Génération du comportement observable d'un système pour l'étude de la diagnosticabilité de défauts

Michel Batteux, Philippe Fiani, Nicolas Rapin, Philippe Dague

Caractérisation du comportement observable d'un système pour l'étude de la diagnosticabilité de défauts

Michel Batteux & Philippe Fiani
Sherpa Engineering
La Garenne Colombes, France
Email : m.batteux@sherpa-eng.com & p.fiani@sherpa-eng.com

Nicolas Rapin
CEA, LIST, Laboratoire d'Ingénierie dirigée par les modèles pour les Systèmes Embarqués, Point Courier 94, Gif-sur-Yvette, 91191 France
Email : nicolas.rapin@cea.fr

Philippe Dague
LRI, Univ. Paris-Sud & CNRS, INRIA Saclay – Île-de-France
Orsay, France
Email : philippe.dague@lri.fr

***Résumé*—Cet article décrit une approche d'étude de la diagnosticabilité des défauts d'un système automatique par caractérisation de son comportement observable. Les systèmes automatiques sont des systèmes complexes comprenant une multitude de composants interagissant les uns avec les autres. Des défauts peuvent y apparaitre avec un impact néfaste sur leur environnement ou leur propre intégrité. Il est donc important de compléter ces systèmes de dispositifs de diagnostic permettant de détecter et d'identifier ces défauts, le plus précisément et le plus tôt possible. Ceci nécessite au préalable de s'assurer de la diagnosticabilité des défauts c'est-à-dire de déterminer dès la phase de conception s'ils seront bien détectés et discriminés par le dispositif de diagnostic. Dans ce document, nous présentons une approche permettant d'identifier et d'intégrer des défauts dans un modèle d'un système. Ces modèles sont ensuite exploités pour l'étude de la diagnosticabilité des défauts.**

Mots-clés: modélisation de défauts, diagnostic à base de modèles, diagnosticabilité.

I. INTRODUCTION

L'essor de l'électronique en général et plus particulièrement des systèmes automatisés prend une part de plus en plus importante dans de nombreux domaines. Ces systèmes, généralement complexes, comprennent une multitude de composants interagissant les uns avec les autres et combinant de multiples phénomènes physiques : électrique, hydraulique, thermodynamique, etc. Or, une des conséquences de cette multiplicité est l'augmentation du risque de défaillances, ou pannes, pouvant impacter le fonctionnement du système ou son environnement. La maîtrise de ces risques est élaborée lors de la conception du système grâce à l'étude de sûreté de fonctionnement ([5] et [6]).

Une des tâches de la sûreté de fonctionnement est donnée par la fonction de surveillance du système. Il s'agit de réaliser, généralement en ligne, la détection et l'isolation d'un défaut dès son apparition. Les méthodologies de diagnostic ([1], [2] et [3]) sont des solutions adéquates pour réaliser ces taches de détection et d'isolation. Elles consistent à vérifier que le comportement réellement observé du système satisfait une certaine propriété à défaut de quoi il est jugé non conforme et utilisé pour déduire les causes des défauts. Pour les méthodes à base de modèles par exemple ([4], [8] et [10]), il s'agit de comparer ce comportement réellement observé à un comportement prédit, issu d'un modèle de bon fonctionnement. Un dispositif de diagnostic fonctionne donc en analysant le comportement observable du système. Le terme "observable" est ici utilisé avec le sens communément admis dans les travaux de diagnosticabilité : visible par un observateur extérieur ; et n'est donc pas utilisé suivant le sens de la communauté de l'automatique.

Un des principaux problèmes qui se pose alors est la diagnosticabilité du système ([14] et [15]). Il s'agit de s'assurer que le dispositif de diagnostic sera d'une part toujours capable de détecter un défaut lorsqu'il apparait (le défaut engendre-t-il un comportement observable anormal ?) et que d'autre part il identifiera toujours un unique défaut répertorié pour un comportement observable anormal donné (plusieurs défauts engendrent-ils un même comportement observable ?). Une approche, pour étudier la diagnosticabilité d'un système, est d'intégrer les défauts potentiels dans le modèle de bon fonctionnement du système ; puis d'exploiter ces différents modèles (de bon fonctionnement et de défauts) afin d'en caractériser les comportements observables. Le dispositif de diagnostic sera par la suite basé sur cette caractérisation des comportements observables. Il est donc nécessaire d'avoir les modèles (de bon fonctionnement et de défauts) du système ainsi qu'une méthode de caractérisation de ses comportements observables.

Ce document présente d'abord une approche, permettant d'identifier et d'intégrer des défauts dans le modèle de bon fonctionnement du système. Il montre ensuite comment exploiter tous ces modèles pour l'étude de la diagnosticabilité. Dans la deuxième partie, nous présentons le formalisme adopté pour modéliser un système et montrons comment y intégrer des défauts. Dans la troisième partie, nous exploitons ces différents modèles afin de définir les comportements observables du système (sous la présence ou non d'un défaut). Dans la quatrième partie, nous étudions la diagnosticabilité du système en analysant ces comportements observables. La dernière partie conclura en résumant les résultats obtenus et ouvrira sur les perspectives pour de futurs travaux.

