N° d'ordre : 1309

THÈSE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNIQUES FLANDRES ARTOIS

pour obtenir le titre de

DOCTEUR DE TROISIEME CYCLE

par

Charles MAGNIEZ

maître es sciences

COMMANDE-CONTROLE DE PROCESSUS PAR TRAITEMENT HIERARCHISE

ETUDE DES ASPECTS SECURITE-DISPONIBILITE

Soutenue le 12 Décembre 1985 devant la Commission d'Examen

Membres du Jury :	MM.	R.	GABILLARD	Président-Rapporteur
		V.	CORDONNIER	Examinateur
		F.	LOUAGE	Examinateur
		Y.	DAVID	Invité
		J.F.	DHALLUIN	Invité
		C.	MARCOVICI	Invité

A Marie Chantal
A Mes parents
A Mes Amis

AVANT - PROPOS

-o-o-o-o-o-o-o-o-o-o-o-o-

Cette étude a été réalisée au Laboratoire de Radiopropagation et Electronique de l'Université des Sciences et Techniques de LILLE, dirigé par le Professeur R. GABILLARD.

Je tiens à lui exprimer mes plus vifs remerciements pour l'opportunité qu'il m'a offerte en me proposant de travailler dans son laboratoire sur un sujet aussi passionnant que celui de la sécurité des systèmes, et pour l'honneur qu'il me fait en présidant le jury.

Mes plus vifs remerciements vont également à messieurs les Professeurs V. CORDONNIER et F. LOUAGE pour le grand honneur qu'ils me font en participant au jugement de ce travail.

Je tiens à remercier Monsieur Y. DAVID, Directeur de l'Institut National de REcherche pour les Transports et leur Sécurité (I.N.R.E.T.S.), de l'honneur qu'il me fait en participant au jury.

Je remercie également Monsieur C. MARCOVICI, Ingénieur du service des transports de la Société MATRA, d'avoir accepté d'apporter son précieux jugement à ce travail.

J'exprime ma profonde reconnaissance à Monsieur J.F. DHALLUIN, Ingénieur à l'institut national de recherche pour les transports et leur sécurité. Je le remercie pour l'aide et le soutien moral qu'il m'a toujours apportés et qui furent indispensables à l'aboutissement de ce travail, fruit de nombreuses et fructueuses discussions entre nous.

Je remercie tous les techniciens, ingénieurs et chercheurs, du laboratoire qui par leur présence ou par leur aide m'ont permis de mener à bien ce travail, ainsi que Madame SZELAG qui a participé avec beaucoup de dynamisme à l'élaboration de ce projet.

Enfin, je n'oublierai pas de citer Madame MEESMAECKER et Monsieur DEHORTER, qui ont assuré la frappe et la reprographie de ce mémoire avec beaucoup de soins.

SOMMAIRE

-o-o-o-o-o-o-o-

CHAPITRE III : SUPPORT DE TRAITEMENT

INTRODUCTION

-o-o-o-o-o-o-o-o-o-o-o-

Depuis plusieurs années, il est possible de constater l'introduction massive des ordinateurs dans les chaines de commande de processus. Cette tendance a été nécessitée par le nombre croissant de variables à contrôler de façon fine. Utilisé d'abord pour des fonctions de télésurveillance, l'ordinateur a ensuite été utilisé pour effectuer lui-même des tâches de commande-contrôle. On parle maintenant de fonctions de commande adaptative ou à auto-organisation et on cherche de plus en plus à relier les problèmes de gestion de l'entreprise à la commande de processus. Le progrès technologique considérable sur les unités de traitement d'informations à microprocesseur a entrainé une évolution profonde des problèmes de commande automatique, les conséquences sont les suivantes :

- une autorité croissante confiée aux organes de traitement informatiques avec de lourdes implications sur la sécurité des personnes ou des biens

- une complexité accrue des fonctions à élaborer.

Quant au processus étudié, il se présente comme un système complexe, géographiquement réparti, c'est-à-dire un ensemble composé de plusieurs sous-systèmes avec en général des interactions entre eux.

L'évènement panne est un évènement naturel durant la vie utile d'un système. Il doit donc être pris en compte et traité de façon naturelle, l'évaluation de la sûreté de fonctionnement du système de commande-contrôle devenant un élément prépondérant lors de la conception des dispositifs.

L'automatisation plus poussée des systèmes de transport guidés tels les métros urbains ou le train, permet d'accroître les performances mais entraîne de ce fait une évolution des problèmes de sécurité.

Notre travail de thèse vient s'insérer dans ce cadre d'activité.

Le travail développé s'inscrit en effet dans un projet global de commande-contrôle de processus géographiquement réparti, appliqué aux transports. L'application que nous avons traitée consiste en effet à gérer en sécurité une tâche globale de commande-contrôle des portes véhicule d'une rame de métro. De premiers résultats ont montré que l'on pouvait, à un niveau localisé, traiter en sécurité le problème de commande-contrôle d'un sous-ensemble relativement simple du processus, tel un mécanisme de porte, avec un intérêt économique certain portant sur l'aide à l'exploitation et l'aide à la maintenance.

Notre contribution à cette étude se situe à un niveau plus global puisque nous avons cherché à traiter les aspects sécurité et disponibilité de la commande et du contrôle de l'ensemble des sous-systèmes interconnectés entre eux par réseau de communication.

