HAL
open science

Etude d'un calculateur tolérant des pannes, ses fiabilité, sécurité, performance et coût

Bernard Courtois

▶ **To cite this version:**

Bernard Courtois. Etude d'un calculateur tolérant des pannes, ses fiabilité, sécurité, performance et coût. Autre [cs.OH]. Institut National Polytechnique de Grenoble - INPG, 1976. Français. NNT : . tel-00010677

HAL Id: tel-00010677

https://theses.hal.science/tel-00010677v1

Submitted on 18 Oct 2005

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

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

THESE

présentée à

Institut National Polytechnique de Grenoble

pour obtenir le grade de
DOCTEUR-INGENIEUR
Spécialité «GENIE INFORMATIQUE»

par

Bernard COURTOIS

ETUDE D'UN CALCULATEUR TOLERANT DES PANNES

SES FIABILITE, SECURITE, PERFORMANCE ET COÛT

Thèse soutenue le 10 décembre 1976 devant la Commission d'Examen

Président	: M. L. BOLLIET
Examinateurs	M. A. COSTES M. C. DURANTE Mme G. SAUCIER
Invités	M. G. LA ROSA M. F. MAISON

Μή, ὦ λαμπρὰ ψυχά, βίον ἀθάνατον σπεῦδε,
τὰν δ'ἔμπρακτον ἄντλει μαχανάν.

PINDARE

Je tiens à remercier,

Monsieur le Professeur L. BOLLIET, Directeur du département informatique de l'Institut Universitaire de Technologie de Grenoble, qui a bien voulu me faire l'honneur de présider le jury;

Monsieur A. COSTES, Maître de Conférences à l'Institut National Polytechnique de Toulouse, Rapporteur, pour l'attention apportée à la lecture du manuscrit et les critiques constructives qui ont permis de l'améliorer;

Monsieur C. DURANTE, Professeur au Laboratoire d'Automatique de Montpellier;

Monsieur G. LA ROSA, Chef du Groupe Informatique et Automatique à la Direction des Recherches et Moyens d'Essais, organisme ayant soutenu financièrement la présente étude;

Monsieur F. MAISON, Directeur Technique à la Compagnie Internationale pour l'Informatique - Honeywell-Bull;

Madame G. SAUCIER, Maître de Conférences à l'Institut National Polytechnique de Grenoble;

qui ont bien voulu accepter de faire partie du jury.

Je voudrais remercier également,

Mes amis, J.M. AYACHE, P. LE DANOIS, M. MOALLA, J. SIFAKIS, M. ZACHARIADES, pour les nombreuses discussions que nous avons eues, souvent prolongées fort tard le soir;

Mesdames A. BOUVET et E. HERMANN, du service de la bibliothèque, bien que l'éloge de ce service ne soit plus à faire;

Monsieur D. IGELSIAS, ainsi que tous le personnel du service de reprographie, pour le soin apporté au tirage de cet ouvrage.

SOMMAIRE

INTRODUCTION

PREMIÈRE PARTIE : SECURITE DES MICROMACHINES

RESUME

I - **INTRODUCTION ET DEFINITIONS** 13
- I - 1. DEFINITIONS 13
- I - 2. JUSTIFICATION 15
- I - 3. COHERENCE 15bis
- I - 4. ILLUSTRATION 16

II - **ETUDE DE QUELQUES SYSTEMES** 18
- II - 1. SYSTEME DUPLEX 18
- II - 2. PREMIER SYSTEME DUPLEX REPLIQUE 20
- II - 3. SYSTEME BDR 24
- II - 4. SYSTEME TMR 26
- II - 5. SYSTEME TMR A DETECTEURS DE PANNE 27

III - **COMPARAISON DES SYSTEMES PROPOSES** 29
- III - 1. INTRODUCTION 29
- III - 2. SECURITE 30
- III - 3. FIABILITE DE MISSION 32
- III - 4. DISPONIBILITE ET FIABILITE DE SIGNAL 33
- III - 5. CONCLUSION PARTIELLE 34

IV - **SYSTEME BI-DUPLEX ET SYSTEMES HYBRIDES - MODELISATION** 35
- IV - 1. SYSTEME A REDONDANCE BI-DUPLEX 35
- IV - 2. SYSTEMES HYBRIDES 36

V - **COMPARAISON DES SYSTEMES BDR ET HYBRIDES** 40
- V - 1. INTRODUCTION 40
- V - 2. ANALYSE DE LA SECURITE ET DE LA FIABILITE DE MISSION POUR DE PETITES UNITES FONCTIONNELLES 40
- V - 3. ANALYSE DE LA SECURITE ET DE LA FIABILITE DE MISSION POUR DES UNITES FONCTIONNELLES PLUS COMPLEXES ET UN TEMPS DE MISSION PLUS LONG 42

VI - CONCLUSION : CHOIX D'UN SYSTEME

REFERENCES

ANNEXE 1 : FIABILITE DE SIGNAL DES SYSTEMES BDR ET TMR
A1 - 1. PREMIER SYSTEME DUPLEX REPLIQUE
A1 - 2. SYSTEME BDR
A1 - 3. SYSTEME TMR

ANNEXE 2 : SECURITE ET FIABILITE DE MISSION D'UN SYSTEME HYBRIDE AVEC SIGNAL DE STOP ET 1 MODULE DE SECOURS
A2 - 1. SECURITE
A2 - 2. FIABILITE DE MISSION

DEUXIÈME PARTIE : FIABILITE, COUT ET PUISSANCE DES MICROMACHINES

RESUME

I - POSITION DU PROBLEME 6

II - EVALUATION DE LA PUISSANCE DES MICROMACHINES 6
II - 1. "BENCHMARK", "KERNEL", "INSTRUCTION-MIX" ? 6
II - 2. CHOIX D'UN "INSTRUCTION MIX" 6

III - MODELISATION DES UNITES FONCTIONNELLES 7
III - 1. MODELISATION DE L'UNITE FONCTIÒNNELLE MEMOIRE DE REGISTRES 7
III - 1.1. Implémentation de redondances 7
III - 1.2. Stratégies d'implémentation de redondances 8
III - 1.3. Illustration sur la mémoire de registres 8
III - 2. MODELISATION DE L'UNITE FONCTIONNELLE UAL 8
III - 2.1. Modélisation des micromachines 8
III - 2.2. Relations coût-fiabilité 8
III - 3. MODELISATION DE LA FONCTION REGISTRE D'ETAT 8
III - 4. MODELISATION DE LA FONCTION REGISTRE INSTRUCTION 9
III - 5. ENSEIGNEMENTS ET FINALITE 9

IV - RELATIONS FIABILITE-COUT-PERFORMANCE 92

IV - 1. RELATIONS COUT-PERFORMANCE 92

IV - 1.1. Influence du mix d'instruction 97

IV - 2. RELATIONS COUT-FIABILITE 100

IV - 2.1. Influence du temps de mission 102

IV - 3. RELATIONS FIABILITE-PERFORMANCE 104

IV - 3.1. Influence du temps de mission 105

IV - 3.2. Influence du mix d'instruction 106

IV - 4. SURFACE FIABILITE COUT-PUISSANCE 107

V - CONCLUSION 109

REFERENCES 110

ANNEXE 3 : PROGRAMME POUR L'ETUDE DES RELATIONS FIABILITE-COUT-PERFORMANCE

A3 - 1. DONNEES FOURNIES PAR L'UTILISATEUR 114

A3 - 2. ENVIRONNEMENT "ETUDE" 115

A3 - 3. ENVIRONNEMENT "INITIAL" 117

A3 - 4. EXEMPLE 119

CONCLUSION GÉNÉRALE 122

REFERENCES 124

ANNEXE 4 : ETUDE DU PARTITIONNEMENT DE SYSTEMES LOGIQUES REDONDANTS

PARTIE I : résultats théoriques

A - Système (1,1,1) 127

B - Système (1,1,2) 128

C - Système (1,1,S) 129

D - Système (3,2,0) 129

E - MTF et R(MTF) du système (3,2,0) 130

PARTIE II : résultats pratiques

A - Existence d'un optimum pour le système (1,1,1) 133

B - Valeurs optimales pour le système (1,1,1) 138

C - Valeurs optimales pour le système (1,1,2), 1ère hypothèse 140

D - Valeurs optimales pour le système (1,1,2) 2e hypothèse 142

E - Choix d'un degré de redondance et de partitionnement pour des systèmes à remplacement 14
F - Valeurs optimales pour le système (3,2,0) 14

CONCLUSION 14

REFERENCES 14

ANNEXE 5 : PROGRAMME D'EVALUATION DE FIABILITE
A5 - 1. SCHEMAS DE REDONDANCES 15
A5 - 2. PARAMETRES 15
A5 - 3. COMMANDES 15
A5 - 4. EXEMPLE 15

INTRODUCTION

Bien qu'étudiée depuis maintenant fort longtemps, la sûreté de fonctionnement est un domaine dont l'importance ne fait que croître, sans doute en raison de la multiplicité des applications de l'informatique.

La présente étude s'insère dans ce domaine de la sûreté de fonctionnement et se veut être une aide à la conception d'un calculateur tolérant des pannes. Plus précisément, nous nous intéresserons à la prise en compte de 4 paramètres : la sécurité, la fiabilité, la performance et le coût de ce calculateur. On suppose que le-dit calculateur est muni d'un programme de test utilisant la méthode dite "boule de neige" c'est-à-dire augmentant progressivement la masse des circuits testés. Il est bien évident que les circuits de départ ne peuvent pas être testés de cette manière : ces circuits constituent ce que l'on appelle généralement le "hardcore" du calculateur.

Ceci nous a amené à classer les circuits en deux catégories : ceux appartenant au "hardcore" et les autres. Pour les circuits du "hardcore", on ne peut utiliser qu'une redondance à masquage de panne, alors que pour les autres on pourra utiliser une redondance à remplacement, puisqu'on saura les tester. Fonctionnellement, le calculateur ainsi défini est représenté par la figure 1 :

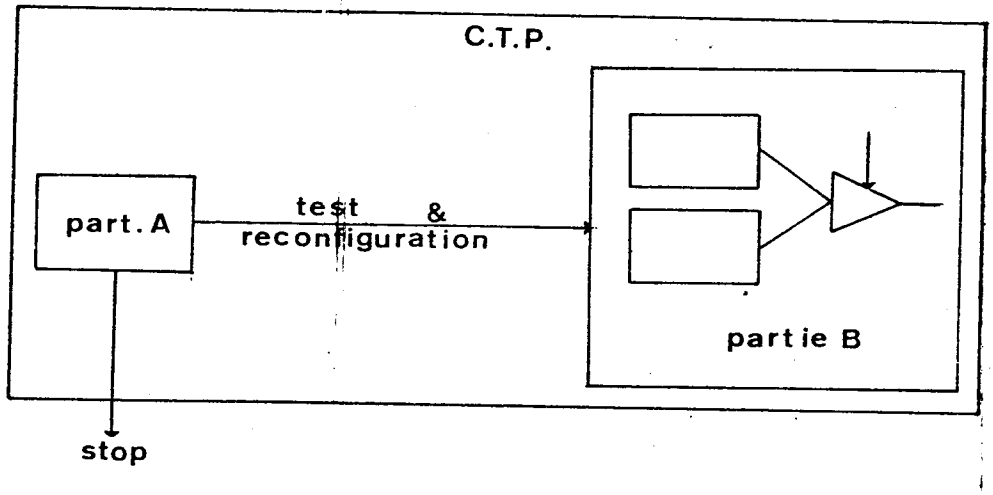


Figure 1. Calculateur tolerant les pannes

L'architecture donnée aux circuits de la partie A va conférer sa sécurité au calculateur, et interférer sur sa fiabilité. Ce sera l'objet de la première partie que d'examiner sous les angles de la sécurité et de la fiabilité des architectures tant classiques que nouvelles. Cette étude restera à un niveau général, par opposition à celle de la seconde partie, qui sera appliquée à une organisation de calculateur existant.

Cette seconde partie concernera l'étude des circuits conférant au calculateur sa performance et apportant une contribution majeure à sa fiabilité et son coût de la manière suivante : étant donnée la macromachine définie par un répertoire d'instructions constant, nous considèrerons plusieurs micromachines susceptibles de simuler la macromachine donnée, tout en conservant un même type d'organisation. Les circuits de ces micromachines étant testables par le calculateur lui-même, on supposera que l'on puisse utiliser des redondances à remplacement. On obtiendra donc des micromachines de caractéristiques de fiabilité, coût et performance différentes. L'examen des micromachines qu'il serait intéressant de construire permettra de mesurer, par exemple, de combien il faut diminuer la puissance de la machine si l'on veut accroître sa fiabilité, ceci sans augmenter son coût. Nous mesurerons également l'influence du paramètre fiabilité sur les études de coût-performance des calculateurs, qui jusqu'à présent ne prennent pas en compte ce paramètre de fiabilité.

PREMIÈRE PARTIE

SECURITE DES MICROMACHINES

RESUME

I - INTRODUCTION ET DEFINITIONS

II - ETUDE DE QUELQUES SYSTEMES

III - COMPARAISON DES SYSTEMES PROPOSES

IV - SYSTEME BI-DUPLEX ET SYSTEMES HYBRIDES - MODELISATION

V - COMPARAISON DES SYSTEMES BDR ET HYBRIDES

VI - CONCLUSION : CHOIX D'UN SYSTEME

REFERENCES

ANNEXES

RESUME

Pendant de nombreuses années les schémas de redondance ont été étudiés afin d'augmenter la fiabilité d'un système. Ainsi les principaux problèmes étaient de maximiser la fiabilité à un certain temps ou bien le temps de mission maximum pour une fiabilité donnée : mentionnons uniquement la modélisation des systèmes nybrides |1| ou bien celle des systèmes à remplacement |2|. Notre but ici sera de différencier les notions de sécurité et fiabilité. En effet, un système très "sûr" peut avoir une faible fiabilité au sens durée de vie : tel est le cas par exemple d'un système dupliqué avec comparateur arrêtant le système total. On définira donc 4 paramètres caractérisant des systèmes ayant deux sorties, l'une information, l'autre étant un signal d'arrêt (paragraphe I). Ces définitions sont cohérentes avec la définition classique de la fiabilité. Les paragraphes II et III concerneront la modélisation et la comparaison de 5 systèmes : duplex, TMR et un nouveau système appelé système à redondance bi-duplex. Ce nouveau système, un peu amélioré, sera comparé dans les paragraphes IV et V à des systèmes hybrides. Enfin, nous concluerons dans le paragraphe VI qu'il n'existe pas de système "optimal".

Dans toute cette première partie, aucune hypothèse ne sera faite sur la loi de dégradation des unités fonctionnelles et des circuits additionnels. Néanmoins, cette loi doit être la même pour les 2 types de circuits.

I - INTRODUCTION ET DEFINITIONS

L'objet de cette première partie est donc d'étudier l'architecture à donner à certains circuits du calculateur : le "hardcore", au sens où nous l'avons défini en introduction.

Le problème soulevé quant aux paramètres intuitifs de "sécurité" et de "fiabilité" au sens durée de vie est evidemment plus général que le cas spécifique du "hardcore" d'un calculateur, et s'applique à quantité d'autres systèmes.

L'étude que nous présentons dans cette partie a donc une portée très générale. Elle est nécessaire pour le choix de tout système devant posséder une certaine sécurité, comme par exemple pour le choix d'un système de contrôle de processus, pour lequel une panne non détectée peut être catastrophique.

I - 1. DEFINITIONS

Nous allons définir quatre termes : sécurité, fiabilité de mission, disponibilité et fiabilité de signal.

Le système général que nous considèrerons est supposé avoir deux sorties, l'une d'information(s), l'autre étant un signal de panne, envoyé au système receveur ou bien déclenchant l'arrêt du système. Un tel système est représenté par la figure 2.

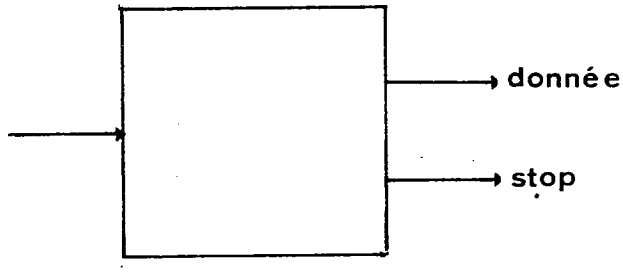


Figure 2.

Sécurité du système

On appellera sécurité la probabilité de ne pas envoyer d'information fausse non détectée, c'est-à-dire :

$1 - S = P$ (information fausse $\cap$ le signal stop n'est pas apparu).

Fiabilité de la mission

La fiabilité de la mission sera la probabilité d'exécuter correctement la mission, c'est-à-dire la probabilité de disposer du système et que l'information soit juste.

Ainsi :

$RM = P$ (le signal stop n'est pas apparu $\cap$ l'information délivrée est juste).

Disponibilité du système

On appellera disponibilité la probabilité de disposer effectivement du système, c'est-à-dire la probabilité que le signal stop ne soit pas apparu.

$A = P$ (le signal stop n'est pas apparu).

Fiabilité du signal

On appellera fiabilité de l'information du système la probabilité que l'information soit juste, sachant qu'il se peut que l'on dispose du système.

Soit :

$RS = P$ (information juste $|$il se peut que l'on dispose du système).

La fiabilité mesure ainsi la confiance que l'on accorde à l'information si l'on en dispose.

Actuellement, certains de ces termes sont propres aux différents auteurs et leur signification peut donc varier de l'un à l'autre. Ceci ne pose pas de problème pour la fiabilité de signal : notre définition s'accorde avec celle de |13|, ni pour la sécurité dont la définition s'apparente à celle de |14|. Pour la disponibilité par contre, il est nécessaire de bien prendre conscience du fait que, disposer du système, au sens où nous l'entendons ici, n'implique pas que l'information soit juste; il en serait ainsi si l'on pouvait construire des systèmes à sécurité parfaite. Ceci constitue la différence fondamentale entre la définition proposée ici pour un système non réparable et celle admise communément pour les systèmes réparables, systèmes pour lesquels il est sous-entendu que le fonctionnement est correct, si l'on en dispose.

I - 2. JUSTIFICATION DE CES DEFINITIONS

Les quatre mesures présentées sont suffisantes pour déterminer un système.

Considérons, en effet, un schéma des états possibles :

le systeme est-il disponible ?	donnée correcte	donnée incorrecte
oui	1	2
?	3	4
non	5	6

Figure 3.

Il y a six états possibles, liés par $\sum_{1}^{6} P(i) = 1$. Donc cinq fonctions sont nécessaires.

Or : S = 1 + 3 + 5 + 6

RM = 1

A = 1 + 2

RS = 1 + 3/1 + 2 + 3 + 4

1 - S donne la probabilité de 2 + 4. RM et A donnent 1 et 2 et par suite 4 est connu. Enfin RS détermine 3. On ne connaît donc que la probabilité de 5 + 6, sans distinction entre ces 2 états. En fait, cette distinction n'est pas nécessaire puisque ces 2 états correspondent respectivement à une information juste et fausse, mais dans un cas d'indisponibilité du système.

I - 3. COHERENCE DE CES DEFINITIONS

Les définitions proposées ci-dessus sont applicables à des systèmes ne possédant pas de signal d'arrêt, redondants ou non.

Considérons, en effet, un système simplex (Fig.4) :

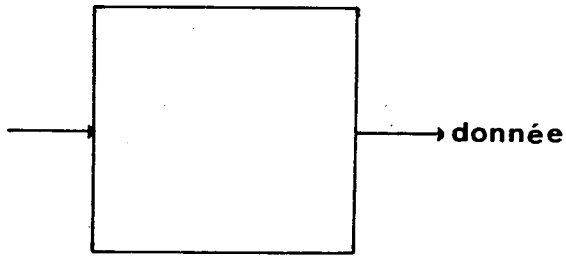


Figure 4.

Sa disponibilité est égale à 1, et sa sécurité, sa fiabilité de signal ainsi que sa fiabilité de la mission, au sens où nous venons de les définir, sont égales entre elles et égales à la fiabilité du système, au sens classique du terme.

En effet, il est aisé de voir que :

$1 - S = 1 - P$ (information fausse)

et

$RM = RS = P$ (information juste), puisque $A = 1$.

Notons qu'il en est de même pour un système simplex ou un système redondant (TMR par exemple) ne possédant pas de signal stop.

On peut donc écrire :

Pour un système ne possédant pas de signal stop :

Disponibilité = 1

Fiabilité de mission = fiabilité au sens classique

Sécurité = fiabilité au sens classique

Fiabilité du signal = fiabilité au sens classique

I - 4. ILLUSTRATION DE CES DEFINITIONS

Considérons le système représenté par la figure 5 et que, par extension des définitions contenues dans |4|, nous appellerons système auto-testable.

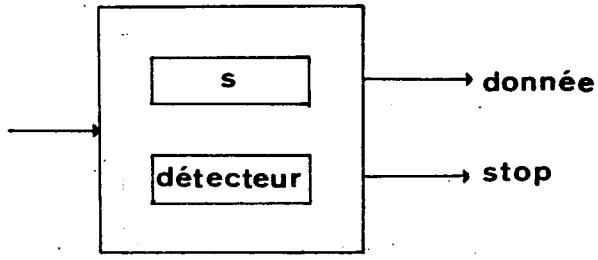


Figure 5. Système auto-testable

Le détecteur vérifie le fonctionnement du système S, éventuellement le sien propre, et émet un signal indiquant que le système global fonctionne correctement ou non. Ce système peut prendre au cours du temps 4 états :

$S.C$ le système S et le détecteur fonctionnent correctement,
$\overline{S}.C$ le système S est en panne et le détecteur fonctionne correctement,
$S.\overline{C}$ le système S fonctionne correctement et le détecteur est en panne,
$\overline{S}.\overline{C}$ le système S et le détecteur sont en panne.

Sécurité du système

Le système est sûr si :

- il est arrêté
- il n'est pas arrêté, mais l'information est juste.

Soit :

$S \geqslant P(SC) + P(\overline{S}C) + P(S\overline{C})$

Disponibilité du système

Lorsque le détecteur est en panne, on ne sait pas si le signal stop fonctionnera ou pas. On établit donc une borne inférieure de la disponibilité.

$A \geqslant P(SC)$

Fiabilité de la mission

Dans l'état considéré ci-dessus, l'information est correcte. D'où :

$RM \geqslant P(SC)$

Fiabilité du signal

Les états où il est possible que l'on dispose du système sont : SC, $S\overline{C}$ et $\overline{SC}$. Parmi ces derniers, ceux où l'information est juste sont : SC et $S\overline{C}$.

D'où :

$$RS \geqslant \frac{P(SC) + P(S\overline{C})}{P(SC) + P(S\overline{C}) + P(\overline{SC})}$$

Naturellement, cette dernière mesure est relative, puisqu'étant une probabilité conditionnelle. Mais elle peut être utile pour comparer 2 systèmes. Considérons, en effet, 2 systèmes tels que celui défini ci-dessus, mais pour lesquels les probabilités de bon fonctionnement du système S et du détecteur sont 0.1 et 0.9 pour le premier, et 0.9 et 0.1 pour le second (Fig.6).

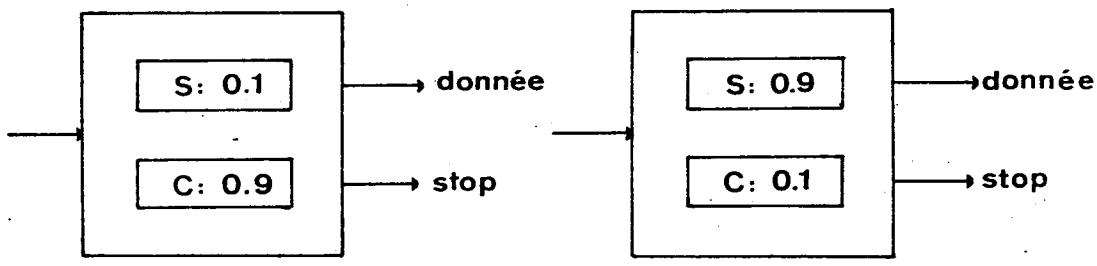


Figure 6.

Ces 2 système ont la même borne inférieure de sécurité :

$S \geqslant 0.91 \qquad S \geqslant 0.91$

Ils ont la même borne inférieure de disponibilité :

$A \geqslant 0.09 \qquad A \geqslant 0.09$

La borne inférieure de la fiabilité de la mission est la même et égale à celle de la disponibilité :

$RM \geqslant 0.09 \geqslant \quad RM \geqslant 0.09$

Mais ils n'ont pas la même borne inférieure de fiabilité de signal :

$RS \geqslant 0.52 \qquad RS \geqslant 0.909$

On retrouve donc ainsi le fait normal que l'on peut accorder une confiance beaucoup plus grande au second système.

II - ETUDE DE QUELQUES SYSTEMES

Nous allons étudier 5 systèmes présentant des caractéristiques intéressantes de sécurité, deux de ces systèmes étant également intéressants au point de vue fiabilité de mission.

II - 1. SYSTEME DUPLEX

Le système sûr (au sens de la sécurité) qui vient immédiatement à l'esprit est : (Fig.7).

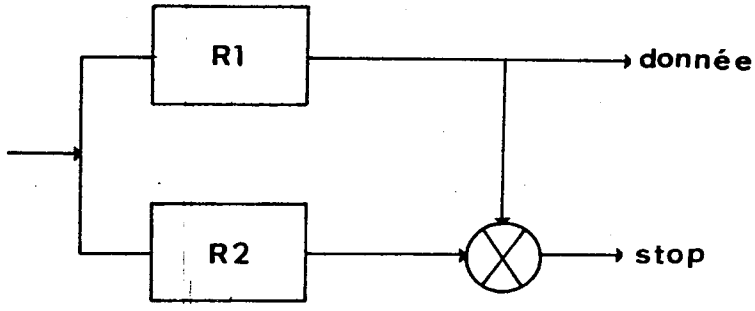


Figure 7. Système I Système Duplex

où R1 et R2 représentent les probabilités de bon fonctionnement de 2 unités identiques et où ⊗ représente un comparateur (disjonction). On suppose que 2 pannes ayant mêmes conséquences n'interviennent pas simultanément dans les 2 unités. Il est aisé d'établir les sécurité, disponibilité et fiabilités d'un tel système :
($\overline{R1}$ désignant par exemple l'état où R1 ne fonctionne pas correctement).

a) Sécurité

$$1 - S \leqslant P(\overline{R1}.R2.\overline{COMP}) + P(\overline{R1}.\overline{R2}.\overline{COMP})$$

Il y a, en effet, 2 états où il est possible que le système ne soit pas arrêté et qu'il transmette une information fausse.

b) Fiabilité de la mission et disponibilité

$$RM = A \geqslant P(R1.R2.COMP)$$

En effet, il n'y a qu'un état pour lequel on est certain de disposer du système. Dans cet état, l'information est juste.

d) Fiabilité du signal

$RS \geq X/Y$ où

$X = P(R1.R2.COMP) + P(R1.R2.\overline{COMP}) + P(R1.\overline{R2}.\overline{COMP})$

$Y = P(R1.R2.COMP) + P(R1.R2.\overline{COMP}) + P(R1.\overline{R2}.\overline{COMP}) + P(\overline{R1}.R2.\overline{COMP})$
$+ P(\overline{R1}.\overline{R2}.\overline{COMP})$

En effet, il y a 5 états où il est possible de disposer du système, et uniquement 3 parmi ces 5 pour lesquels l'information est juste.

En posant R1 = R2 = R et RC la probabilité de bon fonctionnement du comparateur, on obtient alors :

$$1 - S \leq R(1 - R)\ (1 - RC) + (1 - R)^2(1 - RC)$$
$$\leq (1 - RC)\ (1 - R)\ |R + (1 - R)|$$
$$\leq (1 - RC)\ (1 - R)$$

Soit :

$$S \geq 1 - |1 - R - RC + R.RC|$$
$$\geq R(1 - RC) + RC$$
$$RM \geq R^2.RC$$
$$A \geq R^2.RC$$

$RS \geq X/Y$ où

$$X = R^2 + R(1 - R)\ (1 - RC)$$
$$Y = R^2 + (1 - RC)\ |2R(1 - R) + (1 - R)^2|$$
$$= R^2 + (1 - RC)\ (1 - R^2)$$

Les expressions des quatre paramètres peuvent donc se résumer à :

$$S \geq RC + R(1 - RC)$$
$$RM \geq R^2.RC$$
$$A \geq R^2.RC$$
$$RS \geq |R^2 + R\ (1 - R)\ (1 - RC)|/|R^2 + (1 - RC)\ (1 - R^2)|$$

Illustrons ceci par un exemple numérique :

Si R = 0.8 et RC = 0.9, on trouve :

$S \geq 0.98$

$RM \geq 0.58$

$A \geq 0.58$

$RS \geq 0.97$

Ainsi, clairement, on ne disposera que peu souvent du système, mais on a peu de chances d'envoyer une information fausse non détectée.

II - 2. PREMIER SYSTEME DUPLEX REPLIQUE

Un système devant assurer une meilleure disponibilité est le suivant : (Fig.8).

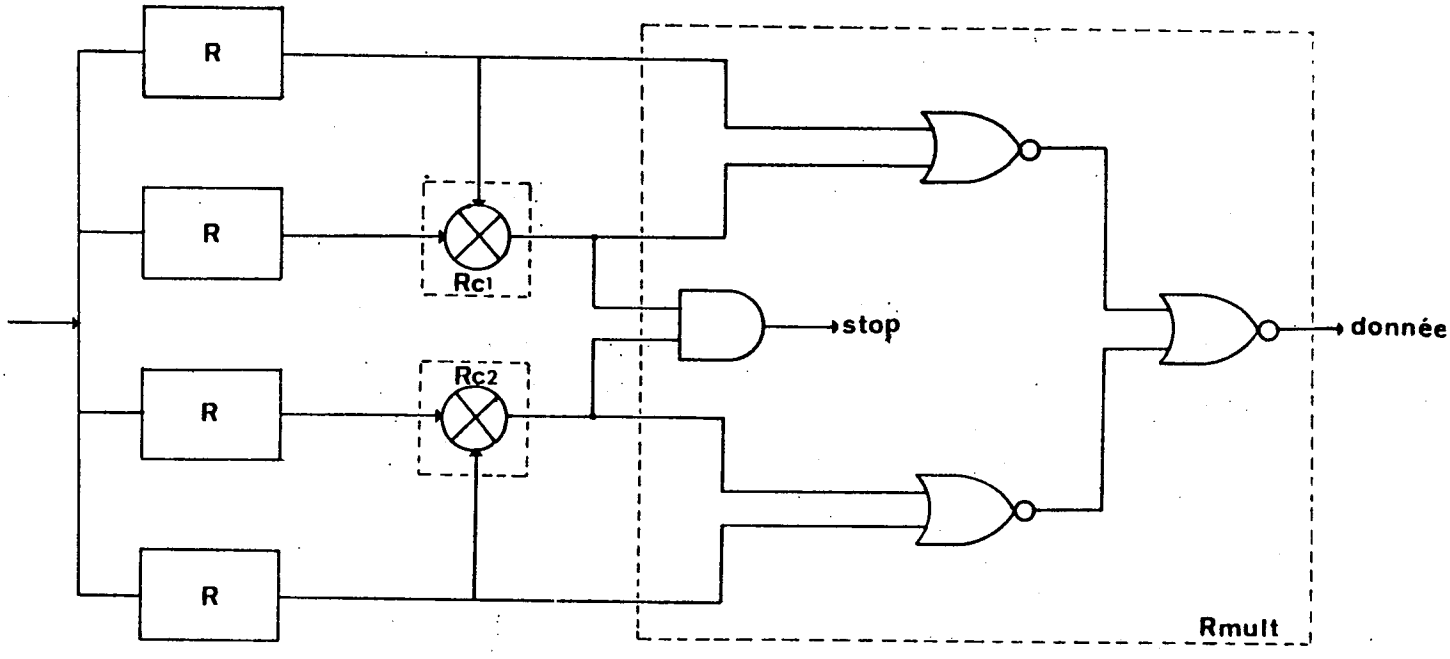


Figure 8. Système II : Premier système duplex répliqué

Lorsqu'un désaccord apparaît entre 2 unités d'un même groupe, l'information est bloquée. Mais il est bien clair que, si 2 unités d'un même groupe sont en panne, ces 2 pannes peuvent se traduire par une même sortie, fausse, et qu'ainsi le comparateur ne bloque pas le passage de cette information fausse. Néanmoins la simplicité des circuits additionnels fait que l'étude de ce système doit être menée.

Nous appellerons R la probabilité de bon fonctionnement de chacune des quatre unités fonctionnelles, R_{C1} et R_{C2} la probabilité de bon fonctionnement des deux comparateurs et R_{MULT} celle de bon fonctionnement du multiplexeur et de la porte ET de signal stop.

On peut alors déterminer : ($\overline{C1}$ désignant l'état où C1 ne fonctionne pas, $\overline{MULT}$ désignant de même celui où MULT ne fonctionne pas).

a) Sécurité

Etablissons les états non sûrs du système. Nous cherchons une borne inférieure de la sécurité, et par conséquent nous nous placerons toujours dans le "pire cas" pour chacun des états (ce "pire cas" est naturellement différent selon le paramètre étudié).

L'état $\overline{MULT}$ est un état non sûr, quel que soit l'état des autres composants, puisque dans ce cas, les sorties de données et d'arrêt peuvent indiquer des valeurs quelconques.

Considérons l'état MULT $\overline{C1}\ \overline{C2}$: si les 4 unités fonctionnelles sont en ordre de marche, il ne peut pas y avoir de sortie fausse non détectée (si $\overline{C1}\ \overline{C2}$ est collé à 11, la donnée de sortie peut être fausse, mais il y aurait alors production du signal d'arrêt, puisque MULT fonctionne correctement).

Si 3 unités fonctionnelles seulement sont en ordre de marche, on peut établir que :

- si R1 est en panne, les 3 autres étant bonnes, on a un état non sûr (si $\overline{C1}\ \overline{C2}$ passe par la valeur 01 par exemple),
- si R2 seule est en panne, on n'a pas d'état non sûr. En effet, la donnée de sortie ne peut être que juste (en provenanve de R1 et/ou R4), sinon il y aurait production du signal d'arrêt.

En examinant de la même manière tous les états possibles du système, on peut montrer que :

$$
\begin{aligned}
1 - S \leqslant\ & \overline{MULT} + \\
& + MULT\ \overline{C1}\ \overline{C2} \left| 2R^3(1-R) + 5R^2(1-R)^2 + 4R(1-R)^3 + (1-R)^4 \right| \\
& + MULT\ \overline{C1}\ C2 \left| R^3(1-R) + 4R^2(1-R)^2 + 4R(1-R)^3 + (1-R)^4 \right| \\
& + MULT\ C1\ \overline{C2} \left| R^3(1-R) + 4R^2(1-R)^2 + 4R(1-R)^3 + (1-R)^4 \right| \\
& + MULT\ C1\ C2 \left| 2R^2(1-R)^2 + 4R(1-R)^3 + (1-R)^4 \right|
\end{aligned}
$$

Soit encore :

$$
\begin{aligned}
1 - S \leqslant\ & \overline{MULT} \\
& + MULT\ \overline{C1}\ \overline{C2}\ \left|1-R\right| \left| 2R^3+5R^2(1-R) + 4R(1-R)^2 + (1-R)^3 \right| \\
& + MULT\ \overline{C1}\ C2\ \left|1-R\right| \left| R^3 + 4R^2(1-R) + 4R(1-R)^2 + (1-R)^3 \right| \\
& + MULT\ C1\ \overline{C2}\ \left|1-R\right| \left| R^3 + 4R^2(1-R) + 4R(1-R)^2 + (1-R)^3 \right| \\
& + MULT\ C1\ C2\ \left|1-R\right| \left| 2R^2(1-R) + 4R(1-R)^2 + (1-R)^3 \right|
\end{aligned}
$$

$$\leq \overline{MULT}$$
$$+ MULT\ \overline{C1}\ \overline{C2}\ (1-R)\,|1+R|$$
$$+ MULT\ \overline{C1}\ C2\ (1-R)\,|1+R-R^2|$$
$$+ MULT\ C1\ \overline{C2}\ (1-R)\,|1+R-R^2|$$
$$+ MULT\ C1\ C2\ (1-R)\,|1+R-3R^2+R^3|$$

D'où l'on peut tirer :

$$S \geq MULT\ |1 - \overline{C1}\ \overline{C2}(1-R^2) - C1\ \overline{C2}(1-2R^2+R^3) - \overline{C1}\ C2(1-2R^2+R^3) - C1\ C2(1-4R^2+4R^3-R^4)|$$

et enfin :

$$S \geq R_{MULT}|1-(1-R_{C1})\ (1-R_{C2})(1-R^2) - R_{C1}(1-R_{C2})(1-2R^2+R^3) - (1-R_{C1})R_{C2}(1-2R^2+R^3) - R_{C1}R_{C2}(1-4R^2+4R^3-R^4)|$$

b) *Disponibilité du système*

Il nous faut considérer tous les états où l'on est certain de disposer du système.

On dispose du système de manière certaine si MULT fonctionne correctement. En effet, si MULT ne fonctionne pas correctement, le système peut être arrêté, à tort ou à raison. Enfin, parmi les états où MULT fonctionne correctement, ceux pour lesquels on dispose du système sont définis par :

$$A \geq R_{MULT}.R_{C1}.R_{C2}|R^4+4R^3(1-R)+2R^2(1-R)^2|$$
$$+ R_{MULT}.(1-R_{C1}).R_{C2}|R^4+2R^3(1-R)+R^2(1-R)^2|$$
$$+ R_{MULT}.R_{C1}.(1-R_{C2})|R^4+2R^3(1-R)+R^2(1-R)^2|$$

Soit encore :

$$A \geq R_{MULT}.R_{C1}.R_{C2}(2R^2-R^4)$$
$$+ R_{MULT}(1-R_{C1})R_{C2}(R^2)$$
$$+ R_{MULT}.R_{C1}(1-R_{C2})(R^2)$$

c) *Fiabilité de la mission*

Parmi les états où l'on est certain de disposer du système, il en existe pour lesquels l'information est fausse.

En effet, si tous les circuits additionnels fonctionnent correctement, mais si 2 unités du même groupe sont en panne, le système ne sera pas arrêté, alors que l'information de sortie peut être fausse (ce cas n'est pas unique).

D'où :

$$RM = R_{MULT}.R_{C1}.R_{C2}|R^4+4R^3(1-R)|$$
$$+ R_{MULT}.(1-R_{C1})R_{C2}|R^4+R^3(1-R)|$$
$$+ R_{MULT}.R_{C1}(1.R_{C2})|R^4+R^3(1-R)|$$

$$RM \geqslant R_{MULT}.R_{C1}.R_{C2}.R^3(4-3R)$$
$$+ R_{MULT(1-R_{C1})R_{C2}}.R^3$$
$$+ R_{MULT}.R_{C1}(1-R_{C2}).R^3$$

d) *Fiabilité du signal*

On peut montrer (Annexe 1) que :

$RS \geqslant X/Y$

avec

$$X = R_{MULT}.R_{C1}.R_{C2}|4R^3-3R^4|$$
$$+ R_{MULT}(1-R_{C1})R_{C2}|2R^2-R^3|$$
$$+ R_{MULT}.R_{C1}(1-R_{C2})|2R^2-R^3|$$
$$+ R_{MULT}(1-R_{C1})(1-R_{C2})|R^2|$$

$$Y = 1-R_{MULT}$$
$$+ R_{MULT}.R_{C1}.R_{C2}.|R^4+4R^3(1-R)+2R^2(1-R)^2+4R(1-R)^3+(1-R)^4|$$
$$+ R_{MULT}(1-R_{C1})R_{C2}|1|$$
$$+ R_{MULT}\ R_{C1}(1-R_{C2})|1|$$
$$+ R_{MULT}(1-R_{C1})(1-R_{C2})|1|$$

II - 3. SYSTEME BDR

Un système palliant les inconvénients du précédent, mais par conséquent plus sophistiqué est le suivant (Fig.9) :

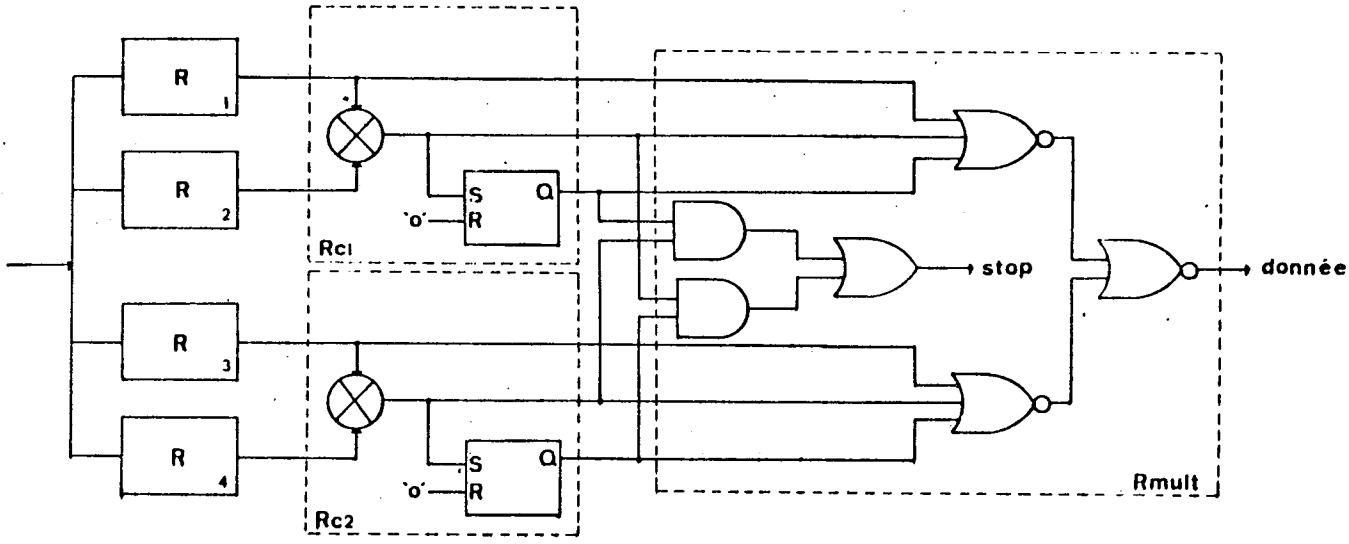


Figure 9 : Système III "Bi-Duplex Redundant System"

Dès que l'une des unités tombe en panne, l'information est bloquée, comme précédemment par le comparateur. Mais ce même comparateur, en agissant sur la bascule RS associée, fait passer la sortie de cette dernière à 1, et ainsi toutes les sorties suivantes seront également bloquées. Il est clair que ce système serait plus sûr que le précédent si les circuits additionnels étaient parfaits.

a) *Sécurité*

$$
\begin{aligned}
1 - S \geqslant\ & 1 - R_{MULT} \\
& + R_{MULT}.(1-R_{C1})(1-R_{C2})\left|2R^3(1-R)+5R^2(1-R)^2+4R(1-R)^3+(1-R)^4\right| \\
& + R_{MULT}(1-R_{C1})R_{C2}\left|R^3(1-R)+3R^2(1-R)^2+3R(1-R)^3+(1-R)^4\right| \\
& + R_{MULT}.R_{C1}.(1-R_{C2})\left|R^3(1-R)+3R^2(1-R)^2+3R(1-R)^3+(1-R)^4\right|
\end{aligned}
$$

Soit encore :

$$1 - S \leq 1 - R_{MULT} + R_{MULT}(1-R_{C1})(1-R_{C2})|1-R^2| + R_{MULT}(1-R_{C1})R_{C2}|1-R| + R_{MULT}\ R_{C1}(1-R_{C2})|1-R|$$

Une expression directe de S peut s'obtenir :

$$1 - S \leq \overline{MULT} + MULT(1-R)|\overline{C1}.\overline{C2}(1+R) + \overline{C1}.C2 + C1.\overline{C2}|$$

D'où :

$$S \geq MULT\ |1-(1-R)(\overline{C1}\ \overline{C2}(1+R) + \overline{C1}\ C2 + C1\ \overline{C2})|$$
$$\geq R_{MULT}\ |1-(1-R)|(1-R_{C1})(1-R_{C2})(1+R) + (1-R_{C1})R_{C2} + (1-R_{C2})R_{C1}||$$
$$\geq R_{MULT}\ |1-(1-R)|1-R_{C1}.R_{C2} + R-R.R_{C1}-R.R_{C2} + RR_{C1}.R_{C2}||$$
$$\geq R_{MULT}|R_{C1}.R_{C2} + R|R_{C1} + R_{C2} - 2R_{C1}.R_{C2} + R(1-R_{C1})(1-R_{C2})||$$

b) *Disponibilité*

La disponibilité, littéralement, est la même que pour le système précédent :

$$A \geq R_{MULT}.R_{C1}.R_{C2}|R^4+4R^3(1-R) + 2R^2(1-R)^2|$$
$$+ R_{MULT}.(1-R_{C1}).R_{C2}|R^4+2R^3(1-R) + R^2(1-R)^2|$$
$$+ R_{MULT}\ R_{C1}(1-R_{C2})|R^4+2R^3(1-R) + R^2(1-R)^2|$$
$$\geq R_{MULT}\ R_{C1}\ R_{C2}(2R^2-R^4)$$
$$+ R_{MULT}(1-R_{C1})R_{C2}(R^2)$$
$$+ R_{MULT}\ R_{C1}(1-R_{C2})R^2$$

c) *Fiabilité de la mission*

De même que pour les deux systèmes précédents, il existe des états où l'on est certain de disposer du système, alors que l'information de sortie peut être fausse.

