FR8002100

Ecole d'été franco-Yougoslave.
Dubrovnik, Yougoslavie, 23 - 28 Juin 1980.
CEA - CONF 5230

SYSTEMES PROGRAMMES POUR LA PROTECTION DES CENTRALES NUCLEAIRES

Pierre JOVER*

Résumé :

Les progrès accomplis dans le domaine des microprocesseurs et des circuits à large intégration associés ont conduit à introduire ces nouvelles tehnologies dans les systèmes de protection des centrales nucléaires. Après avoir rappelé brièvement les principes de conception du matériel et du logiciel pour les systèmes utilisant des microprocesseurs, on décrit un système de protection quadri-redondant, développé en FRANCE pour les centrales nucléaires PWR 1300 MWe.

PROGRAMMED SYSTEM FOR NUCLEAR POWER PLANT PROTECTION

Pierre JOVER*

Abstract :

The progress in the field of microprocessors and large scale integration circuits, have incited to introduce this new technologies into nuclear power plant protection system. The hardware and software design principles are briefly listed ; then, a quad-redundant protection system for 1300 MWe PWR, developped in FRANCE is described.

---

* Communication présentée par J. WEILL, Chef des Services d'Electronique de Saclay

SERVICES D'ELECTRONIQUE DE SACLAY
Service d'Instrumentation pour les
Applications Industrielles

PJ/CB

Saclay, le 27 mars 1980

SYSTEMES PROGRAMMES POUR LA PROTECTION DES CENTRALES NUCLEAIRES

par

Pierre JOVER

1. - INTRODUCTION

Les progrès accomplis dans le domaine des microprocesseurs et des circuits à large intégration associés, ont conduit à introduire ces nouvelles technologies dans les systèmes de protection des centrales nucléaires.

Les avantages que l'on attend de ces nouvelles techniques sont une amélioration de la sûreté de fonctionnement des systèmes de protection, donc une augmentation de la sûreté et de la disponibilité des centrales nucléaires, et aussi une simplification des équipements et installations.

Il est bien admis que les techniques programmées permettent de faire des calculs plus précis, ou de traiter des opérations logiques plus complexes que ne le permettent les techniques conventionnelles telles que amplificateurs opérationnels, ou opérateurs logiques câblés. Cependant, l'avantage principal apporté par les microprocesseurs est de permettre de bâtir des structures décentralisées avec des unités de traitement fonctionnant de façon autonome, donc de diminuer la vulnérabilité de l'ensemble en cas de défaillances d'un composant, en permettant un fonctionnement en mode dégradé.

En fait, l'acceptation de ces techniques se heurte à quelques difficultés :

- analyse de la sûreté de fonctionnement peu aisée, notamment difficulté de quantification,
- comportement en cas de défaillances transitoires, mal connu,
- qualification des logiciels, difficile et coûteuse.

Des travaux sont en cours dans ces domaines.

Néanmoins, l'introduction de ces technologies nouvelles dans les systèmes de protection est irréversible. Plusieurs projets existent actuellement tant en France qu'à l'étranger. Dans cette note, on décrira le projet étudié actuellement pour les centrales nucléaires PWR 1300 MWe.

2. - CONCEPTION DES SYSTEMES DE PROTECTION AVEC MICROPROCESSEURS

2.1. - Matériel

L'utilisation des microprocesseurs permet de répartir les tâches que doit effectuer le système de protection dans des sous-ensembles fonctionnels spécialisés et relativement indépendants : on pourra donc généralement utiliser des microprocesseurs de type courant pour atteindre les objectifs de précision et de temps de réponse fixés. Le découpage du système de protection en sous-ensemble fonctionnel peut se faire de différentes façons. Par exemple, sans tenir compte de la redondance (dont on parlera au chapitre suivant), on peut

découper de deux façons, la partie du système de protection qui effectue les traitements analogiques et logiques des différentes fonctions de protection :

- découpage horizontal (figure 1).

On trouve depuis les capteurs jusqu'à l'entrée des dispositifs actionneurs :

- un sous-ensemble d'acquisition des entrées analogiques et numériques,
- un sous-ensemble pour le traitement des grandeurs d'entrée et la comparaison aux seuils,
- un sous-ensemble pour le traitement logique de décision.

- découpage vertical (figure 2).

- acquisition, traitement et comparaison aux seuils, traitement logique de décision dans le sous-ensemble fonctionnel 1 pour la fonction de protection N° 1.
- acquisition, traitement et comparaison aux seuils, traitement logique de décision dans le sous-ensemble fonctionnel 2 pour la fonction de protection N° 2.
- etc.

Dans tous les cas, la structure du sous-ensemble fonctionnel est pratiquement la même : unité centrale, horloge, mémoires ROM et mémoires RAM, modules d'entrées, modules de sorties, module de communication avec les autres sous-ensembles.

Les sous-ensembles fonctionnels, ou unités fonctionnelles, communiquent entre eux soit en mode parallèle (bus normalisé), soit en mode série (liaison asynchrone). Dans certains cas, si les liaisons entre sous-ensembles fonctionnels demandent une certaine gestion, on trouvera des sous-ensembles fonctionnels spécifiques, appelés unités d'échange.

2.2. - Logiciel

Chaque sous-ensemble fonctionnel possède son propre logiciel, fixé dans des mémoires mortes (ROM ou PROM). Ce logiciel est organisé en un module d'initialisation et en une boucle constituée de modules exécutés cycliquement (figure 3). Cette boucle est répétée indéfiniment. Les interruptions ne sont pas utilisées à l'exception de celle provoquée par la coupure de l'alimentation qui lance une procédure de mise à l'arrêt du microprocesseur.

Le redémarrage du microprocesseur, après coupure secteur, consiste en une reprise du programme depuis le début. Du fait de la structure choisie,

aucune priorité n'est imposée dans les traitements : l'ordre est,par exemple, pour un sous-ensemble particulier :

- initialisation,
- modulesauto-test (début de boucle),
- modules généraux (acquisition),
- modules fonctionnels (traitement),
- modules auto-test (fin de boucle),

et retour en début de boucle.

Les modules auto-test sont des modules spécialisés chargés de surveiller le fonctionnement du sous-ensemble fonctionnel. Leur nombre et leur type dépendent du sous-ensemble fonctionnel : on aura, par exemple, les auto-tests suivants :

- valeur des entrées analogiques supérieure à un seuil fixé : en cas d'erreur, le capteur associé à la valeur erronée est considéré comme hors service.
- vérification des mémoires mortes qui contiennent le programme et les paramètres : en cas d'erreur sur les "checksum", arrêt du traitement.
- vérification du nombre de modules qui constituent le programme : en cas d'erreur, arrêt du traitement.

