



# REFERENTIEL NORMATIF du CNES RNC

Référence: **RNC-CNES-Q-30-504**  
Version 2  
14 Février 2000

## Méthode et Procédure

**EVALUATIONS PREVISIONNELLES  
DE FIABILITE EN ELECTRONIQUE  
( $\lambda$  CONSTANT)**

**APPROBATION**  
Président du CDN ;  
date et nom :



## PAGE D'ANALYSE DOCUMENTAIRE

<b>TITRE</b> : EVALUATIONS PREVISIONNELLES DE FIABILITE EN ELECTRONIQUE ( $\lambda$ CONSTANT)	
<b>MOTS CLES</b> : Evaluations Prévisionnelles, Fiabilité, Electronique	
<b>RESUME</b> : Cette MP (Méthode et Procédure) définit les règles détaillées, les opérations étapes et moyens qui permettent de réaliser les évaluations de la fiabilité des produits (Systèmes, Sous-systèmes et Equipements) en excluant les aspects de disponibilité.	
<b>SITUATION DU DOCUMENT</b> : Ce document fait partie de la collection des Méthodes et Procédures du Référentiel Normatif CNES (RNC). Il est affilié à la norme RNC-CNES-Q-30 "Sûreté de Fonctionnement".	
<b>NOMBRE DE PAGES</b> : 60	<b>LANGUE</b> : Française
<b>SYSTEME HOTE</b> : W97	
<b>SERVICE GESTIONNAIRE</b> : Délégation à l'Assurance de la Qualité du Centre Spatial de Toulouse (CT/AQ)	
<b>AUTEUR(S)</b> : M. SALEMAN	<b>DATE</b> : 25/04/1994
<b>RELECTURE / CONTROLE</b> :	
<b>Pour ACCORD</b> : <b>Le Président du Comité Technique de Normalisation</b> :	

© CNES 1994

Reproduction strictement réservée à l'usage privé du copiste, non destinée à une utilisation collective (article 41-2 de la loi n°57-298 du 11 Mars 1957).

## PAGES DES MODIFICATIONS

VERSION	DATE	PAGES MODIFIEES	OBSERVATIONS
PR		Document initial	
PR	27/01/93	Toutes	Prise en compte des commentaires internes CNES et ceux issus des Industriels.
PR	16/07/93	Toutes	Prise en compte de la réorganisation du CNES
1	25/04/94	i.1 ; i.2 ; 1 ; 2	Approbation du Comité Technique Référentiel et du Comité de Validation
2	14/02/00		Nouvelle codification des documents
2	4/11/2002	3 (mise à jour)	Retrait R8 Modif R9

## LISTE DES SIGLES ET DES ABREVIATIONS

<b>AdC</b>	Arbre de Cause
<b>AMDEC</b>	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
<b>BDF</b>	Bloc Diagramme de Fiabilité
<b>CNES</b>	Centre National d'Etudes Spatiales
<b>ESA</b>	European Space Agency
<b>FIT</b>	Failure In Time
<b>GdM</b>	Graphe de Markov
<b>IM</b>	Instruction de Management
<b>MDT</b>	Mean Down Time
<b>MP</b>	Méthode et Procédure
<b>MTBF</b>	Mean Time To Failure
<b>MTTF</b>	Mean Time To Failure
<b>MUT</b>	Mean Up Time
<b>RdP</b>	Réseau de Pétri
<b>R(t)</b>	Fiabilité ("Reliability")
<b>SCC</b>	Space Component Committee
<b>SdF</b>	Sûreté de Fonctionnement
<b><math>\lambda(t)</math></b>	Taux de défaillance
<b><math>\mu(t)</math></b>	Taux de réparation

---

## SOMMAIRE

<b>1. INTRODUCTION .....</b>	<b>1</b>
<b>2. OBJET .....</b>	<b>1</b>
<b>3. DOMAINES D'APPLICATION .....</b>	<b>1</b>
<b>4. DOCUMENTS DE REFERENCE .....</b>	<b>2</b>
4.1. NORMES ET ASSIMILES .....	2
4.2. OUVRAGES DIVERS .....	3
<b>5. DOCUMENTS APPLICABLES .....</b>	<b>4</b>
<b>6. PRINCIPES FONDAMENTAUX DE LA METHODE .....</b>	<b>4</b>
6.1. PRINCIPES DE BASE .....	4
6.2. HYPOTHESES FONDAMENTALES .....	7
<b>7. DESCRIPTION DE LA PROCEDURE .....</b>	<b>7</b>
7.1. DEMARCHE D'EVALUATION .....	7
7.2. ÉTABLISSEMENT DU MODELE DE FIABILITE .....	8
7.3. DETERMINATION DES DONNEES DU MODELE .....	11
7.3.1. Préliminaire .....	11
7.3.2. Evaluation des données .....	11
7.4. TRAITEMENT DU MODELE : CALCUL DE LA FIABILITE .....	15
7.5. COMPARAISON AUX OBJECTIFS .....	16
7.6. RETOUR D'EXPERIENCE .....	16
<b>8. DOCUMENTS ET RESULTATS ATTENDUS.....</b>	<b>17</b>



<b>ANNEXE 1 : ILLUSTRATION DE LA DEMARCHE .....</b>	<b>19</b>
<b>ANNEXE 2 : METHODES DE MODELISATION .....</b>	<b>23</b>
<b>ANNEXE 3 : METHODES DE CALCUL DES DONNEES DU MODELE .....</b>	<b>37</b>
<b>ANNEXE 4 : COMPLEMENTARITE DES METHODES DE MODELISATION .....</b>	<b>45</b>
<b>ANNEXE 5 : METHODE D'EXPLOITATION DES RESULTATS D'ESSAIS DE FIABILITE AVEC LA LOI DU KHI DEUX.....</b>	<b>59</b>





## 1. INTRODUCTION

Le présent document constitue la Méthode et Procédure pour les évaluations prévisionnelles de fiabilité en électronique.

Il fait partie de la collection des Méthodes et Procédures associées au RNC-CNES-Q-30 "Sûreté de Fonctionnement".

## 2. OBJET

Cette Méthode et Procédure est un guide présentant des méthodes d'évaluation de fiabilité, utilisables dans les domaines définis au chapitre 3.

Un de ses buts essentiels est d'aider à évaluer la fiabilité d'un produit en vue de la comparer aux objectifs spécifiés, eux-mêmes alloués par des méthodes spécifiques.

D'autre part, cette MP propose des critères communs d'évaluations de fiabilité pour les différents niveaux d'un même programme afin d'assurer la cohérence dans le processus global d'estimation.

La MP est un document technique qui définit, de manière ordonnée et logique, les règles détaillées, les opérations, étapes et moyens qui permettent de satisfaire aux exigences exprimées par l'Instruction de Management "Sûreté de Fonctionnement" [R1], pour les évaluations de fiabilité des produits.

En particulier, cette MP identifie les données/entrées/conditions nécessaires à son application.

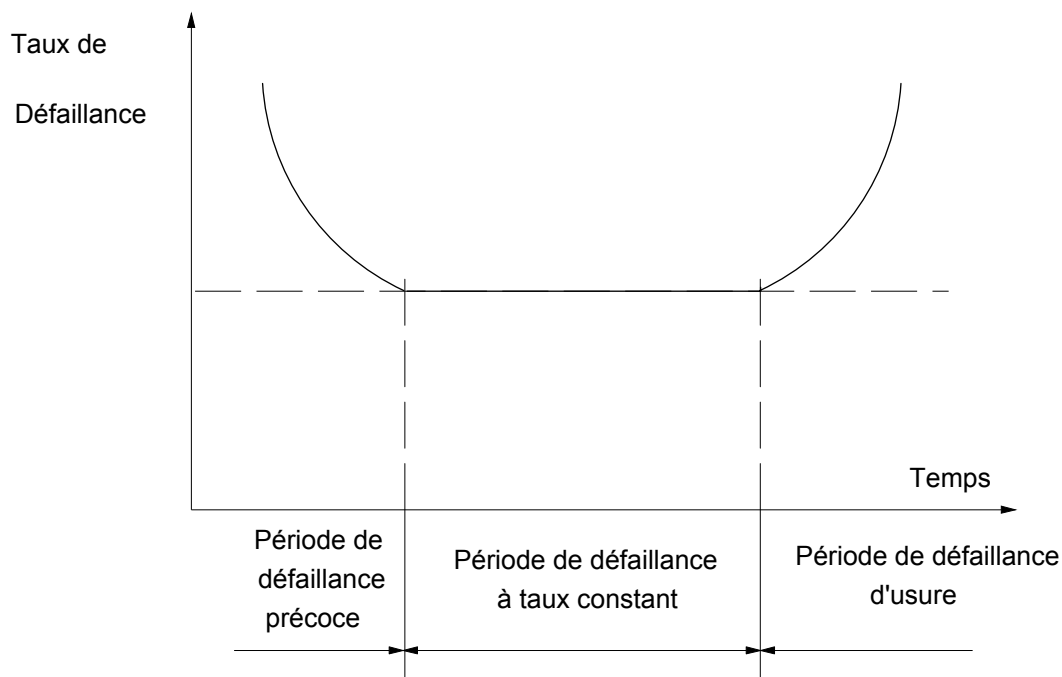
## 3. DOMAINES D'APPLICATION

La présente MP concerne les évaluations **prévisionnelles de fiabilité** et exclut les aspects de disponibilité.

Elle s'applique aux analyses menées au niveau des *Systèmes*, *Sous-Systèmes* et *Equipements* de systèmes spatiaux. Dans la suite du document, le terme "produit" sera parfois utilisé pour désigner un système, sous-système ou un équipement.

Ses domaines d'application sont ceux pour lesquels la loi de fiabilité exponentielle est valide, avec des taux de défaillance constants pour les composants. C'est par exemple le cas dans le domaine électronique. Le domaine électromécanique en est un autre dans la mesure où l'utilisation d'un taux de défaillance constant est justifiée.

Dans ces domaines, les constituants du produit présentent habituellement des taux de défaillance en fonction du temps qui suivent la courbe dite "en baignoire". Sur cette courbe, la durée de vie utile correspond à la période de défaillance à taux constant.



Dans ce cadre, les limites d'utilisation de cette MP est la non prise en compte des processus de vieillissement.

Cette MP concerne les analyses menées lors des phases d'étude et de développement. Elle ne décrit pas les méthodes d'allocation d'objectifs de fiabilité, ni les procédures liées au suivi de la fiabilité des sous-systèmes et équipements en opération, et au traitement des retours d'expérience.

## 4. DOCUMENTS DE REFERENCE

### 4.1. Normes et Assimilés

- [R1] Instruction de Management - Sûreté de Fonctionnement  
RNC-CNES-Q-30
- [R2] Terminologie relative à la Fiabilité - Maintenabilité - Disponibilité.  
NF X 60-500
- [R3] Applications de la statistique: Introduction à la Fiabilité  
NF X 06-501
- [R4] Military Standard - Reliability Modeling and Prediction.  
MIL-STD-756

- 
- [R5] Military Handbook - Electronic Reliability Design Handbook.  
MIL-HDBK-338
- [R6] Failure rates for ESA Space Systems.  
ESA-PSS-01-302
- [R7] Handbook of Reliability Data for components used in Telecommunications Systems.  
BRITISH TELECOM - HRD4 (1987)
- [R8] supprimée
- [R9] RNC-ECSS-Q-60-01  
European Preferred Parts List.
- [R10] Derating requirements and application rules for electronic components.  
ESA-PSS-01-301
- [R11] Nonelectronic Parts Reliability Data  
Reliability Analysis Center - IIT Research Institute.  
DOD

#### 4.2. Ouvrages divers

- [R12] Fiabilité des Systèmes.  
A. PAGES et M.GONDRAN  
Editions Eyrolles (1980)
- [R13] Sûreté de Fonctionnement des Systèmes Industriels.  
A. VILLEMEUR - Collection de la Direction des Etudes et Recherches d'EDF  
Editions Eyrolles (1988)
- [R14] Traité de Fiabilité.  
M. SCHWOB et G. PEYRACHE  
Editions Masson (1969)
- [R15] Du Grafset aux réseaux de Pétri.  
R.DAVID et H.ALLA - CNRS, Laboratoire d'automatique de Grenoble  
Editions Hermes, Paris (1989)
- [R16] Petri Net theory and the modeling of systems.  
J.L. PETERSON  
Editions Prentice Hall, Englewood Cliffs, N.J. (US) (1981)
- [R17] Réseaux de Pétri: Théorie et Analyse.  
G.W. BRAMS  
Editions MASSON (1983)

- [R18] Finite Markov Chain.  
J.G. KEMENY, J.L. SNELL  
D. Van Nostrand Company, Inc. (1960)
- [R19] Elements of the Theory of Markov Processes and their Applications.  
A.T. BHARUCHA - REID  
McGraw Book Company (1960)
- [R20] Military Handbook - Reliability Prediction of Electronic Equipment.  
MIL-HDBK-217

## 5. DOCUMENTS APPLICABLES

néant

## 6. PRINCIPES FONDAMENTAUX DE LA METHODE

### 6.1. Principes de base

La fiabilité d'un produit doit être analysée et construite en étroite collaboration avec le concepteur, au même titre que les autres performances techniques du produit.

En particulier, la fiabilité sera analysée dès les premières phases d'études du produit et prise en compte comme critère pour les comparaisons d'architectures.

L'optimisation de la conception du produit d'un point de vue fiabilité pourra alors être menée de façon itérative, au fur et à mesure de l'avancement dans la connaissance des constituants du produit, et en accord avec les objectifs spécifiés.