D'où :

$$RM \geq R_{MULT}.R_{C1}.R_{C2}|R^4+4R^3(1-R) + 2R^2(1-R)^2|$$
$$+ R_{MULT}(1-R_{C1}).R_{C2}|R^4+R^3(1-R)|$$
$$+ R_{MULT}.R_{C1}(1-R_{C2})|R^4+R^3(1-R)|$$

$$\geq R_{MULT} \cdot R_{C1} \cdot R_{C2} |2R^2 - R^4|$$
$$+ R_{MULT}(1-R_{C1}) \cdot R_{C2} |R^3|$$
$$+ R_{MULT} \cdot R_{C1}(1-R_{C2}) |R^3|$$

d) *Fiabilité du signal*

Les calculs permettant d'évaluer la fiabilité de signal sont consignés en Annexe 1 et donnent :

$$RS \geq X/Y$$

avec

$$X = R_{MULT}\ R_{C1}\ R_{C2} |2R^2 - R^4|$$
$$+ R_{MULT}\ R_{C1}(1-R_{C2}) |R|$$
$$+ R_{MULT}(1-R_{C1}) R_{C2} |R|$$
$$+ R_{MULT}(1-R_{C1})(1-R_{C2}) |R^2|$$

$$Y = 1 - R_{MULT}$$
$$+ R_{MULT} |R_{C1}\ R_{C2}(2R^2 - R^4) + 1 - R_{C1}\ R_{C2}|$$

II - 4. SYSTEME TMR

On peut naturellement penser immédiatement à un système TMR (Fig.10) :

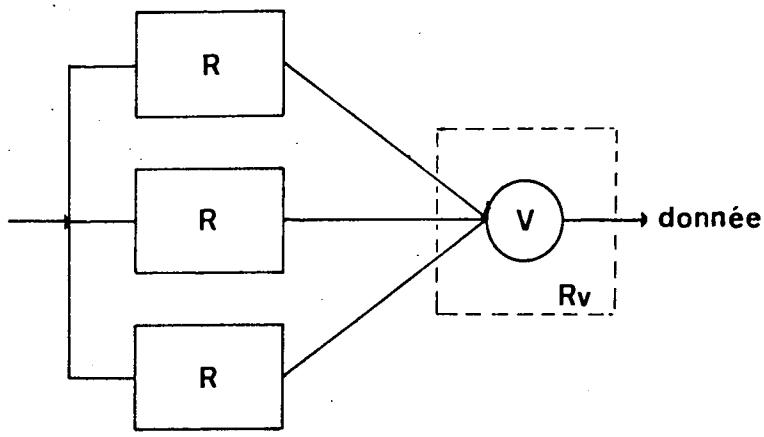


Figure 10 : Système TMR

Un tel système, ne possédant pas de signal stop, a, conformément à ce que nous avons dit précédemment, une disponibilité égale à 1, et une sécurité égale à ses fiabilités.

$$A = 1$$
$$S \geq RM = RS = RV|3R^2 - 2R^3|$$

II - 5. SYSTEME TMR A DETECTEURS DE PANNE

On peut, de même, penser au système TMR plus évolué avec signal d'arrêt. Si l'on s'astreint à ne pas mémoriser les pannes, ce signal doit agir dès qu'une panne survient dans l'une des unités.

En effet, on ne peut attendre une deuxième panne, car on ne saurait pas la détecter (la valeur de référence n'existerait pas). Pour ce faire, on arrive à un schéma de principe du type de celui de la figure 11.

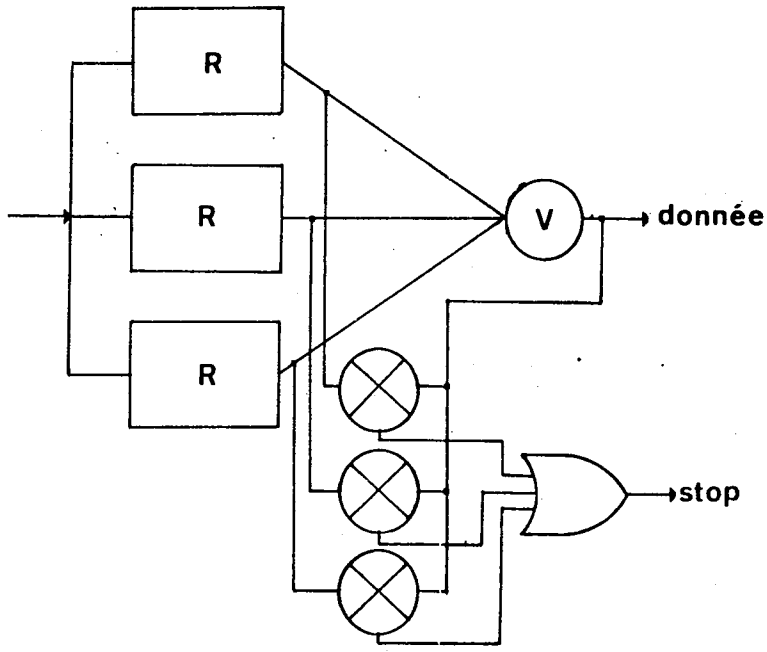


Figure 11. Système TMR à détecteurs de panne

a) Sécurité

$$
\begin{aligned}
1 - S \leq \overline{R}_V + R_V \Big| & R_{C1}R_{C2}(1-R_{C3})(2R(1-R)^2+(1-R)^3) \\
& + R_{C1}(1-R_{C2})R_{C3}(2R(1-R)^2+(1-R)^3) \\
& + (1-R_{C1})R_{C2}R_{C3}(2R(1-R)^2+(1-R)^3) \\
& + R_{C1}(1-R_{C2})(1-R_{C3})(3R(1-R)^2+(1-R)^3) \\
& + (1-R_{C1})(1-R_{C2})R_{C3}(3R(1-R)^2+(1-R)^3) \\
& + (1-R_{C1})R_{C2}(1-R_{C3})(3R(1-R)^2+(1-R)^3) \\
& + (1-R_{C1})(1-R_{C2})(1-R_{C3})(3R(1-R)^2+(1-R)^3) \Big|
\end{aligned}
$$

b) *Fiabilité de la mission*

$$RM \geqslant RV\ R_{C1}\ R_{C2}\ R_{C3}\ R^3$$

c) *Disponibilité*

$$A = RM$$

d) *Fiabilité du signal*

$RS \geqslant X/Y$, avec :

$$\begin{aligned}
X = {} & R_V\ R_{C1}\ R_{C2}\ R_{C3}(R^3) \\
& + R_V\ R_{C1}\ R_{C2}(1-R_{C3})(R^3+R^2(1-R)) \\
& + R_V\ R_{C1}(1-R_{C2})R_{C3}(R^3+R^2(1-R)) \\
& + R_V(1-R_{C1})R_{C2}\ R_{C3}(R^3+R^2(1-R)) \\
& + R_V\ R_{C1}(1-R_{C2})(1-R_{C3})(R^3+2R^2(1-R)) \\
& + R_V(1-R_{C1})\ R_{C2}(1-R_{C3})(R^3+2R^2(1-R)) \\
& + R_V(1-R_{C1})(1-R_{C2})R_{C3}(R^3+2R^2(1-R)) \\
& + R_V(1-R_{C1})(1-R_{C2})(1-R_{C3})(R^3+3R^2(1-R))
\end{aligned}$$

$$\begin{aligned}
Y = {} & (1-R_V) \\
& + R_V\ R_{C1}\ R_{C2}\ R_{C3}(R^3) \\
& + R_V\ R_{C1}\ R_{C2}(1-R_{C3})(R^3+R^2(1-R)+2R(1-R)^2+(1-R)^3) \\
& + R_V\ R_{C1}(1-R_{C2})R_{C3}(R^3+R^2(1-R)+2R(1-R)^2+(1-R)^3) \\
& + R_V(1-R_{C1})R_{C2}\ R_{C3}(R^3+R^2(1-R)+2R(1-R)^2+(1-R)^3) \\
& + R_V\ R_{C1}(1-R_{C2})(1-R_{C3})(R^3+2R^2(1-R)+3R(1-R)^2+(1-R)^3) \\
& + R_V(1-R_{C1})R_{C2}(1-R_{C3})(R^3+2R^2(1-R) + 3R(1-R)^2+(1-R)^3) \\
& + R_V(1-R_{C1})(1-R_{C2})R_{C3}(R^3+2R^2(1-R)+3R(1-R)^2+(1-R)^3) \\
& + R_V(1-R_{C1})(1-R_{C2})(1-R_{C3})
\end{aligned}$$

III - COMPARAISON DES SYSTEMES PROPOSES

III - 1. INTRODUCTION

Afin de comparer les différents systèmes proposés, nous définissons un rapport de complexité entre les unités fonctionnelles et les circuits de détection, commutation. Plus précisément, nous adopterons une unité : le comparateur. Ainsi, si R est la fiabilité d'un comparateur, et si une unité fonctionnelle est T fois plus complexe qu'un comparateur, la fiabilité d'une unité fonctionnelle sera R^T. Nous adopterons donc les conventions suivantes, résultant d'une évaluation de la complexité des circuits mis en jeu :
(on prendra donc garde à ne pas confondre R en partie gauche, représentant la fiabilité d'une unité fonctionnelle avant évaluation de sa complexité, avec R en partie droite, représentant l'unité de fiabilité).

Système I	R	$\rightarrow$	R^T
	R_C	$\rightarrow$	R
Système II	R	$\rightarrow$	R^T
	R_{C1}	$\rightarrow$	R
	R_{C2}	$\rightarrow$	R
	R_{MULT}	$\rightarrow$	R
Système III	R	$\rightarrow$	R^T
	R_{C1}	$\rightarrow$	R^2
	R_{C2}	$\rightarrow$	R^2
	R_{MULT}	$\rightarrow$	R^2
Système IV	R	$\rightarrow$	R^T
	R_V	$\rightarrow$	R
Système V	R	$\rightarrow$	R^T
	R_V	$\rightarrow$	R
	R_{C1}	$\rightarrow$	R
	R_{C2}	$\rightarrow$	R
	R_{C3}	$\rightarrow$	R

Nous n'étudierons pas ici les variations des quatre paramètres en fonction du temps, mais en fonction de la complexité des unités fonctionnelles, pour une valeur déterminée de R, c'est-à-dire pour une valeur du temps de mission.

Nous ne ferons ainsi aucune hypothèse sur la loi de fiabilité des éléments mis en jeu, si ce n'est que les unités fonctionnelles et les circuits additionnels suivent la même loi de dégradation. La valeur choisie pour R est : $1 - 10^{-4}$ (cette valeur correspondrait, par exemple, à un temps de 1000 heures pour un comparateur ayant un taux de panne $10^{-7}/H$).

III - 2. ETUDE DE LA SECURITE

Compte tenu des équivalences précédentes, on peut obtenir le tableau suivant :

Duplex	$S_I \geqslant R+R^T(1-R)$
Premier système duplex répliqué	$S_{II} \geqslant R\left\|1-(1-R)^2(1-R^{2T})-2R(1-R)(1-2R^{2T}+R^{3T})-R^2(1-4R^{2T}+6R^{3T}-3R^{4T})\right\|$
BDR	$S_{III} \geqslant R^2-R^2(1-R^2)^2(1-R^{2T})-2R^4(1-R^2)(1-R^T)$
TMR	$S_{IV} \geqslant R\ (3R^{2T}-2R^{3T})$
TMR à détecteurs de panne	$S_V \geqslant R\left\|1-3R^2(1-R)(1-R^T-R^{2T}+R^{3T})-3R(1-R)^2(1-3R^{2T}+2R^{3T}) -(1-R)^3(1-3R^{2T}+2R^{3T})\right\|$

Les courbes de sécurité (désécurité en fait) des systèmes en fonction de la complexité T des unités fonctionnelles et pour la valeur $R = 1 - 10^{-4}$ sont tracées sur la figure 12.

Ces courbes appellent quelques commentaires. On peut s'étonner de la quasi constance de la sécurité des systèmes III et V. Ceci s'explique par les expressions obtenues à partir des développements limités.

En posant $R \geqslant 1 - \varepsilon$, on peut obtenir :

Duplex	$S_I \geq 1 - T\varepsilon^2 + \varepsilon^2\Psi(\varepsilon)$
1er système duplex répliqué	$S_{II} \geq 1 - (2T+1)\varepsilon + (3T+5T^2)\varepsilon^2 + \varepsilon^2\Psi(\varepsilon)$
BDR	$S_{III} \geq 1 - 2\varepsilon - (4T-1)\varepsilon^2 + \varepsilon^2\Psi(\varepsilon)$
TMR	$S_{IV} \geq 1 - \varepsilon - 3T^2\varepsilon^2 + \varepsilon^2\Psi(\varepsilon)$
TMR à détecteurs de pannes	$S_V \geq 1 - \varepsilon - \varepsilon^2\Psi(\varepsilon)$

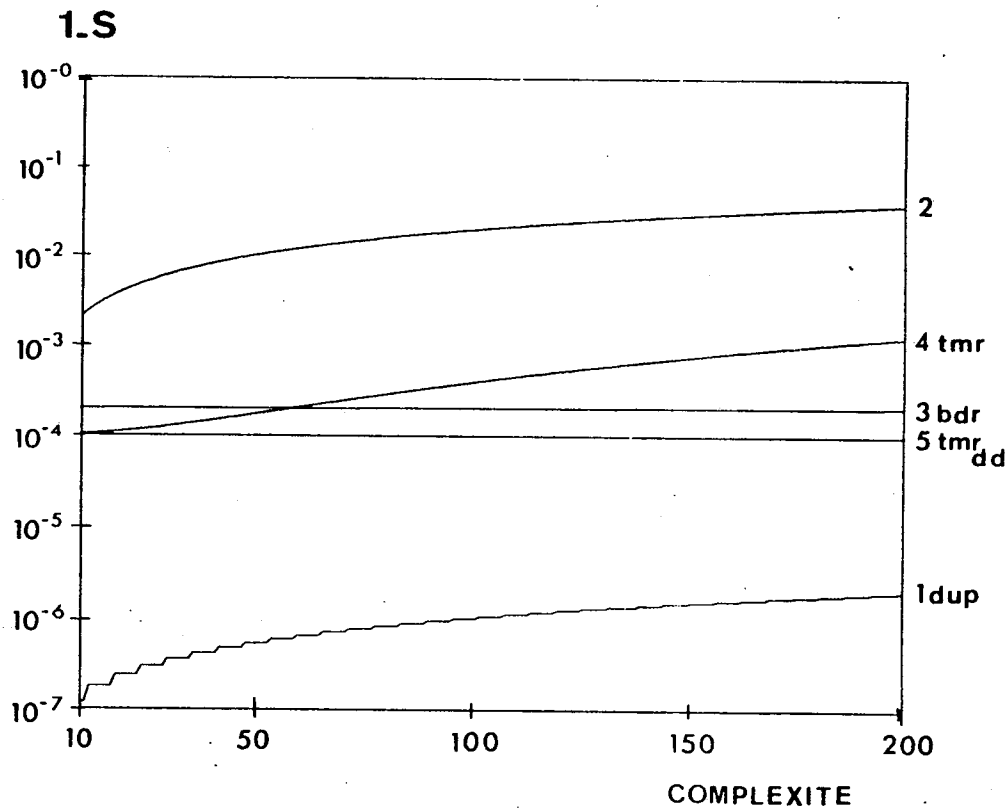


Figure 12. Sécurité

Ainsi : - La sécurité du système I est du deuxième ordre en ε (mais variant avec T), ce qui explique l'imprécision des résultats numériques.

- La sécurité du système II est du premier ordre en ε, et varie avec T.

- La sécurité des systèmes III, IV et V est du premier ordre en ε, mais le coefficient de ce terme ne varie pas avec T.

Remarquons que, malgré l'importance des circuits additionnels du système III sa sécurité est plus grande que celle du système II.

III - 3. ETUDE DE LA FIABILITE DE LA MISSION

Rappelons qu'elle mesure la probabilité de bonne exécution de la mission, c'est-à-dire la probabilité de disposer de l'information et que cette information soit juste. Les courbes sont tracée sur la figure 13.

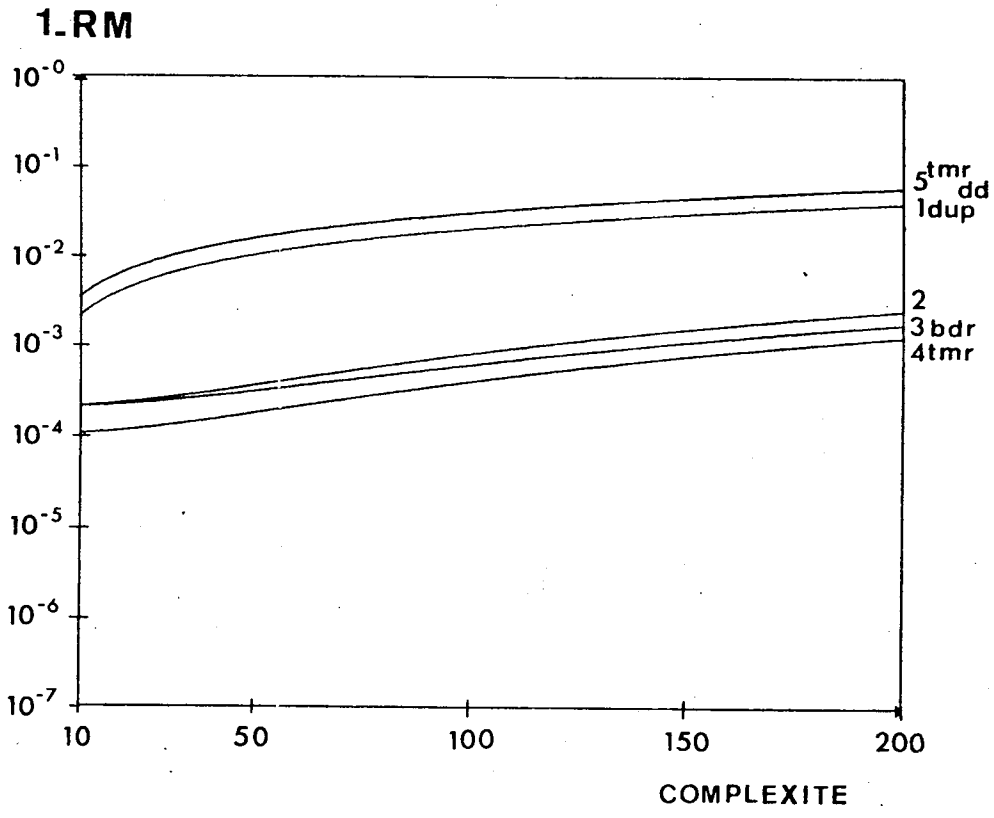


Figure 13. Fiabilité de la mission

On remarque alors que les deux systèmes qui possédaient la meilleure sécurité (systèmes 1 et 5) ont la moins bonne fiabilité de mission. Ces deux systèmes seront donc très rapidement "non disponibles".

Enfin, les systèmes 3 et 4 ont des valeurs de sécurité et de fiabilité de mission comparables. Mais, le système 3 a une sécurité meilleure que le système 4, alors que leurs fiabilités de mission sont à peu près égales.

III - 4. ETUDE DE LA DISPONIBILITE ET DE LA FIABILITE DU SIGNAL

Ces deux paramètres ne sont utiles que lors de la comparaison de deux systèmes, lorsqu'ils ont des valeurs égales de sécurité et de fiabilité de mission. Nous ne commenterons donc pas les courbes représentatives de ces deux paramètres (Fig. 14 et 15), mais nous dirons néanmoins que certaines courbes semblent identiques à celles de sécurité, mais qu'en fait elles en diffèrent par des termes de degré 2.

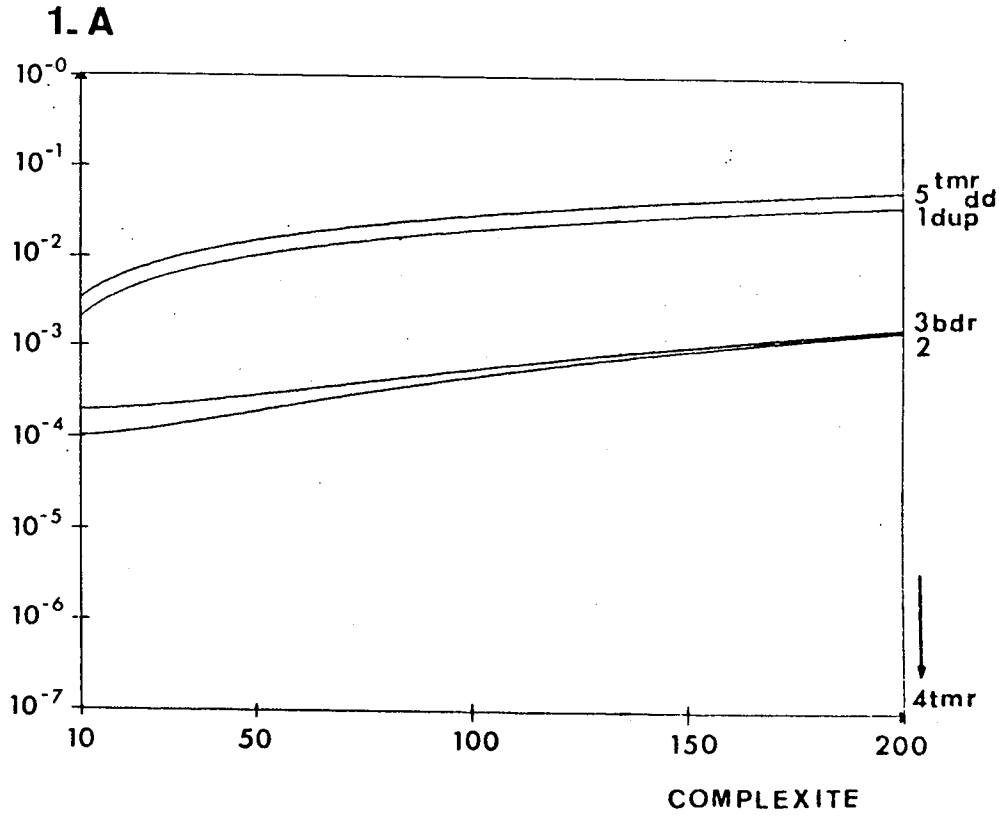


Figure 14. Disponibilité

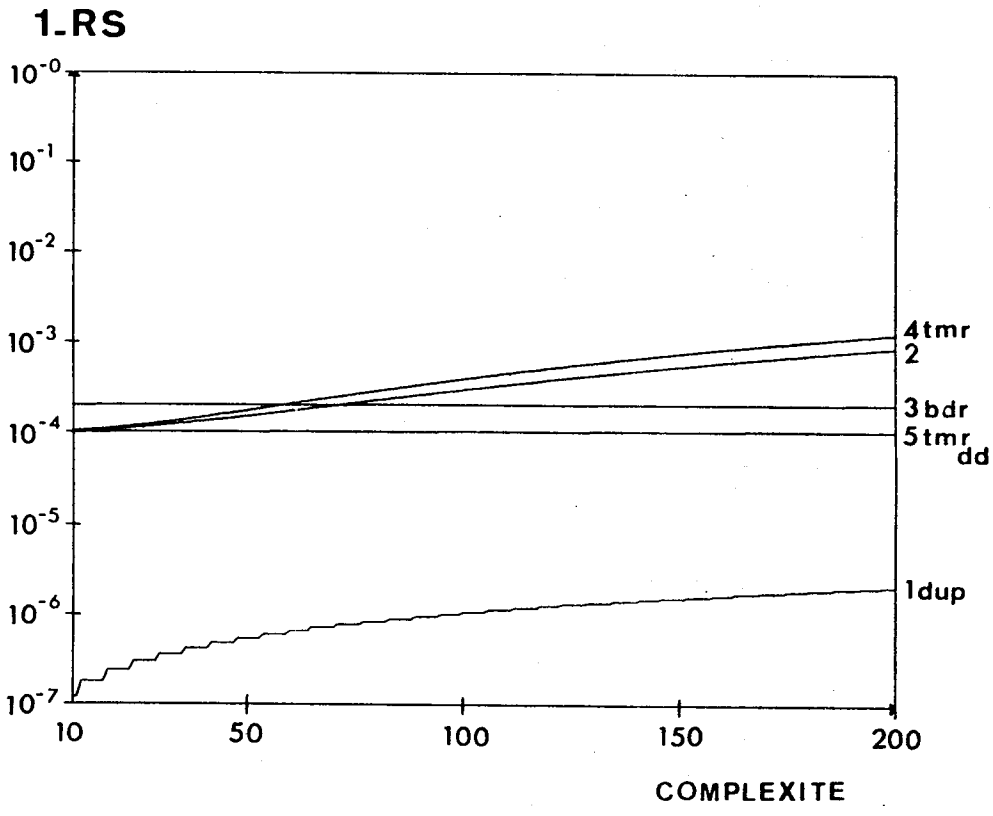


Figure 15. Fiabilité du signal

III - 5. CONCLUSION PARTIELLE

Des résultats des paragraphes précédents, il s'avère que les deux systèmes pouvant réaliser un bon compromis sécurité-fiabilité de mission sont les systèmes 4 (TMR) et 3 (BDR). Mais, bien que le système TMR ait une fiabilité de mission meilleure que le système BDR, la différence est très faible (Fig. 13) et, fait plus important, à partir d'une certaine complexité des unités fonctionnelles, le système BDR a une meilleure sécurité et une allure de courbe beaucoup plus intéressante (quasi linéarité).

IV - SYSTEME BI-DUPLEX ET SYSTEMES HYBRIDES, MODELISATION

Nous avons comparé dans la section précédente des systèmes n'ayant pas un nombre identique d'unités fonctionnelles. C'est pourquoi nous allons maintenant comparer un système à redondance bi-duplex à des systèmes ayant 4 ou 5 unités fonctionnelles. Plus précisément, nous allons considérer des systèmes hybrides avec ou sans signal de stop et composés d'un noyau TMR et d'une ou deux unités fonctionnelles de remplacement. De plus, nous ne considèrerons que les paramètres de sécurité et fiabilité de mission.

IV - 1. SYSTEME A REDONDANCE BI-DUPLEX

Ce système est représenté par la figure 16.

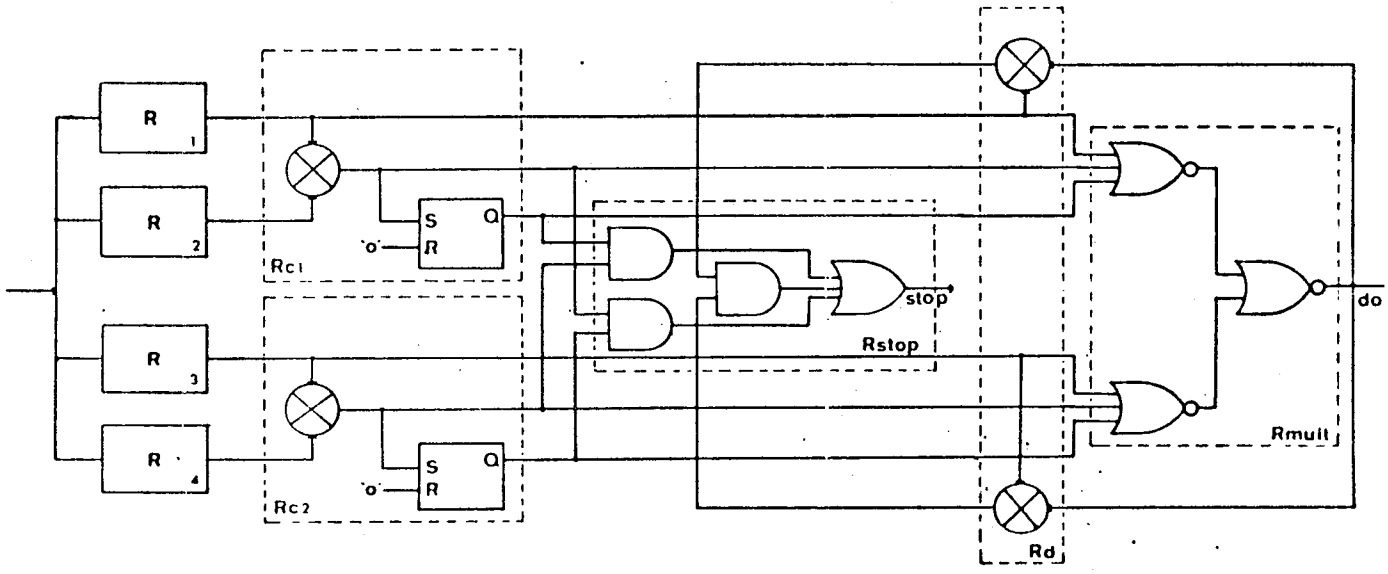


Figure 16. Système à redondance bi-duplex

Les circuits RD ont été ajoutés par rapport au système de la section III afin de protéger le système contre les pannes pouvant survenir dans le multiplexeur. Il nous faut ici mentionner le "detector redundant system" présenté dans |9|. On ne comparera pas ce système avec ceux de cette section car il est difficile de comparer des systèmes ayant des boites appelées "détecteurs" avec des systèmes n'en ayant pas. De plus, si on considère des détecteurs parfaits, le meilleur système sera toujours un système standby.

Sécurité et fiabilité de mission du système BDR

Sécurité

$$
\begin{aligned}
1 - S \leqslant\ & R_{MULT}.(1-R_{STOP})\,|(1-R_{C1})(1-R_{C2}) \\
& + (1-R_{C1})R_{C2}\,|2R^3(1-R) + 6R^2(1-R)^2 + 4R(1-R)^3+(1-R)| \\
& + (1-R_{C2})R_{C1}\,|2R^3(1-R) + 6R^2(1-R)^2 + 4R(1-R)^3 + (1-R)| \\
& + R_{C1}.R_{C2}\,|4R^2(1-R)^2 \\
& + 4R(1-R)^3 + (1-R)^4|| \\
& + R_{MULT}.(1-R_D)R_{STOP}\,|(1-R_{C1})R_{C2}\,|R^3(1-R) + 3R^2(1-R)^2 + 3R(1-R)^3 + (1-R)^4| \\
& + R_{C1}(1-R_{C2})\,|R^3(1-R) + 3R^2(1-R)^2 + 3R(1-R)^3 + (1-R)^4| \\
& + R_{C1}(1-R_{C2})\,|R^3(1-R) + 3R^2(1-R)^2 + 3R(1-R)^3 + (1-R)^4| \\
& + (1-R_{C1})(1-R_{C2})\,|2R^3(1-R) + 5R^2(1-R)^2 + 4R(1-R)^3| \\
& + (1-R)^4|| \\
& + (1-R_{MULT})R_D(1-R_{STOP}) \\
& + (1-R_{MULT})(1-R_D)R_{STOP} \\
& + (1-R_{MULT})(1-R_D)(1-R_{STOP})
\end{aligned}
$$

Fiabilité de mission

$$
\begin{aligned}
RM \geqslant\ & R_{MULT}.R_D.R_{STOP}\,|R_{C1}.R_{C2}\,|R^4 + 4R^3(1-R) + 2R^2(1-R)^2| \\
& + (1-R_{C1})R_{C2}\,|R^4+R^3(1-R)| + R_{C1}(1-R_{C2})\,|R^4 + R^3(1-R)||
\end{aligned}
$$

En effet, dans les états :

$MULT.RD.\overline{STOP}$

$MULT.\overline{RD}.STOP$

$MULT.\overline{RD}.\overline{STOP}$

$\overline{MULT}.RD.STOP$

$\overline{MULT}.RD.\overline{STOP}$

$\overline{MULT}.\overline{RD}.STOP$

$\overline{MULT}.\overline{RD}.\overline{STOP}$

le système peut être arrêté.

IV - 2. SYSTEMES HYBRIDES

Nous allons considérer des systèmes hybrides avec des cellules itératives |10|. Plus précisément, nous aurons un noyau TMR et 1 ou 2 modules de remplacement. Pour les 2 types de systèmes, nous implémenterons ou non un signal de stop, et nous utiliserons une porte à seuil |11|.

Systèmes hybrides sans signal de stop

La logique d'interconnexion avec un voteur à seuil étant plus attractive pour des développements futurs, c'est elle que nous choisirons.

Conformément aux définitions précédentes, ces systèmes ont une sécurité égale à leur fiabilité de mission.

Par examen des divers états d'un système hybride sans signal de stop et ayant un module de secours, on obtient :

$$\begin{aligned} RM \geq\ & R_T|R_{D1}R_{D2}R_{D3}R_{D4}|R^4 + 4R^3(1-R) + 6R^2(1-R)^2| \\ & + R_{D1}R_{D2}R_{D3}(1-R_{D4})|R^3 + 3R^2(1-R)| \\ & + R_{D1}R_{D2}(1-R_{D3})R_{D4}|R^2| \\ & + (1-R_{D1})R_{D2}R_{D3}R_{D4}|R^3 + 3R^2(1-R)|| \end{aligned}$$

Si par exemple, D2 est en panne, il peut transmettre à la 3e cellule le code signifiant : "3 modules ont été trouvés sans panne" et ainsi, seul le 1er module est connecté au voteur (R1 est supposé être bon) alors que D2 peut envoyer une valeur 1 au voteur.

Pour un système ayant 2 modules de secours, on obtient :

$$\begin{aligned} RM \geq\ & R_T|R_{D1}R_{D2}R_{D3}R_{D4}R_{D5}|R^5 + 5R^4(1-R) + 10R^3(1-R)^2 + 10R^2(1-R)^3| \\ & + R_{D1}R_{D2}R_{D3}R_{D4}(1-R_{D5})|R^4 + 4R^3(1-R) + 6R^2(1-R)^2| \\ & + R_{D1}R_{D2}R_{D3}(1-R_{D4})R_{D5}|R^3 + 3R^2(1-R)| \\ & + R_{D1}R_{D2}(1-R_{D3})R_{D4}R_{D5}|R^2| \\ & + (1-R_{D1})R_{D2}R_{D3}R_{D4}R_{D5}|R^4 + 4R^3(1-R) + 6R^2(1-R)^2|| \end{aligned}$$

Systèmes hybrides avec signal de stop

Pour ces systèmes également, nous utiliserons une porte à seuil. En effet, on pourrait penser utiliser un voteur majoritaire et un signal de stop utilisant les 3 entrées et la sortie du voteur. Mais, dans ce cas, dès que D1, par exemple, serait en panne, il pourrait transmettre le code "3 modules ont été trouvés bons" à la 2e cellule. Ainsi, les 3 entrées du voteur pourraient recevoir la même valeur erronée. Après cela, toutes les bascules ayant fonctionné, on aurait 3 entrées identiques, et on ne détecterait pas de désaccord entre les entrées et la sortie du voteur. La figure 17 représente un système hybride avec un noyau TMR, 2 modules de remplacement et un signal de stop.

