COLLOQUE NATIONAL SUR LE TRAITEMENT DU SIGNAL
ET SES APPLICATIONS

NICE du 26 au 30 AVRIL 1977

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT (C.O.P.R.A.)

Messieurs MERAUD et BROWAEYS (S.A.G.E.M.)
" GERMAIN et HERCLET (E.M.D.)

S.A.G.E.M. 16, avenue d'Iéna 75 016 - PARIS

E.M.D. 55, quai Carnot 92 210 - SAINT-CLOUD

RESUME

Le projet COPRA (Calculateur à Organisation Parallèle Reconfigurable Automatiquement) a pour objectif la réalisation d'un multiprocesseur parallèle à haute sûreté de fonctionnement destiné à des applications temps réel pouvant comporter du traitement de signal. Il est exécuté sur contrat D.R.M.E. et représente l'aboutissement d'études menées depuis plusieurs années par la SAGEM (projet SAPHIR) et par l'EMD (projet MECRA).

Les caractéristiques essentielles résultent d'un compromis entre l'état de l'art en matière de tolérance aux pannes et les possibilités de la technologie disponible. Dans ce but la structure est découpée en modules macro-fonctionnels. Ceci facilite l'utilisation des circuits LSI conventionnels les plus intéressants comme le microprocesseur AMD en cours de francisation, ou l'adaptation des modules aux spécifications particulières des applications (implantation de multiplicateurs câblés pour le traitement de signal) ou enfin la réactualisation technologique des modules.

Les composants utilisés n'offrent pas par eux-mêmes de facilité de détection des erreurs. Les techniques de détection et de reconfiguration sont mises en oeuvre au niveau des interfaces des modules. Le recouvrement d'une erreur se fait par reprise automatique de la séquence en cours en un temps de l'ordre de la micro seconde.

L'implantation de l'application doit se faire obligatoirement avec un découpage en tâches hiérarchisées selon leur caractère vital. Ceci permet une éventuelle dégradation contrôlée de la mission en fonction du nombre et de la nature des pannes.

SUMMARY

The goal of the COPRA (Calculateur à Organisation Parallèle Reconfigurable Automatiquement) project is the designing of a highly reliable parallel multiprocessor designed for real time application. This project, sponsored by the D.R.M.E. (Direction des Recherches et Moyens d'Essais) is the outcome of studies conducted for several years by SAGEM and EMD.

The main features result in a trade off between the state of the art in fault tolerance and the available technology. The computer is split into functional cells. This allows the use of on the shelf LSI components and the use of special purpose cells such as hardware multipliers.

The component used does not have any detection of their own. The detection and reconfiguration are implemented at the interface module level. The failure recoveries are done automatically through a rollback of the sequence executed. This rollback last a few micro seconds.

The application is split into tasks depending on their safety requirement. This allows an eventual degradation of the mission depending on the failures.

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT

(C.O.P.R.A.)

Le calculateur COPRA à Organisation Parallèle et Reconfiguration Automatique est le résultat d'une collaboration entre les sociétés SAGEM et EMD, travaillant sous contrat de la D.R.M.E. (Direction des Recherches et Moyens d'Essais).

L'objectif est d'offrir une gamme continue et compatible d'unités centrales embarquables capables d'offrir une haute sûreté de fonctionnement pour permettre la réalisation des futurs systèmes intégrés de conduite des processus.

COPRA a une structure multiprocesseur reconfigurable. Une telle structure est susceptible de couvrir un domaine assez large d'applications, tant en ce qui concerne la puissance de traitement que la sûreté de fonctionnement.

Le traitement des erreurs est global et automatique. Il est réalisé de manière transparente à l'utilisateur. Toutes les composantes de la sûreté de fonctionnement sont accrues : fiabilité, disponibilité, sécurité, crédibilité et maintenabilité. Le logiciel est lui-même conçu pour limiter les causes et les effets des erreurs de programmation.

Les possibilités de dégradation progressive existant dans COPRA permettent de calculer les configurations en fonction des exigences de l'application complète ou de manière plus spécifique en accroissant différemment la sûreté de fonctionnement pour les diverses tâches de l'application.

Au niveau des entrées/sorties, la sécurité des liaisons est assurée par l'utilisation de bus multiplexés reconfigurables à grande sûreté.

1. OBJECTIFS DE FIABILITE

Ils concernent principalement l'amélioration de la sécurité, de la disponibilité et de la maintenabilité et l'établissement d'une méthode de calcul de ces paramètres.

LA SECURITE

Sur un calculateur conventionnel, il est possible d'améliorer la sécurité au niveau du logiciel en effectuant des contrôles s'appuyant sur les spécificités de l'application, ou bien en entrelaçant l'autotest du calculateur avec une répétition des calculs.

L'efficacité de ces solutions est difficile à établir. En outre, elles accroissent le volume de mémoire et diminuent les performances. Enfin, le logiciel est plus coûteux et irrécupérable pour une autre application.

