit structurel avec t13.
- Ceci nous amène par conséquent à l'étude des conditions de sensibilisation de ces transitions, à savoir comment obtenir un marquage suffisant pour pouvoir franchir ces transitions (comment sont marquées les places EV1_OK et EV3_OK en même temps que la place V1_cr). Nous prenons en compte, lors de cette analyse des conflits, les valeurs des seuils (des variables continues) associés aux transitions. Par exemple, pour pouvoir franchir t13 il faut qu'il y ait au moins un jeton dans chacune des places V1_cr et EV1_OK et aussi que la condition ($V1 \geq V_{1\max}$) soit vérifiée.

Afin de mieux analyser les conflits entre les transitions t13, t11 et t14, nous allons réitérer la méthode de recherche de scénarios pour analyser les conditions de tirs des transitions t11 et t14.

Deuxième itération

Commençons tout d'abord par l'étude des conditions de franchissement de t11. A cette transition est associé le seuil $V1 \geq V_{1\max}$. Cette condition est toujours vraie lorsque t13 est franchissable puisque le seuil de t13 est $V1 \geq V_{1S}$ et on a $V_{1S} > V_{1\max}$. Donc si les places EV1_OK et V1_cr sont marquées, t11 sera toujours franchie avant t13, évitant ainsi le débordement. Il est donc nécessaire d'analyser précisément le ou les scénarios amenant à ce marquage. Pour que l'approche soit exactement récursive, nous allons rajouter au modèle RdP du cas d'étude une place virtuelle (cf figure) reliant, par l'intermédiaire d'une transition, les places qui nous intéressent (V1_cr et EV1_OK). Cette place (appelé Etat cible virtuel 1) représente un état virtuel (par rapport au système réel) et n'est autre qu'un artifice pour pouvoir appliquer notre méthode à partir de cet état. En effet, chercher les scénarios produisant un jeton dans cette place c'est exactement rechercher les scénarios amenant à la présence simultanée d'un jeton dans V1_cr et d'un jeton dans EV1_OK.

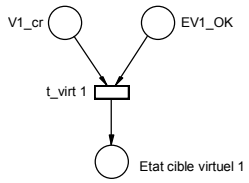


figure 6. Etat cible 1

La méthode de recherche de scénarios donne les résultats suivants :

1. Etats normaux : Ils sont représentés par le marquage des mêmes places rayées à l'exception de EV1_OK et de V1_cr. En effet, comme on se propose d'étudier comment marquer ces places, il faut les soustraire de la liste des états normaux pour pousser le raisonnement arrière plus loin.
2. Etat cible : On s'intéresse au marquage de la place « Etat cible virtuel 1 ».
3. Raisonnement arrière à partir de l'état cible : Le premier pas de cette étape nous ramène dans l'état correspondant au marquages des places V1_cr et EV1_OK. Les transitions en aval de V1_cr sont t12 et t25. Le tir de t12 produit une jeton dans V1_dec qui représente un état normal. Le tir de t15 sera analysé lors de la troisième itération. En aval de V1_dec les transitions rep1 et def1 sont franchies et cela nous ramène de nouveau dans cette place. On obtient le scénario représentant la boucle d'occurrence d'une défaillance de l'électrovanne et de sa réparation (tir des transitions def1 et rep1). L'état conditionneur est alors le marquage de la place EV1_OK.
4. Raisonnement avant à partir de l'état conditionneur : On retrouve le franchissement de def1 ou (ou exclusif) celui de t11.

Troisième itération

Etudions maintenant les conditions de tir de t14. De même que pour t11, le seuil associé est tel que si les places en amont de t14 sont marquées elle sera franchie avant t13 et bloquera l'évolution redouté. On rajoute l'état cible virtuel de la figure 7.

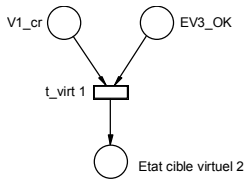


figure 7. Etat cible 2

La méthode de recherche de scénarios donne les résultats suivants :

1. Etats normaux : places rayées du réseau à l'exception de EV3_OK et de V1_cr.
2. Nouvel état cible = C'est le marquage de la place « Etat cible virtuel 2 »
3. Raisonnement arrière à partir de l'état cible : Le premier pas de cette étape nous ramène dans l'état correspondant au marquage des places V1_cr et EV3_OK. A partir de V1_cr on franchit t12 et on marque V1_dec.. On peut marquer la place EV3_OK

de deux façons différentes à l'issue des deux scénarios suivants :

- Le tir de t15 puis de t14 dans le RdP inversé et le marquage des places EV3_OK et V1_cr,
- Le tir de t25 suivi du tir de t24 et le marquage des places EV1_OK et V2_cr. Le premier scénario représente la vidange du réservoir 1 en utilisant l'électrovanne 3 avec succès. Le deuxième scénario illustre l'utilisation de l'électrovanne 3 pour vider le réservoir 2 puis la libération de cette ressource à la fin de la vidange (quand le volume devient inférieur à V_{2min}).