3. - REDONDANCE DANS LES SYSTEMES DE PROTECTION

Indépendamment de toute considération liée à la technologie et au choix des composants, l'utilisation de la redondance dans les systèmes de protection s'est imposée dès les premiers projets de système de protection ; en effet, l'application du critère de défaillance unique conduit à doubler les voies de mesure et les circuits logiques nécessaires pour commander la chute des barres de sécurité, s'il faut arrêter le réacteur en cas d'urgence. On est, assez rapidement, passé à la redondance triple qui permettait de satisfaire le critère de défaillance unique, avec une voie en test ou hors service pour maintenance, la redondance triple associée à des circuits de vote majoritaire 2/3 permettant, par ailleurs, de réaliser le meilleur compromis entre sûreté (faible probabilité de défaillances dangereuses) et disponibilité (faible probabilité de défaillances non dangereuses).

Les exigences de sûreté et de disponibilité devenant de plus en plus sévères et précises, les concepteurs proposent maintenant des systèmes de protection à quatre voies redondantes, ou système quadri-redondants. Cette

./...

redondance d'ordre quatre est justifiée par les raisonnements suivants :

- elle permet l'utilisation du système en 2/3, lorsqu'un capteur est en test ou en maintenance,

- elle permet d'économiser un capteur et une voie de mesure, en autorisant, dans certaines conditions, le raccordement de l'un des quatre capteurs à un système de régulation ou de commande. Le couplage protection-régulation impose en effet que le système de protection puisse continuer avec deux défaillances dangereuses.

Le schéma général d'un système quadri-redondant, tel qu'on le trouve actuellement, est montré figure 4 ; ce schema est celui utilisé pour la protection contre l'augmentation du flux neutronique dans CP1 (programme des centrales 900 MWe). On remarque que le système est quadri-redondant pour les capteurs et le traitement, mais que la commande des interrupteurs d'arrêt d'urgence est faite par un système logique bi-redondant. Ce changement de structure qui résulte d'un compromis fiabilité-coût est parfaitement justifié et on le retrouve dans d'autres projets (passage d'un système quadri-redondant de capteurs et de traitement à un système bi-redondant de trains de sauvegarde, dans les projets de réacteurs à eau pressurisée par exemple).

On remarquera, sur ce schéma, qu'il n'y a aucune communication entre les quatre voies redondantes, sinon au niveau du circuit logique de décision 2/4 : la séparation physique entre voies redondantes peut être réalisée jusqu'à la sortie des signaux logiques issus des unités de traitement.

Un inconvénient de ce schéma est que le passage de logique 2/4 en 2/3, en cas de test (ce qui est un avantage des systèmes quadri-redondants), n'est pas facile puisqu'il conduit nécessairement à une augmentation des interconnexions entre voies redondantes : si en effet, on veut inhiber une voie, il faut tenir compte de cette information dans les circuits logiques de décision ; cette difficulté de réalisation dans les circuits logiques câblés, peut maintenant être levée grâce à l'utilisation des techniques programmées et des techniques de multiplexage.

En résumé, on retiendra que les systèmes quadri-redondants ne sont vraiment intéressants que s'ils permettent d'augmenter la disponibilité (2/4 → 2/3) tout en conservant une grande sûreté.

4. - SYSTEMES QUADRI-REDONDANTS AVEC MICROPROCESSEURS

4.1. - Système avec redondance au niveau capteurs (figure 5).

Chaque voie redondante utilise les signaux en provenance de tous les capteurs. Dans chaque voie redondante, on trouve donc une (ou plusieurs) unité de traitement qui fait l'acquisition des signaux en provenance des capteurs, les traitements correspondants à chaque signal, les comparaisons

aux seuils et les traitements de décision en 2/4 avec inhibition ; les signaux de sortie sont émis vers les circuits logiques câblés 2/4 de commande des actionneurs. On trouve donx deux niveaux de redondance :

- une redondance au niveau des signaux en provenance des capteurs,
- une redondance au niveau de commande des actionneurs.

La présence de tous les signaux en provenance des capteurs à l'entrée de l'unité de traitement permet de faire des comparaisons entre capteurs mesurant un même paramètre et par conséquent de signaler les discordances. On peut aussi traiter les inhibitions des capteurs, puisqu'elles sont acquises par l'unité de traitement.

Pratiquement, pour améliorer les performances du point de vue fiabilité et temps de réponse, on est conduit à un découpage horizontal : quatre unités indépendantes font l'acquisition des signaux en provenance des capteurs, les traitements correspondant à chaque signal et les comparaisons aux seuils, et une unité indépendante fait le traitement de décision en 2/4 avec inhibition (1).

4.2. - Système avec redondance au niveau logique

Chaque voie redondante n'utilise que les signaux en provenance des capteurs de la voie concernée. Dans chaque voie redondante on trouve donc une (ou plusieurs) unité de traitement qui fait l'acquisition des signaux en provenance des capteurs, l'acquisition des signaux de déclenchements partiels des autres voies redondantes, les traitements correspondant à chaque signal, les comparaisons aux seuils, les traitements de décision en 2/4 avec inhibition.

Les signaux de sortie sont de deux types :

- déclenchements partiels, créés dans la voie, émis vers les autres voies redondantes,
- déclenchements globaux, émis vers les circuits logiques câblés 2/4 de commande des actionneurs.

On trouve donc deux niveaux de redondance :

- une redondance au niveau logique de traitement des déclenchements partiels,
- une redondance au niveau de commande des actionneurs.

Ce système est une amélioration des versions câblées utilisées jusqu'à présent, rendue possible grâce à l'utilisation de transmissions multiplexées entre voies redondantes.

./...

Deux projets sont en cours de réalisation.

Dans le premier projet (2), on fait un découpage horizontal (figure 6) : une unité de traitement logique spécialisée reçoit les signaux de déclenchements partiels issus des unités de traitement analogique, et les signaux de déclenchements partiels ainsi que les inhibitions en provenance des trois autres voies redondantes par l'intermédiaire d'unités d'échange unidirectionnelles.

Le second projet, en cours de réalisation pour les centrales nucléaires PWR 1300 MWe est décrit de façon plus détaillée au chapitre suivant (3).