Sur le calculateur COPRA, la sécurité est une caractéristique indépendante du logiciel d'application. Elle s'apprécie par une crédibilité (taux d'erreurs non détectées) qui est sensiblement constante dans le temps et inférieure à 8.10^{-8} par heure de fonctionnement.
Une crédibilité élevée, sur un matériel spécialement conçu, implique l'existence de circuits détecteurs d'erreurs surveillant le flux des opérations pour bloquer celui-ci à la première faute. On évite ainsi la propagation de celle-ci et le risque de production d'un évènement catastrophique (passivation des pannes).

LA DISPONIBILITE

Elle caractérise le rapport temps de service sur temps de mission. Elle est plus particulièrement recherchée pour les missions longues (Applications spatiales, marines, télécommunications, contrôle de processus continu, etc...).

Pour accroître la disponibilité, on a très tôt cherché à dupliquer les équipements conventionnels de l'installation centrale en leur adjoignant des dispositifs de reconfiguration et de reprise, manuels ou automatiques.

L'avantage de ces solutions reconfigurables réside dans les économies de matériel que l'on peut faire en exploitant les possibilités de dégradation progressive de la mission. En effet, dans les conditions normales, les deux calculateurs sont rentabilisés par l'exécution de tâches distinctes. A la suite de la défaillance de l'un d'eux, seules les tâches essentielles sont conservées. Dans ce mode on pourra attendre l'intervention chargée de rétablir manuellement l'intégrité du système.

L'inconvénient majeur des solutions réalisées avec des matériels conventionnels est l'accroissement très important de complexité de l'étude d'application. Il faut en effet faire dialoguer les calculateurs, résoudre le difficile problème des reprises des travaux après incident, vérifier de façon efficace les résultats, avant toute modification irréversible du processus, etc...

En outre, les solutions sont spécifiques de l'application et le gain de fiabilité est difficile à établir.

Le calculateur autoreconfigurable COPRA ne présente pas ces inconvénients parce que les mécanismes de reprise et de reconfiguration sont des caractéristiques de fonctionnement du calculateur qui n'interfèrent pas avec la programmation de l'application.

L'ordre de grandeur des gains de disponibilité apportés par la structure COPRA avec les technologies avions usuelles par rapport à un calculateur conventionnel de 1500 heures de MTBF, est de l'ordre 600 pour des missions de 1 à 10 heures.

LA MAINTENABILITE

Elle caractérise le coût des opérations d'entretien. Ce coût est diminué dans les applications embarquées par la mise en oeuvre des mécanismes de reconfiguration automatique de COPRA qui sont de véritables processus de réparation automatique exploitant le stock des rechanges implantées dans la configuration d'origine. Cette faculté permet de disposer d'un délai important pour les interventions manuelles afin de supprimer l'obligation d'une infrastructure logistique de maintenance décentralisée et donc coûteuse.

CALCUL DE LA FIABILITE PREVISIONNELLE

Ce calcul, fondamental pour la justification des solutions proposant l'utilisation d'un calculateur tolérant les pannes (F.T.C), est évidemment plus complexe que dans le cas d'un calculateur conventionnel.

La méthode de calcul détermine d'abord pour chaque module constituant le calculateur le taux de panne de ses différentes fonctions par les procédés classiques partant des taux de panne des matériels correspondants.

Les paramètres significatifs d'un module sont: la fonction principale (traitement, mémoire, échange, alimentation, horloge) la détection d'erreur et la passivation des pannes.

On établit ensuite le graphe des enchaînements d'états consécutifs à l'apparition des pannes en partant de l'état initial de bon fonctionnement de l'ensemble.

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT
(C.O.P.R.A.)