II. MODELISATION DU SYSTEME ET DES DEFAUTS

Dans le but d'étudier la diagnosticabilité des défauts potentiels d'un système, il faut avoir au préalable un modèle de bon fonctionnement du système, ainsi que les modèles de défauts. Cette partie présente le moyen de les obtenir en

intégrant les défauts potentiels directement dans le modèle de bon fonctionnement du système.

A. Modélisation du système sans défaut

1) Architecture du système complet

Dans la majeure partie des travaux de la littérature, les méthodes mises au point pour le diagnostic se basent sur une représentation du système en boucle ouverte. Or, dans la plupart des applications industrielles, le système est inséré dans une boucle de régulation ou de commande, piloté par un contrôleur afin d'accroître ses performances et de les maintenir en dépit des entrées inconnues pouvant l'affecter. Dans ce contexte, la détection et la localisation de défauts est plus délicate du fait des objectifs contradictoires entre la commande et le diagnostic : l'objectif de la commande est de minimiser, voir d'annuler, les effets des perturbations et des défauts ; alors que celui du diagnostic est justement de mettre en évidence ces défauts.

La solution envisagée est de considérer un modèle du système bouclé complet : le système et son contrôleur. La figure 1 représente l'architecture de l'ensemble complet.

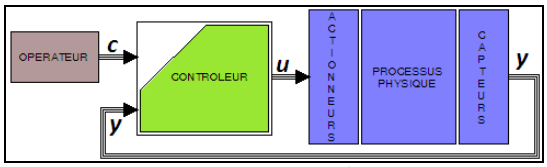

Figure 1 : architecture du système complet

2) Modélisation complète sans défaut

La conception et le développement des systèmes de contrôle commande sont de plus en plus réalisés en utilisant des modèles du système. Ces modèles vont être utilisés pour réaliser l'étude de diagnosticabilité.

Nous supposons donc disposer d'un modèle de bon fonctionnement du système, le plus représentatif possible. Nous supposons la boucle complète représentée par l'ensemble suivant (1) d'équations :

$$\begin{aligned} &x(t+1) = f(x(t),\theta,u(t),d(t)),\ x(0) = x_{init} \\ &y(t) = g(x(t),\theta,u(t),d(t)) \\ &a(t+1) = h(c(t),a(t),y(t)),\ a(0) = a_{init} \\ &u(t) = k(c(t),a(t),y(t)) \end{aligned} \quad (1)$$

où u, x, θ, d et y représentent respectivement les vecteurs de commandes, d'états, de paramètres, de perturbations et de mesures du système ; c et a représentent respectivement les vecteurs de consignes et d'états de la commande. La variable t évolue dans un domaine temporelle discret T.

B. Modélisation des défauts

Les défauts du système peuvent occasionner des dégâts plus ou moins graves. Il est donc important de les identifier et les classifier au préalable pour les intégrer ensuite dans le modèle.

1) Identification des défauts

Une étude de sûreté de fonctionnement ([5], [6] et [7]) permet de répertorier l'ensemble des défauts potentiels du système devant être pris en compte par une démarche de diagnostic. L'utilisation de méthodes complémentaires, telles que l'analyse fonctionnelle, l'analyse préliminaire des risques et l'AMDEC, permet non seulement d'identifier ces défauts potentiels, mais aussi d'analyser leurs causes et déterminer leurs conséquences.

Les défauts potentiels qui devront être pris en compte par le système de diagnostic sont par conséquent définis lors de cette étude de sûreté de fonctionnement. Nous considérons l'ensemble $\Gamma=\{F_0,F_1,\ldots,F_k\}$ des défauts répertoriés où pour simplifier la présentation, la faute F_0 désigne par convention le cas sans défaut.

2) Classification des défauts

Les défauts potentiels, identifiés lors de l'étude de sûreté de fonctionnement du système, peuvent être classifiés afin de permettre leur intégration dans le modèle. De nombreuses classifications de défauts peuvent être trouvées dans la littérature ; toutes font cependant une distinction entre le comportement du défaut de sa localisation et son effet sur le système.

La rupture d'une courroie d'entrainement ou un court-circuit dans une carte de puissance sont des défauts localisés sur des composants différents ; ils ont cependant le même comportement (ils arrivent brusquement et sont permanents). À l'inverse, la rupture de l'axe de transmission d'un compresseur et l'encrassement d'un compresseur sont des défauts localisés sur le même composant mais n'ayant pas les mêmes comportements.

a) Comportement des défauts

Selon [1], [8], [9] et [13], le comportement d'un défaut est caractérisé par son instant d'apparition (aléatoire, à un instant particulier du temps, ou dû à un événement particulier interne ou externe au système), sa force d'apparition (progressive ou brusque) ainsi que par sa durée de présence (permanente, transitoire ou intermittente).

