Analyse fiabiliste des propriétés structurelles des systèmes continus par les réseaux d'activités stochastiques

Samia Maza, Manal Dakil, Christophe Simon

Université de Lorraine, Centre de Recherche en Automatique de Nancy, UMR CNRS 7039, Vandoeuvre-lès-Nancy, F-54506, France
CNRS, Centre de Recherche en Automatique de Nancy, UMR 7039, Vandoeuvre-lès-Nancy, F-54506, France
manal.dakil~;samia.maza~;christophe.simon@univ-lorraine.fr

RÉSUMÉ. *Dans cet article, nous montrons une approche originale de couplage entre l'analyse des systèmes continus et celle des systèmes à événements discrets en phase de conception pour évaluer conjointement les propriétés structurelles (commandabilité, observabilité, etc.) et leurs paramètres de sûreté de fonctionnement. L'analyse de propriétés structurelles des systèmes continus repose sur la théorie des graphes s'appuyant sur la connaissance des phénomènes physiques mis en jeu. L'analyse des paramètres de sûreté de fonctionnement s'appuie d'une part sur la connaissance des relations liant les composants, leur état de fonctionnement et la causalité physique et, d'autre part, sur une modélisation par un formalisme dédié aux systèmes à événements discrets. La démarche est illustrée sur un cas d'étude.*

ABSTRACT. *This paper deals with an original analysis approach of continuous system to study structural properties and their dependability. For this purpose, we combine structural analysis by the graph theory and the analysis of the dependability of the properties by stochastic activity networks. The assessment of the dependability factors is based on the knowledge of the link between componants, their state and their physical causality. Secondly, it is based on discrete events modeling to establish the link between component states and properties dependability. A study case illustrates the approach.*

MOTS-CLÉS : *analyse structurelle, propriétés structurelles, théorie des graphes, sûreté de fonctionnement, réseaux d'activités stochastiques.*

KEYWORDS: *structural analysis, structural properties, graph theory, depenability, stochastic activity network.*

DOI:10.3166/JESA.49.425-448

1. Introduction

Les systèmes continus sont des artefacts dont nous attendons qu'ils jouissent d'un certain nombre de propriétés. Par exemple, un avion, un processus chimique ou thermohydraulique doit être commandable et observable afin de contrôler/réguler et surveiller ses variables d'état critiques pour d'évidents problèmes de sécurité (IEC, 1998). Si nous souhaitons qu'ils soient tolérants aux fautes, cela suppose que nous soyons capables de détecter et d'isoler les fautes. Les systèmes doivent donc posséder la propriété de diagnosticabilité (Basile, Marro, 1969; Boukhobza *et al*., 2014; Hautus, 1983).

L'observabilité est la propriété qui permet de reconstruire le vecteur d'état à partir de certaines mesures disponibles sur le système. La commandabilité est la propriété qui garantit la possibilité d'amener le système dans un état donné en temps fini. La diagnosticabilité est la propriété du système qui garantit de pouvoir détecter et localiser des défauts.

Pour que ces systèmes assurent leurs missions, ces propriétés doivent être maintenues malgré les éventuelles défaillances des composants. Il est donc d'intérêt d'étudier les paramètres de sûreté de fonctionnement de ces propriétés dans une approche conjointe dès la phase de conception. En effet, c'est à partir des spécifications fonctionnelles que la structure puis le dimensionnement des composants, modules et interfaces sont définis. A cette étape, le dimensionnement n'est pas forcément connu. Il faut travailler à partir d'informations structurelles à l'aide de méthodes appropriées *i.e.* avec des modèles mathématiques sans instanciation numérique.

De nombreux travaux exploitent des formes algébriques ou géométriques qui nécessitent une connaissance précise des modèles d'états du système (Kalman, 1968). Cela ne permet pas leur emploi au plus tôt dans le cycle de vie. Ainsi, l'emploi de représentations génériques telles les modèles structurés est essentiel (Dion *et al*., 2003). La connaissance des causalités physiques entre les variables du modèle et les composants est primordiale et relève du champ de compétences de l'ingénierie.

L'analyse des paramètres prévisionnels de sûreté de fonctionnement se déroule dans la même phase du cycle de vie. Cette analyse doit conduire à valider le dimensionnement de l'architecture du système pour les besoins du client. Selon le type de système et ses propriétés attendues, l'analyse prévisionnelle de sûreté de fonctionnement s'attarde sur la fiabilité, la disponibilité ou la maintenabilité du système et fait l'objet de cet article. Dans le domaine de la Sûreté de Fonctionnement (SdF), il existe de nombreuses méthodes d'analyse plus appropriées à l'évaluation de chaque paramètre de la SdF (Prowell.S.J, Poore.J.H, 2004; Ruin, 2013; Staley, Sutcliffe, 1974; Villemeur, 1992). La méthode de modélisation basée sur les Réseaux d'Activités Stochastiques (RAS) qui est proposée dans cet article permet de traiter de manière générique l'ensemble des paramètres grâce à une approche systémique et systématique de complexité polynomiale. Elle repose sur la construction de modèles d'évaluation à partir de petits modules atomiques représentant les composants et fonctions élémentaires. Couplée à la méthode de Monte-Carlo, elle permet de simuler les comporte-

ments dynamiques et aléatoires des modules précédents. Cela permettra l'évaluation quantitative de certains paramètres de sûreté de fonctionnement. Les RAS sont intéressants, car ils permettent d'appréhender les systèmes réparables ou non de manière simple comparativement aux méthodes analytiques ou aux outils comme les automates (Cassandras, Lafortune, 2007). En outre, les RAS permettent de lever des hypothèses restrictives sur les lois de distribution des événements, certaines dépendances et certaines actions comme la réparation, le diagnostic et la reconfiguration (Maza, 2012, 2015).

L'article est organisé comme suit. La section 2 expose les éléments théoriques pour mener une analyse structurelle d'un système continu. La section 3 s'intéresse à la modélisation des résultats de l'analyse structurelle dans le formalisme des RAS. Enfin, la section 4 concerne l'étude d'un système mécanique continu à 4 variables d'état depuis l'analyse structurelle jusqu'à l'aspect évaluation prévisionnelle de paramètres de SdF par les RAS afin d'illustrer la méthodologie. Les résultats de simulation sont discutés. La section 5 conclut l'article.

2. Analyse structurelle

2.1. Représentation graphique

Dans cet article, nous considérons un système linéaire structuré (SLS) de la forme suivante :

$$\Sigma_\Lambda : \begin{cases} \dot{x} = Ax + Bu \\ y = Cx + Du \end{cases} \tag{1}$$

où $x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$, $u = (u_1, \ldots, u_m)^T \in \mathbb{R}^m$ et $y = (y_1, \ldots, y_p)^T \in \mathbb{R}^p$ sont respectivement les vecteurs d'état, d'entrée et de sortie. $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$ et $D \in \mathbb{R}^{p\times m}$ sont des matrices de dimensions appropriées. Elles ne contiennent que des paramètres nuls et/ou des paramètres libres notés $\alpha_1, \alpha_2, \ldots, \alpha_h$ supposés indépendants.

Dans cette section, nous exposons la représentation graphique d'un SLS noté Σ_Λ. Le graphe orienté associé à ce SLS est noté $\mathcal{G}(\mathcal{V}, \mathcal{E})$. Il est constitué d'un ensemble de sommets $\mathcal{V}$ et d'un ensemble d'arcs $\mathcal{E}$. Plus précisément, l'ensemble des sommets est défini par $\mathcal{V} = \mathbf{X} \cup \mathbf{U} \cup \mathbf{Y}$, où $\mathbf{X} = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$, $\mathbf{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ et $\mathbf{Y} = \{\mathbf{y}_1, \ldots, \mathbf{y}_p\}$ sont des ensembles de sommets correspondant respectivement aux variables d'état, d'entrée et de sortie. L'ensemble des arcs est $\mathcal{E} = \mathcal{E}_A \cup \mathcal{E}_B \cup \mathcal{E}_C \cup \mathcal{E}_D$, avec $\mathcal{E}_A = \{(\mathbf{x_j}, \mathbf{x_i}) \,|A(i,j) \neq 0\}$, $\mathcal{E}_B = \{(\mathbf{u_j}, \mathbf{x_i}) \,|B(i,j) \neq 0\}$, $\mathcal{E}_C = \{(\mathbf{x_j}, \mathbf{y_i}) \,|C(i,j) \neq 0\}$ et $\mathcal{E}_D = \{(\mathbf{u_j}, \mathbf{y_i}) \,|D(i,j) \neq 0\}$. La notation $(\mathbf{v}_i, \mathbf{v}_j)$ indique un arc orienté du sommet $\mathbf{v}_i \in \mathcal{V}$ vers le sommet $\mathbf{v}_j \in \mathcal{V}$ signifiant que les variations de $\mathbf{v}_i$ influent sur $\mathbf{v}_j$.

Un graphe biparti noté $\mathcal{B}(V^+, V^-, \mathcal{E}_\mathcal{B})$ est un graphe orienté dont l'ensemble des sommets se divise en deux sous ensembles disjoints V^+ et V^- connectés par un ensemble d'arcs $\mathcal{E}_\mathcal{B}$. V^+ contient tous les sommets ayant des arcs sortants dans $\mathcal{G}(\mathcal{V}, \mathcal{E})$ et V^- contient les sommets ayant des arcs entrants dans $\mathcal{G}(\mathcal{V}, \mathcal{E})$. Ces deux

ensembles V^+ et V^- sont définis comme suit : $V^+ = \{\mathbf{v}_i^+ \in X | \exists(\mathbf{v}_i, \mathbf{v}_j) \in \mathcal{E}\}$ et $V^- = \{\mathbf{v}_h^- \in X \cup Y | \exists(\mathbf{v}_t, \mathbf{v}_h) \in \mathcal{E}\}$. L'ensemble d'arcs $\mathcal{E}_\mathcal{B}$ est défini par : $\mathcal{E}_\mathcal{B} = \{(\mathbf{v}_i^+, \mathbf{v}_j^-) | \mathbf{v}_i^+ \in V^+ ; \mathbf{v}_j^- \in V^+\}$.

