



HAL
open science

Vers une architecture de surveillance de santé d'un système hybride sous incertitudes

Quentin Gaudel, Pauline Ribot, Elodie Chanthery

► To cite this version:

Quentin Gaudel, Pauline Ribot, Elodie Chanthery. Vers une architecture de surveillance de santé d'un système hybride sous incertitudes. Modélisation des Systèmes Réactifs (MSR 2015), Nov 2015, Nancy, France. hal-01224457

HAL Id: hal-01224457

<https://inria.hal.science/hal-01224457>

Submitted on 4 Nov 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Vers une architecture de surveillance de santé d'un système hybride sous incertitudes

Quentin Gaudel^{1,3}, Pauline Ribot^{1,2} and Elodie Chanthery^{1,3}

¹ CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France
quentin.gaudel@laas.fr
pauline.ribot@laas.fr
elodie.chanthery@laas.fr

² Univ de Toulouse, UPS, LAAS, F-31400 Toulouse, France

³ Univ de Toulouse, INSA, LAAS, F-31400 Toulouse, France

Abstract

Ces travaux proposent d'effectuer de la surveillance de santé sous incertitudes pour des systèmes hybrides en utilisant une méthode basée sur des modèles. La surveillance de santé s'effectue grâce à des méthodes de diagnostic et de pronostic et nécessite donc un modèle de comportement et un modèle de dégradation du système. Le formalisme des réseaux de Petri hybrides particuliers (HPPN) est défini dans un contexte de surveillance de santé pour générer des diagnostiqueurs de systèmes hybrides. L'avantage principal des HPPN est la manière dont ils gèrent les incertitudes sur la connaissance du système et les observations. Ils modélisent aussi des incertitudes sur les équations du modèle et sur les observations continues en intégrant un filtrage particulière. Le formalisme prend également en compte la dégradation du système. On utilise ces informations incertaines pour en déduire un résultat de diagnostic sous incertitudes. L'approche est illustrée sur un exemple de système complexe.

1 Introduction

Le développement des systèmes industriels autonomes ou partiellement autonomes (satellites, drones, rovers, etc ...) est devenu de plus en plus complexe. Il devient difficile d'anticiper le comportement de ces systèmes, particulièrement lors de l'occurrence de pannes. Dans un contexte industriel, il est essentiel de réduire les coûts de maintenance et de réparation mais aussi d'assurer l'opérationnalité du système lorsque sa mission est critique. Il est alors nécessaire de connaître l'état de santé du système pour vérifier la faisabilité de sa mission et agir en conséquence. Au delà de l'implémentation de la mission, la conception du système s'élargit donc à la gestion de la santé. Ainsi la planification de mission ou de maintenance devra prendre en compte les résultats d'une fonctionnalité de surveillance de santé du système. Celle-ci s'effectue grâce à des méthodes de diagnostic et de pronostic à partir des observations sur le système.

La fonction de diagnostic vise à déterminer l'état de santé courant du système. C'est l'identification de la cause probable de la ou des défaillances à l'aide d'un raisonnement logique fondé sur un ensemble d'observations du système et d'un modèle de son comportement. Les fautes sont anticipées par un raisonnement de pronostic à partir d'une connaissance sur la dégradation. Le plus souvent, on s'accorde à dire que le pronostic est une prédiction de l'état de santé du système dans le futur. Plus précisément, on associe le pronostic à la prédiction de la durée de vie résiduelle (*remaining useful life* ou *RUL*) d'un système en service, durée pendant laquelle il reste opérationnel. Ces informations sur l'état de santé courant et futur du système servent alors à mettre à jour les plans de mission et de maintenance, d'où l'importance de la qualité du diagnostic et du pronostic.

Dans cet article, nous utiliserons le terme *hybride* pour caractériser un système ayant une dynamique à la fois discrète et continue. Un système hybride a une dynamique discrète qui provient des changements de comportement du système. Ces changements sont dus à la dynamique continue du système ou à des événements discrets internes ou externes au système.

Ce travail a pour objectif de développer une approche basée sur un modèle permettant d'intégrer des méthodes de diagnostic et de pronostic pour les systèmes hybrides sous incertitudes, dans le but de pouvoir orienter les résultats en cas d'ambiguïté. Pour cela, une architecture de supervision de santé est proposée (figure 1). Elle contient un module de surveillance

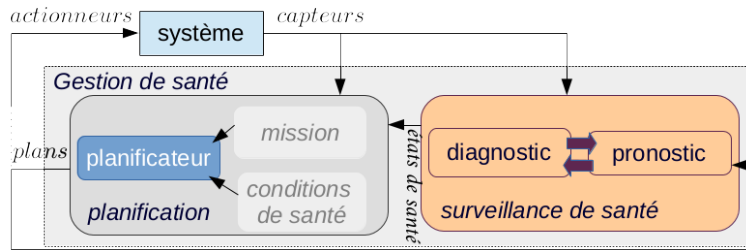


Figure 1: Architecture de supervision de santé de système intégrant diagnostic et pronostic.

de santé déterminant l'état de santé à tout instant du système, et un module de planification permettant une réorganisation du système (reconfiguration/replanification de mission). En plus des données des capteurs, les sorties de chacun des deux modules de planification et de surveillance de santé sont des entrées de l'autre. L'originalité de l'approche réside dans la transmission de données du pronostic vers le diagnostic qui permet d'obtenir des résultats de surveillance de santé plus précis. Néanmoins cet aspect n'est pas l'objet de cet article.

Cet article est organisé comme suit. La section 2 expose un état de l'art des architectures utilisées pour la supervision des systèmes complexes, et présente les formalismes utilisés pour la surveillance des systèmes à base de modèles. Dans la section 3, une méthode est proposée pour effectuer le diagnostic de comportement de systèmes hybrides sous incertitudes. La méthode introduit le formalisme des *réseaux de Petri hybrides particulières (HPPN)* qui intègre un filtrage particulière pour surveiller l'état hybride du système. La section 4 explique comment le modèle des HPPN permet de suivre l'évolution de la dégradation du système basée sur l'état hybride du système. Des résultats de simulation sont donnés et expliqués dans la section 5. La dernière section conclut les travaux et fait le point sur les travaux futurs.

2 État de l'art

La première partie de cet état de l'art vise à étudier les architectures de supervision existantes de façon à définir une architecture qui interface de manière cohérente les modules de planification et de surveillance de santé. La deuxième partie s'attache à étudier les différents formalismes de surveillance de santé pour définir un formalisme permettant de modéliser le comportement du système et sa dégradation pour effectuer du diagnostic et du pronostic.

2.1 Architectures de supervision de système

Une architecture représente la décomposition structurelle d'une tâche à effectuer. Dans la plupart des travaux passés, cette décomposition est propre à l'application. Ces architectures corre-

spondent à la conception d'un système dont l'objectif est la réalisation d'une mission. L'intérêt de l'intégration d'un module de surveillance de santé (principalement diagnostic) apparaît après les premières utilisations du système (problématiques de maintenance et de sécurité). Ce n'est qu'il y a quelques années que des travaux proposent des architectures de système génériques, notamment dans le cadre de la gestion de santé (*Prognostic and Health Management* ou *PHM*). Ces architectures intègrent dès la phase de conception les fonctions de diagnostic et pronostic.