La figure 2 représente les différents comportements de défauts. Les trois premiers graphiques représentent la durée de présence d'un défaut : permanent, transitoire et intermittent. Le premier et le dernier graphiques représentent la force d'apparition d'un défaut : brusque et progressif.

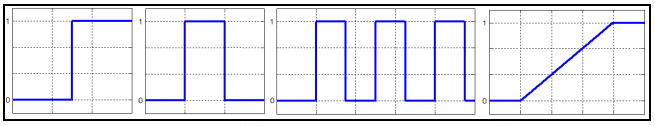

Figure 2: les différents comportements des défauts

b) Effets des défauts sur le système

L'effet d'un défaut sur le système consiste en sa localisation dans le système et les perturbations induites. Selon [1], [10], [4], [8] et [13], différentes localisations de défauts peuvent être établies : dans un capteur, dans un actionneur, dans le processus physique ou dans l'unité de contrôle commande. En ce qui nous concerne, nous ne nous intéressons pas aux défauts dans l'unité de contrôle commande.

Dans un capteur, le défaut se caractérise par un écart entre la valeur réelle de la grandeur et sa mesure ; un défaut de capteur perturbe donc le vecteur y des sorties du modèle. Dans le processus physique, le défaut est dû à des modifications de la structure (fuite, rupture d'un organe, etc.) ou des paramètres du modèle (encrassement d'un tuyau, bouchage partielle d'une conduite, etc.) ; un défaut du processus physique perturbe donc le vecteur x des états ou θ des paramètres du modèle. Enfin dans un actionneur, le défaut se traduit par une incohérence entre les commandes et la sortie du système (pompe délivrant

un débit incohérent avec sa caractéristique hydraulique) ; un défaut d'actionneur perturbe donc le vecteur *u* des commandes du modèle.

Comme décrit dans [13], une perturbation peut être additive, multiplicative, sinusoïdale, limitative ou peut stopper le signal à la dernière valeur de la variable (juste avant l'instant d'occurrence du défaut).

3) Intégration des défauts

Suite à l'identification et la classification des défauts, et toujours dans le but d'obtenir le comportement observable du système sous la présence de défauts, nous pouvons maintenant les intégrer dans le modèle de bon fonctionnement du système.

a) Intégration dans le modèle

Pour un défaut $F \in \Gamma \setminus \{F_0\}$ et un instant d'occurrence $t_n \in T$, le modèle du système, sous la présence du défaut F apparaissant à l'instant d'occurrence t_n, est décrit en considérant l'ensemble d'équations (1) où la variable perturbée considérée v (une commande u, une mesure y, un état x ou un paramètre θ) est remplacée par sa perturbation v_F, décrite par $v_F(t) = \boldsymbol{pert}_F(t,v(t),dft_F(t,t_n))$, où dft_F représente le comportement du défaut et $t_n \in T$ son instant d'occurrence.

Par exemple, pour un défaut F de capteur, représenté par $y_F(t) = \boldsymbol{pert}_F(t,y(t),dft_F(t,t_n))$, le modèle de défaut du système est décrit par l'ensemble suivant (2) d'équations :

$$\begin{aligned} x(t+1) &= f(x(t),\theta,u(t),d(t)),\ x(0) = x_{init} \\ y(t) &= \boldsymbol{pert}_F(t,g(x(t),\theta,u(t),d(t)),dft_F(t,t_n)) \\ a(t+1) &= h(c(t),a(t),y(t)),\ a(0) = a_{init} \\ u(t) &= k(c(t),a(t),y(t)) \end{aligned} \qquad (2)$$

b) La librairie de défauts

En se fondant sur la représentation d'un défaut adoptée précédemment, qui distingue son comportement de son effet, nous avons élaboré pour l'environnement MATLAB/Simulink© une librairie générique de défauts ([13]) permettant d'intégrer facilement des défauts dans un modèle de simulation. Cette librairie est constituée de deux éléments. L'élément '*fault-signal-block*', représentant le comportement du défaut, émet un signal compris entre 0 (absence du défaut) et 1 (présence complète du défaut) paramétrable selon le comportement identifié du défaut. L'élément '*perturbation-block*', représentant l'effet du défaut, permet de perturber un signal (une entrée *u*, une sortie *y*, un état *x* ou un paramètre θ) suivant les composants affectés et dépendant du signal de défaut émit par un '*fault-signal-block*'.

D'une manière générale et suivant la description des effets du défaut sur le système, trois différents cas d'intégration de défauts peuvent être accomplis dans le modèle avec cette librairie :

- Premier cas (Fig. 3, intégration 1) : l'intégration se fait directement sur le lien entre deux composants. Un '*perturbation-block*', contrôlé par un '*fault-signal-block*', perturbe donc ce lien.
- Deuxième cas (Fig. 3, intégration 2) : l'intégration se fait à l'intérieur d'un composant. Un '*perturbation-block*' perturbe une variable ou un paramètre interne du composant et un nouveau signal d'entrée est rajouté au composant pour contrôler ce '*perturbation-block*' par un '*fault-signal-block*'.
- Troisième cas (Fig. 3, intégration 3) : de nouveaux composants sont nécessaires dont un actionneur, contrôlé par un '*fault-signal-block*', et divers composants physiques supplémentaires.