EXEMPLE 1. — *Considérons le SLS ayant la forme donnée par l'équation (1) et défini par :*

$$A = \begin{pmatrix} \alpha_1 & 0 & 0 \\ \alpha_2 & 0 & 0 \\ 0 & \alpha_3 & 0 \end{pmatrix} ; \; B = \begin{pmatrix} \alpha_4 \\ 0 \\ 0 \end{pmatrix} ; \; C = \begin{pmatrix} 0 & \alpha_5 & 0 \\ 0 & 0 & \alpha_6 \\ \alpha_7 & 0 & 0 \end{pmatrix}.$$

Ce système est associé à la représentation graphique de la figure (1). Pour ce système,

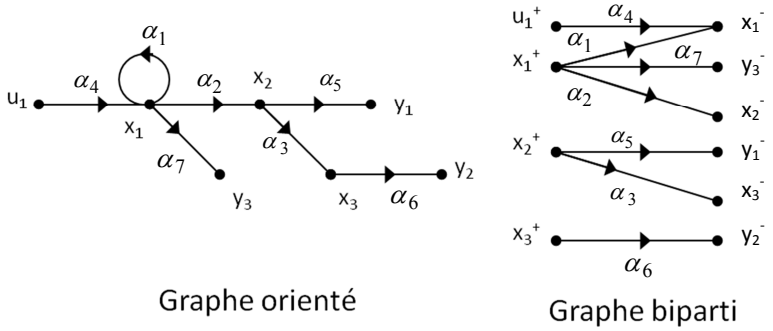


Figure 1. Représentation graphique associée à l'exemple 1

nous avons $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\}$, $\mathbf{U} = \{\mathbf{u}_1\}$, $\mathbf{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3\}$, $\mathbf{X}^+ = \{\mathbf{x}_1^+, \mathbf{x}_2^+, \mathbf{x}_3^+\}$, $\mathbf{U}^+ = \{\mathbf{u}_1^+\}$, $\mathbf{X}^- = \{\mathbf{x}_1^-, \mathbf{x}_2^-, \mathbf{x}_3^-\}$ *et* $\mathbf{Y}^- = \{\mathbf{y}_1^-, \mathbf{y}_2^-, \mathbf{y}_3^-\}$.

2.2. Définitions et notations

– Un chemin p qui couvre les sommets $\mathbf{v}_{r_0}, \ldots, \mathbf{v}_{r_i}$ est noté $p = \mathbf{v}_{r_0} \rightarrow \mathbf{v}_{r_1}, \ldots, \rightarrow \mathbf{v}_{r_i}$ où pour $j = 0, 1, \ldots i-1$, $(\mathbf{v}_{r_j}, \mathbf{v}_{r_{j+1}}) \in \mathcal{E}$.

– Soient $\mathcal{V}_1$ et $\mathcal{V}_2$ deux sous-ensembles de sommets de $\mathcal{V}$. Un chemin p est dit "chemin $\mathcal{V}_1 - \mathcal{V}_2$ " si son sommet de début est dans $\mathcal{V}_1$ et son sommet de fin est dans $\mathcal{V}_2$. De plus, si les seuls sommets de p appartenant à $\mathcal{V}_1 \cup \mathcal{V}_2$ sont ses sommets de début et de fin, alors p est dit "chemin direct $\mathcal{V}_1 - \mathcal{V}_2$" .

– Dans un graphe orienté $\mathcal{G}(\mathcal{V}, \mathcal{E})$, deux sommets $\mathbf{v}_i$ et $\mathbf{v}_j$ sont dit fortement connectés s'il existe un chemin de $\mathbf{v}_i$ à $\mathbf{v}_j$ et un chemin de $\mathbf{v}_j$ à $\mathbf{v}_i$. Cette relation de forte connectivité est une relation d'équivalence. Chaque classe d'équivalence de cette relation est dite "composante fortement connexe" de $\mathcal{G}(\mathcal{V}, \mathcal{E})$ et est notée $Cl(\mathbf{v}_i)$ (Murota, 1987).

– $Succ(\mathbf{v}_i)$ est l'ensemble de successeurs de $\mathbf{v}_i$, *i.e.* il existe un sommet $\mathbf{v}_j$ tel qu'il y a un chemin $\{\mathbf{v}_i\} - \{\mathbf{v}_j\}$.

– $Pred(V_1)$ est l'ensemble de prédécesseurs de tout élément $\mathbf{v}_j$ dans V_1, *i.e.* pour tout sommet $\mathbf{v}_j \in V_1$ il existe un chemin $\{\mathbf{v}_i\} - \{\mathbf{v}_j\}$.

– Dans un graphe biparti, $\theta(\mathcal{V}_1, \mathcal{V}_2)$ est le nombre maximal d'arcs disjoints dont les sommets de début sont dans $\mathcal{V}_1$ et les sommets de fin dans $\mathcal{V}_2$.

– Un couplage dans un graphe biparti $\mathcal{B}(V^+, V^-, \mathcal{E}_\mathcal{B})$ est un ensemble d'arcs $\mathcal{E}_\mathcal{M} \subseteq \mathcal{E}_\mathcal{B}$ tels que tous les arcs de $\mathcal{E}_\mathcal{M}$ sont disjoints. Un couplage est dit complet si sa cardinalité est maximale et égale à $\theta(X^+, X^- \cup Y^-) = card(X^+)$ pour le problème d'observabilité.

– Considérons un couplage complet $\mathcal{E}_\mathcal{M} \subseteq \mathcal{E}_\mathcal{B}$. Chaque couplage complet $\mathcal{E}_\mathcal{M}$ est associé à un graphe biparti non orienté noté $\mathcal{B}_\mathcal{M}(V^+, V^-, \overline{\mathcal{E}_\mathcal{B}})$ où $(\mathbf{v}_i, \mathbf{v}_j) \in \overline{\mathcal{E}_\mathcal{B}} \Leftrightarrow (\mathbf{v}_i, \mathbf{v}_j) \in \mathcal{E}_\mathcal{B}$ or $(\mathbf{v}_j, \mathbf{v}_i) \in \mathcal{E}_\mathcal{M}$. Notons par S_0^+(resp. S_0^-) l'ensemble des sommets dans V^+(resp. dans V^-) non couvert par les arcs appartenant à $\mathcal{E}_\mathcal{M}$.

– Le graphe biparti $\mathcal{B}(V^+, V^-, \mathcal{E}_\mathcal{B})$ peut être décomposé en composantes irréductibles et uniques partiellement ordonnées en utilisant la décomposition Dulmage-Mendelsohn (DM). Cette décomposition est utile pour déterminer les arcs n'appartenant à aucun couplage complet. Elle est décrite dans (Dulmage, Mendelsohn, 1958; Murota, 1987).

2.3. Conditions graphiques pour les propriétés structurelles

La validité des propriétés structurelles d'un système linéaire nécessite la vérification de certaines conditions graphiques. Parmi ces conditions, deux sont nécessaires pour la validité de plusieurs propriétés structurelles. Il s'agit des conditions de connectivité et de couplage complet. Pour des raisons de clarté, nous ne nous focalisons que sur ces deux conditions. Le lecteur trouvera plus de détails dans (Dakil, 2014).

2.3.1. Condition de connectivité

La condition de connectivité entre les ensembles V_1 et V_2 se traduit par l'existence d'un ou plusieurs chemins entre tous les sommets $\mathbf{v}_i \in V_1$, avec $V_1 \subseteq \mathcal{V}$, dans le graphe orienté $\mathcal{G}(\mathcal{V}, \mathcal{E})$ et au moins un sommet de $V_2 \subseteq \mathcal{V}$ par un chemin valide. La condition de connectivité entre les ensembles V_1 et V_2 est notée $CC(V_1, V_2)$ et la condition de connectivité du sommet $\mathbf{v}_i \in V_1$ à V_2 est notée $Con(\mathbf{v}_i)$. $\wedge$ (resp.$\vee$) représente l'opérateur logique "ET" (resp. "OU"). L'expression booléenne $CC(V_1, V_2)$ s'écrit alors :

$$CC(V_1, V_2) = \bigwedge_{\mathbf{v}_i \in V_1} Con(\mathbf{v}_i) \tag{2}$$

La connectivité $Con(\mathbf{v}_i)$ dépend soit de la connectivité directe de $\mathbf{v}_i$ vers V_2 notée $Con_d(\mathbf{v}_i)$ (sans passer par un sommet de sa composante fortement connexe) soit à travers un sommet $\mathbf{v}_j \in Cl(\mathbf{v}_i)$ de la même composante fortement connexe de $\mathbf{v}_i$.

$$Con(\mathbf{v}_i) = Con_d(\mathbf{v}_i) \vee \left(\bigvee_{\mathbf{v}_j \in Cl(\mathbf{x}\mathbf{v}_i) \setminus \{\mathbf{v}_i\}} \left(\bigvee_{p_j \in \text{chemins direct } \mathbf{v}_i - \mathbf{v}_j} \left(\bigwedge_{(\mathbf{v}_\ell, \mathbf{v}_k)_{u_r} \in p_j} (\mathbf{v}_\ell, \mathbf{v}_k) \right) \right) \wedge Con_d(\mathbf{v}_j) \right) \tag{3}$$

où $Con_d(\mathbf{v}_i)$ est la connectivité directe de $\mathbf{v}_i$ vers V_2 sans passer par les sommets appartenant à $Cl(\mathbf{v}_i)$. $Con_d(\mathbf{v}_i)$ est donnée par l'équation suivante :

$$Con_d(\mathbf{v}_i) = \bigvee_{\mathbf{v}_t \in Succ_d(\mathbf{v}_i) \setminus Cl(\mathbf{v}_i)} (\mathbf{v}_i, \mathbf{v}_t) \wedge Con(\mathbf{v}_t) \tag{4}$$

où $\mathbf{v}_t$ est un élément de l'ensemble $\mathcal{V}$. Dans le cas où $\mathbf{v}_i$ n'est le prédécesseur d'aucun élément de V_2, *i.e.* $\mathbf{v}_i \notin Pred(V_2)$, alors $Con(\mathbf{v}_i) = 0$ et $Con_d(\mathbf{v}_i) = 0$

Le principe fondateur de l'équation 3 est de rechercher une connectivité entre V_1 et V_2 de proche en proche. Soit un élément v_i est connecté directement à V_2 soit il est connecté au travers d'un élément de sa classe soit en passant par un autre élément v_j pour rejoindre V_2.