Par exemple, les résultats des évaluations préliminaires seront confrontés aux objectifs, en vue soit d'identifier d'éventuels besoins d'amélioration de la conception et de focaliser les efforts du concepteur sur les zones critiques ou sensibles du produit, soit d'affiner l'allocation des objectifs.

Les actions permettant de fiabiliser le produit, si nécessaire, sont de trois types :

- amélioration de la fiabilité intrinsèque des constituants de base du produit,
- fiabilisation par construction au niveau de l'architecture du produit,
- fiabilisation par amélioration des conditions d'utilisation du produit.

*Par **définition**, la fiabilité d'un produit est son aptitude à accomplir une fonction requise, dans des conditions données et pendant un intervalle de temps donné.*

Elle est mesurée par la probabilité pour que ce produit accomplisse une fonction requise, dans des conditions données et pendant un intervalle de temps donné.

La fonction requise peut correspondre à tout ou partie des fonctions de la mission du produit, et ce pour tout ou partie des phases de la mission.

Ainsi, deux *pré-requis* sont nécessaires pour évaluer la fiabilité du produit :

- l'analyste s'assurera que l'objectif quantitatif de fiabilité, donné dans la spécification technique du produit, est clairement spécifié (valeur d'objectif caractéristiques de missions correspondantes, base de calcul associée) et compris,
- l'analyste disposera des résultats de l'analyse de mission (connaissance des conditions d'utilisation : phases et environnements) et de l'analyse fonctionnelle du produit mettant en évidence les modes de défaillances fonctionnels à prendre en compte (conformément à la MP analyse fonctionnelle).

L'évaluation de fiabilité sera alors structurée autour des 4 tâches suivantes :

- 1 - Etablir un modèle de fiabilité, suivant les objectifs spécifiés,
- 2 - Déterminer les données de base du modèle de fiabilité,
- 3 - Traiter le modèle pour calculer la fiabilité du produit,
- 4 - Comparer les résultats aux objectifs spécifiés.

Cette découpe de la démarche en étapes distinctes aidera l'analyste à séparer clairement les problèmes à résoudre pour mener à bien une évaluation de fiabilité, et lui permettra ainsi :

- d'une part d'offrir une bonne visibilité de sa maîtrise de chacun des problèmes,
- d'autre part de disposer de résultats d'analyse modulaires et facilement évolutifs lors de l'avancement du projet et adaptables pour d'autres besoins. Par exemple, le modèle de base pourra être orienté en vue de calculer les disponibilités de missions nominale et dégradées.

*Quelques relations de base [R12] :*

- Fiabilité  $R(t)$  d'un système S :

$R(t)$  = Probabilité (S non défaillant sur  $[0, t]$ )

$R(t)$  est une fonction non croissante variant de 1 à 0 sur  $[0, +\infty]$

- MTTF : Durée moyenne de bon fonctionnement d'un système avant la première défaillance ("Mean Time To Failure").

$$MTTF = \int_0^{\infty} R(t) \cdot dt$$

- MUT : Durée moyenne de bon fonctionnement après réparation ("Mean Up Time"). Le MUT est différent du MTTF car lorsque le système est remis en service après une défaillance, tous ses éléments défaillants n'ont pas nécessairement été réparés.

- MDT : Durée moyenne de défaillance ("Mean Down Time")

Cette durée moyenne comprend la détection de la panne, la durée d'intervention, la durée de la réparation et la durée de remise en service.

- MTBF : Moyenne des temps entre deux défaillances d'un système réparable ("Mean Time Between Failure")

$$MTBF = MUT + MDT$$

Remarque: Le MTBF est parfois traduit par "moyenne des temps de bon fonctionnement" et correspond alors au MTTF ou au MUT. Pour de nombreux systèmes, MDT est négligeable devant MUT et la différence entre MTTF et MTBF est faible.

- $\lambda(t)$  : Taux de défaillance instantanée

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \text{Probabilité (S tombe en panne entre } t \text{ et } t + \Delta t \text{ sachant qu'il n'a pas eu de défaillance sur } [0, t]).$$

La connaissance de la fonction  $\lambda(t)$  est équivalente à la connaissance de la fonction  $R(t)$ . Elle sont en effet liées par les relations :

$$R(t) = \exp \left[ - \int_0^t \lambda(u) \cdot du \right] \text{ ou } \lambda(t) = - \frac{dR}{dt}(t)$$

Dans le cas d'une loi de durée de vie exponentielle, la fonction  $\lambda(t)$  se réduit à une constante notée  $\lambda$ .

Dans ce cas :

$$R(t) = e^{-\lambda t}$$

## 6.2. Hypothèses fondamentales

L'évaluation prévisionnelle de fiabilité d'un produit, telle que décrite au chapitre 7, s'appuie sur les hypothèses ci-dessous qui sont en partie validées par les actions de l'assurance qualité.

- L'architecture du produit prise en compte pour l'analyse est représentative du produit final embarqué dans le système.
- A l'issue des tests de recette, les composants sont dans leur phase de "vie utile" (déverminage optimal),
- La durée de vie des constituants des produits de la composante spatiale du système (a priori non réparable) est supérieure à la durée de vie spécifiée du système.
- En corollaire de ces deux dernières hypothèses, on suppose que les composants de base du produit restent durant la mission dans leur durée de vie utile et ont un taux de défaillance constant.
- Les composants, matériaux et procédés sont qualifiés pour leur application et les environnements associés.
- Les procédés de production, de test et d'essai n'introduisent pas de détériorations latentes ou de phénomènes de défaillance inconnus, et les contraintes associées n'affectent pas les taux de défaillance des composants; en particulier, les composants sont supposés respecter les taux de "derating".
- La conception des produits est telle qu'elle intègre toutes les marges nécessaires pour garantir les performances nominales en tenant compte des écarts dus aux contraintes lors de la production, aux environnements thermiques et radiatifs en opération et au vieillissement des composants; en particulier, les niveaux de stress effectifs sont cohérents avec les spécifications de "derating", s'il y a lieu.
- En début de mission, le produit a une fiabilité égale à 1 (fonctionnement nominal),
- Les niveaux de qualité attachés aux composants et à la réalisation du produit final sont définis et seront respectés.

## 7. DESCRIPTION DE LA PROCEDURE

### 7.1. Démarche d'évaluation

Avant de réaliser l'évaluation de la fiabilité du produit, l'analyste précisera les informations suivantes :

- l'objectif de l'évaluation, fonction du stade d'avancement du projet. L'approche et le niveau de détail de l'analyse seront en effet adaptés d'après son objectif, depuis la phase d'analyse de faisabilité du produit, jusqu'à sa revue de conception finale.
- l'état du produit analysé, en identifiant tous les documents de référence utilisés.

Sur ces bases sont mises en oeuvre les 4 étapes introduites au chapitre 6.1 et détaillées ci-après :

- 1 - Etablir un modèle de fiabilité, suivant les objectifs spécifiés,
- 2 - Déterminer les données de base du modèle de fiabilité,
- 3 - Traiter le modèle pour calculer la fiabilité du produit,
- 4 - Comparer les résultats aux objectifs spécifiés.

L'analyste modulera le niveau de détail de l'étude et l'effort associé, en fonction du stade d'avancement du projet et de la criticité des constituants analysés, en jouant soit sur le choix de la technique de modélisation, soit sur la finesse et l'exactitude du modèle, soit sur la précision des calculs des données liées au modèle. Cette modulation est illustrée par la figure 1 donnée en annexe 1 et précisée dans les chapitres suivants, pour chaque étape de la démarche.

Dans tous les cas, si l'analyste doit faire des hypothèses lors de l'étude, il se placera dans le cas le plus pessimiste, puis mentionnera et justifiera clairement ces hypothèses.

L'évaluation de fiabilité, et en particulier l'élaboration du modèle, seront orientées en fonction des objectifs spécifiés et s'appuieront sur la connaissance des conditions d'utilisation du produit (phases, environnements) et sur les résultats de l'Analyse Fonctionnelle.

Au fur et à mesure de l'avancement du projet, le modèle établi sera enrichi puis validé à l'aide des résultats des AMDEC.

Bien que limitée à l'analyse des défaillances "simples", l'AMDEC permet en particulier de mieux connaître les modes de défaillance des éléments du produit, leur criticité et les capacités de reconfiguration (détection, localisation, réaction), et ainsi de valider la prise en compte de ces éléments dans le modèle (Point de Panne Unique, propagations de panne...), et ce de façon systématique. Ce processus est illustré en annexe 1.

## **7.2. Etablissement du modèle de fiabilité**

Le modèle de fiabilité est établi en vue de décrire les scénarios d'événements qui rendent le produit non fiable et de permettre l'évaluation de la probabilité d'occurrence de ces scénarios.

Un ou plusieurs modèles pourront être réalisés, en fonction du nombre de phases et de fonctions concernées par l'objectif de fiabilité spécifié et de la technique de modélisation utilisée.



Il existe plusieurs techniques de modélisation. Les plus couramment mises en oeuvre et préconisées ici sont :

- Le Bloc Diagramme de Fiabilité (BDF),
- L'Arbre de Cause (AdC) (ou arbre de défaillance),
- Le Graphe de Markov (GdM),
- Le réseau de Pétri (RdP).

Afin d'optimiser l'étude, l'analyste choisira d'utiliser l'une ou l'autre de ces techniques, en fonction de la complexité des phénomènes à décrire et des objectifs alloués (avancement de l'étude, moyens, finesse des objectifs spécifiés).

Dans tous les cas, l'analyste privilégiera le modèle permettant de décrire puis d'évaluer le plus simplement et le plus clairement le produit tout en garantissant une bonne confiance dans le résultat de l'évaluation.

La démarche proposée est de mettre en oeuvre dans un premier temps la technique de modélisation la plus immédiate, éventuellement en faisant des hypothèses simplificatrices, puis d'enrichir le modèle à l'aide de techniques plus riches, ponctuellement, lorsque les hypothèses simplificatrices s'avèrent trop sensibles sur le résultat final, ou que la technique de modélisation initiale atteint ses limites.

Dans la mesure du possible, et en priorité, l'analyste réalisera la modélisation à l'aide d'un **Bloc Diagramme de Fiabilité** [R4, R12 & R13].

Le BDF est l'association série et/ou parallèle, du point de vue fiabilité, des constituants du produit participant à la réalisation de sa fonction.

L'analyste s'appuiera, pour l'élaboration du BDF, sur la découpe technique du produit en constituants, et sur les résultats de l'analyse fonctionnelle. En particulier il y aura correspondance entre les identifiants utilisés dans le schéma fonctionnel et du BDF.

L'intérêt du BDF est sa facilité de mise en oeuvre pour des produits dont les constituants sont, d'un point de vue "chemin de fiabilité", soit en série, soit en parallèle.

Par contre, les BDF ne sont pas adaptés à la description de phénomènes dynamiques, et ne permettent pas de décrire simplement tous les types d'événements et de combinaisons d'événements entraînant une perte du bon fonctionnement.

Si nécessaire, l'analyste pourra alors mettre en oeuvre des techniques de modélisation plus riches, soit globalement pour l'ensemble du modèle de fiabilité du produit, soit ponctuellement pour affiner la modélisation puis l'évaluation de la fiabilité de certains constituants apparaissant dans le BDF initial.

Dans ce but, plusieurs techniques sont alors disponibles. Elles sont recensées ci-après par ordre croissant suivant leur richesse de modélisation.

**L'Arbre de Cause** [R12 & R13] : il permet de modéliser les scénarios d'événements (événement simple ou combinaison d'événements) entraînant l'occurrence d'un événement redouté donné.

L'intérêt de l'AdC réside dans :

- sa structure hiérarchisée et descendante (approche déductive), qui permet de moduler le niveau de détail de l'analyse, en fonction de la maturité de la conception et de la criticité des événements identifiés,
- la possibilité de prendre en compte des événements de types différents dans le modèle qualitatif, même si tous ces événements ne sont pas considérés dans l'évaluation quantitative. Par exemple, un AdC permet d'intégrer dans les modèles, en plus des défaillances, des événements extérieurs au produit analysé, des événements normaux (hors défaillance) dans le fonctionnement du produit, des interventions humaines...
- l'aptitude des AdC à identifier les modes communs, lors de la réduction de l'équation booléenne associée à l'arbre initial (identification des coupes minimales par "réduction de l'arbre initial").

Lors de l'utilisation d'un AdC, l'analyste s'assurera d'inclure dans la définition des événements possibles les conditions suivantes, s'il y a lieu:

- invalidité des systèmes de prévention (pour cause de maintenance ou de panne),
- procédures d'opération et/ou de maintenance incorrectement ou non suivies,
- éléments redondants inhibés lors de la maintenance préventive.

Les AdC atteignent leur limite, lorsqu'il s'agit de modéliser des phénomènes dynamiques (conditionnels, séquentiels, temporels). Dans ce cas, et si nécessaire, il est préconisé d'utiliser des techniques telles que les Graphes de Markov ou les Réseaux de Pétri.

**Les Graphes de Markov** [R12, R13, R18, R19] : Ce sont des graphes d'états à taux de transition constants.

Les GdM permettent de modéliser les évolutions d'un produit entre ses différents états de fonctionnement, lorsque les transitions entre ces états sont caractérisées par des lois à taux constants.

Les GdM sont intéressants essentiellement pour:

- intégrer dans un même modèle l'ensemble des états du produit (fonctionnement nominal, dégradé, en réparation, en panne ...),
- prendre en compte les phénomènes de réparation (taux de réparation),
- modéliser les phénomènes séquentiels.

Par contre, les GdM sont limités à des processus à taux de transition inter-états constants, et ne permettent pas de traiter les aspects déterministes.

