

Evaluation de la Sûreté de Fonctionnement de systèmes complexes et optimisation des architectures

André Cabarbaye

CAB INNOVATION

3, rue de la Coquille

31500 Toulouse

Tél. 05 61 54 68 08

Andre.Cabarbaye@cabinnovation.fr

Roland Laulheret

Centre National d'Etudes Spatiales (CNES)

18 avenue Edouard Belin

31401 Toulouse Cedex 4

Tél. 05 61 27 47 19

Roland.laulheret@cnes.fr

Mots-clés : disponibilité, fiabilité, Markov, arbre de causes, Monte-Carlo, modélisation, optimisation, maintenance.

RESUME :

Après avoir rappelé les enjeux de l'optimisation vis-à-vis de la Sûreté de Fonctionnement, cet article présente une méthode originale d'évaluation et d'optimisation de systèmes complexes, caractérisés par une interdépendance entre leurs divers constituants. Cette méthode hybride fait appel à diverses techniques existantes (arbre des causes, traitements markoviens, simulation de Monte-Carlo) pour résoudre des problématiques relativement complexes issues du domaine spatial (satellites et centres de contrôle). Supporté par les outils de la société CAB INNOVATION, la modélisation reste accessible à des concepteurs non spécialisés, en étant en grande partie automatisée, et l'évaluation est suffisamment rapide pour permettre un couplage direct avec des techniques de recherche de l'optimum global (Algorithmes Génétiques et simplexe non linéaire) selon un critère défini par l'utilisateur (maximisation de la disponibilité du service rendu au meilleur coût).

Introduction

L'optimisation de l'architecture, de la mise en oeuvre et de la maintenance des systèmes, en regard de la disponibilité du service rendu à l'utilisateur, recouvre des enjeux souvent considérables. Suivant la problématique rencontrée, l'objectif recherché peut consister à minimiser le coût global de possession (acquisition, exploitation, maintenance...) tout en respectant un objectif de disponibilité, maximiser la disponibilité dans une enveloppe de coût donné ou respecter un critère élaboré à partir de ces différents résultats.

Cette optimisation résulte de choix multiples portant notamment sur :

- la répartition des fonctions du système dans des constituants de diverses natures,
- la fiabilité des constituants qui dépend des technologies mises en oeuvre et de la qualité des composants utilisés,
- les taux d'utilisation,

- les redondances éventuelles et les caractéristiques de celle-ci,
- l'existence d'éventuels modes de fonctionnement dégradés,
- la durée des reconfigurations,

et pour les éléments réparables :

- la durée des réparations sur site ou via un retour en usine,
- l'utilisation éventuelle et le dimensionnement de lots de rechange sur site,
- etc.

L'évaluation de la disponibilité peut être menée par diverses méthodes de modélisation (Bloc Diagramme de Fiabilité, graphe de Markov, réseau de Petri...) et de traitement (calcul analytique, traitement markovien, simulation de Monte-Carlo...). Mais dans un contexte industriel, cette évaluation est fortement contrainte par sa durée, qui couvre la modélisation par l'analyste et le traitement informatique, et par la justesse des résultats attendus. En effet l'évaluation s'inscrit souvent dans le cadre d'une activité d'ingénierie concurrente ou de réponse à appel d'offre et les entreprises sont de plus en plus directement concernées par le bon fonctionnement de leurs produits en exploitation par le jeu de mécanismes contractuels d'intéressement ou de pénalité. Cette évaluation doit, par ailleurs, être d'autant plus courte qu'elle s'inscrit dans un processus d'optimisation de la conception et non pas de simple vérification de la tenue d'allocation ou d'objectif.

1 - Problématiques :

C'est dans un tel cadre que le CNES est confronté à deux types de problématique d'évaluation et d'optimisation :

- Les satellites qui sont des systèmes non réparables mais reconfigurables en utilisant des redondances embarquées ou en entrant dans des modes de fonctionnement dégradés.
- Les moyens au sol (station de réception, centre de contrôle ou d'exploitation, réseau de télécommunication...) qui sont des systèmes reconfigurables et réparables.

Indépendamment de leur taille (de l'ordre d'une centaine d'équipements différents), ces deux types de systèmes peuvent être qualifiés de complexes dans la mesure où ils sont constitués d'éléments interdépendants. Les caractéristiques stochastiques (taux de défaillance...) d'un élément en redondance froide seront par exemple conditionnées (passage à l'état OFF ou ON) par l'état des éléments nominaux (en fonctionnement ou en panne). De même les caractéristiques de maintenance d'un élément (durée de réparation...) pourront être affectées par l'état plus ou moins dégradé des autres éléments en raison d'un partage de ressources (stocks de rechanges, équipes de maintenance...).

2 – Cadre méthodologique :

Sur le plan méthodologique, deux principaux critères sont à retenir dans ce contexte :

- la modélisation doit pouvoir être validée par les concepteurs, en étant si possible accessible à des non-spécialistes,
- la durée d'évaluation doit être compatible avec la recherche d'une configuration optimale d'architecture.