Les architectures décomposées en niveaux hiérarchiques sont très fréquentes. Un certain nombre d'entre elles sont définies sur trois niveaux hiérarchiques. Ainsi [1] propose un module de fonctionnalité de haut niveau (planification), un module de fonctionnalité de bas niveau (contrôle) et un niveau de diagnostic de faute. La planification reste le cœur du système.

L'architecture *FDIR* (*fault detection, isolation and recovery*) est très utilisée dans le domaine spatial. Elle repose sur quatre niveaux hiérarchiques représentatifs des niveaux de criticité progressifs. Les trois premiers niveaux de criticité sont gérés par le système de manière autonome. Au dernier niveau, le système laisse les opérateurs humains traiter la situation. Bien que la stratégie *FDIR* soit rapide et efficace en terme d'isolation de faute, la volonté des auteurs de [11] est de repousser la limite du dernier niveau pour rendre le système plus autonome. L'architecture proposée vise la généralité pour permettre la distribution de méthodes *FDIR* sur les composants et répondre aux contraintes d'embarquabilité. Cependant, aucune méthode de pronostic ou autre méthode de prédiction n'est envisagée.

Certains auteurs proposent des architectures intégrant le diagnostic et le pronostic pour la surveillance de santé de systèmes continus. Dans [18], la surveillance de santé d'un système exposé à des fautes multiples est considérée. L'approche est intéressante car les auteurs considèrent que la présence d'une faute a une conséquence sur les prochaines occurrences des fautes. L'algorithme de pronostic n'est déclenché que lorsque le système est dans un état dégradé. Le diagnostic ne peut donc pas utiliser les résultats du pronostic. Dans [12], la surveillance de santé considère la progression des fautes des paramètres par rapport à un modèle nominal. Le pronostic se base sur le diagnostic pour produire une distribution de RUL mais les travaux ne considèrent aucun retour du pronostic vers le diagnostic.

Dans [2] et [16], une architecture de surveillance de santé de systèmes hybrides est présentée. Les méthodes de diagnostic et de pronostic sont intégrées dans un processus unique. Les résultats du pronostic sont utilisés pour lever les ambiguïtés des résultats du diagnostic. L'intégration d'un module de planification n'est cependant pas proposée.

Une architecture pour la prise de décision d'un rover autonome, utilisant les résultats de diagnostic et de pronostic pour influencer la planification de la mission est présentée dans [10]. Un module de décision est intégré à l'architecture pour maximiser les objectifs de la mission. L'architecture est décomposée en quatre modules : contrôle de bas niveau, diagnostic, pronostic et prise de décision. L'utilisation des résultats de pronostic pour la détermination du diagnostic du système n'est pas envisagée mais le pronostic utilise la connaissance sur le plan de mission du système.

À notre connaissance, il n'existe pas aujourd'hui d'architecture de supervision de santé intégrant un module de planification et de surveillance de santé, avec un retour du pronostic vers le diagnostic. C'est pour cela que nous avons proposé une nouvelle architecture de supervision de santé (voir figure 1).

2.2 Formalismes pour la surveillance de système

Le *diagnostiqueur* a été introduit pour la surveillance des systèmes [13]. C'est un moniteur qui traite les observations et en déduit l'ensemble des fautes possibles cohérent avec ces observa-

tions et le modèle de comportement. Cette approche est restreinte aux Systèmes à Événements Discrets (SED) et ne gère pas les incertitudes liées à la connaissance sur le système ou aux observations. Les réseaux de Petri (RdP) sont souvent plus appropriés pour des travaux de modélisation [5] car ils ont une représentation plus compacte et plus intuitive que les automates. Certains travaux, comme [6][14], étendent ainsi l’approche diagnostique aux SED modélisés par des RdP. Cependant, aucune de ces approches ne considère les aspects continus ou même les incertitudes sur la connaissance et les observations du système. [14] propose une approche pour la localisation de fautes intermittentes à partir d’observations partielles. D’autres travaux s’intéressent aux incertitudes sur les observations. [15] utilise les réseaux de Petri partiellement observés. Ces réseaux sont transformés en des réseaux de Petri labellisés et un moniteur est construit pour diagnostiquer les fautes et délivrer une croyance sur leurs occurrences. Cette approche ne considère qu’une incertitude au niveau du résultat du diagnostic mais pas celles liées au modèle ou aux observations des événements. [8] utilise les RdP stochastiques pour construire un modèle de chaque composant d’une architecture modulaire avionique intégrée. Dans toutes ces approches, aucun aspect continu n’est considéré dans le modèle du système. Le formalisme des RdP particuliers modifiés (*Modified Particle Petri Nets* ou *MPPN*) est proposé dans [19] pour traiter toutes les incertitudes relatives au système et aux observations continues et discrètes. Les MPPN sont une extension des RdP particuliers, introduits dans [9], qui combinent un modèle à événements discrets (réseau de Petri) et un modèle continu (équations dynamiques). L’avantage principal des MPPN est qu’ils considèrent la dynamique hybride du système sous incertitudes. Un filtrage particulier est utilisé pour intégrer les probabilités dans le processus d’estimation de l’état continu. Dans [19], l’application est orientée vers la surveillance de mission. Les états de santé du système ne sont pas considérés. De plus, il n’y a pas de correspondance avec l’objet diagnostique défini dans la littérature. Dans [20], les auteurs proposent d’intégrer la conception du système et sa surveillance en un formalisme unifié générique pour la génération automatique de moniteur de composant. Cependant, l’observateur généré n’est pas formellement défini et toujours pas comparé à un diagnostiqueur ni appliqué dans un contexte de gestion de santé.

Plusieurs méthodes de modélisation ont été développées pour effectuer de la surveillance de systèmes hybrides. Des modèles, initialement continus, ont été étendus par l’intégration d’aspects événementiels [3]. Les RdP hybrides [17] étendent des modèles à événements discrets en intégrant des aspects continus. Les automates hybrides [7] ou les RdP particuliers [9] combinent de manière explicite un modèle à événements discrets et un modèle continu. L’avantage de ces modèles est qu’ils offrent une modélisation naturelle de la partie continue et de la partie discrète, propice à l’intégration du calcul de pronostic. [2] propose une surveillance de santé intégrant des méthodes de diagnostic et de pronostic. Un modèle basé sur les automates hybrides représente le comportement des systèmes hybrides ainsi que leur dégradation. Dans la suite des travaux [16], les résultats du pronostic sont utilisés pour lever les ambiguïtés des résultats du diagnostic.