Dans un premier chapître, après avoir rappelé les notions classiques de sécurité utilisées antérieurement dans le domaine des transports guidés, nous exposons les notions de sécurité probabiliste et de disponibilité utilisées aujourd'hui et appliquées aux systèmes microinformatiques. Le domaine particulier qui nous intéresse, nous amène à choisir une structure hiérarchisée de commande-contrôle dont nous définissons les caractéristiques dans les chapîtres suivants.

L'étude des problèmes de sécurité et de disponibilité posés par la communication entre les unités font l'objet du second chapître. Dans un premier temps, nous développons l'étude de l'architecture du réseau de communication, ce qui nous conduit à retenir une solution en étoile pour satisfaire au mieux le compromis sécurité-disponibilité. Nous développons ensuite les problèmes de gestion des accès au réseau et de détection des pannes de transmission. Enfin, nous définissons une hiérarchie restreinte des tâches à exécuter, s'appliquant à la transmission d'informations en sécurité.

Le troisième chapître est consacré à la définition d'un logiciel de traitement des informations de commande et de contrôle à un niveau centralisé. Nous définissons un mode de traitement hiérarchisé sur deux niveaux, permettant de gérer aisément, en plus de la tâche d'application, les aspects sécurité et disponibilité de l'ensemble du système.

CHAPITRE I

-o-o-o-o-o-o-o-o-o-

CHAPITRE I

-o-o-o-o-o-o-o-o-o-

I. 1 - SITUATION DU PROBLÈME -

DÉFINITION DES OBJECTIFS À ATTEINDRE

L'évolution des modes nouveaux de transport s'accompagne d'une nécessaire évolution des techniques. L'homme est peu à peu remplacé par des automatismes qui gèrent les tâches répétitives et permettent d'accroître les performances.

La suppression progressive de l'opérateur humain ne doit pas se faire au détriment de la qualité du service. Son rôle de superviseur doué d'intelligence, et donc capable de prendre des décisions en présence d'une situation anormale, ne peut être supprimé. Ce rôle est précisément celui qui est confié aux dispositifs destinés à assurer la sécurité.

Les concepts utilisés pour garantir la sécurité d'un équipement diffèrent suivant le domaine d'application :

- En avionique, la notion de sécurité est confondue avec la sûreté de fonctionnement des matériels.
- Les transports terrestres guidés possèdent, vis-à-vis des voyageurs, un état de sécurité physiquement défini ; c'est l'état basse énergie à savoir tous les véhicules arrêtés, alimentations coupées et dégagement possible des voyageurs.

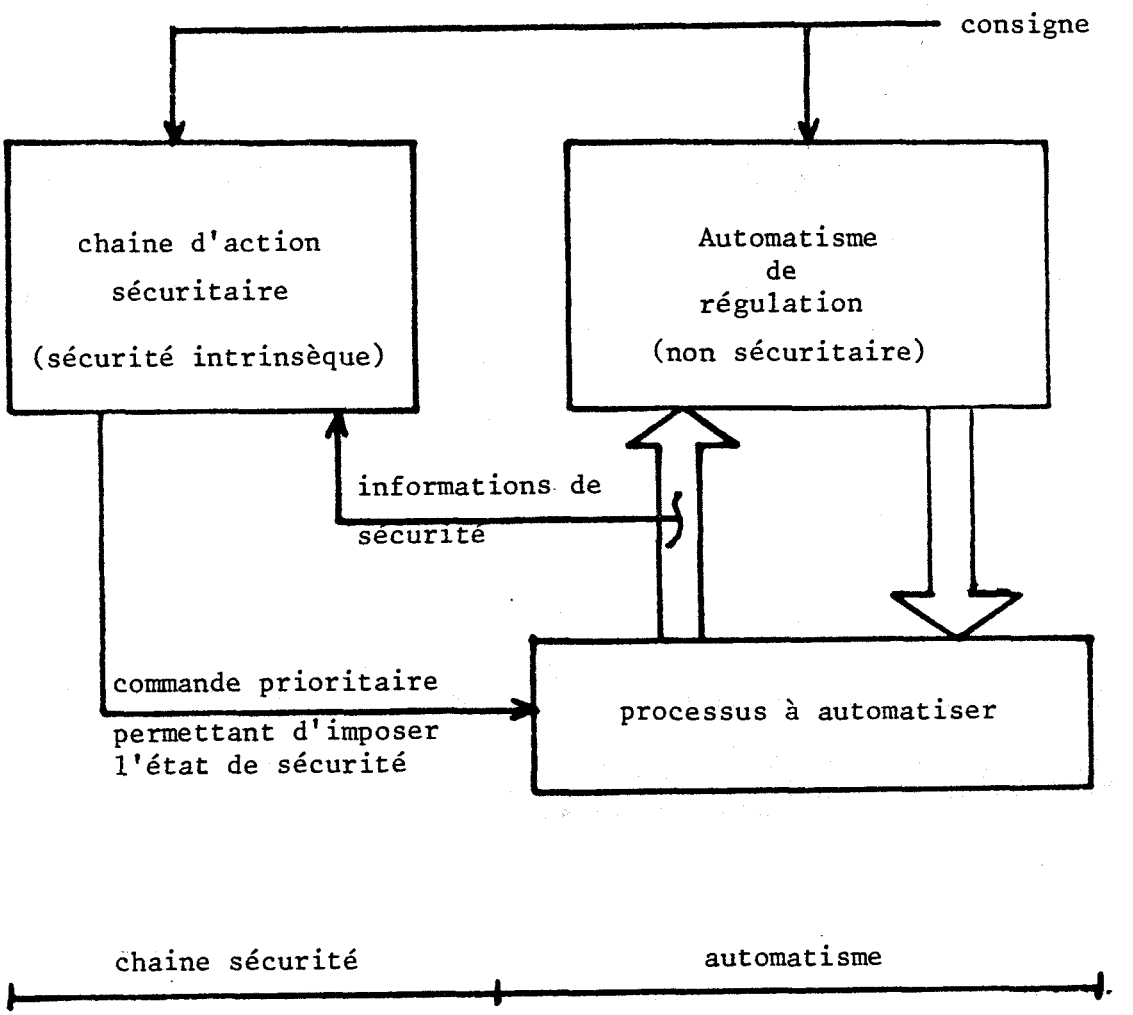


Figure I.1 : Architecture générale d'un dispositif classique de commande de processus en sécurité