4. Raisonnement avant à partir des états conditionneurs : On a trois états conditionneurs : V1_dec, V2_cr et EV3_OK. Cela donne les ramifications suivantes :
   - A partir de V2_cr : soit le tir de t23 et le marquage de la place E_red2 (débordement du réservoir 2) soit le tir de t21 (en supposant que la place EV2_OK est aussi marquée) et le marquage de V2_dec et de EV2_OK. Ce scénario correspond à la fermeture de l'électrovanne 2 quand le volume dans le réservoir 2 dépasse V_{2max}.
   - A partir de V1_dec, l'unique évolution est celle correspondant à l'ouverture de l'électrovanne 1 quand le volume franchit le seuil V_{1min} (tir de t12). On retrouve la situation de conflit que nous sommes en train d'étudier entre t11, t13 et t14.
   - A partir de EV3_OK, un scénario correspond au tir de la transition def3 (défaillance de l'électrovanne 3 de secours). Un autre scénario possible, en conflit avec le précédent est le tir de t12 et de t14. Le troisième, en conflit avec les deux précédents, consiste à tirer t24.

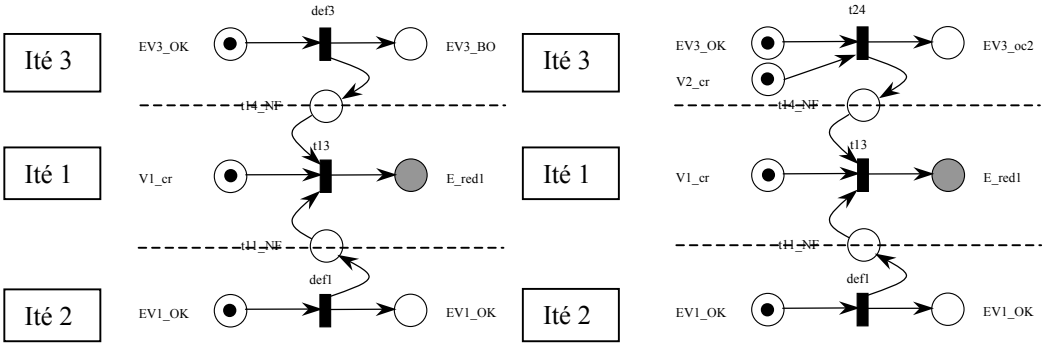
La transition t14 est sensibilisée si les deux places V1_cr et EV3_OK sont marquées. Les possibilités pour qu'il n'y ait pas de jetons dans la place EV3_OK sont soit le tir de def3 (défaillance de l'électrovanne 3) soit le tir de t24 sans le tir de t25 (vidange du réservoir 2 par l'électrovanne 3). Pour pouvoir tirer t24, il faut qu'il ait un jeton dans chacune des places EV3_OK et V2_cr.

Résultats

L'état redouté ne sera atteint que par le franchissement de t13. Comme nous l'avons déjà dit, à cause des seuils associés aux transitions t11, t14 et t13, la transition t13 n'est franchie que si t11 et t14 ne sont pas sensibilisées. Cela veut dire que les scénarios redoutés seront composés d'une part de scénarios comprenant des transitions en conflit avec t11 et t14, et d'autres part du scénario de franchissement de t13. Ce dernier scénario a été défini par la première itération de la méthode. Le scénario empêchant le tir de t11 est issu de la deuxième itération, et les deux scénarios empêchants le tir de t14 sont issus de la troisième itération.