L’incertitude du diagnostic de systèmes hybrides est parfois étudié mais peu de travaux concernent le couplage du diagnostic et du pronostic pour les systèmes hybrides. De plus, le pronostic de systèmes hybrides seul est rarement abordé car la connaissance des résultats de diagnostic est généralement considérée comme une initialisation pour le calcul du pronostic.

3 Diagnostic de comportement

Dans cette section, une méthode est proposée pour effectuer le diagnostic de comportement de systèmes hybrides sous incertitudes. La méthode introduit le formalisme des *réseaux de*

Petri hybrides particulières (HPPN) qui intègre un filtrage particulière pour estimer l'état de santé hybride du système. L'avantage principal de la méthode est que les incertitudes sur la connaissance du système ainsi que sur les observations, qui peuvent être fausses, manquantes ou imprécises, sont prises en compte dans le suivi de l'état du système.

Les HPPN sont composés de deux niveaux. Le *niveau de comportement* est basé sur le formalisme des réseaux de Petri particulières modifiés [19]. Plus de détails sur le formalisme pourront être trouvés dans [5]. Il permet de suivre l'état continu et l'état discret du système hybride. Le *niveau hybride* des HPPN permet quant à lui de suivre l'évolution de la dégradation du système qui dépend à la fois de l'état continu et de l'état discret du système.

3.1 Modélisation du comportement du système hybride : gestion des incertitudes

Le niveau de comportement d'un HPPN est un n-uplet $\langle P, T, Pre, Post, X, C, \gamma, \Omega, M_0 \rangle$ pour lequel : P est l'ensemble des places, composé de places numériques P^N et de places symboliques P^S ; T est l'ensemble des transitions (numériques T^N , symboliques T^S et mixtes T^M); Pre et $Post$ sont les matrices d'incidence du réseau, de dimension $|P| \times |T|$; $X \subset \mathbb{R}^n$ est l'espace d'état du vecteur d'état numérique; C est l'ensemble des équations dynamiques du système associées aux places numériques, qui représentent l'évolution de l'état continu; $\gamma(p^S)$ est la fonction qui associe les jetons à chaque place symbolique $p^S \in P^S$; Ω est l'ensemble des conditions associées aux transitions (numériques Ω^N et symboliques Ω^S); M_0 est le marquage initial du réseau.

Les places numériques P^N modélisent les différentes dynamiques continues du système. Elles sont marquées par un ensemble de particules $\pi_k^i = [x_k^i, w_k^i]$ avec $i \in \{1, \dots, |M_k^N|\}$ où M_k^N est l'ensemble de toutes les particules du réseau au temps k . Une particule est définie par son vecteur d'état numérique $x_k^i \in X$ et son poids $w_k^i \in [0, 1]$ au temps k . L'ensemble des particules représentent une distribution d'imprécision sur la valeur du vecteur d'état numérique du système à un instant donné.

Les places symboliques P^S modélisent les états discrets du système. Elles sont marquées par un ensemble de configurations δ_k^j avec $j \in \{1, \dots, |M_k^S|\}$ où M_k^S est l'ensemble des configurations du réseau au temps k . L'ensemble des configurations représentent tous les états possibles du système à un instant donné.

Le marquage M_k du niveau de comportement du HPPN au temps k est constitué de l'ensemble des jetons des deux types numériques (particules) et symboliques (configurations) : $M_k = \{M_k^S, M_k^N\}$.

Les places numériques représentent les différentes dynamiques continues du système, et les places symboliques représentent les différents états discrets du système. Les conditions symboliques sont utilisées pour modéliser l'occurrence d'un événement discret, qu'il soit observable ou non observable (faute, événement de mission, interaction avec l'environnement, ...). Les conditions numériques modélisent un changement de dynamique continue observable. Les dynamiques continues du système sont représentées par des équations différentielles.

Un *mode de santé* (ou état) q_m du système est un état hybride (p_i^S, p_j^N) :

$$q_m = (p_i^S, p_j^N) \in Q \text{ if } \exists t_l \in T, (p_i^S, p_j^N) \in (Post(t_l))^2. \quad (1)$$

Tant qu'aucun événement de faute ne survient, le système est dans un *mode nominal*. Les fautes suivies sont considérées permanentes, c'est à dire que sans action de réparation, l'évolution du système mène à un *mode de défaillance* dans lequel le système n'est plus opérationnel.

Les règles de tirage des transitions du HPPN sont les suivantes. Une transition modélise un changement de dynamique continue et/ou une occurrence d'un événement observable ou

non observable. Une transition symbolique est conditionnée par un événement discret. Une transition numérique est conditionnée par un ensemble de contraintes sur les variables du vecteur d'état numérique. Une transitions mixte modélise une interaction entre la dynamique discrète et la dynamique continue du système. Elle est donc conditionnée par l'observation d'un événement discret et par un ensemble de contraintes sur les variables du vecteur d'état numérique.

Une transition numérique ou symbolique t_j est franchissable si le nombre de jetons dans une place en entrée de t_j est supérieur ou égal au nombre imposé par la matrice Pre . Une transition mixte t_j est franchissable si le nombre de configurations dans une place symbolique en entrée de t_j est supérieur ou égal au nombre imposé par la matrice Pre .

Lors du tirage d'une transition numérique $t_j \in T^N$, les particules qui satisfont les conditions numériques franchissent t_j et les configurations sont dupliquées dans la place symbolique en sortie, c'est ce qu'on appelle le pseudo-tirage. La duplication des configurations au temps k modélise une incertitude sur l'occurrence d'un événement non observable au temps k qui est supporté par une condition sur les variables continues (un événement de faute par exemple).

Lors du tirage d'une transition symbolique $t_j \in T^S$, les particules et les configurations sont dupliquées dans les places symboliques et numériques en sortie. Ce pseudo-tirage de tous les jetons au temps k modélise une incertitude sur l'occurrence d'un événement au temps $k+1$ (un événement observable non observé à cause d'une erreur de modélisation ou de capteur ou une incertitude sur un événement de faute par exemple).

Le tirage d'une transition mixte $t_j \in T^M$ utilise le concept de tirage traditionnel pour les particules qui satisfont les conditions numériques et le concept de pseudo-tirage pour les configurations qui satisfont les conditions symboliques. Le pseudo-tirage des configurations au temps k modélise une incertitude sur l'occurrence d'un événement observable supporté par un changement de dynamique continue au temps k et observé par erreur (une erreur de modélisation ou de capteur par exemple).

3.2 Suivi de l'état de santé du système hybride

3.2.1 Génération du diagnostiqueur

La méthode de diagnostic doit estimer l'état de santé courant du système. Une méthode connue dans le cadre des SED est la génération d'un diagnostiqueur du système à partir de son modèle [13]. Un diagnostiqueur est un moniteur capable de traiter toutes les observations du système et de déduire l'ensemble des fautes possibles dont les occurrences sont cohérentes avec les observations. L'inconvénient de cette approche est que le diagnostic basé SED n'est pas bien adapté pour le pronostic qui utilise la plupart du temps des outils probabilistes. Le niveau de comportement des HPPN permet de tenir compte de l'incertitude sur la connaissance du système, mais aussi sur ses observations. Un diagnostiqueur basé sur le niveau de comportement des HPPN a donc été proposé dans [5] pour estimer l'état de santé du système. Ce diagnostiqueur est lui-même un HPPN défini par un n-uplet $\langle P, T, Pre, Post, X, C, \gamma, \Omega, M_0 \rangle$. Il est généré à partir de différentes manipulations des transitions du modèle HPPN de comportement. Le résultat du diagnostic est donné à chaque impulsion d'horloge par l'état du diagnostiqueur.