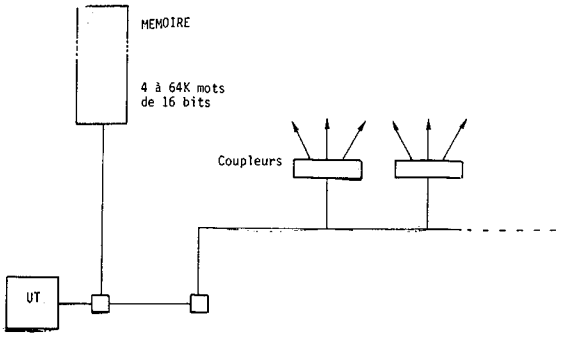


FIGURE 1 - MONOPROCESSEUR CONVENTIONNEL

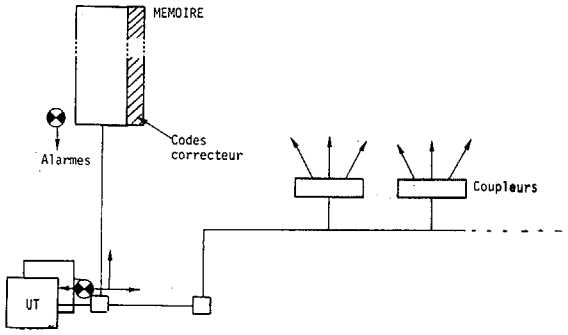
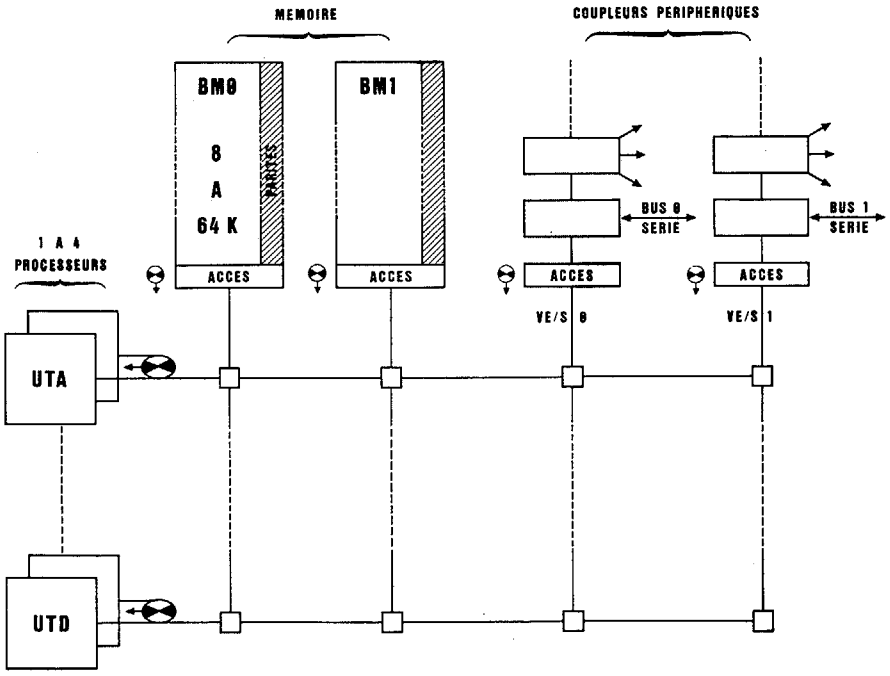


FIGURE 2 - MONOPROCESSEUR HAUTE SECURITE TOLERANT LES TRANSITOIRES

- **1 à 4 processeurs duplex de 300 K.O.P.S. chacun**
- **8 à 64 K mots de 16 bits en mémoire centrale duplex**
- **Programmation structurée surveillée dynamiquement**
- **Système de gestion multitâche temps réel**



Par heure, pour un biprocesseur de 20 K mots utiles:

- **insécurité : 8.10^{-8} (erreurs non détectées)**
- **indisponibilité : 9.10^{-7}**

- **Résistance aux transitoires d'environnement par reprise automatique**
- **Survie à toute première panne de composant au moins**
- **Dégradation contrôlée par reconfiguration des tâches sur incident**

FIGURE 3 - SYNOPTIQUE GENERAL

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT

(C.O.P.R.A.)

Ce graphe et les taux de panne précédemment calculés permettent d'établir la matrice des probabilités de transition d'état. On exploite ensuite cette matrice sur ordinateur à l'aide des méthodes numériques de traitement des processus de Markov pour en déduire les probabilités d'apparition des états terminaux du graphe (panne non détectée, perte totale signalée, pertes partielles).

L'ordre de grandeur des résultats peut être retrouvé par des calculs simplifiés car l'architecture de COPRA se prête à une découpe en un petit nombre de sous-ensembles fonctionnels.
Cette méthode suppose évidemment que l'ensemble est sans vices résiduels de conception, et en particulier qu'il n'y a pas de fautes dans le logiciel.

La satisfaction de cette hypothèse nécessite l'exécution d'une campagne d'essais exhaustifs de certification.

2. DESCRIPTION GENERALE (figure 3)

Afin de favoriser l'utilisation des techniques de reconfiguration et de dégradation de performances après pannes, tout en offrant une structure parallèle, COPRA est un multiprocesseur banalisé. Toutes les unités de traitement (UT) sont identiques pour être interchangeables.

La structure est composée des modules suivants :

- une à quatre unités de traitement microprogrammées. Elles assurent le traitement des instructions, des 8 niveaux d'interruption, des bus multiplexés, des erreurs et de la fonction canal. Elles utilisent les techniques LSI,
- un à deux bancs mémoires adressables par mot de 16 bits. Ils ont une capacité maximum de 64 K. Ils utilisent des circuits intégrés RPROM et des RAM en MOS et CMOS, mais peuvent aussi utiliser des mémoires à tores en option,
- une à deux voies d'entrées/sorties. Elles peuvent être utilisées soit en mode canal, soit en mode liaison programmée. Dans ce dernier mode, elles reçoivent notamment l'ensemble des signaux discrets regroupés par niveaux d'interruption.

Dans COPRA, le découpage est exécuté au niveau de cellules fonctionnelles de tailles importantes pour les raisons suivantes :

- il diminue le poids des interconnexions,
- il diminue le pourcentage de matériel non redondant dévolu au système de détection d'erreur et de reprise, diminuant ainsi l'importante du matériel critique (hardcore)
- il facilite l'utilisation de circuits LSI standards (microprocesseurs), l'adaptation des cellules à des spécifications particulières, et leur réalisation technologique.