Détaillons ce dernier point. Lors du raisonnement avant à partir des états conditionneurs, nous avons vu qu'il y avait deux cas pour lesquels la transition t14 n'était pas franchie à cause du conflit autour de la place EV3_OK. Il s'agit soit du franchissement de def3 (l'électrovanne 3 est définitivement hors d'usage) soit du franchissement de t24 (vidange de secours du réservoir 2) impliquant un jeton dans V2_cr. Ces deux cas étant exclusifs, nous aurons donc deux scénarios redoutés. Ces deux scénarios comprendront également le scénario obtenu lors de la deuxième itération raisonnement avant qui franchit la transition def1. Ces scénarios définissent des relations d'ordre entre les franchissements des transitions et peuvent donc être représentés par les deux réseaux de Petri de la figure 8. Ces réseaux de Petri sont des graphes d'événements c'est à dire qu'ils ne comportent aucun conflit. La partie, notée Ité 2 sur la figure 8, des deux scénarios correspond au résultat de la deuxième itération et la partie Ité 3 correspond aux deux cas trouvés lors de la troisième itération. La place reliant def1 à t13 exprime le fait que pour ne pas franchir t11 il faut franchir def1 avant t13. De même, la place reliant def3 à t13 exprime le fait que t14 ne doit pas être franchie. Par contre, aucune relation d'ordre n'existe entre le tir des transitions def1 et def3 pour le cas (a) et def 1 et t24 pour le cas (b). Un scénario correspond donc à un ensemble de séquences de tirs de transitions. Par exemple le scénario (a) correspond aux séquences (def1 ; def3 ; t13) et (def3 ; def1; t13).

La symétrie du fonctionnement des deux réservoirs (qui se traduit par une symétrie dans le modèle RdP) permet d'étendre les résultats obtenus au réservoir 2.



a)- Premier scénario redouté

b)- Deuxième scénario redouté

figure 8. Les deux scénarios redoutés sous forme de 2 RdP

Comparaison avec les arbres de défaillances

La description du scénario que nous venons de donner se présente sous la forme d'un arbre dont les nœuds sont les événements et les arcs les états partiels.
La méthode la plus utilisée dans les études de Sûreté de Fonctionnement pour l'identification des situations redoutés est la méthode des arbres de défaillances. Elle donne une représentation des causes de défaillances et de leurs combinaisons conduisant à une situation redoutée.
Nous allons dans cette section comparer l'arbre que nous avons obtenu avec les arbres de défaillances en nous appuyant sur le système de régulation du volume de deux réservoirs.

Arbre de défaillance classique

Il ne fait intervenir que les états (défaillants ou en bon fonctionnement) des composants nécessaires à l'occurrence d'une situation redoutée. L'arbre relatif au débordement du réservoir 1 est présenté sur la figure suivante :

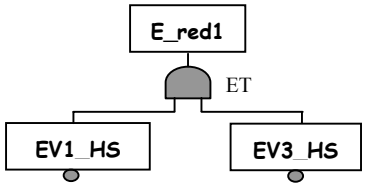


figure 9. Arbre de défaillance du débordement du réservoir 1

Il exprime le fait qu'il est suffisant que les deux électrovannes 1 et 3 soient défaillantes (EV1_HS et EV3_HS) pour que le réservoir 1 déborde (c'est la situation redoutée notée E_red1). En fait cet arbre est incorrect car l'électrovanne 3 peut ne pas être disponible sans être pour autant hors service. Nous avons affaire à un système dynamique.

Arbre de défaillances avec prise en compte des états

Avec une connaissance des états de l'électrovanne 3, il est possible d'utiliser la notion d'arbres de défaillances et les outils associés (outil SOFIA de Sofreten [4]) pour générer un arbre de défaillances ne se restreignant pas uniquement aux états de bon ou mauvais fonctionnement.
Dans l'exemple des deux réservoirs, il existe alors un deuxième scénario qui mène à la situation redoutée correspondant à la défaillance de l'électrovanne 1 et à l'utilisation de l'électrovanne 3 pour vider le réservoir 2 (cf figure 10).

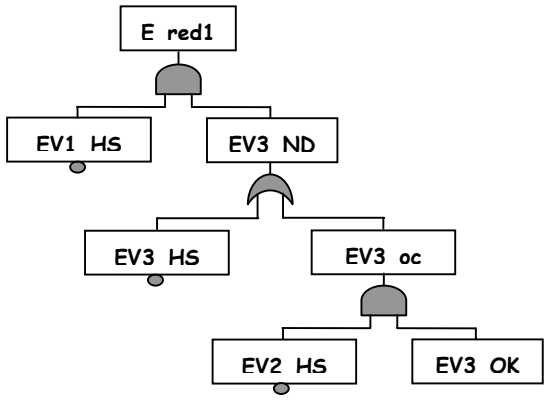


figure 10. Arbre de défaillance avec prise en compte des états de l'électrovanne 3