Les GdM sont souvent utilisés pour les calculs de disponibilité.

**Les Réseaux de Pétri** [R13, R15, R16, R17] : Ils permettent de modéliser les interactions entre les constituants du produit, et ainsi ses évolutions entre ses différents états.

Les RdP sont adaptés pour décrire les aspects dynamiques du produit, mettre en valeur le facteur temps et les éventuels synchronisations et conditionnements (évolutions simultanées).

Ils sont d'autre part souvent utilisés pour simuler le comportement des systèmes.

Les limites des Réseaux de Pétri peuvent être la complexité des modèles élaborés et la difficulté pour les valider, pour des produits comportant de nombreux constituants. Cette limite peut être atténuée grâce à certains outils adaptés.

Une description succincte de chaque méthode de modélisation est donnée en annexe 2, et un exemple présentant leur complémentarité en annexe 4.

### 7.3. Détermination des données du modèle

#### 7.3.1. Préliminaire

Il s'agit lors de cette étape de déterminer les données de base nécessaires pour traiter le modèle élaboré et calculer la fiabilité du produit.

Ces données seront généralement les taux de défaillance (ou la fiabilité) et les taux de réparation des constituants du produit apparaissant dans le modèle.

Pour des modèles dynamiques (GdM ou RdP) il s'agira en fait des taux de transition entre les états du produit (modes de fonctionnement nominaux, dégradés, perte de fonction...), ou autres paramètres tels que les temps de reconfiguration, les taux de détection de panne...

#### 7.3.2. Evaluation des données

Les données peuvent être calculées au moyen :

- de banques ou recueil de données : [A1], [R6], [R7], [R11],
- de base de données techniques internes enrichies par des résultats d'essais (calculés suivant la méthode donnée en annexe 5) ou un suivi en exploitation de produits de technologies similaires et utilisés dans des environnements de même type,

- de méthodes de calculs spécifiques,
- d'avis d'experts,

et dépendent des **informations d'entrée** suivantes :

- conditions d'utilisation du produit : durées des phases opératoires et environnements associés, modes de fonctionnement, taux d'utilisation ("duty cycle"),
- caractéristiques techniques des constituants du produit analysé,
- niveaux de qualité,
- contraintes opérationnelles des composants de base du produit : contraintes électriques, thermiques, mécaniques, radiations.

L'origine des données sera précisée et justifiée, en particulier pour les données de sources non communes.

Les contraintes électriques opérationnelles des composants de base du produit seront données par les responsables technique du produit et les contraintes thermiques seront issues de l'analyse thermique (température moyenne du cycle fin de vie).

Les taux de charge (deratings) associés à ces composants devront être conformes aux taux de charge admissibles définis dans les documents [R9] et [R10].

Les informations considérées pour le calcul des données sont plus ou moins détaillées, suivant l'avancement du projet et la connaissance des constituants du produit et de ses conditions d'utilisation. La modulation du niveau de détail des évaluations, au niveau sous-système puis au niveau équipement, est présentée ci-après. Dans tous les cas, les estimations tiendront compte des niveaux qualité associés au produit et des conditions d'utilisation, en particulier : l'environnement du produit, sa température, et son taux d'utilisation.

**Au niveau sous-système** et lors des évaluations préliminaires, l'analyste calculera les données associées aux équipements en utilisant:

- dans la mesure du possible (s'il a déjà une bonne visibilité sur l'architecture et les composants de l'équipement), la méthode "part count" décrite dans le document MIL-HDBK-217 [A1] et présentée en annexe 3.
- sinon des données forfaitaires de niveau bloc fonctionnel ou équipement issues de base de données techniques internes à l'industriel ou autres.

Lors des phases suivantes, ces données d'entrée seront enrichies par les résultats des évaluations menées sur les équipements. La Figure 1 donnée en annexe 1 illustre cette démarche.

**Au niveau équipement**, le calcul des données associées aux composants élémentaires sera fait en utilisant les données issues de la base MIL-HDBK-217 [A1] ou d'une autre base de données, telle que [R6], [R7], voire de résultats d'essais de fiabilité spécifiques. Dans le cas d'exploitation de résultats d'essais de fiabilité, la loi du Khi deux telle que définie en annexe 5 sera utilisée. Dans tous les cas, l'analyste justifiera l'origine et la validité des données utilisées et détaillera les hypothèses associées à leurs estimations. Il veillera d'autre part à optimiser l'homogénéité des références utilisées durant les évaluations.

Lors des phases de conception préliminaire, les évaluations de niveau équipement seront menées suivant la technique "part count" décrite dans le document [A1].

Lors des phases de conception finale, les contraintes opérationnelles des constituants seront intégrées et les évaluations précisées à l'aide, si possible, de la méthode "part stress" décrite dans le document [A1].

Les méthodes Part Count et Part Stress consistent en l'utilisation d'un modèle mathématique donnant le taux de défaillance d'un composant en fonction d'un ensemble de paramètres tels que : l'environnement, la température, les contraintes électriques, le niveau de qualification...

Dans le cas de la méthode Part Count, les taux de défaillance sont extraits de tables données pour chaque famille de composants. Ils sont calculés à partir des modèles mathématiques en considérant des valeurs moyennes forfaitaires pour la plupart des paramètres ; seuls le niveau de qualification des composants et leur environnement réels sont pris en compte.

Dans le cas de la méthode Part Stress, les taux de défaillance sont à calculer à partir des modèles mathématiques en intégrant l'ensemble des valeurs réelles des paramètres, et ce pour chaque composant.

Ces deux méthodes de calcul, Part Count et Part Stress, sont présentées en annexe 3.

Les **déviations** suivantes à la MIL-HDBK-217 seront appliquées dans le cadre de niveau de qualité spatial :

$$\left. \begin{array}{l} \text{- trous métallisés :} \\ \quad + \\ \text{soudures manuelles} \end{array} \right\} \lambda = 0,1 \cdot 10^{-9}/h$$
$$\text{- sertissage :} \quad \lambda = 0,1 \cdot 10^{-9}/h$$

Les calculs pourront être réalisés à l'aide d'outils tels que, par exemple, l'outil MilStress (Item) qui intègre la base de référence MIL-HDBK-217.

Si d'autres outils sont mis en oeuvre (outils internes par exemple), l'analyste précisera leurs caractéristiques et s'assurera de leur validité. En cas de besoin, il justifiera par échantillonnage la cohérence entre les résultats obtenus à l'aide de l'outil et les règles applicables.

Dans le cas où un élément a plusieurs modes de défaillance avec des effets différents au niveau supérieur, l'analyste pourra intégrer cet aspect dans le modèle qualitatif de fiabilité. D'un point de vue quantitatif, si la donnée associée au mode de défaillance considéré n'existe pas, l'analyste se placera dans un pire cas. Par exemple, à la perte d'une fonction switch d'un circuit intégré HCC4066BD (intégrant 4 switches) pourra être associé le taux de défaillance global du circuit intégré.

Pour les composants **non-alimentés**, le taux de défaillance sera égal au dixième du taux de défaillance en fonctionnement à conditions d'environnement identiques. D'autres données peuvent être utilisées avec justification.

Pour les éléments à **fonctionnement périodique** ayant un **taux d'utilisation inférieur à 100%** (taux d'utilisation = "duty cycle" = % du temps durant lequel l'élément est ON), le facteur correctif multiplicatif à appliquer au taux de défaillance de l'élément sera calculé sur la base de l'hypothèse donnée ci-dessus pour les composants non alimentés. On aura donc:

$$\text{Facteur correctif} = F_c = \% \text{ durée ON} * 1.0 + \% \text{ durée OFF} * 0.1$$

et un taux de défaillance équivalent pour l'élément :  $\lambda = F_c * \lambda \text{ (ON)}$

**Remarque :** Dans le cas d'une redondance froide p/n avec un taux d'utilisation inférieur à 100 %, l'analyste veillera à appliquer correctement ce facteur multiplicatif, uniquement sur les éléments activés. La formule générale donnant la fiabilité pour ce type de configuration est donnée en annexe 2.

Pour les **composants commutables**, l'analyste s'assurera que le nombre de commutations reste conforme aux caractéristiques du composant et intégrera ce paramètre dans l'évaluation de fiabilité. Plusieurs cas se présentent :

- soit le nombre de commutations est un paramètre intégré au modèle mathématique utilisé, et sa prise en compte est alors immédiate. Exemple: "Cycling factor" dans le modèle des switches [A1].
- soit le modèle n'intègre pas ce paramètre, et dans ce cas l'analyste décrira le phénomène au niveau du modèle de fiabilité de l'équipée, dans la mesure du possible. Par exemple, la probabilité de défaillance d'un composant à la sollicitation pourra être prise en compte à l'aide d'un modèle dynamique (Graphe de Markov ou Réseau de Pétri).

Les **coefficients qualité** ( $\pi q$ ) pour les composants américains sont ceux de la MIL-HDBK-217. Conformément à la référence [R9] et à la comparaison des files de sélection des composants, pour les composants européens, on utilisera les équivalences suivantes :

TYPES DE COMPOSANTS	NIVEAUX QUALITE EUROPEENS	COEFFICIENTS QUALITE EQUIVALENTS (d'après MIL-HDBK-217)
Passifs	SCC B SCC C	MIL S MIL R
Relais	SCC B	0,5 * MIL R
Actifs discrets	SCC B SCC C	0,5 * MIL JAN TXV MIL JAN TXV
Circuits intégrés	SCC B SCC C	MIL S MIL B
Hybrides	Ligne qualifiée CNES-ESA Autres	S B-1

**Tableau 7.3.2-1: Correspondance entre les niveaux qualité Européens et Américains**

L'emploi de ces valeurs est strictement limité aux composants approvisionnés suivant les niveaux de qualité indiqués. Dans le cas contraire, la valeur du coefficient de qualité sera justifiée.

#### **7.4. Traitement du modèle : calcul de la fiabilité**

L'analyste calculera la fiabilité du produit à partir du modèle établi et des données estimées.

Le traitement du modèle permettra d'extraire des résultats qui pourront être directement comparés aux objectifs spécifiés.

Seront également extraits des résultats intermédiaires en vue d'être en mesure de donner au responsable technique la contribution, vis-à-vis des résultats globaux, des différents constituants du produit.

Le traitement pourra être mené à l'aide d'outils informatiques. Dans ce cas, l'analyste donnera les références de l'outil.

### 7.5. Comparaison aux objectifs

La fiabilité évaluée, et autres performances demandées dans les exigences, seront comparées aux objectifs spécifiés.

Dans le cas où les objectifs ne sont pas atteints, l'analyste donnera la contribution des différents constituants du produit, et pourra mener des analyses de sensibilité, sur la base du modèle établi.

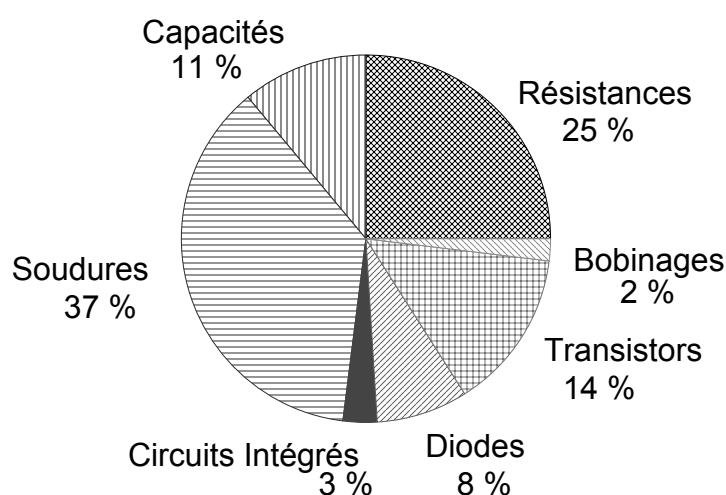
L'objectif est de fournir les éléments qui permettront au responsable technique d'orienter les actions en vue d'améliorer l'architecture du produit.

### 7.6. Retour d'expérience

Bien que non traité dans cette MP, il est à rappeler l'importance de la mise en place d'une structure de traitement des retours d'expérience, en particulier pour l'enrichissement de banques de données de fiabilité ou de bases de données techniques internes, en vue de crédibiliser les prévisions de fiabilité et d'enrichir la maîtrise des produits développés.

La présentation des données et résultats prévisionnels pourra être orientée afin de faciliter le traitement des retours d'expérience. Par exemple, la répartition des taux de défaillance du produit pourra être présentée par type de composant comme le montre l'exemple ci-dessous :

Répartition du taux de défaillance  
par type de composant



**EXEMPLE DE PRESENTATION  
DES DONNEES PREVISIONNELLES**



## 8. DOCUMENTS ET RESULTATS ATTENDUS

Un document d'évaluation de fiabilité du produit sera établi à l'issue des analyses menées, pour chaque phase du projet.

Ce document devra présenter clairement :

- une **description** succincte du produit :

- . identification des références des documents de définition/description et/ou de spécifications,
- . schémas fonctionnels, description technique, modes opératoires,
- . rappel des objectifs de fiabilité,

- la **démarche** et les **moyens** mis en oeuvre pour mener l'évaluation :

- . méthodes,
- . banques de données,
- . outils : dans le cas où un outil est utilisé, les données et le modèle peuvent être fournis au client sous une forme négociée a priori,

- les **hypothèses** et **résultats** de l'analyse :

a. modèle :

- . hypothèses faites lors de l'élaboration du modèle de fiabilité,
- . modèle de fiabilité

b. données du modèle

- . origine des données, méthode de calcul,
- . hypothèses : températures spécifiées (par exemple : la température moyenne de fin de vie ou la température maximale d'acceptance...), derating, niveau qualité...
- . données calculées, sous forme de tableaux, par élément.

c. résultats détaillés puis globaux de l'évaluation :

- . hypothèses de traitement : durée, nombre de simulation (s'il y a lieu)...
- . résultats détaillés par sous-ensemble du produit. Les résultats détaillés seront présentés en cohérence avec le modèle établi. Par exemple, pour les BDF, la fiabilité des différents blocs du BDF sera clairement donnée.
- . résultats globaux, en vue d'être comparés aux objectifs,
- . courbe  $R(t)$  : fiabilité en fonction du temps,



- *l'analyse de sensibilité*, s'il y a lieu,

- *une conclusion* :

- . comparaison de la fiabilité du produit à l'objectif spécifié,
- . rappel des hypothèses critiques pouvant avoir une influence importante sur le résultat,
- . recommandations.