2.3.2. Condition de couplage complet

La condition de couplage complet pour l'observabilité consiste à avoir un nombre d'arcs disjoints dans le graphe biparti $\mathcal{B}(V^+, V^-, \mathcal{E}_\mathcal{B})$ égal à la dimension du vecteur V^+ (*e.g.* observabilité) ou au vecteur V^- (*e.g.* commandabilité). La condition de couplage complet entre l'ensemble V^+ et l'ensemble V^- est notée $MC(V^+, V^-)$.

Dans le graphe biparti $\mathcal{B}(V^+, V^-, \mathcal{E}_\mathcal{B})$, $\mathcal{E}^*$ est un ensemble d'arcs et ne contient que les arcs de la même classe après la DM décomposition de $\mathcal{B}(V^+, V^-, \mathcal{E}_\mathcal{B})$. Seuls les arcs appartenant à $\mathcal{E}^*$ peuvent être utilisés dans un couplage complet et donc $MC(V^+, V^-)$ ne dépend que des arcs appartenant à $\mathcal{E}^*$.

La condition de couplage complet peut donc s'écrire comme suit :

$$MC(V^+, V^-) = Exp(V^+, \mathcal{E}^*) \tag{5}$$

Exp est une expression booléenne récursive. Pour déterminer un couplage complet dans le graphe biparti, Exp considère un arc dans $\mathcal{E}$ puis s'appelle elle-même en fonction des autres arcs disjoints avec l'arc choisi. Son prototype $Exp(W, E)$ est donné par l'équation suivante :

$$\begin{aligned} Exp(W, E) = \bigvee_{(\mathbf{v}_i^+, \mathbf{v}_t^-) \in E} & \Big((\mathbf{v}_i^+, \mathbf{v}_t^-) \wedge Exp\left(W \setminus \{\mathbf{v}_i^+\}, \right. \\ & \left. f\left(W \setminus \{\mathbf{v}_i^+\}, E \setminus \{(\mathbf{v}_i^+, \mathbf{v}_k^-) | \mathbf{v}_k^- \in Succ(\mathbf{v}_i^+)\} \cup \{(\mathbf{v}_\ell^+, \mathbf{v}_t^-) | \mathbf{x}_\ell^- \in Pred(\mathbf{v}_t^-)\}\right)\right) \end{aligned} \tag{6}$$

où W est un ensemble de sommets, E est un ensemble d'arcs et $f(W, E)$ est la fonction qui calcule la DM décomposition du graphe biparti $\mathcal{B}(V^+, V^-, E)$ et qui retourne les ensembles d'arcs intra-classes. $\mathbf{v}_k^-$ et $\mathbf{v}_t^-$ sont des éléments de l'ensemble V^-.

Quand l'ensemble W contient un seul sommet $\mathbf{v}_i^+$, l'expression $Exp(W, E) = Exp(\{\mathbf{v}_i^+\}, E)$ est donnée par :

$$Exp(\{\mathbf{v}_i^+\}, E) = \bigvee_{(\mathbf{v}_i^+, \mathbf{v}_t^-) \in E} \left(\mathbf{v}_i^+, \mathbf{v}_t^-\right) \tag{7}$$

Le principe exploité ici est de recherché dans un graphe bipartite un nombre de couplage équivalent au nombre d'éléments dans V^+. Pour cela, en choisissant un arc reliant un élément de V^+ à V^- alors tous les arcs partant de cet élément de V^+ deviennent inexploitables. Le graphe est réduit aux nœuds et arcs utilisables pour rechercher un nouvel arc liant V^+ à V^- jusqu'à épuisement des nœuds source dans V^+.

Ainsi, l'observabilité d'un système Σ_Λ, par exemple, nécessite la vérification des conditions de connectivité $CC(X, Y)$ et de couplage complet $MC(X^+, X^- \cup Y^-)$:

$$Obs_{\Sigma_\Lambda} = CC\varphi(X, Y) \wedge MC\varphi(X^+, X \cup Y^-)$$

De la même façon, en inversant le sens des arcs, la commandabilité d'un système Σ_Λ nécessite la vérification des conditions de connectivité $CC(X, U)$ et de couplage complet $MC(X^-, U^+ \cup X^+)$:

$$Cmd = CC(X, U) \wedge MC(X^-, U^+ \cup X^+) \tag{8}$$

3. Analyse fiabiliste par les réseaux d'activités stochastiques

La modélisation physique d'un système et la mise en équation des relations de cause à effet de celui-ci permettent d'établir son modèle d'état structuré comme indiqué dans la section précédente. Dans ce modèle, aux paramètres α_i des matrices A, B et C (et donc les arcs correspondants dans le graphe) sont associés des composants physiques du procédé lui-même (matrice A), de ses actionneurs (matrice B) et de ses capteurs (matrice C) qui assurent la relation causale. La défaillance d'un de ces composants peut invalider un arc et avoir un impact sur la satisfaction des propriétés étudiées (Dakil, 2014; Maza *et al.*, 2012).

L'approche proposée dans cet article se décline en deux étapes principales. Dans la première étape, l'analyse structurelle identifie les éléments des matrices A, B ou C qui sont nécessaires à la validité de la propriété étudiée (cf. Section 2). Une expression logique basée sur l'existence des arcs est fournie puis traduite en une expression d'état des composants. Dans la seconde étape, qui fait l'objet de cette section, nous proposons de construire un modèle dynamique permettant de simuler une multitude de scénarios dans lesquels des événements représentants l'état défaillant des composants essentiels précédents seront générées de façon aléatoire. Ce modèle permettra de quantifier la fiabilité et la disponibilité des propriétés structurelles par la simulation. Ce modèle prendra également en compte des procédures de tolérance aux fautes comme la redondance, le diagnostic et la maintenance.

L'outil de modélisation choisi est les réseaux d'activités stochastiques ou *RAS*. Ce choix se justifie par la capacité de cet outil à modéliser des comportements dynamiques déterministes et aléatoires de façon simple et compacte en comparaison à d'autres outils dynamiques comme les automates.

3.1. Les réseaux d'activités stochastiques (RAS)

Les RAS sont une extension des réseaux de Petri (RdPs) classiques et sont assez proches des réseaux de Petri stochastiques généralisés (*RdPSG*). Ce formalisme a été introduit au milieu des années 80 pour l'évaluation des performances des systèmes complexes (Mogavar, Meyer, 1984).

Cette section donne la définition formelle des *RAS* et les concepts associés (Mogavar, Meyer, 1984).

Définition formelle Un réseau d'activités stochastiques *RAS* est un quintuple $RAS = (RA, \mu_0, C, F, G)$, avec :

1. $RA = (P, A, I, O, \gamma, \tau, \iota, o)$ un réseau d'activité (RA) tel que :

- P est l'ensemble des places et A est l'ensemble des activités qui sont l'équivalent des transitions pour les *RdPs*.

- I est un ensemble fini de portes d'entrée et O un ensemble fini de portes de sortie reliant respectivement des places d'entrée ou de sortie à une activité.

- $\gamma : A \rightarrow Y^*$ est la fonction qui spécifie pour chaque activité $a \in A$ le nombre $\gamma(a)$ de possibilités d'accomplissement de celle-ci appelés *cas de probabilité*.

- $\tau : A \rightarrow \{Temporisée, Immédiate\}$ est une fonction qui spécifie si une activité est temporisée ou immédiate.

- $\iota : I \rightarrow A$ est la fonction qui associe chaque porte d'entrée à une activité via un arc.

- $o : O \rightarrow (a, c) \,|a \in A$ et $c \in \{1, 2, \ldots, \gamma(a)\}$ est la fonction qui associe chaque porte de sortie à un *cas de probabilité* c de l'activité a associée.

2. μ_0 est un marquage initial du réseau pour lequel le RA est stable.

3. $C_a : \mu \times \{1, 2, \ldots, \gamma(a)\} \rightarrow [0, 1]$ est une fonction de distribution de probabilité attribuée aux cas de probabilité c d'une activité a pour un marquage donné μ des places d'entrée et de sortie de l'activité a.

4. $F_a : M_p \times \mathbb{R}^+ \rightarrow [0, 1]$ est la fonction qui affecte pour chaque activité temporisée a et pour un marquage donné $\mu \in M_p$ des places d'entrée de a et, une distribution de probabilité associée à la durée de temporisation $T_a \in \mathbb{R}^+$ de l'activité a.