Les dispositifs de sécurité sont composés d'une chaine d'action sécuritaire, en sécurité intrinsèque, qui peut à tout moment et prioritairement agir sur les actionneurs et imposer au véhicule un état de sécurité (freinage d'urgence) si celui-ci sort des limites imposées par la sécurité.

L'architecture globale des automatismes actuellement employés est définie de la manière suivante (Figure I.1) :

- Une chaine d'action non sécuritaire qui commande et contrôle le processus. Ce dispositif gère les automatismes complexes et fait appel à des circuits de technologie actuelle en logique microprogrammée.

- Une chaine d'action sécuritaire, en sécurité intrinsèque, qui sur la base de quelques signaux significatifs de l'état du processus (informations de sécurité) laisse ou non agir l'automatisme non sécuritaire.

Notre travail se situe dans le cadre d'une démarche nouvelle, entreprise depuis plusieurs années consistant à regrouper dans une même chaine d'action les automatismes de commande et les fonctions de sécurité. La définition d'un système microinformatique capable de remplir cette double fonction présente les avantages suivants :

- Simplification des systèmes au niveau de l'architecture.
- Simplification, voire disparition de certaines maintenances préventives sur lesquelles s'appuie la sécurité.
- Amélioration de la disponibilité par tolérance aux fautes.
- Accroissement de la souplesse et des performances.

Une application de notre étude est destinée à la commande et au contrôle en sécurité d'un ensemble de portes véhicule d'une rame de métro de type VAL. Toutefois, l'étude s'inscrit dans un cadre plus général de commande-contrôle de processus lents et discontinus avec exigence de sécurité.

Probabilités / Conséquences	10^{-5} fréquent ou peu fréquent	10^{-7} rare	10^{-9} extrêmement rare	10^{-9} extrêmement improbable
mineures				
significatives				
critiques				
catastrophiques				

Tableau I.1 : Objectifs partiels de sécurité

I. 1. 1 - CONTRAINTES IMPOSEES PAR LA SECURITE

Avant d'entreprendre un programme d'élaboration et éventuellement de démonstration de la sécurité, il importe de fixer les objectifs de ce programme le plus clairement possible |Réf.25|. L'objectif de sécurité peut être quantitatif, en particulier, ce peut être la valeur maximale de la probabilité p qu'un individu ait un accident mortel du fait du système pendant une heure d'exposition au risque. Cette probabilité p est référée à l'ensemble du système : il s'agit donc du risque moyen. Différents éléments interviennent dans l'allocation d'un objectif de sécurité :

- La sécurité atteinte dans le passé par les systèmes comparables ; en aucun cas le développement d'un nouveau système ne peut s'accompagner d'une augmentation du risque.
- La sécurité atteinte dans le présent par les autres systèmes de transport.
- La gravité des conséquences de l'accident.
- Le réalisme de l'objectif de sécurité.

Ainsi on peut définir des critères applicables à la majorité des systèmes grâce à des "grilles" de probabilités acceptables en fonction des conséquences des défauts (Tableau I.1). Ces grilles peuvent être modifiées dans chaque cas particulier pour tenir compte des éléments qui viennent d'être énumérés ci-dessus. Les classes de gravité et les classes de probabilités sont définies de la manière suivante |Réf.25| :

* Classes de gravité :

- Conséquences mineures : il n'y a ni dégradation sensible des performances du système, ni interruption de la mission, ni blessure de personnes, ni endommagement notable des biens ou du système.
- Conséquences significatives : il y a dégradation sensible des performances du système, pouvant entrainer l'interruption de la mission. Mais il n'y a ni blessure de personne, ni endommagement notable des biens ou du système.

- Conséquences critiques : il peut y avoir blessure de personnes et/ou endommagement notable des biens ou du système. Est également considérée comme critique toute situation qui exige une action correctrice immédiate pour assurer la survie des personnes ou du système.
- Conséquences catastrophiques : il y a destruction du système et/ou plusieurs blessés graves et/ou mort de personnes.

* Classes de probabilité :

- Evènement fréquent : évènement dont la probabilité d'apparition est supérieure à 10^{-3}/h.
- Evènement peu fréquent : évènement dont la probabilité d'apparition est comprise entre 10^{-3}/h et 10^{-5}/h.
- Evènement rare : évènement dont la probabilité d'apparition est comprise entre 10^{-5}/h et 10^{-7}/h.
- Evènement extrèmement rare : évènement dont la probabilité d'apparition est comprise entre 10^{-7}/h et 10^{-9}/h. C'est un évènement qui normalement ne doit pas arriver au cours de la vie de l'ensemble des systèmes en service mais qui doit néanmoins être considéré comme possible.
- Evènement extrèmement improbable : évènement dont la probabilité d'apparition est inférieure à 10^{-9}/h. C'est un évènement pour lequel on a la quasi certitude qu'il ne se produira jamais au cours de la vie de l'ensemble des systèmes en service.