5. - SYSTEME DE PROTECTION INTEGRE NUMERIQUE

5.1. - Description générale (figure 7)

Le système de protection intégré numérique (SPIN) comprend :

- quatre unités d'acquisition et de traitement pour la protection (UATP) indépendantes, raccordées chacune à l'un des quatre groupes de capteurs redondants,
- deux unités logiques de sauvegarde (ULS) indépendantes, qui sont raccordées chacune à un train d'actionneurs de sauvegarde.

Les UATP émettent, après traitement des informations issues des capteurs, des ordres de déclenchement vers les dispositifs actionneurs de protection, soit directement (Arrêt d'urgence), soit par l'intermédiaire des ULS (Sauvegarde).

Unité d'acquisition et de traitement pour la protection

Une unité est constituée de sous-ensembles fonctionnels qui ont pour mission :

- l'acquisition des signaux analogiques, numériques, impulsionnels ou logiques représentant les paramètres à surveiller pour la protection,
- l'acquisition des commandes manuelles permettant le blocage de certaines protections en fonction du niveau de puissance du réacteur et l'inhibition ou la mise en position sûre de certains signaux de déclenchement dans des conditions données.
- le traitement des signaux issus des capteurs et les calculs éventuels,
- la comparaison de ces signaux à des seuils fixes ou calculés,
- les échanges d'informations avec les autres UATP,
- le traitement des résultats de comparaisons aux seuils, élaborés par les quatre UATP redondantes, par une logique 2/4 qui tient compte des inhibitions éventuelles des capteurs (on ne peut faire qu'une seule inhibition pour un groupe de quatre capteurs mesurant le même paramètre),

./...

- l'émission des ordres de protection vers les interrupteurs d'arrêt d'urgence ou les ULS,

- l'émission d'informations vers la salle de conduite (traitement centralisé des informations, écrans de visualisation).

Unité logique de sauvegarde

Une unité est constituée de deux sous-ensembles logiques identiques qui reçoivent les ordres de protection en provenance des UATP. Chaque ULS est raccordées aux quatre UATP.

5.2. - Principaux sous-ensembles d'une UATP (figure 8).

Chaque UATP comprend principalement :

- des unités fonctionnelles (UF) qui effectuent les traitements pour l'émission des ordres de protection à partir, d'une part des signaux issus des capteurs reliées à cette UATP, et d'autre part, des signaux de dépassement de seuil et d'inhibition élaborés par les unités fonctionnelles correspondantes des autres UATP.

- des unités d'échange (UE) qui assurent l'émission des signaux de dépassement de seuil et d'inhibition élaborés dans les unités fonctionnelles vers les autres UATP, ou la réception de ces mêmes signaux en provenance d'une autre UATP et leur transmission aux unités fonctionnelles concernées.

Deux unités d'échange spécialisées assurent d'autre part l'émission d'informations vers la salle de conduite (traitement centralisé des informations et écrans de visualisation).

Les communications entre les unités fonctionnelles et les unités d'échange se font par l'intermédiaire de mémoires partagées qui servent de lieu de stockage intermédiaire pour les informations.

Unités fonctionnelles (figure 9)

Une unité fonctionnelle comprend des circuits d'entrée, des circuits de sortie, le microprocesseur et ses mémoires associées, un bus spécialisé pour les entrées-sorties, et un bus spécialisé pour les mémoires partagées.

Le microprocesseur est l'organe qui effectue les traitements dans l'unité fonctionnelle et qui contrôle l'acquisition des entrées et la restitution des sorties. La séquence des opérations est stockée dans une mémoire morte (PROM). L'exécution du programme débute à la mise sous tension et se répète indéfiniment (voir paragraphe 2.2.).

./...

Chaque microprocesseur de chaque unité fonctionnelle dispose de sa propre horloge ; il fonctionne donc de façon asynchrone par rapport aux autres. Un certain nombre de tests sont intégrés dans le programme et exécutés à chaque passage en vue de détecter d'éventuelles anomalies, soit dans le traitement lui-même, soit dans les échanges d'informations avec l'extérieur. Un "chien de garde" vérifie l'activité du microprocesseur ; si une anomalie est détectée, elle est signalée et le microprocesseur est arrêté.

Les mémoires partagées sont des mémoires vives (RAM) accessibles à deux microprocesseurs : elles permettent de transférer des informations d'une unité fonctionnelle à une unité d'échange (ou inversement). Les deux microprocesseurs qui ont accès à une mémoire partagée effectuent leur traitement de façon asynchrone ; les demandes d'accès à la mémoire étant aléatoires, un dispositif qui évite les conflits est nécessaire. Pour simplifier la réalisation des mémoires partagées, le transfert d'information est uni-directionnel. Des procédures de surveillance permettent de s'assurer de leur bon fonctionnement : le microprocesseur qui acquiert les informations vérifie, par exemple, qu'elles sont remises à jour périodiquement par celui qui les fournit.

Unités d'échange

Les unités d'échange ont la même structure que celle des unités fonctionnelles. Seuls les circuits d'entrée-sortie sont différents. D'autre part, le programme exécuté par le microprocesseur est simplifié, la tâche essentielle de celui-ci concernant la détection des erreurs de transmission. Les échanges d'informations entre unités d'échange appartenant à des UATP différentes, ne se fait que dans un seul sens par l'intermédiaire de coupleurs série asynchrone associés à des fibres optiques : une unité d'échange est donc soit émettrice (UEE), soit réceptrice (UER).

5.3. - Réalisation technique

Le projet SPIN a été étudié par un groupe de travail mixte FRAMATOME, MERLIN-GERIN et C.E.A. Le prototype construit par MERLIN-GERIN est en cours d'essai : il comprend une UATP et une ULS. Chaque UATP comprend sept unités fonctionnelles, dans lesquelles sont réparties les fonctions de protection prévues pour la centrale nucléaire PWR, 4-boucles, 1300 MWe, et six unités d'échange. Les unités fonctionnelles et les unités d'échange sont bâties autour du microprocesseur MOTOROLA 6800. Deux unités fonctionnelles affectées aux nouvelles protections (calcul de DNB et de puissance linéique)

./...

utilisent un opérateur à virgule flottante (OVF) couplé au microprocesseur, de façon à pouvoir faire les calculs nécessaires dans le temps prescrit (mémoire-programme = 15 K-octets ; durée d'un cycle = 0,7 seconde).