**Annexe 1**

**ILLUSTRATION DE LA DEMARCHE**

La figure 1 illustre de quelle façon l'analyste pourra moduler

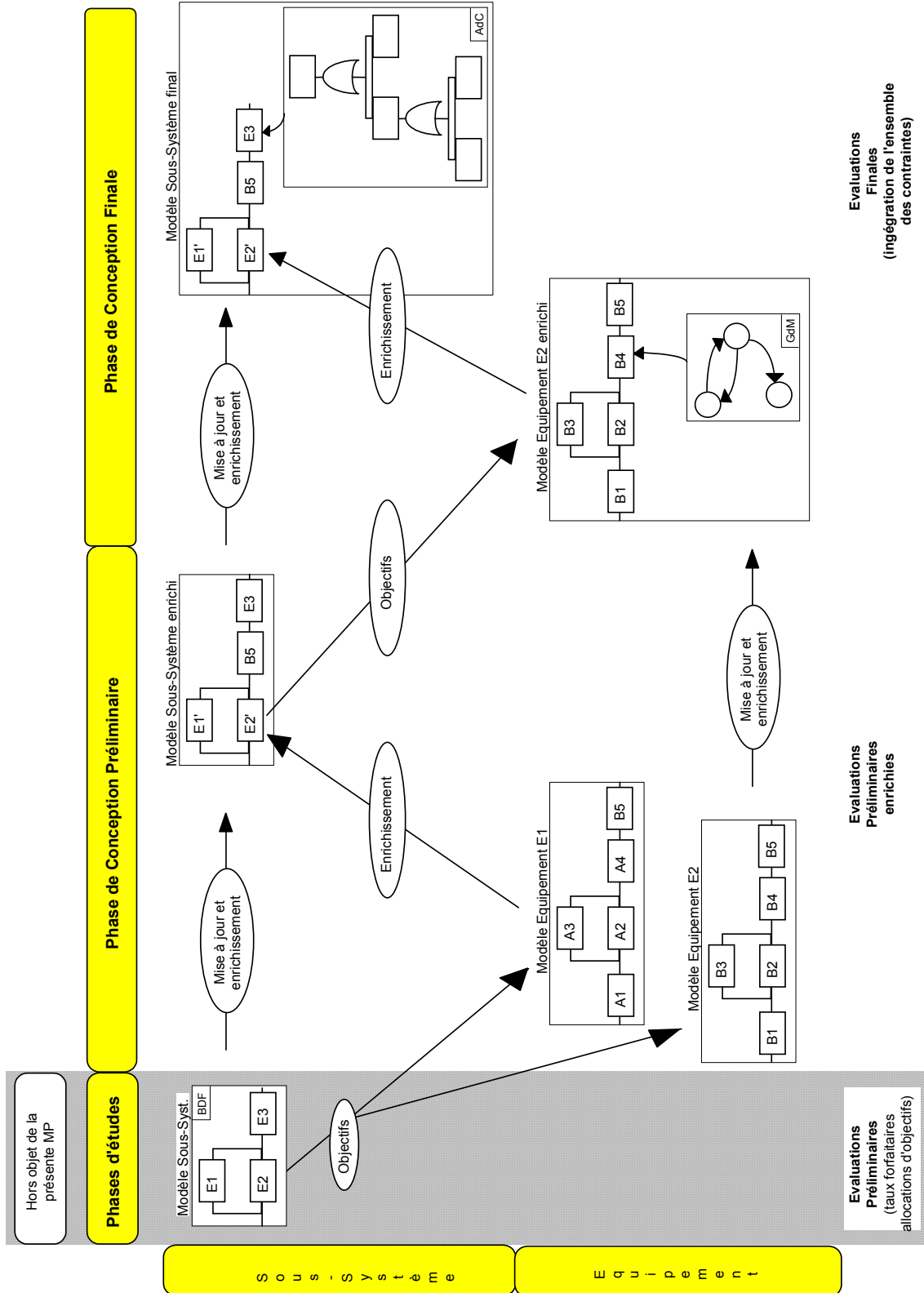
- . le choix de la (ou des) technique(s) de modélisation,
- . la finesse (niveau de détail) et l'exactitude des modèles,
- . la précision des calculs des données,

en fonction

- . des objectifs spécifiés,
- . de l'avancement du projet et de la connaissance des constituants du produit et de leurs conditions d'utilisation,
- . de la complexité des phénomènes à décrire.

Elle précise également comment les résultats de l'AMDEC peuvent enrichir le modèle de fiabilité préliminaire. Dans cet exemple, un mode commun (B5) aux équipements E1 et E2 a été identifié dans l'AMDEC de niveau équipement et intégré en tant que point de panne unique dans le BDF sous-système.

Figure 1 : Modulation de la démarche d'analyse





Page laissée intentionnellement blanche



**Annexe 2**

**METHODES DE MODELISATION**

Les méthodes de modélisation préconisées dans cette MP sont détaillées dans les documents de référence.

Cette annexe a pour but de présenter succinctement les caractéristiques essentielles de chaque technique. Elle donne :

- pour chaque méthode :
  - . documents de référence,
  - . principes et description de la méthode,
  - . intérêts essentiels,
  - . inconvénients/limites,
  
- un tableau de synthèse.

Les méthodes présentées sont :

- . le Bloc Diagramme de Fiabilité (BDF)
- . l'Arbre de Cause (AdC)
- . les Graphes de Markov (GdM)
- . les Réseaux de Pétri (RdP).

**Remarque :**

Le seul objectif de cette annexe est d'introduire chacune des techniques préconisées dans cette MP. Il est bien entendu que le choix d'une méthode plutôt qu'une autre, pour traiter un problème, n'est pas seulement guidé par les caractéristiques des techniques, mais dépendra aussi de critères tels que le besoin exprimé (analyse préliminaire ou fine), les moyens existants (outils...), la maîtrise des techniques par l'analyste...



**BLOC DIAGRAMME DE FIABILITE (BDF)**

**Références :** [R12], [R13], [R4]

**Principes et description :**

Le bloc diagramme de fiabilité d'un système est l'association série et/ou parallèle d'un point de vue fiabilité des éléments participant à la réalisation de la fonction du système.

Association série : Si les éléments sont nécessaires à la réalisation de la fonction du système.

Association parallèle : Si les éléments sont en redondance pour la réalisation de la fonction du système.

Le symbolisme est le suivant :

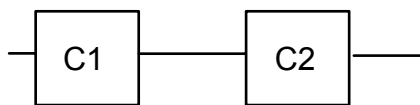


Diagramme Série

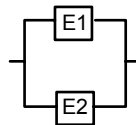


Diagramme parallèle  
(redondance chaude)

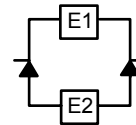


Diagramme parallèle  
(redondance froide)

Les formules mathématiques donnant la fiabilité associée aux configurations les plus courantes sont données page suivante.

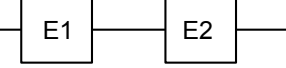
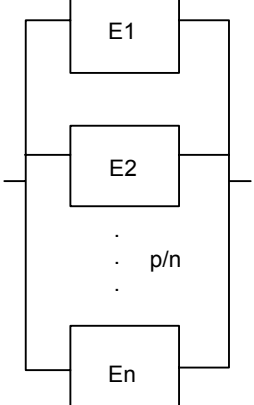
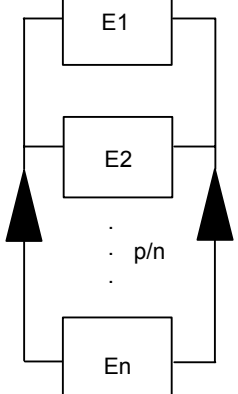
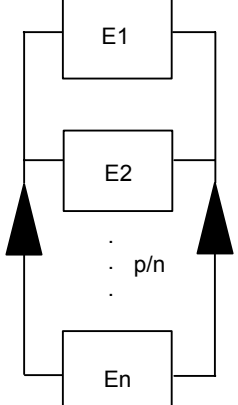
Le bloc diagramme de fiabilité pourra être enrichi par une symbologie complémentaire pour modéliser des systèmes plus complexes (commutateur, ressource, relation de dépendance, etc...).

**Intérêts :**

- Facilité et rapidité d'élaboration du modèle pour les systèmes comprenant des redondances inter-blocs,
- Adapté aux systèmes dont la découpe technique est proche de la découpe fonctionnelle (éléments mono-fonction),
- Visualisation directe des redondances,
- Décomposition du système adaptée en vue d'une évaluation de fiabilité par bloc.

**Inconvénients / limites :**

- Non explicitation précise des défaillances associées aux blocs du diagramme,
- Incapacité à modéliser les phénomènes dynamiques (séquentiels et temporels).

BLOC DIAGRAMME DE FIABILITE		
Symbole	Type de redondance	Fiabilité
	Diagramme Série	$R(t) = \prod_{i=1}^n R_i(t)$
	Redondance chaude p parmi n	$R(t) = \sum_{i=0}^{n-p} C_n^i (1 - e^{-\lambda t})^i e^{-(n-i)\lambda t}$
	Redondance froide p parmi n (taux d'utilisation 100% $\tau = 1$ )	$R(t) = e^{-\alpha_0 t} + \sum_{i=1}^{n-p} \frac{\prod_{j=0}^{i-1} \alpha_j}{\lambda_0^{i-1} i!} (1 - e^{-\lambda_0 t})^i e^{-\alpha_i t}$ <p>avec <math>\lambda_0 = \lambda / k</math> (<math>\lambda</math> dormant)</p> $\alpha_i = p \lambda + (n - p - i) \lambda_0$
	Redondance froide p parmi n (taux d'utilisation 100% [ $0 < \tau < 1$ ])	$R(t) = e^{-\alpha_0 t} + \sum_{i=1}^{n-p} \frac{\prod_{j=0}^{i-1} \alpha_j}{\lambda_0^{i-1} i!} (1 - e^{-\lambda_0 t})^i e^{-\alpha_i t}$ <p>avec <math>\lambda_0 = \lambda / k</math> (<math>\lambda</math> dormant)</p> $\alpha_i = (p \cdot \tau) \lambda + (n - p \cdot \tau - i) \lambda_0$ <p><math>\tau =</math> taux d'utilisation des éléments fonctionnant nominalement</p>

**ARBRE DE CAUSE (AdC)**

**Références :** [R12], [R13]

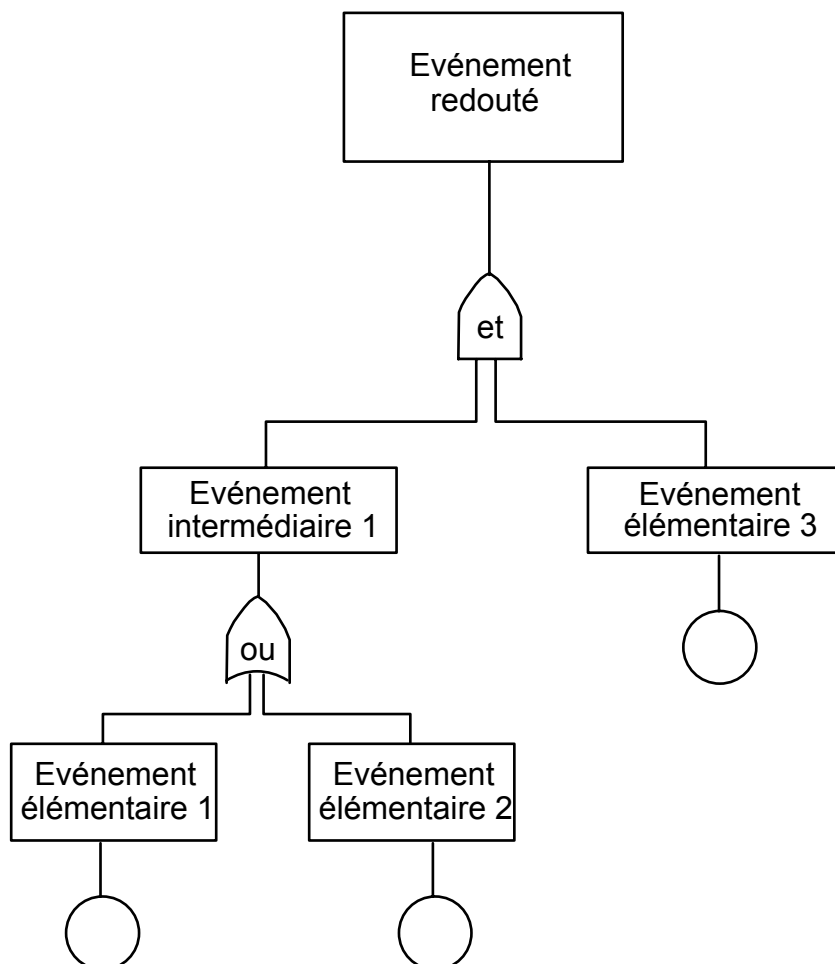
**Principes et description :**

Méthode graphique permettant la recherche déductive systématique de toutes les combinaisons possibles d'événements qui entraînent un événement redouté.