3.2.2 Estimation de l'état du diagnostiqueur

L'estimation d'état dans les HPPN est basé sur un filtrage particulière : une étape de prédiction et une étape de correction sont réalisées sur les jetons du niveau de comportement. Le marquage initial du niveau de comportement est $M_0 = \{M_0^S, M_0^N\}$ et le marquage estimé au temps

k est $\hat{M}_k = \{\hat{M}_k^S, \hat{M}_k^N\}$ où $\hat{M}_k = \hat{M}_{k|k}$. Les observations commencent au temps $k = 1$, $O_1 = (O_1^S, O_1^N)$ où O^S et O^N représentent respectivement les observations discrètes et continues.

L'étape de *prédiction* se base sur l'évolution du marquage et sur l'estimation des valeurs des particules. Elle vise à déterminer tous les prochains états possibles du système $\hat{M}_{k+1|k} = \{\hat{M}_{k+1|k}^S, \hat{M}_{k+1|k}^N\}$. Un bruit est ajouté lors de la mise à jour des valeurs des particules pour prendre en compte les incertitudes sur la partie continue du système.

L'étape de *correction* se base sur une mise à jour de la prédiction en accord avec les nouvelles observations du système : une correction numérique, basée sur l'étape de correction du filtrage particulaire, produit une distribution de probabilité Pr_{DN} des particules $\hat{M}_{k+1|k+1}^N$ sur la valeur du vecteur d'état numérique. Durant cette étape, la mise à jour des poids des particules utilise une fonction de distribution de probabilité qui dépend d'un bruit aléatoire modélisant une incertitude sur les observations continues O_{k+1}^N . Une correction symbolique, produit une distribution de probabilité Pr_{DS} sur les états hybrides du système, en fonction des observations discrètes O_{k+1}^S et Pr_{DN} , rendant le processus hybride. Pour mettre à jour le marquage symbolique prédit $\hat{M}_{k+1|k}^N$ en $\hat{M}_{k+1|k+1}^N$, un algorithme de prise de décision est requis.

Les bruits ajoutés lors des étapes de prédiction et correction du processus d'estimation d'état représentent respectivement des incertitudes liées aux équations dynamiques du système et aux observations continues. Le résultat du processus d'estimation d'état est le marquage estimé au temps $k + 1$, $\hat{M}_{k+1|k+1} = \{\hat{M}_{k+1|k+1}^S, \hat{M}_{k+1|k+1}^N\}$.

3.2.3 Résultat du diagnostic de comportement

En utilisant le niveau de comportement (section 3.1) et le processus d'estimation d'état (section 3.2.2), le diagnostic Δ_k au temps k est la distribution de croyance des états de santé qui dépend des particules et des configurations incluses dans le marquage du diagnostiqueur au temps k :

$$\Delta_k = \hat{M}_k = \{\hat{M}_k^S, \hat{M}_k^N\}. \quad (2)$$

Le marquage \hat{M}_k porte donc la croyance sur les occurrences des fautes. Il apporte la même information qu'un diagnostiqueur de modes traditionnel en termes d'occurrences de fautes, avec la même ambiguïté. La différence majeure est que dans un diagnostiqueur traditionnel, tous les diagnostics possibles ont le même degré de croyance. Avec un diagnostiqueur basé sur les HPPN, l'ambiguïté est quantifiée par les caractéristiques des particules et des configurations.

4 Diagnostic de dégradation

Cette section introduit le second niveau des HPPN appelé *niveau hybride* [4]. Ce niveau a été défini pour pouvoir représenter et faire évoluer des caractéristiques qui ne dépendent pas seulement de la dynamique continue ou de l'état discret mais des deux. Un ensemble d'équations dynamiques est utilisé pour modéliser l'évolution des caractéristiques hybrides à suivre. Dans un contexte de gestion de santé, ces travaux s'intéressent particulièrement aux lois de dégradation du système, dépendantes du mode de santé courant. La mise à jour des valeurs de dégradation à chaque impulsion d'horloge est réalisée par la fonction de diagnostic de dégradation.

4.1 Modélisation de la dégradation d'un système

Le niveau hybride des HPPN est défini par le n-uplet $\langle P^H, T^H, H, \mathcal{F}, \Omega^H \rangle$ dans lequel : P^H est l'ensemble des places hybrides; T^H est l'ensemble des transitions hybrides; $H \subset \mathfrak{R}^n$

est l'espace d'état du vecteur d'état hybride; \mathcal{F} est l'ensemble des équations dynamiques du système associées aux places hybrides, et qui représentent les évolutions des caractéristiques hybrides; Ω^H est l'ensemble des conditions associées aux transitions hybrides.

Un RdP hybride particulière complet, composé du niveau de comportement et du niveau hybride, est donc défini par le n-uplet $\langle P, T, Pre, Post, X, C, H, \mathcal{F}, \gamma, \Omega, M_0 \rangle$.

Les places hybrides représentent tous les états hybrides possibles du système, c'est-à-dire les modes de santé définis précédemment. Seuls les couples appartenant à l'ensemble des sorties d'une même transition sont considérés comme des états hybrides :

$$p_l^H = (p_i^S, p_j^N) \in P^H \text{ if } \exists t_m \in T, (p_i^S, p_j^N) \in (Post(t_m))^2. \quad (3)$$

Les couples qui ne satisfont pas la condition 3 sont considérés comme des *états intermédiaires*.

Une place hybride est marquée par des jetons hybrides $h_k^i = [s_k^i, d_k^i]$ avec $i \in \{1, \dots, |M_k^H|\}$ où M_k^H est l'ensemble de tous les jetons hybrides dans le réseau au temps k . Un jeton hybride est défini par un couple $s_k^i = (d_k^j, \pi_k^l)$ de jetons circulant dans le niveau de comportement et par son vecteur d'état $d_k^i \in H$. Puisque que les jetons hybrides sont dépendants des configurations et des particules, ils sont créés dès la création d'une configuration ou d'une particule. Le marquage complet d'un HPPN est $M_k = \{M_k^S, M_k^N, M_k^H\}$.