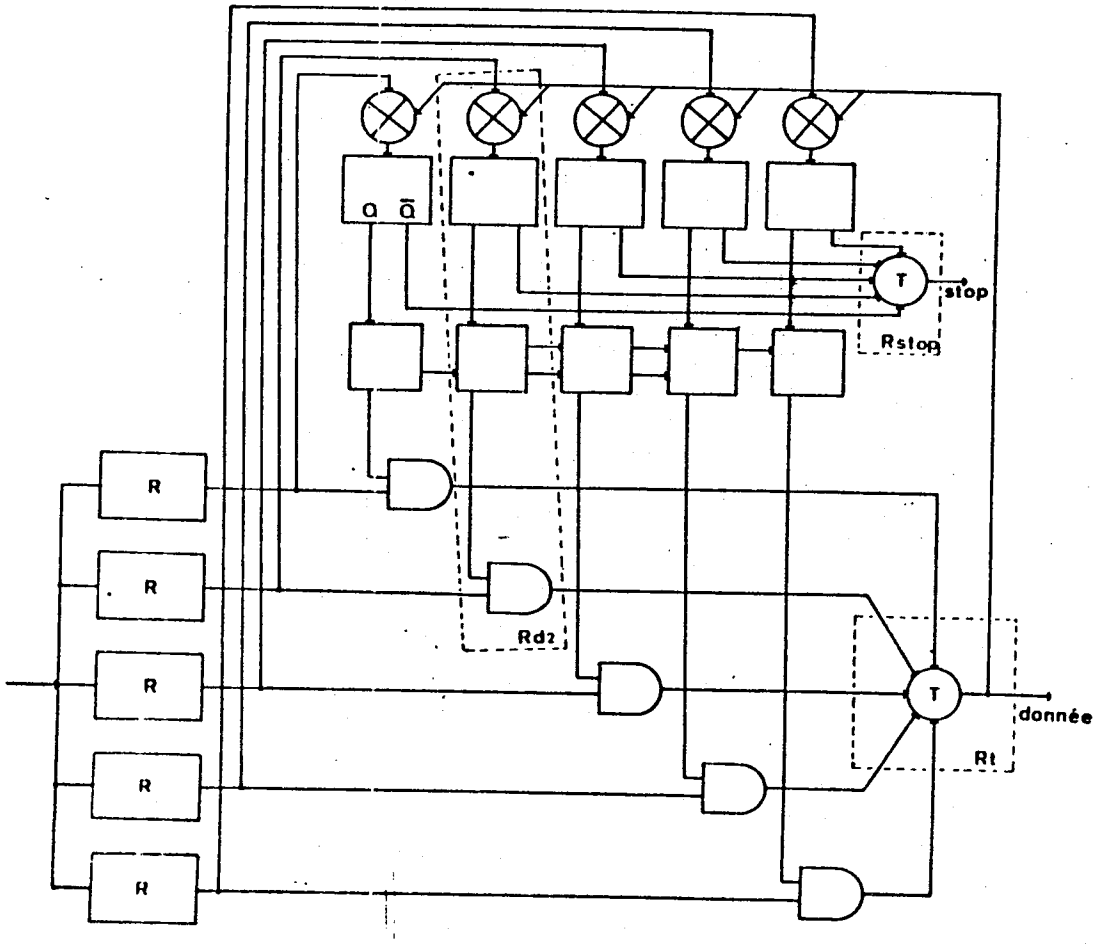


Figure 17. Système hybride avec signal stop

Sécurité d'un système hybride avec signal de stop et 1 module de secours

On peut montrer (Annexe II) que :

$$
\begin{aligned}
1 - S \leq\ & (1-R_{STOP})\,|1\text{- fiabilité du même système sans signal de stop}| \\
& + R_{STOP}\,|R_{D1}R_{D2}(1-R_{D3})(1-R_{D4}) \\
& \quad + R_{D1}(1-R_{D2})R_{D3}(1-R_{D4}) \\
& \quad + R_{D1}(1-R_{D2})(1-R_{D3}) \\
& \quad + (1-R_{D1})R_{D2}R_{D3}(1-R_{D4}) \\
& \quad + (1-R_{D1})R_{D2}(1-R_{D3}) \\
& \quad + (1-R_{D1})(1-R_{D2})|
\end{aligned}
$$

Sécurité d'un système hybride avec signal de stop et 2 modules de secours

En procédant de manière analogue à celle utilisée pour un système à 1 seul module de secours, on obtient :

$$
\begin{aligned}
1 - S \leqslant\ & (1-R_{STOP})\,|1 - \text{Fiabilité du même système sans signal de stop}| \\
& + R_{STOP}\,|R_{D1}.R_{D2}.R_{D3}(1-R_{D4})(1-R_{D5}) \\
& \quad + R_{D1}.R_{D2}.(1-R_{D3})R_{D4}.(1-R_{D5}) \\
& \quad + R_{D1}.R_{D2}.(1-R_{D3})(1-R_{D4}) \\
& \quad + R_{D1}(1-R_{D2})R_{D3}.R_{D4}(1-R_{D5}) \\
& \quad + R_{D1}(1-R_{D2})R_{D3}(1-R_{D4}) \\
& \quad + R_{D1}(1-R_{D2})(1-R_{D3}) \\
& \quad + (1-R_{D1})R_{D2}.R_{D3}.R_{D4}(1-R_{D5}) \\
& \quad + (1-R_{D1})R_{D2}.R_{D3}(1-R_{D4}) \\
& \quad + (1-R_{D1})(1-R_{D2}) \\
& \quad + (1-R_{D1})R_{D2}(1-R_{D3})|
\end{aligned}
$$

Fiabilité de mission d'un système hybride avec signal de stop et 1 module de secours

On peut montrer (Annexe 2) que :

$$
\begin{aligned}
RM \geqslant\ & R_{STOP}.R_T\,|R_{D1}.R_{D2}.R_{D3}.R_{D4}\,|R^4+4R^3(1-R) + 6R^2(1-R)^2| \\
& + R_{D1}.R_{D2}.R_{D3}(1-R_{D4})\,|R^4+4R^3(1-R) + 3R^2(1-R)^2| \\
& + R_{D1}.R_{D2}(1-R_{D3})R_{D4}\,|R^4+2R^3(1-R) + R^2(1-R)^2| \\
& + (1-R_{D1})R_{D2}.R_{D3}.R_{D4}\,|R^4+2R^3(1-R)||
\end{aligned}
$$

Fiabilité de mission d'un système hybride avec signal de stop et 2 modules de secours

On obtient :

$$
\begin{aligned}
RM \geqslant\ & R_{STOP}.R_T\,|R_{D1}.R_{D2}.R_{D3}.R_{D4}.R_{D5}\,|R^5+5R^4(1-R) + 10R^3(1-R)^2+ 10R^2(1-R)^3| \\
& \quad + R_{D1}.R_{D2}.R_{D3}.R_{D4}(1-R_{D5})\,|R^5+5R^4(1-R) + 10R^3(1-R)^2+6R^2(1-R)^3| \\
& \quad + R_{D1}.R_{D2}.R_{D3}(1-R_{D4})R_{D5}\,|R^5+5R^4(1-R)+ 7R^3(1-R)^2+3R^2(1-R)^3| \\
& + R_{D1}.R_{D2}(1-R_{D3})R_{D4}.R_{D5}\,|R^5+3R^4(1-R) + 3R^3(1-R)^2+R^2(1-R)^3| \\
& + (1-R_{D1})R_{D2}.R_{D3}.R_{D4}.R_{D5}\,|R^5+5R^4(1-R)+ 7R^3(1-R)^2+3R^2(1-R)^3||
\end{aligned}
$$

V - COMPARAISON DES SYSTEMES BDR ET HYBRIDES

V - 1. INTRODUCTION

D'une manière analogue au paragraphe III, nous définirons un rapport de complexité entre les unités fonctionnelles et les circuits de détection commutation. On adoptera donc les conventions suivantes :

Système BDR	R	$\rightarrow$	R^T
	R_{C1}	$\rightarrow$	R^2
	R_{C2}	$\rightarrow$	R^2
	R_{MULT}	$\rightarrow$	R
	R_{STOP}	$\rightarrow$	R
	R_D	$\rightarrow$	R
Systèmes hybrides	R	$\rightarrow$	R^T
	R_{Di}	$\rightarrow$	R^2
	R_T	$\rightarrow$	R^2
	R_{STOP}	$\rightarrow$	R^2

V - 2. ANALYSE DE LA SECURITE ET DE LA FIABILITE DE MISSION POUR DE PETITES UNITES FONCTIONNELLES

On considèrera tout d'abord de petites unités fonctionnelles (de 10 à 200 fois un X - OR ou un multiplexeur pour le système BDR) et un temps de mission correspondant à $R = 1 - 10^{-4}$. Les figures 18 et 19 montrent la sécurité et la fiabilité de mission. Les notations sont :

BDR : système à redondance bi-duplex
H4 : système hybride avec 4 unités fonctionnelles
H4S : système hybride avec 4 unités fonctionnelles et un signal de stop
H5 : système hybride avec 5 unités fonctionnelles
H5S : système hybride avec 5 unités fonctionnelles et un signal de stop

C'est dans ce cas que les circuits additionnels ont un gros impact. Le système BDR a la meilleure sécurité parce qu'il n'y a pas de lien entre les 2 groupes bi-duplex alors que dans le cas des systèmes hybrides, il y a transfert d'information de la i^e cellule à la $i + 1^e$. De plus, si 2 cellules Di sont tombées en panne, on peut avoir un état non sûr. Ce fait est aussi responsable de la meilleure sécurité du système H4S par rapport à celle du système H5S. H4 et H5 n'ayant pas de signal de stop, ils ont la moins bonne sécurité.

La sécurité étant "payée" par une perte de fiabilité de mission, le système BDR a la moins bonne probabilité d'exécuter correctement la mission. H4S et H5S ont environ la même fiabilité de mission et enfin H4 et H5 sont les meilleurs systèmes si on prend uniquement en compte le paramètre de fiabilité de mission.

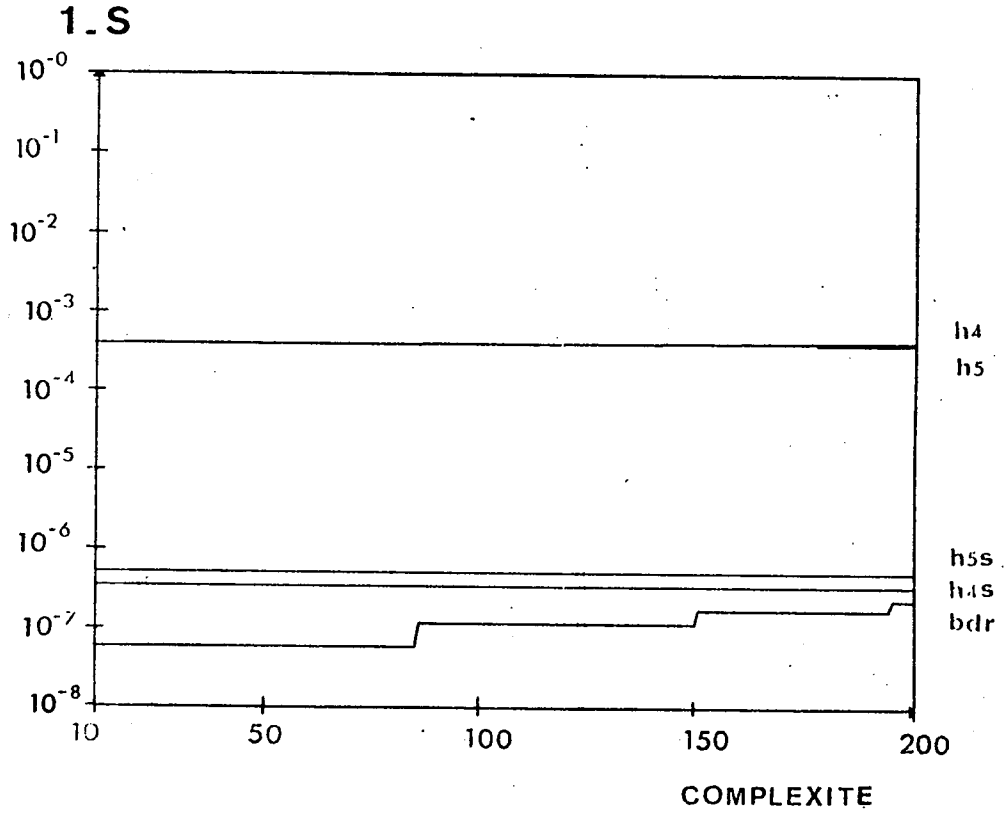


Figure 18.

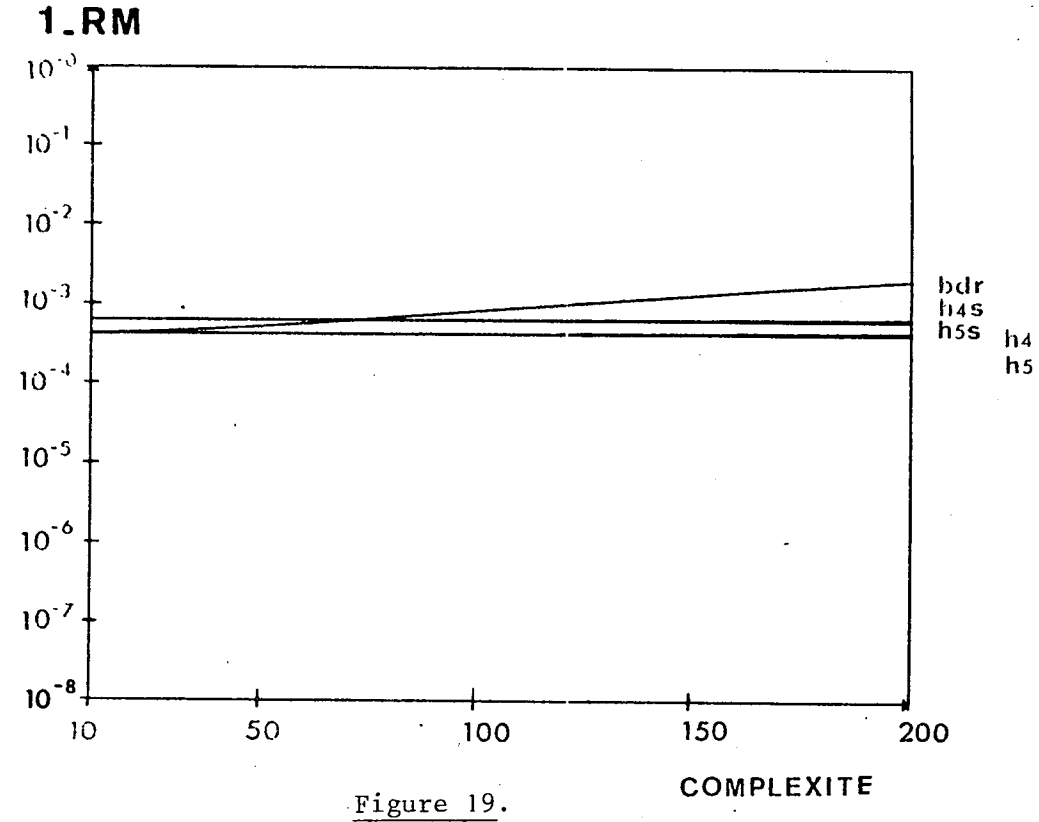


Figure 19.

V - 3. ANALYSE DE LA SECURITE ET DE LA FIABILITE DE MISSION POUR DES UNITES FONCTIONNELLES PLUS COMPLEXES ET UN TEMPS DE MISSION PLUS LONG

Si l'on s'intéresse aux courbes de sécurité et fiabilité de mission pour des unités fonctionnelles plus complexes et pour un temps de mission plus long correspondant à $R = 1 - 10^{-3}$, (Fig. 20 & 21), on peut voir que les 5 systèmes ont tous une très faible fiabilité de mission. Mais, en fonction de la complexité des unités fonctionnelles, le système BDR, ou bien H4S ou bien H5S a la meilleure sécurité : il y a 4 points d'intersection sur la figure. De la même manière que pour de petites unités fonctionnelles et $R = 1 - 10^{-4}$, H4S a une meilleure sécurité que H5S, lorsque le rapport de complexité est d'environ 100. Pour de plus grandes complexités, les pannes dans les unités fonctionnelles ont plus d'influence que les pannes dans les circuits additionnels.

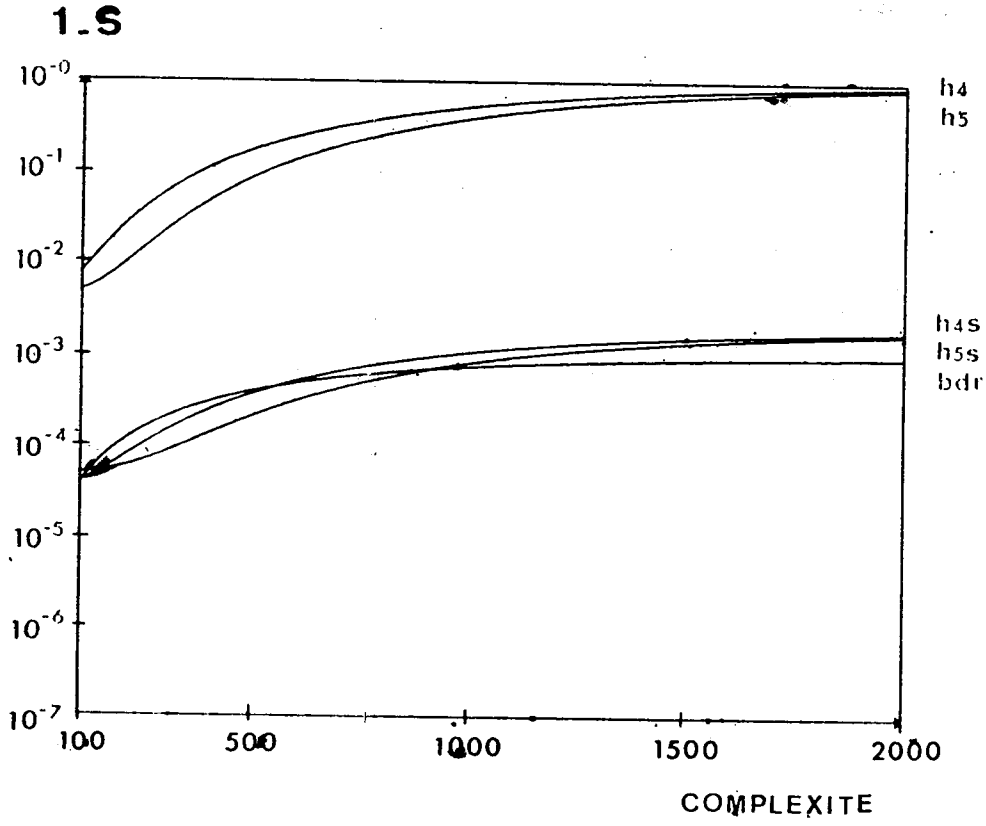


Figure 20.

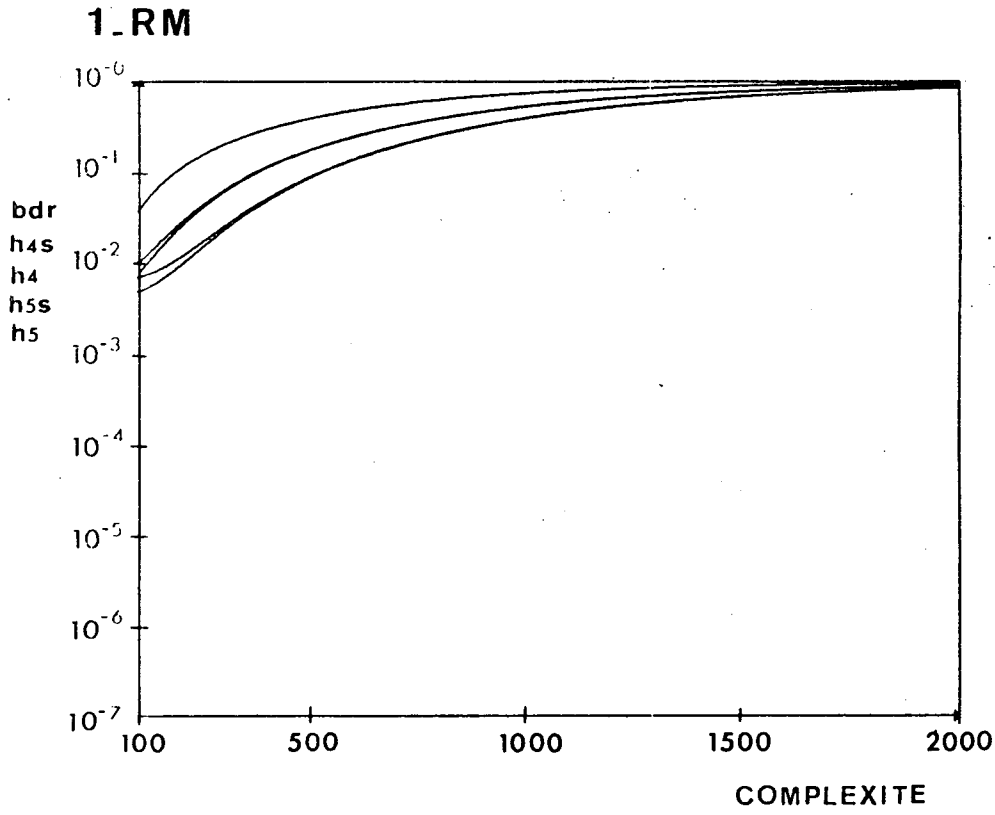

1_RM
10^-0
10^-1
10^-2
10^-3
10^-4
10^-5
10^-6
10^-7
bdr
h4s
h4
h5s
h5
100
500
1000
1500
2000
COMPLEXITE

Figure 21.

VI - CONCLUSION : CHOIX D'UN SYSTEME

Des résultats du paragraphe III, il s'avère que les deux systèmes pouvant réaliser un bon compromis sécurité-fiabilité de mission étaient les systèmes 4 (TMR) et 3 (BDR). Mais, bien que le système TMR ait une fiabilité de mission meilleure que le système BDR, la différence est très faible (Fig.13), et fait plus important, à partir d'une certaine complexité des unités fonctionnelles, le système BDR a une meilleure sécurité et une allure de courbe beaucoup plus intéressante (quasi-linéarité). Les résultats de la section précédente sont plus significatifs car les systèmes comparés ont des coûts plus voisins (4 modules si l'on considère les systèmes BDR, H4S et H4).

Remarquons néanmoins, que le système BDR a un coût moindre que celui du système H4S, et que le système H5S est celui qui coûte le plus cher.

Mais ces résultats ne sont que partiels, puisque toutes les fonctions dépendent des 2 paramètres temps et complexité et que nous n'avons tracé des courbes qu'en fonction de la complexité pour un temps de mission fixé. Une visualisation des courbes en fonction simultanément des 2 paramètres serait un atout pour mieux cerner les propriétés de chacun des systèmes et nous permettrait de tirer des conclusions un peu plus fortes.

Néanmoins, le problème qui se pose au concepteur n'en serait pas résolu pour autant. Ce problème peut, en effet, se formuler de la manière suivante : les temps de mission et complexité des unités fonctionnelles étant déterminés par les contraintes inhérentes au système, le concepteur doit déterminer une fonction objective à partir des coûts (positifs ou négatifs) de réussite effective de la mission, de désécurité, etc...

Maximiser la fonction objectif permettrait alors au concepteur de choisir le système le mieux adapté aux contraintes.

Ceci montre clairement qu'il ne peut exister un système "optimal" parmi ceux présentés dans cette première partie.

REFERENCES

1) R.C. OGUS : "Fault-tolerance of the iterative cell array switch for hybrid redundancy", IEEE Trans. Comput. Vol. C-23, juillet 1974.

2) J. LOSQ : "Influence of fault-detection and switching mechanisms on the reliability of standby systems". IEEE Fault-Tolerant Computing Symposium. Paris, juin 1975.

3) B. COURTOIS : "Logical systems for security and reliability". Rapport interne ENSIMAG n° 14, Grenoble (France), Computer Repository n° 76-30, février 1976.

4) J.F. WAKERLY : "Partially self-checking circuits and their use in performing logical operations". IEEE Trans. Comp., vol C-23, juillet 1974.

5) B.R. BORGERSON : "A fail-softly system for time sharing use". Fault-tolerant Computing Symposium, Newton (USA) 1972.

6) B. COURTOIS, C. GUERIN, Ch. ROBACH, G. SAUCIER, A. VERDILLON : "Computer Test Program". Workshop on Diagnosis and Reliable Design of Digital Systems Pasadena (USA) 1973.

7) B. COURTOIS : "On balancing safety and reliability of hybrid and Bi-duplex systems", IEEE Fault-tolerant Computing Symposium, Pittsbrugh (USA) juin 1976.

8) B. COURTOIS : "Redundancy : reliability and/or security", Fault Diagnosis of Digital Networks and Fault-Tolerant Computing Symposium, Katowice (Pologne) avril 1975.

9) C.V. RAMAMOORTHY, YIH-WU HAN : "Reliability analysis of systems with concurrent error detection", IEEE Trans. Comp. Vol. C-24, septembre 1975.

10) D.P. SIEWIOREK, E.J. Mc CLUSKEY : "An iterative cell switch design for hybrid redundancy", IEEE Trans. Comp. Vol. C-22, mars 1973.

11) D. HAMPEL, R.O. WINDER : "Threshold logic", IEE Spectrum, Vol.8, mai 1971.

12) H. MINE, Y. KOGA : "Basic properties and a construction method for fail-safe logic systems", IEEE Trans. Election, Comp. Vol. EC-16, juin 1967.

13) R. OGUS : "The probability of a correct output from a combinatorial circuit", IEEE Fault-tolerant Computing Symposium, Champaign, Illinois, juin 1974.

14) J.C. LAPRIE : "Prévision de la sûreté de fonctionnement et architecture de structures numériques temps réel réparables", thèse de doctorat d'état, toulouse, juin 1975.

ANNEXE 1

FIABILITE DE SIGNAL DES SYSTEMES BDR ET TMR

A1 - 1. PREMIER SYSTEME DUPLEX REPLIQUE

A1 - 2. SYSTEME BDR

A1 - 3. SYSTEME TMR

A1 - 1. PREMIER SYSTEME DUPLEX REPLIQUE

Nous devons considérer tous les états où il se peut que l'on dispose du système, et parmi ceux-ci, ceux pour lesquels l'information est juste. Les états où il se peut que l'on dispose du système peuvent être représentés par :

$$Y = \overline{MULT}$$

$$+ MULT\ C1\ C2 \quad |\textit{4 unités marchent + 3 parmi 4 marchent + 3 dans le même groupe marmi 4 marchent + 1/4 marche + 0/4 marche}|$$

$$+ MULT\ \overline{C1}\ C2\ |1|$$

$$+ MULT\ C1\ \overline{C2}\ |1|$$

$$+ MULT\ \overline{C1}\ \overline{C2}\ |1|$$

Soit :

$$Y = 1 - R_{MULT}$$

$$+ R_{MULT}.R_{C1}.R_{C2}|R^4 + 4R^3(1-R) + 2R^2(1-R)^2 + 4R(1-R)^3 + (1-R)^4|$$

$$+ R_{MULT}.(1-R_{C1})R_{C2}|1|$$

$$+ R_{MULT}.R_{C1}(1-R_{C2})|1|$$

$$+ R_{MULT}(1-R_{C1}).(1-R_{C2})|1|$$

Parmi ces états où il se peut que l'on dispose du système, nous devons considérer ceux pour lesquels la sortie est bonne :

$$X = MULT.C1.C2|R^4 + 4R^3(1-R)|$$

$$+ MULT.\overline{C1}.C2|R^4 + 3R^3(1-R)$$

Si 1 en panne, C1 peut laisser passer une valeur fausse.
Si 2 en panne, C1 peut laisser passer une valeur bonne.
Si 3 en panne, dans le cas où le système n'est pas arrêté, la valeur est bonne.
Si 4 en panne, idem.

$$+ 2R^2(1-R)^2$$

Si 1 et 2, 1 et 3, ou 1 et 4 sont en panne, la valeur est fausse si elle existe.
Si 2 et 3, ou 2 et 4 sont en panne, la valeur est bonne si elle existe.

Si 3 et 4 sont en panne, il se peut que, si la valeur existe, elle soit fausse.

$+ 0 + 0 |1|$

Si 1, 2 et 3 en panne, valeur fausse
Si 1, 2 et 4 " " "
Si 1, 3 et 4 " " "
Si 2, 3 et 4 " " "
Si 1, 2, 3, 4 " " "

$+ \text{MULT } C1\ \overline{C2} |R^4 + 3R^3(1-R) + 2R^2(1-R)^2 |$

$+ \text{MULT } \overline{C1}\ \overline{C2} |R^4 + 2R^3(1-R)$

Si 1 en panne, valeur fausse
Si 2 en panne, valeur bonne
Si 3 en panne, valeur fausse
Si 4 en panne, valeur bonne.

$+ R^2(1-R)^2$

Si 1 et 2 en panne, valeur fausse
Si 1 et 3 " " "
Si 1 et 4 " " "
Si 2 et 3 " " "
Si 2 et 4 en panne, valeur bonne
Si 3 et 4 en panne, valeur fausse.

$+ 0 + 0 |$

Ce qui peut s'écrire :

$$X = R_{MULT} \cdot R_{C1} \cdot R_{C2} |4R^3 - 3R^4|$$
$$+ R_{MULT}(1-R_{C1})R_{C2} |2R^2 - R^3|$$
$$+ R_{MULT}\ R_{C1}(1-R_{C2}) |2R^2 - R^3|$$
$$+ R_{MULT}(1-R_{C1})(1-R_{C2}) |R^2|$$

On a alors la fiabilité du signal par :

$$RS = X/Y$$

A1 - 2. <u>SYSTEME BDR</u> (n° 3 de la section II)

On aura

RS X/Y

Etats où l'on peut disposer du système :

$Y = \overline{MULT}$

+ MULT.C1.C2 |*4 unités marchent + 3 parmi 4 marchent + 2 dans le*
+ MULT $\overline{C1}$ C2 |1| *même groupe marchent*|
+ MULT C1 $\overline{C2}$ |1|
+ MULT $\overline{C1}$ $\overline{C2}$ |1|

Etats où la sortie est bonne, si elle existe :

X = MULT.C1.C2 |*4 marchent + 3/4 marchent + 2 dans le même groupe marchent*|
+ MULT $\overline{C1}$ C2 $|R^4 + 3R^3(1-R)$

Si 1 en panne, valeur fausse
Si 2 en panne, valeur bonne
Si 3 " " "
Si 4 " " "

$+ 3R^2(1-R)^2$

Si 1 et 2 en panne, valeur fausse si elle existe
Si 1 et 3 en panne, " " "
Si 1 et 4 en panne, " " "
Si 2 et 3 en panne, valeur bonne si elle existe
Si 2 et 4 en panne, " " "
Si 3 et 4 en panne, " " "

$+ R(1-R)^3|$

Si 1, 2 et 3 en panne, valeur fausse
Si 1, 2 et 4 en panne, " "
Si 1, 3 et 4 en panne, " "
Si 2, 3 et 4 en panne, valeur bonne.

+ MULT C1 $\overline{C2}|R^4 + 3R^3(1-R) + 3R^2(1-R)^2 + R(1-R)^3|$

+ MULT $\overline{C1}$ $\overline{C2}|R^4 + 2R^3(1-R)$

Si 1 en panne, valeur fausse
Si 2 en panne, valeur bonne
Si 3 en panne, valeur fausse
Si 4 en panne, valeur bonne

$+ R^2(1-R)^2 |$

Si 1 et 2 en panne, valeur fausse
Si 1 et 3 en panne, valeur fausse
Si 1 et 4 en panne, valeur fausse
Si 2 et 3 en panne, valeur fausse
Si 2 et 4 en panne, valeur bonne
Si 3 et 4 en panne, valeur fausse

Reprenons l'expression de Y :

$$
\begin{aligned}
Y = \overline{MULT}\ & \\
& MULT\ C1\ C2 |R^4 + 4R^3(1-R) + 2R^2(1-R)^2| \\
& MULT\ C1\ \overline{C2} |1| \\
& MULT\ \overline{C1}\ C2\ |1| \\
& MULT\ \overline{C1}\ \overline{C2}\ |1| \\
= 1 - R_{MULT} & \\
+ R_{MULT} & |R_{C1}\ R_{C2}(2R^2 - R^4) + 1 - R_{C1}\ R_{C2}|
\end{aligned}
$$

Reprenons l'expression de X :

$$
\begin{aligned}
X = MULT\ C1\ C2 & |2R^2 - R^4| \\
+ MULT\ C1\ \overline{C2} & |R| \\
+ MULT\ \overline{C1}\ C2 & |R| \\
+ MULT\ \overline{C1}\ \overline{C2} & |R^2| \\
= R_{MULT}\ R_{C1}\ R_{C2} & |2R^2 - R^4| \\
+ R_{MULT}\ R_{C1}(1-R_{C2}) & |R| \\
+ R_{MULT}(1-R_{C1})\ R_{C2} & |R| \\
+ R_{MULT}(1-R_{C1})(1-R_{C2}) & |R^2|
\end{aligned}
$$

A1 - 3. SYSTEME TMR (n° V de la section II)

Nous allons considérer les états où il se peut que l'on dispose du système, ainsi que la valeur délivrée :

$\overline{RV}$	*Sortie fausse*
$RV\ C1\ C2\ C2\ R^3$	*Sortie juste*
$RV\ C1\ C2\ \overline{C3}\ R^3$	*Sortie juste*
$RV\ C1\ C2\ \overline{C3}\ R^2(1-R)$	*Sortie juste (n° 3 en panne)*

$RV\ C1\ C2\ \overline{C3}\ R(1-R)^2$	*Sortie fausse (n° 3 et 1 en panne)*
$RV\ C1\ C2\ \overline{C3}\ R(1-R)^2$	*Sortie fausse (n° 3 et 2 en panne)*
$RV\ C1\ C2\ \overline{C3}(1-R)^3$	*Sortie fausse*
$RV\ C1\ \overline{C2}\ C3\ R^3$	*Sortie juste*
$RV\ C1\ \overline{C2}\ C3\ R^2(1-R)$	*Sortie juste*
$RV\ C1\ \overline{C2}\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ C1\ \overline{C2}\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ C1\ \overline{C2}\ C3(1-R)^3$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ C3\ R^3$	*Sortie juste*
$RV\ \overline{C1}\ C2\ C3\ R^2(1-R)$	*Sortie juste*
$RV\ \overline{C1}\ C2\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ C3(1-R)^3$	*Sortie fausse*
$RV\ C1\ \overline{C2}\ \overline{C3}\ R^3$	*Sortie juste*
$RV\ C1\ \overline{C2}\ \overline{C3}\ R^2(1-R)$	*Sortie juste (n° 2 en panne)*
$RV\ C1\ \overline{C2}\ \overline{C3}\ R^2(1-R)$	*Sortie juste (n° 3 en panne)*
$RV\ C1\ \overline{C2}\ \overline{C3}\ R(1-R)^2$	*Sortie fausse (n° 2 et 3 en panne)*
$RV\ C1\ \overline{C2}\ \overline{C3}\ R(1-R)^2$	*Sortie fausse (n° 2 et 1 en panne)*
$RV\ C1\ \overline{C2}\ \overline{C3}\ R(1-R)^2$	*Sortie fausse (n° 3 et 2 en panne)*
$RV\ C1\ \overline{C2}\ \overline{C3}(1-R)^3$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ \overline{C3}\ R^3$	*Sortie juste*
$RV\ \overline{C1}\ C2\ \overline{C3}\ R^2(1-R)$	*Sortie juste*
$RV\ \overline{C1}\ C2\ \overline{C3}\ R^2(1-R)$	*Sortie juste*
$RV\ \overline{C1}\ C2\ \overline{C3}\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ \overline{C3}\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ \overline{C3}\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ C2\ \overline{C3}(1-R)^3$	*Sortie fausse*
$RV\ \overline{C1}\ \overline{C2}\ C3\ R^3$	*Sortie juste*
$RV\ \overline{C1}\ \overline{C2}\ C3\ R^2(1-R)$	*Sortie juste*
$RV\ \overline{C1}\ \overline{C2}\ C3\ R^2(1-R)$	*Sortie juste*
$RV\ \overline{C1}\ \overline{C2}\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ \overline{C2}\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ \overline{C2}\ C3\ R(1-R)^2$	*Sortie fausse*
$RV\ \overline{C1}\ \overline{C2}\ C3(1-R)^3$	*Sortie fausse*
$RV\ \overline{C1}\ \overline{C2}\ \overline{C3}\ (3R^2-2R^3)$	*Sortie juste*
$RV\ C1\ C2\ C3\ \lvert 1 - (3R^2 - 2R^3)\rvert$	*Sortie fausse*

Compte tenu de ce qui précède, on peut établir l'expression de la fiabilité du signal :

$$RS \geq X/Y$$

$$\begin{aligned}
Y = {} & (1-R_V) \\
& + R_V\, R_{C1}\, R_{C2}\, R_{C3}(R^3) \\
& + R_V\, R_{C1}\, R_{C2}(1-R_{C3})(R^3+R^2(1-R) + 2R(1-R)^2 + (1-R)^3) \\
& + R_V\, R_{C1}(1-R_{C2})\, R_{C3}(R^3+R^2(1-R) + 2R(1-R)^2 + (1-R)^3) \\
& + R_V(1-R_{C1})R_{C2}\, R_{C3}(R^3+R^2(1-R) + 2R(1-R)^2 + (1-R)^3) \\
& + R_V\, R_{C1}(1-R_{C2})(1-R_{C3})(R^3 + 2R^2(1-R) + 3R(1-R)^2 + (1-R)^3) \\
& + R_V(1-R_{C1})R_{C2}(1-R_{C3})(R^3+2R^2(1-R) + 3R(1-R)^2 + (1-R)^3) \\
& + R_V(1-R_{C1})(1-R_{C2})R_{C3}(R^3+2R^2(1-R) + 3R(1-R)^2 + (1-R)^3) \\
& + R_V(1-R_{C1})(1-R_{C2})(1-R_{C3})
\end{aligned}$$

$$\begin{aligned}
X = {} & R_V\, R_{C1}\, R_{C2}\, R_{C3}(R^3) \\
& + R_V\, R_{C1}\, R_{C2}(1-R_{C3})(R^3+R^2(1-R)) \\
& + R_V\, R_{C1}(1-R_{C2})R_{C3}(R^3+R^2(1-R)) \\
& + R_V(1-R_{C1})R_{C2}\, R_{C3}(R^3+R^2(1-R)) \\
& + R_V\, R_{C1}(1-R_{C2})(1-R_{C3})(R^3+2R^2(1-R)) \\
& + R_V(1-R_{C1})(1-R_{C2})\, R_{C3}(R^3+2R^2(1-R)) \\
& + R_V(1-R_{C1})R_{C2}(1-R_{C3})(R^3+2R^2(1-R)) \\
& + R_V(1-R_{C1})(1-R_{C2})(1-R_{C3})(R^3+3R^2(1-R))
\end{aligned}$$

ANNEXE 2

SECURITE ET FIABILITE DE MISSION D'UN SYSTEME HYBRIDE AVEC SIGNAL DE STOP ET 1 MODULE DE SECOURS

A2 - 1. SECURITE

A2 - 2. FIABILITE DE MISSION

A2 - 1. SECURITE

Etats non sûrs

$\overline{STOP}$ (Etats non sûrs du système semblable sans signal de stop)

Etat STOP D1 D2 D3 D4 : pas d'états non sûrs

Etat STOP D1 D2 D3 $\overline{D4}$

0 module en panne : bon

1 module en panne :

1	en panne	:	arrêt si désaccord avec		2 et 3
2	"	:	"	"	" 1 et 3
3	"	:	"	"	" 1
4	"	:	"	"	1, 2 et 3

2 modules en panne :

1 et 2	en panne	:	arrêt si désaccord avec		3
1 et 3	"	:	"	"	" 2
1 et 4	"	:	"	"	" 2 et 3
2 et 3	"	:	"	"	" 1
2 et 4	"	:	"	"	" 1 et 3
3 et 4	"	:	"	"	" 1 et 2

3 modules en panne :

1, 2 et 3	en panne	:	arrêt
1, 2 et 4	"	:	" avec 3
2, 3 et 4	"	:	" avec 1
1, 3 et 4	"	:	" avec 2

4 modules en panne : arrêt

→ Pas d'état non sûr

Etat STOP D1 D2 $\overline{D3}$ D4

0 module en panne : bon

1 module en panne :

1	en panne	:	arrêt si désaccord avec		2 et 4
2	"	:	"	"	" 1 et 4
3	"	:	"	"	" 1, 2 et 4
4	"	:	"	"	" 1 et 2

2 modules en panne :

1 et 2	en panne	:	arrêt si désaccord avec 4		
1 et 3	"	:	"	"	" 2 et 4
1 et 4	"	:	"	"	" 2
2 et 3	"	:	"	"	" 1 et 4
2 et 4	"	:	"	"	" 1
3 et 4	"	:	"	"	" 1 et 2

3 modules en panne :

1, 2 et 3	en panne	:	arrêt si désaccord avec 4
1, 2 et 4	"	:	arrêt
2, 3 et 4	"	:	arrêt si désaccord avec 1
1, 3 et 4	"	:	" " " 2

4 modules en panne : arrêt

→ Pas d'état non sûr

Etat STOP D1 $\overline{D2}$ D3 D4

0 module en panne : arrêt si désaccord avec 1, 3 et 4

1 module en panne :

1	en panne	:	arrêt	avec 3 et 4
2	"	:	"	" 1, 3 et 4
3	"	:	"	" 1 et 4
4	"	:	"	" 1 et 3

2 modules en panne

1 et 2	en panne	:	arrêt	avec 3 et 4
1 et 3	"	:	"	" 4
1 et 4	"	:	"	" 3
2 et 3	"	:	"	" 1 et 4
2 et 4	"	:	"	" 1 et 3
3 et 4	"	:	"	" 1

3 modules en panne

1, 2 et 3	en panne	:	arrêt avec 4
1, 2 et 4	"	:	" " 3
1, 3 et 4	"	:	arrêt
2, 3 et 4	"	:	arrêt avec 1

4 modules en panne : arrêt

→ Pas d'état non sûr

Etat STOP $\overline{D1}$ D2 D3 D4

0 module en panne : arrêt avec 2, 3 et 4

1 module en panne

1 en panne	:	arrêt	avec	2, 3 et 4
2 "	:	"	"	3 et 4
3 "	:	"	"	2 et 4
4 "	:	"	"	2 et 3

2 modules en panne

1 et 2 en panne	:	arrêt	avec	3 et 4
1 et 3 "	:	"	"	2 et 4
1 et 4 "	:	"	"	2 et 3
2 et 3 "	:	"	"	4
2 et 4 "	:	"	"	3
3 et 4 "	:	"	"	2

3 modules en panne

1, 2 et 3 en panne	:	arrêt	avec	4
1, 2 et 4 "	:	"	"	3
1, 3 et 4 "	:	"	"	2
2, 3 et 4 "	:	arrêt		

4 modules en panne : arrêt

→ Pas d'état non sûrs

Tous les autres états : 2 Di sont en panne et par suite tous ces états sont non sûrs, quels que soient les états des modules.

Compte tenu de ce qui précède, on obtient :

$$
\begin{aligned}
1 - S \leq\ & (1 - R_{STOP})\ |1 - \text{fiabilité du même système sans signal s'arrêt}| \\
& + R_{STOP} | R_{D1} . R_{D2} (1 - R_{D3})(1 - R_{D4}) \\
& \quad + R_{D1} . (1 - R_{D2})\ R_{D3} (1 - R_{D4}) \\
& \quad + R_{D1} . (1 - R_{D2})(1 - R_{D3}) \\
& \quad + (1 - R_{D1})\ R_{D2} . R_{D3} (1 - R_{D4}) \\
& \quad + (1 - R_{D1}) R_{D2} (1 - R_{D3}) \\
& \quad + (1 - R_{D1})(1 - R_{D2}) |
\end{aligned}
$$

A2 - 2. FIABILITE DE MISSION

L'étude des états du système montre que :

- le voteur à seuil doit fonctionner
- le signal de stop doit fonctionner

sinon il y a arrêt possible du système.