5. $G_a : M \rightarrow 2^M$ est la fonction de réactivation qui indique l'ensemble des marquages de réactivation d'une activité a valide.

Les RAS sont similaires aux *RdPs* classiques, avec quelques éléments supplémentaires comme les portes d'entrée, les portes de sortie et les places étendues (cf. Figure 2). Ces éléments donnent plus de possibilités dans la modélisation. En effet, les portes permettent de réaliser des opérations plus sophistiquées sur les marquages. Quant aux places étendues, elles sont similaires aux places colorées dans les RdPs colorés (Sanders, Meyer, 2001).

Une porte d'entrée d'une activité se caractérise par deux fonctions : le prédicat et la fonction d'entrée. La fonction de prédicat définit les conditions de marquage de

ses places d'entrée qui valident cette porte et l'activité associée. La fonction d'entrée définit le changement de marquage que subiront les places d'entrée de la porte lorsque l'activité associée se réalise. La porte de sortie se caractérise par une fonction : la fonction de sortie. Cette dernière permet de définir le nouveau marquage des places de sortie de l'activité après sa réalisation.

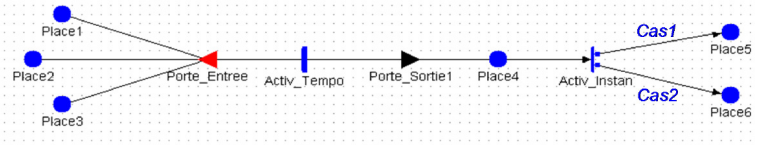


Figure 2. Exemple d'un réseau d'activités stochastiques (RAS)

3.2. Approche de modélisation par les RAS

Comme expliqué précédemment, le but est de construire un modèle *RAS* permettant de simuler l'occurrence aléatoire d'événements e_i, modélisant la suppression d'un arc α_i dans le(s) graphe(s) suite à l'occurrence de défaillances sur certains composants physiques du système. On ne s'intéressera pas à ces défaillances directement, mais plutôt à une des conséquences possibles, ici l'annulation des paramètres associés et impliquant la suppression d'arcs. On suppose qu'une analyse préliminaire du système permettra d'établir ce lien entre les défaillances physiques et leurs conséquences, mais celle-ci ne fait pas l'objet de cet article.

Dans cette section, l'approche de modélisation systématique et modulaire des systèmes tolérants aux fautes par les *RAS* proposée dans (Maza, Petin, 2012) sera utilisée pour l'évaluation de la fiabilité et la disponibilité des propriétés structurelles. Cette approche, adaptée à l'étude actuelle, est décrite ci-après.

3.2.1. Modélisation des composants physiques

Un composant physique C_k à états binaires peut être modélisé par une paire de places $\left(C_k^{Ok}, C_k^{Ko}\right)$ où un jeton dans la place C_k^{Ok} (resp. C_k^{Ko}) signifie que le composant C_k est opérationnel (resp. défaillant) comme indiqué sur la figure 3. Le marquage de ces places vérifie $M(C_k^{Ok}) + M(C_k^{Ko}) \leq 1$ et initialement $M(C_k^{Ok}) = 1$ et $M(C_k^{Ko}) = 0$. Ces deux places sont reliées via une activité temporisée, $Défaillance_k$, dont la temporisation suit par exemple une loi exponentielle de paramètre λ_k qui est le taux de défaillance de C_k. A une date aléatoire tirée selon la loi de distribution de l'activité $Défaillance_k$, le jeton passera de la place C_k^{Ok} à C_k^{Ko} pour modéliser la défaillance. Si le composant est réparable, l'action de maintenance sera modélisée par une autre activité temporisée qui aura pour place de sortie la place C_k^{Ok} dans ce modèle élémentaire. Cette action permet de remettre en service le composant réputé défaillant (jeton dans la place C_k^{Ok}). Dans cet article on s'intéressera aux événements représentant l'annulation des paramètres des matrices de l'équation d'état du système au lieu des défaillances de composants. Ainsi, le module élémentaire de la figure 3

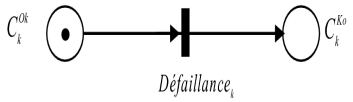


Figure 3. Modélisation d'un composant physique par les RAS

sera utilisé pour modéliser l'occurrence d'un événement e_i représentant l'annulation d'un paramètre α_i dans les matrices A, B ou C (cf. eq. 1). Un tel événement peut avoir lieu suite à la défaillance de certains composants physiques du système. La non-occurrence d'un événement ei est modélisée par la place ei_N et son occurrence par la place ei. Cette dernière est la place de sortie d'une activité temporisée Occ_i modélisant l'instant d'occurrence de e_i. Cette temporisation est aléatoire et peut suivre une distribution de probabilité quelconque.

3.2.2. Modélisation de la redondance matérielle et du diagnostic

Un des intérêts de calculer les éléments qui sont essentiels aux propriétés structurelles est de permettre d'identifier les éléments importants sur lesquels doivent être concentrés les efforts pour préserver au mieux les propriétés. Ces efforts peuvent passer par le choix de composants hautement fiables, ou encore par la mise en place de procédures de tolérance aux fautes comme la redondance matérielle et la reconfiguration.

Pour les procédures de tolérance aux fautes, un composant de secours sera modélisé comme un composant physique ordinaire par une paire de places $\left(P^{Ok}_{Secours}, P^{Ko}_{Secours}\right)$. Toutefois, le marquage initial dépendra de la politique de redondance employée :

- $M_0(P^{Ok}_{Secours}) = 1$ si la redondance est active.
- $M_0(P^{Ok}_{Secours}) = 0$ si la redondance est passive.

Ici on ne modélisera pas les composants physiques de secours directement, mais le paramètre qui leur est associé α'_i et redondant à α_i , ainsi que l'événement e'_i (*i.e.* représentant l'annulation de α'_i). Cet événement sera modélisé de la même manière qu'un composant physique en redondance passive ou active. Celui-ci aura lieu si certains composants de secours sont défaillants et annulent le paramètre associé comme vu dans la section 3.2.1.

La redondance passive nécessite la mise en place d'une procédure de diagnostic permettant de détecter et de localiser le défaut. Ceci permettra d'enclencher une procédure de reconfiguration matérielle (Maza, 2012). Cependant, le diagnostic de défaut peut être imparfait (fausse détection/Manque à la détection) puisqu'il repose sur un ensemble de paramètres tels que le seuil de détection ou les caractéristiques du système. Cela a un impact sur des actions comme la reconfiguration et par voie de conséquence sur la fiabilité et la disponibilité des propriétés structurelles. Ainsi, le diagnostic pourrait être pris en compte du point de vue de ses performances et sa capacité à détecter

correctement un défaut. Celle-ci sera exprimée par une probabilité de bonne détection qu'on notera $TauxD$.

Dans le cas d'une redondance passive avec diagnostic, la performance du diagnostic est modélisée par une activité temporisée représentant l'occurrence de l'événement indésirable et ayant deux cas de probabilité (figure 4) :

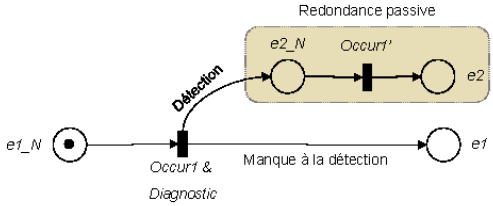


Figure 4. Modules RAS du diagnostic et la reconfiguration

– Le Cas 1 a une probabilité égale à $TauxD$ caractérisant la bonne détection ainsi que la reconfiguration vers l'élément de secours en redondance passive.

– Le Cas 2 modélisera le manque à la détection et l'échec de la reconfiguration avec une probabilité égale à $(1 - TauxD)$.

3.2.3. Modélisation des opérateurs logiques

Les modules *RAS* des différents éléments nécessaires aux propriétés structurelles peuvent être connectés les uns aux autres moyennant des activités et selon des opérateurs logiques de type *ET/OU*. L'opérateur *ET* peut être modélisé par une activité ayant plusieurs places d'entrées. Ainsi, l'activité sera valide uniquement si toutes ses places en amont sont marquées. L'opérateur *OU* peut être modélisé par plusieurs activités ayant chacune une place d'entrée modélisant un événement impliqué dans cette relation logique. L'ensemble de ces activités possède une place de sortie commune qui représente le résultat de cette opération logique. Cette dernière sera marquée dès qu'une des activités précédentes se réalise (figure 5). L'approche de modélisation pro-

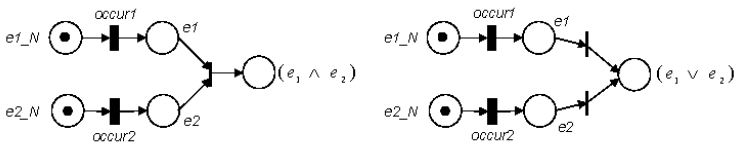


Figure 5. Module RAS des opérateurs logiques ET/OU

posée ici est modulaire et générique. Elle permet une construction aisée et systématique des modèles *RAS*. Elle a une complexité polynomiale puisque le nombre de places et d'activités du modèle est proportionnel au nombre d'éléments essentiels à

la propriété structurelle. Cela représente un avantage significatif par rapport à l'utilisation d'autres formalismes de modélisation tels que les automates et chaînes de Markov. En effet, l'utilisation de ces derniers implique des opérations de composition synchrone entraînant une explosion du nombre d'états par rapport au nombre d'éléments essentiels.