En prenant pour référence les données relatives au système actuellement en service |Réf. 1|, le cumul des probabilités d'apparition de pannes conduisant à un état d'insécurité doit être inférieur au seuil de $2\ 10^{-6}$/heure porte (accidents individuels).

Ceci nous contraint à respecter pour l'ensemble du dispositif de commande-contrôle et du processus, un objectif de sécurité de $p = 1{,}2\ 10^{-5}$/h (six portes par véhicule).

Les conséquences des pannes entrainant une insécurité sont les suivantes :

- porte ouverte alors que le véhicule est en ligne
- mauvais fonctionnement du système d'évacuation d'urgence
- portes bloquées fermées côté quai en station sur un véhicule
- passager coincé lors d'une fermeture de porte d'accès et démarrage du véhicule
- ouverture du mauvais côté des portes d'un véhicule en station.

L'étude de sécurité de l'ensemble du dispositif peut être décomposée en deux parties distinctes et indépendantes :

- L'étude de sécurité de la commande et du contrôle du processus à partir d'un système microinformatique en bon état de fonctionnement. Une telle étude prend en compte toutes les pannes possibles sur les voies de commande, les voies de mesure et sur le processus. Cette étude conduit à l'élaboration d'une méthode sûre de détection permanente des pannes |Réf. 2| |Réf. 3|.

- L'étude de sécurité du système microprocesseur lui-même, en vue de définir une structure matérielle et logicielle capable de détecter ses propres défauts de fonctionnement et capable, en cas d'avarie, de se reconfigurer de manière à ne pas créer par rapport à son environnement une situation dangereuse |Réf. 2|.

Il faut se prémunir des dangers suivants :

- <u>vis-à-vis du processus</u> : une commande intempestive contraire à la sécurité peut être engendrée par un microprocesseur défectueux.
- <u>Vis-à-vis du système d'exploitation</u> : celui-ci peut recevoir des messages intelligibles mais non significatifs et contraires à la sécurité, capables d'induire en erreur sur la conduite à adopter.

I. 1. 2 - AMELIORATION DE LA DISPONIBILITE

L'amélioration de la disponibilité peut être envisagée par rapport à deux types de défauts.

* Défauts propres au processus

L'établissement de procédures de détection et de localisation des défauts sur les capteurs et les effecteurs ainsi que sur les voies de mesure ou de commande associées permet de tolérer une partie des défauts qui peuvent affecter ces organes. La tolérance d'un défaut permet la poursuite de l'exploitation normale lorsque la commande reste possible et que le vecteur de contrôle est dimensionné de manière à tolérer ce défaut (redondance des informations) ou la poursuite de l'exploitation en mode dégradé lorsque le processus reste observable mais que la commande n'est plus possible. La poursuite de l'exploitation en mode dégradé nécessite que le processus se trouve dans un état non contraire à la sécurité et se traduit par l'inhibition des commandes destinées au système défaillant. Pour un mécanisme de porte, le fonctionnement dégradé correspond à la condamnation de la porte (préalablement fermée et verrouillée).

* Défauts propres au système de commande-contrôle

Une redondance du traitement des informations par des unités distinctes permet une reconfiguration du système de commande-contrôle en présence d'un défaut affectant le fonctionnement d'une unité. Pour pouvoir tolérer un défaut sans affecter la sécurité de l'ensemble, il est nécessaire que chaque unité soit en autotest et puisse se déconnecter de son environnement lorsqu'une panne se produit de manière à ne pas perturber les autres unités qui constituent les ressources encore disponibles du système. On peut alors utiliser un mode de fonctionnement dégradé dès lors que l'unité défaillante est localisée.

L'amélioration de la disponibilité par tolérance aux fautes s'accompagne nécessairement d'une dégradation du niveau de sécurité car la présence

d'un défaut diminue le niveau de redondance et peut remettre en cause la validité des procédures de détection de défauts. Pour cette raison, la présence d'un défaut doit être immédiatement signalée et la tolérance momentanée de ce défaut doit permettre de planifier au mieux la remise en état du système. Dans le cas du métro, la tolérance d'un défaut permet de terminer un trajet avant de rejoindre le garage atelier et procéder à la réparation.

I. 1. 3 - AIDE A LA MAINTENANCE

L'utilisation des microprocesseurs permet d'apporter une aide appréciable à la maintenance qui va de pair avec l'amélioration de la disponibilité. Ces deux objectifs intimement liés sont rendus accessibles grâce d'une part :

- à la possibilité de stockage d'informations. La localisation précise des défauts, nécessaire pour poursuivre momentanément l'exploitation, est mise à profit pour stocker, ensuite restituer aux agents de maintenance des informations précises sur l'origine des pannes. L'apport le plus intéressant est constitué par la possibilité de garder en mémoire la trace de défauts fugitifs qui constituent l'un des problèmes majeurs rencontrés par les agents de maintenance.

- et d'autre part aux possibilités multiples offertes par une structure microprogrammée. On peut inclure dans la définition des logiciels des possibilités de mesure du temps d'évolution du processus ou de niveaux de tension... qui permettent grâce à un traitement statistique des valeurs recueillies, d'anticiper sur les procédures de maintenance curative en remplaçant les organes qui vieillisent avant qu'ils ne tombent en panne. Cette maintenance préventive (ou pré-curative) permet, d'une part, d'améliorer la disponibilité de l'ensemble et d'autre part de ne remplacer les organes qu'au terme de leur durée de vie utile.