Etat D1 D2 D3 D4 : 2 parmi 4 modules doivent fonctionner

Etat D1 D2 D3 $\overline{D4}$:

0 module en panne : bon

1 module en panne : bon

2 modules en panne :

1 et 2 en panne	:	arrêt possible
1 et 3 "	:	" "
1 et 4 "	:	bon
2 et 3 "	:	arrêt
2 et 4 "	:	bon
3 et 4 "	:	bon

3 modules en panne : arrêt

Etat D1 D2 $\overline{D3}$ D4 :

0 module en panne : bon

1 module en panne :

1 en panne	:	arrêt possible
2 "	:	" "
3 "	:	bon
4 "	:	bon

2 modules en panne :

1 et 2 en panne	:	arrêt
1 et 3 "	:	"
1 et 4 "	:	"
2 et 3 "	:	"
2 et 4 "	:	"
3 et 4 "	:	bon

3 modules en panne : arrêt

Etat D1 $\overline{D2}$ D3 D4

0 module en panne : arrêt

Etat $\overline{D1}$ D2 D3 D4

0 module en panne : bon

1 module en panne :

1	en panne	: bon
2	"	: "
3	"	: arrêt
4	"	: "

2 modules en panne : arrêt

Autres états : la valeur de sortie peut être fausse. On peut alors obtenir l'expression de la fiabilité de mission :

$$
\begin{aligned}
RM \geq\ & R_{STOP}.R_T|R_{D1}.R_{D2}.R_{D3}.R_{D4}|R^4+4R^3(1-R) + 6R^2(1 - R)^2| \\
& + R_{D1}.R_{D2}.R_{D3}(1 - R_{D4})\ R^4+4R^3(1 - R) + 3R^2(1 - R)^2| \\
& + R_{D1}.R_{D2}(1 - R_{D3})R_{D4}|R^4+2R^3(1 - R) + R^2(1 - R)^2| \\
& + (1 - R_{D1})R_{D2}.R_{D3}.R_{D4}|R^4+2R^3(1 - R)||
\end{aligned}
$$

DEUXIÈME PARTIE

FIABILITE, COUT ET PUISSANCE DES MICROMACHINES

RESUME

I - POSITION DU PROBLEME

II - EVALUATION DE LA PUISSANCE DES MICROMACHINES

III - MODELISATION DES UNITES FONCTIONNELLES

IV - RELATIONS FIABILITE-COUT-PERFORMANCE

V - CONCLUSION

REFERENCES

ANNEXE

RESUME

Cette seconde partie est consacrée à l'étude des relations fiabilité-coût-puissance. Cette étude est appliquée à une machine fictive, dérivée d'une machine réelle. Le premier paragraphe décrira la méthode générale envisagée alors que le second tentera de faire une synthèse des méthodes d'évaluation de performances, afin de déterminer un critère qui sera utilisé dans la suite de l'étude. Dans le troisième paragraphe, les différentes unités fonctionnelles sont modélisées en fonction de leur contribution à la puissance de la machine. Les possibilités de redondance sont étudiées, afin de ne conserver dans la suite que des solutions intéressantes. Enfin, le quatrième paragraphe sera consacré à l'étude des relations fiabilité-coût-puissance au niveau de la machine totale, les relations étant explicitées entre 2 paramètres, le 3e restant constant. On y étudie, par exemple, les relations coût-performance obtenues avec ou sans prise en considération du paramètre fiabilité, l'influence du choix du critère de performance retenu ainsi que celle du temps de mission choisi.

I - POSITION DU PROBLEME

L'objectif de cette seconde partie est d'étudier les relations de fiabilité, coût et performance des micromachines que l'on pourrait construire pour exécuter un certain répertoire d'instructions considéré constant. Cette étude a été amenée par la question suivante : peut-on modifier l'expression de la fiabilité d'un circuit par son taux d'utilisation ?

Formulons le problème plus clairement. Considérons un certain système, ce système pouvant être un circuit, un ensemble de circuits ou un chemin de données. Il est naturel de penser que si, à la limite, on ne se sert pas de ce système, le fait qu'il fonctionne correctement ou non importe peu. Il existe donc une relation entre la fiabilité du système et l'utilisation effective qu'on en fait. D'une manière plus précise, si une mission à accomplir consiste à faire effectuer un certain traitement par le système, la probabilité d'exécution de la mission doit être plus importante, si on ne se sert que peu souvent du système, et ceci même si le système s'use. Ainsi, si l'utilisation du système est discrète et qu'on ne l'utilise qu'à 2 instants t_1 et t_2 ($t_2 > t_1$) et si la probabilité d'exécution de la mission à l'instant t_1 est P_1, cette probabilité d'exécution ne doit pas décroitre du fait qu'entre t_1 et t_2 le système peut tomber en panne.

Si la probabilité de survie du matériel est représentée par la courbe suivante, la probabilité d'exécution de la mission au delà de l'instant t_1 et avant l'instant t_2 sera P_1 et non P_i.

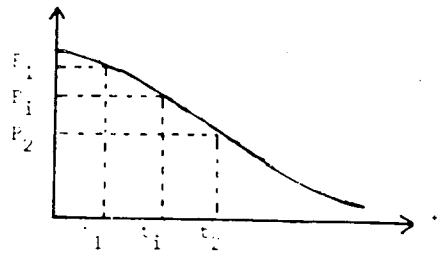


Figure 1.

Formulons le problème mathématiquement.

Soit X la variable aléatoire de durée de vie du système. La fiabilité du système est alors $P(X \geq t)$.

Soit M la variable aléatoire de durée de vie de la mission. Considérons que le processus de demande d'exécution de traitement se fait avec un taux instantané constant a, soit P(t < demande <(t + dt) = adt, qui ne dépend pas de t. Le processus de demande est un processus de Poisson, d'intensité a.

Si N est le nombre de demandes pendant $|0, t|$, $N \sim P(at)$ c'est-à-dire,

$$P(N = n) = \frac{e^{-at}(at)^n}{n!}$$

M, durée de vie de la mission est la durée pendant laquelle (à partir de 0) les demandes de traitement sont satisfaites. La fiabilité de la mission est ainsi $P(M \geq t)$, soit :

$$P(M \geq t) = P(X \geq D_1 + D_2 + \ldots + D_N)$$

où D_i est le temps écoulé entre la $(i-1)^{\text{ème}}$ demande et la $i^{\text{ème}}$.

$D_1 + D_2 + \ldots + D_N$ est ainsi l'instant de la dernière demande avant t.

Les durées D_i sont indépendantes et de même loi $\gamma(1, a)$.

On a :

$$P(M \geq t) = \sum_{n=0}^{\infty} P(X \geq D_1 + \ldots D_N \mid N = n) . P(N = n)$$

C'est-à-dire en posant $Y_n = D_1 + D_2 \ldots D_n$

$$P(M \geq t) = \sum_{n=0}^{\infty} P(X \geq Y_n) . P(N = n)$$

Or, X et Y_n sont indépendantes, puisque l'utilisation du système n'affecte pas la fiabilité de ce dernier. On a donc :

$X \sim \gamma(1, \lambda)$

$Y_n \sim \gamma(n, a)$

$$P(X \geq Y_n) = \iint_{x>y} \delta_X(x)\, \delta_Y(y)\, dx\, dy$$

$$= \int_0^{\infty} \left| \frac{a^n}{(n-1)!} e^{-ay} y^{n-1} \int_y^{\infty} \lambda e^{-\lambda x}\, dx \right| dy$$

$$= \frac{a^n}{(n-1)!} \int_0^{\infty} e^{-y(a+\lambda)} y^{n-1}\, dy$$

$$= \frac{a^n}{(n-1)!} \int_0^{\infty} e^{-U} \frac{U^{n-1}}{(a+\lambda)^n}\, dU$$

$$= \left(\frac{a}{a+\lambda}\right)^n$$

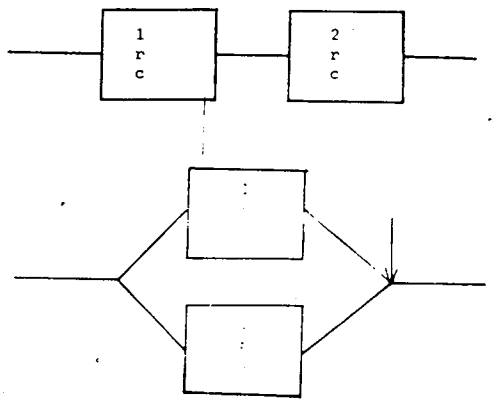
$$\text{D'où } P(M \geq t) = \sum_{n=0}^{\infty} \frac{\left(\frac{a}{a+\lambda}\right)^n e^{-at} (at)^n}{n!}$$

$$= e^{-at\left(1-\frac{a}{a+\lambda}\right)}$$

$$= e^{-\left(\frac{a\lambda}{a+\lambda}\right)t}$$

Ainsi, la fiabilité de la mission est toujours plus grande que la fiabilité du système. Considérons alors notre calculateur, et plus particulièrement un module ou un ensemble de modules constituant un chemin de données, que nous appellerons système. Bien que les fréquences d'utilisation des instructions puissent être bien différentes les unes des autres, ces fréquences sont toujours telles que $a \gg \lambda$ et ainsi on aura toujours $P(M \geq t) \simeq P(X \geq t)$ quels que soient les systèmes considérés. Par suite, la contribution de deux systèmes équivalents en taux de pannes, mais d'utilisation différente, à la fiabilité générale est la même. Mais, si la simulation de ces 2 circuits par une autre partie du calculateur demande le même temps supplémentaire, il peut être intéressant de supprimer le circuit à taux d'utilisation le plus faible et d'implémenter une redondance sur le circuit restant, ce qui, pour un coût total constant, augmente la fiabilité et diminue la puissance.

Schématiquement on aurait donc :



Fiabilité : r^2
Coût : 2c
Puissance : p

Fiabilité : $2r - r^2$
Coût : 2c
Puissance : $p' < p$

Figure 2.

Notre objectif est donc de généraliser cet exemple en considérant toutes les micromachines pouvant simuler une macromachine donnée. Un exemple pratique fera plus aisément comprendre cet objectif. Supposons une macromachine disposant de l'instruction de multiplication flottante. Cette instruction peut être réalisée par le matériel de manière automatique, ou bien être réalisée par microprogrammation. Ces 2 solutions peuvent faire appel à un multiplieur matériel ou non, qui lui-même peut faire appel à un additionneur série ou parallèle. Chacune de ces solutions est caractérisée par la "puissance" conférée à la machine.

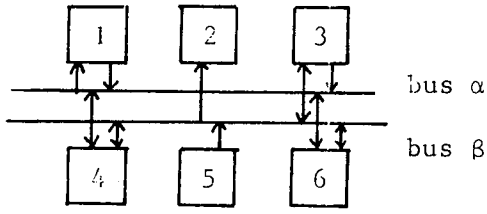
Nous verrons ultérieurement que cette puissance sera mesurée en nombre d'instructions par unité de temps. De la même manière chaque solution est caractérisée par la fiabilité conférée à la machine. Ce paramètre de fiabilité peut être modifié par l'adjonction de redondances. Enfin, le coût de chaque solution sera mesuré par le nombre d'équivalent-portes nécessaires.

De manière un peu plus formelle, on appellera unité fonctionnelle un ensemble de circuits réalisant une fonction pouvant être modélisée indépendemment des autres, l'indépendance étant entendue sous les angles de fiabilité et de puissance conférés à la machine.

Cette unité fonctionnelle réalise une partie de la macromachine. Chaque unité fonctionnelle peut être simulée de différentes manières pour former des parties de différentes micromachines. Enfin, à son tour, une partie de micromachine peut être rendue plus ou moins fiable par redondance.

Nous verrons dans le second paragraphe que nous évaluerons la puissance par le nombre d'instructions exécutées par unité de temps. L'inverse de ce nombre est évidemment égal au temps d'exécution d'une instruction. La référence étant prise égale à ce temps moyen pour la machine la plus puissante, nous calculerons pour chaque micromachine de chaque unité fonctionnelle l'augmentation de ce temps moyen.

Cette étude ne pouvant être faite qu'appliquée à un cas concret, nous avons choisi le géoprocesseur et plus particulièrement une partie de ce calculateur. Notre but n'étant pas ici de présenter le géoprocesseur nous ne décrirons pas en détail la structure de cette machine, qui peut être trouvée dans |29| ou |30|, et nous nous contenterons de spécifier la partie du calculateur utilisée.



1 : registre instruction
2 : registre d'état
3 : mémoire de registres
4 : mémoire centrale
5 : mémoire de contrôle
6 : unité arithmétique et logique

Figure 3.

II - EVALUATION DE LA PUISSANCE DES MICROMACHINES

II - 1. "BENCHMARK", "KERNEL", "INSTRUCTION-MIX"...?

Notre propos ne sera pas ici de lister de manière exhaustive les techniques d'évaluation de performances existantes avec leurs avantages, leurs défauts et leur domaine d'utilisation respectifs. Nous nous bornerons à définir clairement les termes utilisés et à tenter d'établir une hiérarchie d'utilisation afin de justifier notre choix.

Jusque vers 1969, les techniques utilisées sont désignées par l'emploi de "Benchmarks", "Kernels", Instructions-mixes", "timing", sans oublier la simulation et les méthodes de "software/hardware monitoring" (|1|, |2|). Par le terme timing, on entend généralement temps de cycle ou temps d'addition. Il est évident que nombre de critiques peuvent être faites à propos de la crédibilité de telles mesures. On trouvera de telles critiques dans |3| ou |4|, par exemple. Néanmoins, certains auteurs semblent encore accorder un crédit à ces mesures. Un premier pas semble être franchi vers 1963-1964 avec l'apparition "d'instructions-mixes" |5||6|. On affecte alors un poids aux différentes instructions du répertoire, ces instructions étant groupées en catégories.

Cette méthode permet d'évaluer la vitesse de l'unité centrale, sans tanir compte des E/S, ni de la richesse du répertoire d'instructions. Plus récemment, une grande compagnie française a utilisé (entre autre) une méthode semblable en affectant des poids à certaines instructions de haut niveau (COBOL), afin de mesurer les performances obtenues, soit en compilant effectivement ces instructions, soit en les codant directement afin d'optimiser le programme résultant.

Nous appellerons ces "instructions-mixes" des "instructions-mixes" de haut niveau. La lecture des articles les plus significatifs publiés dans le domaine, montre qu'une certaine confusion règne quant à l'emploi des termes "kernel" et "benchmark", si l'on veut outrepasser les inconvénients des "instructions-mixes". Il semble qu'une classification pourrait être de réserver : le terme "kernel" pour désigner un problème bien spécifique tel qu'une inversion de matrice, une évaluation de polynôme etc.., et le terme "benchmark" à un niveau supérieur indiquant une répartition de travaux tels que "compilation FORTRAN", "exécution COBOL" etc.., ou encore une répartition de commandes de haut niveau d'un système de temps partagé telle qu'on peut en trouver dans |12| ou |13|.

Cette classification s'accorde avec l'apparition, à partir de 1969 |14|, des termes "synthetic program" et "synthetic workload" (|14|,... |17|). Un "synthetic program" écrit initialement en PL/1 par Bucholz puis étendu au FORTRAN |18| est un prolongement précis d'un ancien "kernel" consistant en la mise à jour de fichiers, assortie d'un noyau de calcul. Des paramètres concernant le nombre, la taille des fichiers etc.., caractérisent le programme et agissent sur les variables définissant l'activité du système, telles que le temps CPU ou le nombre d'E/S.

Il est alors possible |19| de construire un "synthetic workload" constitué d'un petit nombre de "synthetic programs" et reflétant la charge du système. On peut résumer ce qui précède par le graphique de la figure 4 qui est loin d'être exhaustif quant aux caractéristiques de chacune des mesures qui peuvent être trouvées dans la littérature et qui ne porte pas mention des méthodes de "hardware/firmware monitoring" permettant d'alimenter des simulateurs.

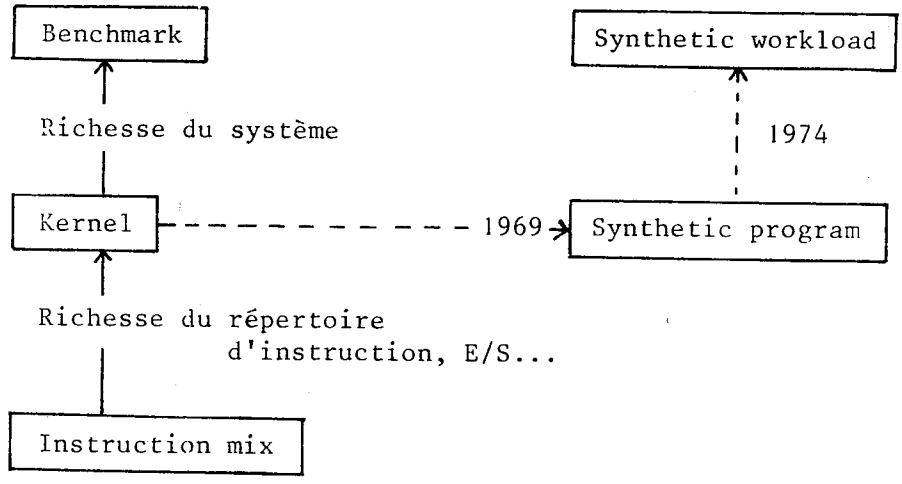


Figure 4.

Notre but étant d'évaluer la performance d'une unité centrale, deux techniques pourraient être employées : choisir un "kernel" ou une "instruction-mix". Dans le cas d'un "kernel" il faudrait se poser le problème de sa représentativité et de toutes manières, puisque nous avons posé comme hypothèse de garder le répertoire d'instructions constant, ce "kernel" ou même cet ensemble de "kernels" se traduirait en fait par une "instruction-mix". Nous nous tournerons vers cette dernière technique.

II - 2. CHOIX D'UN "INSTRUCTION-MIX"

On ne saurait commencer cette section sans citer le mix Gibson |20|, qui est sans doute le plus connu mais sur lequel on a, en fait, peu de renseignements. Ce mix obtenu sur l'IBM 7090 est le suivant :

Chargements-rangements	31.2	49.2
Index	18	
Branchements	16.6	20.4
Comparaisons	3.8	
Arithmétique fixe	6.9	19.1
Arithmétique flottante	12.2	
Décalages-logique	6.0	
Autres	5.3	5.3

Le mix de Gibson a l'avantage d'être complet par rapport à celui cité dans |4|, et qui ne considère pas, par exemple, les opérations sur virgule fixe.

Add-sous flottantes	0.5
Multiplication flottante	5.6
Division flottante	2.0
Chargements-rangements	28.5
Index	22.5
Branchements conditionnels	13.2
Autres	18.7

Un troisième mix de la même génération est donné dans |5| mais est encore plus partiel :

Add-sous fixes	10
Multiplication fixe	6
Division fixe	2
Add-sous flottantes	10
Autres	72

Plus récemment, des résultats obtenus sur le HP2100 ont été publiés |22| et concernent l'exécution d'un "kernel" mathématique, ainsi que différents types de programmes :

	FORTRAN	ASSEMBLEUR	CHARGEUR	SCIENTIFIQUE
Logique	6.6	7.9	9.5	11.4
Branchements	5.5	18.8	17.3	12.9
Chargements-rangements	26.0	14.4	16.2	10.8
E/S	3.5	7.5	5.6	3.1
Décalages	18.5	13.2	19.2	33.4
Saut sous-programme	3.2	6.8	8.8	2.1
Addition	5.0	9.6	7.0	5.8
Comparaison	1.8	3.9	0.4	7.1
ISZ	14.1	3.9	7.2	7.7
Mult-Div	0.	0.	0.	1.9
Autres	5.8	4.0	8.8	3.8

Malheureusement, les auteurs n'expliquent pas le nombre important de décalages et comparent ces résultats à |4| et |5| sans remarquer la nature différente des opérations fixes et flottantes. Néanmoins, la méthode utilisée pour accèder à ces chiffres est intéressante : la trace des instructions est obtenue par modification des microprogrammes. Les résultats les plus intéressants sont, en fait, ceux de Flynn, obtenus à partir de ceux de Winder |24|. Flynn tente d'expliquer les différences notables qui existent entre les résultats de Gibson sur le 7090 et ceux concernant le 360, ces résultats correspondant à un environnement de calcul. Flynn définit 3 types d'instructions :

- M-instructions, telles que LOAD et STORE qui transfèrent des données
- P-instructions, qui déterminent le séquencement des instructions : BRANCH, COMPARE
- F-instructions qui transforment les données; opérations arithmétiques ou logiques.

Les résultats obtenus sont alors :

	COMPILATION Tech	CODE Tech	TECHNIQUE	COMPOSITE
Chargements-rangements entre mémoire et registres	39.7	50.5	45.1	36.1
Branchements	34.2	20.7	27.5	35.8
Comparaisons	14.1	7.8	10.8	12.0
Virgule fixe	5.5	9.7	7.6	6.7
Virgule flottante	0.	6.3	3.2	1.0
Booléen-décalages	5.0	4.0	4.5	2.9
Autres	1.5	1.0	1.3	5.5

Puis il calcule les rapports suivants :

- Rapport M

GIBSON	360
$M = \frac{M\ type}{F\ type} = 1.95$	$\frac{M\ type}{F\ type} = 2.9$
$\frac{M\ type + accumulateur}{F\ type} = 1.24$	$\frac{M\ type + reg.\ Flot.}{F\ type\quad reg.\ Flot.} = 1.4$

- Rapport P

GIBSON	360
$\frac{P\ type}{F\ type} = 0.81$	$\frac{P\ type}{F\ type} = 2.5$

Le rapport M fondé sur l'accumulateur et sur les registres flottants reflète l'activité mémoire réelle par instruction de calcul et ne varie pas sensiblement du 7090 au 360. Mais, la présence de 16 registres généraux dans le 360 au lieu d'un seul accumulateur dans le 7090 n'a pas fait diminuer $\frac{M\ type}{F\ type}$ comme on aurait pû le penser puisque ce rapport a été porté à 160% de ce qu'il était dans le 7090. Parmi les remarques de Flynn tentant d'expliquer ceci, citons l'allocation dynamique de mémoire, l'évolution du FORTRAN lui-même, un usage intensif de la multiprogrammation mieux connue qu'au temps du 7090, la réservation de certains registres à des usages particuliers tels que l'operating system ou l'édition de liens.

Le rapport P montre un accroissement des instructions de séquencement. Flynn avance des explications telles que le branchement à 3 directions par l'instruction COMPARE du 7090, en plus du test, l'évolution des langages de haut niveau qui permettent plus d'options et de test, en particulier pendant la phase de compilation, de nouvelles techniques mettant en jeu, par exemple, les matrices creuses.

Un rapide calcul des rapports P et M montre que ces 2 rapports s'accroissent lorsqu'on passe successivement des environnements "exécution de code scientifique" à "composite" puis à "compilation scientifique", avec une progression plus rapide pour le rapport P. Il serait naturellement intéressant de disposer de chiffres différents pour la compilation et l'exécution dans

un environnement dit "commercial". De la table I, rassemblant les chiffres présentés ci-dessus et quelques autres, on peut, par exemple, remarquer que le système SOCRATE donne un rapport M élevé : 5.5.

Le calculateur que nous allons considérer dans la suite étant plus proche dans sa structure et sa complexité du 7090 que du 360, nous avons conservé un M-rapport égal à celui du 7090, mais nous avons choisi un P-rapport égal à 1.5 au lieu de 0.8 pour le 7090 et 2.5 pour le 360, afin de tenir compte essentiellement de la présence de branchements à 2 directions. Les pourcentagès relatifs des différentes opérations fixes et flottantes sont tirés de |4| et |5|. Compte tenu de ces hypothèses, le mix choisi est le suivant :

Branchements conditionnels		15%
Branchements inconditionnels		8%
Comparaisons		9%
Transferts		16,4%
Indexage		15,2%
Arithmétique fixe	Add Sub	3,5%
	Mult	1,8%
	Div	0,6%
Arithmétique flottante	Add Sub	5,7%
	Mult	3,4%
	Div	1,2%
Logique		5,1%
Contrôle		2,5%
E/S (initialisation)		2,5%

Une question venant immédiatement à l'esprit est l'influence du choix d'un mix sur l'évaluation de la performance de la machine. La grande compagnie française déjà citée, a procédé à l'évaluation de la performance de plusieurs machines à partir de plusieurs méthodes : "mixes", "mixes"de haut niveau et "kernels" (tels que définis auparavant). On peut remarquer quelques variations dans les résultats obtenus. Ceci peut provenir de la diversité des mixes utilisés et du fait que la traduction en langage machine des différents "kernels" et "mixes" de haut niveau ne correspond peut-être pas à la même distribution des instructions que si l'on choisit un "mix". En fait, le "mix" composite semblant être le plus réaliste s'accorde assez bien avec celui de Flynn pour ce qui concerne les instructions de type F, alors que des variations sensibles peuvent être remarquées pour celles de type M et P. Ceci justifie que nous fassions par la suite varier légèrement les coefficients choisis, afin de mesurer les différentes performances obtenues..

	CII [25]			IBM 360 [24]	UNIVAC [26]	IBM 360 [27]	IBM 7090 [20]	IBM 360 [23]				[4]	[5]
	Compilateur LP70 sans moniteur	Compilateur LP70 avec moniteur	Compilateur FORTRAN sans moniteur	Tris Exec. Compil. COBOL FORT.	Composite	Système SOCRATE	Scientifique	Composite	Compilation Scientifique	Code Scientifique	Scientifique · Général	Scientifique	Scientifique
Branch. condit.	32.3	33.3	36.8	35.2	27.1	29.3	16.6	35.8	34.2	20.7	27.5	13.2	
Branch. incond.				20.9 / 13.3	18.1 / 9						16.5 / 9.		
Compar.	14.4	14.9	20.6	8.8	+ skips 29.3	6.9	3.8	12.0	14.1	7.8	10.8		
Charg. Rang.	34.7	28.0	25.5	30.2	10.2 / 25.2	51.7	49.2 (Index : 18.0)	36.1	39.7	50.5	45.1	51.0 (Index : 22.5)	
Virgule fixe Ad/So	10.2	11.1	7.4	4.4		2.8							10.
Virgule fixe Mult.				1.1	0.1	3.3 / 0.0	6.9	6.7	5.5	9.7	7.6		18. / 6.
Virgule fixe Div.					0.07	0.5							2.
Virgule flottante Ad/So												9.5	10.
Virgule flottante Mult.							12.2	1.0	0.	6.3	3.2	17.1 / 5.6	
Virgule flottante Div.												2.0	
Décal. Booléen	3.1	4.0	4.8		2.8	6.1	6.0	2.9	5.0	4.0	4.5		
Total	94.7	91.3	95.1	79.7	94.6	97.3	94.7	94.5	98.5	99.0	98.7	81.3	28.9

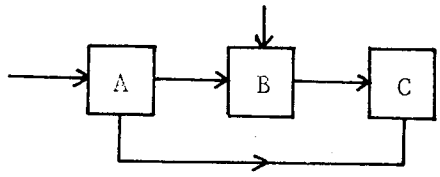
TABLE 1.

III - MODELISATION DES UNITES FONCTIONNELLES

Le but de cette section est de calculer les coûts, fiabilité et performances de toutes les possibilités de micromachines.

III - 1. MODELISATION DE L'UNITE FONCTIONNELLE MEMOIRE DE REGISTRES

Dans le géoprocesseur effectivement construit, cette unité fonctionnelle est composée de 16 registres de 20 bits. Schématiquement, elle se présente ainsi :



A : contrôle
B : registre d'entrée des données
C : registres

Figure 5.

Nous allons, pour notre part, considérer 3 possibilités de micromachines fonctionnelles : l'une avec effectivement 16 registres matériels, une seconde avec uniquement 8 registres matériels, les 8 autres étant simulés par microprogrammation en mémoire centrale et enfin une 3e possibilité dans laquelle il n'y aurait que 4 registres matériels, 12 étant simulés en mémoire centrale.

Les coûts estimés des différentes parties sont en équivalent porte :

B : 140 Quel que soit le nombre de registres de C

A : 90 Quel que soit le nombre de registres de C. En effet, le registre d'adresse de C, qui fait partie de A, n'a qu'une importance minime.

C : 1900 Si 16 registres
1050 Si 8 registres
650 Si 4 registres

Multiplexeurs 20 bits pour redondance standby de degré 1 : 60
" " " " " 2 : 100

Compte tenu de la structure du flot d'informations, les possibilités de redondance sont les suivantes :

1 : simplex
5 : duplication de C
6 : duplication de C et B ensemble →
7 : duplication de A, B et C ensemble
8 : triplication de C
9 : triplication de C et B enselbme
10 : triplication de A, B et C ensemble

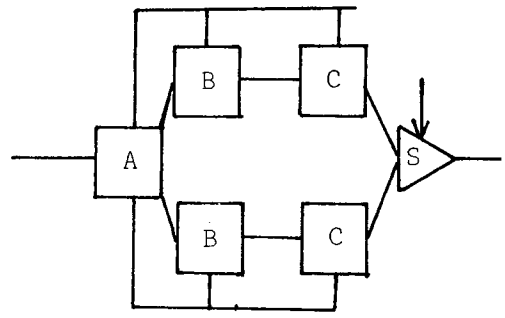


Figure 6.

En effet, B et A sont trop peu importants pour permettre une implémentation propre de redondance (B tout seul ou A tout seul).

Les évaluations de fiabilité qui vont suivre sont faites pour un temps normalisé 10^{-4} par équivalent-porte, ce qui correspondrait à des taux de pannes 16^{-6} pour 1000 heures de fonctionnement d'un boitier de 10 équivalent-porte (les courbes fonction du temps ne seront pas explicitées ici, mais peuvent être trouvées dans |31|, pages 4-34).

Micromachine fonctionnelle n° 1 : 4 registres matériels

	Fiabilité	Coût
1 (simplex)	0.916	890
5	0.968	1590
6	0.980	1730
7	0.987	1820
8	0.967	2280
9	0.981	2560
10	0.989	2740

Micromachine fonctionnelle n° 2 : 8 registres matériels

	Fiabilité	Coût
1(simplex)	0.881	1280
5	0.962	2390
6	0.973	2530
7	0.980	2620
8	0.967	3480
9	0.980	3760
10	0.988	3940

Micromachine fonctionnelle n° 3 : 16 registres matériels

	Fiabilité	Coût
1(simplex)	0.809	2130
5	0.943	4090
6	0.952	4230
7	0.958	4320
8	0.963	6030
9	0.975	6310
10	0.983	6490

On remarque alors immédiatement que les solutions 8 et 9 des micromachines 1 et 2 ne sont pas du tout intéressantes puisqu'il existe d'autres solutions, de coût inférieur et de fiabilité supérieure. C'est ce que nous allons éclaircir par le paragraphe suivant.

Auparavant, il nous faut indiquer la puissance des machines que l'on obteindrait avec ces solutions.

Compte tenu du mix d'instruction que nous avons défini, il est possible de déterminer quels registres fonctionnels il faudrait implémenter en matériel et ceux qu'il faudrait simuler en mémoire centrale si l'on disposait d'une mémoire locale de 4, 8 ou 16 registres. Ceci étant, on peut calculer quelle serait la dégradation de puissance si l'on passait de 16 puis à 8 puis à 4 registres.

- Avec 4 registres, le temps moyen d'exécution d'une instruction serait augmenté de 0.785 µs.
- Avec 8 registres, ce temps moyen serait augmenté de 0.285 µs.

Les évaluations sont faites par rapport au temps moyen de la machine la plus puissante (il n'y aurait pas de dégradation, avec 16 registres). Le temps moyen d'exécution d'une instruction est dans ce cas de 1.089 µs.

III - 1.1. Implémentation de redondances

Nous allons montrer combien il est nécessaire de faire une étude minutieuse de la fiabilité d'un système redondant. En effet, nous allons voir un exemple où un accroissement de coût semblant devoir augmenter la fiabilité diminue en fait cette dernière.

a) Considérons les deux systèmes suivants :

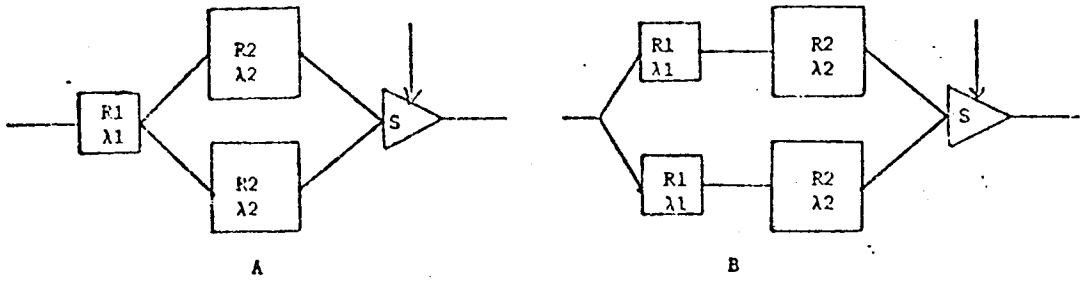


Figure 7.

Ils illustrent 2 systèmes en redondance sélective active de degré 1 où $\lambda_1 < \lambda_2$, soit R1 > R2. S représente un commutateur parfait. Intuitivement, le système B est plus fiable que le système A, ce qui est aisément vérifiable :

$$R_B - R_A = 2R1R2 - R1^2R2^2 - (2R1R2 - R1R2^2)$$
$$= R1R2^2\ (1-R1) > 0$$

b) Une conclusion identique est obtenue pour 2 systèmes en redondance sélective active de degré 3.

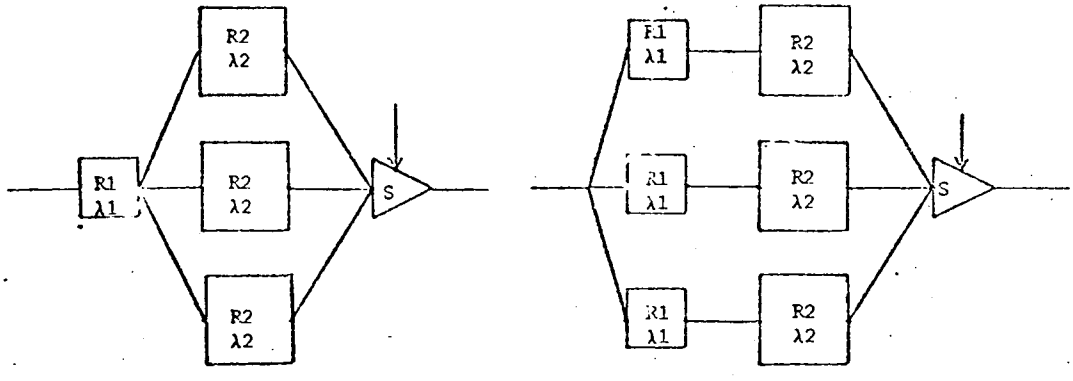


Figure 8.

$$R_B - R_A = R1R2\ (R1^2R2^2 - 3R1R2 + 3 - R2^2 + 3R2 - 3)$$
$$= R1R2^2\ \left|3 - R2 - R1\ (3-R1R2)\right|$$

Cette différence ne peut s'annuler que si :

$$R2 = \frac{3}{R1+1} \geqslant \frac{3}{2}$$

c) Mais considérons maintenant les 2 systèmes suivants : (les notations étant les mêmes que précédemment).

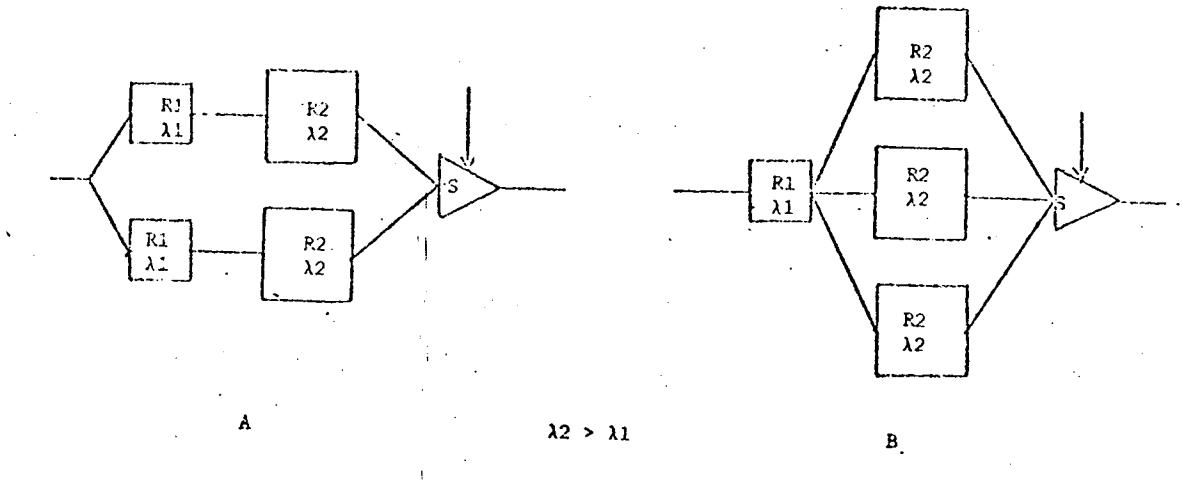


Figure 9.

On ne peut décider à priori de la fiabilité comparée des 2 systèmes.

Intuitivement on pourrait penser que le système B serait plus fiable que le système A. Nous allons voir qu'en fait ce n'est pas toujours le cas et que pour des missions demandant de très hautes fiabilités, le système B sera toujours moins fiable que A, bien que coûtant plus cher.

$$R_B - R_A = R1 \left| R2^3 - 3R2^2 + 3R2 - 2R2 + R1R2^2 \right|$$
$$= R1R2 \left| R2^2 - 3R2 + R1R2 + 1 \right|$$

Cette différence ne peut s'annuler que si :

$$R1 = \frac{-R2^2 + 3R^2 - 1}{R2} = f(R2)$$

L'étude de R1 = f(R2), courbe représentative des points où la différence $R_B - R_A$ est nulle, montre que le plan R1R2 est séparé en 2 régions, l'une où B est plus fiable que A et l'autre où l'inverse se produit. Cette courbe est tracée sur la figure 10.

On ne s'intéresse qu'à la région R1 > R2. La zone indiquée ⊖ est celle où le système B, bien que coûtant plus cher que A est moins fiable. Celle indiquée par ⊕ est celle où B est intéressant. Notons que la courbe R1 = f(R2) est tangeante à R1 = 1 au point (1,1) et que par conséquent, pour des systèmes devant atteindre de très hautes fiabilités, le schéma B ne serait jamais intéressant, c'est-à-dire qu'une redondance de degré 1 serait non seulement moins chère mais aussi meilleure en fiabilité qu'une redondance de degré 2 (dans les conditions biens précises des schémas A et B naturellement).

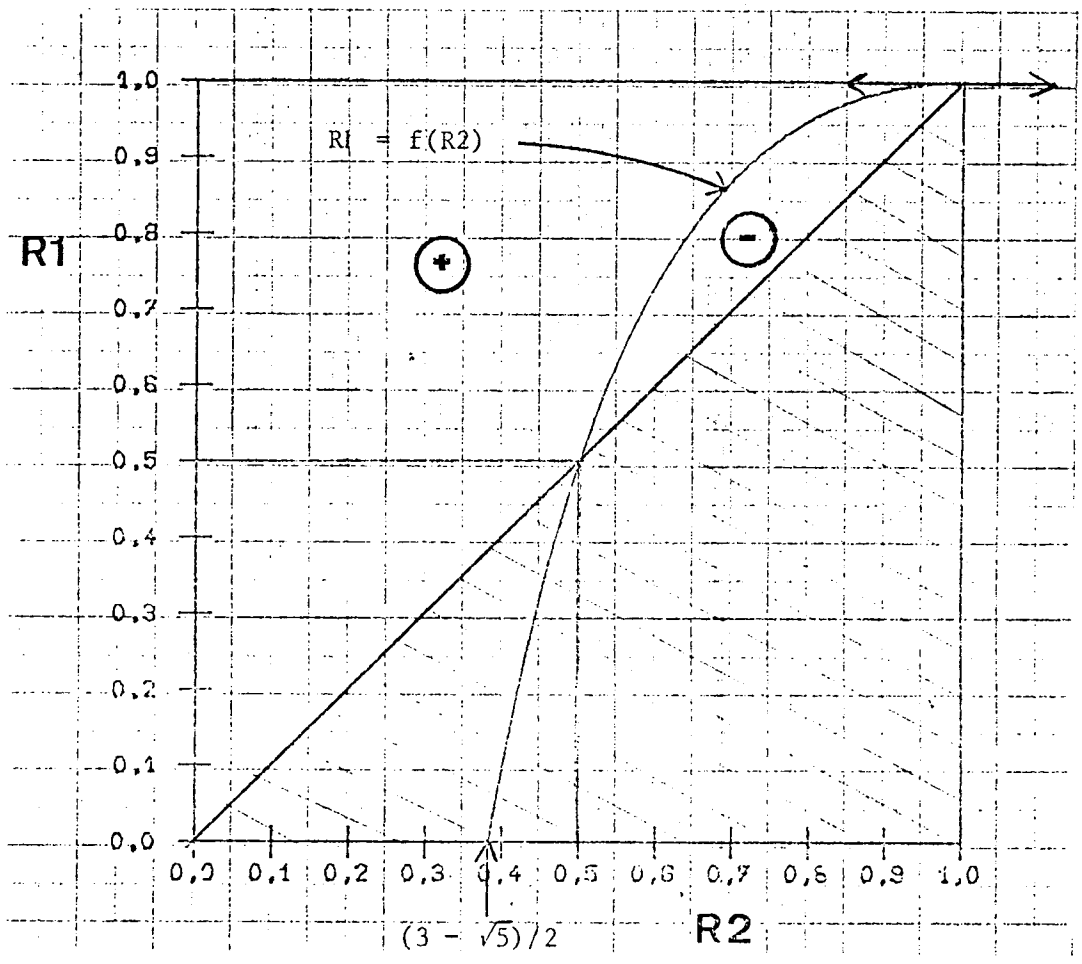


Figure 10.

III - 1.2. Stratégies d'implémentation de redondance

On connaît les résultats disponibles, par exemple dans |32|, |33| ou |34|, sur les variations du coût d'un système en fonction de l'allocation des redondances. Ces résultats montrent la décroissance logarithmique de la défiabilité en fonction du coût du système. Plus clairement, la fiabilité coûte de plus en plus cher à mesure que l'on alloue des redondances. Mais ces résultats mettent en jeu l'allocation de redondance sur un système dont on ne remet pas en cause la partition, et ne prennent pas en compte, par exemple, la stratégie suivante :

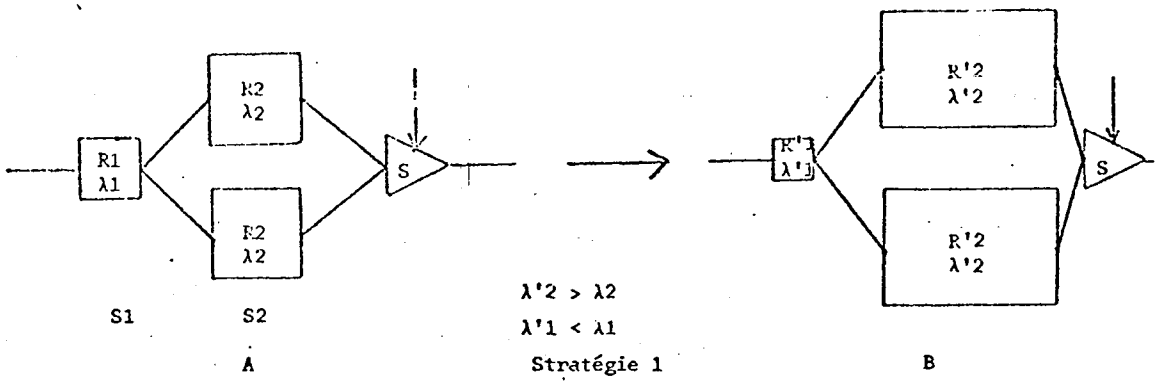


Figure 11.