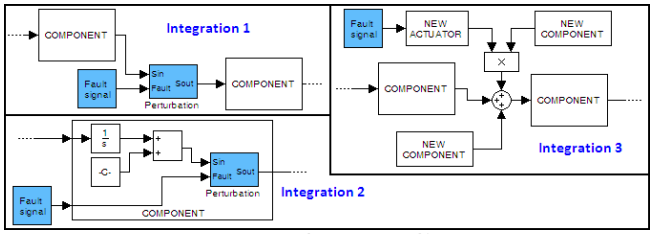

Figure 3 : intégration de défauts

Cette librairie est bien adaptée pour les systèmes modélisés par un assemblage de plusieurs composants variés. En effet, même si un défaut perturbe plusieurs composants, seul un unique '*fault-signal-block*' sera nécessaire pour représenter son comportement. De plus, tous les défauts potentiels d'un composant peuvent être intégrés à l'intérieur même de ce composant en y incorporant les '*perturbation-block*' adéquates ; un signal d'entrée est rajouté au composant pour contrôler ces '*perturbation-block*' par un '*fault-signal-block*'. Ceci est particulièrement intéressant lors de la réutilisation des composants pour modéliser d'autres systèmes.

III. COMPORTEMENTS OBSERVABLES

L'insertion de défauts, dans le modèle de bon fonctionnement d'un système, permet d'obtenir les modèles de défauts. Ce sont tous ces modèles qui vont nous permettre d'obtenir et de caractériser le comportement observable du système sous la présence, ou non, d'un défaut.

Le comportement du système représente sa manière de fonctionner suivant les consignes données par l'opérateur. Il s'agit donc des valeurs que prennent les variables du système lors de son fonctionnement. Le comportement observable du système est obtenu à partir du comportement du système en ne le considérant que sur les variables observables. Comme indiqué précédemment, le terme "observable" est utilisé dans le sens des travaux de diagnosticabilité : visible par un observateur extérieur, comme un système de diagnostic par exemple.

A. Préliminaires

L'ensemble des variables du modèle complet est donné par $V=\{c;a;u;x;y;d\}$ et l'ensemble des variables observables est $V_{Obs}=\{c;u;y\}$. Nous notons C, A, U, X, Y et D les domaines respectifs des valeurs possibles des variables *c*, *a*, *u*, *x*, *y* et d.

Une instruction de l'opérateur correspond à l'évolution de la consigne dans le temps. Formellement, il s'agit d'une suite *cons*, d'une fenêtre temporelle $I_{cons} \subseteq T$, supposée commencer à 0, dans l'ensemble C (*cons* : $I_{cons} \rightarrow C$). Dans la suite, nous considérons un ensemble *Cons* d'instructions le plus représentatif possible : c'est-à-dire permettant d'obtenir l'ensemble des plages de fonctionnement du système. De plus, comme chaque instruction est définie suivant sa propre fenêtre temporelle I_{cons}, nous posons $I=\max\{I_{cons}\}$ et définissons sur I chaque instruction *cons* par extension de la dernière valeur $cons(\max(I_{cons}))$ lorsque $I_{cons} \subset I$.

Pour un vecteur $v = (v_1,\ldots,v_n)$ et $k\in\{1,\ldots,n\}$, nous notons $p_k(v)=v_k$ le k-ième élément de v. Pour un produit d'ensembles $E = E_1\times\cdots\times E_n$, pour un sous-ensemble $G \subseteq E$ et pour des indices $i_1,\ldots,i_k\in\{1,\ldots,n\}$ avec $k\leq n$; la projection des éléments de G sur l'ensemble $Ei_1\times\cdots\times Ei_k$ est l'ensemble :

$$\Pr_{E_{i_1}\times\cdots\times E_{i_k}}(G) = \{(p_{i_1}(v),\cdots,p_{i_k}(v))\in E_{i_1}\times\cdots\times E_{i_k} \setminus v\in G\}.$$

B. Comportements du système

Un comportement du système représente l'ensemble des valeurs prises par les variables lors de son fonctionnement suivant une instruction de l'opérateur. Ce fonctionnement pouvant être sous la présence, ou non, d'un défaut. Un comportement est donc déterminé non seulement en fonction d'une instruction $cons\in Cons$ donnée mais aussi en fonction d'un défaut $F\in\Gamma$ considéré.