I. 2 - JUSTIFICATION DU CHOIX D'UNE SOLUTION DÉCENTRALISÉE

Souvent, un processus se présente comme une interconnexion de sous-systèmes monovariables ou multivariables, avec des rebouclages, qui sont géographiquement répartis. Le système de commande doit tenir compte de l'ensemble des variables et être en mesure d'atteindre la commande désirée avant que d'autres modifications que celles ayant motivé une nouvelle commande ne se présentent. L'utilisation d'un système de commande-contrôle centralisé présente différents inconvénients parmi lesquels on peut citer :

- des performances nécessaires en capacité et rapidité de calcul qui s'accroissent très vite avec le nombre de variables à prendre en compte.

- un câblage important pour relier les différents capteurs et effecteurs au système central.

- une modification, même légère, dans la structure du système ou du processus, nécessite de reprendre l'ensemble du problème et une transposition des résultats à un processus semblable à celui étudié est toujours difficile, ce qui est regrettable vu le coût de telles études.

Une solution décentralisée permet de résoudre ces problèmes et de hiérarchiser le système de commande-contrôle. Une telle décentralisation des fonctions systématiques est rendue possible et intéressante depuis l'apparition des microprocesseurs. La commande hiérarchisée non seulement fournit les moyens de contourner les difficultés de calcul, mais également facilite la synthèse du système de commande grâce à l'utilisation de plusieurs unités de commande simples. Elle permet de résoudre des problèmes très complexes dont on ne peut envisager le traitement global et un changement au niveau du sous-processus est pris en compte de façon simple sans avoir à reconsidérer l'ensemble du problème (analyse structurée du problème).

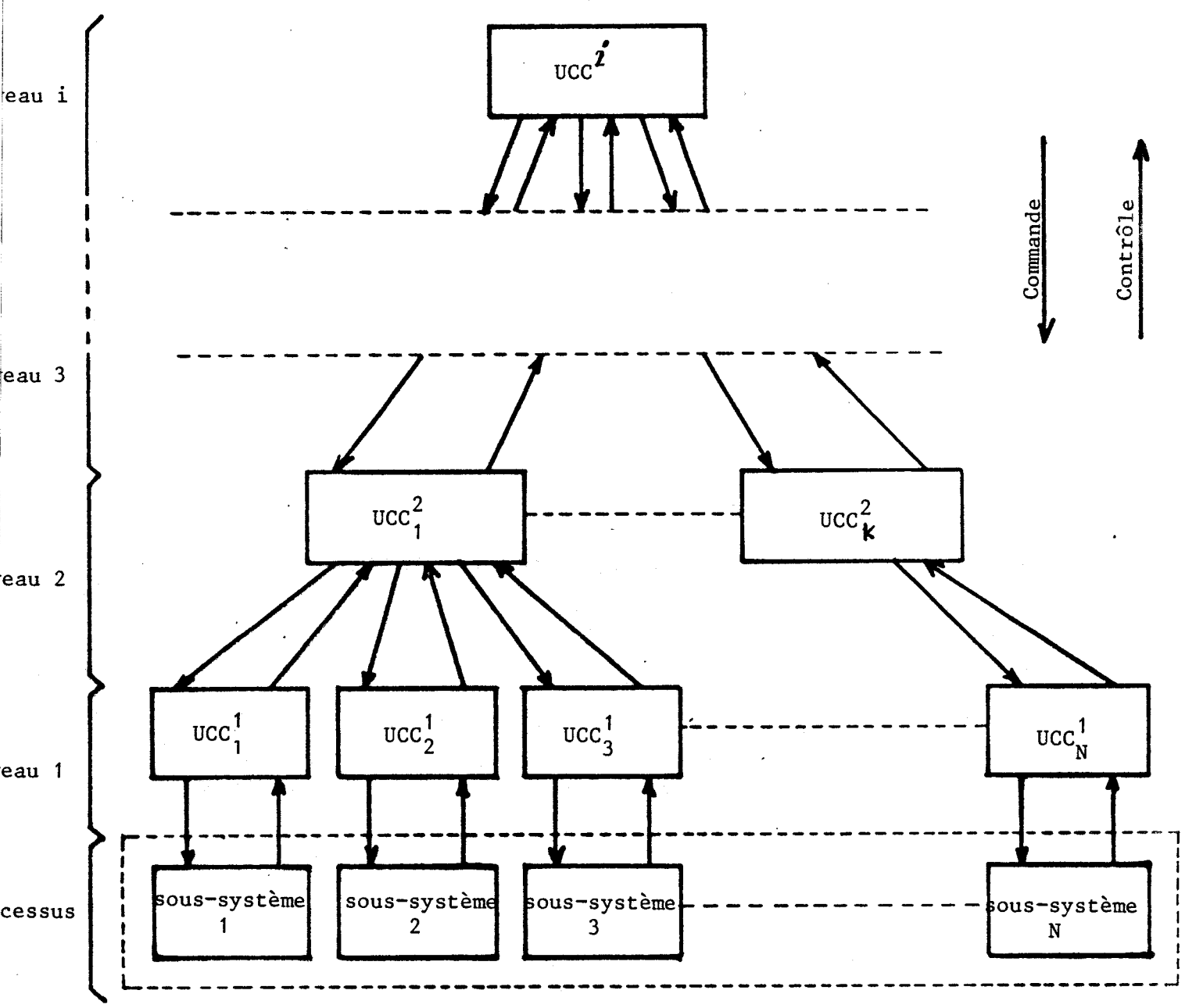


Figure I.2 : Structure de commande-contrôle hiérarchisée appelée aussi structure pyramidale

Le principe de la commande hiérarchisée est de définir des sous-problèmes qui peuvent être considérés comme indépendants et c'est par action sur la définition de ces sous-problèmes qu'on atteint la solution globale. Deux notions fondamentales sont à la base de l'élaboration des systèmes de commande hiérarchisée : ce sont la répartition des tâches et la coordination. La répartition des tâches pouvant être réalisée simultanément par :

- Une décomposition verticale de la fonction de commande globale en fonctions de commande plus simples.