Cette optimisation peut s'opérer par des analyses de sensibilité menées individuellement sur chacun des paramètres. Mais celles-ci montrent vite leurs limites quand les variables sont nombreuses et les optima multiples. Il devient alors nécessaire de coupler l'évaluation à des techniques d'optimisation automatisées, issues des domaines de la recherche opérationnelle et de l'intelligence artificielle.

Dans ce schéma, la simulation de Monte-Carlo conduit à des durées souvent rédhibitoires.

Les traitements markoviens présentent des avantages significatifs, en terme de temps de calcul et de précision, par rapport aux techniques de simulation, même s'ils sont limités par l'explosion combinatoire. Cependant la modélisation sous forme de graphe de Markov est relativement complexe et ne peut être réellement mise en œuvre que par des spécialistes.

La modélisation par arbre d'événements est particulièrement simple et conduit à des traitements analytiques rapides. Mais elle présente un caractère statique incompatible avec la prise en compte de la complexité (dépendances stochastiques).

Supportée par les outils de la société CAB INNOVATION (SUPERCAB : traitements markoviens, CABTREE : arbre de causes, GENCAB : optimisation et SIMCAB : simulation), une hybridation de ces diverses méthodes a permis cependant de traiter l'essentiel des problématiques rencontrées.

3 – Les méthodes utilisées :

Le principe d'évaluation et d'optimisation retenu est fondé sur :

- le couplage entre des arbres de causes et des traitements markoviens,
- l'utilisation de modèles markoviens génériques (redondance M parmi N) et d'un outil de modélisation automatique,
- le couplage entre des outils d'évaluation et d'optimisation (Algorithmes génétiques et simplexe non linéaire).
- le couplage entre des outils d'évaluation et de simulation (Monte-Carlo) pour rendre compte des dispersions sur les résultats.

3.1 - Traitement de la complexité

La prise en compte de la complexité dans l'absolu apparaît aujourd'hui insoluble. En effet les dépendances stochastiques entre constituants d'un système ne peuvent pas être considérées dans les arbres de défaillances. S'ils sont modélisables par graphe de Markov, c'est seulement pour des systèmes de faible dimension en raison de l'explosion combinatoire (2^n états pour n éléments en bon fonctionnement ou en panne). Ils peuvent être traités par simulation mais la durée de celle-ci peut être élevée. Cependant l'étude des systèmes réels permet d'observer une complexité généralement localisée, les systèmes étant le plus souvent constitués de sous-ensembles indépendants composés eux-mêmes d'éléments interdépendants. Le couplage entre un outil d'arbres d'événements (CABTREE), pour décrire le fonctionnement du système à partir de celui de ses sous-ensembles, et un outil markovien (SUPERCAB), pour modéliser le comportement de ces derniers, permet alors de traiter un grand nombre de problèmes dont l'essentiel de ceux que le CNES doit résoudre. Ce couplage est illustré par l'exemple de la figure 1.