Passer de A à B revient à faire entrer plus de circuits du mode simplex dans le système duplex. Nous allons comparer les rapports coût-fiabilité de cette stratégie à celle qui consiste à allouer une redondance supplémentaire, c'est-à-dire :

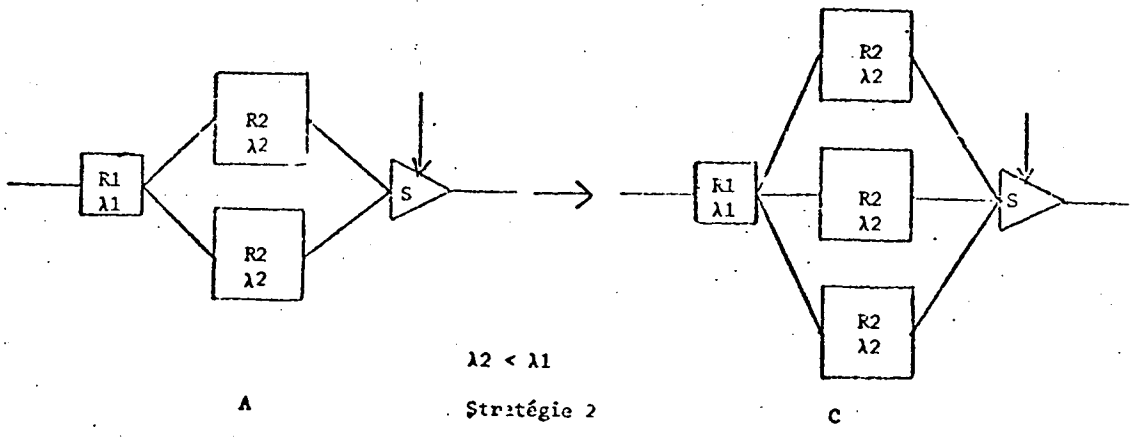


Figure 12.

1) La stratégie 1 est représentée sur un diagramme coût-fiabilité par une courbe exponentielle lorsque la taille relative de R1, R2 varie.

Soient $\lambda 1$ et $\lambda 2$ les taux de panne normalisés de S1 et S2, $\lambda_M = \lambda 1 + \lambda 2$, C = coût du système. $\lambda 2$ varie de 0 à λ_M et $\lambda 1$ varie de λ_M à 0.

On a :

$$R = R1(2R2 - R2)^2 \qquad C = (\lambda 1 + 2\lambda 2)K$$

$$R = R1R2(2 - R2)$$

$$= e^{-\lambda M}(2 - e^{-2\lambda M+\lambda 1})$$

$$= 2e^{-\lambda M} - e^{-2\lambda M+\lambda 1}$$

$$= K' - e^{-C/K}$$

2) Pente de la courbe coût-fiabilité de la stratégie 1 :

$$\frac{dR}{dC} = \frac{1}{K} e^{-C/K}$$

$$= \frac{1}{K} e^{-(\lambda 1+2\lambda 2)}$$

3) Pente de la courbe coût-fiabilité de la stratégie 2 lorsqu'on passe de A à C :

$$R = e^{-\lambda 1} \left|1-(1-e^{-\lambda 2})^n\right| \qquad C = K(\lambda 1+n\lambda 2)$$

$$\frac{dR}{dn} = -e^{-\lambda 1}(1-e^{-\lambda 2}) \operatorname{Log}(1-e^{-\lambda 2}) ; \frac{dC}{dn} = K\lambda 2$$

D'où

$$\frac{dR}{dC} = -\frac{e^{-\lambda 1}}{K\lambda 2}(1-e^{-\lambda 2})^n \operatorname{Log}(1-e^{-\lambda 2})$$

$$= -\frac{e^{-\lambda 1}}{K\lambda 2}(1-e^{-\lambda 2})^n \operatorname{Log}(1-e^{-\lambda 2})$$

4) Rapport des pentes des stratégies 2 et 1

$$q = \frac{\frac{dR}{dC}_2}{\frac{dR}{dC}_1} = -\frac{(1-e^{-\lambda 2})^n \operatorname{Log}(1-e^{-\lambda 2})}{\lambda 2\, e^{-2\lambda 2}}$$

Ce rapport vaut 1 lorsque $\lambda 2 = \operatorname{Log} 2$. Dès que $\lambda 2 < \operatorname{Log} 2$, il décroît en fonction de $\lambda 2$ et tend vers 0 avec $\lambda 2$.

III - 1.3. Illustration sur la mémoire de registres

Revenons aux 3 possibilités de mémoires de registres retenues. Les courbes de coût-fiabilité sont les suivantes :

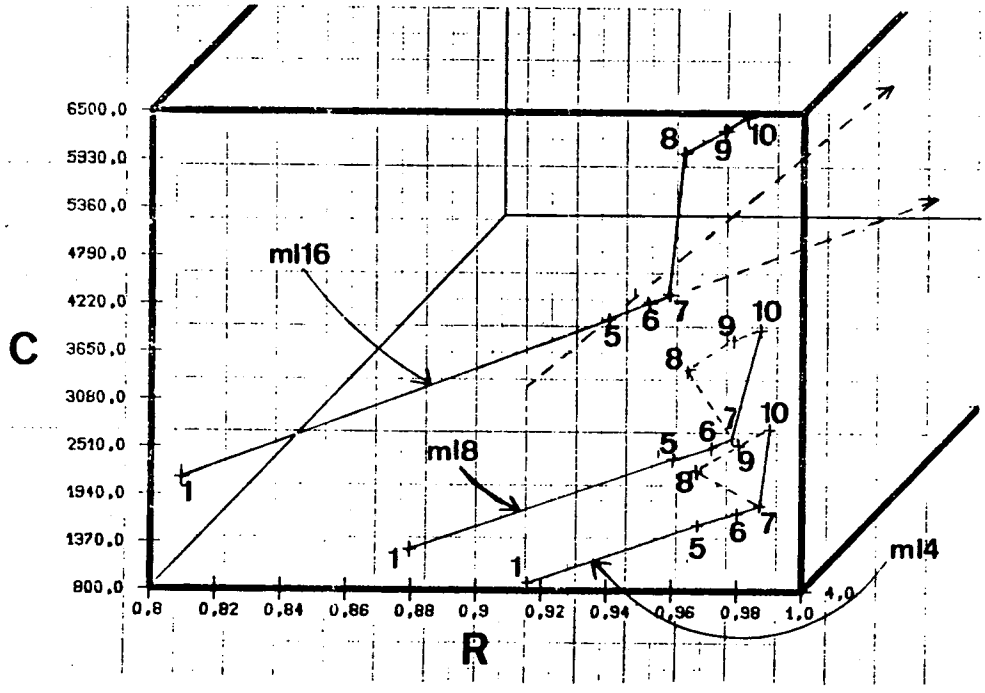
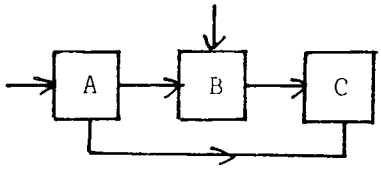


Figure 13.

Rappelons les notations :



A : contrôle

B : registre d'entrée des données

C : registres

→ : indique le cheminement des informations

1 : simplex

5 : duplication de C

6 : duplication de C et B ensemble

7 : duplication de A, B et C ensemble

8 : triplication de C

9 : triplication de C et B ensemble

10 : triplication de A, B, C ensemble

Ml.16 : 16 registres

Ml 8 : 8 registres

Ml. 4 : 4 registres

Les points (1, 5, 6, 7) appartiendraient à une courbe exponentielle (stratégie 1) si l'on excepte la fiabilité des commutateurs.

Les points (1, 5, 8), (1, 6, 9), (1, 7, 10) appartiendraient à une courbe exponentielle (|2|, stratégie 2) sous la même hypothèse.

Les points (1, 8, 9, 10) n'appartiennent pas à une courbe exponentielle (aisément vérifiable).

On remarque alors avec intérêt :

- Les points 8 et 9 des courbes ML4 et ML8. Ils illustrent le phénomène étudié en 1.1 et correspondent à des schémas de redondance tels qu'il existe un autre schéma de redondance de degré inférieur, qui coûte moins cher et qui est plus fiable. Le phénomène est encore accentué par la fiabilité des commutateurs.

- Les pentes des courbes (1, 5, 6, 7), (1, 5, 8), (1, 6, 9), (1, 7, 10), (1, 5, 6, 7) illustrent la stratégie 1. La pente $\frac{dC}{dR}$ est sensiblement égale à 1.5×10^4 aux points 5, 6 et 7, alors que les pentes de (1, 5, 8) ou point 5, (1, 6, 9) ou point 6 et (1, 7, 10) ou point 7, sont environ égales à $\frac{dC}{dR} = 3.6 \times 10^4$.
  Les pentes de (1, 5, 6, 7) et (1, 5, 8) ou point 5 sont tracées sur la courbe ML16.

Le rapport des pentes des stratégies est ici égal à 0,4 environ (on tient compte en effet dans l'application de la fiabilité des commutateurs), c'est-à-dire que la stratégie 1 s'avère être 2,5 fois plus intéressante que la stratégie 2 en ce qui concerne l'amélioration de la fiabilité en fonction du coût. Cette application est choisie de manière à faire varier la fiabilité entre environ 0.8 et 1.0. Mais dans le domaine des très hautes fiabilités, le rapport d'intérêt de la stratégie 1 s'avèrerait encore plus intéressant. Il tend vers l'infini puisque lim q = 0.

III - 2. MODELISATION DE L'UNITE FONCTIONNELLE UAL

III - 2.1. Modélisation des micromachines

Nous allons considérer 3 possibilités de micromachines fonctionnelles.

Micromachine n° 1 : addition entière parallèle
multiplication entière série par automate (additions-décalages : 20 cycles pour 20 bits)
traitement des flottants par microprogrammation

Micromachine n° 2 : addition entière parallèle
multiplication entière accélérée par automate (10 cycles pour 20 bits par un algorithme de Booth)
traitement des flottants par microprogrammation

Micromachine n° 3 : addition entière parallèle
multiplication entière accélérée (idem n° 2)
traitement automatique des flottants par automates.

Etude de la micromachine n° 1

La structure de cette micromachine serait la suivante :

C : Contrôle
H,N,M : Registres - multiplexeurs
ADD : Additionneur
α,β : Bus

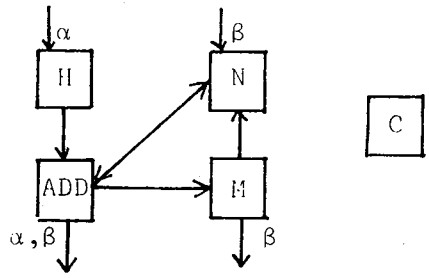


Figure 14.

Compte tenu de la structure des circuits, les possibilités suivantes de redondance peuvent être examinées :

1 : simplex
2 : H doublé
3 : N "
4 : ADD "
5 : M "
6 : H doublé, N doublé
7 : H " , ADD "
8 : H " , M "
9 : N " , ADD "
10 : N " , M "
11 : ADD " , M "
12 : H " , N " , ADD doublé
13 : H " , N " , M "
14 : N " , ADD " , M "
15 : H " , ADD " , M "
16 : H " , ADD " , M " , N doublé
17 : H et ADD doublés ensemble
18 : " " " , M doublé
19 : " " " , N "
20 : " " " , M " , N doublé

21 : H, N, ADD, M doublés ensemble

22 : H, N, ADD, M, contrôle doublés ensemble

23 : H, N, ADD, M, triplés ensemble

24 : H, N, ADD, M, contrôle triplés ensemble

Les coûts des différentes parties peuvent être estimés de la manière suivante :

Contrôle : 100

H : 202

ADD : 384

N : 220

M : 200

Compte tenu de ces coûts, de la fiabilité des multiplexeurs nécessaires et dans les mêmes hypothèses de temps normalisé que pour la fonction mémoire de registres, les fiabilités et coûts de ces diverses solutions seraient :

	Fiabilité	Coûts
1	0.896	1106
2	0.914	1368
3	0.916	1386
4	0.923	1556
5	0.908	1369
6	0.933	1648
7	0.942	1818
8	0.926	1631
9	0.944	1836
10	0.928	1649
11	0.936	1819
12	0.962	2098
13	0.946	1911
14	0.957	1099
15	0.954	2101
16	0.975	1355
17	0.941	1758
18	0.953	1021
19	0.961	2038
20	0.974	2283
21	0.981	2292
22	0.989	2392
23	0.960	3418
24	0.970	3618

On peut remaruqer dès à présent qu'une redondance de degré 3 serait plus nuisible qu'intéressante.

Micromachine n° 2

La structure de cette micromachine serait la même que celle de la précédente avec des coûts :

Contrôle : 161
H : 202
ADD : 384
N : 260
M : 248

Pour les mêmes possibilités de redondance, toujours compte tenu des coût et fiabilité des multiplexeurs, on aurait :

	Fiabilité	Coût
1	0.883	1255
2	0.800	1517
3	0.905	1575
4	0.910	1705
5	0.898	1566
6	0.923	1837
7	0.928	1967
8	0.916	1818
9	0.933	2025
10	0.921	1886
11	0.926	2010
12	0.951	2287
13	0.940	2148
14	0.949	2336
15	0.944	2278
16	0.968	2598
17	0.926	1907
18	0.943	2218
19	0.950	2227
20	0.967	2538
21	0.973	2529
22	0.986	2690
23	0.954	3743
24	0.969	4065

Micromachine n° 3

Pour cette micromachine, la structure serait la suivante :

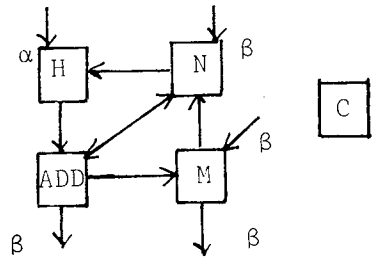


Figure 15.

Avec

Contrôle : 620

H : 417

ADD : 383

N : 425

M : 371

Et on aurait :

	Fiabilité	Coût
1	0.802	2217
2	0.835	2694
3	0.836	2700
4	0.827	2667
5	0.826	2651
6	0.869	3179
7	0.860	3144
8	0.800	3128
9	0.861	3152
10	0.806	3136
11	0.851	3095
12	0.896	3629
13	0.895	3613
14	0.887	3591
15	0.886	3578
16	0.922	4063
17	0.858	3084
18	0.883	3518
19	0.893	3569
20	0.920	4003
21	0.920	3994

22	0.961	4614
23	0.910	5311
24	0.963	6951

Compte tenu du mix d'instruction que nous avons défini et des temps d'exécution des diverses opérations réalisées par les 3 possibilités de micromachines, l'augmentation du temps moyen d'exécution d'une instruction est égale à :

Micromachine n° 1 : 0,154 µs
Micormachine n° 2 : 0.118 µs
Micromachine n° 3 : 0

Rappelons que le temps moyen d'exécution d'une instruction pour la machine la plus puissante est de 1.089 µs.

Les courbes de fiabilité des micromachines 2 et 3, en fonction du temps, peuvent être trouvées dans |31|, pages 41 à 98.

III - 2.2. Relations coût-fiabilité

Considérons, par exemple, la micromachine n° 2 et plus particulièrement les résultats de coût-fiabilité. On peut y relever un certain nombre de possibilités de redondance qui ne sont pas intéressantes, en ce sens qu'il existe d'autres possibilités coûtant moins cher et qui sont plus fiables. Tel est le cas, par exemple, des possibilités 5, 10, 11, 15 etc. Ceci provient de l'influence de la fiabilité des multiplexeurs. En effet, doubler M nécessite un switch à 21 positions, alors que pour H il n'en faut que 20. Ainsi, la solution 5 n'est pas intéressance par rapport à la solution 2. De même, la solution 16 n'est pas intéressante par rapport à la solution 21. Pour la solution 16, la redondance est appliquée à un niveau plus bas (partitionnement) mais il faut un switch de plus, ce qui donne un effet négatif. En fait, il semble difficile d'apprécier si une solution est intéressante ou pas sans effectuer les calculs nécessaires.

Observons alors un graphique coût-fiabilité pour cette micromachine, (Fig. 16).

Les points reliés entre eux représentent des solutions intéressantes, alors que les points isolés représentent des solutions qui ne le sont pas. (Les points correspondant aux solutions 23 et 24 seraient en dehors de l'échelle). Nous trouvons encore, comme lors de l'étude de la fonction mémoire locale, des points disposés sensiblement de manière linéaire. La pente

de cette droite serait approximativement égale à $\frac{dC}{dR} = 1.5\ 10^4$, comme pour la fonction mémoire de registres. Cette pente dépend naturellement du temps de mission normalisé choisi.

Enfin, par exemple, pour la micromachine n° 3, la solution 24 devient intéressante alors qu'elle ne l'est pas pour la micromachine n° 2 et ainsi, après une croissance linéaire de la courbe avec toujours la même pente, on obtient une brusque montée.

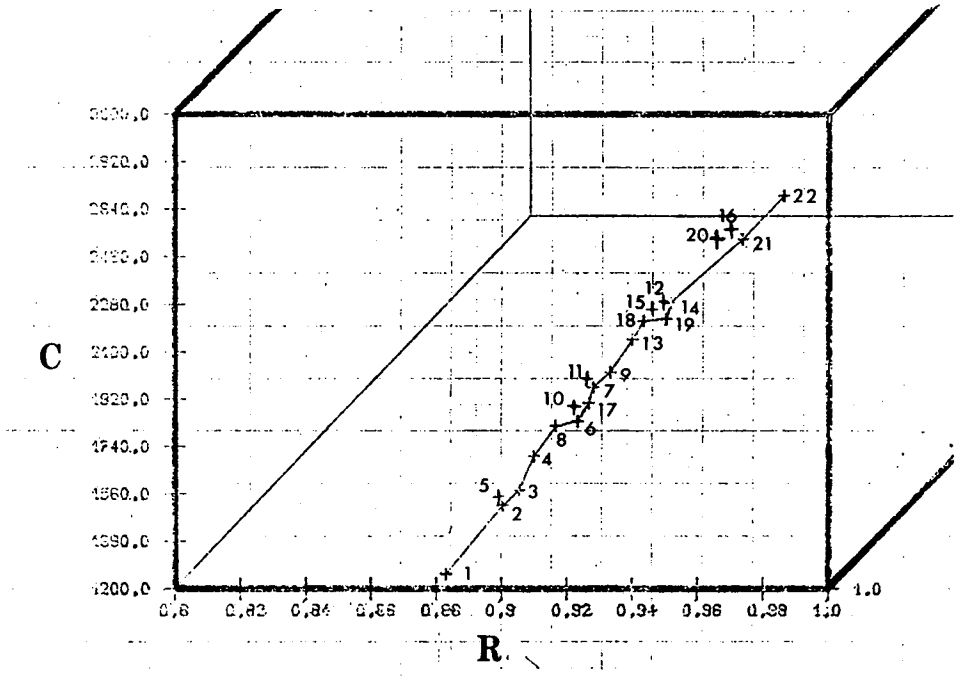


Figure 16.

III - 3. MODELISATION DE LA FONCTION REGISTRE D'ETAT

Fonctionnellement, ce registre se présente comme suit :

et on ne considèrera qu'une seule possibilité de micromachine.

Les coûts estimés sont les suivants :

RE : 165

Multiplexeurs 16 positions pour redondance sélective active de degré 1 : 48

" " " " " 2 : 80

Les possibilités de redondance étudiées sont :

1 : simplex

2 : RE doublé

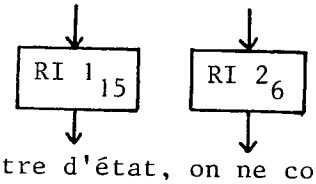
3 : RE triplé

Ce qui donne :

	Fiabilité	Coût
1	0.983	165
2	0.995	278
3	0.992	575

III - 4. MODELISATION DE LA FONCTION REGISTRE D'INSTRUCTION

Fonctionnellement ce registre se compose de 2 parties, l'une de 15 bits l'autre de 6 bits :



et comme pour le registre d'état, on ne considèrera qu'une possibilité de micromachine, les coûts estimés étant :

RI 1 : 182

RI 2 : 63

Multiplexeurs pour RI 1 doublé : 46

" " RI 2 " : 18

" " RI 1 triplé : 75

" " RI 2 " : 30

Les possibilités de redondances étudiées sont :

1 : simplex

2 : RI 2 doublé

3 : RI 1

4 : RI 1 et RI 2 doublés

6 : RI 1 triplé, RI 2 doublé

7 : RI 1 et RI 2 triplé

Ce qui donne :

	Fiabilité	Coût
1	0.975	245
2	0.980	326
3	0.989	472

4	0.993	553
6	0.990	765
7	0.989	840

III - 5. ENSEIGNEMENTS ET FINALITE

Le fait notoire que nous devons souligner ici est le soin avec lequel les calculs de fiabilité doivent être menés si l'on veut éviter un résultat contraire à celui initialement prévu. Il serait illusoire de penser que la solution la meilleure puisse être trouvée à priori sans avoir effectué de nombreux calculs, puisque nous avons été amenés à rejeter à peu près 1/3 de solutions de redondance, qui pourtant, à première vue, ne semblaient pas être aberrantes.

Qu'allons-nous faire des données dont maintenant nous disposons ?

Nous pouvons réaliser chaque unité fonctionnelle de différentes manières, chacune conférant une certaine puissance à la machine. Pour chacune de ces solutions ("morceaux" de micromachine fonctionnelle), il existe différentes possibilités d'accroître la fiabilité (celles que nous venons d'étudier). Il existe donc un très grand nombre de micromachines que l'on pourrait construire.

Mais ces machines ne seraient pas toutes intéressantes, en ce sens qu'une machine est intéressante s'il n'en existe pas d'autre de même puissance et même fiabilité mais de coût inférieur, ou bien de même coût et même puissance mais de fiabilité inférieure, etc...

Un programme d'aide à la conception a donc été développé, qui permet d'éliminer toutes les machines inintéressantes et d'étudier les variations des 3 paramètres coût-fiabilité-performance.

Disons brièvement, en renvoyant à l'annexe 3 pour plus de détails, qu'à partir d'une certaine machine de caractéristiques de coût, fiabilité performance, on cherche à se déplacer dans l'espace R-C-P en maintenant l'un des paramètres constant.

IV - RELATIONS FIABILITE-COUT-PERFORMANCE

Ces relations vont être étudiées par les coupes obtenues lorsque l'un des paramètres est constant.

En ce qui concerne les relations coût-performance nous étudierons tout d'abord les courbes obtenues si l'on ne prend pas en compte le paramètre de fiabilité, c'est-à-dire si l'on considère des machines sans redondance. Ceci nous permettra de comparer les résultats de la présente étude à ceux communément admis dans le domaine, mais dont les paramètres utilisés sont différents. L'influence du paramètre fiabilité sera ensuite étudiée, ainsi que celle du "mix" d'instructions. Enfin, les relations coût-diabilité et fiabilité-performance seront mesurées, ainsi que l'influence sur ces dernières du temps de mission et du "mix" d'instructions retenues.

IV - 1. RELATIONS COUT-PERFORMANCE

La relation communément admise dans ce domaine est : $P = KC^g$.

GROSH, le premier |36|, nota cette relation et estima la valeur de $g = 2$.

ADAMS |37| suggèra $g = 1/2$, mais il mesure la puissance des machines considérées par le temps d'accès en mémoire et la valeur $g = 1/2$ n'est pas probante (ce qui peut provenir du nombre et de la diversité des machines considérées). Les courbes de ADAMS sont reproduites sur la figure 17.

SOLOMON, par contre, a montré dans |38|, pour la série 360, que la loi de GROSH est bien vérifiée pour certains modèles, alors que d'autres seraient sur une courbe de pente un peu moins forte (Fig. 18).

Les modèles 30, 40, 50, 65 et 75 vérifient bien la loi de GROSH, pour une configuration moyenne. Si on considère le coût du processeur seul, une valeur $g = 1$ pourrait être appropriée. Mais toutes ces études considèrent le coût de location des machines. Elles dépendent donc de la politique commerciale du constructeur (ainsi le modèle 350-44 n'est sur aucune courbe).

Observons tout d'abord les relations obtenues sans tenir compte de la fiabilité (on ne considère que des micromachines simplex). On obtient 5 micromachines de puissance différente qu'il serait intéressant de construire. Ces micromachines (courbe A, points 1, 2, 3, 4, 5 Fig. 19 et 20) sont :

1) Unité fonctionnelle

Mémoire de registre : 1ère possibilité de micromachine
Unité fonctionnelle
UAL : 1ère possibilité de micromachine
Unité fonctionnelle
Registre d'état : 1ère possibilité de micromachine
Unité fonctionnelle
Registre d'instruction : 1ère possibilité de micromachine

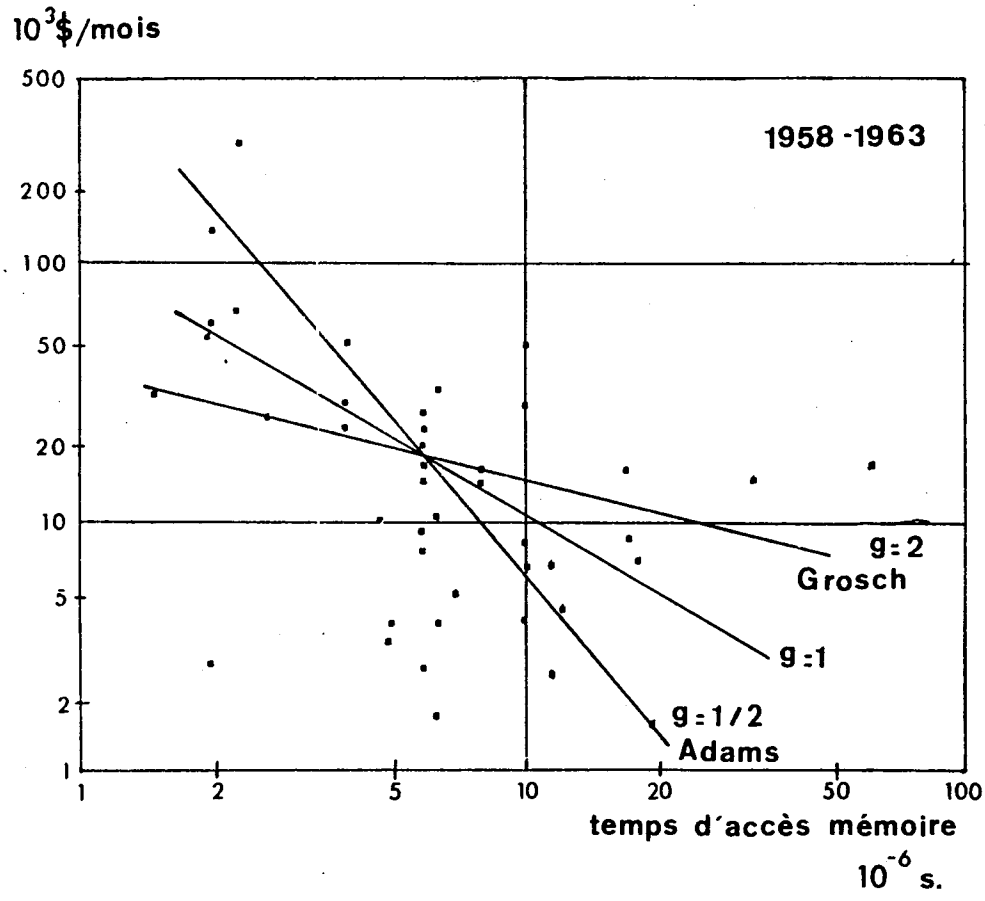


Figure 17.

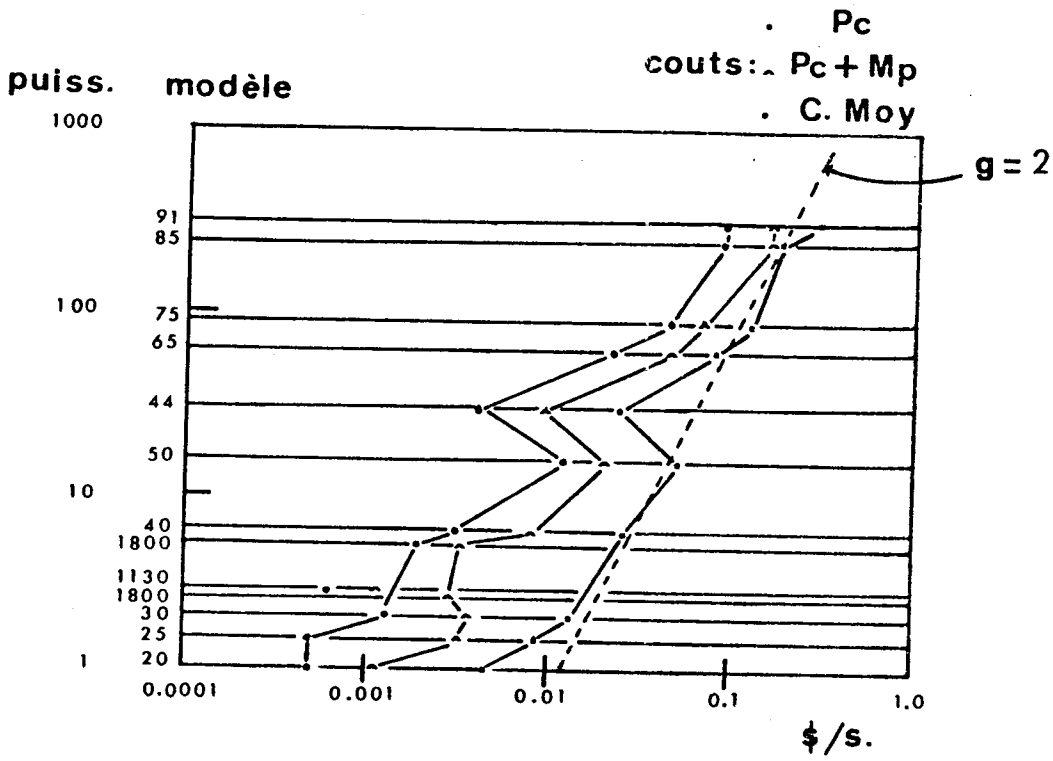


Figure 18.

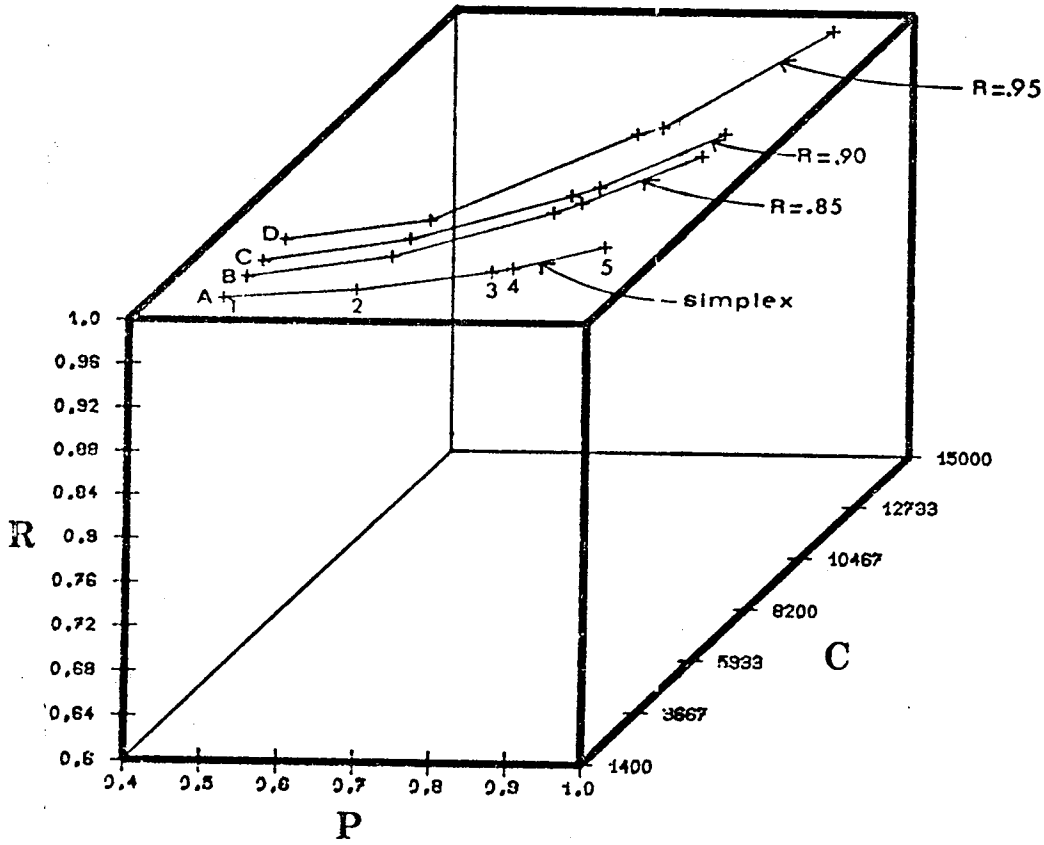


Figure 19. Coût-performance

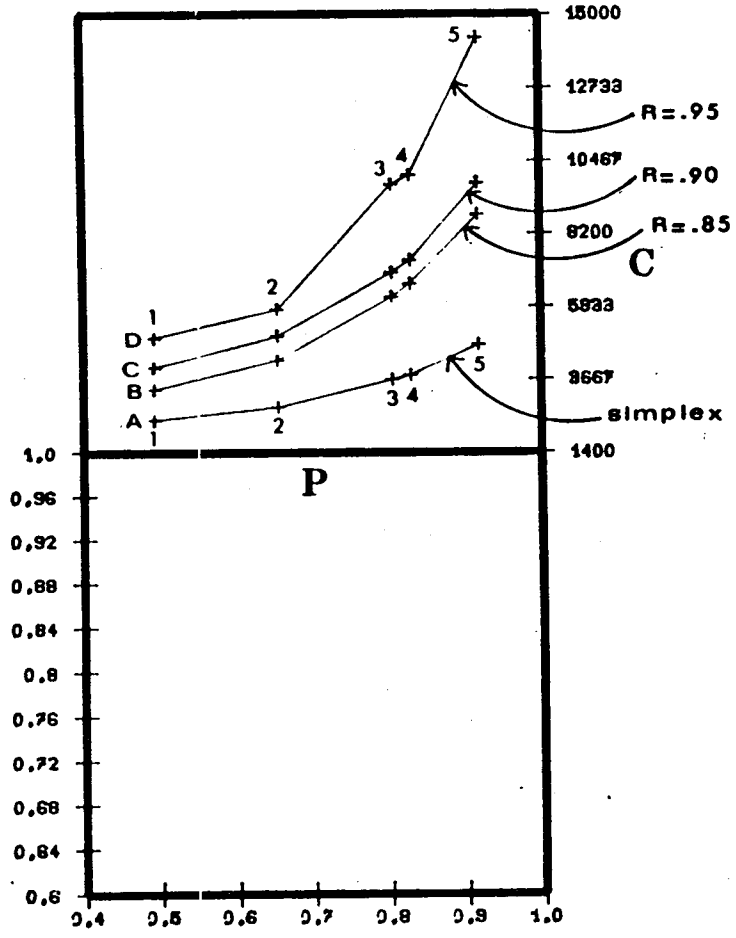


Figure 20. Coût-performance

2) Unité fonctionnelle

Mémoire de registre : 2e possibilité

Unité fonctionnelle

UAL : 1ère possibilité

Unité fonctionnelle

Registre d'état : 1ère possibilité

Unité fonctionnelle

Registre d'instruction : 1ère possibilité

3) Unité fonctionnelle

Mémoire de registre : 3e possibilité

Unité fonctionnelle

UAL : 1ère possibilité

Unité fonctionnelle
Registre d'état : 1ère possibilité

4) Unité fonctionnelle

Mémoire de registre : 3e possibilité
Unité fonctionnelle
UAL : 2e possibilité
Unité fonctionnelle
Registre d'état : 1ère possibilité
Unité fonctionnelle
Registre d'instruction : 1ère possibilité

5) Unité fonctionnelle

Mémoire de registre : 3e possibilité
Unité fonctionnelle
UAL : 3e possibilité
Unité fonctionnelle
Registre d'état : 1ère possibilité
Unité fonctionnelle
Registre d'instruction : 1ère possibilité

La courbe A indique clairement que la puissance coûte de plus en plus cher, si l'on prend en compte le coût des circuits et non le coût commercial d'une machine. Ce fait est évidemment normal. Si l'on admettait une relation du type $P = K\ C^g$ (ce qui n'est pas possible) il faudrait un exposant g inférieur à 1.

Prenons en compte le paramètre de fiabilité, et cherchons à nous déplacer en maintenant la fiabilité constante. Pour des valeurs de fiabilité 0,85 et 0.90 (courbes B et C), on obtient des courbes sensiblement parallèles, alors que la pente $\frac{dC}{dP}$ est plus forte pour une fiabilité 0,95. Ceci provient du fait que pour 0,85 et 0,90, le degré de redondance reste inférieur ou égal à 2, alors que pour atteindre une fiabilité 0,95 il faut des degrés de redondance égaux à 3. (Passer des points 2 à 3 exige une redondance d'ordre 3, et passer des points 4 à 5 en exige une seconde).

Il est bien clair que, sans redondance, la puissance coûte de plus en plus cher, et que si l'on veut maintenir une même fiabilité, cette puissance coûte encore plus cher. Ce coût s'accroît encore lorsque la fiabilité désirée s'élève.

IV - 1.1. Influence du mix d'instruction

Il est naturel de se poser la question de savoir si le mix d'instruction que nous avons choisi a une grande influence sur les résultats ci-dessus. Considérons alors un autre mix tel que les poids relatifs de toutes les instructions de calcul soient doublés au détriment des instructions de chargement-rangement. On obtient alors :

Branchements conditionnels :	15%
" inconditionnels :	8%
Comparaisons	9%
Chargement-rangement	16,1%
Indexation	9,3%
Arithmétique fixe : Add-Sous	7%
: Mult.	3,6%
: Division	1,2%
Arithmétique flottante: ADD-sous	11,4%
: Mult.	6,8%
: Div.	2,4%
Logique	5,1%
Contrôle	2,5%
E/S	2,5%

Remarquons que ce mix est fortement différent du précédent. Compte tenu de ce nouveau mix, les taux d'utilisation de toutes les parties des micromachines sont changés et on obtient :

Temps moyen d'exécution d'une instruction pour la machine la plus puissante : 1,181 µs.

Accroissement de ce temps pour la micromachine n° 1 de l'unité fonctionnelle mémoire de registres : 0,899 µs.

Accroissement de ce temps pour la micromachine n° 2 de l'unité fonctionnelle mémoire de registres : 0,265 µs.

Accroissement de ce temps pour la micromachine n° 1 de l'unité fonctionnelle UAL : 0,301 µs.

Accroissement de ce temps pour la micromachine n° 2 de l'unité fonctionnelle UAL : 0,236 µs.

Il est à noter que selon le mix choisi, il se pourrait que des micromachines fonctionnelles intéressantes dans un cas ne le soient pas dans un autre, et que des implémentations fonctionnelles soient différentes. Dans le cas de l'unité fonctionnelle mémoire de registres par exemple, il se pourrait que les registres à simuler en mémoire pour la micromachine n° 2 diffèrent selon le mix choisi.

En fait, il s'avère que les micromachines intéressantes ne sont plus les mêmes que précédemment. Ces micromachines sont : (Fig.21).

1) Unité fonctionnelle mémoire de registre : 1ère possibilité de micromachine

Unité fonctionnelle UAL : 1ère possibilité
Unité fonctionnelle registre d'état : 1ère possibilité
Unité fonctionnelle registre d'instruction : 1ère possibilité

2) Unité fonctionnelle mémoire de registres : 2e possibilité

Unité fonctionnelle UAL : 1ère possibilité
Unité fonctionnelle registre d'état : 1ère possibilité
Unité fonctionnelle registre d'instruction : 1ère possibilité

3) Unité fonctionnelle mémoire de registre : 2e possibilité

Unité fonctionnelle UAL : 2e possibilité
Unité fonctionnelle registre d'état : 1ère possibilité
Unité fonctionnelle registre d'instruction : 1ère possibilité

4) Unité fonctionnelle mémoire de registres : 3e possibilité

Unité fonctionnelle UAL : 2e possibilité
Unité fonctionnelle registre d'état : 1ère possibilité
Unité fonctionnelle registre d'instruction : 1ère possibilité

5) Unité fonctionnelle mémoire de registres : 3e possibilité

Unité fonctionnelle UAL : 3e possibilité
Unité fonctionnelle registre d'état : 1ère possibilité
Unité fonctionnelle registre d'instruction : 1ère possibilité

Ces changements de micromachines fonctionnelles intéressantes proviennent du poids accordé aux instructions de calcul, doublé par rapport à ce qu'il était précédemment.

Si l'on observe alors les relations de coût-performance obtenues pour des micromachines sans redondance et pour des fiabilités constantes, on peut remarquer que la forme des courbes est sensiblement altérée (Fig.21).