1) Comportements normaux du système

Pour une instruction $cons\in Cons$, le comportement normal du système est l'ensemble, noté $B(cons,F_0)$, de vecteurs $(t,v(t))\in T\times C\times A\times U\times X\times Y\times D$ de données, ordonnés dans la fenêtre temporelle I. $v(t)=(c(t),a(t),u(t),x(t),y(t),d(t))$ est le vecteur des valeurs des variables à chaque instant $t\in I$. Cet ensemble $B(cons,F_0)$ de vecteurs vérifie :

a. Existence et unicité dans le temps : pour tout instant $t\in I$, il existe un unique vecteur $v(t)\in C\times A\times U\times X\times Y\times D$ tel que $(t,v(t))\in B(cons,F_0)$.
b. Construction suivant l'instruction $cons$: pour tout instant $t\in I$, $p_1(v(t)) = cons(t)$.
c. Satisfaction des conditions initiales : $p_2(v(0))=a_{init}$, $p_4(v(0))=x_{init}$.
d. Satisfaction des équations du système en fonctionnement normal : pour tout instant $t\in I$,
   i. $p_4(v(t+1)) = f(p_4(v(t)),\theta,p_3(v(t)),p_6(v(t)))$
   ii. $p_5(v(t)) = g(p_4(v(t)),\theta,p_3(v(t)),p_6(v(t)))$
   iii. $p_2(v(t+1)) = h(p_1(v(t)),p_2(v(t)),p_5(v(t)))$
   iv. $p_3(v(t)) = k(p_1(v(t)),p_2(v(t)),p_5(v(t)))$

2) Comportements avec défauts du système

Une des caractéristiques du comportement d'un défaut est son instant d'apparition. Nous avons vu qu'il peut apparaitre aléatoirement, à un instant donné ou à cause d'un événement particulier. Pour la suite de l'étude, nous ne considérons que des défauts apparaissant à un instant particulier t_n du temps ; en effet, ce qui nous intéresse est de s'assurer qu'un défaut soit diagnosticable lorsqu'il apparait et non de prédire son instant d'occurrence.

Le comportement du système, suivant une instruction $cons\in Cons$ et sous la présence d'un défaut $F\in\Gamma\setminus\{F_0\}$ apparaissant à un instant $t_n\in I$ du temps, est l'ensemble noté $B(cons,F,t_n)$ et défini comme dans le cas normal où les points (c) (si $t_n = 0$) et (d) sont remplacés par la satisfaction des équations du modèle de défaut F.

C. Comportements observables du système

Le comportement observable du système désigne sa manière, visible par un observateur extérieur, de fonctionner suivant une instruction de l'opérateur. Il s'agit de la projection du comportement du système sur uniquement l'ensemble des variables observables. La détection et l'indentification d'un défaut n'ont par ailleurs de sens que si elles s'effectuent en un temps borné b après son apparition (borne supposée supérieur au temps de réponse du système). La projection du comportement du système ne se considère donc uniquement sur l'intervalle de temps $[t_n,t_n+b]$, avec $t_n\in J = [0;\max(I)-b]\subseteq I$.

Formellement, pour un comportement normal $B(cons,F_0)$, et pour un instant $t_n\in J$, le comportement observable $ObsB(cons,F_0,t_n)$ sous-jacent est la projection de $B(cons,F_0)$ sur l'ensemble produit $[t_n,t_n+b]\times C\times U\times Y$ des variables observables : $ObsB(cons,F_0,t_n) = \Pr_{[t_n;t_n+b]\times C\times U\times Y}(B(cons,F_0))$. De même pour un comportement de défaut $B(cons,F,t_n)$, le comportement observable $ObsB(cons,F,t_n)$ sous-jacent est la projection de $B(cons,F,t_n)$ sur l'ensemble produit des variables observables : $ObsB(cons,F,t_n) = \Pr_{[t_n;t_n+b]\times C\times U\times Y}(B(cons,F,t_n))$

Comme un comportement observable est déterminé en fonction d'une instruction $cons\in Cons$, d'un défaut $F\in\Gamma$ et d'un instant d'apparition $t_n\in J$. L'ensemble $ObsBeh_{Cons}(F)$ des comportements observables, suivant l'ensemble $Cons$ des instructions et sous la présence d'un défaut $F\in\Gamma$, est donc la réunion de tous les comportements observables pour tous les instants d'apparition et toutes les instructions : $ObsBeh_{Cons}(F)=\cup_{c\in Cons}\cup_{t\in J}\{ObsB(c,F,t)\}$. Par conséquent, l'ensemble des comportements observables suivant l'ensemble $Cons$ des instructions est la réunion de tous les ensembles des comportements observables pour tous les défauts : $ObsBeh_{Cons}=\cup_{F\in\Gamma}\{ObsBeh_{Cons}(F)\}$. La fenêtre temporelle d'un comportement observable $ob\in ObsBeh_{Cons}$ est de la forme $[t_{ob};t_{ob}+b]$ et est notée $TDom(ob)$.

Dans la pratique, les ensembles des comportements observables peuvent être obtenus grâce à l'utilisation d'outils de simulation.

IV. ÉTUDE DE LA DIAGNOSTICABILITE DU SYSTEME

Intuitivement, un défaut $F\in\Gamma$ est diagnosticable si le comportement observable du système avec ce défaut n'est pas "le même" que le comportement observable du système avec un autre défaut $F'\in\Gamma\setminus\{F\}$. Cet autre défaut pouvant soit être le cas nominal F_0, ou soit un autre défaut $F'\in\Gamma\setminus\{F,F_0\}$; ce qui exprime donc les deux notions de détection et d'identification.