Le niveau hybride des HPPN permet d'introduire des lois de dégradation dans le modèle. Elles dépendent des niveaux de stress des modes de santé représentés par les places hybrides. Les lois de dégradation sont considérées connues : $\mathcal{F} = \{F^{p_i^H}, p_i^H \in P^H\}$ est l'ensemble des lois de dégradation associées aux places hybrides du HPPN. $F^{p_i^H}$ est le vecteur des lois de dégradation des fautes anticipées de la place $p_i^H = (p_i^S, p_j^N)$. Par exemple, dans un système où n_f fautes sont considérées : $F^{p_i^H}(t) = [f_1^{p_i^H}(t) \ f_2^{p_i^H}(t) \ \dots \ f_{n_f}^{p_i^H}(t)]^T$ où $f_j^{p_i^H}$ représente la distribution de probabilité de la faute f_j à tout instant dans la place p_i^H .

4.2 Suivi de l'état de dégradation du système hybride

Cette section complète la section 3.2 avec le niveau hybride pour construire le diagnostiqueur utilisant le formalisme complet des HPPN. Ce diagnostiqueur permet de suivre en parallèle le comportement et la dégradation du système hybride sous incertitudes.

Le processus d'estimation en ligne du niveau de comportement hybride dépend entièrement du processus d'estimation d'état du niveau de comportement et les deux s'effectuent simultanément.

Les valeurs des jetons hybrides évoluent en accord avec les lois de dégradation associées aux places hybrides. En effet, puisque les jetons du niveau de comportement changent de places durant l'étape de prédiction, les jetons hybrides changent simultanément de places hybrides et leurs valeurs sont mises à jour comme suit :

$$\forall h_{k+1|k}^i \in \hat{M}_{k+1|k}^H(p_j^H), \quad d_{k+1}^i = F_{k+1}^j(d_k^i) \quad (4)$$

où $F_k^j \in \mathcal{F}$ est l'ensemble des équations dynamiques associé à la place hybride p_j^H . Puisque d_{k+1}^i dépend de d_k^i , la continuité de la valeur d^i peut être assurée.

Les règles de tirage des transitions hybrides sont maintenant détaillées. Chaque place hybride est liée avec toutes les autres places hybrides par une transition hybride $t_j^H \in T^H$. $\forall p_i \in P$, $M_k(p_i)$ est l'ensemble des jetons dans p_i au temps k et $m_k(p_i) = |M_k(p_i)|$ est le nombre de jetons dans p_i au temps k . Une transition hybride $t_j^H \in T^H$ est franchissable au temps k si le nombre de jetons hybrides dans une place à l'entrée de t_j^H est supérieure ou égale au nombre imposé par la matrice d'incidence.

On introduit les notations suivantes : $P(\delta^j) = p_j^S$ et $P(\pi^l) = p_l^N$ désignent les projections de δ^j et π^l sur l'espace des places P . et $P(s^i) = (p_j^S, p_l^N)$ désigne la place hybride d'un couple $s^i = (\delta^j, \pi^l)$. Chaque transition hybride est associée aux conditions hybrides $\Omega^H(t_j^H)$ qui sont satisfaites si $\Omega^H(t_j^H)(h^i) = 1$. Un jeton hybride est déplacé dans la place hybride p'^H si $P(s^i) = p'^H$:

$$\forall h^i = [s^i, d^i], \quad \Omega^H(t_j^H)(h^i) = \begin{cases} 1 & \text{si } P(s^i) = p'^H \\ 0 & \text{sinon} \end{cases} \quad (5)$$

$\mathcal{S}_k^H(p^H)$ est l'ensemble des jetons hybrides dans p^H qui satisfont les conditions hybrides $\Omega^H(t_j^H)$ au temps k . L'équation 5 implique que chaque transition hybride t_j^H a une seule place hybride p'^H en sortie et toute autre place hybride p^H en sortie. Le tirage d'une transition hybride franchissable $t_j^H \in T^H$ au temps k est défini par :

$$\begin{cases} M_{k+1}^H(p^H) = M_k^H(p^H) \setminus \mathcal{S}_k^H(p^H) \\ M_{k+1}^H(p'^H) = M_k^H(p'^H) \cup \mathcal{S}_k^H(p^H) \end{cases} \quad (6)$$

Un exemple de tirage d'une transition hybride dans le niveau hybride est présenté dans la figure 2. Dans cet exemple, il y a deux places hybrides $p_1^H = (p_1^S, p_1^N)$ et $p_2^H = (p_2^S, p_2^N)$. Au temps k , les deux jetons hybrides $h_k^1 = [s_k^1, d_k^1]$ et $h_k^2 = [s_k^2, d_k^2]$ suivent les caractéristiques de l'état hybride représenté par p_1^H , donc la transition t_2^H est franchissable. $P(s_k^1)$ vaut (p_1^S, p_1^N) mais $P(s_k^2)$ vaut (p_2^S, p_2^N) donc $\Omega^H(t_2^H)(h^2)$ est satisfaite et h^2 est déplacé dans p_2^H . Ainsi donc, h^2 est dans la place hybride p_2^H au temps $k+1$ et suit les caractéristiques de l'état hybride (p_2^S, p_2^N) .

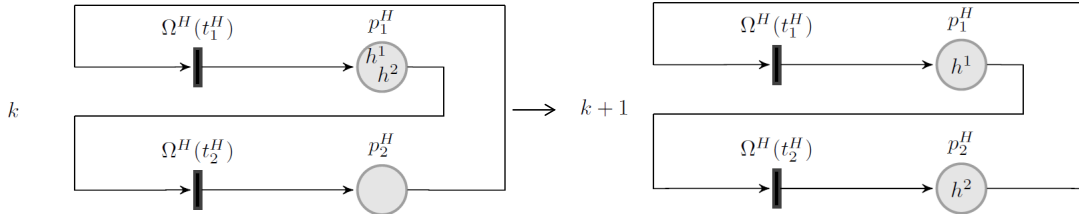


Figure 2: Illustration de la règle de tirage d'une transition hybride.

En utilisant le niveau hybride des HPPN, le diagnostic Δ_k du système au temps k est le marquage complet du diagnostiqueur :

$$\Delta_k = \hat{M}_k = \{\hat{M}_k^S, \hat{M}_k^N, \hat{M}_k^H\}. \quad (7)$$

La valeur du marquage $\{\hat{M}_k^S, \hat{M}_k^N\}$ représente la croyance sur les modes de santé à travers une distribution de probabilité. La valeur du marquage \hat{M}_k^H représente la croyance sur l'état de dégradation à travers une distribution de dégradation sur les modes de santé du système.

5 Étude de cas par simulation

Des scénarios de simulation sur un système à trois réservoirs (figure 3) sont présentés dans cette section et leurs résultats sont expliqués.

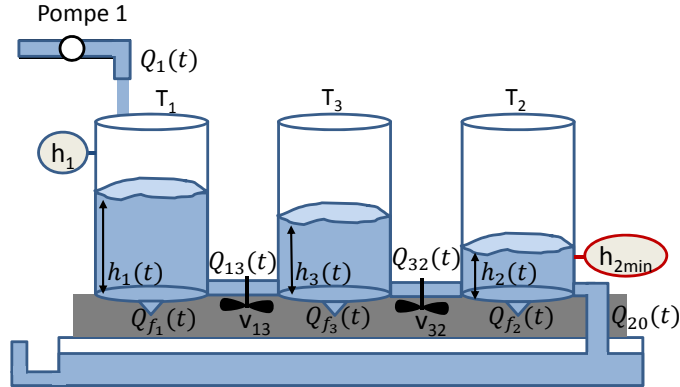


Figure 3: Système des trois réservoirs.