L'approche sera donc utilisée pour développer des modèles *RAS* pour l'évaluation de la fiabilité et la disponibilité des propriétés structurelles. Une simulation de Monte-Carlo du modèle *RAS* permettra l'évaluation quantitative des paramètres de SdF des propriétés structurelles.

La section suivante illustre cette approche de modélisation et d'analyse sur un cas d'étude par simulation.

4. Cas d'étude

Pour ce cas d'étude à vocation illustrative, nous avons choisi un système de positionnement de 4 chariots M1 à M4 modélisé sous la forme d'un système masses-ressorts. La mission du système est l'asservissement de position des 4 chariots. Pour cela, la commandabilité est une propriété nécessaire. Si une défaillance survient (*e.g.* rupture k_1, c_1), il pourrait y avoir en conséquence la perte de la commandabilité et donc impossibilité d'asservir le système. Cela entraîne l'échec de la mission assignée à ce système.

4.1. Description du système

Soit le système masses-ressorts illustré par la figure 6. Ce système est composé de 4 masses M_1, M_2, M_3 et M_4 repérées par leurs positions p_1, p_2, p_3 et p_4 et de valeurs de masse m_1, m_2, m_3 et m_4. Les 4 masses sont reliées en série par 3 ressorts dont les coefficients de raideur sont respectivement k_1, k_2 et k_3 et les coefficients de frottement visqueux sont respectivement c_1, c_2 et c_3. Le système est excité par des forces F_i exercées par des actionneurs (moteurs) A_i et agissant sur M_1, M_3 et M_4. Les positions p_2, p_3 et p_4 sont mesurées par des capteurs S_i. L'analyse de ce système

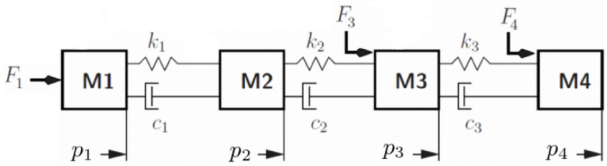


Figure 6. Système masses-ressorts

masses-ressorts permet d'obtenir les équations linéaires suivantes :

$$\begin{cases} m_1\ddot{p}_1 = -k_1p_1 - c_1\dot{p}_1 + k_1p_2 + c_1\dot{p}_2 + A_1F_1 \\ m_2\ddot{p}_2 = k_1p_1 + c_1\dot{p}_1 - (k_1+k_2)p_2 - (c_1+c_2)\dot{p}_2 + k_2p_3 + c_2\dot{p}_3 \\ m_3\ddot{p}_3 = k_2p_2 + c_2\dot{p}_2 - (k_1+k_2)p_3 - (c_1+c_2)\dot{p}_3 + k_3p_4 + c_3\dot{p}_4 + A_2F_3 \\ m_4\ddot{p}_4 = k_3p_3 + c_3\dot{p}_3 - k_3p_4 - c_3\dot{p}_4 + A_3F_4 \end{cases} \tag{9}$$

Dans cette section, nous nous intéressons à l'étude de la commandabilité de ce système linéaire. Ainsi, il n'est pas nécessaire de prendre en compte l'équation de sortie du système. Nous considérons donc le vecteur d'état $X = (p_1, \dot{p}_1, p_2, \dot{p}_2, p_3, \dot{p}_3, p_4, \dot{p}_4)^T = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6, \mathbf{x}_7, \mathbf{x}_8)^T$ et le vecteur d'entrées $U = (F_1, F_3, F_4)^T$ *i.e.* $U = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)^T$. L'équation 9 peut s'écrire sous la forme matricielle :

$$\begin{pmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \\ \dot{x_4} \\ \dot{x_5} \\ \dot{x_6} \\ \dot{x_7} \\ \dot{x_8} \end{pmatrix} = \begin{pmatrix} 0 & \alpha_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha_6 & 0 & 0 & 0 & 0 \\ \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha_{13} & 0 & 0 \\ 0 & 0 & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_{20} \\ 0 & 0 & 0 & 0 & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ \alpha_{25} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \alpha_{26} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \alpha_{27} \end{pmatrix} . \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \tag{10}$$

où les α_i dépendent des paramètres physiques du système *i.e.* m_i, c_i et k_i.

Le graphe orienté représentant ce système, en ne tenant compte que de l'équation de commande (cf. eq. 10) est donné à la figure 7.

4.2. Etude de la commandabilité totale de l'état

Comme présenté dans la section 2, la commandabilité totale de l'état d'un système linéaire nécessite la vérification de deux conditions graphiques élémentaires : conditions de connectivité et de couplage complet. Elle est donnée par l'équation 8.

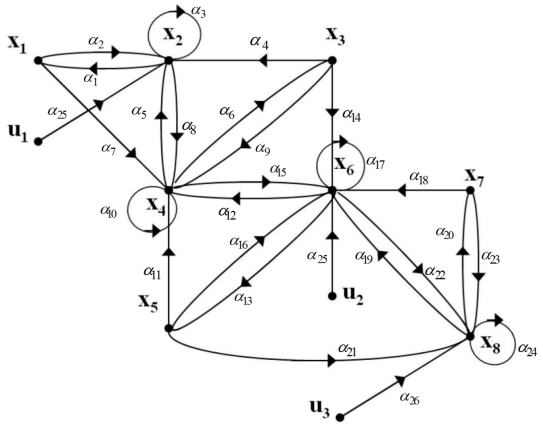


Figure 7. Graphe orienté associé au système pour l'étude de la commandabilité

4.2.1. Condition de connectivité

Pour le calcul de la connectivité $CC(X,U)$, nous utilisons l'approche présentée dans la section 2. La condition de connectivité entre X et U peut s'exprimer de la manière suivante :

$$CC(X,U) = \bigwedge_{\mathbf{x}_i \in X} Con(\mathbf{x}_i) \tag{11}$$

Nous calculons d'abord la connectivité directe $Con_d(\mathbf{x}_i)$ de chaque élément $\mathbf{x}_i \in X$ sachant que pour ce système, tous les éléments $\mathbf{x}_i \in X$ appartiennent à une seule et unique composante fortement connexe. Ainsi, il vient :

$$\begin{array}{ll} Con_d(\mathbf{x_1}) = faux & Con_d(\mathbf{x_5}) = faux \\ Con_d(\mathbf{x_2}) = (\mathbf{u_1}, \mathbf{x_2}) & Con_d(\mathbf{x_6}) = (\mathbf{u_2}, \mathbf{x_6}) \\ Con_d(\mathbf{x_3}) = faux & Con_d(\mathbf{x_7}) = faux \\ Con_d(\mathbf{x_4}) = faux & Con_d(\mathbf{x_8}) = (\mathbf{u_3}, \mathbf{x_8}) \end{array}$$

Le sommet $\mathbf{x}_1$ peut être connecté à U à travers $\mathbf{x}_2$, $\mathbf{x}_3$, $\mathbf{x}_4$, $\mathbf{x}_5$, $\mathbf{x}_6$, $\mathbf{x}_7$ ou $\mathbf{x}_8$. L'expression $Con(\mathbf{x}_1)$ est donc un "OU" logique entre sa connectivité directe $Con_d(\mathbf{x}_1)$ ainsi que les expressions assurant la connectivité entre $\mathbf{x}_1$ et U à travers les différents sommets de sa composante fortement connexe. Par exemple, la connectivité entre $\mathbf{x}_1$ et U à travers $\mathbf{x}_2$ est :

$$\mathbf{x_2} : \ Con_d(\mathbf{x_2}) \wedge (\mathbf{x_2}, \mathbf{x_1})$$

et la connectivité entre $\mathbf{x}_1$ et U à travers $\mathbf{x}_3$ est :

$$\mathbf{x_3} : \ Con_d(\mathbf{x_3}) \vee \Big((\mathbf{x_3}, \mathbf{x_2}) \wedge (\mathbf{x_2}, \mathbf{x_1}) \Big) \vee \Big((\mathbf{x_3}, \mathbf{x_4}) \wedge (\mathbf{x_4}, \mathbf{x_2}) \wedge (\mathbf{x_2}, \mathbf{x_1}) \Big)$$

Cette équation explicite soit une connectivité directe de x_3, soit une connectivité à x_1 à travers x_2, soit la connectivité à x_1 à travers x_4 et x_2.