Une combinaison d'événements (scénario) correspond à une association logique d'événements via des portes logiques.

Les associations de base correspondent à des "OU" et "ET" logiques. D'autres types d'association sont cependant disponibles, telles que le "OU conditionnel", le "ET conditionnel", les Combinaisons (p/n)... L'ensemble des symboles est présenté dans les documents de référence.

Formalisme de l'Arbre de Cause :



La démarche d'analyse est la suivante :

1. Etablissement de l'arbre de défaillance, représentant les scénarios d'événements entraînant l'occurrence de l'événement redouté de plus haut niveau.
2. Réduction de l'équation booléenne non minimale associée à l'arbre de défaillance, par application des propriétés de l'algèbre de Boole, en vue d'identifier les coupes minimales entraînant l'événement redouté.
3. Traitement des coupes minimales.

L'étape 2 est indispensable avant tout traitement quantitatif d'un arbre de défaillance. Elle permet entre autre de mettre en évidence les modes communs du système.

**Intérêts :**

- Démarche structurée et descendante: possibilité de moduler le niveau de détail de l'analyse,
- Prise en compte d'événements de types différents (défaillance, erreur humaine, événement extérieur au système, événement normal...)
- Adapté pour l'identification des modes communs d'un système.

**Inconvénients/limites :**

- Systèmes fortement redondants,
- Non adapté à la modélisation des phénomènes dynamiques (séquentiels et temporels).

**GRAPHES DE MARKOV (GdM)**

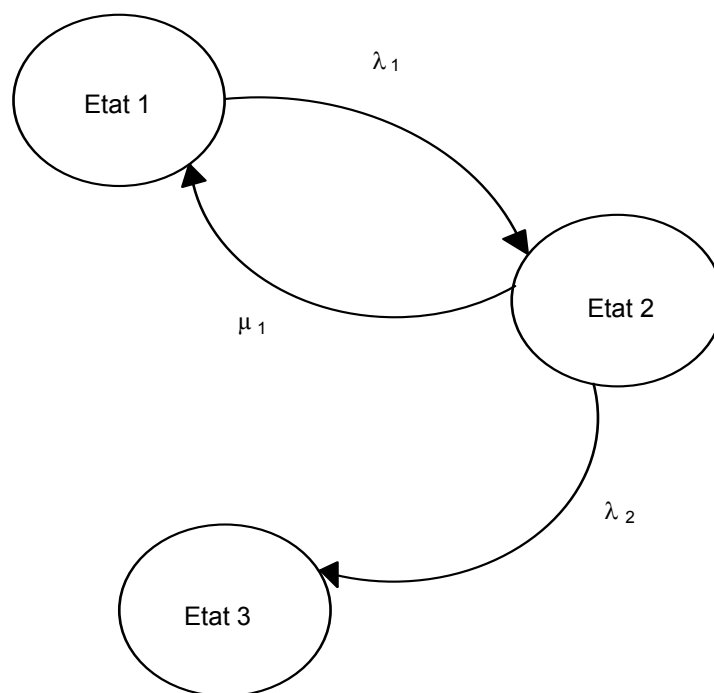
**Références :** [R12], [R13], [R18], [R19]

**Principes et description :**

Les Graphes de Markov sont des graphes d'états à taux de transition constants.

Ils permettent de modéliser les évolutions d'un produit entre ses différents états de fonctionnement, lorsque les transitions entre ces états sont caractérisées par des lois à taux constants.

Les états du système sont représentés par des cercles ; les transitions entre états sont représentées par des arcs orientés.



La matrice des taux de transition associée à ce graphe est la suivante :

	1	2	3
1		$\lambda_1$	
2	$\mu_1$		$\lambda_2$
3			

Il est, en général, préférable d'établir directement la matrice des taux de transition, en particulier pour les systèmes complexes, en utilisant si besoin la technique d'insertion matricielle, afin de limiter les risques d'erreur (exhaustivité des états et des transitions).

La démarche de construction d'un graphe de Markov est la suivante :

1. Détermination de l'ensemble des états d'un système,
2. Identification des transitions entre les états, caractérisées par des taux de transition. Dans les applications liées aux analyses de sûreté de fonctionnement, les taux de transitions sont essentiellement des taux de défaillance  $\lambda$  ou des taux de réparation  $\mu$ .

**Intérêts :**

- Adapté à l'analyse de systèmes réparables,
- Intégration dans un modèle unique de l'ensemble des états d'un système (fonctionnement nominal, dégradé, en réparation, en panne...),
- Directement utilisable pour les évaluations de disponibilité.

**Inconvénients/limites :**

- Limité aux processus à taux de transition inter-états constants. Entre autre, les GdM ne permettent pas la modélisation de phénomènes déterministes.
- Modélisation difficile, sans outil adapté, pour les systèmes comprenant un nombre important d'états.



## RESEAUX DE PETRI (RdP)

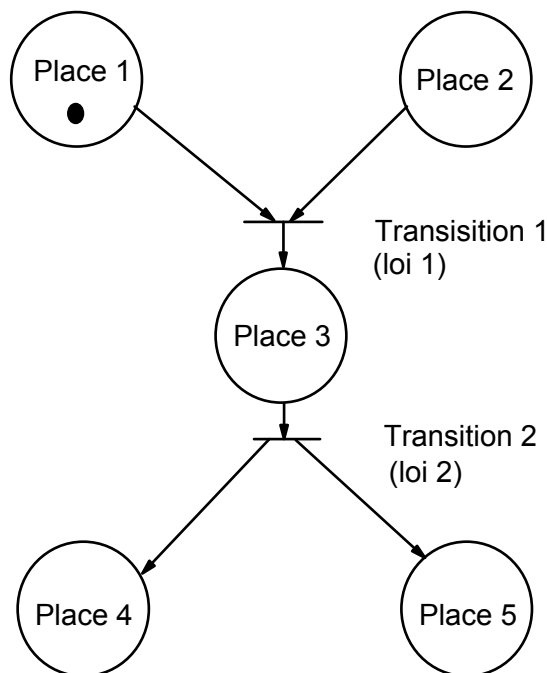
Références : [R13], [R15], [R16], [R17]

Principes et description :

Les Réseaux de Pétri sont un outil graphique et mathématique permettant de modéliser et de simuler le comportement de systèmes. Ils sont particulièrement adaptés pour les applications où les notions d'événements et d'évolutions simultanées sont très importantes.

Un RdP comprend :

- des PLACES, caractérisées par un marquage à un instant donné (nombre de jetons dans la place),
- des TRANSITIONS entre places, caractérisées par des conditions de marquages des places amont et une loi de tirage de la transition,
- des ARCS.



**Intérêts :**

- Richesse du modèle: prise en compte des aspects séquentiels, temporels (synchronisations, conditionnements),
- Possibilité de modéliser tout type de loi de transition,
- Description dans un modèle unique de l'ensemble des comportements d'un système,
- Directement utilisable pour l'évaluation de performances plus larges : études de disponibilité, temps de séjours et nombre de passage dans chaque état du système, simulations de comportement...

**Inconvénients/limites :**

- Modélisation difficile, sans outil adapté, pour les systèmes nécessitant des modèles importants: difficulté de validation du modèle.

**TABLEAU DE SYNTHESE DES METHODES DE MODELISATION**

Cette synthèse ne reprend pas l'ensemble des caractéristiques et intérêts des méthodes décrites dans la MP. Elle se limite à la présentation de l'intérêt de ces méthodes pour la modélisation de certains types de phénomènes: redondance chaude, redondance froide, aspects séquentiels et aspects temporels.

Caractéristiques	Redondances		Phénomènes Séquentiels	Phénomènes Temporels
	Chaudes	Froides		
BDF	OUI	OUI	NON	NON
AdC	OUI	Difficile	Partiel (Redondance avec priorité)	NON
GdM	OUI	OUI	OUI	NON
RdP	OUI	OUI	OUI	OUI



Page laissée intentionnellement blanche



**Annexe 3**

**METHODES DE CALCUL DES DONNEES DU MODELE**

Cette annexe décrit succinctement deux modes de calcul des taux de défaillance de composants, données d'entrée des modèles de fiabilité :

- la méthode Part Count,
- la méthode Part Stress.

Ces deux méthodes sont détaillées dans le document MIL-HDBK-217 [A1].

Les exemples présentés dans cette annexe sont extraits du document MIL-HDBK-217-E.

Les méthodes Part Count et Part Stress consistent en l'utilisation d'un modèle mathématique donnant le taux de défaillance d'un composant en fonction d'un ensemble de paramètres tels que : l'environnement, la température, les contraintes électriques, le niveau de qualification...

**Exemple** : modèle mathématique associé aux circuits intégrés linéaires, bipolaires et MOS.

#### **Monolithic Bipolar and MOS Linear Devices**

*Part operating failure rate model ( $\lambda_p$ ) :*

$$\lambda_p = \pi_Q (C_1 \pi_T \pi_V + C_2 \pi_E) \pi_L \text{ Failures}/10^6 \text{ hours}$$

where :

$\lambda_p$  is the device failure rate in F/10<sup>6</sup> hours

$\pi_Q$  is the quality factor, Table 5.1.2.7-1

$\pi_T$  is the temperature acceleration factor, based on technology (Table 5.1.2.7-4) and is found in Tables 5.1.2.7-10 or 5.1.2.7-13

$\pi_V$  is the voltage stress derating factor, Table 5.1.2.7-14

$\pi_E$  is the application environment factor, Table 5.1.2.7-3

$C_1$  is the circuit complexity factor based on transistor count as follows :

For 1 to 100 transistors,  $C_1 = 0.01$

For > 100 to 300 transistors,  $C_1 = 0.02$

For > 300 to 1000 transistors,  $C_1 = 0.04$

$C_2$  is the package complexity failure rate, Table 5.1.2.7-16

$\pi_L$  is the device learning factor, Table 5.1.2.7-2

La **méthode Part Count**, consiste à utiliser directement les résultats du traitement de ces modèles, effectué en considérant des valeurs moyennes forfaitaires pour la plupart des paramètres du modèle; seuls le niveau de qualification des composants et leur environnement réels sont pris en compte.

Ces résultats (taux de défaillance) sont donnés dans des tables, par type de composant.

**Exemple** : table donnant les taux de défaillance des différents types de résistances, pour différents environnements. Ces taux de défaillance sont à corriger en fonction du facteur qualité (multiplicatif) donné dans le tableau associé.

**GENERIC FAILURE RATE<sub>0</sub>,  $\lambda_G$ , (f./10<sup>6</sup> hr.) FOR RESISTORS (Cont'd)**  
(See table 5.2-29 for N<sub>Q</sub> Values)

RESISTORS, FIXED			USE ENVIRONMENT												
CONSTRUCTION	SITL MIL-A-SPEC		G <sub>F</sub>	G <sub>M</sub>	M <sub>L</sub>	M <sub>FA</sub>	M <sub>FF</sub>	M <sub>P</sub>	M <sub>M</sub>	M <sub>S</sub>	M <sub>SB</sub>	M <sub>U</sub>	M <sub>UU</sub>	S <sub>F</sub>	U <sub>SL</sub>
Composition	RCR	39008	.0021	.011	.038	.012	.0076	.0052	.0095	.0038	.0029	.033	.0048	.0005	.015
Composition	RC	11	.011	.054	.19	.058	.038	.026	.048	.019	.015	.17	.024	.0025	.076
Film	RLR	39017	.0033	.012	.047	.017	.013	.011	.019	.0064	.0057	.027	.017	.0005	.034
Film	RL	22684	.016	.061	.23	.085	.063	.057	.095	.032	.029	.14	.086	.0025	.17
Film	MHR	55182	.0037	.014	.054	.019	.014	.013	.021	.0072	.0064	.031	.019	.0006	.038
Film	RM	10509	.018	.070	.27	.097	.072	.064	.11	.036	.032	.16	.093	.0028	.19
Film Power	RD	11804	.030	.11	.51	.20	.15	.13	.22	.063	.063	.21	.22	.012	.41
Film Network	RZ	83401	.087	.047	1.8	.52	.38	.27	.51	.17	.15	1.5	.26	.025	.79
Wire wound	SSR	39005	.021	.095	.40	.16	.11	.10	.16	.046	.046	.18	.16	.013	.31
Accurate	RS	93	.11	.48	2.0	.78	.55	.52	.80	.23	.23	.91	.82	.064	1.6
Wire wound	RSR	39007	.023	.15	.65	.24	.18	.16	.25	.076	.076	.32	.21	.0083	.45
Power	RW	26	.12	.75	3.3	1.2	.90	.81	1.2	.38	.38	1.6	1.1	.042	2.1
Wire wound	RER	39009	.022	.091	.39	.14	.11	.093	.15	.044	.044	.20	.12	.0080	.26
Ch. Mount	RE	18546	.11	.45	2.0	.72	.53	.47	.72	.22	.22	.99	.60	.040	1.1

**Table 5.2-29**  
 **$\pi_Q$  FACTOR FOR RESISTORS AND CAPACITORS**

FAILURE RATE LEVEL	* $\pi_Q$
L	1.5
M	1.0
P	.3
R	.1
S	.03

Dans le cas de la **méthode Part Stress**, les taux de défaillance sont à calculer à partir des modèles mathématiques en intégrant l'ensemble des valeurs réelles des paramètres, et ce pour chaque composant.

**Exemple** : modèle complet (modèle mathématique + valeurs des paramètres) associé aux diodes de groupe IV (Silicon, general purpose).