Les échanges entre UATP sont faits par des liaisons série asynchrone à 76 kilobauds, sur fibres optiques.

Les circuits logiques câblés sont utilisés pour le regroupement de certains ordres de protection dans les UATP, et surtout dans les ULS où les ordres de protection sont combinés aux commandes manuelles ; ce sont des circuits logiques à pannes orientées, du type logique dynamique.

6. - CONCLUSION

L'utilisation de microprocesseurs et des circuits à large intégration associés permet de concevoir des systèmes largement décentralisés pour la protection des centrales nucléaires. Le système de protection intégré numérique en cours de réalisation actuellement, est un exemple d'application de ces nouvelles technologies.

REFERENCES

(1) P. DARIER
"La fiabilité informatique dans l'instrumentation nucléaire"
Congrès MESUCORA, Paris (1979).

(2) J.M. GALLAGHER et Al.
"Design of internal architecture for Westinghouse microprocessor based integrated protection system".
Colloque International sur la commande et l'instrumentation des Centrales Nucléaires - CANNES (1978) - AIEA-SM-226/112.

(3) J.L. SAVORNIN et Al.
"Système de protection intégré numérique"
Colloque International sur la commande et l'instrumentation des Centrales Nucléaires - CANNES (1978) - AIEA-SM-226/93.