Si on négligeait le poids des interconnexions, l'accroissement de la finesse du découpage améliorerait le taux de reconfiguration, donc la résistance aux pannes. En réalité, un découpage trop fin du calculateur rend difficile sinon impossible l'utilisation pour des fonctions annexes du matériel de secours, ce qui accroit le coût de la redondance.
D'autre part, la machine doit être capable en cas d'incident d'exécuter une reconfiguration. Si à la suite d'un découpage trop fin du calculateur, il n'existe aucune cellule fonctionnelle capable d'exécuter ce travail, il serait nécessaire de créer une unité spéciale de reconfiguration ce qui alourdirait considérablement la structure.

Le fonctionnement de cette machine repose sur les principes suivants :

- une interconnexion matricielle permet une liaison point à point de chaque module "unité de traitement" (UT) avec n'importe lequel des autres modules, blocs mémoire (BM) et voie d'entrée/sortie (VE/S),
- toutes les UT peuvent dialoguer simultanément avec des BM ou VES distincts. Les liaisons point à point évitent les problèmes de partage de bus (débit global et fiabilité insuffisants),
- l'accès à un BM ou une VE/S n'est autorisé, à un instant donné, qu'à une seule UT à la fois. Dans ce but, un interface standard d'exclusion (composé d'un circuit de priorité circulante) est associé à chaque BM,
- tous les modules d'un même type sont physiquement identiques. En particulier il n'existe pas d'UT maître et BM spécifiquement système.Les traitements propres au système ou à l'application peuvent donc être exécutés par n'importe quelle UT. La mémorisation des informations correspondantes peut également être faite dans n'importe quel BM. De même, les VE/S sont totalement banalisées,
- toutes les configurations que peut prendre cette structure, de la configuration minimum comprenant 1 UT, 1 BM et 1 VE/S, à la configuration maximum à 4 UT et 2 BM ou VE/S, ne se distinguent que par leur puissance, la machine virtuelle restant la même dans tous les cas.

Cette structure présente l'intérêt suivant :

- elle possède les avantages propres à toute structure multiprocesseur : modularité de la puissance et bonne adéquation aux technologies LSI (peu de types différents de composants, et composants d'un même type employés en plusieurs exemplaires),
- elle se présente comme une structure à redondance active.

Du point de vue de la sûreté de fonctionnement, tous les modules peuvent être considérés comme des ressources de réserve. A ce niveau, il y a donc identité du matériel fonctionnel et du matériel redondant. Le coût de ce dernier est en conséquence moins élevé que dans une structure redondante classique où les redondances ont pour unique fonction la tolérance aux pannes.

Cette redondance structurelle, exploitée par des mécanismes de reconfiguration automatique décrits plus loin, fait de COPRA un calculateur dont la fiabilité et la disponibilité - comme la puissance - peuvent être taillées "sur mesure" en fonction des exigences des applications. Les figures 1, 2 et 3 illustrent différentes configurations allant de la plus simple, qui est monoprocesseur et non redondante, à la plus puissante à 4 processeurs capable de survivre à plusieurs pannes puis de passiver les suivantes.

3. SURETE DE FONCTIONNEMENT

Elle utilise le principe de l'implantation de redondances actives et de la détection d'erreur.

Le mécanisme met en jeu une chaîne allant de la détection à la reconfiguration et la reprise, en passant par le diagnostic et les réessais pour filtrer les transitoires.

Une sécurité élevée est assurée par une détection simple, efficace et autotestée.

Tous les maillons de la chaîne détection-réessais-diagnostic-reconfiguration-reprise, sont mis en oeuvre automatiquement au niveau du matériel de la microprogrammation ou du logiciel système sans imposer une

programmation particulière à l'utilisateur.

En particulier, ce dernier n'a pas à se préoccuper des procédures de test ou de diagnostic, ni de l'implantation des points de reprise.

Cette implantation est réalisée automatiquement à l'assemblage. Elle consiste à découper les programmes en séquences répétables à partir de l'état courant de la mémoire et des valeurs sauvegardées des registres UT au début de la séquence. Une instruction de point de reprise est injectée en début de séquence pour commander l'exécution de ces sauvegardes.

La seule contribution de l'utilisateur est située dans le choix des stratégies de dégradation à mettre en oeuvre après la perte d'un module. Ces stratégies dépendent en effet de la nature de l'application et se situent à un niveau logique qui ne peut pas être pris en compte par le système seul.

FIABILISATION DES UNITES DE TRAITEMENT

Détection des fautes

Une unité de traitement est constituée de deux unités identiques, sruveillées par comparaison des sorties (information et commandes).

Passivation des pannes

Tout désaccord entre les unités de traitement génère un signal d'erreur qui inhibe l'utilisation du bus pour empêcher la propagation.

Ce signal commande la génération d'un cycle d'attente de protection du calculateur pendant le passage de l'éventuelle perturbation cause de l'erreur.

A la fin de ce cycle, toutes les UT exécutent le microprogramme de reprise après effacement des bascules de mémorisation de l'alarme.

L'état "reprise en cours" est mémorisé pour l'ensemble des UT. Si en cours de reprise une panne réapparait elle est cette fois interprétée comme une panne permanente de l'UT. Ce signal commande le basculement en position "H.S" du bistable magnétique de mémorisation de panne. L'UT n'est alors plus alimentée ce qui l'isole électriquement par ses sorties 3 états.