- Une division horizontale en découpant le processus en processus plus simples commandés suivant des critères locaux.

Ces actions locales sont coordonnées par une unité supérieure.

On retrouve l'aspect fondamental d'une hiérarchie qui est qu'une unité de commande s'intéresse à des aspects d'autant plus généraux du système global qu'elle appartient à un niveau élevé de la hiérarchie. Elle est liée à des dynamiques d'autant plus faibles que ce niveau est élevé.

La première étape à aborder est celle de la définition des sous-problèmes (sous-systèmes). Cette décomposition doit s'appuyer sur la nature physique du processus. Cette étape est très importante car de là va dépendre la complexité de la tâche de coordination.

L'étape suivante consiste à déterminer les transferts d'informations entre niveaux afin de préciser ce qui est nécessaire à chacun d'eux.

On peut alors définir des algorithmes coordonnateurs et retenir le plus performant. Il est à remarquer que la régulation de processus continus fait très souvent appel aux mêmes méthodes. L'appareillage sera quelquefois différent mais la philosophie générale est la même.

Si le découpage des fonctions utilisateurs en tâches élémentaires est effectué correctement, la disponibilité d'un nombre d'unités de traitement quasi autonomes qui en découle rend possible un parallélisme d'exécution. Il est donc possible, si les traitements sont suffisamment indépendants entre eux, d'accroître la vitesse de traitement du système par rapport à un système centralisé. Les possibilités de reconfiguration automatique et de dégradation progressive des performances permettent d'augmenter la disponibilité en autorisant une maintenance en ligne ou la commande de modes alternés ou dégradés.

La décomposition des tâches oblige le concepteur à créer un logiciel modulaire. L'utilisation d'une solution décentralisée va donc dans le sens d'une amélioration de la sûreté de fonctionnement.

La structure pyramidale d'un système hiérarchisé complexe n'est en fait qu'une structure à deux niveaux dont le niveau inférieur a été décomposé en structures à deux niveaux jusqu'à atteindre des fonctions de commande élémentaires. On voit donc l'intérêt de l'étude d'une structure à deux niveaux qui fait appel à un réseau local de commande-contrôle.

Dans un réseau local de commande-contrôle, quelle que soit sa conception, on peut distinguer deux sous-ensembles élémentaires :

- Le support de traitement qui regroupe l'ensemble des moyens matériels et logiciels destinés au prélèvement des données, au traitement de l'information et à l'activation des commandes.

- Le support de communication qui est constitué par l'ensemble des moyens matériels et logiciels permettant aux abonnés du réseau de communiquer entre eux et d'effectuer la coordination souhaitée.

La distinction entre ces deux sous-ensembles est une distinction conceptuelle. Au niveau d'une réalisation, cette distinction peut :

- rester virtuelle : les abonnés effectuant en temps partagé les procédures liées au traitement et celles liées à la communication.

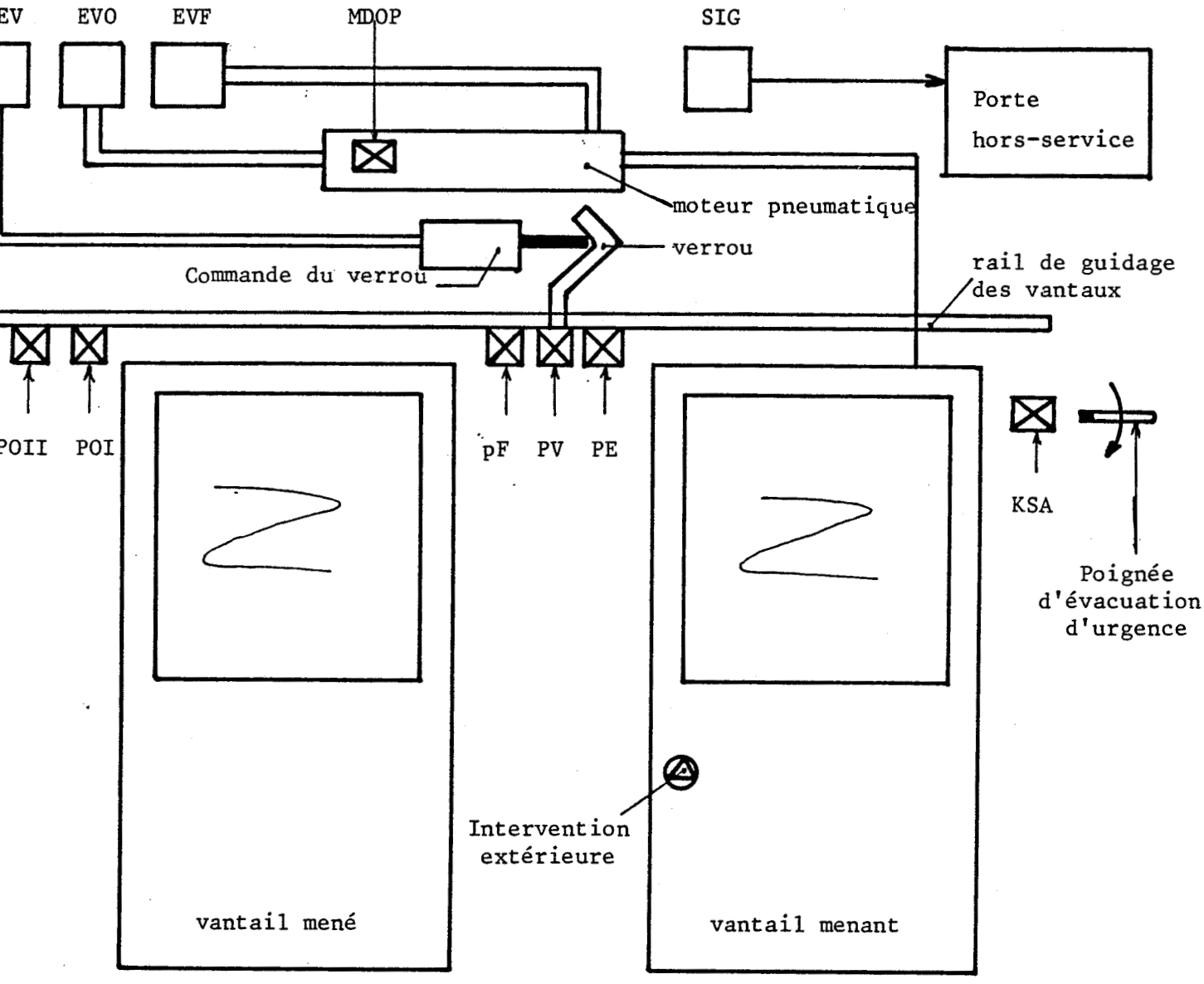
- être physiquement matérialisée : le support de communication constitue un véritable sous système qui assure les fonctions de communication laissant ainsi aux abonnés la totalité de leur puissance pour les procédures de traitement.