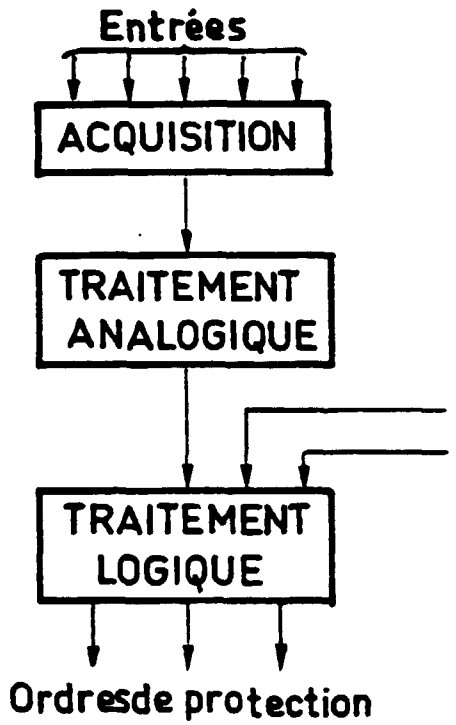


Fig.1 _ DECOUPAGE HORIZONTAL _

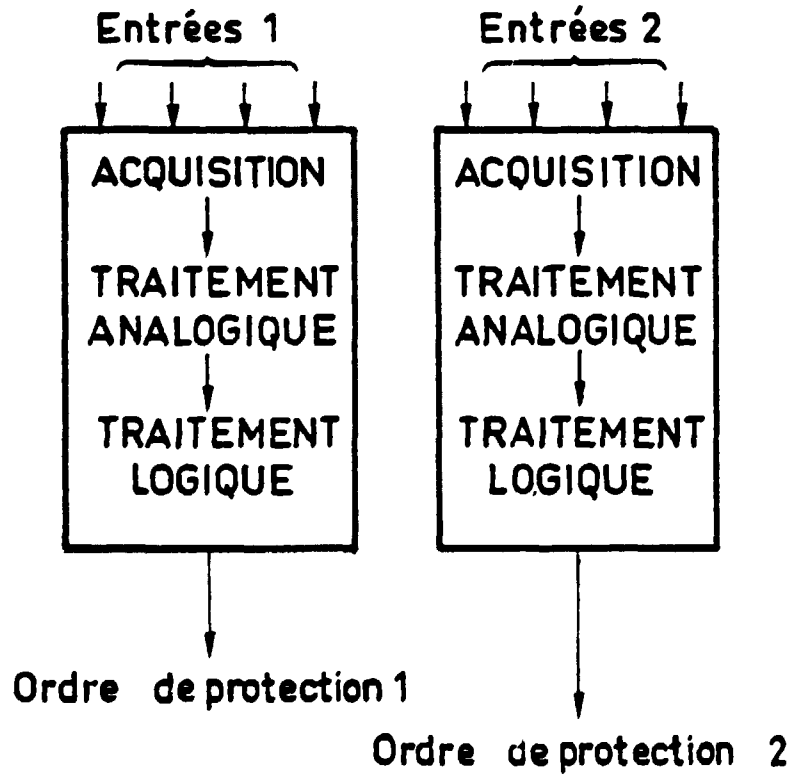


Fig. 2 _ DECOUPAGE VERTICAL _