5.1 Description du système des trois réservoirs

Le flux $Q_1(t)$ délivré par la pompe est supposé constant. Le réservoir T_2 se vide avec le flux $Q_{20}(t)$. Les observations sur le système sont le niveau d'eau $h_1(t)$ dans le réservoir T_1 et la masse totale $W(t)$ de l'eau dans les trois réservoirs. Les vannes v_{13} et v_{32} permettent le transfert de l'eau entre les réservoirs connectés en série. Elles sont contrôlées par les actionneurs discrets observables $open_{v_{13}}$, $close_{v_{13}}$, $open_{v_{32}}$ et $close_{v_{32}}$. Les événements de faute f_1 , f_2 et f_3 sont non observables et représentent des fuites qui peuvent apparaître dans les réservoirs T_1 , T_2 et T_3 . f_4 et f_5 sont des événements de faute qui peuvent se produire sur les vannes. La vanne v_{13} (respectivement v_{32}) peut se bloquer en position fermée f_4 (respectivement f_5). L'objectif du système est de maintenir le niveau d'eau $h_2(t)$ dans le réservoir T_2 au dessus de la valeur minimum h_{2min} fixée. On suppose que le système est défaillant si f_1 ou f_4 ou f_5 se produit, ou bien si f_2 et f_3 se produisent.

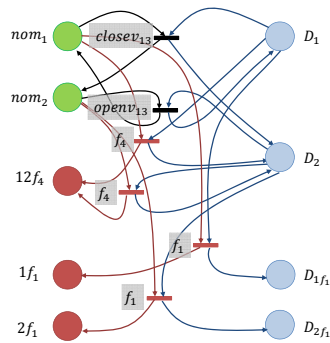


Figure 4: Modèle partiel de comportement du système des trois réservoirs utilisant les HPPN.

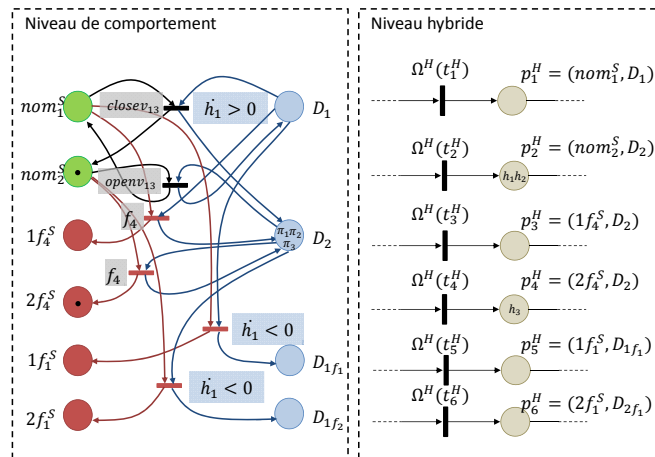


Figure 5: Diagnostiqueur partiel du système des trois réservoirs utilisant les HPPN.

Pour cet exemple, 40 modes de santé ont été identifiés. Par souci de lisibilité, la figure 4 ne présente que 5 modes de santé du modèle de comportement du système et les notations sont simplifiées. Quatre dynamiques continues sont représentées par les places numériques D_1 , D_2 , D_{1f_1} et D_{2f_1} et cinq états discrets par les places symboliques nom_1 , nom_2 , $12f_4$, $1f_1$ et $2f_1$. Dans certains cas, deux états discrets (ou plus) ont la même dynamique, il n'est alors pas nécessaire de définir un comportement continu différent pour chacun de ces états discrets. Chaque dynamique continue identifiée est représentée par une place numérique. Par exemple, la place numérique D_1 est définie par la dynamique suivante :

$$\begin{cases} \dot{h}_1(t) &= \frac{1}{S_1}(Q_1(t) - K_{13}\sqrt{|h_1(t) - h_3(t)|}) \\ \dot{h}_2(t) &= \frac{1}{S_2}(K_{32}\sqrt{|h_3(t) - h_2(t)|} - Q_{20}(t)) \\ \dot{h}_3(t) &= \frac{1}{S_3}(K_{13}\sqrt{|h_1(t) - h_3(t)|} - K_{32}\sqrt{|h_3(t) - h_2(t)|}) \end{cases} \quad (8)$$

avec S_1, S_2, S_3 les sections des réservoirs et K_{ij} les coefficients de gain. Cette dynamique est suivie lorsque les deux vannes v_{13} et v_{32} sont ouvertes.

Les modes de santé $q_1 = (nom_1, D_1)$ et $q_2 = (nom_2, D_2)$ sont des modes nominaux. Le système passe de q_1 à q_2 (et inversement) lorsque la condition $occ(close_{v_{13}})$ ou $occ(open_{v_{13}})$ est satisfaite. Trois modes de défaillance $q_3 = (12f_4, D_2)$, $q_4 = (1f_1, D_{1f_1})$ et $q_5 = (2f_1, D_{2f_1})$ sont atteignables depuis les modes nominaux q_1 et q_2 par satisfaction des conditions $occ(f_1)$ ou $occ(f_4)$ (simplifiées en f_1 et f_4 pour des raisons de clarté dans la figure).

La partie droite de la figure 5 représente le niveau hybride du modèle partiel du système. Ce modèle partiel représente cinq modes de santé et donc le niveau hybride possède cinq places hybrides $p_1^H = (nom_1, D_1)$, $p_2^H = (nom_2, D_2)$, $p_3^H = (12f_4, D_2)$, $p_4^H = (1f_1, D_{1f_1})$ et $p_5^H = (2f_1, D_{2f_1})$. Cinq transitions hybrides $t_1^H \dots t_5^H$ permettent les accès aux cinq places hybrides lorsque leurs conditions hybrides sont satisfaites. Les distributions de probabilité de fautes F^j associées à chaque place hybride p_i^H sont représentées par un modèle de Weibull à deux paramètres : $f_j^{p_i^H}(t) = W(t, \beta_j, \eta_j)$. En fixant $\beta = 1$, le modèle de Weibull décrit des défaillances aléatoires et est similaire à une loi exponentielle. Le second paramètre η est une fonction qui dépend du niveau de stress du système dans chaque mode de santé associé à une place hybride p_i^H . Les distributions de probabilité des fautes de fuite f_1, f_2 et f_3 sont définies avec trois valeurs différentes pour le paramètre η représentant trois niveaux de stress différents définis par les modes de santé du système. Par exemple, pour la place hybride $p_2^H = (nom_2, D_2)$ correspondant au mode de santé dans lequel la vanne v_{13} est fermée et v_{32} est ouverte, les distributions de probabilité des fautes associées sont

$$F^{p_2^H} : [f_1^{p_2^H}(t) \quad f_2^{p_2^H}(t) \quad f_3^{p_2^H}(t)]^T = [W(t, 60000) \quad W(t, 100000) \quad W(t, 100000)]^T \quad (9)$$