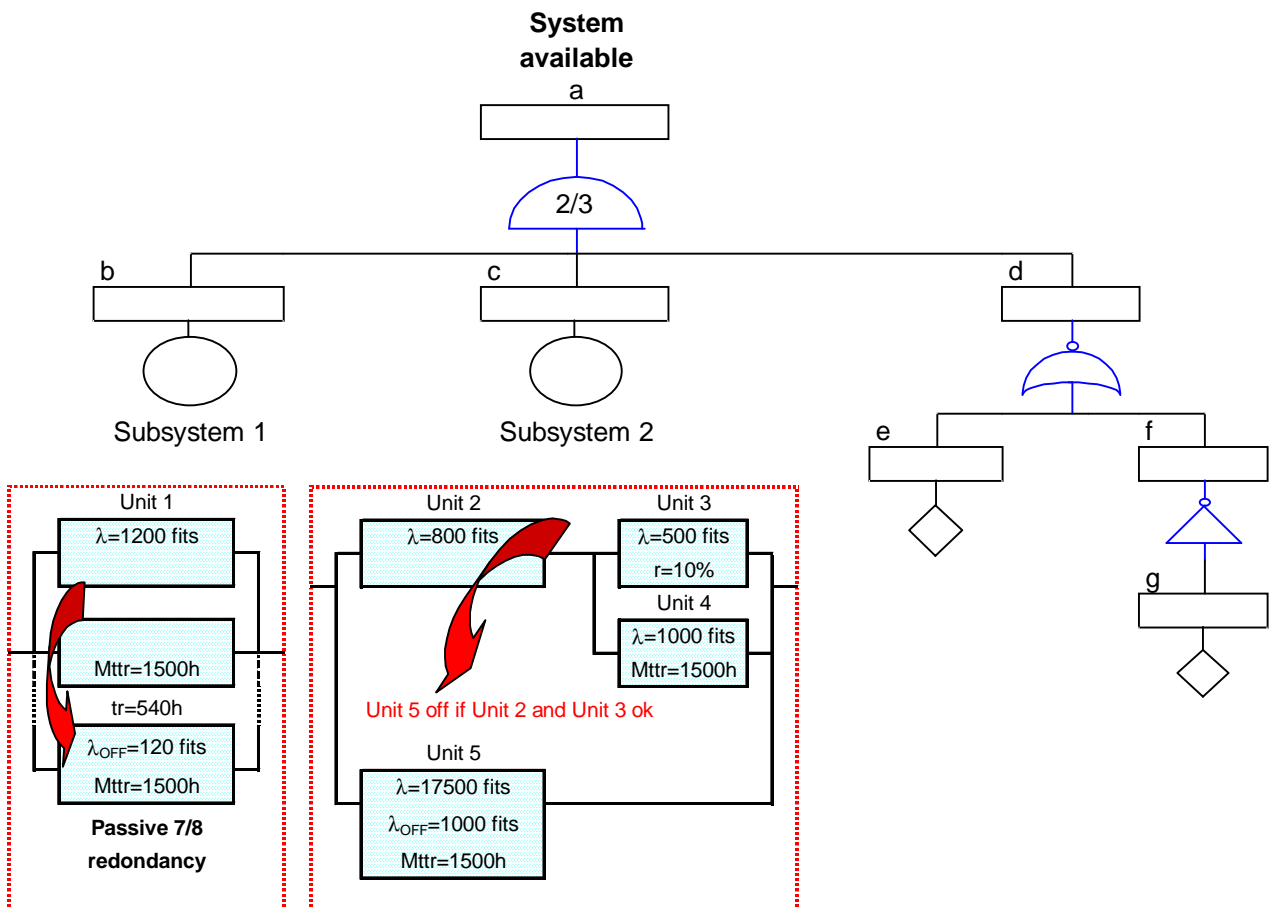


Figure 1 . Couplage entre arbre des causes et traitements markoviens

3.2 - La modélisation markovienne automatisée

La modélisation sous forme de graphe de Markov est longue, fastidieuse et relativement complexe. Aussi, le risque d'erreur est non négligeable, surtout si la modélisation est réalisée par un concepteur non spécialisé. C'est pourquoi l'outil SUPERCAB intègre un modèle générique de redondance M parmi N et une fonction originale de génération automatique de modèles markoviens.

3.2.1 - Modèles de redondance M parmi N

Le principe mis en oeuvre par l'outil consiste à générer puis traiter (en régime transitoire ou stationnaire) une matrice de Markov à partir d'une fonction paramétrique comme le montre la figure 2.

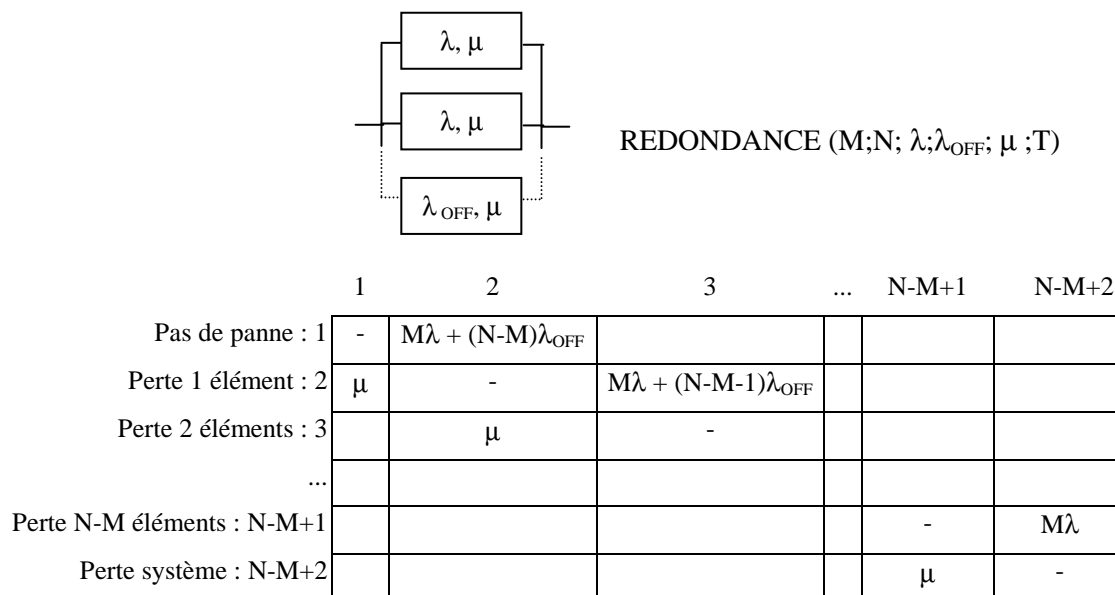


Figure 2 . Redondance froide M parmi N d'éléments réparables (1 réparateur)

Un modèle plus générique a été établi afin de traiter tous les types de redondances rencontrés relatifs à des systèmes réparables (stations au sol) ou reconfigurables (satellites). Celui-ci permet notamment de prendre en compte un taux de défaillance à l'état ON (λ) et à l'état OFF (λ_{OFF}), une probabilité d'échec à la sollicitation (γ), une durée moyenne de reconfiguration pendant laquelle le système est indisponible (MDT_s) et une durée moyenne de remise en état d'un élément après panne (MDT_l). Ces temps pouvant être modélisés par des taux (μ_i) ou par des lois d'Erlang simple à k_i états fictifs. Différentes politiques de maintenance peuvent être considérées avec 1 ou n réparateurs, ou un temps de remise en état du système complet indépendant du nombre d'éléments à réparer.

$$\text{REDONDANCE (M;N; } \lambda; \lambda_{OFF}; \gamma; T; \text{MDT}_l; k_l; \text{Type}_l; \text{MDT}_s; k_s; \text{Type}_s; R)$$

Cette fonction paramétrique renvoie une valeur de disponibilité (à t ou l'infini) ou une valeur de fiabilité en considérant la perte du système comme un état absorbant.