Reconfiguration

L'état "H.S" du bistable se présente en interruption aux autres UT. L'une d'entre elles, démasquée à cette IT, se chargera du recouvrement des tâches abandonnées.

FIABILISATION DES ACCES AUX MEMOIRES ET AUX VE/S

Ces logiques d'accès étant identiques sont traitées ensemble dans ce qui suit.

Détection des fautes

L'information est surveillée par 4 bits de parité émis ou contrôlés par l'UT selon le sens de l'échange.

L'efficacité de ce contrôle est assurée par un découpage en tranche de 4 bits du matériel traversé par l'information jusqu'à son exploitation dans le module.

Les commandes arrivent dupliquées en provenance des UT maîtres et esclaves.
La surveillance s'effectue par comparaison des sorties entre les chaînes de commande maître et esclaves. Le résultat est retourné en alarme aux UT.

Toute erreur est, en l'absence d'erreur de l'UT, attribuée par celle-ci au module mémoire ou voie d'entrée/sortie avec lequel elle dialogue.

Toute demande d'accès ou attente de fin de cycle qui déborde d'une constante de temps fixée est également attribuée par l'UT au module attendu.

L'UT qui reçoit en outre le retour alarme de la surveillance des chaînes de commande, détermine donc totalement les fautes des autres modules avec lesquels elle dialogue et peut donc initier la procédure de reprise automatique ou de reconfiguration.

Découplage des pannes d'interconnexions

Les bus A, B (jusqu'à C ou D s'il y a 3 ou 4 processeurs) n'ont aucun circuit en commun.

Il n'y a donc pas de configuration de panne simple de composant pouvant compromettre l'exploitation de plus d'un bus et entraîner une panne catastrophique. Une telle panne en effet ne serait possible que par commande de fermeture des sorties à la fois sur les bus A et B. Les boîtiers d'interface n'exécutant cette commande que sur condition d'existence d'une demande de sélection sur le bus correspondant, cette configuration ne peut apparaître avec une panne simple.

En conclusion, le réseau d'interconnexion n'est pas un matériel critique. La panne d'un noeud de la matrice d'interconnexion ne peut dans le cas le plus défavorable, que mettre en panne la ligne et la colonne correspondantes, soit par une altération (collage à 0 ou à 1) des entrées et des sorties du boîtier d'interconnexion soit par un blocage à l'état fermé d'un ou de plusieurs interrupteurs ou de leurs commandes.

Passivation d'un module mémoire ou VE/S

Après un diagnostic de panne permanente réalisé par une UT, celle-ci commande la mise "hors service" du module correspondant en forçant le basculement du bistable magnétique d'isolement. Le retour à l'état travail ne peut se faire désormais que par une intervention de la maintenance sur la prise de test extérieure. Dans cet état le module, privé d'alimentation, est isolé électriquement du reste de la structure au niveau de ses boîtiers d'interfaces à sorties 3 états.

L'état "H.S" du bistable d'isolement est retourné à l'UT pour masquer l'adressage du module.

FIABILISATION DE LA MEMOIRE

Détection des erreurs

La détection des fautes est assurée à la lecture dans l'UT par l'exploitation du code de parité 4 bits associé aux 16 bits d'information. La décomposition en tranches de 4 bits de la mémoire assure la détection de toute faute provenant du malfonctionnement d'un circuit.

Diagnostic et passivation des pannes permanentes

Toute erreur mémoire détectée déclenche une reprise immédiate des séquences en cours sur les UT dans un mode reprise mémorisant une erreur d'origine mémoire. Cette reprise est identique à celle qui est effectuée à la suite d'une erreur d'UT.

Si en cours de reprise une erreur mémoire est détectée par une UT, celle-ci commande le basculement du bistable d'isolement déjà cité de l'accès à cette mémoire.

Reconfiguration de la mémoire

La transmission comme on l'a vu dans les UT de la posi-

tion "H.S" du bistable de l'accès mémoire réalise le masquage de l'adressage de cette mémoire dans les opérations d'écriture et de lecture.

Remarques

1. Les fautes de mémoires n'étant constatées qu'en lecture peuvent provenir d'une erreur transitoire d'écriture mémorisée dans la partie RAM. Ces erreurs éventuelles sont filtrées par réactualisation automatique microprogrammée de la position fausse à partir de la position image sur la copie.

2. Il est inutile pour des missions courtes, de recycler périodiquement un test d'état de l'information mémorisée car le calcul montre que la probabilité de panne double sur la même position des deux copies est négligeable.

Pour les missions longues de type marine, ce test périodique à faire en même temps que l'autotest de la machine complète doit être recyclé toutes les quelques heures à des instants qui ne perturbent pas l'exécution de la mission.