L'étude de la diagnosticabilité est inhérente au procédé d'analyse du dispositif de diagnostic. En effet, lors du fonctionnement du système, le dispositif de diagnostic contrôlera si le comportement observable du système vérifie une certaine propriété de bon fonctionnement. Dans le cas contraire il recherchera quelle propriété de mauvais fonctionnement vérifie ce comportement observable. C'est donc à partir de ces propriétés, caractérisant le comportement observable du système sous la présence, ou non, d'un défaut, que se fera l'étude de la diagnosticabilité. C'est ce que nous appelons la caractérisation des défauts.

A. Caractérisation des défauts

Pour chaque défaut $F\in\Gamma$, nous devons construire une propriété P_F portant sur l'ensemble de tous les comportements

observables du système et caractérisant le comportement observable du système sous la présence du défaut. Chaque propriété doit au moins être vérifiée par les comportements observables sous la présence du défaut considéré. Nous allons proposer deux types de caractérisations.

1) Caractérisation parfaite

Pour caractériser le comportement observable du système sous la présence d'un défaut $F \in \Gamma$, la solution la plus naturelle est de simplement considérer les ensembles $ObsBeh_{Cons}(F)$. Un comportement observable $ob \in ObsBeh_{Cons}$ quelconque vérifie la caractérisation parfaite d'un défaut $F \in \Gamma$ si et seulement si $ob \in ObsBeh_{Cons}(F)$. La propriété P_F sous-jacente est donc $P_F(ob)$ est vraie si et seulement si $ob \in ObsBeh_{Cons}(F)$.

Cette caractérisation est parfaite dans le sens où il n'est pas possible de caractériser d'une meilleure façon les comportements observables. En effet, chaque ensemble $ObsBeh_{Cons}(F)$ est par définition le comportement observable du système sous la présence d'un défaut, il n'est donc pas possible de mieux le décrire.

Comme ces ensembles sont construits suivant un ensemble *Cons* d'instructions, il doit donc être le plus représentatif possible. Ceci car en fonctionnement, la vérification de l'appartenance, du comportement réellement observé (sur une fenêtre temporelle glissante [t;t+b]) à un des ensembles $ObsBeh_{Cons}(F)$, se fait d'abord en recherchant un comportement observable enregistré ayant le même morceau d'instruction *cons*.

2) Caractérisation par formules temporelles

Le second type de caractérisation des défauts se base sur une description des comportements observables par des formules temporelles. Pour ce faire, nous considérons une adaptation de la logique temporelle MITL ([11]), qui permet de spécifier des propriétés temps réel bornées. Nous considérons des formules temporelles construites suivant l'ensemble V_{Obs} des variables observables du système et interprétées sur l'ensemble des comportements observables du système. Les formules atomiques sont des comparaisons (égalités ou inégalités) entre deux expressions arithmétiques (ex : $v + 3 < 5$) ; et les formules temporelles sont construites en utilisant les opérateurs logiques classiques (négation, conjonction, …) et des opérateurs temporels tels que $G_{[\alpha;\beta]}$ (toujours dans une fenêtre temporelle bornée par α et β) ou $E_{[\alpha;\beta]}$ (au moins une fois dans une fenêtre temporelle bornée par α et β). La formule φ_{ex}: $((0 \leq c) \wedge (c < 20)) \Rightarrow (E_{[0;5]}(|y| \leq 0.1)))$ exprime que si la variable *c* est dans l'intervalle [0;20[, alors la variable *y* sera au moins une fois dans l'intervalle [0;0.1] dans un futur proche d'au plus 5 unités de temps.

Par analyse des ensembles $ObsBeh_{Cons}(F)$ obtenus par simulation, une formule temporelle spécifique φ_F est déterminée pour chaque défaut $F \in \Gamma$. Pour le cas nominal, φ_{Fo} exprime l'évolution temporelle des variables observables du système suivant la dynamique des ordres venant de l'opérateur (Fig. 4). Lors d'un changement important de la consigne, une sous-partie dynamique est vérifiée à partir de ce changement et durant le temps de réponse du système ; alors que lors de faibles changements, c'est une sous-partie statique qui est vérifiée. Pour les cas des défauts, les formules sont obtenues en considérant de plus le comportement et l'effet du défaut.

Un comportement observable $ob \in ObsBeh_{Cons}$ quelconque vérifie la caractérisation d'un défaut $F \in \Gamma$ si et seulement si *ob* valide la formule φ_F (noté $ob \models \varphi_F$). La propriété P_F sous-jacente est donc $P_F(ob)$ est vraie si et seulement si $ob \models \varphi_F$. Lors des simulations, ces formules sont vérifiées en temps réel grâce à l'outil ARTiMon©, du CEA, LIST ([12]), interfacé directement à MATLAB/Simulink©.