Si le système n'est pas indisponible pendant les reconfigurations, cette fonction est traitée par construction de la matrice de Markov de la figure 3 de dimension $N-M+2$.

	1	2	3	4	...	N-M+1	N-M+2
Pas de panne : 1	-	$M\lambda(1-\gamma) + (N-M)\lambda^*$	$M\lambda\gamma(1-\gamma)$	$M\lambda\gamma^2(1-\gamma)$		$M\lambda\gamma^{N-M-1}(1-\gamma)$	$M\lambda\gamma^{N-M}$
Perte 1 élément : 2	μl_1	-	$M\lambda(1-\gamma) + (N-M-1)\lambda^*$	$M\lambda\gamma(1-\gamma)$		$M\lambda\gamma^{N-M-2}(1-\gamma)$	$M\lambda\gamma^{N-M-1}$
Perte 2 éléments : 3	$\mu l'$	μl_2	-	$M\lambda(1-\gamma) + (N-M-2)\lambda^*$		$M\lambda\gamma^{N-M-3}(1-\gamma)$	$M\lambda\gamma^{N-M-2}$
Perte 3 éléments : 4	$\mu l''$		μl_3	-		$M\lambda\gamma^{N-M-4}(1-\gamma)$	$M\lambda\gamma^{N-M-3}$
...							
Perte N-M éléments : N-M+1	$\mu l''$					-	$M\lambda$
Perte système : N-M+2	$\mu l'''$					μl_{N-M+1}	-

Figure 3 . Redondance M parmi N (système disponible pendant les reconfigurations)

Si le système est indisponible pendant les reconfigurations, cette fonction est traitée par construction de la matrice de Markov de la figure 4 de dimension $2(N-M)+2$.

	1	2	3	4	5	6	...	$2(N-M)+2$
Pas de panne : 1	-	$M\lambda$	$(N-M)\lambda^*$					
Reconfiguration : 2	μl_2	-	$\text{tr}(1-\gamma)$	$\text{tr}\gamma + (M-1)\lambda + (N-M)\lambda^*$				
Perte 1 élément : 3	μl_1		-	$M\lambda$	$(N-M-1)\lambda^*$			
Reconfiguration : 4			μl_2	-	$\text{tr}(1-\gamma)$	$\text{tr}\gamma + (M-1)\lambda + (N-M-1)\lambda^*$		
Perte 2 éléments : 5			μl_1		-	$M\lambda$		
Reconfiguration : 6						-		
...								
Reconfiguration : $2(N-M)$								$\text{tr}\gamma + (M-1)\lambda + \lambda^*$
Perte N-M éléments : $2(N-M)+1$								$M\lambda$
Perte système : $2(N-M)+2$								-

Type_1 = 1 : 1 réparateur ($\mu l_i = \mu l$, $\mu l' = \mu l'' = 0$)

Type_1 = 2 : n réparateurs ($\mu l_i = i * \mu l$, $\mu l' = \mu l'' = 0$)

Type_1 = 3 : durée réparation indépendante du nombre d'éléments en cause ($\mu l_i = 0$, $\mu l' = \mu l$, $\mu l'' = \mu l$ si R = Faux)

Type_s = Vrai : remise en état pendant la reconfiguration

R = Vrai (fiabilité) entraîne μl_{N-M+1} et $\mu l''' = 0$.

Figure 4 . Redondance M parmi N (système indisponible pendant les reconfigurations)

Une évolution de ce dernier modèle est prévue pour traiter les redondances M parmi N dont S éléments constituent un stock de rechanges, en paramétrisant le nombre $N-M-S$ d'états de reconfiguration dans lesquels le système est disponible. Ce type de redondance est illustré par la figure 5.