FIABILISATION DES ENTREES/SORTIES

Elle est réalisée au moyen des mécanismes suivants :

- pour les interruptions par duplication et transmission à toutes les U.T, Celles-ci les exploitent à travers un masque de reconfiguration modifiable par programmation,
- pour les voies d'entrées/sorties par duplication et comparaison,
- pour les autres E/S, le filtrage des erreurs et pannes étant tributaire de l'application est traité par le logiciel à l'aide des données du mot d'état indiquant les conditions dans lesquelles s'est exécuté un échange. Le logiciel décide des répétitions ou reconfigurations nécessaires.

SURVEILLANCE DES ALIMENTATIONS ET SERVITUDES

Passivation des courts-circuits

Chacune des deux alimentations suffit à délivrer la puissance utile nécessaire au fonctionnement normal du calculateur. Une diode de puissance en sortie protège chaque alimentation contre la défaillance de l'autre. En fonctionnement normal, chaque voie ne délivre que la moitié de sa puissance nominale ce qui accroit sa fiabilité.

La protection contre les courts-circuits est disposée dans chaque carte module. Elle consiste en un détecteur de surintensité placé sur l'entrée d'alimentation de chaque module. Cette détection commande le basculement du bistable d'isolement sur la position panne affichée. L'alimentation du module est alors coupée. Les circuits d'interface sont choisis pour isoler le module dans la structure quand ils ne sont plus alimentés.
La protection contre les coupures ou d'autres perturbations du réseau est assurée dans l'alimentation par des détecteurs qui génèrent une IT de remise en route.

Les horloges et servitudes diverses représentent peu de matériel et sont fiabilisées par vote.

EVALUATION DE LA FIABILITE

Cette évaluation est faite au moyen d'un modèle markovien du comportement de la structure qui permet de suivre l'enchaînement des états de celle-ci à partir d'un état origine fixé et compte tenu du taux de panne de chaque composant.

Ce modèle est exploité à l'aide d'un programme écrit en Fortran.

Un extrait des résultats sous forme de courbes de sécurité et disponibilité est donné en figures 4 et 5.

Ces courbes correspondent à l'exemple de configuration donné au paragraphe 5. Il s'agit d'un bi-processeur muni d'une mémoire duplex de 20K mots utiles, capable au moins de résister à toute première panne et de passiver la suivante.

Les calculs ont été faits en fonction des recommandations de la norme MIL HDBK 217B, pour les conditions opérationnelles embarquées avec 50° d'ambiance. Les composants ont été choisis dans des séries usuelles fabriquées en grande série et correspondant à la catégorie B2 (Vendor équivalent).

Seuls quelques composants critiques (de l'ordre de 1% du matériel total) ont été choisis en classe A.

Les résultats peuvent être résumés par les chiffres suivants:

Insécurité

La crédibilité ou probabilité d'indétection d'une erreur par heure de fonctionnement est inférieure à 8.10^{-8}. Elle s'améliore légèrement avec le temps à cause de la diminution progressive du taux de panne du aux reconfigurations. Cette valeur est un majorant de l'insécurité.

Indisponibilité

La probabilité de perte totale ou de faute non détectée du calculateur pendant la première heure de fonctionnement est inférieure à 7.10^{-7}.

Pour les missions longues les résultats seraient meilleurs avec une version tri-processeur ou même quadri-processeur, associé à l'option de reconfiguration par pages de la mémoire. Le gain potentiel est limité à 10 avec les composants retenus.

4. CARACTERISTIQUES GENERALES

Caractéristiques fonctionnelles

Organisation	Monoprocesseur ou multiprocesseur reconfigurable (maximum : 4 processeurs, 2 bancs, 2 voies entrées/sorties multiplexées).
Type	Universel et microprogrammé utilisant le microprocesseur AMD 2900.
Parallèlisme	16 bits dans toute la machine
Format des opérandes - virgule fixe - virgule flottante	 16 bits et 32 bits 24 bits de mantisse et 8 bits d'exposant
Format des instructions	16 bits et 32 bits
Format des micro-instructions	48 bits

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT

(C.O.P.R.A)

Adressage	Segmenté. Table d'accès contrôlé aux segments (TAS) 5 bases (pointant en tête de segment ou d'espace local) 6 index Indirection
Registres généraux de calcul	8 (accumulateurs, index ou base)
Répertoire d'instructions	- répertoire fixe de 150 instructions - répertoire optionnel de 20 instructions (opérations flottantes, manipulation de caractères,...) - provision pour instructions spécifiques
Niveaux d'interruptions	8 dont 4 disponibles pour l'application

Performances d'un module UT	Registre à registre	Opérande en mémoire
Add, Su, Ld, St,..	0,9 µs	1,8µs
Mult Fixe	4,1 µs	4,8µs
Div. Fixe	5,3 µs	6 µs
Add, Su.flottante	7,1 µs	7,8µs
Multiplication flot.	11,1 µs	11,8µs
Division flottante	18,7 µs	19,4µs
Indexation	0,0 µs	
Indirection	0,4 µs	
Echanges		
- liaison programmée	40K mots/s	
- canal	300K mots/s	

Mémoire	
Technologie	Semi-conducteurs (tores en option)
Cycle	REPROM (0,8µs), RAM (0,4µs)
Modularité en capacité	2K mots (CI) (8K mots en tores)
Capacité maximale de la mémoire centrale	64K mots
Capacité maximale d'adressage en mémoire virtuelle	Pratiquement infinie grâce au système d'adressage basé sur segments