De cette manière, nous calculons $Con(\mathbf{x_i})$. Selon l'expression 11, la condition $CC(X,U)$ est donnée par :

$$\begin{aligned} CC(X,U) = {} & (\mathbf{x_2},\mathbf{x_1}) \wedge (\mathbf{x_4},\mathbf{x_3}) \wedge (\mathbf{x_6},\mathbf{x_5}) \wedge (\mathbf{x_8},\mathbf{x_7}) \wedge \\ & \Bigg(\Bigg((\mathbf{u_1},\mathbf{x_2}) \wedge (\mathbf{x_2},\mathbf{x_4}) \wedge (\mathbf{u_3},\mathbf{x_8}) \wedge \Big((\mathbf{u_2},\mathbf{x_6}) \vee (\mathbf{x_8},\mathbf{x_6}) \Big) \Bigg) \vee \\ & \Bigg(\Big((\mathbf{u_3},\mathbf{x_8}) \vee (\mathbf{x_6},\mathbf{x_8}) \Big) \wedge \Bigg(\Big((\mathbf{u_1},\mathbf{x_2}) \wedge (\mathbf{u_2},\mathbf{x_6}) \wedge (\mathbf{x_6},\mathbf{x_4}) \Big) \vee \\ & \Big((\mathbf{x_4},\mathbf{x_2}) \wedge (\mathbf{u_2},\mathbf{x_6}) \wedge (\mathbf{x_6},\mathbf{x_4}) \Big) \vee \Big((\mathbf{u_1},\mathbf{x_2}) \wedge (\mathbf{x_2},\mathbf{x_4}) \wedge (\mathbf{x_4},\mathbf{x_6}) \Big) \Bigg) \Bigg) \Bigg) \end{aligned} \tag{12}$$

4.2.2. Condition de couplage complet

Le développement de la condition de couplage complet est effectué sur un graphe biparti. Pour ce système, le graphe biparti associé à ce système pour l'étude de la commandabilité est donné à la figure 8. Dans ce graphe biparti, nous avons 5 composantes

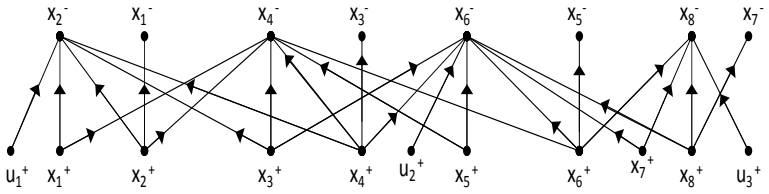


Figure 8. Graphe biparti associé au système

de Dulmage-Mendelson (V_∞, V_1, V_2, V_3, V_4), et plusieurs arcs reliant deux sommets de composantes différentes ne sont pas considérés dans notre étude. Par conséquent, nous considérons le graphe biparti sur la figure 9 avec l'ensemble d'arcs $\mathcal{E}^*$. Calcu-

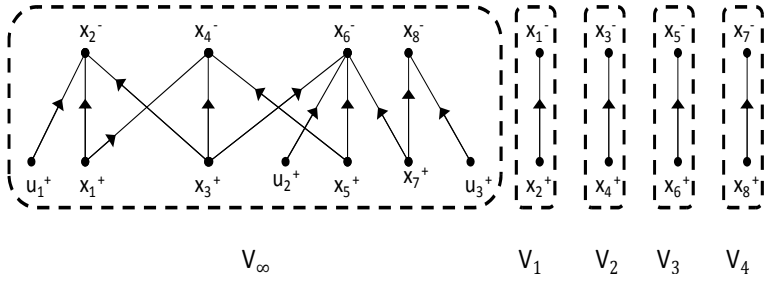


Figure 9. Graphe biparti associé au système après la DM décomposition

lons maintenant l'expression booléenne $MC(X^-, U^+ \cup X^+) = Exp(X^-, \mathcal{E}^*)$. Le

développement de l'expression $Exp(X^-, \mathcal{E}_\mathcal{B})$ peut commencer par la connexion de $\mathbf{x}_8^+$ à V^-. Il vient :

$$Exp(X^-, \mathcal{E}_\mathcal{B}) = \Big((\mathbf{u}_3^+, \mathbf{x}_8^-) \wedge Exp\big(\{\mathbf{x}_1^-, \mathbf{x}_2^-, \mathbf{x}_3^-, \mathbf{x}_4^-, \mathbf{x}_5^-, \mathbf{x}_7^-, \mathbf{x}_8^-\}, \mathcal{E}_\mathcal{B} \setminus \{(\mathbf{u}_3^+, \mathbf{x}_8^-), (\mathbf{x}_7^+, \mathbf{x}_8^-)\}\big)\Big) \vee$$
$$\Big((\mathbf{x}_7^+, \mathbf{x}_8^-) \wedge Exp\big(\{\mathbf{x}_1^-, \mathbf{x}_2^-, \mathbf{x}_3^-, \mathbf{x}_4^-, \mathbf{x}_5^-, \mathbf{x}_6^-, \mathbf{x}_7^-\}, \mathcal{E}_\mathcal{B} \setminus \{(\mathbf{u}_3^+, \mathbf{x}_8^-), (\mathbf{x}_7^+, \mathbf{x}_8^-), (\mathbf{x}_7^+, \mathbf{x}_6^-)\}\big)\Big)$$

REMARQUE 2. — *L'ordre de traitement des sommets $\mathbf{x}_i^-$ est arbitraire. Le résultat final i.e. l'expression booléenne $Exp(X^-, \mathcal{E}_\mathcal{B})$ est toujours la même quelque soit l'ordre de traitement des sommets $\mathbf{x}_i^+$.*

En suivant la récurrence, nous obtenons l'expression booléenne de la condition de lien complet donnée par :

$$\begin{aligned}
&MC(X^-, U^+ \cup X^+) = (\mathbf{x}_2^+, \mathbf{x}_1^-) \wedge (\mathbf{x}_4^+, \mathbf{x}_3^-) \wedge (\mathbf{x}_6^+, \mathbf{x}_5^-) \wedge (\mathbf{x}_8^+, \mathbf{x}_7^-) \\
&\wedge\Bigg(\Bigg(\Big((\mathbf{u}_3^+, \mathbf{x}_8^-) \vee (\mathbf{x}_7^+, \mathbf{x}_8^-)\Big) \wedge \Bigg(\Big((\mathbf{x}_5^+, \mathbf{x}_6^-) \vee (\mathbf{u}_3^+, \mathbf{x}_8^-) \vee (\mathbf{x}_3^+, \mathbf{x}_8^-)\Big) \wedge \\
&\Big((\mathbf{x}_5^+, \mathbf{x}_4^-) \vee (\mathbf{x}_3^+, \mathbf{x}_2^-)\Big) \wedge \Big((\mathbf{u}_1^+, \mathbf{x}_2^-) \vee (\mathbf{x}_1^+, \mathbf{x}_2^-) \vee (\mathbf{x}_3^+, \mathbf{x}_2^-)\Big)\Bigg) \vee \\
&\Big(\Big((\mathbf{u}_2^+, \mathbf{x}_6^-) \wedge (\mathbf{x}_3^+, \mathbf{x}_4^-)\Big) \wedge \Big((\mathbf{u}_1^+, \mathbf{x}_2^-) \vee (\mathbf{x}_1^+, \mathbf{x}_2^-)\Big)\Big) \vee \\
&\Big((\mathbf{x}_1^+, \mathbf{x}_4^-) \wedge \Big((\mathbf{u}_1^+, \mathbf{x}_2^-) \vee (\mathbf{x}_3^+, \mathbf{x}_2^-)\Big) \wedge \Big((\mathbf{x}_3^+, \mathbf{x}_6^-) \vee (\mathbf{u}_2^+, \mathbf{x}_6^-)\Big)\Big)\Bigg)\Bigg)
\end{aligned} \tag{13}$$

À partir des équations 12 et 13, nous pouvons écrire l'expression de Cmd selon l'équation 8. Il vient :

$$\begin{aligned}
&Cmd = (\mathbf{x}_2, \mathbf{x}_1) \wedge (\mathbf{x}_4, \mathbf{x}_3) \wedge (\mathbf{x}_6, \mathbf{x}_5) \wedge (\mathbf{x}_8, \mathbf{x}_7) \wedge (\mathbf{u}_3, \mathbf{x}_8) \wedge (\mathbf{u}_1, \mathbf{x}_2) \\
&\wedge(\mathbf{x}_1, \mathbf{x}_4) \wedge \Big((\mathbf{u}_2, \mathbf{x}_6) \vee (\mathbf{x}_7, \mathbf{x}_6)\Big)
\end{aligned} \tag{14}$$

Les arcs de l'expression Cmd peuvent liés aux paramètres α_i des matrices A et B et aux composants physiques assurant ce lien. Ainsi, il vient :

$$Cmd = \alpha_1 \wedge \alpha_6 \wedge \alpha_{13} \wedge \alpha_{20} \wedge \alpha_{27} \wedge \alpha_{25} \wedge \alpha_7 \wedge \Big(\alpha_{26} \vee \alpha_{18}\Big) \tag{15}$$

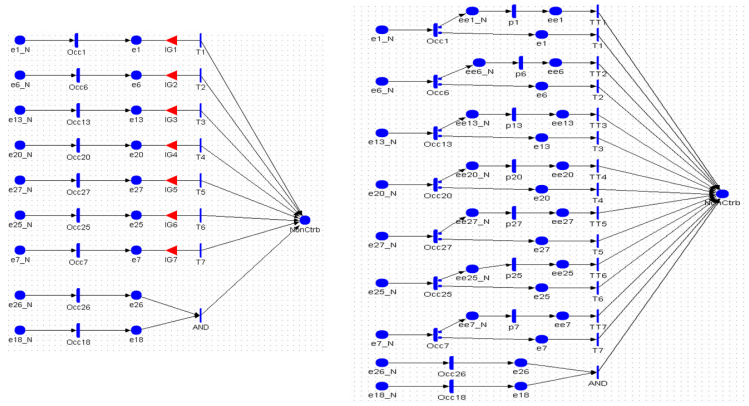
Cette dernière expression permet l'étude des paramètres de sûreté de fonctionnement de cette propriété structurelle.

4.3. Analyse de la sûreté de fonctionnement

Plusieurs modèles *RAS* ont été développés afin d'étudier la fiabilité et la disponibilité de la commandabilité en intégrant aussi bien les redondances matérielles que les

performances du diagnostic. Deux modèles *RAS* permettant l'analyse de la fiabilité sont donnés à la figure 10.

Le premier (figure 10.a) permet d'évaluer la fiabilité de la commandabilité par la simulation. Quant au second (figure 10.b), il prend en compte en plus la redondance passive et le diagnostic de défaut (cf. section 3.2.2). La place $NonCtrb$ modélise la perte de la commandabilité suite à l'occurrence de certains événements. Tous les modèles RAS sont développés sur la plateforme logiciel *Mobius*.