Les distributions de probabilité des fautes f_4 et f_5 sur les vannes évoluent avec le nombre d'ouvertures et fermetures de celles-ci. η_{13} pour la vanne v_{13} (respectivement η_{32} pour la vanne v_{32}) dépend du coefficient de cyclage α_{13} (respectivement α_{32}) qui évolue après chaque occurrence des événements discrets $open_{v_{13}}$ ou $close_{v_{13}}$ (respectivement $open_{v_{32}}$ ou $close_{v_{32}}$):

$$f_4^{p_i^H}(t) = W(t, \eta_{13}(\alpha_{13})), \quad f_5^{p_i^H}(t) = W(t, \eta_{32}(\alpha_{32})). \quad (10)$$

À l'état initial, dans le mode de santé (nom_1, D_1) , $\alpha_{13} = \alpha_{32} = 1$ et $\eta_{13} = \eta_{32} = 20000$.

5.2 Génération du diagnostiqueur basé sur les HPPN

La génération du diagnostiqueur basé sur les HPPN a été implémentée dans le langage Python. Le modèle du système des trois réservoirs possède 40 places symboliques, 28 places numériques

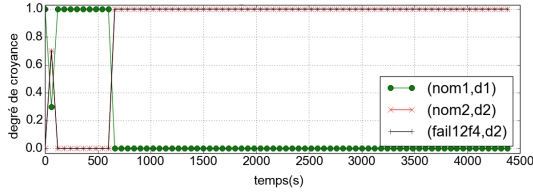


Figure 6: Scénario 1 : degrés de croyance des modes de santé.

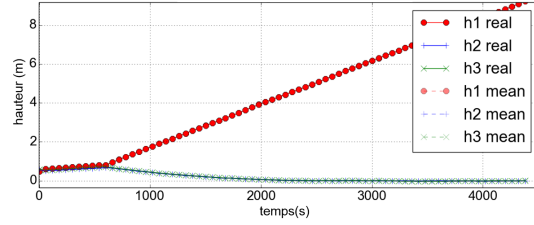


Figure 7: Scénario 1 : surveillance des niveaux d'eau.

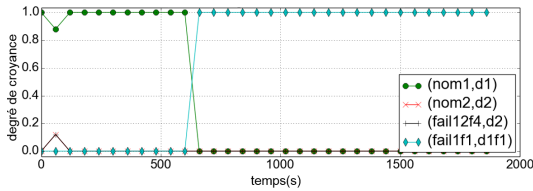


Figure 8: Scénario 2 : degrés de croyance des modes de santé.

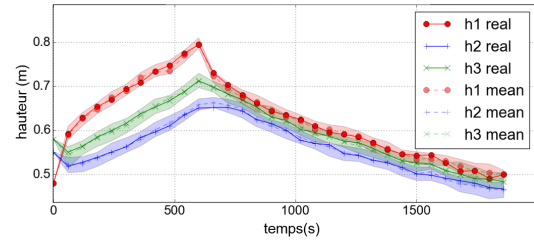


Figure 9: Scénario 2 : surveillance des niveaux d'eau.

et 120 transitions. Un bruit gaussien centré sur 0 et avec un écart type de $0.01m$ a été ajouté à chaque équation d'état. L'imprécision de la mesure de h_1 est modélisée par un bruit gaussien centré sur 0 et un écart type de $0.01m$. L'imprécision de la mesure de la masse totale d'eau est modélisée par un bruit gaussien centré sur 0 et un écart type de $0.1kg$. L'état initial est $[H_{10}, H_{20}, H_{30}] = [0.48, 0.55, 0.58]$ et les vannes v_{13} et v_{32} sont ouvertes. La période d'échantillonnage de la simulation est $60s$. Cette valeur reste correcte vis à vis de la constante de temps du système. Le diagnostiqueur généré à partir du modèle HPPN ne possède plus que 40 transitions, ce qui représente une réduction du nombre de transitions de 66%.

5.3 Résultats de simulation

Le scénario 1 illustre l'incertitude sur l'occurrence d'un événement non observable (événement de faute). A 720s, la vanne v_{13} est fermée et l'événement $closev_{13}$ se produit. À 1980s, f_4 se produit. À 3240s, v_{13} est ouverte et l'événement $openv_{13}$ se produit. Au début, la simulation (figure 6) montre une incertitude sur la croyance du mode préféré à cause de la similarité entre les dynamiques continues D_1 et D_2 . Ensuite, jusqu'à 720s, le degré de croyance du mode de santé (nom_1, D_1) domine largement les autres. Après avoir fermé v_{13} , le diagnostic prend en compte l'incertitude sur l'occurrence de la faute et les degrés de croyance de (nom_2, D_2) et ($12f_4, D_2$) dominant car ils ont la même dynamique continue. La faute f_4 n'est donc pas diagnosticable (ne peut être détectée sans ambiguïté). La figure 7 présente l'estimation des niveaux d'eau (valeurs moyennes des particules) en comparaison aux niveaux d'eau réels.

Le scénario 2 illustre une incertitude sur l'occurrence d'un événement discret non observable, supporté par un changement de dynamique continue. À 720s, une fuite dans le réservoir T_1 se produit. La figure 8 montre que la faute f_1 est détectée en seulement une période d'échantillonnage grâce au changement de dynamique du système. La figure 9 présente l'estimation des niveaux d'eau en comparaison aux niveaux d'eau réels. Les enveloppes autour

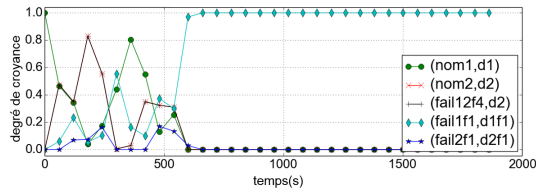


Figure 10: Scénario 3 : degrés de croyance des modes de santé.

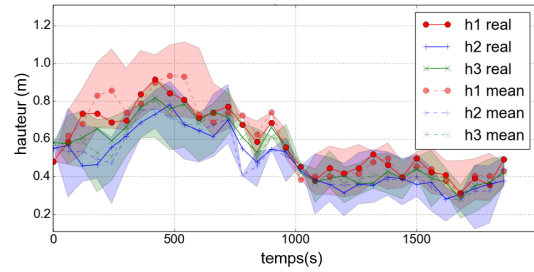


Figure 11: Scénario 3 : surveillance des niveaux d'eau.

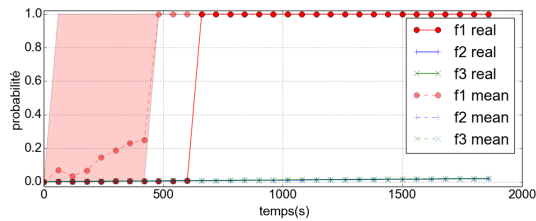


Figure 12: Scénario 3 : suivi des probabilités des fautes.