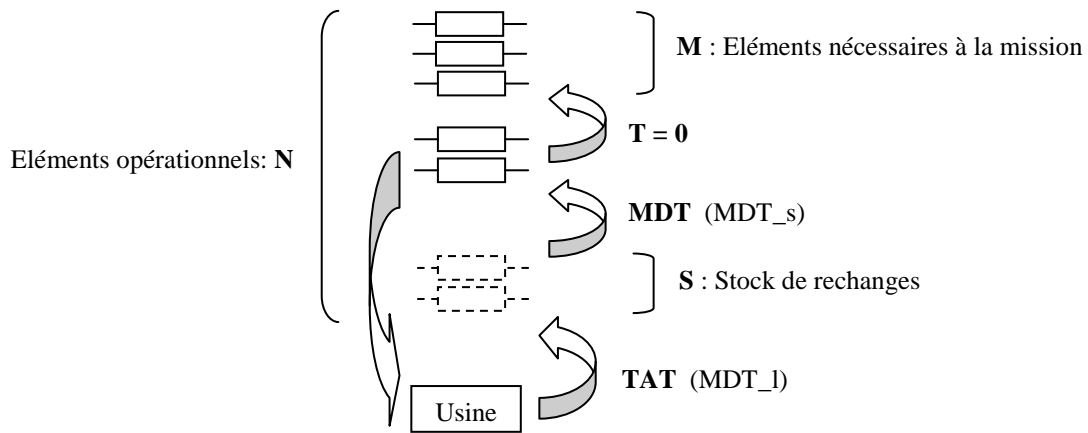


Figure 5 . Redondance M parmi N dont S éléments en stock

3.2.2 - Génération automatique de modèles markoviens

Afin de pouvoir modéliser des architectures diverses, l'outil recouvre une fonction originale de génération automatique de modèles markoviens à partir d'expressions logiques caractérisant le fonctionnement du sous-ensemble considéré. Son principe est illustré par la figure 6.

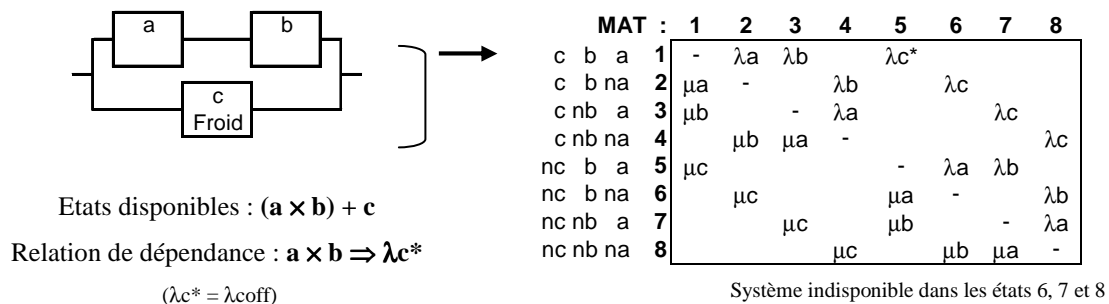


Figure 6 – Principe de la génération automatique des matrices de Markov

L'utilisateur définit les états dans lesquels le système fonctionne, par une expression logique utilisant les opérateurs OU (+), ET (x), NON (n), ainsi que d'éventuelles relations de dépendance, liant certaines valeurs de taux de transitions à des états du système (redondance froide, maintenance conditionnelle...). Dans l'exemple ci-dessus, l'élément c est à l'état off si les éléments a et b fonctionnent.

Quand les éléments du système ne sont pas tous considérés comme individuellement réparables, certains états sont généralement équivalents en terme de fonctionnement et peuvent être regroupés par l'outil afin d'optimiser la dimension de la matrice générée. L'exemple précédent est ainsi repris à la figure 7.

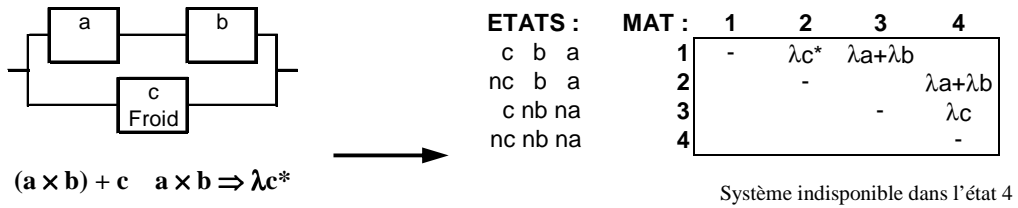


Figure 7 – Génération automatique avec optimisation

Afin d'identifier les états regroupés, on donne à chacun d'eux le nom de l'état du groupe qui comprend le plus d'éléments en panne (c nb na = c b na + c nb a + c nb na et nc nb na = nc b na + nc nb a + nc nb na).

Des taux de réparation relatifs à des blocs peuvent être introduits ultérieurement par l'utilisateur dans la matrice réduite (par exemple le taux de réparation de l'ensemble ab).

Bien que très dépendante des architectures considérées, cette méthode d'identification et de regroupement automatique des états équivalents est relativement efficace pour traiter des systèmes non réparables tels que des sous-ensembles de satellites. Cette efficacité est illustrée par les deux exemples de la figure 15 qui conduisent respectivement à des matrices de dimension 8 au lieu de 32 (2^5) et 10 au lieu de 64 (2^6).