(a) Système avec sa structure de base (b) Système avec une structure redondante et diagnostic

Figure 10. Modèles RAS pour l'évaluation de la fiabilité de la commandabilité

L'hypothèse est faite que l'occurrence de chaque événement e_i modélisant l'annulation d'un paramètre α_i suit une loi de distribution exponentielle de paramètre λ_i, dont les valeurs sont reportées dans la Tableau 1.

Tableau 1. Taux de défaillances associées aux éléments essentiels à la commandabilité

Taux	λ_1	λ_6	λ_{13}	λ_{20}	λ_{27}
Val. en $(u.t)^{-1}$	10^{-4}	2.10^{-4}	3.10^{-4}	4.10^{-4}	2.10^{-4}
Taux	λ_{25}	λ_7	λ_{26}	λ_{18}	
Val. en $(u.t)^{-1}$	3.10^{-4}	2.10^{-4}	8.10^{-4}	9.10^{-4}	

Des simulations de Monte-Carlo (MC) sont conduites sur les modèles *RAS* (cf. figure 10) afin de faire une évaluation quantitative de la sûreté de fonctionnement de la propriété de commandabilité du système.

Le principe des simulations MC en sûreté de fonctionnement consiste à simuler un grand nombre de fois le comportement dynamique des composants d'un système, afin d'évaluer ses paramètres FMDS (Lasnier, 2011). La simulation d'un scénario possible est appelée une histoire. Plus le nombre d'histoires simulées est grand, meilleure sera la précision des résultats. Deux critères d'arrêt sont possibles : le nombre maximal N_{max} d'histoires à simuler et la précision atteinte par les résultats des simulations.

Cette précision s'exprime par un intervalle de confiance et un niveau de confiance. Le niveau de confiance donne la probabilité désirée pour que la valeur exacte de la variable mesurée soit à l'intérieur de l'intervalle de confiance autour de la valeur estimée. Ici, le nombre maximal d'histoires simulées est 50 000 avec un niveau de confiance 99 % et intervalle de confiance de ± 5 %. Cela signifie que 99 % des résultats obtenus doivent être contenus dans l'intervalle ± 5 % autour de leur valeur moyenne.

4.4. Etude de la fiabilité de la commandabilité

4.4.1. Comparaison calcul théorique et par la simulation

La fiabilité de la commandabilité sur un horizon de fonctionnement de 3 500 *unités de temps* (*ut*) évaluée par la simulation et par le calcul exact sont illustrées à la figure 11. Celle-ci indique que les deux courbes sont confondues ce qui montre la bonne précision du calcul par la simulation *MC*.

L'observation de la courbe de la fiabilité montre que celle-ci décroît très vite avec le temps. En effet, à l'instant $t = 500$ $u.t$, la fiabilité de la commandabilité est d'environ 38 % seulement. C'est-à-dire qu'au bout d'un temps de mission égale à un cinquième du temps de mission globale, il y a une probabilité de 62 % que le système devienne non contrôlable. Ce qui est, par hypothèse, nécessaire à sa mission. En conséquence, la perte de controllabilité entraîne la défaillance du système. Si le système a

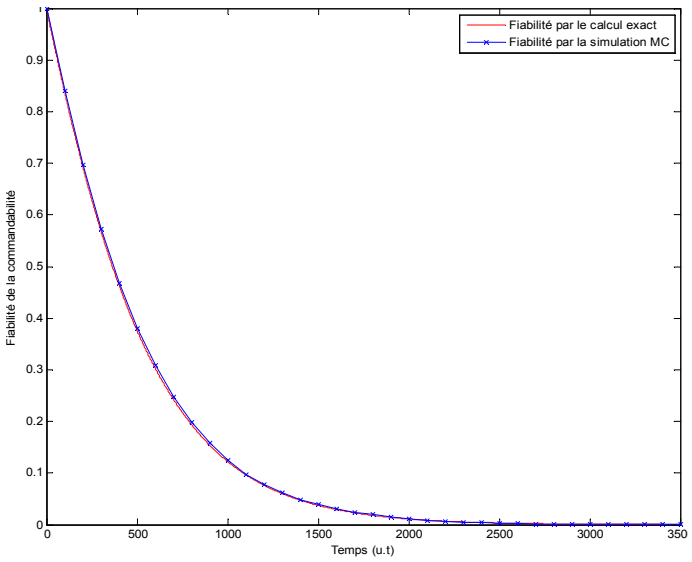


Figure 11. Evolution de la fiabilité de la commandabilité en fonction du temps

un temps de mission supérieur à 500 $u.t$, il est indispensable d'envisager des procédures de fiabilisation des éléments essentiels à la commandabilité. Ceci pourrait se faire en prévoyant des composants en redondance par exemple.

4.4.2. Impact de la redondance

La redondance matérielle consiste à mettre en place des composants de secours. Ceux-ci peuvent être en redondance active, *i.e.* qu'ils fonctionnent en même temps que les composants principaux, ou en redondance passive *i.e.* en attente. Dans ce dernier cas, ils seront sollicités suite à une opération de reconfiguration par exemple lorsqu'une défaillance est détectée. On peut chercher à vérifier quelle politique de redondance améliore vraiment la fiabilité et de combien celle-ci est améliorée par rapport à une structure non redondante.

Pour notre étude, les deux types de redondance ont été modélisés à des fins de comparaison. Les éléments redondants sont supposés avoir les mêmes caractéristiques fiabilistes que les éléments principaux qu'ils redondent. La fiabilité pour chaque type de redondance est illustrée à la figure 12. Au vu de ces résultats, il est clair que l'amé-

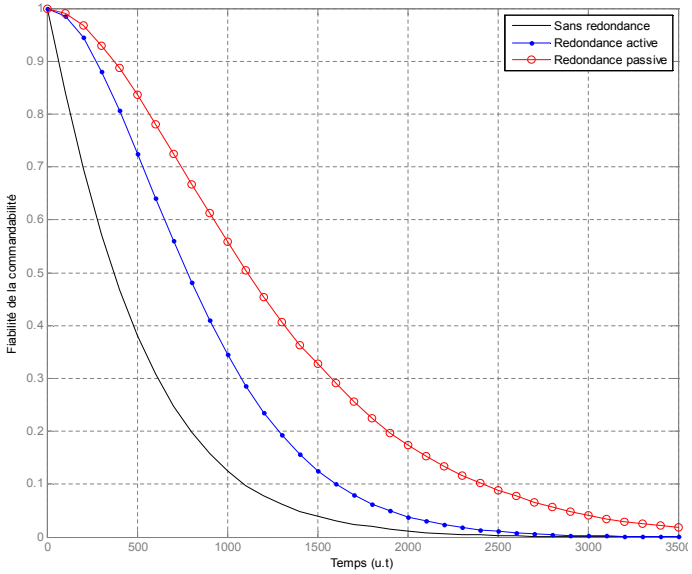


Figure 12. Evolution de la fiabilité de la commandabilité en fonction du temps et de la politique de redondance

lioration est apportée par une redondance matérielle sur les éléments essentiels à la commandabilité. En effet, à l'instant $500\ u.t$ par exemple, la fiabilité est doublée puisqu'elle vaut 0,72 lorsqu'une redondance active est employée et 0,84 si redondance passive. Ce résultat est conforme à l'attendu usuel. La figure 12 montre également que la politique de redondance passive est la meilleure notamment lorsque la durée de mission est plus élevée ($\approx 1500\ ut$).

Ce résultat s'explique par le fait que les éléments redondants qui fonctionnent en même temps que leurs éléments principaux peuvent tomber en panne aussi souvent que ces derniers contrairement à la redondance passive. Pour cette dernière, ils ne seront sollicités que dans le cas où l'élément principal est défaillant. Cela suppose

donc la possibilité de détecter les défaillances sur les éléments principaux essentiels à la commandabilité et que leur mise en fonctionnement ne soit pas un vecteur de panne.

4.4.3. Impact du diagnostic

Dans le paragraphe précédent, il a été supposé que la reconfiguration matérielle se faisait avec succès dès qu'un élément principal est défaillant. Ceci suppose qu'une fonction de diagnostic permet de détecter et de localiser les défaillances pour que la reconfiguration matérielle soit possible. Or, la fonction de diagnostic n'est généralement pas parfaite.

La figure 13 montre les résultats pour la fiabilité de la commandabilité pour différentes valeurs de la probabilité de bonne détection $TauxD$ du système de diagnostic. Ces résultats montrent clairement que la fiabilité décroît avec la probabilité de bonne détection. En effet, en pratique, la détection ne se fait pas toujours avec succès et au bon moment, car cela dépend de plusieurs facteurs (Maza, Petin, 2012). La fiabilité reste cependant meilleure que celle obtenue avec une structure non redondante. Pour

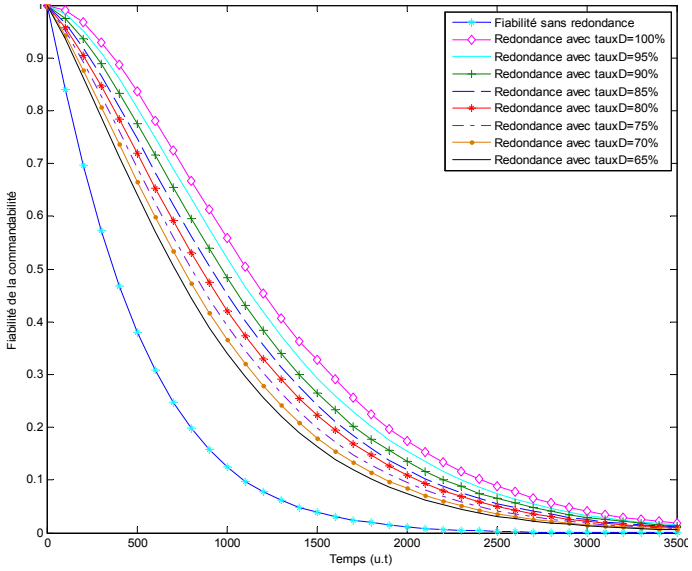


Figure 13. Impact du diagnostic et de la redondance passive sur la fiabilité de la commandabilité

décider quelle politique de redondance choisir, il faut comparer les deux politiques en incluant explicitement les performances du diagnostic. En effet, l'hypothèse consistant à supposer que la détection et la reconfiguration se font avec certitude et instantanément est optimiste. Elle constitue la borne supérieure sur la fiabilité qu'il est possible d'obtenir avec une redondance de degré 1 (*i.e.* un seul élément de secours).