Sûreté de fonctionnement

Détection des erreurs en mémoire	Mémoire intégrée Par parité de 1 à 4 bits par mots de 16 bits, associée à une structuration en tranches de la mémoire Mémoire à tores Par combinaison de parités sur 4 bits par mots, adaptée à l'architecture de la mémoire.
Détection des erreurs de logique	Par système duplex comparé et dispositif écho, combiné avec un test périodique du matériel de détection
Survie aux pannes transitoires	Par reprise automatique de la séquence en cours sans changement de configuration
Survie aux pannes permanentes de processeur	Par reprise automatique de la séquence en cours sur l'un des processeurs restant disponibles
Survie aux pannes permanentes de la mémoire	Par reprise automatique à partir d'une copie si elle existe ou par reconfiguration des tâches
Dégradation contrôlée de la mission après panne	Elle a lieu tâche par tâche chaque fois que l'une d'elles cesse d'être exécutable, soit par perte d'un équipement extérieur soit par perte d'information mémoire, soit par faute de programmation, soit par pertes de processeurs. Les filiations logiques des tâches à arrêter sont déterminées automatiquement
Protection mémoire	- Protection écriture par segment - Protection d'accès à l'information par clés d'accès aux segments
Entrées/sorties	Par bus duplex multiplexé sur liaison programmée.
Temps de recouvrement d'une panne transitoire	De l'ordre d'une fraction de ms à quelques ms selon réglage de la constante de temporisation de protection.
Temps de recouvrement d'une panne permanente	De l'ordre d'une fraction de ms à quelques ms selon règlage de la constante de temporisation de protection

Par heure, pour un biprocesseur avec 20 K mots utiles.		
INSECURITE	8.10^{-8}	probabilité d'apparition d'une erreur non détectée
INDISPONIBILITE	7.10^{-7}	probabilité de perte ou de faute non vue du calculateur.

5. CARACTERISTIQUES D'UNE VERSION EMBARQUEE TYPE

Caractéristiques de configuration

La configuration illustrée par la figure 6 est un biprocesseur à deux bancs mémoires, correspondant à une organisation duplex. Elle comporte :

- 4 cartes modules UT formant les deux processeurs duplex UTA et UTB,
- 2 cartes modules mémoire à circuits intégrés de 20K mots, dont :
  - . 16K mots d'instructions et constantes
  - . 4K mots de zone de travail non volatile
- 1 carte module d'entrées/sorties duplex,
- 1 carte module alimentation et servitudes duplex.

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT

(C.O.P.R.A)

Caractéristiques de fiabilité

Cette configuration présente une insécurité inférieure à 8.10^{-8} et une indisponibilité inférieure à 9.10^{-7} pendant la première heure de fonctionnement.

Elle résiste aux fautes provenant des perturbations dues à l'environnement, par reprise automatique après une temporisation de protection suivant la détection d'erreur.

Elle survit à toute première panne de composant, puis encore à un certain nombre d'autres pannes tout en maintenant une sécurité élevée.

Le logiciel machine est structuré et dynamiquement surveillé pour permettre la détection d'un certain nombre de fautes usuelles de programmation. Ces fautes détectées conduisent à une reconfiguration des tâches et à l'exécution d'une mission de survie.

Maintenabilité

La reconfiguration automatique de la machine, au prix éventuellement d'une dégradation contrôlée de la mission, assure une réparation automatique tant que les redondances fonctionnelles vis-à-vis des tâches vitales ne sont pas épuisées.

Les dispositifs de survie aux pannes assurent en grande partie automatiquement la surveillance et le diagnostic de pannes. Chaque panne de module est signalée (qu'il s'agisse d'une panne franche ou qu'il s'agisse d'un taux de pannes transitoires ayant dépassé un seuil d'alerte).

On dispose donc d'un préavis pour réparer si les ressources restantes sont suffisantes pour assurer la prochaine mission avec la fiabilité normalement exigée. Un voyant magnétique visualise même hors tension la désélection du module défaillant. Au premier niveau de maintenance, il suffit de réaliser l'échange standard de ce module.