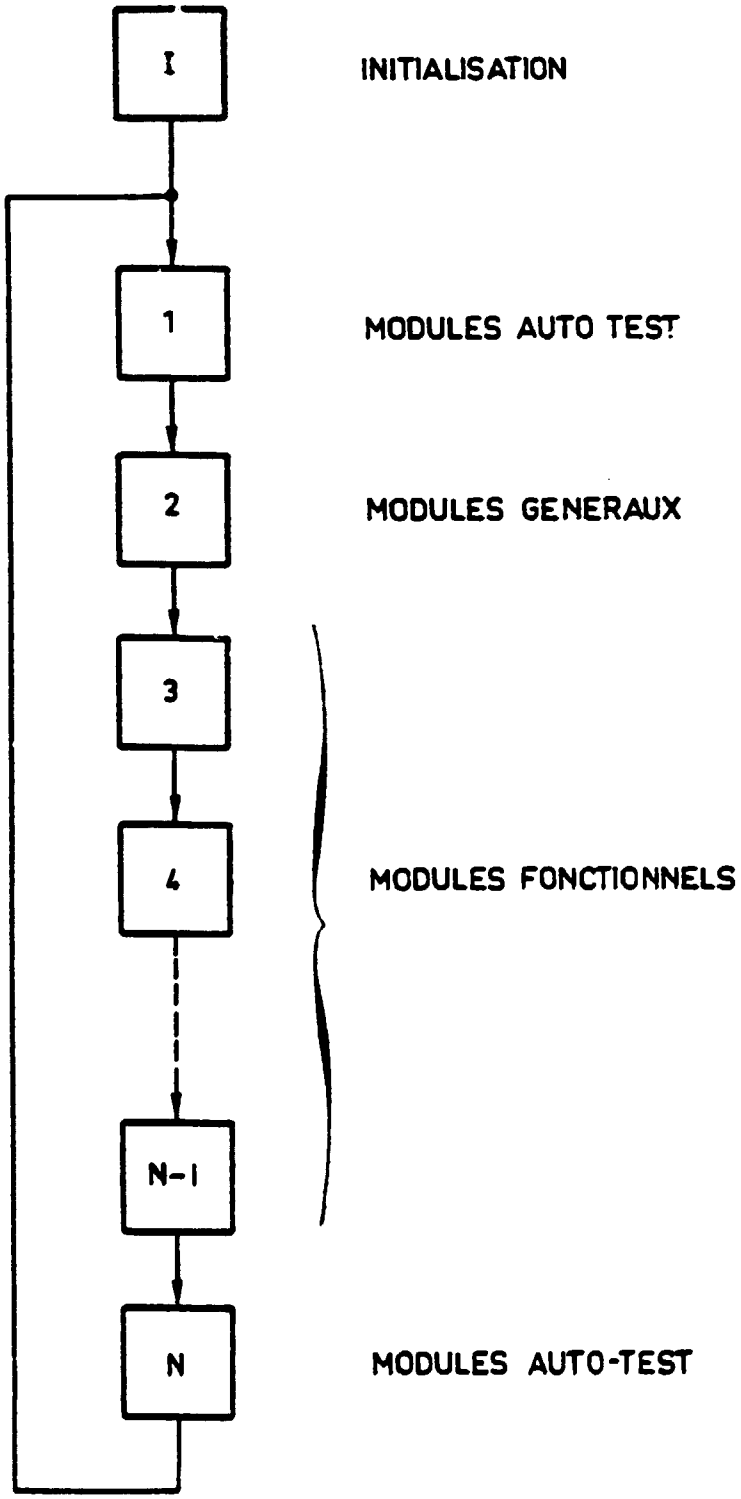


Fig.3 ORGANISATION DU LOGICIEL

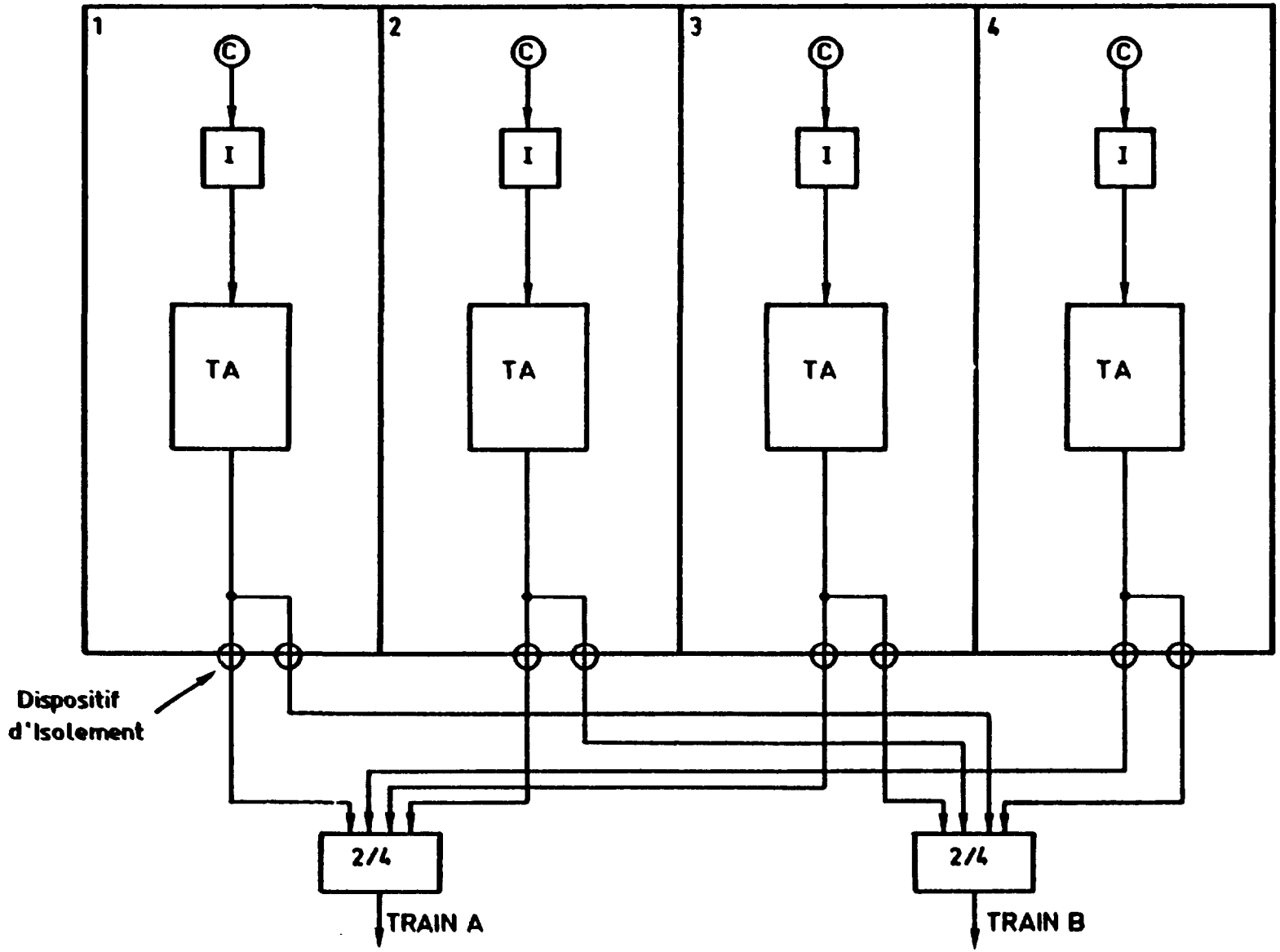
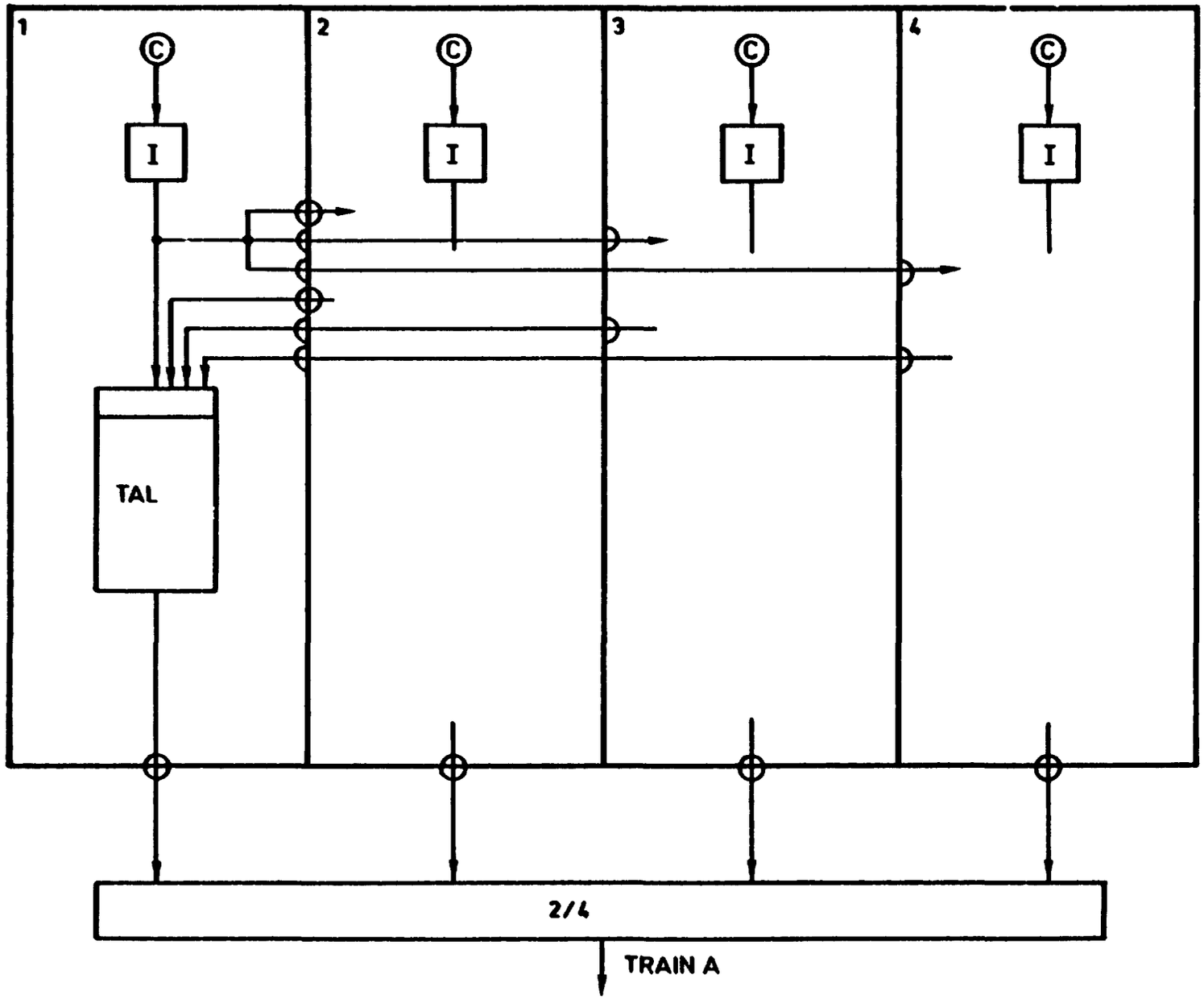