Discussion

L'arbre de défaillances de la figure 10 ne fait référence qu'à des états de composants et n'explicite pas les changements d'états. On trouve ainsi les deux situations critiques (électrovannes 1 et 3 hors service ou électrovanne 1 et 2 hors service et électrovanne 3 occupée à vidanger le réservoir 2) sans pour autant savoir quelle est la suite de changements d'états qui mène d'un état de bon fonctionnement à l'une des deux situations redoutées. En conséquence les scénarios qui mènent à ces situations redoutés ne peuvent pas être déduits de cet arbre, et comme le système est dynamique la connaissance des probabilités des états partiels de chaque composant ne suffit pas pour déduire la probabilité des situations redoutés.
La méthode des graphes de flux dynamiques [5] a été introduite pour prendre en compte les évolutions temporelles dans les arbres de défaillances. Elle est basée sur une modélisation hybride du système et une génération automatique d'arbres de défaillances temporisées. Cette approche impose une discrétisation systématique du temps et des variables continues, ce qui entraîne une explosion combinatoire des états.
Notre approche est également basée sur un modélisation hybride du système. Le fait que cette modélisation soit fondée sur les réseaux de Petri permet la mise en évidence des scénarios menant aux états redoutés sans discrétisation du temps.
Chaque scénario est généré sous la forme d'un graphe orienté. En inversant les flèches de ces graphes et en considérant que les transitions sont de conjonctions on obtient des descriptions proches de celle des arbres de défaillances. En effet, chaque nœud est un état partiel comme c'est le cas dans l'arbre de défaillances de la figure 10. Les transitions du graphe à la fois jouent le rôle des portes ET des arbres de défaillances et celui des repères des changements d'états dans les arbres temporisés.

Conclusion

La méthode que nous avons présentée est basée sur modélisation préalable d'un système mécatronique sous la forme d'un réseau de Petri et d'un ensemble d'équations différentielles. Cette modélisation hybride présente l'avantage de séparer clairement les aspects discrets et continus. Ceci nous permet une analyse logique (fondée sur la logique Linéaire [6]) des causalités résultant des changements d'états. Grâce à cette analyse, il est possible à partir d'un état redouté de remonter les chaînes de causalité et de mettre ainsi en évidence tous les scénarios possibles conduisant à une situation critique. Chaque scénario est donné sous la forme d'un ordre partiel entre les événements nécessaires à l'apparition de l'état redouté contrairement aux arbres de défaillances qui donnent un ensemble de combinaisons d'états partiels nécessaire à la réalisation de la situation critique.

Il faut souligner le fait que l'approche que nous avons développée à partir de la logique Linéaire [3] [7] et n'implique pas une énumération brutale et globale de tous les états accessibles du système. Au contraire elle permet de se focaliser sur le voisinage de l'état redouté en faisant une énumération locale d'états partiels. Autrement dit, nous ne considérons que les états des composants directement impliqués dans l'apparition de l'état redouté.

Le travail se poursuit par une meilleure formalisation des algorithmes de recherche des scénarios redoutés en vue de leur automatisation.

A plus long terme, nous envisageons de proposer une méthode d'analyse quantitative utilisant éventuellement la

simulation de Monte Carlo s'appuyant sur la connaissance des scénarios redoutés

Références

[1] Gilles Moncelet, « Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile », Thèse de Doctorat, N°3076, Université Paul Sabatier, Toulouse.

[2] R. Champagnat, P. Esteban, P. Pingaud, R. Valette, « Modeling and simulation of a hybrid system through Pr/Tr PN DAE model, *ADPM'98 3rd International Conference on Automation of Mixed Processes*, 19-20 March 1998, Reims, France p. 131-137.

[3] S. Khalfaoui, E.Guilhem, H. Demmou, N. Rivieres, «Extraction de scénarios critiques à partir d'un modèle RdP à l'aide de la logique Linéaire », MSR'2001 Modélisation des systèmes réactifs, 17-19 Octobre 2001, Toulouse, France p. 409-424.

[4] Manuel d'utilisation de l'outil Sofia de la sociéte Sofreten, disponible à partir de la page web «http://www.sofreten.fr/Aide%20Simfia/index.htm»

[5] 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.

[6] J.Y Girard, « Linear Logic », *Theoretical Computer Science*, 50, 1987, p.1-102.

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