Ces courbes représentent :

A : micromachines sans redondance
micromachines à fiabilité constante

B : R = 0,85
micromachines à fiabilité constante

C : R = 0,90
micromachines à fiabilité constante

D : R = 0,96

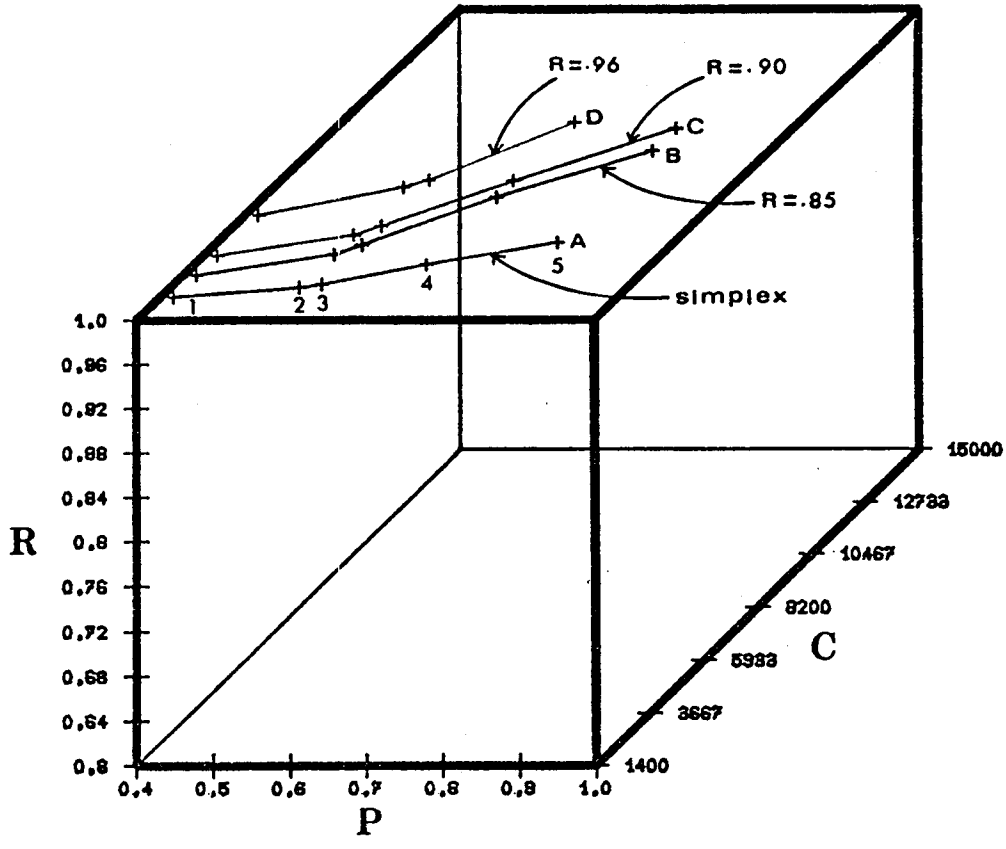


Figure 21. Coût-performance, influence du "mix" d'instructions

En effet, les différentes unités fonctionnelles, de par le poids accordé aux instructions de calcul, ont maintenant une "utilité" semblable à partir d'une certaine puissance. On obtient donc, à partir d'un certain point des courbes coût-performance plus linéaires que les précédentes. Si ces "utilités" étaient rigoureusement identiques, on aurait des pentes $\frac{DC}{DR}$ légèrement décroissantes, ce qui se produit en fait ici.

Il ressort donc de cette étude que les micromachines intéressantes peuvent ne pas être les mêmes selon le mix d'instruction choisi.

L'utilisation future de la machine a donc une grande importance sur sa conception et, de manière générale, selon les évolutions des rapports coût-performance apportés par chaque unité fonctionnelle, les courbes coût-performance seraient une alternance de segments de courbes de type GROSH (puissance de moins en moins chère) et de courbes "contraires" (puissance de plus en plus chère).

IV - 2. RELATIONS COUT-FIABILITE

Nous avons déjà rappelé qu'il était commun de considérer une relation exponentielle entre le coût et la fiabilité d'un système. PIERCE dans |39| montre par exemple que lorsque $C \to \infty$, on a $1 - R \sim n\, e^{-C/\Gamma}$ où n et Γ sont des constantes et lorsque les différents sous-systèmes ont des redondances du type K parmi N (K unités doivent fonctionner pour que le système fonctionne).

Mais, ces résultats ne considèrent pas la fiabilité des commutateurs à mettre en oeuvre, ce qui permet de considérer des degrés de redondance élevés. Or, en pratique, on ne pourra jamais considérer des degrés élevés de redondance. Nous avons vu qu'une redondance de degré 3 est déjà rarement intéressante. Bien que la prise en compte de la fiabilité des commutateurs ne pourrait qu'accroître l'exponentialité citée, nous avons vu à propos de chacune des micromachines des unités fonctionnelles qu'en fait lorsque l'on se limite à un degré de redondance égal à 2, ou si l'on applique la stratégie 1, on obtient des points sensiblement distribués sur une droite. Si le degré de redondance augmente, on a alors une rupture, mais si après cette rupture on réapplique la stratégie 1, qui n'augmente pas le degré de redondance, on retrouve la même pente initiale (v. unité mémoire de registres). Ces phénomènes réapparaissent au niveau des micromachines complètes (Fig.22 et 23).

Les pentes des différents segments sont sensiblement les mêmes que celles des micromachines partielles (en toute rigueur, la pente $\frac{dC}{dR}$ d'une partie linéaire diminuerait lorsque la fiaibliré augmenterait). La rupture de pente au point 1 (courbe A) correspond à un passage à un degré de redondance 3 sur l'unité fonctionnelle mémoire de registre et la rupture de pente au point 2 est due à un second passage à une redondance 3 (unité fonctionnelle UAL).

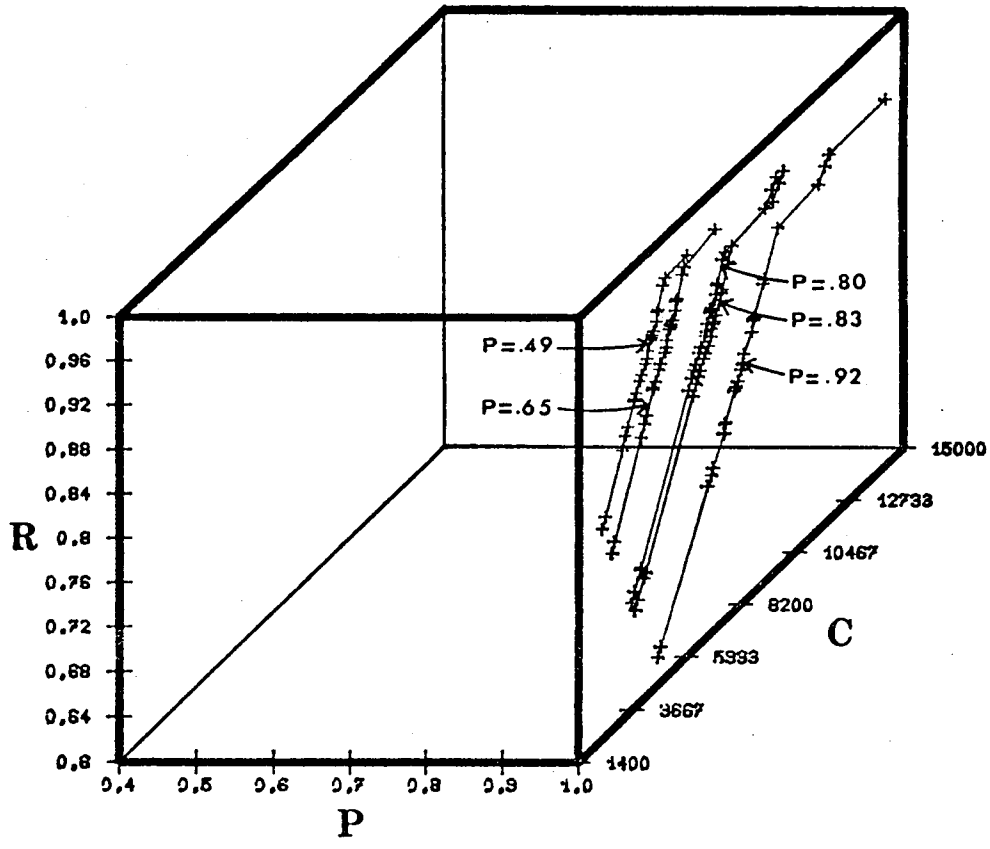


Figure 22. Coût-fiabilité

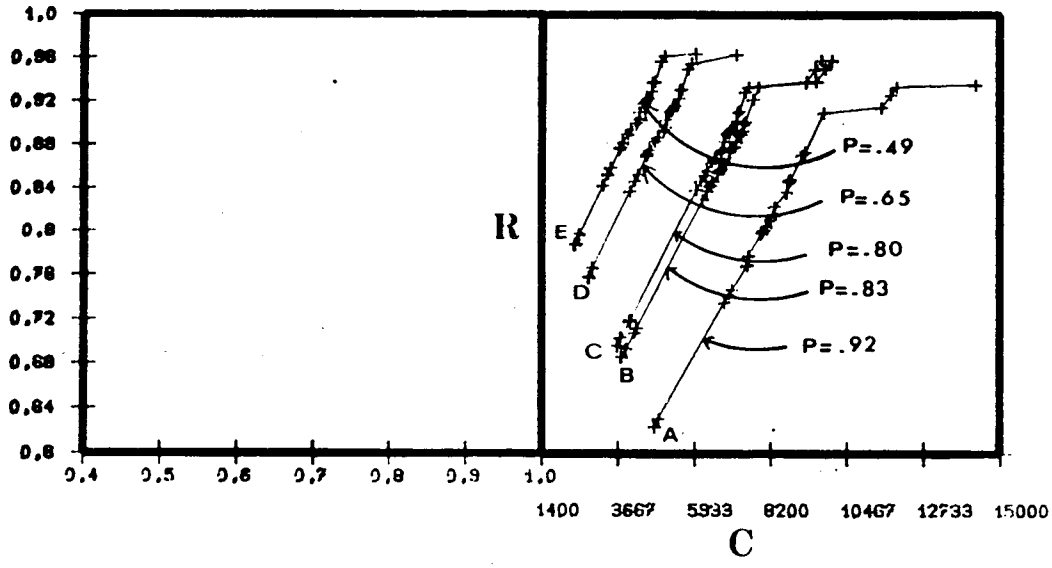


Figure 23. Coût-fiabilité

IV - 2.1. Influence du temps de mission

Toutes les valeurs de fiabilité que nous avons calculé l'ont été pour un certain temps de mission. Que se passe-t-il si l'on considère un autre temps de mission ? On ne se préoccupera pas d'explorer ce qui se passe si le temps de mission est plus long que celui que nous avons choisi. En effet, toutes les valeurs de fiabilité seraient translatées vers des valeurs inférieures, ce qui nous amènerait à des valeurs trop faibles pour être susceptibles d'être intéressantes. (La structure de la machine elle-même serait alors à revoir).

Considérons, par contre, un temps inférieur. Au niveau de chaque unité fonctionnelle, les structures de redondance qu'il serait intéressant de construire pour chaque micromachine ne seraient peut-être pas les mêmes qu'auparavant. Il suffit de considérer, par exemple, le problème soulevé à propos de la mémoire de registres (implémentation de redondance). Dans ce cas, la solution intéressante dépend du rapport R1/R2, donc des taux de panne $\lambda 1$ et $\lambda 2$ pour un même temps, ou bien des temps de mission différents pour un même λ. Il est donc difficile de déterminer à priori les structures intéressantes. Considérons néanmoins pour chaque unité fonctionnelle les micromachines à degré de redondance inférieur ou égal à 2. Pour toutes les structures, les points représentatifs sont à peut près sur une droite, même ceux représentant des structures non intéressantes (v. modélisation UAL).

Pour toutes ces structures, la fiabilité varie linéairement avec le temps (ceci vient du fait que l'on évolue dans un domaine de fiabilité proche de l'unité |5|). Raisonnons alors en termes de défiabilité. Pour chaque structure de micromachine de chaque unité fonctionnelle, on a $f_1 = a_{ijk}\ t_1$ avec :

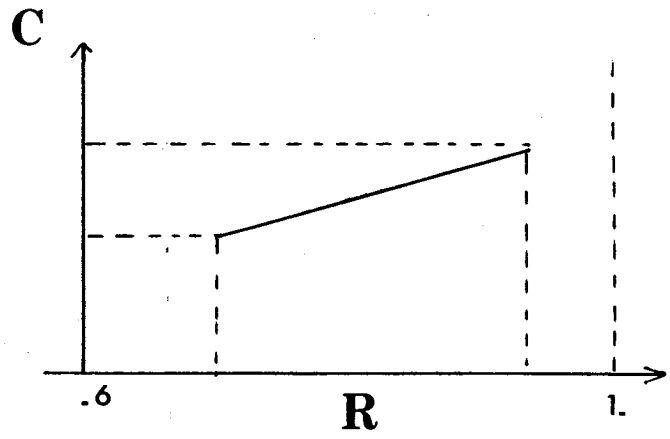
i n° d'unité fonctionnelle

j n° de micromachine fonctionnelle

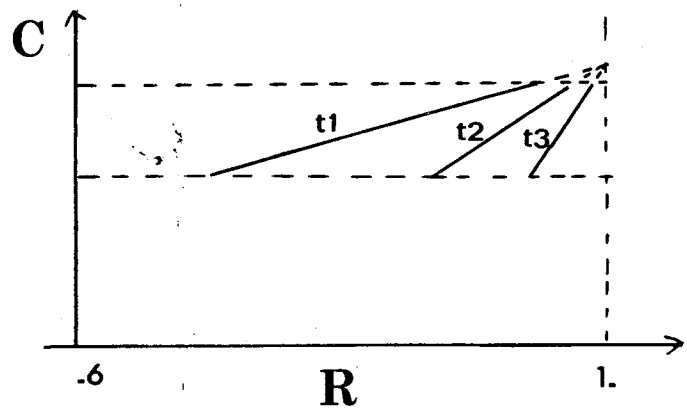
k n° de structure de redondance

Donc, chaque point représentatif au niveau de la machine totale va se déplacer vers un point de même coût, de même performance et de défiabilité $F_2 = \prod_i a_{ijk}\ t_2 = \rho F_1$, avec $\rho = (\frac{t2}{t_1})^c$. Toutes les structures intéressantes seront donc sensiblement alignées sur une droite.

Supposons, par exemple, que l'on ait pour un temps de mission t_1 et une puissance p :



Pour des temps de mission décroissants, on aura :



La pente $\frac{dC}{dR}$ augmente naturellement pour tendre vers l'infini quant $t \to 0$, ce qui correspondrait à des micromachines de fiabilité 1 et des coûts différents, ce qui est normal puisque la redondance devient inutile si le temps de mission tend vers 0.

IV - 3. RELATIONS FIABILITE-PERFORMANCE

Si l'on cherche à se déplacer en maintenant constant le paramètre de coût, on obtient des courbes telles que celles de la figure 24. Les courbes XYZT sont obtenues pour des couts respectifs 4000, 6000, 7100 et 9800. Les points représentatifs de la courbe X sont obtenus pour des micromachines dont le degré de redondanc reste inférieur ou égal à 2. La valeur absolue de la pente $\frac{dR}{dP}$ s'accroît lorsque la puissance augmente. Pour ce coût égal à 4000, la puissance maximale que l'on peut atteindre est 0,82. Observons alors la courbe Y, représentant les micromachines de coût 6000. Le segment 2-3 est parallèle au segment 2-3 correspondant à la courbe X, mais le segment 1-2 présente une courbe de pente $\frac{dR}{dP}$ en valeur absolue, inférieure à celle du segment correspondant de la courbe X. Ceci provient du fait que le point 1 de la courbe Y représente une micromachine ayant une redondance de degré 3, alors que le point 2 représente une micromachine de degré de redondance 2. C'est pourquoi on "perd" moins en fiabilité quand on passe au point 2. Le point 3 correspond lui aussi à un degré de redondance 3, ce qui donne les segments 2-3 parallèles pour les courbes X et Y. Pour ce qui concerne la courbe Z, le point 1 est à redondance 3, mais le point 2 est à redondance 2. La pente du segment 1-2 de la courbe Z est donc différente de la pente des segments 2-3 des courbes X et Y.

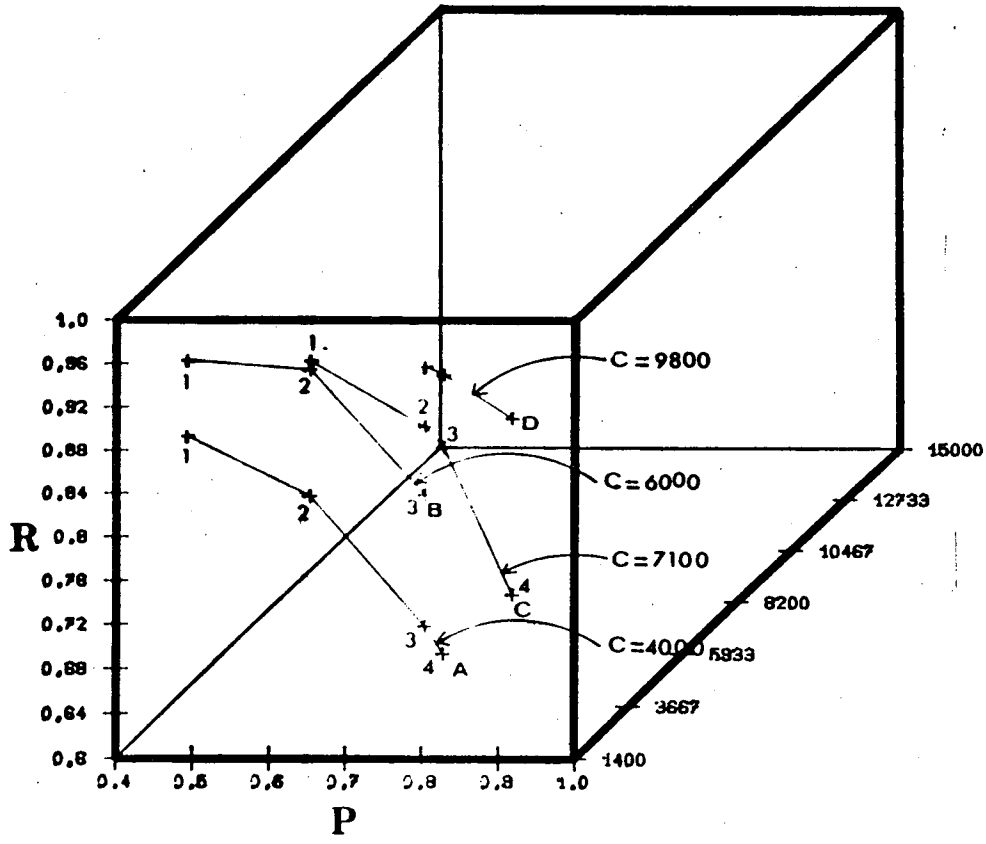
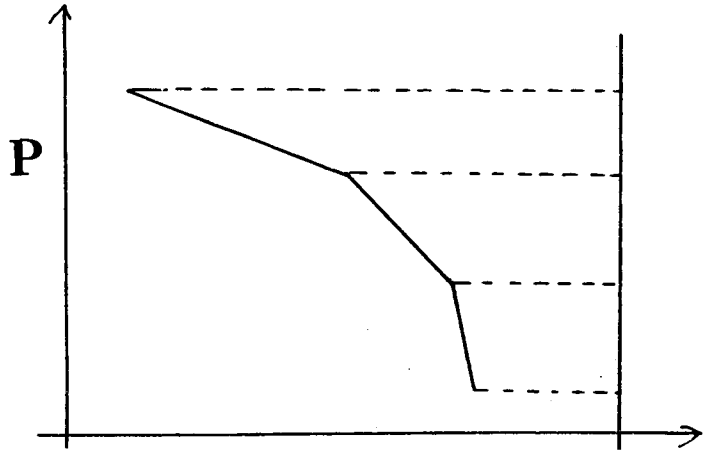


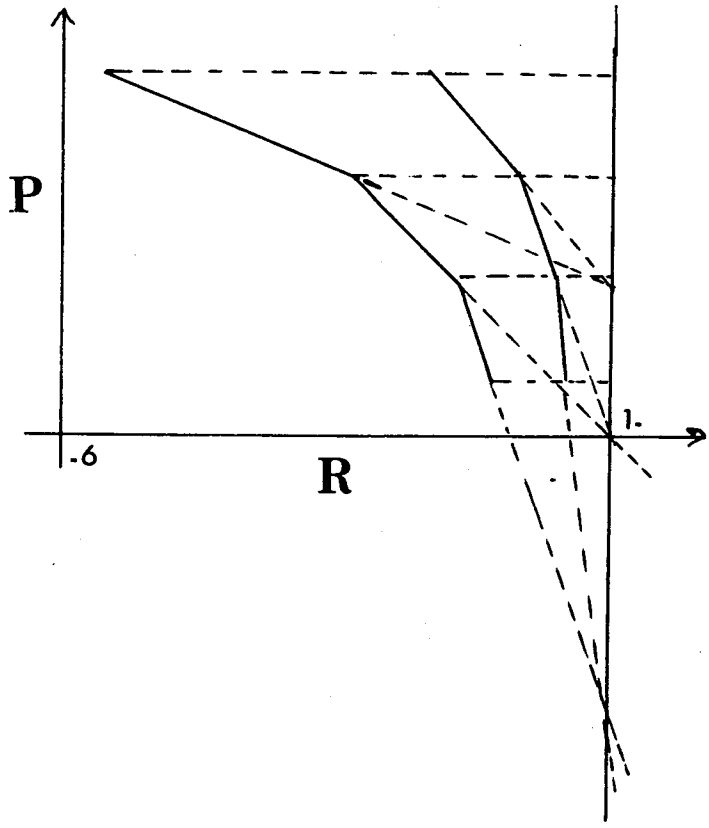
Figure 24. Fiabilité-performance

IV - 3.1. Influence du temps de mission

De même que pous les relations de coût-fiabilité, considérons une diminution du temps de mission. Même s'ils ne correspondent pas exactement aux mêmes structures redondantes, on obteindra par une coupe à coût constant, des points de coordonnées P, C, ρ F. Les courbes vont donc se transformer d'une manière analoque à ce que nous avons déjà vu. Si pour le temps de mission t on a :



On obtiendra pour des temps de mission décroissants :



Quand le temps de mission tend vers 0, la courbe tend naturellement vers R = 1 avec des puissances différentes, ce qui est normal puisque la redondance devient inutile.

IV - 3.2. Influence du mix d'instruction

Si maintenant on fait varier le mix d'instruction de la manière qui a été utilisée pour l'étude coût-performance, on obtient des courbes de formes semblables à celles obtenues pour le mix originel. Ces courbes sont représentées par la figure 25, avec les commentaires suivants :

A : micromachines de coût égal à 4000
B : " " 6000
C : " " 7000

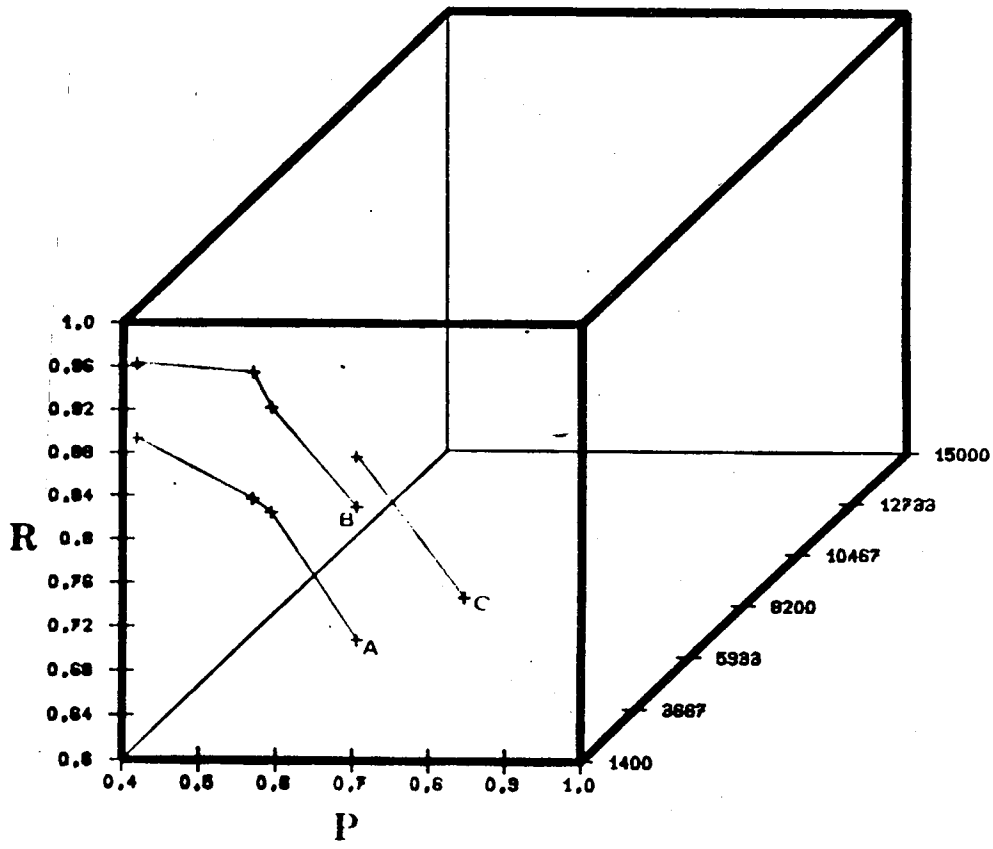


Figure 25. Fiabilité-performance, influence du mix d'instruction

IV - 4. SURFACE FIABILITE-PERFORMANCE

Toutes les micromachines qu'il serait intéressant de construire, pour le temps de mission et le mix originels sont situées sur une surface dont les courbes étudiées jusqu'à présent font partie. Tous les points RCP non situés sur cette surface correspondent à des machines inintéressantes ou bien à des machines ne pouvant exister. Cette surface est représentée sur la figure suivante par les coupes que nous avons vues précédemment. Les micromachines intéressantes sont au nombre de 125, alors que les possibilités que nous avons étudiées lors de la modélisation avaient donné naissance à 31750 micromachines.

Cette importante réduction du nombre de machines est normale si l'on considère que certaines micromachines fonctionnelles non redondantes ne sont pas intéressantes (existence d'une machine de coût moindre, et de puissance supérieure). Le fait d'ajouter des redondances ne pouvant pas, bien naturellement, renverser cette situation, beaucoup de micromachines sont éliminées. Il ne faudrait cependant pas en conclure qu'une certaine partie du travail fait lors de la modélisation des unités fonctionnelles est inutile. Toutes les possibilités étudiées lors de cette étape sont utilisées dans une machine intéressante.

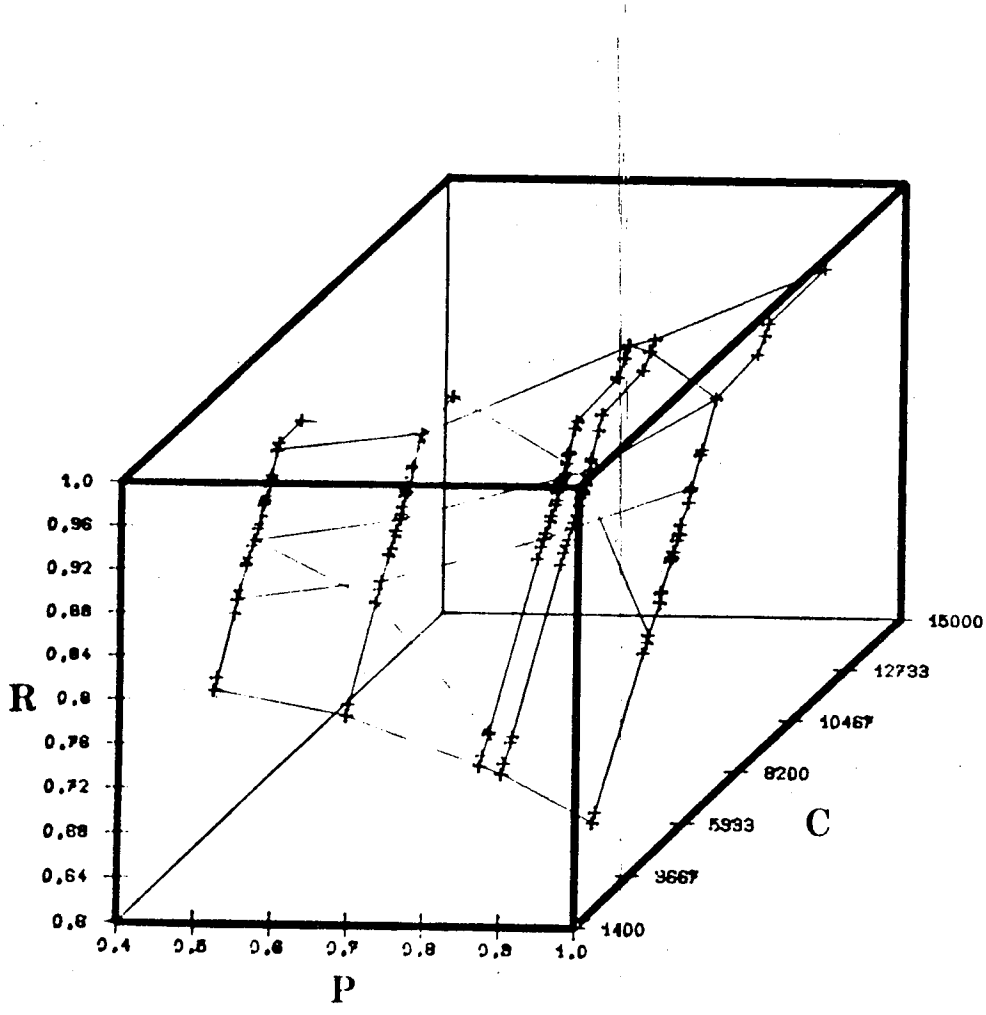


Figure 26. Surface Fiabilité-Coût-Performance

V - CONCLUSION

Que doit-on retenir de cette seconde partie ? Tout d'abord que l'analyse de la fiabilité n'est pas une notion intuitive et que de nombreux calculs doivent être faits si l'on veut apprécier le gain réel de fiabilité.

D'autre part, ce paramètre de fiabilité vient augmenter le coût de la puissance d'une machine : sans considérer de redondances, nous avons pu voir que la puissance coûte de plus en plus cher (au sens naturellement où nous avons défini le coût) et si l'on veut maintenir une certaine fiabilité à la machine, ce coût augmente encore plus.

Un autre point à souligner est l'importance de l'utilisation future de la machine : les machines intéressantes dépendent du "mix" d'instruction choisi.

Enfin, la prise en compte des 3 paramètres a permis de montrer qu'à partir de 30 000 micromachines "constructibles", une centaine seulement présentaient une bonne structure, ce qui montre tout l'intérêt des études que nous avons présentées.

REFERENCES

1) P. CALINGAERT : "System Performance Evaluation : Survey and Appraisal", Comm. of the ACM, janvier 1967.

2) J.M. SMITH : "A Review and Comparison of Certain Methods of Computer Performance Evaluation", the Computer Bulletin, mai 1968.

3) H.C. LUCAS : "Performance Evaluation and Monitoring", Computing Surveys, Sept. 1971.

4) R.A. ARBUCKLE : "Computer Analysis and throughput Evaluation", Computers and Automation, janvier 1966.

5) K.E. KNIGHT : "A Study of Technological Innovation. The Evolution of Digital Computers", Carnegie Institute of Technology, 1963.

6) E. RAICHESON, G. COLLINS : "A Method for Comparing the Internal Operating Speeds of Computers", Comm. of the ACM, mai 1964.

7) J.R. HILLEGASS : "Standardized Benchmarks Problems Measure Computer Performance", Computers and Automation, janvier 1966.

8) E.O. JOSLIN, JJ. AIKEN : "The Validity of Basing Selections on Benchmark Results" Computers and Automation, janvier 1966.

9) H. HELLERMAN, T.F. CONROY : "Computer system performance", Mc Graw Hill, 1975.

10) E.O. JOSLIN : "Computer Selection", Addison-Wesley Publishing Company, 1968.

11) S.H. FULLER : "Price/performance Comparison of C.mmp and the PDP-10", 3rd Annual Symp. on Computer Architecture, Tampa (Florida) 19-21 janvier 1976.

12) A.L. SCHERR : "An Analysis of Time-shared Computer System", Projet MAC 1965.

13) J. LEROUDIER : "Analyse d'un Système à Partage de Ressources", journées ACM/IRIA, Mesures et Evaluations des Systèmes Informatiques, oct. 1974.

14) W. BUCHOLZ : "A Synthetic Job for Measuring System Performance", IBM Systems Journal, 8-4-1969.

15) F.J. BUCKLEY : "Estimating the Timing of Workload on ADP Systems : An Evaluation of Methods Used", Computers and Automation février 1969.

16) D.C. WOOD, E.H. FORMAN : "Throughput Measurement Using a Synthetic Job Steam", Fall Joint Computer Conference, 1971.

17) D. FERRARI : "Workload Characterization and Selection in Computer Performance Measurement", Computer, juillet-Août 1972.

18) "FORTRAN version of Bucholz's Synthetic Program", Proc. 3rd Meeting of the Computer Performance Evaluation Users Committee, juillet 1971.

19) K. SREENIVASAN, A.J. KEIMAN : "On the Construction of a Representative Synthetic Workload", Comm. of the ACM, mars 1974.

20) J.C. GIBSON : "The Gibson Mix", TR.00.2043, IBM Systems Development Division Poughkeepsie, N.Y. (cité dans |21|).

21) C. BELL, A. NEWELL : "Computers Structures : Readings and Examples", Mc Graw Hill Book Compagny, 1971.

22) K.S. SANFORD, LL. WEAR : "Dynamic Instruction Set Evaluation", SIGMICRO, Palo-Alto, septembre 1974.

23) M.J. FLYNN : "Trends and Problems in Computer Organizations", Information Processing, august 1974.

24) R.O. WINDER : "A Data Base for Computer Performance Evaluation", Computer, mars 1973.

25) TASSO : "Hiérarchisation et Reconfiguration Transparentes des Ressources Basées sur la Structure des Programmes et des Données", Thèse Sc. Maths, Paris 1970.

26) D.T. BRODSEN : "Univac 1108 Hardware Instrumentation System", ACM-SIGOPS Workshop on System Performance Evaluation, Harward Univ. avril 1971.

27) G. MAZARE : "Note sur l'Utilisation des Instructions du Code 360 par SOCRATE", Grenoble.

28) B. COURTOIS, G. SAUCIER : "Performance, Cost, Reliability of Different Micromachines for a Given Macromachine", CEE Advanced Course on Computer Systems Architecture, Serre Chevalier (France) décembre 1974.

29) F. ANCEAU, DROUET, BEAUDUCEL, COURBOULAY, CRETIN : "Géoprocessor, Computer for Geophysical Research", IFIP 1974.

30) F. ANCEAU : "Contribution à l'Etude des Systèmes Hiérarchisés de Ressources dans l'Architecture des Machines Informatiques", Thèse d'Etat, Grenoble 1974.

31) B. COURTOIS : "Annexe Technique au Rapport de Contrat DRME 75/169".

32) W.H. PIERCE : "Failure-Tolerant Computer Design", Academic Press 1965.

33) G.H. SANDLER : "System Reliability engineering", Prentice-Hall Space Technology Series, 1963.

34) BARLOW, PROSCHAN : "Mathematical Theory of Reliability", John Wiley and Sons Inc. 1965.

35) B. COURTOIS, G. SAUCIER : "On Balancing Hardware-Firmware for Designing a Fault-Tolerant Computer's Series", 8th Annual Workshop on Microprogramming, Chicago, septembre 1975.

36) H.R.J. GROSCH : "High Speed Arithmetic. The Digital Computer as a Research Tool", J. of Optical Society of America, APR 1953.

37) C.W. ADAMS : "Grosch's Law Repealed". Datamation. Jul. 1962.

38) SOLOMON : "Economies of Scale and the IBM System 360", Comm. ACM vol.9 n° 6, juin 1968.

39) W.H. PIERCE : "Failure-Tolerant Computer Design", Academic Press 1965.

40) B. COURTOIS, G. SAUCIER : "Microprogramming as a Means of Evaluation of a Computer's Performance and Reliability", EUROMICRO, Nice, juin 1975.

41) B. COURTOIS : "Designing a Fault-Tolerant Computer : its Security, Reliability, Performance and Cost", Organisation Logique des Calculateurs et leur Microprogrammation. Accords CNRS-Académie des Sciences de Pologne, Varsovie, octobre 1975.

ANNEXE 3

PROGRAMME POUR L'ETUDE DES RELATIONS FIABILITE-COUT-PUISSANCE

A3 - 1. DONNEES FOURNIES PAR L'UTILISATEUR

A3 - 2. ENVIRONNEMENT "ETUDE"

A3 - 4. ENVIRONNEMENT "INITIAL"

A3 - 4. EXEMPLE

AVERTISSEMENTS

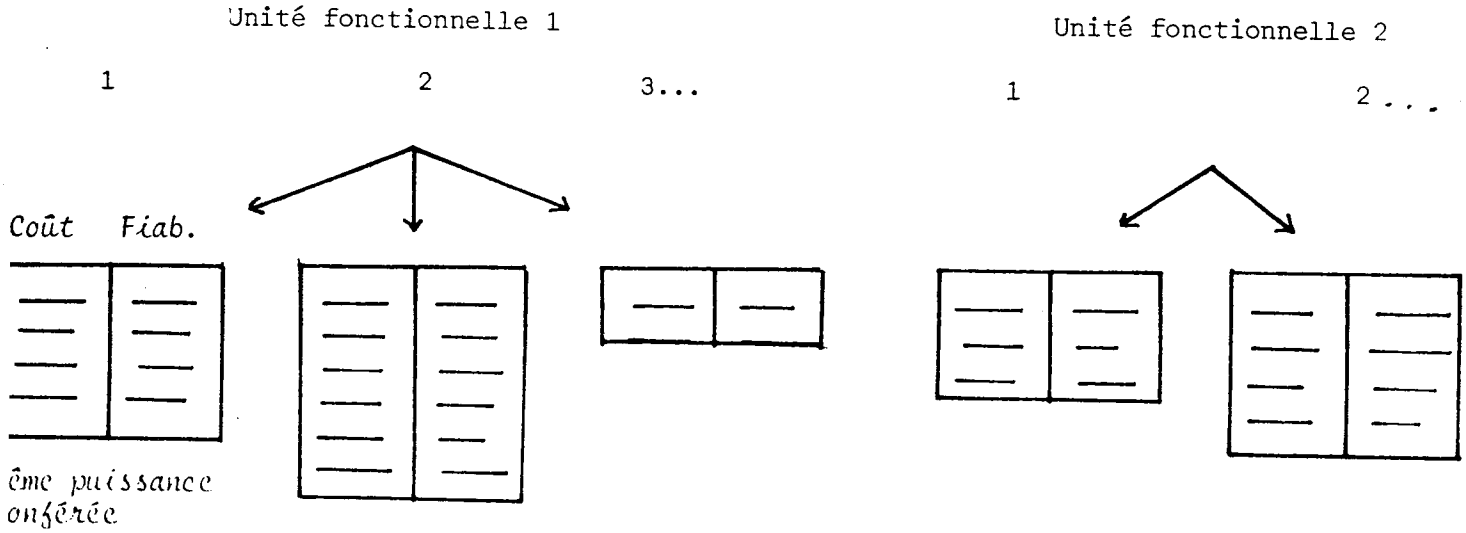
Dans toute cette section, on emploiera le terme *fiabilité* au sens de *fiabilité de mission* tel que défini dans la 1ère partie.

On ne décrira le programme *que vu par l'utilisateur*, sans entrer dans aucun détail interne.

A3 - 1. DONNEES FOURNIES PAR L'UTILISATEUR

Conformément à ce que nous avons déjà écrit plus haut, on appelle unité fonctionnelle un ensemble de circuits réalisant une fonction pouvant être modélisée indépendamment des autres, l'indépendance étant entendue sous les angles de fiabilité et de puissance conférée à la machine. Cette unité fonctionnelle réalise une partie de la macromachine. A titre d'exemple, la partie calcul de la macromachine est une unité fonctionnelle. Chaque unité fonctionnelle peut être réalisée de différentes manières pour former des parties de différentes micromachines. A titre d'exemple, la partie calcul peut être réalisée avec un multiplieur entier ou non, avec une propagation rapide des retenues ou non, etc.. A son tour, une partie de micromachine peut être implémentée avec différentes redondances, ce qui donne des micromachines de même caractéristiques de puissance mais avec des paramètres de coût et de fiabilité différents. Toutes les fiabilités sont supposées être calculées pour un même temps de mission. Si l'on considère toutes les combinaisons possibles, en prenant une micromachine pour chaque unité fonctionnelle, on obtient toutes les micromachines possibles dans l'espace (fiabilité, coût, puissance).

Schématiquement, on a donc :



$\bigcup_j$ de (*unité fonctionnelle j*) = *macromachine*

$\bigcup_i$ de (*solution k de la ie possibilité pour l'unité fonctionnelle j*) = *micromachine*

Chaque solution i de chaque unité fonctionnelle est caractérisée par la puissance conférée à la machine si on choisit cette solution. Cette puissance est mesurée en nombre d'instructions par seconde, donc par l'inverse du temps moyen d'exécution d'une instruction. Le paramètre de puissance caractérisant la solution i de chaque unité fonctionnelle est l'accroissement apporté à ce temps moyen d'exécution, par rapport à un temps de base qui est celui de la machine la plus puissante que l'on puisse construire.