Fig.4 SYSTEME DE PROTECTION TYPE CP1



TAL : Traitement Analogique et Logique

Fig.5 REDONDANCE AU NIVEAU CAPTEURS

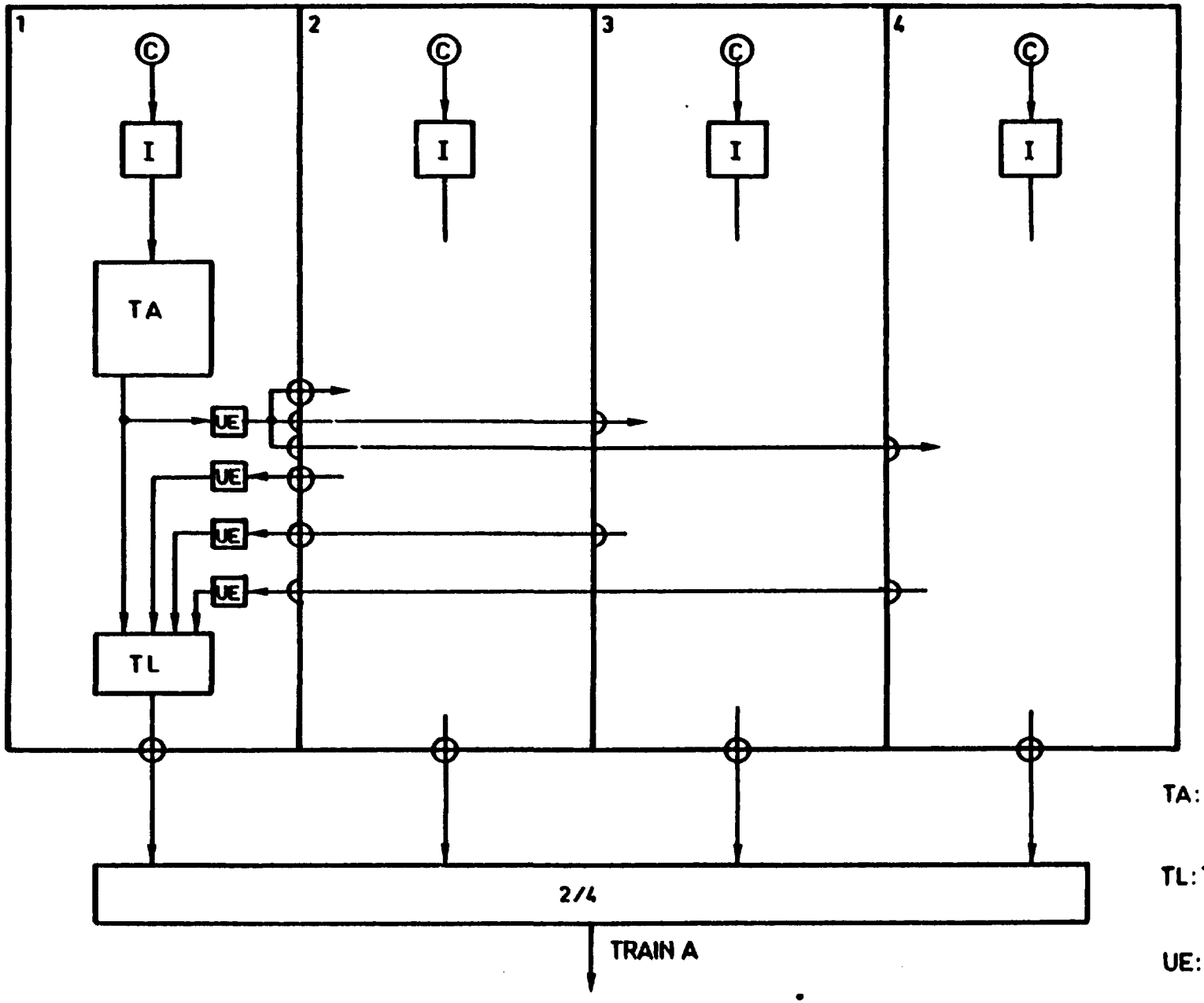


Fig.6. REDONDANCE AU NIVEAU LOGIQUE