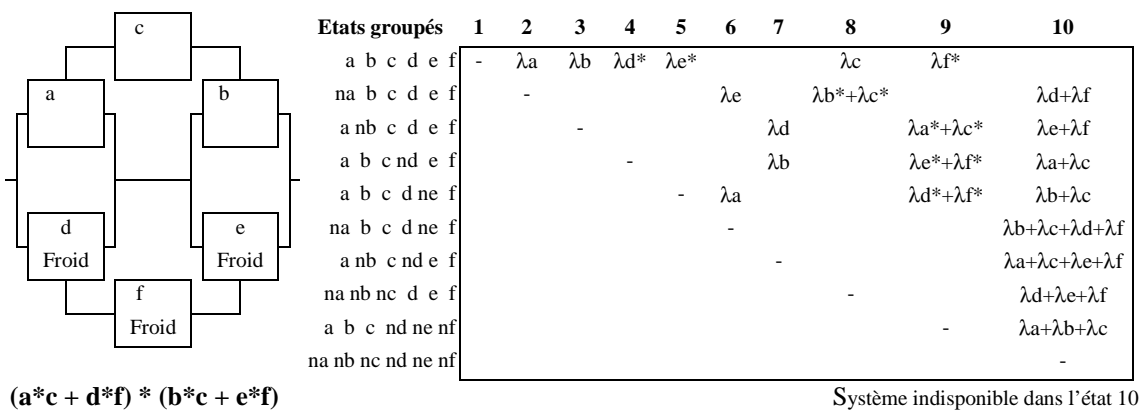
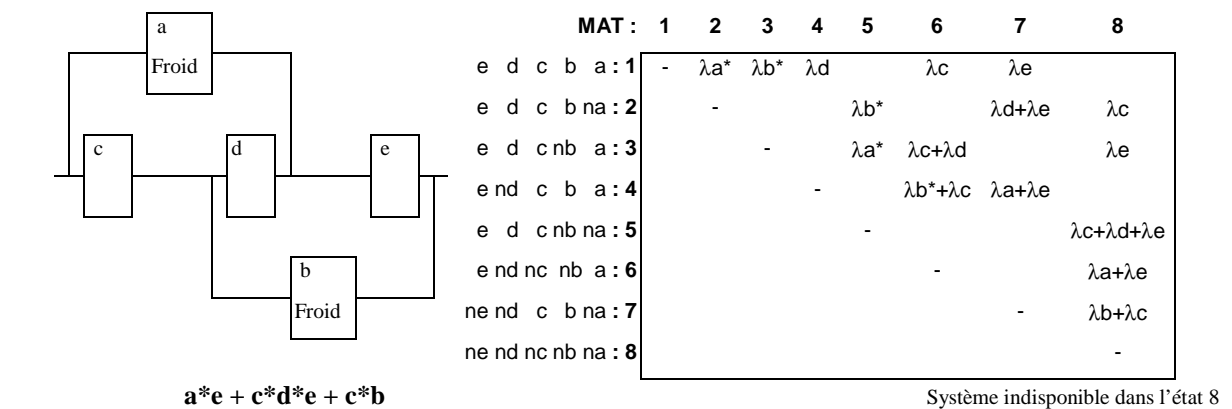


Figure 8 – Exemples de regroupement d'états équivalents

3.3 - L'optimisation

Le couplage entre des outils d'évaluation et d'optimisation permet d'automatiser la recherche de l'architecture la plus performante selon un critère donné ; ce dernier regroupant par exemple les coûts d'acquisition et de maintenance du système et sa disponibilité (ou sa fiabilité). L'outil GEN CAB permet un tel couplage. Basé sur une technique de recherche de l'optimum global par une méthode hybride couplant Algorithmes Génétiques et Simplexe non linéaire (algorithmes de Nelder Mead), son principe est illustré par la figure 9.

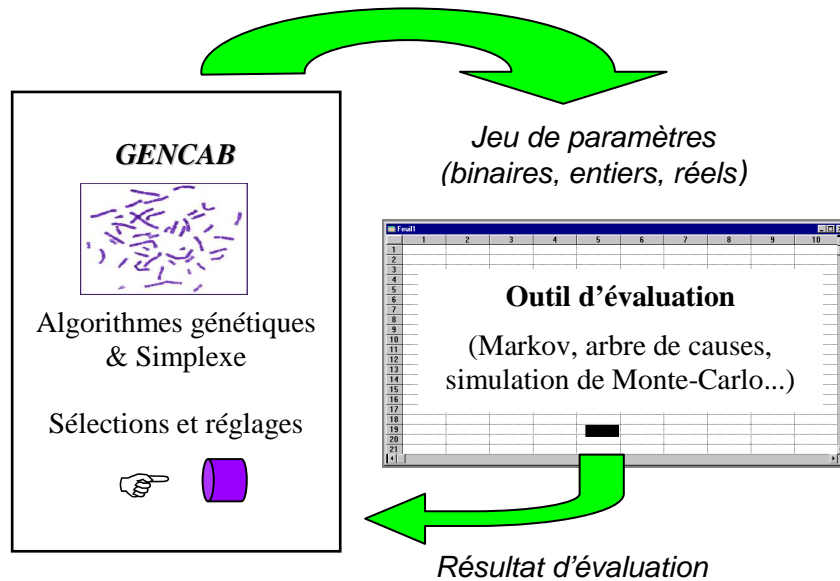


Figure 8 – Principe de l'outil générique d'optimisation GEN CAB

L'outil recherche la configuration optimale de paramètres (de type binaire, entier ou réel) qui maximise ou minimise le résultat de la fonction d'évaluation, sans s'arrêter au premier optimum local trouvé. La figure 9 illustre cette possibilité de couplage pour optimiser le coût global de possession d'un système. Evalué par l'outil SUPERCAB la disponibilité est ramenée à un coût d'indisponibilité du service rendu à l'utilisateur.