**DISCRETE SEMICONDUCTORS**

**DIODES, GENERAL PURPOSE**

**Diodes, Groud IV**

**SPECIFICATION**

MIL-S-19500

**STYLE**

**DESCRIPTION**

Silicon, General Purpose  
Germanium, General Purpose

Part operating failure rate model ( $\lambda_p$ ) :

$$\lambda_p = \lambda_0 (\pi_E \times \pi_Q \times \pi_R \times \pi_A \times \pi_{S2} \times \pi_C) \text{ failures}/10^6 \text{ hours}$$

where the factors are shown in Tables 5.1.3.4-1 through 5.1.3.4-8.

**GROUP IV TRANSISTORS ENVIRONMENTAL MODE FACTORS**

ENVIRONMENT	$\pi_E$	ENVIRONMENT	$\pi_E$
G <sub>B</sub>	1	A <sub>IB</sub>	30
G <sub>MS</sub>	1.4	A <sub>IA</sub>	25
G <sub>F</sub>	3.9	A <sub>IF</sub>	35
G <sub>M</sub>	18	A <sub>UC</sub>	25
M <sub>P</sub>	12	A <sub>UT</sub>	30
N <sub>SB</sub>	4.8	A <sub>UB</sub>	50
N <sub>S</sub>	4.8	A <sub>UA</sub>	40
N <sub>U</sub>	21	A <sub>UF</sub>	50
N <sub>H</sub>	19	S <sub>F</sub>	1
N <sub>UU</sub>	20	M <sub>FF</sub>	12
A <sub>RW</sub>	27	M <sub>FA</sub>	17
A <sub>IC</sub>	15	U <sub>SL</sub>	36
A <sub>IT</sub>	20	M <sub>L</sub>	41
		C <sub>L</sub>	690



**DISCRETE SEMICONDUCTORS**

**DIODES, GENERAL PURPOSE**

**$\pi_Q$  FOR GROUP IV DIODES**

Quality Level	$\pi_Q$
JANTXV	0.15
JANTX	0.3
JAN	1.5
Lower*	7.5
Plastic**	15.0

\* Hermetic packaged devices

\*\* Devices sealed or encapsulated with organic materials

**$\pi_R$  FOR GROUP IV DIODES**

Current Rating (amps)	$\pi_R$
$\leq 1$	1
> 1 to 3	1.5
> 3 to 10	2.0
> 10 to 20	4.0
> 20 to 50	10.0

**$\pi_A$  FOR GROUP IV DIODES**

Application	$\pi_A$
Analog Circuits (<500 ma)	1.0
Switching (<500 ma)	0.6
Power Rectifier ( $\geq 500$ ma)	1.5
Poqwer Rectifier (HV stacks) Vmax > 600	2.5/junction

**DISCRETE SEMICONDUCTORS**

**DIODES, GENERAL PURPOSE**

**$\pi_{S2}$  FOR GROUP IV DIODES**

Voltage Stress,  $S_2 = \frac{\text{Applied } (V_R)}{\text{Rated } (V_R)} \times 100$

$V_R$  = diode reverse voltage

<b><math>S_2</math> (Percent)</b>	<b><math>\pi_{S2}</math></b>
0 to 60	0.70
> 60 to 70	0.75
> 70 to 80	0.80
> 80 to 90	0.90
> 90 to 100	1.0

**$\pi_C$  CONSTRUCTION FACTOR**

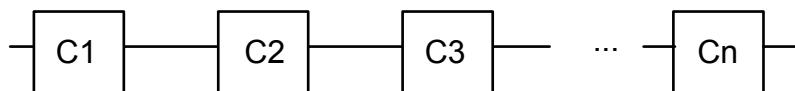
<b>Contact Construction</b>	<b><math>\pi_C</math></b>
Metallurgically Bonded	1
Non-metallurgically Bonded (spring loaded contacts)	2



Exemple d'utilisation des **méthodes Part Count et Part Stress** :

Pour le calcul du taux de défaillance d'un équipement, le modèle de fiabilité associé à l'équipement est souvent un BDF série. On considère dans ce cas que tous les composants de l'équipement pris en compte dans l'évaluation de fiabilité sont en série, c'est-à-dire nécessaires d'un point de vue fiabilité.

Le modèle est du type :



On calcule alors le taux de défaillance  $\lambda_i$  de chaque composant  $C_i$ , soit suivant la méthode part count, soit suivant la méthode part stress si les caractéristiques opérationnelles des composants sont connues.

Etant donné le modèle de fiabilité de l'équipement, le taux de défaillance  $\lambda$  de l'équipement s'écrit alors :

$$\lambda = \sum_{i=1}^n \lambda_i$$



## Annexe 4

**EXEMPLE : Complémentarité des méthodes de modélisation**

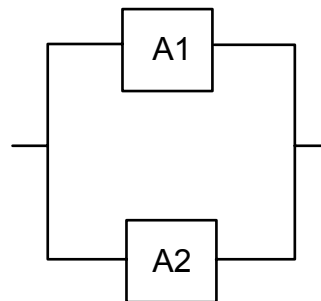
**Exemple 1 : Redondance chaude 2 pour 1**

**Domaine d'application** : Soient deux équipements A1 et A2 identiques, assurant la même fonction et utilisés de façon simultanée.

**Hypothèse** : A1 et A2 ne sont pas réparables. Les pannes de A1 et A2 sont indépendantes c'est à dire que la panne de A1 ou A2 n'entraîne pas la perte de la fonction à assurer.

**a) Modélisation par block diagramme de fiabilité**

On a le BDF suivant :



En notant :  $P(A_i)$  la probabilité de bon fonctionnement pendant la durée de mission, (c'est-à-dire la fiabilité) de l'équipement  $A_i$ .

R : la fiabilité de l'ensemble

On a  $P(A1) = P(A2) = P(A)$

et

$$R = P(A1 + A2)$$

$$R = P(A1) + P(A2) - P(A1)P(A2)$$

$$R = 2P(A) - [P(A)]^2$$

$$R = 1 - [1 - P(A)]^2$$

Rappel :  $R(t) = e^{-\lambda(t).t} = e^{-\lambda.t}$  si  $\lambda$  est constant.

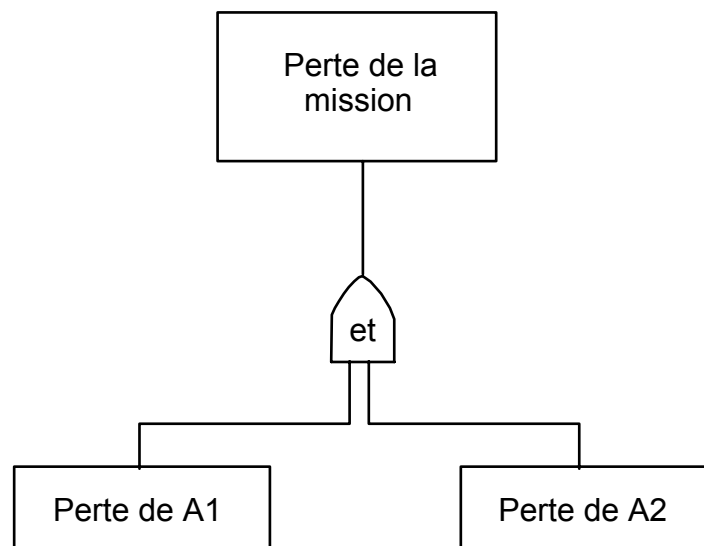
**Application numérique :**

Si la durée de la mission est de 5 ans (43 800 heures) et que le taux de défaillance d'un équipement est de  $\lambda = 1\ 000$  FIT (1 FIT =  $10^{-9}$  panne/heure)

$$R_{5\text{ans}} = 1 - (1 - e^{-1000 \cdot 10^{-9} \times 43800})^2 = 0,9981$$

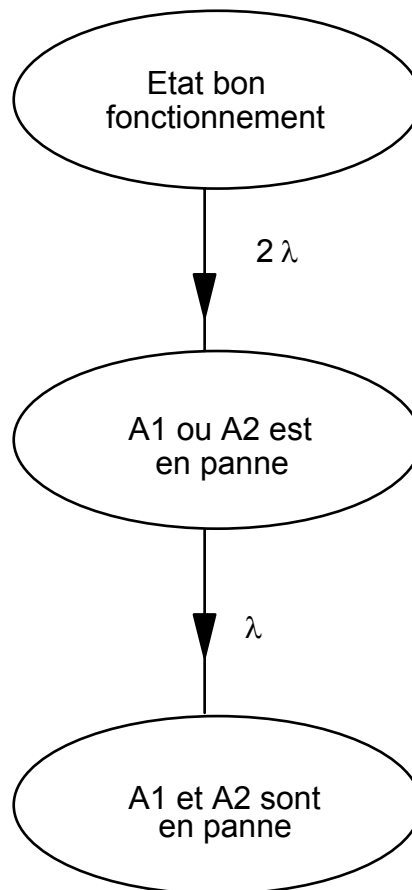
**b) Modélisation par un Arbre de Cause**

L'arbre de cause est le suivant :



c) Modélisation par Graphe de Markov

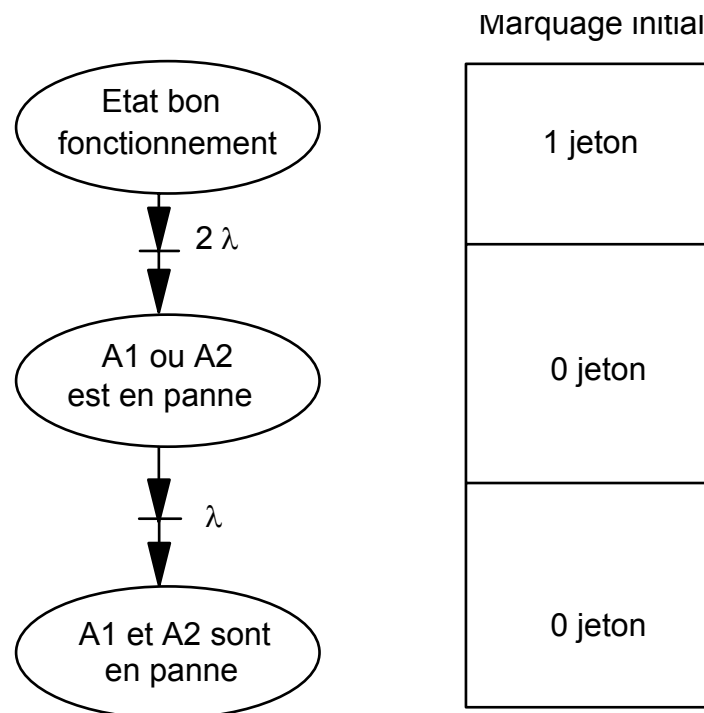
Le graphe de Markov est le suivant :





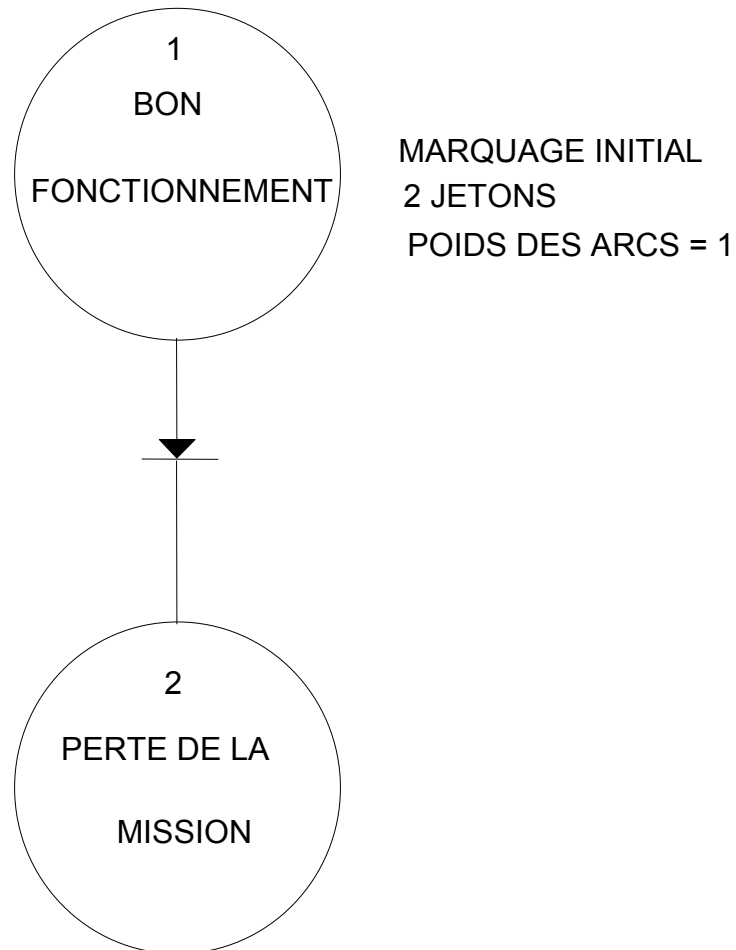
d) Modélisation par réseau de Pétri

Le RdP est le suivant :



La modélisation par réseau de Pétri n'apporte ici aucune plus value vis à vis de la modélisation par Graphe de Markov.