Chaque micromachine simulant la macromachine donnée est donc caractérisée par :

$$\text{Coût} = \sum_j \text{Coût de la solution k de la solution i de l'unité fonctionnelle j}$$

$$\text{Fiabilité} = \prod_j \text{Fiabilité de la solution k de la solution i de l'unité fonctionnelle j}$$

$$\text{Temps moyen d'exécution d'une instruction} = \text{Temps de base} + \sum_j \text{Accroissement de temps de la solution i de l'unité fonctionnelle j}$$

A3 - 2. COMMANDES POUVANT ETRE EMISES PAR L'UTILISATEUR DANS L'ENVIRONNEMENT "ETUDE"

Dans l'environnement ETUDE, un certain nombre de commandes sont disponibles pour l'utilisateur, afin d'étudier les différentes machines possibles, ou de changer d'environnement.

Toutes les commandes relatives à l'étude des machines peuvent être suivies d'un astérisque. Dans ce cas, la commande est itérée jusqu'à épuisement des possibilités. Chaque commande possède également une forme abrégée. L'utilisateur peut émettre plusieurs commandes en même temps. Dans ce cas, elles doivent être séparées par au moins un caractère "blanc".

La table I résume les commandes disponibles.

Environnement ETUDE

MAINIT I	Machine initiale
CCONPC CPC |*|	Coût constant puissance croissante
CCONPD CPD |*|	Coût constant puissance décroissante
RCONPC RCP |*|	Fiabilité constante- puissance croissante
RCONPD RPD |*|	Fiabilité constante puissance décroissante
PCONRC PRC |*|	Puissance constante fiabilité croissante
PCONRD PRD |*|	Puissance constante fiabilité décroissante
SIMPC SPC |*|	Simplex-puissance croissante
SIMPD SPD |*|	Simplex-puissance décroissante
BR	Changement de dessin
MC	Machine courante
END (CR)	Sortie du programme
INIT	Environnement INITIAL

TABLE I

A titre d'exemple, la commande CCONPC (coût constant, puissance croissante) a l'effet suivant :

A partir de la machine courante, on cherche à augmenter la puissance au détriment de la fiabilité, le coût de la machine restant constant. En toute rigueur, on ne peut trouver des machines ayant un coût identique, sauf coïncidence. On s'intéresse donc aux machines dont le coût s'approche du coût courant d'une différence telle que la valeur relative de cette différence

soit inférieure à un certain paramètre. La valeur de ce paramètre peut être changée dans l'environnement INITIAL. S'il n'existe pas de machine répondant à ce critère, ce fait est signalé à l'utilisateur. Si on ne peut pas augmenter la puissance, il n'y a pas de machine pouvant répondre à la commande, et la-dite commande devient sans effet sur la machine courante qui reste la même (signalé à l'utilisateur). Si au contraire, la commande peut être exécutée, la machine courante est changée. Si la commande est suivie d'un astérisque, elle est itérée jusqu'à l'impossibilité. A chaque changement de machine courante, la structure de la machine est indiquée, ainsi que la valeur des 3 paramètres, fiabilité, coût, puissance.

A3 - 3. COMMANDES POUVANT ÊTRE EMISES PAR L'UTILISATEUR DANS L'ENVIRONNEMENT INITIAL

Les commandes accessibles dans cet environnement servent à déterminer les valeurs de certains paramètres, valeurs qui seront utilisées tout au long d'une étude (environnement étude).

Les commandes sont résumées dans la table II.

	Environnement INITIAL
PLOT	Appel au traceur de courbes
NECR	Pas de résultats sur console
ECR	Résultats console
CHMT	Changements de valeurs de certains paramètres
CR	Environnement ETUDE

TABLE II

L'organisation générale est donc celle de la table III.

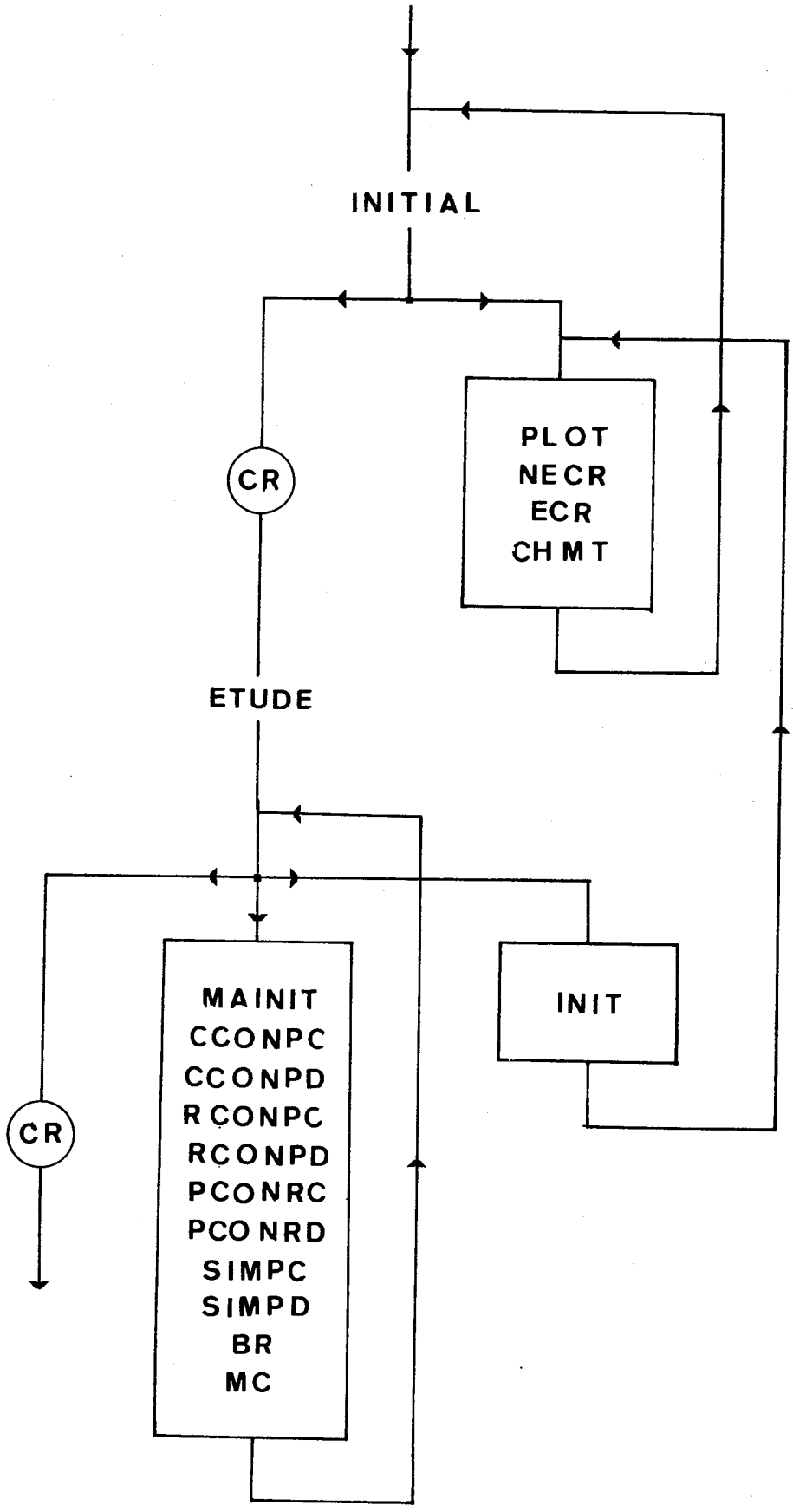


TABLE III

A3 - 4. EXEMPLE

Considérons une macromachine que l'on a décomposée en 2 unités fonctionnelles U1 et U2. U1 peut être simulée de 2 manières différentes : si l'on adopte la première, l'augmentation du temps moyen d'exécution d'une instruction est égale à 3, alors que si l'on adopte la seconde, cette augmentation est nulle. On peut supposer, par exemple, pour fixer les idées, que cette unité fonctionnelle correspond à N registres généraux de la macromachine. Le programmeur a donc toujours N registres à sa disposition. Mais ces registres peuvent être physiquement présents ou non dans la micromachine. La première solution de U1 pourrait correspondre à N/2 registres physiques, les autres étant simulés, alors que la seconde solution correspondrait à N registres physiques.

Supposons alors que, si l'on adopte la première solution pour U1, le coût et la fiabilité de cette partie de micromachine soient respectivement 2 et 0,8. Mais, si l'on implémente une certaine redondance, ce coût et cette fiabilité passent à 3 et 0,9. De la même manière, si l'on adopte la seconde solution, rendant la machine plus puissante, on a deux possibilités : l'une non redondante avec 3 et 0,7 et l'autre avec 4 et 0,85.

En ce qui concerne U2, supposons également 2 solutions : l'une augmentant le temps moyen d'exécution de 2, l'autre n'augmentant pas ce temps moyen. On ne peut implémenter une redondance que sur la seconde solution. Schématiquement on a donc :

U1

2	0,8
3	0,9

3	0,7
4	0,85

U2

5	0,6

6	0,4
7	0,5

$\Delta T = 3$ $\Delta T = 0$ $\Delta T = 2$ $\Delta T = 0$

Adoptons la notation suivante afin de caractériser une machine,

U1 | i, j
U2 | i, j

Et qui signifie :

pour U1 : i^e solution, j^e possibilité de redondance

pour U2 : i^e solution, j^e possibilité de redondance

Ainsi :

U1	1, 2
U2	2, 2

correspond à :

U1 1ère solution, 2e possibilité de redondance, soit une augmentation du temps d'exécution égale à 3, avec redondance, c'est-à-dire un coût 3 et une fiabilité 0,9.

U2 2e solution, 2e possibilité de redondance, soit une augmentation du temps d'exécution nulle, avec un coût 7 et une fiabilité 0,5.

Cette machine aura :

- un temps d'exécution moyen égal à : temps de base + 3 + 0, soit une puissance en nombre d'instructions par unité de temps :

$$\frac{1}{\text{temps de base} + 3 + 0}$$

- un coût : 3 + 7 = 10
- une fiabilité : 0,9 x 0,5 = 0,45

<u>Exemple d'étude</u> : On ne peut pas initialiser l'étude par cette machine :

U1	1	2
U2	2	2

En effet, il existe par exemple la machine

U1	2	2
U2	1	1

qui coûte 9, à une fiabilité 0,51 et une augmentation de temps d'exécution égale à 2 + 0. C'est-à-dire que cette machine est plus puissante, plus fiable et coûte moins cher. Voyons ci-dessous quelques exemples possibles :

MAINIT

U1	1	2
U2	1	1

: CCONPC→

U1	2	1
U2	1	1

: PCONRC→

	2	2
	1	1

: RCONPC→

	2	2
	2	2

CCONPD

U1	2	2
U2	1	1

: RCONPD→

U1	1	1
U2	1	1

MAINIT

U1	2	1
U2	2	1

: SIMPD→

U1	2	1
U2	1	1

: SIMPD→

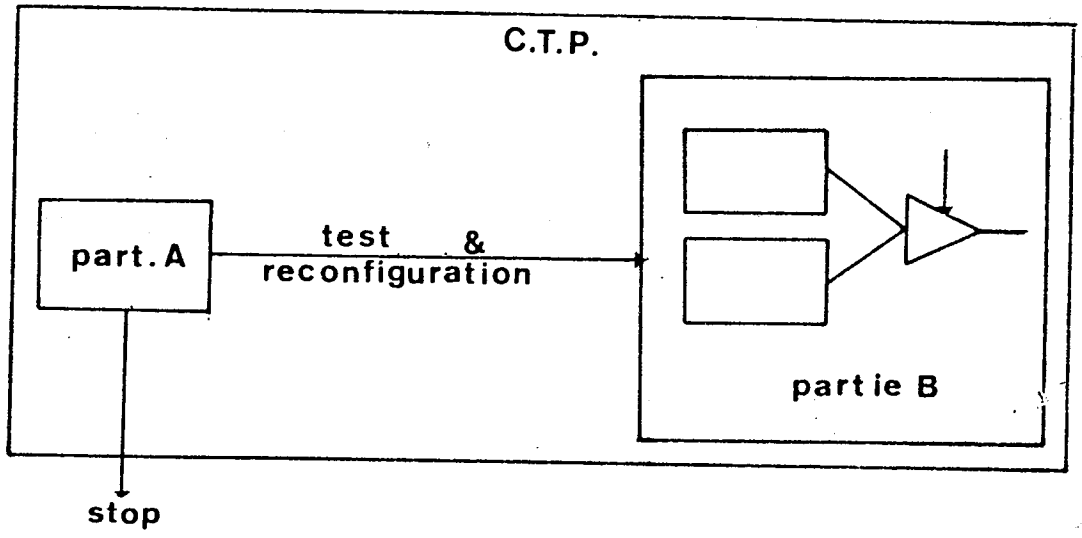
U1	1	1
U2	1	1

L'ensemble des programmes comporte environ 1800 instructions fortran.

CONCLUSION GÉNÉRALE

Revenons, dans cette conclusion générale, au calculateur tel que nous l'avons défini en introduction, c'est-à-dire composé de deux classes de circuits : l'un formé du "hardcore", l'autre formé du reste. La première partie de la présente étude donne la voie pour le choix d'une architecture, conférant aux circuits de la partie A une certaine fiabilité et une certaine sécurité. Une étude similaire à celle de la seconde partie permettrait de déterminer une architecture pour les circuits ne faisant pas partie du hardcore (partie B). Cette architecture confèrerait une fiabilité aux circuits de la partie B et une certaine puissance au calculateur.

Or, les circuits de la partie A, s'ils sont dans un état sûr, sont capables d'arrêter le calculateur si les circuits de la partie B ne peuvent plus donner d'informations justes. La sécurité du calculateur est donc égale à la sécurité de la partie A. Par contre, la fiabilité de mission du calculateur est égale au produit des fiabilités de mission des parties A et B. On a donc (Fig.1) :



S_A
RM_A

$S_B = RM_B$

$$S_{CALC} = S_A$$
$$RM_{CALC} = RM_A \cdot RM_B$$

Figure 1.

Indiquons maintenant quelques applications ou développement possibles de cette étude. La technologie actuelle tend à intégrer les circuits à une très grande échelle. Dès à présent, cette tendance doit passer par des méthodes de reconfiguration telles que celles utilisées pour la définition de mémoires hautement intégrées |1|.

Le facteur coût prendrait ici la signification d'espace total disponible sur un chip, celui de rendement de fabrication prendrait la place du paramètre de fiabilité, et interagirait sur la performance des circuits obtenus.

On pourrait objecter que le calculateur a été considéré comme un système non réparable. Nous sommes effectivement placés dans l'optique d'un calculateur embarqué, pour l'étude duquel il serait, par exemple, intéressant de construire simultanément 2 versions de caractéristiques de coût, fiabilité performance différentes, l'un de ces calculateurs étant effectivement destiné à l'application, donc très fiable, l'autre pouvant servir au développement du logiciel, puisque les 2 calculateurs auraient le même répertoire d'instructions.

Mais, que se passe-t-il si l'on considère la réparabilité du calculateur ? Augmenter la durée de vie du système diminue les charges de maintenance, puisque le-dit système tombera moins souvent en panne et par suite augmente sa disponibilité, au sens classique du terme |2|,|3|.

Augmenter la durée de vie peut être fait de la mnaière que nous avons vue et/ou à l'aide d'un calculateur connecté pilotant des dégradations successives de performances |4|, si l'on dispose d'un modèle tel que celui dérivé des réseaux de contrôle de processus parallèles |5|,|6| et présenté dans |7|. Tout ceci introduit un axe de développements futurs : celui de systèmes multiprocesseurs, où cette fois-ci des critères de fiabilité, performance, sécurité, disponibilité, interviendraient à 2 niveaux et interagiraient tous entre eux.

1) J.M. AYACHE : "Design of a very large reconfigurable memory", 2nd European Solid State Circuits Conference, Toulouse, sept. 1976.

2) B. COURTOIS : "Interaction sécurité-disponibilité-maintenance", Actes du IIIe Congrès National de Fiabilité. Perros Guirrec, Sept. 1976.

3) B. COURTOIS : "Fiabilité et sécurité de quelques systèmes logiques", Congrès AFCET, Automatismes Logiques : recherche et applications industrielles. Paris, Décembre 1976.

4) CHAUPIN, TREMBLET : "Téléreconfiguration d'un MITRA 15", Projet de fin d'études ENSIMAG, Juin 1976.

5) J. SIFAKIS : "Modèles temporels des systèmes logiques", Thèse de Docteur-Ingénieur, Grenoble, Mars 1974.

6) M. MOALLA, G. SAUCIER, J. SIFAKIS, M. ZACHARIADES : "A Design tool for the multilevel description and simulation of systems of interconnected modules", 3rd Annual Symposium on Computer Architecture, Tampa (Floride), Janvier 1976.

7) B. COURTOIS : "Models for the control of the test and of the reconfiguration of a computer", 3rd European Meeting on Cybernetics and Systems Research, Vienne (Autriche) avril 1976.

ANNEXE 4

ETUDE DU PARTITIONNEMENT DE SYSTEMES LOGIQUES REDONDANTS

Partie I : Résultats théoriques

Partie II: Résultats pratiques

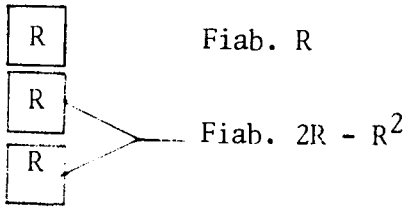
Le but de cette annexe est d'étudier l'influence du partitionnement sur certains systèmes logiques redondants, sous des hypothèses tant idéales que pratiques. En effet, la partie I concernera l'étude du partitionnement quand on considère les commutateurs parfaits. On montrera dans cette partie des résultats admis généralement au vu d'estimations numériques, ou bien pouvant être trouvés différents dans la littérature.
La partie II concernera l'étude de ce partitionnement quand on tient compte de la fiabilité des commutateurs. Pour ce faire, on considèrera un rapport de complexité entre les unités fonctionnelles et les circuits additionnels, de manière analogue à l'étude des systèmes logiques faite à propos de la sécurité des micromachines.

En accord avec les définitions précédentes, on utilisera le terme fiabilité pour fiabilité de mission, sécurité ou fiabilité du signal, puisque les systèmes que nous allons considérer ne possèdent pas de signal d'arrêt.

PARTIE I

A - Système standby (1, 1, 1)

Le premier système que l'on considèrera est un système standby, avec une unité de secours (les notations utilisées sont celles de (2)).



Soit R la fiabilité initiale du système. Le système redondant à une fiabilité :

$$R = (2R^{\frac{1}{W}} - R^{\frac{2}{W}})^{W}$$

$$R = (R^{\frac{1}{W}}(2-R^{\frac{1}{W}}))^{W}$$

$$= R\ (2-R^{\frac{1}{W}})^{W} = R.Q$$

Calculons la limite de $Q = (2-R^{\frac{1}{W}})^{W}$ q d, $w \to \infty$

$$\text{Log } Q = w \text{ Log}(2-R^{\frac{1}{W}})$$

$$= w \text{ Log}(1+1-R^{\frac{1}{W}})$$

q d, $w \to \infty$, $\frac{1}{w} \to 0$

$$R^{\frac{1}{W}} \to 1$$

$$1-R^{\frac{1}{W}} \to 0$$

$$\text{Log } Q = w((1-R^{\frac{1}{W}}) + (1-R^{\frac{1}{W}})\ \varepsilon\ (1-R^{\frac{1}{W}}))$$

$$\varepsilon\ (1-R^{\frac{1}{W}}) \to 0 \text{ qd } w \to \infty$$

Calculons la limite L de $w(1-R^{\frac{1}{W}})$

Lorsque $w \to \infty$

Soit $u = 1/w$ $u \to 0$

$$L = \frac{1}{u}\ (1-R^{u}) = \frac{1-R^{u}}{u}$$

Par la règle de L'Hôpital :

$$\underset{u \to 0}{\text{limite}}\ L = \lim_{u \to 0} \frac{-R^u \operatorname{Log} R}{1}$$

$$= - \operatorname{Log} R$$

Donc $W(1-R^{\frac{1}{W}}) \underset{W \to \infty}{\to} - \operatorname{Log} R$

D'où $\operatorname{Log} Q \to - \operatorname{Log} R + \underbrace{- \operatorname{Log} R\ \varepsilon\ (1-R^{1/W})}_{\to 0}$

$$\to - \operatorname{Log} R$$

$$Q \to 1/R$$

D'où $\quad R \to R\ \frac{1}{R} = 1$

On peut donc écrire :

<u>Théorème 1</u> : La limite de la fiabilité d'un système standby (1, 1, 1) est égale à 1 lorsque le degré de partitionnement tend vers l'infini.

B - <u>Système standby</u> (1, 1, 2)

On peut faire un raisonnement identique pour la redondance de degré 2, et montrer que $R \to 1$

$$R = (R^{1/W}(R^{\frac{2}{W}} - 3R^{\frac{1}{W}} + 3))^W$$

$$= R\ Q$$

$$\operatorname{Log} Q = W \operatorname{Log} (3 - 3R^{\frac{1}{W}} + R^{\frac{2}{W}})$$

$$= W \operatorname{Log} (1 + 2 - 3R^{1/W} + R^{\frac{2}{W}})$$

$$= W\ ((2 - 3R^{1/W} + R^{\frac{2}{W}}) + (2 - 3R^{1/W} + R^{\frac{2}{W}})\ (\quad))$$

$$\to - \operatorname{Log} R \qquad\qquad \to 0$$

$R \to 1$

D'où

<u>Théorème 2</u> : La limite de la fiabilité d'un système standby (1, 1, 2) est égale à 1 lorsque le degré de partitionnement tend vers l'infini

C - Système Standby (1, 1, S)

On peut écrire :

$$R = (1 - (1 - R^{\frac{1}{w}})^{S+1})^{w}$$

$$\text{Log } R = w \text{ Log } (1 - (1 - R^{\frac{1}{w}})^{S+1})$$

$$= w\,(-\,(1 - R^{\frac{1}{w}})^{S+1} + (1 - R^{\frac{1}{w}})^{S+1}\,\varepsilon\,(1 - R^{\frac{1}{w}})^{S+1})$$

$$= -\,w\,(1 - R^{\frac{1}{w}})\,(1 - R^{\frac{1}{w}})^{S} + w\,(1 - R^{\frac{1}{w}})^{S+1}\,\varepsilon\,(1 - R^{\frac{1}{w}})^{S+1}$$

Ainsi, si S = 0, on a un système simplex et Log R → Log R

On retrouve ainsi qu'un système simplex a toujours la même fiabilité, quel que soit le degré de partitionnement.

Si S = 1,

Log R → 0 puisque

$$-\,w\,(1 - R^{\frac{1}{w}})\,(1 - R^{\frac{1}{w}}) \to 0$$

et R → 1

Ceci est le théorème 1.

Et, pour tout S > 1

Log R → 0 car

$$-\,w\,(1 - R^{\frac{1}{w}})\,(1 - R^{\frac{1}{w}})^{S} \to 0 \text{ quand } w \to \infty$$

Ceci permet d'écrire :

Théorème 3 : Quel que soit le nombre de modules de remplacement (≠ 0), la fiabilité d'un système standby tend vers 1 lorsque le degré de partitionnement tend vers l'infini.

D - Système TMR (3, 2, 0)

$$R = (R^{\frac{3}{w}} + 3R^{\frac{2}{w}}(1 - R^{\frac{1}{w}}))^{w}$$

$$= (R^{\frac{2}{w}}(R^{\frac{1}{w}} + 3\,(1 - R^{\frac{1}{w}}))^{w}$$

$$= R^{2}\,(3 - 2R^{\frac{1}{w}})^{w}$$

Calculons la limite de :

$$Q = (3 - 2R^{\frac{1}{w}})^w$$

$$\text{Log } Q = w \text{ Log } (3 - 2R^{\frac{1}{w}})$$

$$= w \text{ Log } (1 + 2\ (1 - R^{\frac{1}{w}}))$$

$$= w\ (2\ (1 - R^{\frac{1}{w}}) + 2\ (1 - R^{\frac{1}{w}})\ \varepsilon\ (1 - R^{\frac{1}{w}}))$$

$$\to\ -2 \text{ Log } R \qquad\qquad \to 0$$

D'où

$$Q \to +\frac{1}{R^2}$$

et $\quad R \longleftrightarrow R^2 + \frac{1}{R^2} = 1$

D'où

Théorème 4 : La fiabilité d'un système TMR tend vers la valeur 1 quand le degré de partitionnement tend vers l'infini.

E - MTF et R (MTF) des systèmes TMR (3, 2, 0)

Après avoir montré les limites de la fiabilité des systèmes standby et TMR, on s'intéresse ici au temps dit "mean time to failure" et à la fiabilité à ce temps. Ces résultats ne s'accordent pas avec l'un de ceux trouvés dans la littérature (3) où il est dit que R(MTF) tend vers une borne supérieure $e^{-\pi/4}$ lorsque w tend vers l'infini. Nous allons montrer ici que MTF tend vers l'infini et que R(MTF) tend vers la valeur 1.

La fiabilité d'un système TMR partitionné est égale à :

$$R(t, w) = (3\ e^{\frac{-2\lambda t}{w}} - 2\ e^{\frac{-3\lambda t}{w}})^w$$

Montrons tout d'abord que cette fonction est croissante en fonction de w.

$$R\ (t, w) = y = (f(w))^w$$

$$f(w) = 3R^{\frac{2}{w}} - 2R^{\frac{3}{w}}$$

En posant $x = R^{\frac{1}{w}}$

$$\text{Log } x = \frac{1}{w} \text{ Log } R$$

$$\text{soit } \frac{x'}{x} = \text{Log } R\ .\ \frac{-1}{w^2}$$

$$f(w) = 3x^2 - 2x^3$$

Dérivons /w

$$\frac{y'}{y} = \text{Log } f(w) + w\,\frac{f'(w)}{f(w)}$$

$$f'(w) = (6x - 6x^2) \,.\, x \,.\, \text{Log } R \,.\, \frac{-1}{w^2}$$

$$= \frac{-6\ x\ \text{Log } R}{w^2}\,(x - x^2)$$

$$= \frac{6x^2\ \text{Log } R}{w^2}\,(x - 1)$$

D'où :

$$\frac{y'}{y} = \text{Log } (3x^2 - 2x^3) + w\,\frac{6x^2\ \text{Log } R\ (x-1)}{w^2(3x^2 - 2x^3)}$$

$$= \text{Log } (x^2(3 - 2x)) + \frac{6x^2\ \text{Log } R\ (x-1)}{w\ x^2(3 - 2x)}$$

$$= 2\ \text{Log } x + \text{Log } (3 - 2x) + \frac{6\ \text{Log } (R\ x-1)}{w\ \ (3 - 2x)}$$

$$= 2\ \text{Log } x + \text{Log } (3 - 2x) + 6\ \text{Log } x\,\frac{(x - 1)}{3 - 2x}$$

$$= \text{Log } (3 - 2x) + 2\ \text{Log } x\ (1 + 3\frac{(x - 1)}{3 - 2x})$$

$$= \text{Log } (3 - 2x) + 2\ \text{Log } x\ (\frac{3 - 2x + 3x - 3}{3 - 2x})$$

$$\frac{y'}{y} = \text{Log } (3 - 2x) + 2\ \text{Log } x\ (\frac{x}{3 - 2x})$$

Donc y' du signe de : $\text{LOG } (3 - 2x) + \frac{x\ \text{Log } x}{3 - 2x} = V$

Puisque $y > 0$

$$V' = \frac{-2}{3 - 2x} + 2\,\frac{(\text{Log } x + 1)\ (3 - 2x) - x\ \text{Log } x\ (-2)}{(3 - 2x)^2}$$

$$= \frac{-2\ (3 - 2x) + 2\ (3 - 2x)\ (\text{Log } x + 1) + 4x\ \text{Log } x}{(3 - 2x)^2}$$

$$= \frac{-6 + 4x + 2\ (3\ \text{Log } x + 3 - 2x\ \text{Log } x - 2x) + 4x\ \text{Log } x}{(3 - 2x)^2}$$

$$= \frac{6 \text{ Log } x}{(3 - 2x)^2}$$

$0 < x < 1$

$V' < 0$

Donc V décroissant quand x croît de 0 à 1.

Or V décroît de : Log 3 à 0

Donc V toujours positif

Et par suite $\frac{Y'}{Y}$ toujours positif

Donc R(TMR (3, 2, 0)) croissant en fonction de w ce qui peut se résumer par :

Théorème 5 : La fiabilité d'un système TMR (3, 2, 0) est croissante en fonction de w.

Par suite, $MTF(w) = \int_0^\infty (3\, e^{\frac{-2\lambda t}{w}} - 2\, e^{\frac{-3\lambda t}{w}})^w \, dt$ est croissante également en fonction de w. Donc MTF (w) tend vers l'infini ou bien vers une valeur finie.

- Si MTF(w) tend vers l'infini, R(MTF∞) tend vers la valeur 1, puisque la fiabilité tend vers 1 quand $w \to \infty$ (Théorème 4, 2 valeurs différentes ne peuvent pas exister à l'infini).

- Si MTF(w) tend vers une valeur finie; soit k cette valeur. On aura $MFT(w) \leq k$ puisque MTF(w) est croissante en fonction de w, et $R(MTF(w), w) \geq R(k, w)$ puisque R est décroissante en fonction du temps. Donc

$$\lim_{w \to \infty} R(MTF(w, w) \geq \lim_{w \to \infty} R(k, w)$$

Mais $\lim_{w \to \infty} R(k, w) = 1$ (théorème 4)

et ainsi :

$$\lim_{w \to \infty} R(MTF(w)) = 1$$

- Ainsi que MTF(w) tende vers l'infini ou bien vers une valeur finie, R(MTF) tend vers la valeur 1.

Ceci peut se résumer par :

Théorème 6 : La fiabilité au temps moyen de panne d'un système TMR partitionné tend vers la valeur 1 quand le degré de partitionnement tend vers l'infini.

PARTIE II

En fait, la fonction de commutation n'est jamais parfaite et est même loin de l'être (du fait entre autre de la "largeur" des données).

Cette fonction étant réalisée aussi par des circuits, on appelera R sa fiabilité, et R^T la fiabilité des circuits sur lesquels on implémente la redondance. Il y a donc un rapport T entre le nombre de circuits du système originel et le switch.

Ces notations sont cohérentes avec l'étude de la sécurité des micromachines. En effet, un commutateur pour une redondance standby de degré 1 a une complexité sensiblement égale à celle d'une disjonction ou d'un voteur.

On a vu précédemment que, si les switches sont parfaits la fiabilité tend vers 1 quand $w \to \infty$. L'objectif de cette partie est de montrer rigoureusement qu'il y a un optimum de w, que cet optimum correspond à des w petits, et qu'il est très sensible aux valeurs du temps de mission et des taux de pannes, tout ceci lorsque les switches ne sont pas parfaits.

A - Existence de l'optimum-standby de degré 2

a) Calcul de sgn $\frac{\partial R}{\partial w}$

$$R = ((2R^{T/w} - R^{\frac{2T}{w}})\ R)^w$$

$$= (R\ .\ R^{T/w}(2-R^{T/w}))^w$$

$$= R^T(R(2-R^{T/w}))^w$$

$$\text{sgn}\ \frac{\partial R}{\partial w} = \text{sgn}\ \frac{\partial}{\partial w}\ (R(2-R^{T/w}))^w$$

$$= \text{sgn}\ \frac{\partial}{\partial w}\ (y) = \text{sgn}\ \frac{\partial}{\partial w}\ (f(w))^w$$

$$\frac{y'}{y} = w\ \frac{f'(w)}{f(w)} + \text{Log}\ (f(w))$$

$$\text{sgn}\ y' = \text{sgn}\ (w\ \frac{f'(w)}{f(w)} + \text{Log}\ (f(w)))$$

$$f(w) = R(2 - R^{T/w})$$

$$f'(w) = R(+ R^{T/w} \text{ Log } R. \frac{+T}{w^2}$$

$$= R.\ R^{T/w}.\ \text{Log } R.\ \frac{T}{w^2}$$

D'où :

$$\text{sgn } y' = \text{sgn } (w \frac{R.\ R^{T/w}.\text{Log } R.\ \frac{T}{w^2}}{R(2 - R^{T/w})} + \text{Log } (f(w))$$

$$= \text{sgn } (w.\ R.\ R^{T/w}.\ \text{Log } R.\ \frac{T}{w^2} + R(2 - R^{T/w}) \text{ Log } (R(2 - R)))$$

$$= R \text{ sgn } (w.\ R^{\frac{T}{W}}.\ \text{Log } R.\ \frac{T}{w^2} + (2 - R^{\frac{T}{W}}) \text{ Log } (R(2 - R^{\frac{T}{W}})))$$

$$= \text{sgn } (R^{\frac{T}{W}}.\ \text{Log } R.\ \frac{T}{W} + (2 - R^{\frac{T}{W}}) \text{ Log } (R(2 - R^{\frac{T}{W}})))$$

b) Pour $w = T$ (degré maximum de partitionnement) la dérivée $\frac{\partial R}{\partial w}$ est négative

$w = T$

$$\text{sgn } \frac{\partial R}{\partial w} = \text{sgn } y' =$$

$$= \text{sgn } (R.\ \text{Log } R + (2 - R) \text{ Log } (R(2 - R))$$

$$= \text{sgn } (R.\ \text{Log } R + (2 - R) \ (\text{Log } R + \text{Log } (2 - R))$$

$$= \text{sgn } (R.\ \text{Log } R + 2\text{Log } R - R \text{ Log } R + (2 - R) \text{ Log } (2 - R))$$

$$= \text{sgn } (2\text{Log } R + (2 - R) \text{ Log } (2 - R))$$

$$= \text{sgn } (V)$$

Etudions le signe de V.

$$\frac{dV}{dR} = V' = \frac{2}{R} + (2 - R).\ \frac{-1}{2-R} + (-1) \text{ Log } (2 - R)$$

$$= \frac{2}{R} - 1 - \text{Log } (2 - R)$$

$$V' \geqslant \frac{2}{R} - 1 - \text{Log } 2$$

$$V' \geqslant 2 - 1 - \text{Log } 2$$

$$V' > \forall R$$

D'où (V) croissant en fonction de R

$$R = 0 \Rightarrow V \to -\infty$$

$$R = 1 \to V \to 0$$

Donc $V \leqslant 0$

Par suite, $\frac{\partial R}{\partial w} \leqslant 0$

pour $w = T$

c) Pour $w = 1$, (degré minimum de partitionnement), le signe de $\frac{\partial R}{\partial w}$ est difficile à expliciter.

Considérons alors la fonction $R(w)$

$$\lim_{w \to 0} R(w) = \lim_{w \to 0} R^T \left(R(2 - R^{T/w})\right)^w$$

$$\frac{T}{w} \to \infty \quad R^{\frac{T}{w}} \to 0$$

$$\lim_{w \to 0} R(w) = R^T \lim \left(R(2 - R^{T/w})\right)^w$$

$$= R^T$$

= fiabilité du système simplex

<u>Par convention, nous dirons que $w = 0$ correspond au système simplex.</u>

Montrons que la dérivée, pour $w = 0$ est positive :

$$\operatorname{sgn} \left(\frac{\partial R}{\partial w}\right)_{w=0} = \operatorname{sgn} \left(\underbrace{R^{\frac{T}{w}}. \operatorname{Log} R. \frac{T}{w}}_{\to 0} + (2 - R^{\frac{T}{w}}) \operatorname{Log} \left(R(2 - R^{\frac{T}{w}})\right)\right)$$

$$= \operatorname{sgn} (2 \operatorname{Log} 2R)$$

$$\left(\frac{\partial R}{\partial w}\right)_{w=0} > 0 \text{ si } R > \frac{1}{2}$$

Dans la suite, on ne s'intéressera qu'aux cas $R > 1/2$

d) Il existe un optimum : en effet, la fonction $R(w)$, $0 \leq w \leq T$ est continue en w en posant $R(0) = R^T$.

La dérivée est de même continue, en posant $\left(\frac{\partial R}{\partial w}\right)_{w=0} = \lim \left(\frac{\partial R}{\partial w}\right)_{w \to 0}$

Cette dérivée est positive en $w = 0$ et négative en $w = T$.

Donc (Th. III p. 94 (4))

$\exists$ au moins un $w_0 / \left(\frac{\partial R}{\partial w}\right)_{w_0} = 0$

e) Cette valeur w_0 est unique.

Rappelons que l'on a

$$f(w) = R(2 - R^{\frac{T}{w}})$$

$$f'(w) = R. R^{\frac{T}{w}}. \operatorname{Log} R. \frac{T}{w^2}$$

D'où

$$\frac{y'}{y} = w \frac{R.\ R^{\frac{T}{w}}.\ \text{Log}\ R\ \frac{T}{w^2}}{R(2 - R^{\frac{T}{w}})} + \text{Log}\ (R(2 - R^{\frac{T}{w}}))$$

$$= \frac{R.^{\frac{T}{w}}\ \text{Log}\ R.\ \frac{T}{w}}{2 - R^{\frac{T}{w}}} + \text{Log}\ (R(2 - R^{\frac{T}{w}}))$$

Posons $R^{\frac{T}{w}} = U$, $0 < U < 1$ quand $0 < w < T$

$$\frac{T}{w}.\ \text{Log}\ R = \text{Log}\ U$$

Il vient alors

$$\frac{y'}{y} = \frac{U.\ \text{Log}\ U}{2 - U} + \text{Log}\ (R(2 - U))$$

$$= \underbrace{\frac{U.\ \text{Log}\ U}{2 - U}}_{y1} \underbrace{+ \text{Log}\ R + \text{Log}\ (2 - U)}_{-y2}$$

Nous allons étudier l'intersection de y1 et y2

i) Etude de y1

$$y1 = \frac{U.\ \text{Log}\ U}{2 - U}$$

$$y'1 = \frac{(\text{Log}\ U + 1)\ (2 - U) + U\ \text{Log}\ U}{(2 - U)^2}$$

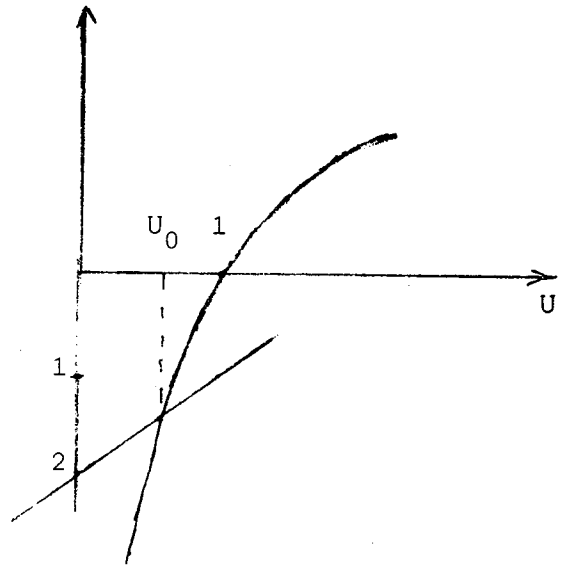
$$= \frac{2\ \text{Log}\ U + 2 - U\ \text{Log}\ U - U + U\ \text{Log}\ U}{(2 - U)^2}$$

$$= \frac{2\ \text{Log}\ U + 2 - U}{(2 - U)^2}$$

zéros de y'1 : $2\ \text{Log}\ U + 2 - U = 0$

$$\text{Log}\ U = \frac{U - 2}{2}$$

U	0		U_0		1
y'1	$-\infty$	-	0	+	1
y1	0	↘	$\frac{-U_0}{2}$	↗	0



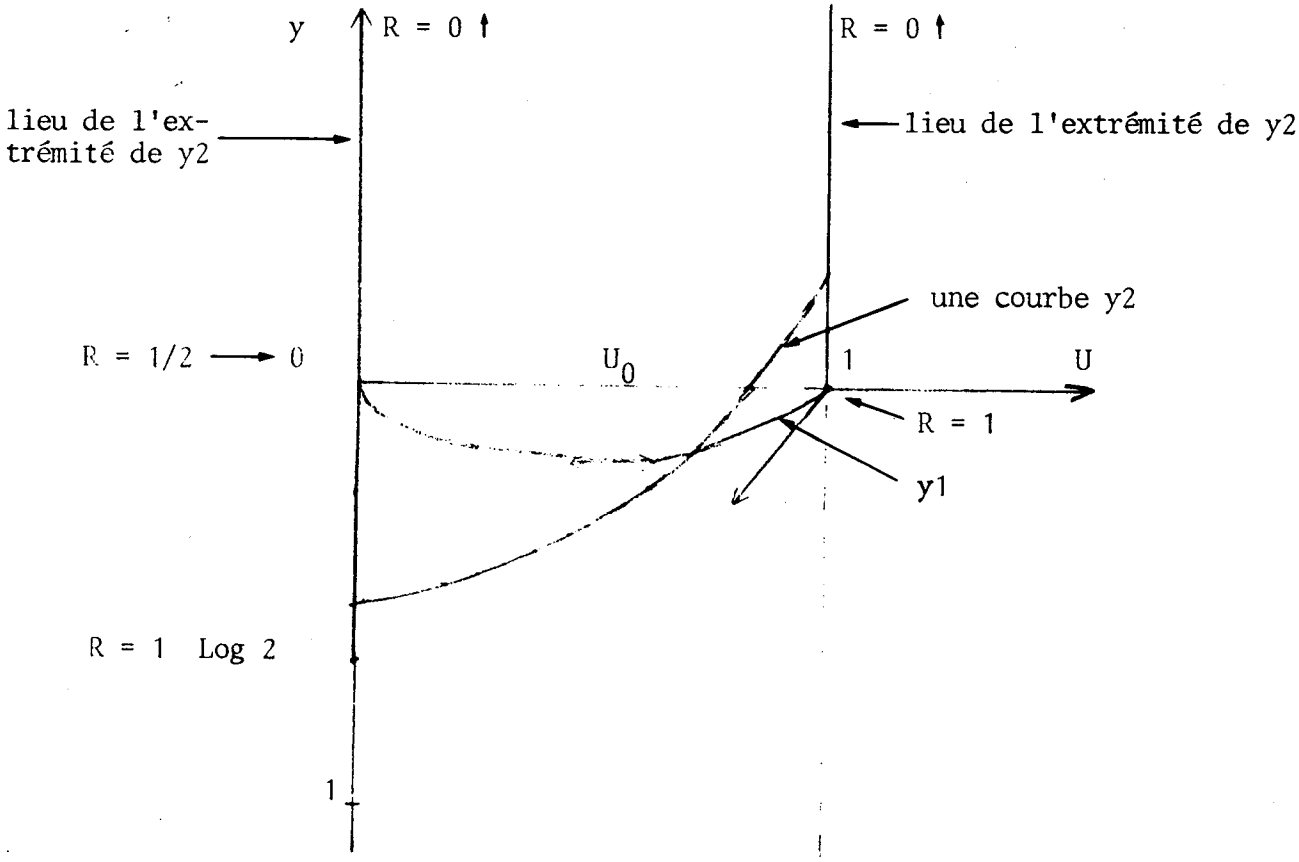
ii) Etude de y2

$$y2 = - \text{Log } R - \text{Log } (2 - U)$$

$$y'2 = \frac{+1}{2-U} < 0$$

U	0		1
y'2	+1/2	+	+1
y2	Log 2R	↗	Log R

iii) Etude de l'intersection



Montrons qu'il n'y a qu'un point d'intersection.