4.5. Analyse de la disponibilité de la commandabilité

Supposons maintenant que le système soit réparable et qu'une opération de maintenance corrective soit prévue à chaque fois que le système perd sa propriété de commandabilité. La figure 14 donne la valeur de la disponibilité instantanée de la commandabilité en fonction du temps pour un système sans et avec redondance passive. Les performances du diagnostic y sont également incluses.

L'analyse de la figure 14 montre aussi l'amélioration apportée par l'action de maintenance. En effet, plus le taux de bonne détection est élevé, plus des actions de maintenance seront entreprises sur les composants défaillants afin de les remettre en service, pendant que les composants redondants prennent le relais. Cela améliore la disponibilité de l'ensemble. Il est à noter que nous n'avons pas introduit, pour des raisons de clarté, d'autres paramètres comme l'efficacité de la maintenance ou les différents taux de diagnostic mais ceux-ci peuvent être intégrés facilement (Maza, 2015).

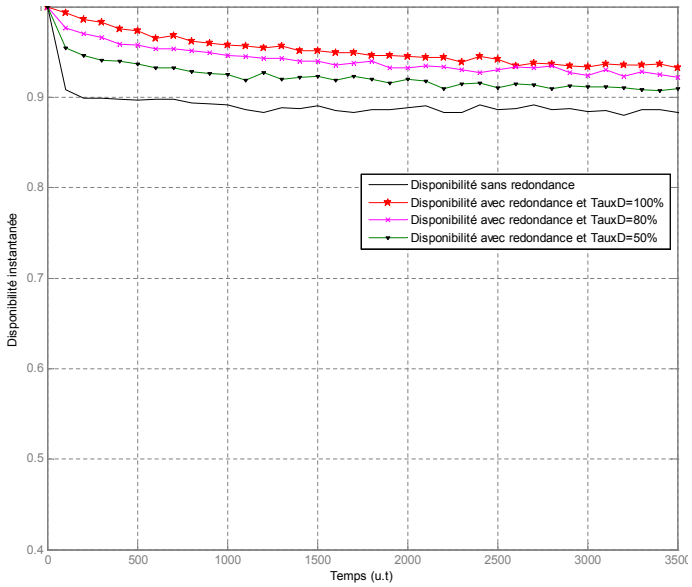


Figure 14. Impact du diagnostic et de la redondance passive sur la disponibilité instantanée de la commandabilité

5. Conclusion

Dans cet article nous avons développé un continuum entre l'analyse des systèmes continus et notamment de leurs propriétés et l'analyse des systèmes à événements discrets liés aux défaillances. La connaissance physique des systèmes continus nous permet de représenter sa structure par un graphe dit structurel qui traduit la causalité des variables physiques.

L'analyse de ce graphe permet de déterminer les conditions graphiques de satisfaction de propriétés nécessaires pour l'usage des systèmes continus comme la commandabilité, l'observabilité, etc. Par la connaissance de la relation entre les variables physiques et les composants assurant cette relation, il est possible de donner automatiquement les conditions de maintien de ces propriétés attendues sans en connaître le dimensionnement. Ainsi, cette analyse peut être réalisée au plus tôt dans la phase de conception.

L'identification des éléments essentiels pour la satisfaction des propriétés permet l'analyse des propriétés de sûreté de fonctionnement des systèmes continus et de planifier toute action nécessaire pour le maintien des propriétés selon les attentes du client (fiabilité, tolérance aux défaillances, disponibilité, maintenance, etc).

Plusieurs paramètres de SdF peuvent être évalués pour un ensemble de propriétés structurelles selon l'exigence du client. Ainsi, la méthodologie proposée a l'avantage d'être modulaire et générique. Elle permet l'analyse de différents paramètres de SdF et différentes propriétés structurelles. Elle permet également de prendre en compte des procédures de tolérance aux fautes mises en place comme le diagnostic et la reconfiguration.

L'analyse des paramètres de sûreté de fonctionnement par les réseaux d'activités stochastiques est ici particulièrement intéressante, car elle exploite directement les résultats de l'analyse structurelle. Le modèle RAS est alors construit de manière systématique et permet l'étude de nombreux paramètres de la sûreté de fonctionnement sur la base du même modèle élémentaire.

Contrairement à des modèles markoviens, la construction des modèles RAS proposés dans cet article a une complexité polynomiale proportionnellement au nombre de composants essentiels aux propriétés étudiées.

Étant donné que l'approche d'analyse structurelle a également une complexité po-lynomiale, le couplage entre ces approches continues et systèmes à évènements discrets (SED) présentées dans cet article est particulièrement adapté à l'étude des sys-tèmes complexes et de grande dimension.

Ce travail liant l'analyse structurelle et l'analyse fiabiliste doit être poursuivi par la construction des liens directs entre la défaillance des composants et des paramètres α des équations d'état. Par ailleurs, d'autres paramètres de sûreté de fonctionnement pourraient être étudiés. Enfin, la méthodologie étant générique et de complexité polynomiale, un passage à l'échelle est une perspective d'intérêt.

Bibliographie

Basile G., Marro G. (1969). On observability of linear time-invariant systems with unknown inputs. *Journal of Optimization Theory and Applications*, vol. 3, n° 6, p. 410-415.

Boukhobza T., Hamelin F., Simon C. (2014). Partial state observability recovering for linear systems by additional sensor implementation. *Automatica*, vol. 50(3), p. 858-863.

Cassandras C. G., Lafortune S. (2007). *Introduction to discrete event systems* (2nd éd.; Springer-Verlag, Ed.). New-York, USA.

Dakil M. (2014). *Développement d'une méthodologie conjointe d'analyse structurelle et de sûreté de fonctionnement des propriétés d'un système complexe*. Thèse de doctorat, Université de Lorraine, Université de Lorraine.

Dion J.-M., Commault C., van der Woude J. (2003). Generic properties and control of linear structured systems: A survey. *Automatica*, vol. 39, n° 7, p. 1125-1144.

Dulmage A. L., Mendelsohn N. S. (1958). Coverings of bipartite graphs. *Canadian Journal of Mathematics*, vol. 10, p. 517-534.

Hautus M. (1983). Strong detectability and observers. *Linear Algebra and its Applications*, vol. 50, p. 353-360.

IEC. (1998). *Iec61508:Functional safety of Electrical/Electronic/Programmable electronic safety-related systems.* (International Electrotechnical Commission, London, UK)

Kalman R. E. (1968). Lectures on controllability and observability. In *Proceedings of c.i.m.e. (international mathematical summer center).* Bologna, Italy.

Lasnier G. (2011). Sûreté de fonctionnement des équipements et calculs de fiabilité. *Lavoisier, Paris.*.

Maza S. (2012). Dynamic modeling and simulation of fault tolerant systems based on stochastic activity networks. *Proc IMechE Part O: Journal of Risk and Reliability*, vol. 226, p. 455-463.

Maza S. (2015). Diagnosis modelling for the dependability assessment of fault-tolerant systems based on stochastic activity networks. *Quality and Reliability Engineering International.*, vol. 31, n° 6, p. 963-976.

Maza S., Petin J.-F. (2012). Evaluation de la disponibilité d'un système tolérant aux fautes à l'aide des réseaux d'activités stochastiques. *Congrés Lambda Mu'12, Tours, France*.

Maza S., Simon C., Boukhobza T. (2012). The impact of actuator failures on the structural controllability of linear systems: A graph theoretical approach. *I.E.T. Control Theory & Applications*, vol. 6, p. 412-419.

Mogavar A., Meyer J. (1984). Performability modeling with stochastic activity network. *In proceeding of real-time systems symposium, pp.215-224, Austin TX, USA*.

Murota K. (1987). Refined study on structural controllability of descriptor systems by means of matroids. *SIAM Journal of Control and Optimization*, vol. 25, n° 4, p. 967-989.

Prowell.S.J, Poore.J.H. (2004). Computing system reliability using markov chain usage models. *The Journal of Systems and Software*, p. 219 - 225.

Ruin T. (2013). *Contribution à la quantification des programmes de maintenance complexes*. Thèse de doctorat non publiée, Université de Lorraine.

Sanders W., Meyer J. (2001). Stochastic activity networks: Formal definitions and concepts. In E. Brinksma, H. Hermanns, J.-P. Katoen (Eds.), *Lectures on formal methods and performanceanalysis*, vol. 2090, p. 315-343. Springer Berlin Heidelberg.

Staley J., Sutcliffe P. (1974). Reliability block diagram analysis. *Microelectronics Reliability*, vol. 13(1), p. 33-47.

Villemeur A. (1992). *Reliability, availability, maintainability and safety assessment: methods and techniques* (Wiley, Ed.). Transleted from French Edition by A. Cartier and M.C. Lartisien.

Article soumis le 28 juin 2015
Accepté le 7 octobre 2015