Afin de simplifier ce modèle vis à vis du graphe de Markov on pourrait faire le réseau de Petri suivant :



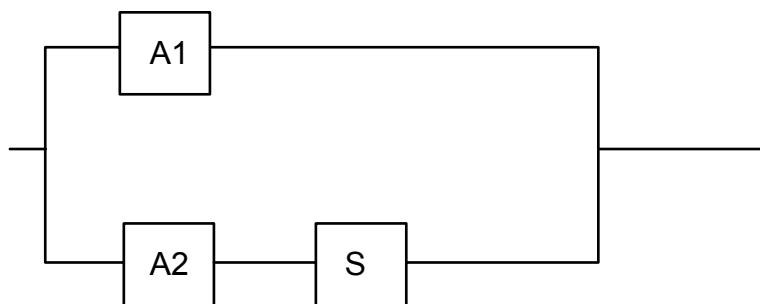
L'inconvénient est de rendre plus délicate l'observation des états dégradés. Il faudrait pour cela :

- soit observer les places 1 et 2 en même temps
- soit disposer d'un outil permettant de définir des états comme :
  - \* Etat nominal : marquage de la place 1 = 2
  - \* Etat dégradé : marquage de la place 1 = 1
  - \* Perte mission : marquage de la place 1 = 0

**Remarque sur l'exemple 1**

La modélisation par graphe de Markov et par Réseau de Pétri ne présente qu'un faible intérêt pour cet exemple et compte tenu des hypothèses simplificatrices. Maintenant, si on suppose qu'en cas de défaillance de A1, il est nécessaire de commuter un switch S pour utiliser A2, on peut dire que le dispositif A2 ne sera disponible que si le dispositif S fonctionne.

On obtient le block **diagramme de fiabilité** suivant :



Si le bon fonctionnement de S s'exprime en probabilité instantanée de succès à la sollicitation, l'utilisation de BDF pour la résolution numérique est problématique puisque cette association n'est ni une véritable association parallèle (S ne suit pas une loi exponentielle) ni une association série. La probabilité de bon fonctionnement du système s'exprime :

$$TR = P (A1 + A2.S)$$

$$TR = P (A1) + P (A2). P (S) - P (A1). P (A2). P (S)$$

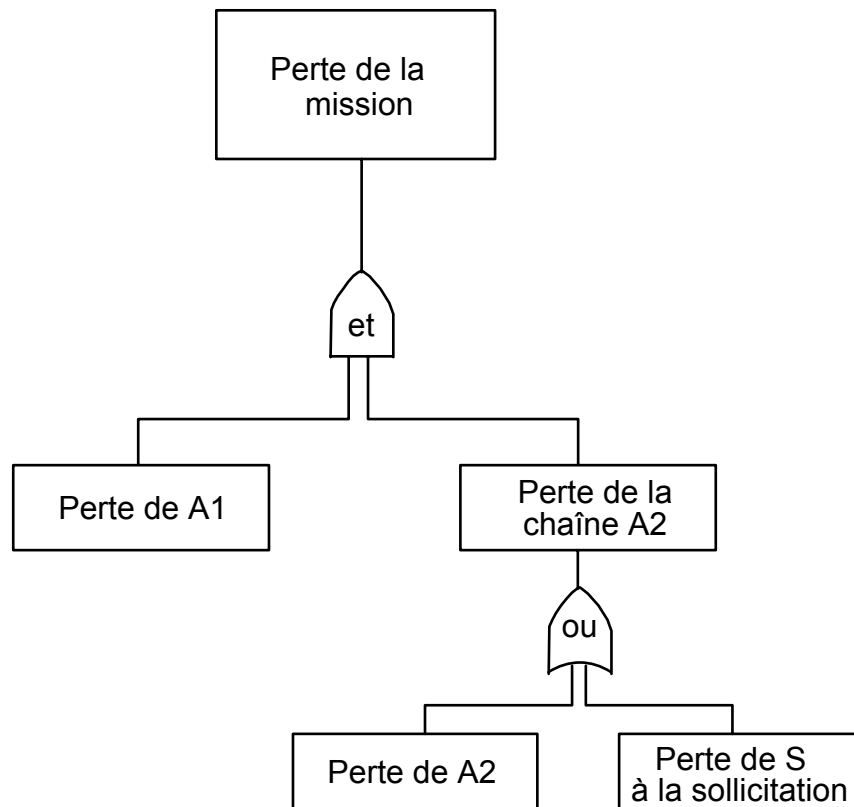
$$TR = P (A) [1 + P (S) - P (A). P (S)]$$

**Application numérique**

Avec les mêmes durées et taux de défaillance que précédemment et en supposant que  $P (S) = 0,8$  (80 % de chance que S commute correctement), on obtient :

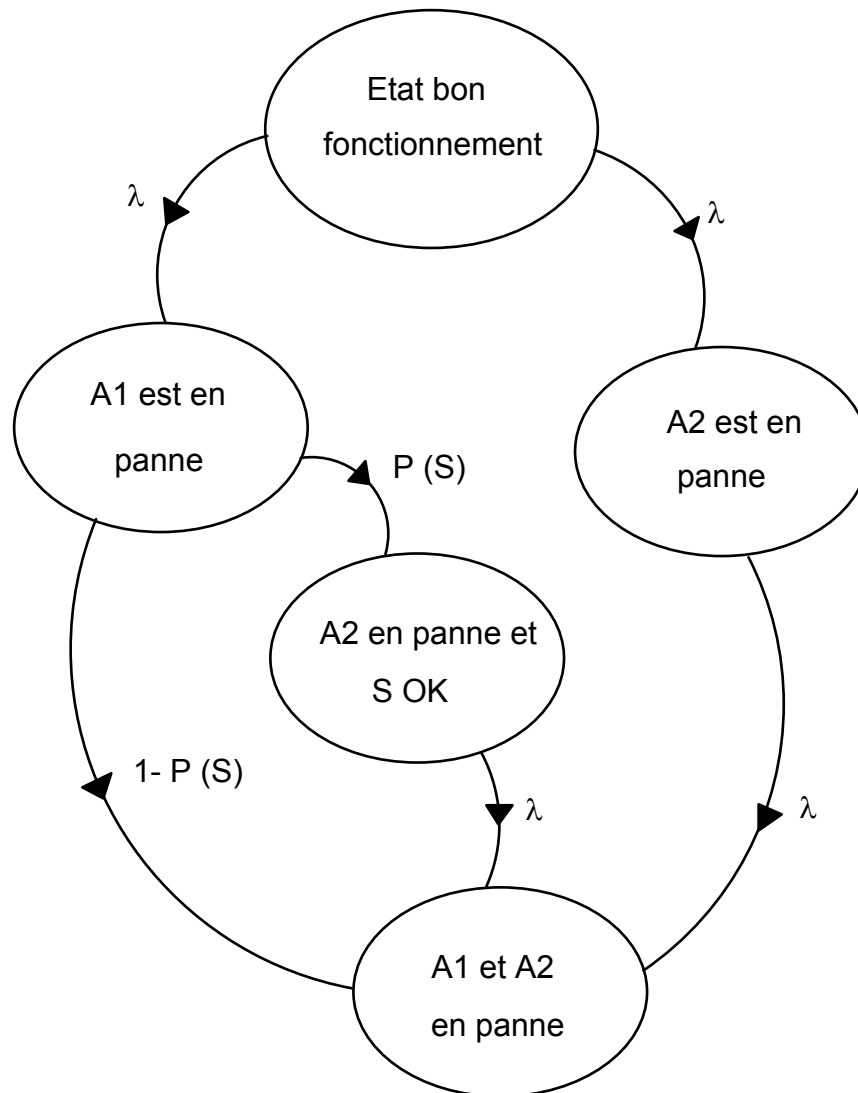
$$R = 0,9899$$

La modélisation par Arbre de Cause devient



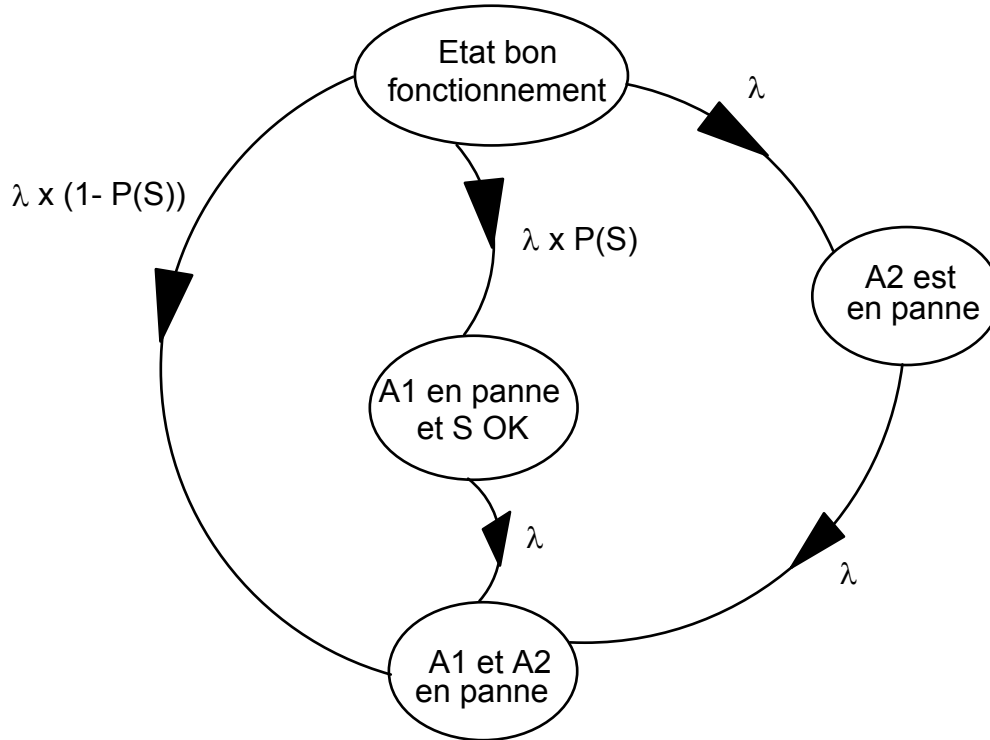
Ici, on ne rencontre aucun problème pour la résolution numérique avec des outils classiques, les événements étant facilement modélisables.

La modélisation par graphe de Markov devient :

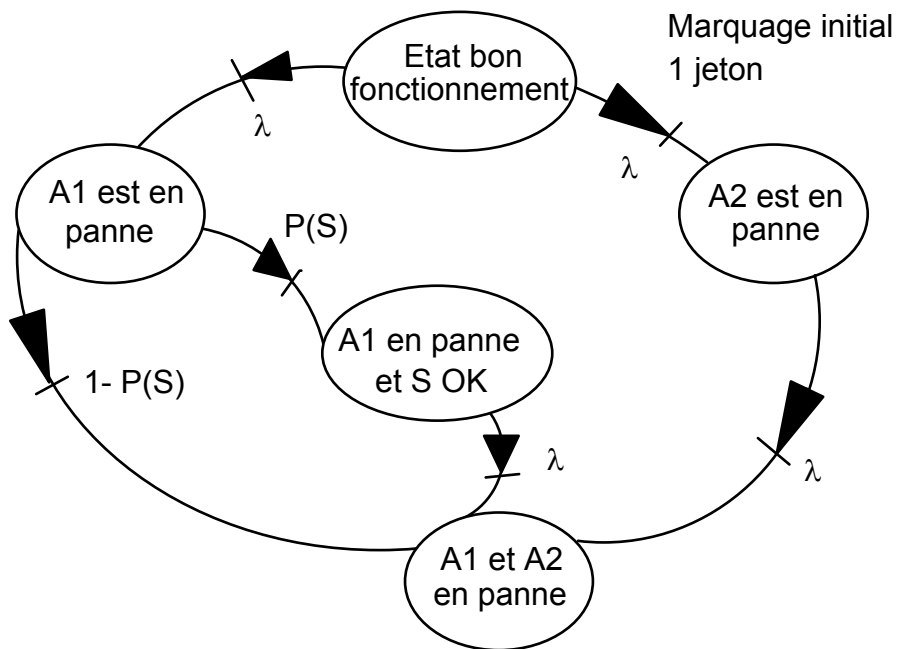


Mais ce graphe n'est pas un véritable graphe de Markov, les transitions  $P(S)$  et  $1-P(S)$  n'étant pas homogène à un taux de transition constant.

Pour obtenir un véritable graphe de Markov, il faut effectuer la transformation suivante :



La modélisation par réseau de Pétri devient par exemple :



Ici, les différents modes de fonctionnement peuvent être modélisés tels qu'ils se déroulent réellement. Des transitions instantanées avec une probabilité constante peuvent être modélisées.