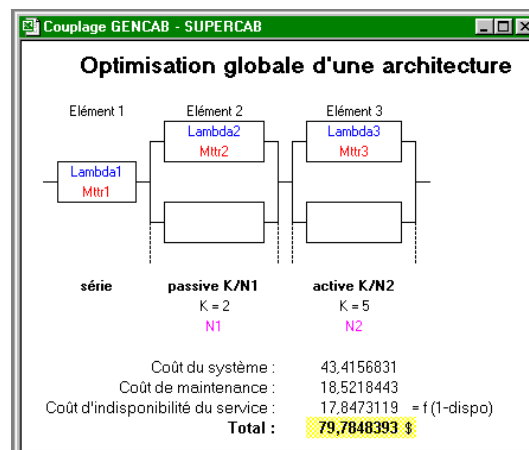


Figure 9 – Exemple d'optimisation d'architecture (6 paramètres réels et 2 entiers)

3.3 - L'analyse des dispersions

Si la durée d'une simulation de Monte-Carlo rend souvent incompatible son couplage direct à des outils d'optimisation (le nombre de pas de simulation de chaque évaluation étant multiplié par le nombre de pas d'optimisation, en première approximation), le couplage entre des outils d'évaluation et de simulation permet d'appréhender la variabilité des résultats obtenus en fonction de la dispersion des variables d'entrée.

Cette possibilité de couplage, mise en oeuvre par l'outil SIMCAB, est illustrée par deux cas simples : L'exemple de la figure 10 montre comment les dispersions sur les entrées (MTTF : durées de bon fonctionnement) influencent le résultat d'un traitement markovien.

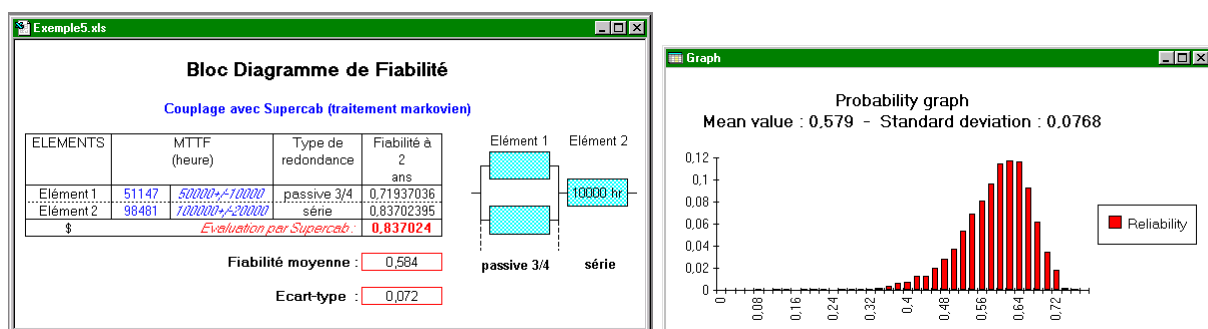


Figure 10 – Dispersion sur la fiabilité d'une architecture de système

De même l'exemple de la figure 11, montre la dispersion de la probabilité de l'événement sommet d'un arbre de causes en fonction de celle des événements de base (traitement analytique sans approximation).

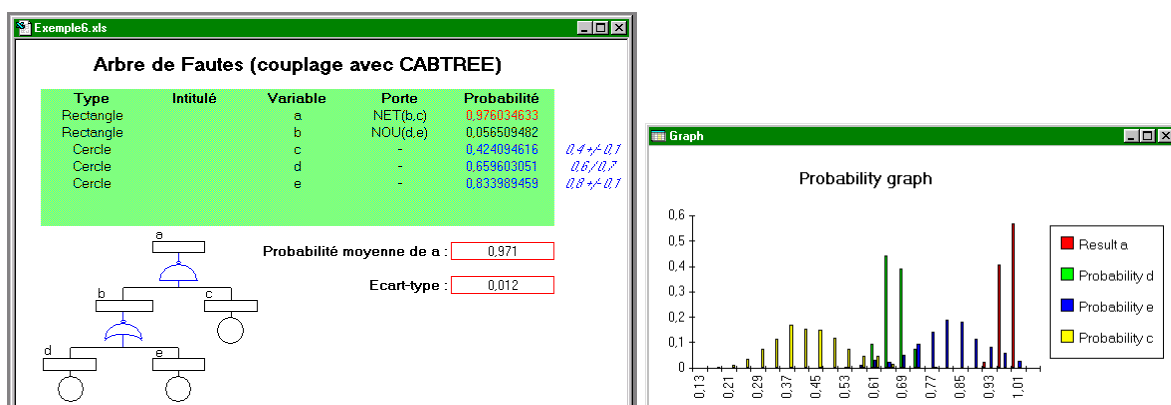


Figure 11 – Dispersion sur la probabilité d'un événement

Conclusion :

Au travers des outils présentés dans cet article, nous n'avons pas l'ambition de proposer une méthode générique d'évaluation de la Sûreté de Fonctionnement des systèmes et d'optimisation des architectures, mais seulement de présenter des réponses à des besoins relativement complexes rencontrés dans le domaine spatial. En effet le choix des méthodes ne peut se faire qu'en regard des problématiques et non pas des outils disponibles.