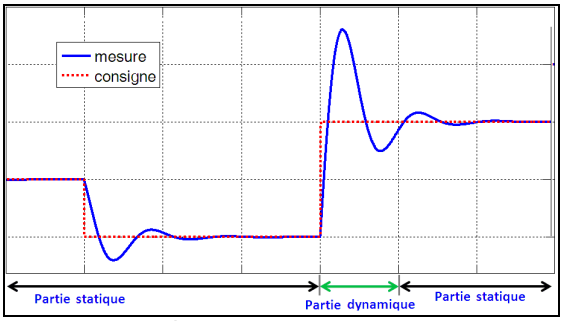

Figure 4 : évolution dynamique de la consigne.

B. Diagnosticabilité du système

Grâce à la caractérisation des défauts, nous pouvons définir formellement la notion de diagnosticabilité. Cette notion est définie indépendamment de la caractérisation considérée (parfaite ou par formules temporelles).

1) Définitions formelles

Un défaut $F \in \Gamma$ est *éligible* ssi quelle que soit sa date t_n d'apparition alors le comportement observable sous sa présence et de domaine $[t_n,t_n+b]$ satisfait la propriété P_F. Formellement, si pour toute consigne $c \in Cons$ et pour toute occurrence $t_n \in J$ de *F*, $P_F(Bobs(c,F,t_n))$ est vraie.

Un défaut $F \in \Gamma \backslash \{F_0\}$ est *détectable* ssi quelle que soit sa date t_n d'apparition alors le comportement observable sous sa présence et de domaine $[t_n,t_n+b]$ ne satisfait pas la propriété P_{Fo}. Formellement, si pour toute consigne $c \in Cons$ et pour toute occurrence $t_n \in J$ de *F*, $P_{Fo}(Bobs(c,F,t_n))$ est fausse.

Un défaut $F \in \Gamma \backslash \{F_0\}$ est *isolable* ssi quelle que soit sa date t_n d'apparition alors le comportement observable sous sa présence et de domaine $[t_n,t_n+b]$ ne satisfait aucune des propriétés $P_{F'}$, pour tout autre défaut $F' \in \Gamma \backslash \{F_0;F\}$. Formellement, si pour toute consigne $c \in Cons$ et pour toute occurrence $t_n \in J$ de *F* et pour tout défaut $F' \in \Gamma \backslash \{F_0;F\}$, $P_{F'}(Bobs(c,F,t))$ est fausse.

Un défaut $F \in \Gamma$ est *diagnosticable* s'il est éligible, détectable et isolable.

2) Analyse et résultats suivant le type de caractérisation

La diagnosticabilité est définie indépendamment de la caractérisation des défauts considérée; ainsi, bien que nous n'en ayons présenté que deux, d'autres peuvent être utilisées.

La diagnosticabilité est définie pour tous les défauts de l'ensemble Γ. Pour le cas nominal F_0, il ne s'agit donc que de vérifier son éligibilité.

La notion d'éligibilité a été introduite pour forcer les propriétés à au moins valider leur défaut. En effet, comme la diagnosticabilité est définie suivant une caractérisation de

défauts, il pourrait être possible que des défauts ne soient pas éligibles pour certaines caractérisations : une propriété ne validerait pas son défaut. Ce n'est néanmoins pas le cas de la caractérisation parfaite pour laquelle tous les défauts sont éligibles par définition des ensembles $ObsBeh_{Cons}(F)$.

Dans la pratique, l'isolabilité d'un défaut ne se considère que s'il est détectable et qu'avec les autres défauts détectables. Comme l'étude de la diagnosticabilité est inhérente au processus d'analyse du dispositif de diagnostic ; si un défaut n'est pas détectable, il ne sera alors pas détecté par le dispositif. Ainsi, le comportement observable du système sous la présence du défaut sera donc analysé par le dispositif comme normal. Il est donc inutile, en pratique, d'en étudier son isolabilité.

Si un défaut n'est pas diagnosticable avec la caractérisation parfaite, il ne le sera alors pas avec la caractérisation par formules temporelles. En effet, cette caractérisation par formules temporelles est obtenue en exploitant les ensembles de données $ObsBeh_{Cons}(F)$, elle peut donc être considérée comme une réduction de ces ensembles ; les exigences de diagnosticabilité en sont par conséquent plus faibles. Nous allons voir juste après que ce résultat est fortement utile.

En utilisation par un dispositif de diagnostic, l'espace mémoire et la puissance de calcul nécessaires seront beaucoup plus importants pour la caractérisation parfaite que pour la caractérisation par formules temporelles.

- Pour la caractérisation parfaite : à chaque instant t du temps, le dispositif de diagnostic enregistrera le comportement réellement observé *obs* du système sur la fenêtre temporelle glissante [t-b;t], puis recherchera d'abord si *obs* appartient à $ObsBeh_{Cons}(F_0)$ et sinon rechercher à quel ensemble $ObsBeh_{Cons}(F)$ appartient *obs*. Il faudra donc sauvegarder tous les ensembles $ObsBeh_{Cons}(F)$ ainsi que le comportement réellement observé *obs* (sur la fenêtre temporelle glissante [t;t+*b*]). La comparaison de *obs* se fera, dans le pire des cas, à tous les comportements observables des ensembles $ObsBeh_{Cons}(F)$ enregistrés, en commençant par ceux de $ObsBeh_{Cons}(F_0)$.
- Pour la caractérisation par formules temporelles : à chaque instant t du temps, le dispositif de diagnostic vérifiera d'abord si le comportement réellement observé valide la formule nominale φ_{Fo} ; et si elle n'est pas validée, il recherchera quelle formule de défaut φ_F est validée. Il faudra donc sauvegarder toutes les formules temporelles ainsi que le comportement réellement observé *obs*. La satisfaction par *obs* se fera, dans le pire des cas, à toutes les formules, en commençant par la formule nominale φ_{Fo}.