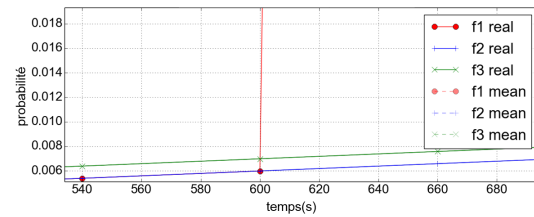


Figure 13: Scénario 3 : zoom sur le suivi des probabilités des fautes.

des valeurs moyennes des particules représentent les incertitudes sur l'estimation des niveaux.

Le scénario 3 illustre les incertitudes sur les équations dynamiques et sur les observations continues. Il s'agit du même scénario que le scénario 2 avec des bruits 10 fois plus importants (excepté pour la mesure de la masse totale d'eau). La figure 11 montre l'incertitude sur les équations d'état et sur les mesures. Le résultat du diagnostic (figure 10) présentent plus d'hypothèses sur les modes de santé que les précédents scénarios. Néanmoins, le diagnostic reste cohérent avec la réalité. Après 720s, même si les valeurs estimées des niveaux sont bruitées, la faute f_1 est détectée sans ambiguïté. La figure 12 donne les valeurs de dégradation estimées (valeurs des jetons hybrides) calculées à partir des lois de dégradation. La dégradation représentée par des probabilités de faute évolue entre 0 et 1. L'enveloppe autour de la valeur moyenne de f_1 représente l'incertitude sur les modes de santé. Certains jetons hybrides représentent le système dans un mode nominal alors que d'autres représentent le système dans un mode de défaillance de f_1 . La figure 13 détaille les valeurs de dégradation estimées pour f_2 et f_3 qui ne sont pas aussi significatives que celle de f_1 mais qui augmentent avec le temps.

6 Conclusion

En conclusion, cet article montre qu'utiliser les résultats d'un diagnostiqueur basé sur les HPPN est naturel dans le cadre de la gestion de santé. En effet, dans un cas de prise de décision, il est très difficile de "choisir" l'état du système en présence d'ambiguïté avec un diagnostiqueur traditionnel. L'utilisation d'un diagnostiqueur basé sur les HPPN permet de quantifier chaque état possible du système en traitant plusieurs types d'incertitude.

Les travaux futurs visent à développer la méthode de pronostic basée sur le niveau hybride des HPPN, et à intégrer ce module de surveillance de santé avec le module de planification.

References

- [1] R. Alami, R. Chatila, S. Fleury, M. Ghallab, and F. Ingrand. An Architecture for Autonomy. *The International Journal of Robotics Research*, 17(4):315–337, 1998.
- [2] E. Chanthery and P. Ribot. An integrated framework for diagnosis and prognosis of hybrid systems. In *3rd Workshop on Hybrid Autonomous System (HAS)*, 2013.
- [3] M. Djeziri, R. Merzouki, B. Bouamama, and G. Dauphin-Tanguy. Robust fault diagnosis by using bond graph approach. *IEEE/ASME Transactions on Mechatronics*, 12(6):599–611, 2007.
- [4] Q. Gaudel, E. Chanthery, and P. Ribot. Health monitoring of hybrid systems using Hybrid Particle Petri Nets. In *Annual Conference of the Prognostics and Health Management Society*, 2014.
- [5] Q. Gaudel, E. Chanthery, P. Ribot, and E. Le Corrnc. Hybrid systems diagnosis using Modified Particle Petri Nets. In *Proceedings of the 25th International Workshop on Principles of Diagnosis (DX'14)*, 2014.
- [6] S. Genc and S. Lafortune. Distributed diagnosis of place-bordered Petri Nets. *IEEE Transactions on Automation Science and Engineering*, 4(2):206–219, April 2007.
- [7] M. Hofbaur and B. Williams. Mode estimation of probabilistic hybrid system. *Hybrid Systems: Computation and Control (HSCC'02). Lecture Notes in Computer Science*, 2289:253–266, 2002.
- [8] W. Jianxiong, X. Xudong, B. Xiaoying, L. Chuang, K. Xiangzhen, and L. Jianxiang. Performability analysis of avionics system with multilayer HM/FM using stochastic Petri nets. *Chinese Journal of Aeronautics*, 26(2):363–377, 2013.
- [9] C. Lesire and C. Tessier. Particle Petri nets for aircraft procedure monitoring under uncertainty. In *Applications and Theory of Petri Nets*, pages 329–348. Springer, 2005.
- [10] S. Narasimhan, E. Balaban, M. Daigle, I. Roychoudhury, A. Sweet, J. Celaya, and K. Goebel. Autonomous decision making for planetary rovers using diagnostic and prognostic information. In *8th IFAC Symposium on Fault Detection*, 2012.
- [11] X. Olive, S. Clerc, and D. Losa. Smart architecture for highly available, robust and autonomous satellite. In *18th IFAC World Congress*, 2011.
- [12] I. Roychoudhury and M. Daigle. An integrated model-based diagnostic and prognostic framework. In *Proceedings of the 22nd International Workshop on Principle of Diagnosis (DX'11)*, 2011.
- [13] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzi. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.
- [14] S. Soldani, M. Combacau, A. Subias, and J. Thomas. On-board diagnosis system for intermittent fault: Application in automotive industry. In *7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems*, volume 7-1, pages 151–158, 2007.
- [15] R. Yu and N.C. Hadjicostis. Fault diagnosis in discrete event systems modeled by Partially Observed Petri Nets. *Discrete Event Dynamic Systems*, 19(4):551–575, 2009.
- [16] S. Zabi, P. Ribot, and E. Chanthery. Health monitoring and prognosis of hybrid systems. In *Annual Conference of the Prognostics and Health Management Society 2013*, 2013.
- [17] A. Zaidi, N. Zanzouri, and M. Tagina. Modelling and monitoring of hybrid systems by hybrid Petri nets. In *Proceedings of the 10th WSEAS International Conference on SYSTEMS*, 2006.
- [18] B. Zhang, C. Sconyers, R. Patrick, and G. Vachtsevanos. A multi-fault modeling approach for fault diagnosis and failure prognosis of engineering systems. In *Annual Conference of the Prognostics and Health Management Society*, 2009.
- [19] L. Zouaghi, A. Alexopoulos, A. Wagner, and E. Badreddin. Modified particle Petri nets for hybrid dynamical systems monitoring under environmental uncertainties. In *IEEE/SICE International Symposium on System Integration (SII)*, pages 497–502. IEEE, 2011.
- [20] L. Zouaghi, A. Alexopoulos, A. Wagner, and E. Badreddin. Probabilistic online-generated monitoring models for mobile robot navigation using Modified Petri Net. In *15th International Conference on Advanced Robotics (ICAR)*, pages 594–599. IEEE, 2011.