Cependant, outre la qualité des outils, l'optimisation en conception est souvent freinée par le manque de modèles paramétriques de coût et la difficulté à obtenir des données opérationnelles pertinentes.

REFERENCES SUCCINTES

Ouvrages de référence

- [1] A. Pages & M. Gondran - *Fiabilité des systèmes* - Edition Eyrolles, Paris 1980
- [2] A. Villemeur - *Sûreté de Fonctionnement des systèmes industriels* - Edition Eyrolles, Paris 1987

Dernières publications des auteurs

- [1] André Cabarbaye - *SUPERCAB PRO : Un atelier d'Ingénierie Système sous Microsoft Excel®* - 2^{ème} Conférence Annuelle d'Ingénierie Système, organisée par l'AFIS, TOULOUSE, 26-28 juin 2001.
- [2] André Cabarbaye - *SIMCAB : Un outil générique de Simulation sous Microsoft Excel®* - 3^e Conférence Francophone de Modélisation et Simulation (MOSIM'01), Troyes 25 au 27 avril 2001.
- [3] André Cabarbaye - *Simulation dynamique des arbres d'événements* - 4^e Congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement (Qualita 2001), Annecy 22 et 23 mars 2001.
- [4] Roland Laulheret, André Cabarbaye - *Elaboration d'une politique de Retour d'Expérience en Sûreté de Fonctionnement dans le domaine spatial* - 4^e Congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement (Qualita 2001), Annecy 22 et 23 mars 2001.
- [5] A. Cabarbaye, Julien Séroi - *Optimisation dans le domaine de la Sûreté de Fonctionnement* - 12^e Colloque National de Sûreté de Fonctionnement (λ/μ 12), Montpellier 28 - 30 mars 2000.
- [6] Linda Tomasini, André Cabarbaye, Julien Séroi, Frédéric Garcia, - *Optimisation de la maintenance d'une constellation de satellites* - 12^e Colloque National de Sûreté de Fonctionnement (λ/μ 12), Montpellier 28 - 30 mars 2000.
- [7] André Cabarbaye, Lamine Ngom - *Simulation dynamique des arbres d'événements* - 12^e Colloque National de Sûreté de Fonctionnement (λ/μ 12), Montpellier 28 - 30 mars 2000.
- [8] André Cabarbaye - *Outil générique d'optimisation par Algorithmes Génétiques et Simplexe* - 8^{èmes} Journées Nationales du groupe Mode (Mathématique de l'Optimisation et de la Décision) de la SMAI, Toulouse 23 - 25 mars 2000.
- [9] A. Cabarbaye - *Optimisation dans le domaine de la Sûreté de Fonctionnement* - Qualité Espace N°36, décembre 1999.
- [10] André Cabarbaye, Julien Séroi, Linda Tomasini - *Optimisation de la Sûreté de Fonctionnement des systèmes spatiaux* - 3^e Congrès International de Génie Industriel, Montréal 26 - 28 mai 1999.
- [11] A. Cabarbaye, L. Tomasini, L. Ngom, S. Allibe - *Apport des algorithmes génétiques à la Sûreté de Fonctionnement et à l'optimisation des systèmes* - Congrès Qualita 99, Paris 25-26 mars 99.

- [12] R. Laulheret, A. Cabarbaye - *Evolution des études qualitatives de Sûreté de Fonctionnement dans le domaine spatial* - Congrès Qualita 99, Paris 25-26 mars 99.
- [13] A. Cabarbaye, L. Ngom - *Mise en œuvre de la méthode des états fictifs et génération automatique des matrices de Markov* - Congrès Qualita 99, Paris 25-26 mars 99.
- [14] A. Cabarbaye, F. Garcia, L. Tomasini - *Apport de l'apprentissage par renforcement aux problèmes de maintenance optimale : application aux constellations de satellites* - Congrès ROADEF '99.
- [15] L. Ngom, J.C. Geffroy, C Baron, A. Cabarbaye - *Prise en compte des relations de dépendances dans la simulation de Monte-Carlo des arbres de défaillances non cohérents* - Phoebus N° 9 – 1999
- [16] A.Cabarbaye - *Apports, difficultés et perspectives dans le domaine de l'évaluation quantitative en Sûreté de Fonctionnement* - Qualité Espace N°33, 1998.
- [17] A. Cabarbaye, *Modélisation et évaluation des systèmes* - Cours de technologies spatiales Edition Cepadues Toulouse 1998.