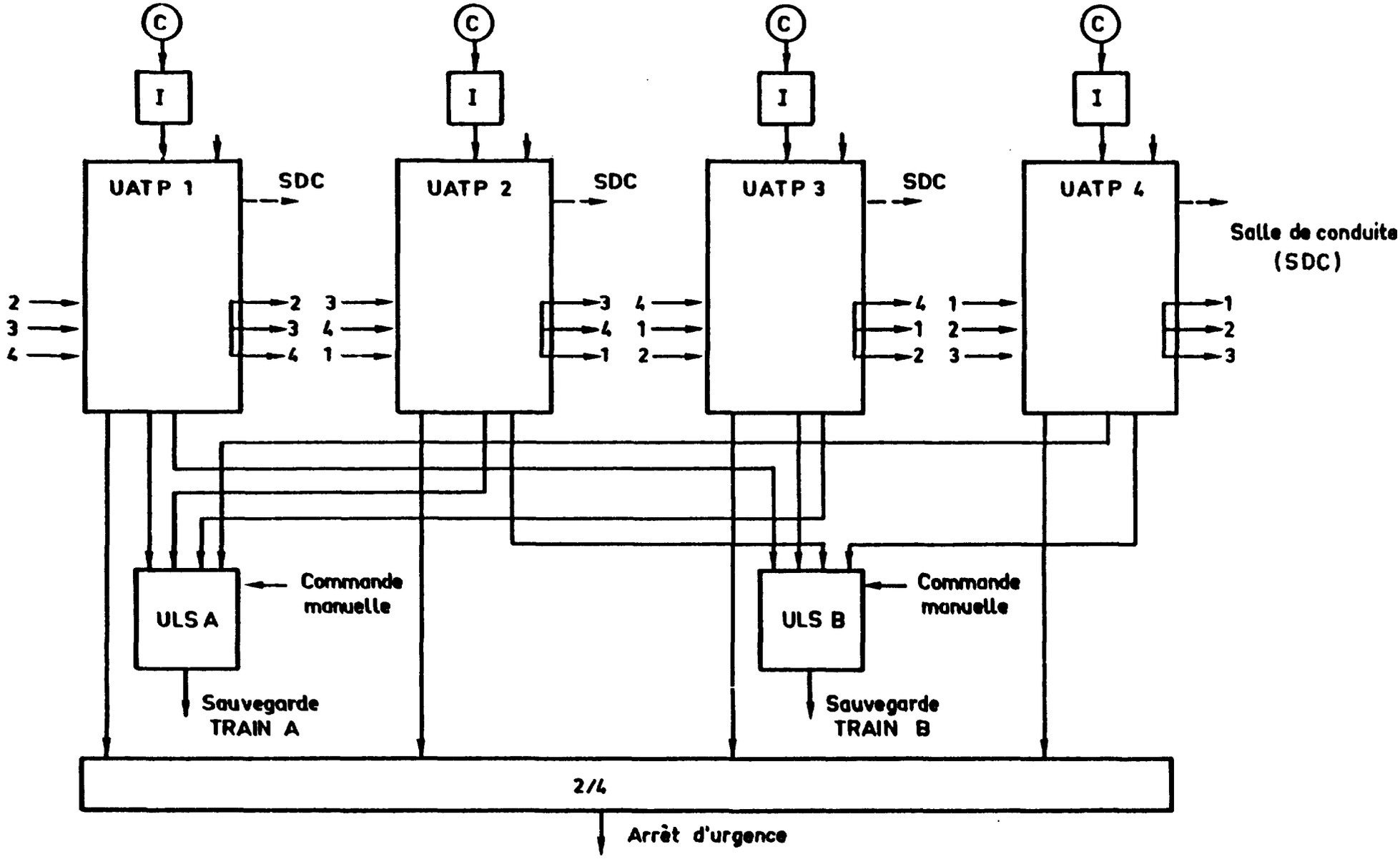


Fig.7 SYSTEME DE PROTECTION INTEGRE NUMERIQUE

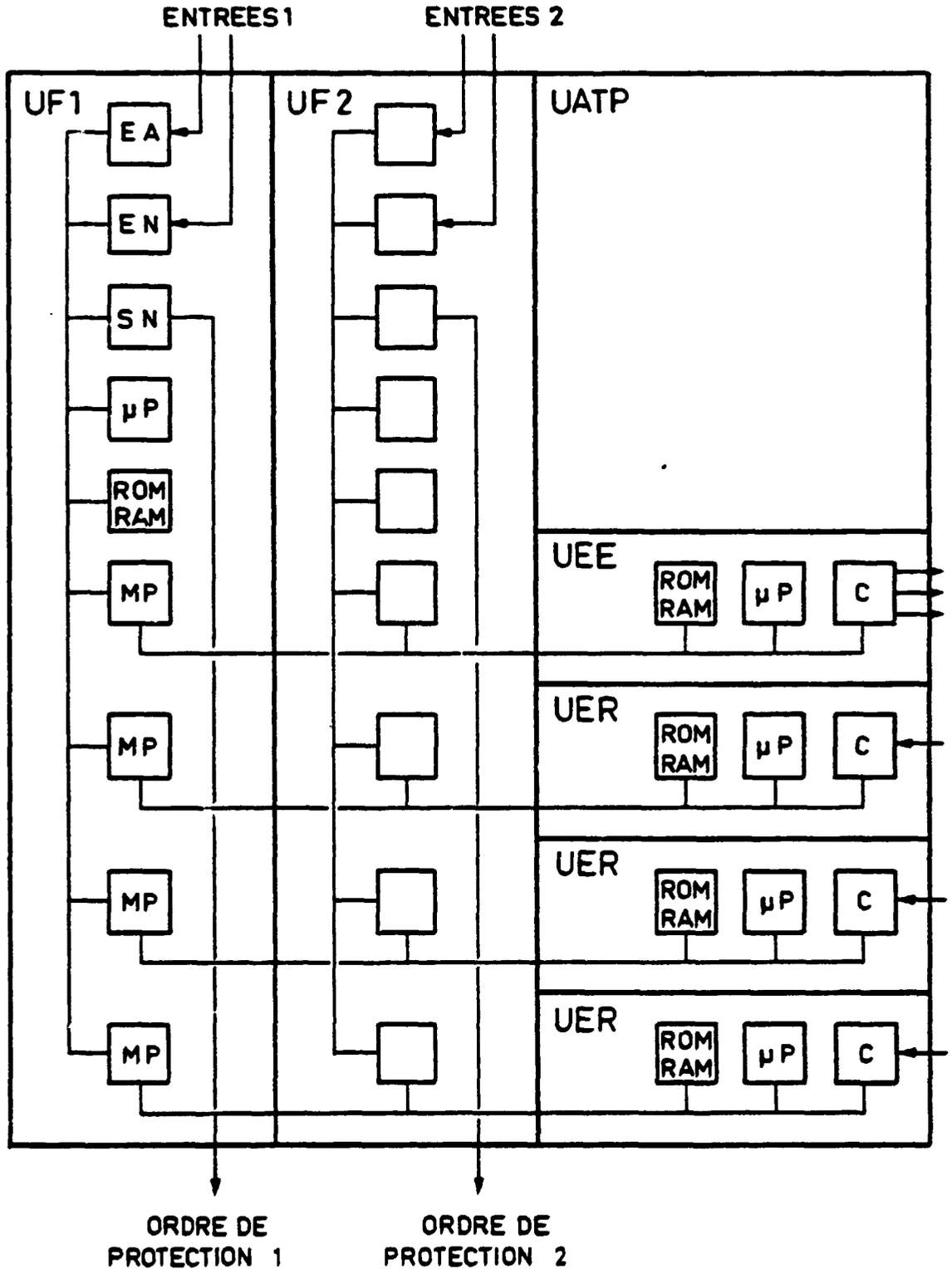


FIG 8 : STRUCTURE D'UNE UATP

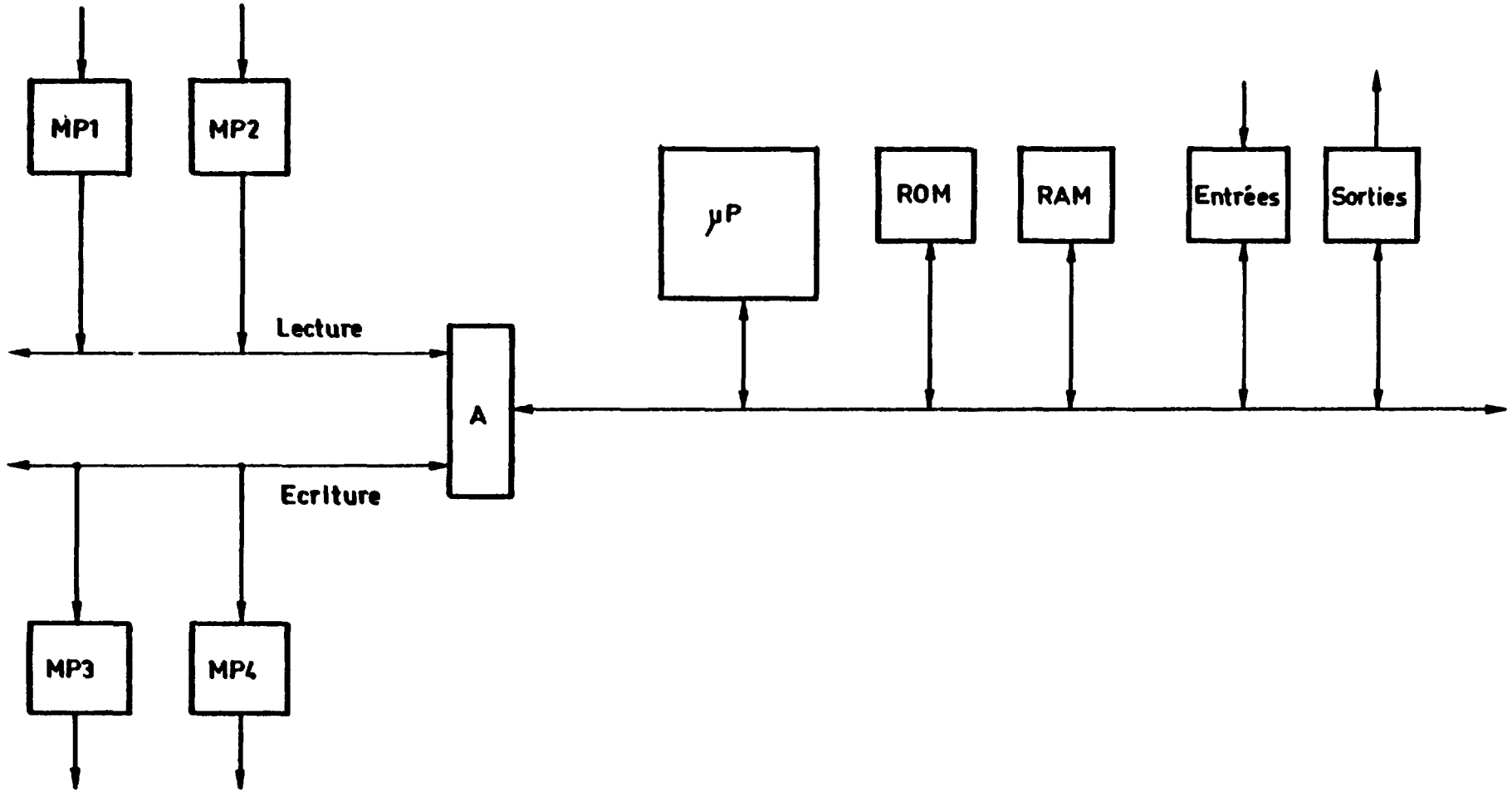


Fig 9 _ UNITE FONCTIONNELLE