I. 3 - PRÉSENTATION DE LA RÉALISATION

Notre application consiste à gérer en sécurité le fonctionnement des portes d'accès à un véhicule d'une rame de métro. Chaque porte est un dispositif autonome commandé par trois électrovalves et muni de sept capteurs permettant de contrôler son état (Figure I.3).

La répartition spatiale du processus à commander justifie l'utilisation d'un système de commande-contrôle décentralisé. Les unités de commande-contrôle de niveau 1 (satellites) son regroupées par paires au sein d'une même carte électronique afin de réduire le câblage et l'encombrement. Chacune de ces cartes commande deux mécanismes de portes opposées dans le véhicule et est placée à proximité des portes commandées. Le système coordonnateur élabore les télécommandes spécifiques à chaque unité et centralise les informations de télémesure pour en établir une synthèse. Le dispositif coordonnateur dialogue avec le dispositif de conduite automatique (DCA) hiérarchiquement plus élevé d'où il reçoit les télécommandes globales et à qui il rend compte de ses activités (synthèse des télémesures). La Figure I.4 montre l'architecture du dispositif et la répartition géographique des différentes unités.

Notre travail consiste à définir les caractéristiques du réseau d'interconnexion et du système coordonnateur de manière à atteindre les objectifs de sécurité et de disponibilité attendues de l'ensemble du système.



Vecteur de commande

- EVO électrovalve d'ouverture
- EVF " de fermeture
- DEV " de déverrouillage
- SIG voyant de signalisation

Vecteur de contrôle

- pV Contact porte verrouillée
- pF " " fermée
- POI " " ouverte n° 1
- POII " " ouverte n° 2
- KSA " sécurité alarme
- MDOP manostat de détection d'obstacle à la fermeture
- PE Contact de déverrouillage extérieur

Figure I.3 : Représentation schématisée d'un mécanisme de porte.