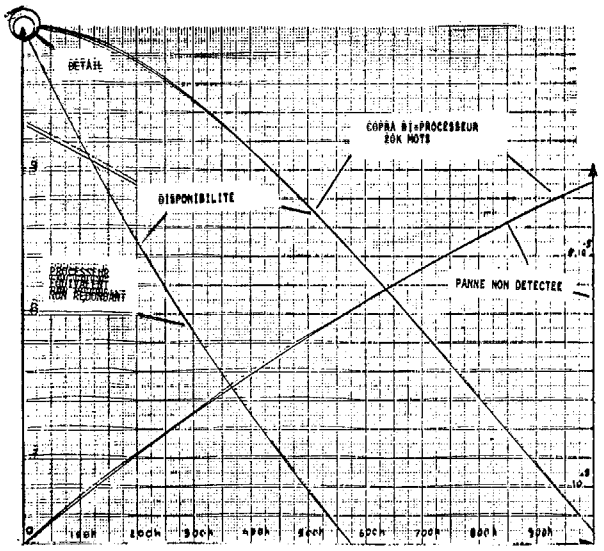


FIGURE 4

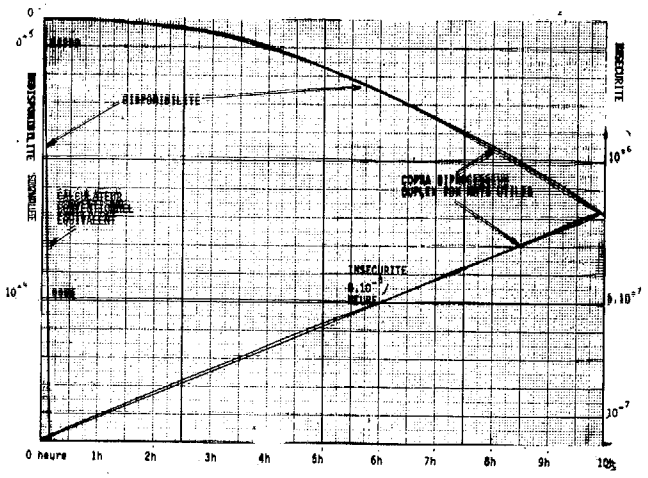


FIGURE 5

CALCULATEUR A ORGANISATION PARALLELE RECONFIGURABLE AUTOMATIQUEMENT

(C.O.P.R.A)

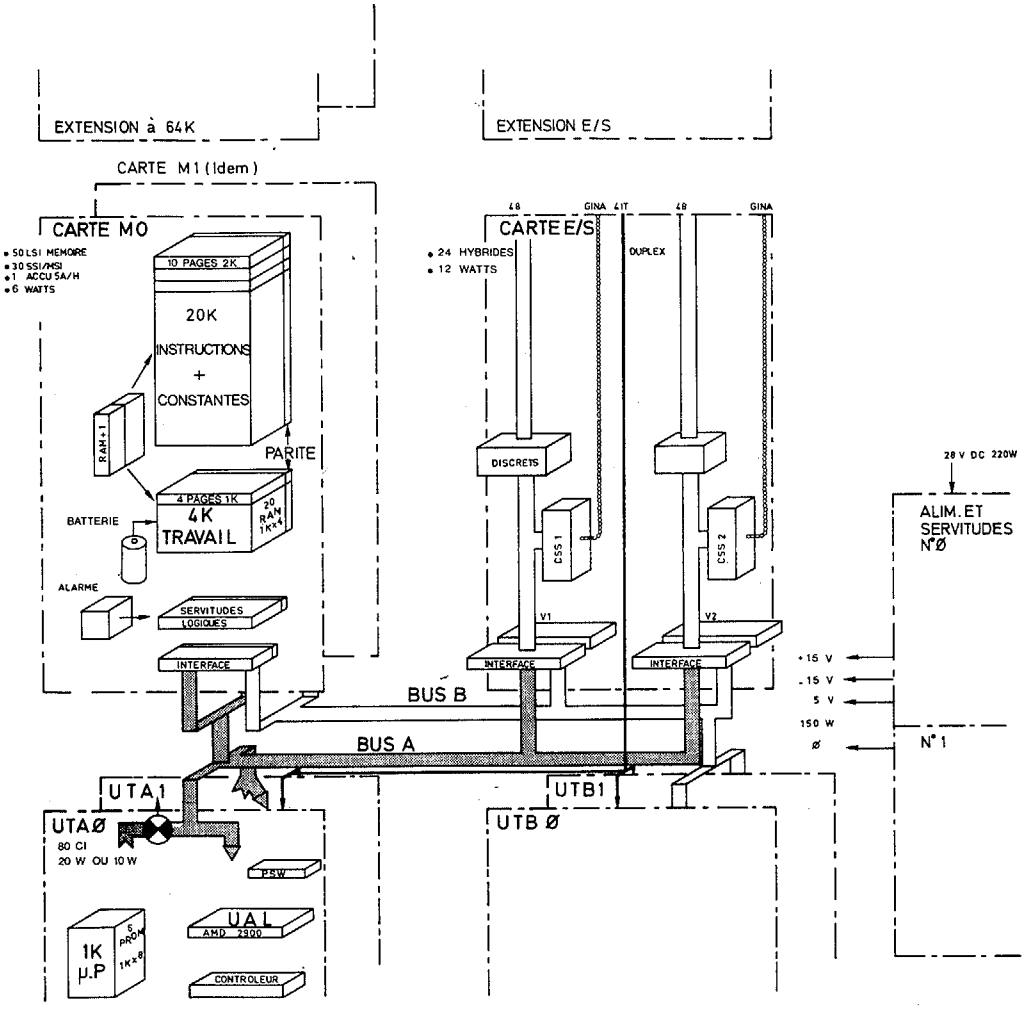


FIGURE 6 - COPRA - CONFIGURATION DU PROCESSEUR DUPLEX AVEC 24K MOTS UTILES