### Exemple 2 - Redondances mixtes

Domaine d'application :

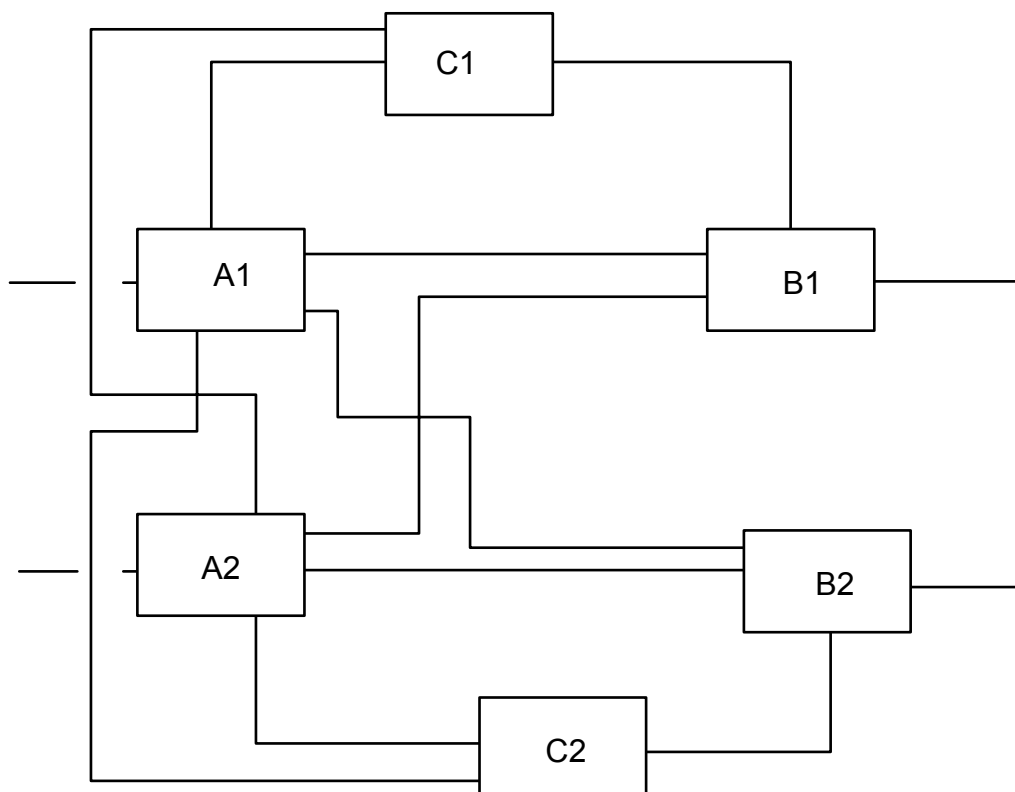
Soient A1, A2, B1, et B2 des cartes de traitement de signal, C1 et C2 des cartes d'alimentation. Ces cartes sont supposées non réparables.

A1 et A2 sont identiques et assurent la même fonction. A1 est utilisé en priorité, A2 n'est pas mis sous tension tant que A1 fonctionne correctement et n'est utilisé que si A1 tombe en panne.

B1 et B2 sont identiques, assurent la même fonction et sont utilisés de façon simultanée.

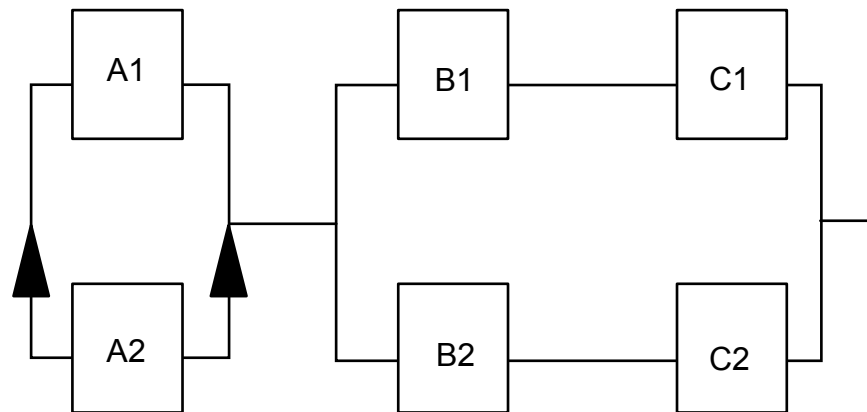
Chacune des cartes C peut alimenter indifféremment A1 et A2. Mais C1 ne peut alimenter que B1 et C2, B2.

Le synoptique électrique est :



a) Modélisation par bloc diagramme de fiabilité

On a le BDF suivant :

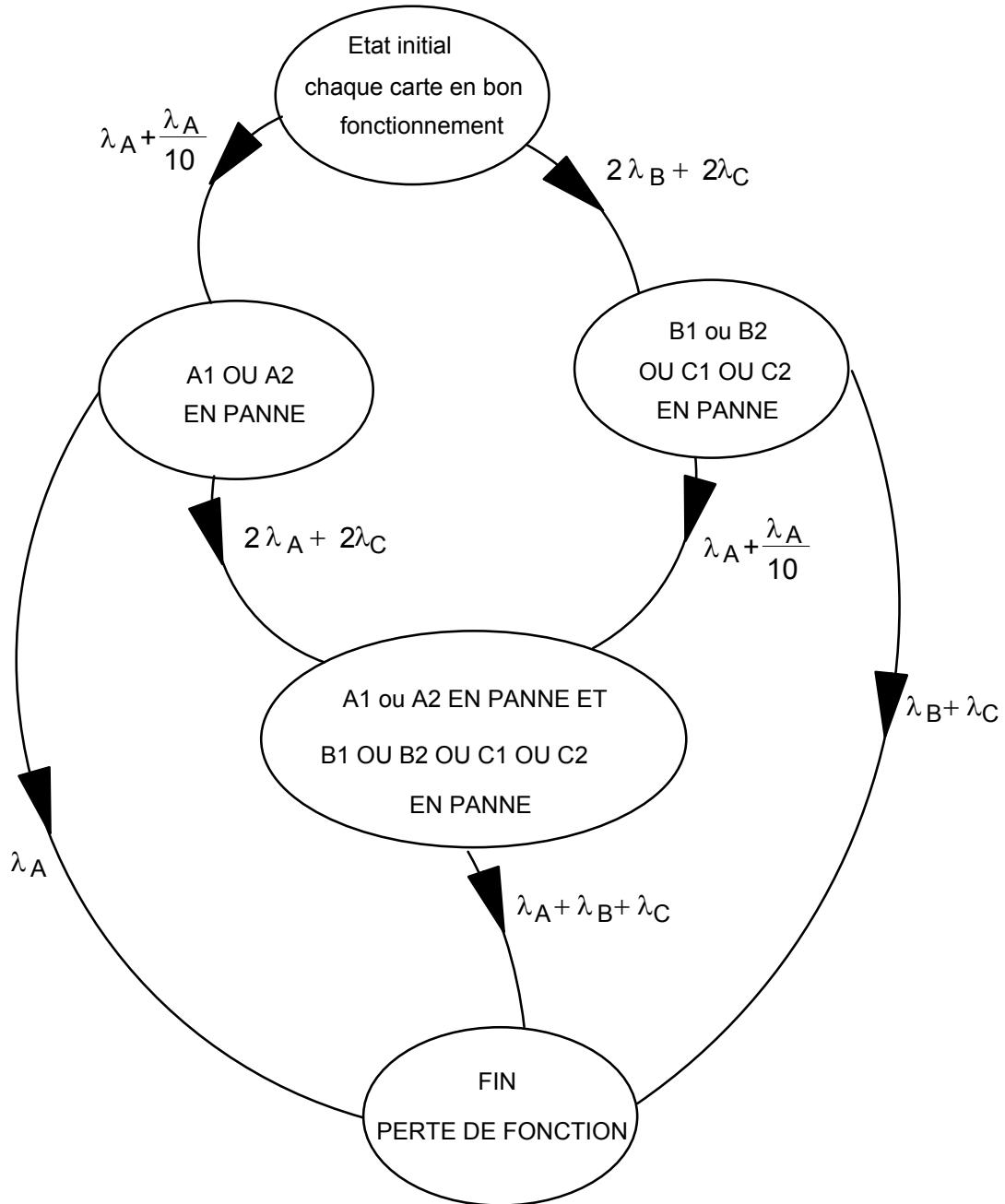


b) Modélisation par Arbre de Cause

Cette méthode est peu adaptée au traitement de cet exemple. En effet, des redondances froides sont difficilement modélisables à cause du facteur dormant appliqué à l'élément non alimenté.

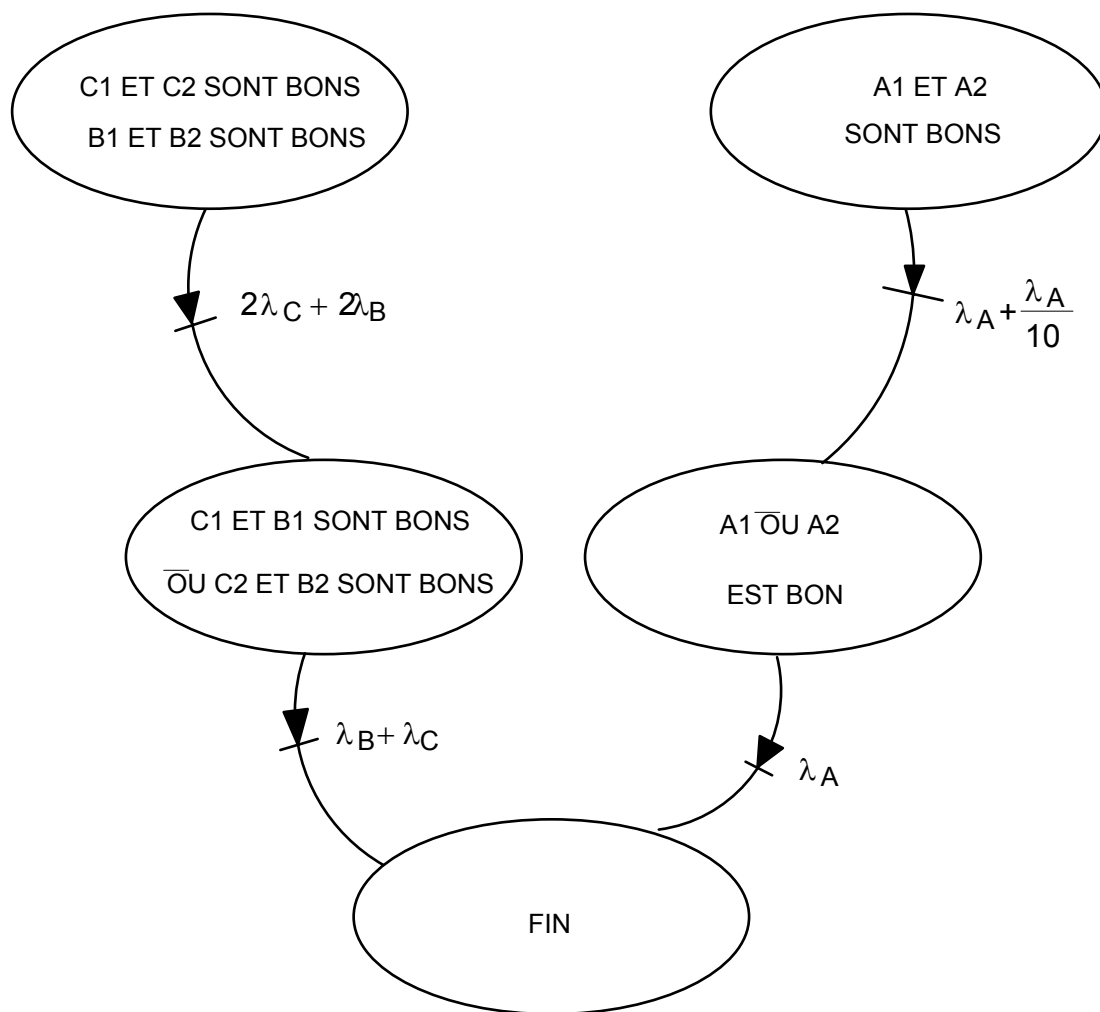


c) Modélisation par graphe de Markov



d) Modélisation par réseau de Pétri

On a le RDP suivant :



On voit que les chaînes fonctionnelles sont modelisables de façon indépendante.



**Annexe 5**

**METHODE D'EXPLOITATION DES RESULTATS D'ESSAIS  
DE FIABILITE AVEC LA LOI DU Khi DEUX**

Dans le cas d'exploitation des résultats d'essais de fiabilité pour évaluer le taux de défaillance des composants élémentaires, la loi du Khi Deux sera utilisée.

Soit T le temps cumulé d'essai pendant lequel les composants ont fonctionné correctement.

Soit f le nombre total de défaillances rencontrées.

Soit  $n = 2f + 2$

Le taux de défaillance peut être évalué à l'aide de la formule suivante :

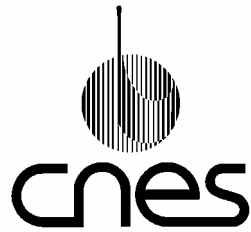
$$\text{Taux de défaillance } (10^{-9}) = \frac{\chi^2_{\bar{n}} \times 10^9}{2 T}$$

avec pour  $\chi^2$  (Khi deux) leurs valeurs suivantes :

**DISTRIBUTION  $\chi^2$  (CONFIANCE 60%)**

n	$\chi^2$	n	$\chi^2$	n	$\chi^2$	n	$\chi^2$
1	0.708	10	10.500	19	19.900	36	37.500
2	1.830	11	11.500	20	21.000	38	39.600
3	2.950	12	12.600	22	23.000	40	41.600
4	4.040	13	13.600	24	25.100	42	43.700
5	5.130	14	14.700	26	27.200	44	45.700
6	6.210	15	15.700	28	29.200	46	47.800
7	7.280	16	16.800	30	31.300	48	49.800
8	8.350	17	17.800	32	33.400	50	51.900
9	9.410	18	18.900	34	35.400		

Pour  $n > 50$  utiliser la formule suivante :  $\chi^2 = \frac{1}{2} (0.253 + \sqrt{2n-1})^2$



**AGENCE FRANÇAISE DE L'ESPACE**

**REFERENTIEL NORMATIF REALISE PAR :**

**Centre Spatial de Toulouse**  
**Délégation à l'Assurance de la Qualité**  
**18 Avenue Edouard Belin**  
**31401 TOULOUSE CEDEX 9**

**Tél : 61 27 31 31 - Fax : 61 27 31 79**

---

**CENTRE NATIONAL D'ÉTUDES SPATIALES**

---

Siège social : 2 pl. Maurice Quentin 75039 Paris cedex 01 / Tel. (33) 01 44 76 75 00 / Fax : 01 44 46 76 76  
RCS Paris B 775 665 912 / Siret : 775 665 912 00082 / Code APE 731Z