Pour des systèmes complexes ayant un domaine de fonctionnement important, la caractérisation parfaite pourrait donc être inexploitable par un dispositif embarqué de diagnostic ; du fait des capacités mémoire et de calcul fortement limitées. Elle est néanmoins très utile lors des phases de conception du système, afin de s'assurer intrinsèquement de la diagnosticabilité des défauts.

Enfin, bien que l'approche présentée soit exploitable pour le cas de plusieurs defaults simultanés, nous n'avons étudié que le cas des défauts uniques. Il est donc possible de traiter le cas des défauts simultanés du système pour être le plus représentatif possible.

V. CONCLUSION ET PERSPECTIVES

Dans ce document, notre but était d'étudier la diagnosticabilité des défauts en exploitant les modèles de défauts d'un système. Nous avons d'abord présenté la modélisation d'un système, en le considérant avec sa partie contrôle ; puis montré comment y intégrer des défauts, identifiés et classifiés au préalable. Nous avons ensuite pu définir les comportements observables du système et les utiliser pour en étudier sa diagnosticabilité.

Cette étude de la diagnosticabilité fut accomplie en caractérisant le comportement observable du système sous la présence de défauts. Deux caractérisations ont été proposées : l'une parfaite permet de s'assurer de manière intrinsèque de la diagnosticabilité des défauts ; l'autre, utilisant le formalisme de logique temporelle, permet d'être facilement embarquée dans un contrôleur.

Cette approche par caractérisation des défauts est actuellement testée sur un exemple industriel (un système pile à combustible [13]). Elle pourra par la suite prendre en compte le cas de défauts simultanés ; et être cumulée avec l'utilisation d'un modèle embarqué du système dans le dispositif de diagnostic. Ces futurs travaux seront présentés dans de prochains documents.

VI. REFERENCES

[1] J. Brunet, D. Jaume, M. Labarrère, A. Rault et M. Vergé. "Détection et diagnostic de pannes". Hermès,1990.

[2] V. Venkatasubramanian, R. Rengaswamy, K. Yin et S. N. Kavuri. "A review of process fault detection and diagnosis. 'part I to III'". Computers and Chemical Engineering, 2003.

[3] M. Basseville et I. V. Nikiforov. "Detection of Abrupt Changes : Theory and Application". Prentice-Hall, 1993.

[4] M. Blanke, M. Kinnaert, J. Lunze et M. Staroswiecki. "Diagnosis and fault-tolerant control". Springer-Verlag, 2006.

[5] J.C. Laprie, J. Arlat, J-P. Blanquart, A. Costes, Y. Crouzet, Y. Deswarte, J-C. Fabre, H. Guillermain, M. Kaaniche, C. Mazet, D.Powell, C. Rabéjac et P. Thévenod. "Guide de la Sûreté de Fonctionnement". 2ème édition (Cépaduès).

[6] R. F. Stapelberg, "Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design", Springer-Verlag, London, 2009.

[7] P. Moro, J. Girard, G. Tabet, J.C. Laprie, C. Duquesne et F. Codet. "Sûreté de fonctionnement", Revue de l'Electricité et de l'Electronique, n°11, décembre 2004.

[8] R. Isermann, "Fault Diagnosis Systems", Springer-Verlag, Berlin, 2006.

[9] R. Isermann, "Supervision, fault-detection and fault-diagnosis methods — An introduction", in Control Engineering Practice, vol. 5(5), May 1997, pp. 639-652, 2006.

[10] M. Basseville, "On fault detectability and isolability", Research Report IRISA no 1240, 1999.

[11] R. Alur, T. Feder, and T.A. Henzinger, "The Benefits of Relaxing Punctuality", Journal of the ACM 43, 116-146 (1996).

[12] N. Rapin, "Procédé et système permettant de générer un dispositif de contrôle à partir de comportements redoutés spécifiés", demande de brevet Français n°0804812 déposé le 2 septembre 2008.

[13] M. Batteux, P. Dague, N. Rapin, and P. Fiani, "Fuel cell system improvement for model-based diagnosis analysis", in the IEEE Vehicle Power and Propulsion Conference (VPPC), September 2010.

[14] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete event system", *IEEE* Transactions on Automatic Control, 40(9), 1555–1575, 1995.

[15] L. Travé-Massuyès, M.O. Cordier, and X. Pucel, "Comparing diagnosability in CS and DES", DX'06, Aranda de Duero (Spain), June 26-28, 2006.