En effet, comparons les pentes de y1 et y2

$$\frac{y'1}{y'2} = \frac{(2\text{Log } U + 2 - U)\ (2 - U)}{(2 - U)^2}$$

$$= \frac{2 \text{ Log } U + 2 - U}{2 - U}$$

$$\frac{y'1}{y'2} - 1 = \frac{2 \text{ Log } U + 2 - U - 2 + U}{2 - U}$$

$$= \frac{2 \text{ Log } U}{2 - U} \leqslant 0$$

$$\frac{y'1}{y'2} \leqslant 1$$

$$y'1 \leqslant y'2$$

Il n'y a donc qu'un point où $\frac{y'}{y}$ s'annule.

Tout ceci permet de calculer aisément la valeur (entière) optimale pour w, puisqu'il suffit d'observer le changement de signe de la pente R(w)et de choisir parmi les 2 valeurs entières entourant immédiatement le changement de signe.

On peut résumer par :

Théorème 7 : Sous les hypothèses précédentes, pour tout système standby (1, 1, 1) il existe une valeur optimale du degré de partitionnement, et cette valeur est unique.

B - Valeurs optimales de w_0 pour des systèmes standby (1, 1, 1)

Rappelons que R est la fiabilité du switch et que R^T est celle de l'unité fonctionnelle. La valeur optimale w_0 dépend de ces 2 paramètres. La valeur de R dépend du temps de mission et est fixée quand ce temps de mission est déterminé. On trouve dans la table I les valeurs de w, de la fiabilité correspondante, ainsi que la fiabilité du système simplex correspondant. Les renvois des parties X et Y seront davantage explicités après.

T \ 1-R	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
10	2 0.56 0.35	1 0.98 0.90	1 0.999 0.990	1 0.9999 0.9990	1 0.99999 0.99990	1 0.999999 0.999990	1 0.9999999 0.9999994
20	4 0.31 0.12	2 0.96 0.82	2 0.999 0.980	1 0.9999 0.9980	1 0.99999 0.99981	1 0.999999 0.999981	1 0.9999999 0.9999988
50	11 0.05 0.005	5 0.91 0.61	2 0.996 0.951	1 0.9998 0.9950	1 0.9999 0.9995	1 0.999999 0.999952	1 0.9999999 0.9999970
100	22 0.003 0.00003	9 0.83 0.37	3 0.99 0.90	1 0.9998 0.9900	1 0.99998 0.99900	1 0.999999 0.999904	1 0.9999999 0.9999904
500		45 0.38 0.006	15 0.97 0.61	5 0.999 0.951	2 0.9999 0.9950	1 0.99999 0.99952	1 0.9999999 0.9999702
1000		90 0.14 0.00004	31 0.94 0.36	10 0.998 0.905	3 0.9999 0.9901	1 0.99999 0.99905	1 0.9999999 0.9999404
5000			153 0.73 0.007	49 0.99 0.60	16 0.999 0.951	5 0.99999 0.99524	1 0.999999 0.999702
10000			306 0.53 0.00004	99 0.98 0.36	31 0.999 0.905	10 0.9999 0.9905	2 0.999999 0.999404
50000				495 0.90 0.007	157 0.996 0.607	49 0.9999 0.9534	12 0.99999 0.99702
100000				990 0.82 0.00005	315 0.993 0.369	98 0.9998 0.9090	24 0.999997 0.994057

Table I

Partie X

Partie Y

C - Valeurs optimales de w pour des systèmes standby (1, 1, 2) si R est la fiabilit du switch

D'une manière semblable, on peut calculer les valeurs optimales de w, en considérant R pour la fiabilité du switch. Remarquons dès maintenant qu'un switch à 3 positions, pour des systèmes (1, 1, 2) est plus complexe qu'un switch à 2 positions pour des systèmes (1, 1, 1). Les résultats obtenus ne permettent pas de comparaison réaliste avec les résultats précédents. (ceci sera fait dans D). La table II donne les valeurs optimales de w et la fiabilité obtenue. Pour ces calculs nous admettrons qu'il existe une valeur optimale, obtenue par observation de la dérivée. On a :

$$R(w) = R^T \left((R^{\frac{2T}{w}} - 3R^{\frac{T}{w}} + 3)\, R\right)^w$$

quand $w \to 0$, $R(w) \to R^T$ = simplex

$$\operatorname{sgn} \frac{\partial R}{\partial w} = \operatorname{sgn} \frac{\partial}{\partial w}\left((R^{\frac{2T}{w}} - 3R^{\frac{T}{w}} + 3)\, R\right)^w$$

$$= \operatorname{sgn} \frac{\partial}{\partial w} \left((f(w))^w\right)$$

$$\operatorname{sgn} \frac{\partial R}{\partial w} = \operatorname{sgn} \left(w \frac{f'(w)}{f(w)} + \operatorname{Log} f(w)\right)$$

$$f(w) = R\, (R^{\frac{2T}{w}} - 3R^{\frac{T}{w}} + 3)$$

$$f'(w) = R.\ \operatorname{Log} R.\ \frac{T}{w^2}\ .\ R^{\frac{T}{w}}(- R^{\frac{T}{w}} + 3).$$

T \ 1-R	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
10	2 0.70 0.35	1 0.989	1 0.998	1 0.9999	1 0.99999	1 0.999999	1 0.9999999
20	4 0.49	1 0.98	1 0.998	1 0.9999	1 0.99999	1 0.999999	1 0.9999999
50	10 0.17	3 0.96	1 0.998	1 0.99989	1 0.99999	1 0.999999	1 0.9999999
100	19 0.03	5 0.92	1 0.998	0.99989	0.99999	0.999999	0.9999999
500	96	25 0.67	6 0.99	1 0.999	1 0.9999	1 0.999999	1 0.9999999
1000		51 0.45	12 0.98	3 0.999	1 0.9999	1 0.999999	1 0.9999999
5000		253 0.02	59 0.91	13 0.998	3 0.9999	1 0.99999	1 0.9999999
10000			118 0.83	26 0.99	6 0.9999	1 0.99999	1 0.9999999
50000			592 0.40	132 0.98	29 0.999	6 0.99999	1 0.9999999
100000				264 0.96	58 0.999	12 0.9999	2 0.999999

Table II

D - Valeurs optimales de w pour des systèmes standby (1, 1, 2) si R^2 est la fiabilité du switch

Pour les raisons exposées dans C, nous ferons ici l'hypothèse que R^2 est la fiabilité d'un switch à 3 positions si R est celle d'un switch à 2 positions. Ainsi, les résultats seront directement comparables à ceux de B.

On a ainsi :

$$R = ((R^{\frac{3T}{w}} - 3R^{\frac{2T}{w}} + 3R^{\frac{T}{w}})\ R^2)^{w}$$

$$= R^T\ ((R^{\frac{2T}{w}} - 3R^{\frac{T}{w}} + 3)\ R^2)^{w}$$

quand $w \to 0$, $R \to R^T$ = simplex

Admettons encore que l'optimum existe.

Le signe de la dérivée devient :

$$\text{sgn}\ \frac{\partial R}{\partial w} = \text{sgn}\ \frac{\partial}{\partial w}\ ((f(w))^{w})$$

$$\text{avec } f(w) = (R^{\frac{2T}{w}} - 3R^{\frac{T}{w}} + 3)\ R^2$$

$$f'(w) = R^2.\ \text{Log}\ R.\ \frac{T}{w^2}\ .\ R^{\frac{T}{w}}\ (3 - R^{\frac{T}{w}})$$

$$\text{sgn}\ \frac{\partial R}{\partial w} = \text{sgn}\ (w\ \frac{f'(w)}{f(w)} + \text{Log}\ f(w))$$

On obtient alors la table III, les valeurs indiquées ayant la même signification que pour la table I.

Table III

Partie X

T \ 1-R	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
10	1 0.59 0.35	1 0.979 0.904	1 0.998 0.990	1 0.9998 0.9990	1 0.99998 0.99990	1 0.999998 0.999990	1 0.9999998 0.9999994
20	3 0.35 0.12	1 0.97 0.81	1 0.9979 0.9801	1 0.9998 0.9980	1 0.99998 0.9998	1 0.999998 0.999980	1 0.9999998 0.9999988
50	7 0.075 0.005	2 0.94 0.61	1 0.998 0.951	1 0.9997 0.9950	1 0.99998 0.99950	1 0.999998 0.999952	1 0.9999998 0.9999970
100	13 0.00562 0.00003	4 0.88 0.36	1 0.99 0.90	1 0.9997 0.9900	1 0.99998 0.99900	1 0.999998 0.999904	1 0.999999 0.999994
500		19 0.54 0.006	5 0.98 0.60	1 0.999 0.951	1 0.9999 0.9950	1 0.99999 0.9995	1 0.999999 0.999970
1000		38 0.28 0.00004	9 0.97 0.36	2 0.999 0.904	1 0.9999 0.9900	1 0.99999 0.99904	1 0.999999 0.999940
5000			46 0.86 0.006	10 0.99 0.606	2 0.9999 0.951	1 0.99999 0.995	1 0.999999 0.999702
10000			92 0.75 0.00004	21 0.99 0.37	5 0.999 0.90	1 0.99999 0.99	1 0.999999 0.999
50000				104 0.96 0.007	23 0.999 0.61	5 0.9999 0.95	1 0.999999 0.997
100000				208 0.94 0.00004	46 0.99 0.97	10 0.9999 0.91	2 0.999999 0.994

Partie Y

E - Choix d'un degré de redondance et de partitionnement pour des systèmes standby

Si l'on suppose avoir le choix entre 1 et 2 modules de secours, il est aisé de déterminer à partir des tables I et III quelles sont les valeurs optimales à donner à w. Soient w-opt 1 et w-opt 2 ces deux valeurs. Mais il n'est pas évident qu'une redondance de degré 2 soit meilleure qu'une redondance de degré 1 (dont le coût est naturellement moindre). En fait, il faut considérer la fiabilité du système conférée par les deux types de redondance lorsque le partitionnement est w-opt 1 et w-opt 2. Ainsi, la partie X figurant sur les tables I et III est le domaine où une redondance de degré 1 donne une fiabilité générale meilleure qu'avec une redondance de degré 2. D'une manière semblable, la partie Y est celle où une redondance de degré 2 est meilleure.

La partie X est le domaine des petits systèmes (jusqu'à une complexité de 1000), alors que la partie Y est celui des systèmes plus importants et pour des temps de mission longs. Remarquons que pour la partie X, la valeur optimale de w est 1, c'est à dire qu'on n'a jamais intérêt à partitionner le système. Remarquons enfin que pour la table I, si l'on appelle ρ le rapport $\frac{T}{w_0}$, ρ a sensiblement les valeurs :

5	pour	R = 1 -	10^{-1}
10	"	"	10^{-2}
33	"	"	10^{-3}
100	"	"	10^{-4}
300	"	"	10^{-5}
1000	"	"	10^{-6}
4000	"	"	10^{-7}

lorsque $w \neq 1$.

ρ varie dans un rapport environ égal à 3 lorsque 1-R passe de $1-10^{-2}$ à $1-10^{-7}$.

En ce qui concerne la table III, on peut remarquer que ρ a sensiblement les valeurs :

7	pour	R = 1 -	10^{-1}
20	"	"	10^{-2}
100	"	"	10^{-3}
500	"	"	10^{-4}
1000	"	"	10^{-5}
10000	"	"	10^{-6}
50000	"	"	10^{-7}

lorsque $w \neq 1$; ρ varie dans un rapport sensiblement égal à 5 lorsque 1-R passe de $1-10^{-2}$ à $1-10^{-7}$.

T \ 1-R	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
10	4 0.36 0.35	2 0.96 0.90	1 0.998 0.990	1 0.99989 0.999	1 0.99999 0.9999	1 0.999999 0.99999	1 0.9999999 0.999999
20	8 0.13 0.12	3 0.94 0.81	1 0.99 0.98	1 0.9998 0.998	1 0.99998 0.9998	1 0.999999 0.99998	1 0.9999999 0.999998
50	20 0.006 0.005	8 0.84 0.60	3 0.99 0.95	1 0.999 0.99	1 0.9999 0.999	1 0.999999 0.9999	1 0.9999999 0.99998
100	40 0.00004 0.00002	16 0.71 0.36	5 0.98 0.90	2 0.999 0.99	1 0.9999 0.999	1 0.999999 0.9999	1 0.9999999 0.99999
500		79 0.18 0.0006	27 0.94 0.60	9 0.99 0.95	3 0.9999 0.99	1 0.99999 0.999	1 0.9999999 0.9999
1000		157 0.03 0.00004	53 0.89 0.36	17 0.99 0.90	5 0.999 0.99	2 0.99999 0.999	1 0.9999999 0.9999
5000		786	266 0.58 0.006	86 0.98 0.60	27 0.999 0.95	8 0.99998 0.99	2 0.999999 0.999
10000			531 0.33 0.00004	172 0.96 0.37	54 0.9989 0.90	17 0.9999 0.99	4 0.999999 0.999
50000			2656	858 0.84 0.006	272 0.99 0.60	84 0.999 0.95	21 0.99999 0.99
100000				1715 0.70 0.00004	545 0.98 0.36	169 0.999 0.909	42 0.99999 0.99

Table IV

F - Valeurs optimales de w_0 pour des systèmes TMR (3, 2, 0)

Ces valeurs ont été calculées en considérant qu'un voteur est à peu près équivalent à un switch à 2 positions, pour une redondance standby de degré 1. C'est à dire qu'une fiabilité R a été prise pour un voteur, alors qu'une fiabilité R^T a été prise pour les unités fonctionnelles. La table IV résume les résultats.

CONCLUSION

Des résultats des parties I et II, on peut voir aisément que les résultats théoriques sont profondément modifiés lorsque des hypothèses réalistes sont faites sur les fonctions de commutation et de vote. En outre, les résultats présentés ici ne sont pas complets en ce sens que nous n'avons pas calculé les valeurs pour des degrés de redondance supérieure à 2. Remarquons néanmoins qu'il existe une différence non négligeable lorsque l'on fait une hypothèse différente sur les fiabilités des switches à 3 Positions : R ou R^2. Cette différence est d'environ 20% lorsque les valeurs optimales sont différentes de 1. Ceci mesure l'importance des hypothèses faites.

Supposons que l'on désire fabriquer un chip LSI redondant, pour des raisons de fiabilité (en prenant soin de l'isolation des pannes sur le chip). Si l'on suppose que ce chip doit avoir 20 lignes d'entrée-sortie, la fiabilité d'un switch de 20 lignes sera R. Si initialement la complexité du chip est 20 000, on devra utiliser les complexités 20 000/20 = 1 000 pour les tables 1 et III si l'on désire une redondance standby. Ces tables donnent immédiatement le nombre de blocs devant être considérés. Si par exemple une redondance de degré 1 est choisie pour des raisons de place sur le chip, la table I donne immédiatement une valeur 1 pour un temps de mission court, alors que pour un temps de mission plus long, une valeur variant de 30 à 3 devrait être employée.

Enfin, le partitionnement de systèmes sûrs tels qu'étudiés par ailleurs (BDR..) n'a pas été abordé. Mais, si pour certaines complexités des unités fonctionnelles le partitionnement pouvait augmenter la fiabilité, au sens fiabilité de mission, ceci serait accompagné fatalement par une diminution de la sécurité du système global, puisque les circuits d'arêts seraient plus nombreux.

REFERENCES

1) B. COURTOIS : "Systèmes logiques pour la sécurité et la fiabilité". Séminaire ENSIMAG. Septembre 1975.

2) F.P. MATHUR, P.T. de SOUSA : "GMR : General Modular Redundancy". FTC 4 Champaign - Illinois - USA, juin 1974.

3) F.P. MATHUR : "Reliability modeling and architecture of ultra-reliable fault-tolerant digital computers". Ph. D. Thesis, University of California, 1970.

4) CAGAC, RAMIS, COMMEAU : "Traité de Mathématiques Spéciales". Ed. Masson et Cie.

5) B. COURTOIS, G. SAUCIER : "On Partitionning a Redundant System Under Realistic Assumptions". Informatica 75 Bled (Yougoslavie).

ANNEXE 5

PROGRAMME D'EVALUATION DE FIABILITE

A5 - 1. SCHEMAS DE REDONDANCE

A5 - 2. PARAMETRES

A5 - 3. COMMANDES

A5 - 4. EXEMPLE

Le but de cette annexe est de présenter très brièvement le programme ayant permis toutes les évaluations de fiabilité faites au cours de cette étude. Ce programme est une amélioration et une extension du programme CARE (Computer-Aided Reliability Estimation) du Professeur MATHUR. Le système complet comporte environ 5000 instructions FORTRAN IV/IBM.

Les résultats sont fournis sous forme de tabulation ou de graphiques. Les calculs faits sont fonction de requêtes émises par l'utilisateur, au moyen d'un langage de commandes. Après avoir listé les équations et les paramètres utilisés, on décrira brièvement chaque commande, sans entrer dans les détails, qui peuvent être trouvés dans les pages 20 à 90 du rapport de contrat DRME n° 73-787.

A5 - 1. SCHEMAS DE REDONDANCE

Les systèmes de redondance considérés sont les suivants : (repérés par le numéro d'équation qu'ils portent dans le programme).

1) Système hybride (NMR si S = 0)

A : dormancy factor'K' à valeur finie

B : dormancy factor'K' à valeur non finie

(le paramètre K est défini dans "Paramètres").

2) Système à remplacement

A : idem 1

B : idem 1

4) Système TMR - hybride/simplex

A : idem 1

B : idem 1

Ce système est caractérisé par le fait suivant : dès que l'une des 3 dernières unités tombe en panne, on déconnecte une unité parmi les 2 restantes. Ceci augmente la probabilité de survie.

5) Système TMR avec probabilité de collage de ligne à 0 ou 1. Ce système prend en compte le fait suivant : lorsque 2 unités d'un système TMR sont tombées en panne, le système peut néanmoins continuer à fonctionner si ces 2 pannes sont caractérisées par un collage de ligne à 0 (resp.1) et un autre à 1 (resp. 0).

6) Système simplex (pas de redondance).

A5 - 2. PARAMETRES

Paramètres généraux

. Paramètres de structure

LAMBDA : taux de panne des modules actifs.

MU : taux de panne des modules de secours.

K : = LAMBDA/MU

En effet, les modules de secours ont un taux de panne μ inférieur à λ lorsqu'ils ne sont pas sous tension. On peut alors considérer que les modules de secours sont dans l'un des 3 modes suivants :

Mode actif : Le taux de panne μ est égal à λ. Les modules de secours sont sous-tension et l'on a alors $K = 1$.

Mode inerte : Le taux de panne μ est égal à zéro. On a alors K = infini.

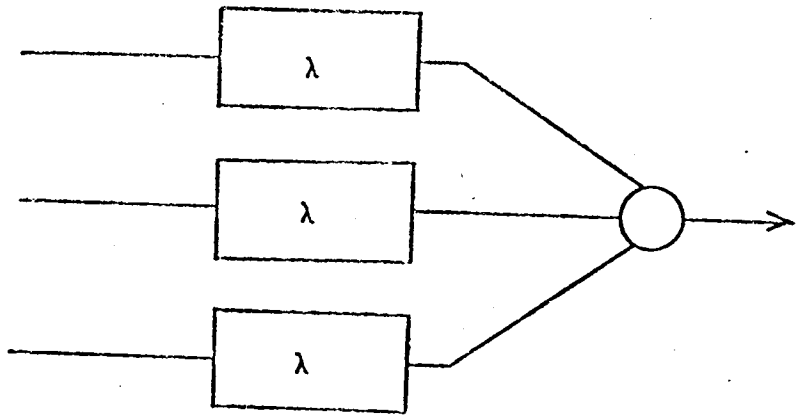
Mode dormant : Le taux de panne μ est supérieur à zéro, mais il reste inférieur à λ. K est alors compris entre 1 et l'infini.

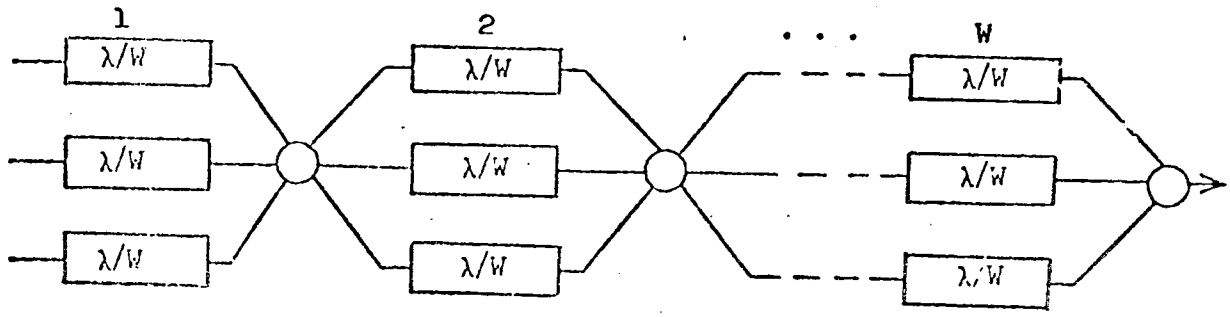
S : nombre d'unités de remplacement dans les systèmes à remplacement ou les systèmes hybrides.

n : correspond au nombre d'unités répliquées dans les systèmes NMR ou hybrides. On a alors $N = 2n+1$. Ainsi, le cas $n = 1$ correspond au système TMR.

W : degré de partitionnement du système lorsque ce-dit système peut se décomposer en w sous-systèmes, à taux de pannes w fois plus faible. Un exemple fera comprendre la signification de ce paramètre.

Pour un système TMR on a :





Z : nombre de sous-systèmes identiques dans un système.

C : probabilité qu'un système à remplacement se reconfigure si une panne est détectée.

RV : fiabilité de l'organe de vote dans les systèmes hybrides (NMR si S = 0).

. Paramètres de temps

T : temps de mission réel.

LAMT : temps de mission normalisé. Il est égal au produit du temps réel et du taux de panne.

ELAMT : = exp (-LAMT).

On spécifie indifféremment 1 parmi les 3 variables de temps.

. Paramètres de calcul

MIN : minimum de T, LAMT ou ELAMT.

B : paramètre d'intégration pour les évaluations de MTBF.

STEP : pas de calcul général pour les évaluations de fiabilité.

P : probabilité de collage de ligne à 1 (ou 0) pour les systèmes TMR à compensation de panne (équation 5).

Les calculs sont faits en fonction du temps de mission T ou du temps de mission normalisé LAMT, entre les valeurs MIN et (T ou ELAMT ou LAMT) par pas déterminé par STEP.

B est un paramètre utilisé par les sous-programmes d'intégration. Sa connaissance approximative peut améliorer les temps de calcul. OPTION est le paramètre de DIFF, déterminé auparavant dans le système questions-réponses ou par la commande DIFF. Il peut donc être modifié ici.

L'utilisateur peut spécifier plusieurs valeurs pour chaque paramètre de structure (16 au maximum). Pour chaque jeu de valeurs, le programme effectue automatiquement les calculs.

Tous les paramètres ont des valeurs par défaut :

MU : 0	C : 1. 0
K : ∞	RV : 1. 0
W : 1	MIN : 0. 0
Z : 1	STEP : 1. 0
S : 0	OPTION : 2
n : 1 (correspondant au système TMR)	P : 1. 0

A5 - 3. COMMANDES DISPONIBLES

Les commandes soulignées sont celles prises par défaut. L'exécution commence à l'apparition de la commande GO, ou après l'envoi d'une ligne blanche.

Calculs effectués quelles que soient les commandes

Le programme calcule la fiabilité (REL), la probabilité de panne (UNREL), la fiabilité du système simplex associé (SIMREL), les rapports REL/SIMREL (SIMGAIN) et (1-SIMREL)/(1-REL) (SIMRIF), sur la plage de temps déterminée par l'un des 3 paramètres T, LAMT ou ELAMT, et pas choisi par STEP.

La valeur des paramètres est indiquée avant chaque calcul de fiabilité et le calcul est fait automatiquement pour chaque jeu de valeurs des paramètres (16 valeurs différentes possibles pour chaque paramètre).

QR

Dès l'apparition de cette comande, il y a réinitialisation générale des variables et déroulement du système en questions-réponses. Ce mode est destiné à un utilisateur inexpérimenté. On peut, en effet, demander à voir lister au terminal la définition des équations et des paramètres, ainsi que demander à recevoir des instructions avant d'avoir à répondre à chaque question (définition des calculs possibles, paramètres d'exécution). Cette commande peut ne pas être la première.

NOQR

Constitue l'option par défaut. L'analyse des commandes continuera jusqu'à l'apparition de la commande GO ou de l'envoi d'une ligne blanche, ce qui déclenchera l'exécution.

PRO

Produit de plusieurs équations différentes. Il s'agit de spécifier plusieurs systèmes en série jusqu'à 10 au maximum. Les calculs de fiabilité sont faits pour chaque sous-système, puis la fiabilité du système total est calculée. Cette commande inhibe PLOT, MMT2 et DIFF. On peut encore spécifier jusqu'à 16 valeurs pour chaque paramètre de chaque système.

NOPRO

Constitue l'option par défaut : on n'étudie qu'un seul système.

PLOT

Cette commande fera générer un fichier de données qui est ensuite repris par 2 programmes de tracé de courbes à l'imprimante off-line et sur le traceur BENSON. Cette méthode est avantageuse car la seule connaissance de la structure du fichier est suffisante pour réécrire rapidement des programmes de tracé sur d'autres matériels. On trace ainsi la fiabilité du système, en fonction du temps de mission ou du temps de mission normalisée, entre les valeurs déterminées par MIN et (T ou ELAMT ou LAMT). Les valeurs des paramètres sont transmises et répétées sur les displays de sortie. On trouve sur un même dessin les courbes correspondant au paramètre qui a été spécifié. Il y aura autant de dessins que de jeux de valeurs des paramètres autres que celui qui a été spécifié, et on pourra indifféremment tracer les courbes sur l'imprimante (ou au terminal) et/ou sur le traceur de courbes.

NOPLOT constitue l'option par défaut

MMT1

Calcule le temps de mission maximum pour une fiabilité donnée. Si l'entrée est faite en temps normalisé, on calcule LAMTMAX, temps de mission normalisé maximum ainsi que le temps correspondant pour le système simplex associé SIMLAMTMAX et le rappart des deux. Si l'étude est faite en temps réel, on calcule TMAX le temps de mission maximum, le temps correspondant pour le système simplex SIMTMAX, et le rapport des 2. On évitera d'essayer de calculer le temps de mission pour une fiabilité qu'il n'est pas possible d'atteindre (cas de systèmes à vote où RV est différent de 1.0).

NOMMT1 constitue l'option par défaut

MMT2 $\left(\begin{matrix}1\\2\\3\end{matrix}\right)$

Compare les temps de mission maximum pour 2 valeurs différentes du paramètre spécifié, entre les valeurs de fiabilité minimum et maximum, par pas RISTEP.

On peut spécifier l'une des trois options suivantes :

1) Comparaison entre toutes les valeurs du paramètre spécifié.
2) Comparaison entre les 2 dernières valeurs du paramètre.
3) Le programme demande, lors de l'exécution, entre quelles valeurs les comparaisons sont à faire.

Dans les 3 cas, on calcule le temps de mission maximum pour la 1ère valeur : TMAX1, le temps de mission maximum pour la seconde, ainsi que le rapport TMAX2/TMAX1 : RATIF.

On évitera, de même que pour MMT1, d'essayer de calculer un temps de mission pour une fiabilité notoirement impossible à atteindre.

NOMMT2 constitue l'option prise par défaut.

DIFF $\begin{pmatrix}0\\1\\2\end{pmatrix}$ Calcule la différence de fiabilité pour 2 valeurs différentes du paramètre spécifié. DIFF est en fiabilité ce que MMT2 est au temps de mission. On peut spécifier l'une des 3 options suivantes :

0) Le programme demande à l'exécution entre quelles valeurs il faut faire les comparaisons, les seules valeurs possibles du paramètre étant celles calculées à cet instant.

1) Comparaison entre toutes les valeurs du paramètre spécifié.

2) Comparaison entre les 2 dernières valeurs du paramètre. L'option 2 est prise par défaut. Si l'utilisateur spécifie une option différente de 0, 1 ou 2, il y aura détection d'erreur. L'option pourra être encore modifiée lors de l'entrée des données par $VAR... $END en spécifiant une valeur du paramètre OPTION.

Dans les trois cas on calcule la différence de fiabilité R2-R1 (DIFF), le rapport R2/R1 (RIF) ainsi que le rapport (1-R2)(1-R1) : GAIN en fonction du temps de mission ou du temps de mission normalisé entre les valeurs déterminées par MIN et (T ou LAMT) par pas STEP. (Si l'option PLOT est active, il y a changement dynamique du pas).

NODIFF constitue l'option par défaut.

MTF

Calcule la MTBF ainsi que la fiabilité R(MTF) lors de chaque calcul de fiabilité, donc pour chaque jeu de valeurs des paramètres. Cette option utilise le paramètre B, borne d'intégration pour la première itération. Le programme intègre en effet entre 0 et B et calcule pour cet intervalle une fonction erreur. Si cette erreur est trop grande, il intègre entre B et 3B, etc.. La connaissance approximative de B permet donc de diminuer les temps de calcul. Si ce paramètre n'a pas été spécifié lors de l'entrée des données dans $ VAR...$ END, le programme demandera lors de l'utilisation de donner une valeur, ou bien de refuser l'intégration.

NOMTF

ECR

Ecrire au terminal les 101 valeurs de fiabilité calculées pour la génération des courbes, si PLOT est active. PLOT provoque en effet un changement de valeur de STEP, de telle manière qu'il y ait 101 points.

La valeur de STEP est restaurée en fin d'écriture sur le fichier de données.

Cette commande implique PLOT par défaut.

NOECR Constitue l'option par défaut et implique PLOT.

GO

Déclanche l'exécution dès son apparition. Cette commande a le même effet que l'envoi d'une ligne blanche.

Commandes de fin d'exécution

A la fin d'une exécution on peut spécifier un autre paramètre, pour la ou les équations, avec les mêmes valeurs ou bien demander une nouvelle exécution avec d'autres commandes et d'autres équations, soit par le système question-réponse, soit par l'une des 3 commandes :

NPAR : - Spécification d'un nouveau paramètre

NRUN : - Nouvelle exécution du programme avec d'autres données

END ou ligne blanche : - Fin de session.

A5 - 4. EXEMPLE

Il s'agit d'un système à remplacement que l'on désire étudier entre T = 2 et T = 6. Les valeurs des paramètres sont rentrées par une NAMELIST. Le taux de panne des éléments actifs est de 1,25, celui des modules de secours est de 1,35 fois plus faible. On étudie le système avec 1, 2 ou 3 modules de secours.

Les commandes sont : DIFF, MMT1, MMT2, GO.

```
15:30:09 LOAD MAIN CARE1 CARE2 CARE3 CARE4
15:30:20 START
EXECUTION BEGINS...
RUN OPTIONS ?
diff nmt1     nmt2  go
EQ.NUMBER?-COL.1
2
VARIABLES FOR EQ. 2?-$VAR-COL.2
 $var
 b=15.0
 t=0
 min=2
 lambda=1.25
 k=1.35
 s=1,2,3
 $end
ALT.$LIST?-YES/NO
n
INPUT THE FOLLOWING 4 VARIABLES EACH WITH FORMAT F8.0
COLUMNS  1-8  - REFERENCE RELIABILITY R2
COLUMNS  9-16 - MINIMUM RELIABILITY R1
COLUMNS 17-24 - MAXIMUM RELIABILITY R1
COLUMNS 25-32 - RELIABILITY R1 STEP SIZE
1.0      0..02      0.8      0.2
PARAMETER?
s
```

CALCULATIONS FOR EQUATION 2A (* MEANS NOT COMPUTED)

PARAMETER IS S

LAMBDA	MU	S	N	K	COST
.1250000D 01	.9259259D 00	1	***	.1350000D 01	.2000000E 01

C	KV	Z	W	P	MUT
.1000000D 01	.1000000D 01	1	1	**********	**********

T	REL	UNREL	SIMREL	SIMGAIN	SIMRIF
2.000	0.1755078	0.8244922	0.0820850	.2138124E 01	.1113309E 01
3.000	0.0532927	0.9467074	0.0235177	.2200002E 01	.1031450E 01
4.000	0.0156101	0.9843899	0.0007379	.2310747E 01	.1009012E 01
5.000	0.0045111	0.9954889	0.0019305	.2330824E 01	.1002592E 01
6.000	0.0012900	0.9987032	0.0005531	.2344781E 01	.1000744E 01

MEAN TIME TO FAILURE - MTF = .12595745E 01
UPPER LIMIT FOR INTEGRATION - B = .33750000E 02
RELIABILITY AT MTF = .39962115E 00

MAXIMUM MISSION TIME REFERENCE R2 = 1.00000

R1	SIMTMAX	TMAX	SIMTIF
0.20000	.1287550E 01	.1886948E 01	.1405533E 01
0.40000	.7330326E 00	.1258712E 01	.1717129E 01
0.60000	.4080065E 00	.8495842E 00	.2078948E 01

CALCULATIONS FOR EQUATION 2A (* MEANS NOT INPUTED)
PARAMETER IS S

LAMBDA	MU	S	N	K	COST
.1250000D 01	.9259259D 00	2	***	.1350000D 01	.3000000D 01

C	RV	Z	W	P	MLT
.1000000D 01	.1000000D 01	1	1	**********	**********

T	REL	UNREL	SINREL	SINGAIN	SINTIF
2.000	0.2680513	0.7319487	0.0820850	.3265534E 01	.1254069E 01
3.000	0.0861029	0.9138971	0.0235177	.3661188E 01	.1068481E 01
4.000	0.0257781	0.9742219	0.0067379	.3825814E 01	.1019544E 01
5.000	0.0075138	0.9924862	0.0019305	.3892267E 01	.1005025E 01
6.000	0.0021674	0.9978326	0.0005531	.3918790E 01	.1001617E 01

MEAN TIME TO FAILURE - MTF = .15819625E 01
UPPER LIMIT FOR INTEGRATION - B = .33750000E 02
RELIABILITY AT MTF = .41190148E 00

MAXIMUM MISSION TIME REFERENCE R2 = 1.00000

R1	SINTMAX	TMAX	SINTIF
0.20000	.1287550E 01	.2268368E 01	.1761770E 01
0.40000	.7330326E 00	.1611836E 01	.2198860E 01
0.60000	.4086605E 00	.1168728E 01	.2859899E 01

MAXIMUM MISSION TIME FOR S = 0.100000D 01
AND S = 0.200000D 01 FOLLOWS FOR EQUATION 2 A
REFERENCE R2 = 1.00000

R1	TMAX1	TMAX2	RATIF
0.20000	0.1886948E 01	0.2268368E 01	0.1202136E 01
0.40000	0.1258712E 01	0.1611836E 01	0.1280544E 01
0.60000	0.8495842E 00	0.1168728E 01	0.1375047E 01

DIFF, RIF, AND GAIN FOR S = 1.000000
AND S = 2.000000 FOLLOWS FOR EQUATION 2A

T	DIFF	RIF	GAIN
2.00000	0.925435E-01	0.112643E 01	0.152729E 01
3.00000	0.328102E-01	0.103590E 01	0.161500E 01
4.00000	0.101680E-01	0.101044E 01	0.165137E 01
5.00000	0.300271E-02	0.100303E 01	0.166562E 01
6.00000	0.870560E-03	0.100087E 01	0.167128E 01

CALCULATIONS FOR EQUATION 2A (* MEANS NOT INPUTED)
PARAMETER IS S

LAMBDA	MU	S	N	K	COST
.1250000D 01	.9259259D 00	3	***	.1350000D 01	.4000000D 01

C	RV	Z	W	P	MLT
.1000000D 01	.1000000D 01	1	1	**********	**********

T	REL	UNREL	SINREL	SINGAIN	SINRIF
2.000	0.3551726	0.0448274	0.0820850	.4320890E 01	.1423505E 01
3.000	0.1204630	0.8795370	0.0235177	.5122215E 01	.1110223E 01
4.000	0.0368527	0.9631473	0.0067379	.5469432E 01	.1031206E 01
5.000	0.0108342	0.9891659	0.0019305	.5612228E 01	.1009001E 01
6.000	0.0031356	0.9968643	0.0005531	.5669639E 01	.1002530E 01

MEAN TIME TO FAILURE - MTF = .18302384D 01
UPPER LIMIT FOR INTEGRATION - U = .33750000D 02
RELIABILITY AT MTF = .41841908E 00

MAXIMUM MISSION TIME REFERENCE R2 = 1.00000

R1	SINTMAX	TMAX	SINTIF
0.20000	.1287550E 01	.2549045E 01	.1979703E 01
0.40000	.7330320E 00	.1877712E 01	.2501500E 01
0.60000	.4080605E 00	.1410170E 01	.3465409E 01

MAXIMUM MISSION TIME FOR S = 0.200000E 01
AND S = 0.300000D 01 FOLLOWS FOR EQUATION 2 A
REFERENCE R2 = 1.00000

R1	TMAX1	TMAX2	RATIF
0.20000	0.2268300E 01	0.2549045E 01	0.1123734E 01
0.40000	0.1611830E 01	0.1877712E 01	0.1164951E 01
0.60000	0.1108728E 01	0.1410170E 01	0.1211723E 01

DIFF, RIF, AND GAIN FOR S = 2.000000
AND S = 3.000000 FOLLOWS FOR EQUATION 2A

T	DIFF	RIF	GAIN
2.00000	0.871214E-01	0.113511E 01	0.132502E 01
3.00000	0.343601E-01	0.103907E 01	0.139906E 01
4.00000	0.110740E-01	0.101150E 01	0.142961E 01
5.00000	0.332031E-02	0.100330E 01	0.144189E 01
6.00000	0.968367E-03	0.100037E 01	0.144678E 01

REQUEST?
end
R; T=5.74/8.89 15:40:38

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Président : M. Philippe TRAYNARD

Vice-Président : M. Pierre-Jean LAURENT

PROFESSEURS TITULAIRES

MM.	BENOIT Jean	Radioélectricité
	BESSON Jean	Electrochimie
	BLOCH Daniel	Physique du solide
	BONNETAIN Lucien	Chimie Minérale
	BONNIER Etienne	Electrochimie et Electrométallurgie
	BOUDOURIS Georges	Radioélectricité
	BRISSONNEAU Pierre	Physique du solide
	BUYLE-BODIN Maurice	Electronique
	COUMES André	Radioélectricité
	DURAND Francis	Métallurgie
	FELICI Noël	Electrostatique
	FOULARD Claude	Automatique
	LESPINARD Georges	Mécanique
	MOREAU René	Mécanique
	PARIAUD Jean-Charles	Chimie-Physique
	PAUTHENET René	Physique du solide
	PERRET René	Servomécanismes
	POLOUJADOFF Michel	Electrotechnique
	SILBER Robert	Mécanique des Fluides

PROFESSEUR ASSOCIE

M.	ROUXEL Roland	Automatique

PROFESSEURS SANS CHAIRE

MM.	BLIMAN Samuel	Electronique
	BOUVARD Maurice	Génie Mécanique
	COHEN Joseph	Electrotechnique
	LACOUME Jean-Louis	Géophysique
	LANCIA Roland	Electronique
	ROBERT François	Analyse numérique
	VEILLON Gérard	Informatique Fondamentale et Appliquée
	ZADWORNY François	Electronique

MAITRES DE CONFERENCES

MM.	ANCEAU François	Mathématiques Appliquées
	CHARTIER Germain	Electronique
	GUYOT Pierre	Chimie Minérale
	IVANES Marcel	Electrotechnique
	JOUBERT Jean-Claude	Physique du solide
	MORET Roger	Electrotechnique Nucléaire
	PIERRARD Jean-Marie	Mécanique
	SABONNADIERE Jean-Claude	Informatique Fondamentale et Appliquée
Mme	SAUCIER Gabrièle	Informatique Fondamentale et Appliquée

MAITRE DE CONFERENCES ASSOCIE

M. LANDAU Ioan	Automatique

CHERCHEURS DU C.N.R.S. (Directeur et Maître de Recherche)

MM. FRUCHART Robert	Directeur de Recherche
ANSARA Ibrahim	Maître de Recherche
CARRE René	Maître de Recherche
DRIOLE Jean	Maître de Recherche
MATHIEU Jean-Claude	Maître de Recherche
MUNIER Jacques	Maître de Recherche

dernière page de la thèse

AUTORISATION DE SOUTENANCE

VU les dispositions de l'article 3 de l'arrêté du 16 avril 1974,

VU les rapports de présentation de

Madame G. SAUCIER, Maître de Conférences I.N.P. GRENOBLE

Monsieur A. COSTES, Maître de Conférences I.N.P. TOULOUSE,

Monsieur C O U R T O I S Bernard

est autorisé à présenter une thèse en soutenance pour l'obtention du diplôme de DOCTEUR-INGENIEUR, spécialité "GENIE INFORMATIQUE".-

Fait à Grenoble, le 23 Novembre 1976

Le Président,