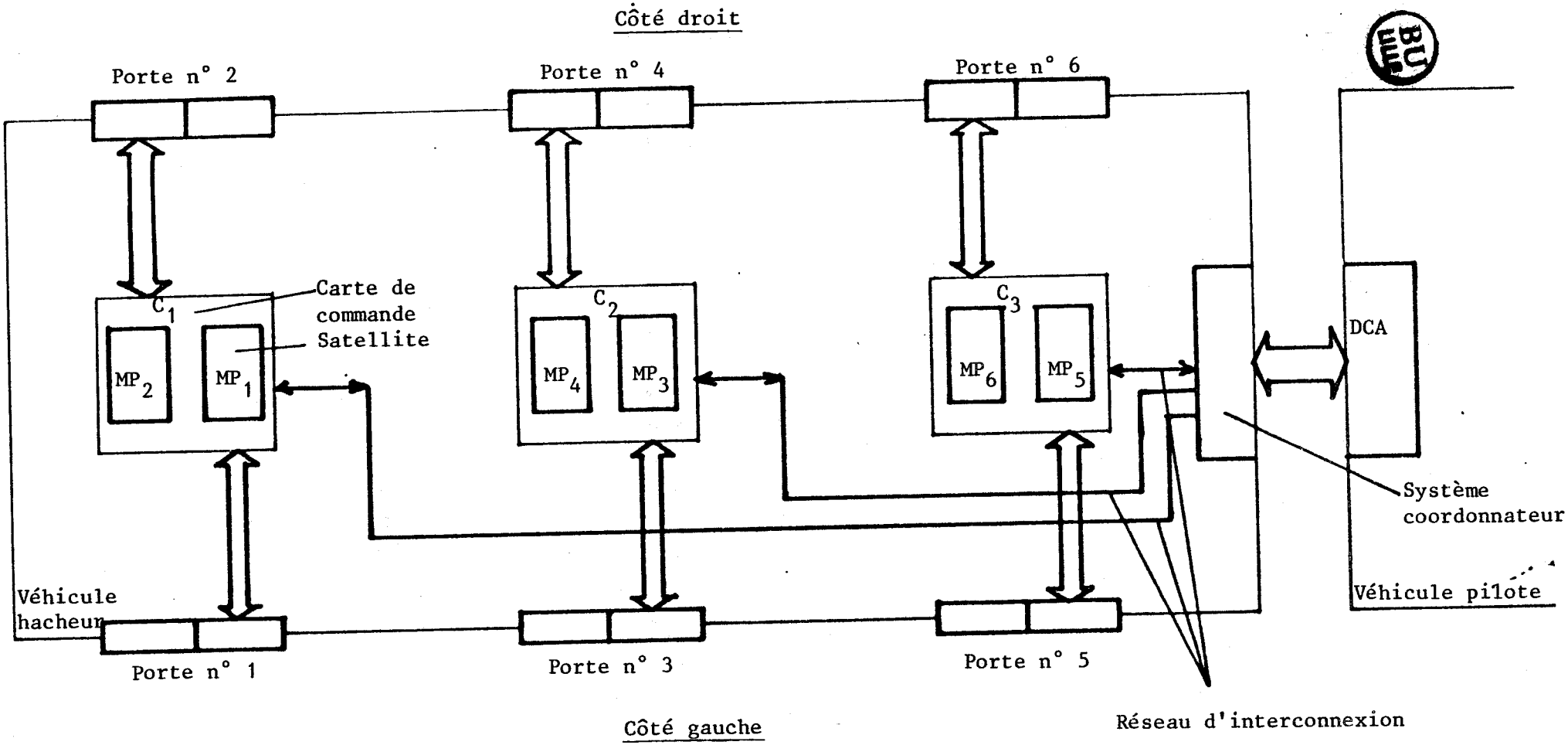


Figure I.4 : Architecture globale du dispositif de commande de portes au sein d'un véhicule

I. 4 - RAPPEL DES PRINCIPES DE SÉCURITÉ EN VIGUEUR DANS LES TRANSPORTS

La sécurité dans le domaine des transports en site propre repose sur la mise en sécurité des différents dispositifs qui constituent le moyen de transport. Chacun de ces dispositifs peut imposer de manière prioritaire un état de sécurité à l'ensemble du système (vehicule arrêté, haute tension coupée, dégagement possible des voyageurs).

Le rôle du concepteur d'un dispositif de sécurité consiste à proposer une solution où aucune panne ne peut être dangereuse. Pour parvenir à cette solution, il faut entreprendre une étude technologique approfondie des différents composants qui constituent le système. Pour un type de panne considéré sur un composant, deux solutions sont à envisager :

- il faut éviter que la panne ne se produise et pour celà démontrer que ce mode de panne est technologiquement impossible (il peut subsister un risque très faible mais non quantifiable)

- si on ne peut éviter la panne, il faut étudier ses conséquences sur le fonctionnement du montage et s'arranger pour que la perturbation engendre un mode de fonctionnement tel que la sortie prenne l'état de sécurité. Cette contrainte doit être appliquée à tous les types de pannes possibles sur tous les éléments du montage. Toute panne non détectée (ou panne dormante) n'est tolérable que dans la mesure où, combinée avec toutes les autres pannes cataloguées, elle conduit à un mode de fonctionnement sécuritaire.

Dans la mesure où l'étude de sécurité a été menée de façon rigoureuse et exhaustive et que les critères de sécurité sont applicables à tous les éléments du montage, la structure est dite en sécurité intrinsèque et présente une sécurité considérée comme absolue.

Ce type de réalisation n'est possible que pour des structures simples utilisant un nombre limité de composants réalisés à partir d'une technologie parfaitement maitrisée.

Pour une fonction à concevoir, il n'existe pas forcément une solution en sécurité intrinsèque et le concepteur est souvent amené, pour mettre son dispositif en sécurité, à avoir recours à des solutions probabilistes.

La sécurité probabiliste consiste à calculer la probabilité d'apparition des pannes dangereuses et à rendre cette probabilité inférieure à l'objectif de sécurité en redondançant les éléments déterminants pour la sécurité. L'utilisateur a pour contrainte de vérifier périodiquement le bon fonctionnement de ces éléments et éventuellement de les remplacer périodiquement. La périodicitié des vérifications est établie à partir des taux de défaillance des éléments et de l'objectif de sécurité alloué au système.

I. 5 - PRINCIPES DE SÉCURITÉ UTILISÉS POUR NOTRE ÉTUDE

La mise en oeuvre de structures microprogrammées repousse, dans le cadre de notre travail, toute approche exhaustive du problème posé par la sécurité car la logique programmée se distingue de la logique câblée et de la logique traditionnelle à éléments électroniques discrets par l'existence de deux composantes : d'une part, une composante matérielle faisant appel à une unité centrale réalisée à l'aide d'un microprocesseur, d'une structure multiprocesseurs, ou d'un processeur câblé et chargé de traiter les informations et d'émettre les ordres de commande désirés, d'autre part, une composante logicielle décrivant l'aspect fonctionnel de l'application et assurant le séquencement des diverses tâches à exécuter.

Le choix d'une logique programmée pose de nouveaux problèmes au niveau de la sécurité par rapport aux techniques traditonnelles :

- l'utilisation en logique programmée d'une majorité de circuits séquentiels (bascules, compteurs, registres ou mémoires vives) est un inconvénient majeur pour la sécurité des systèmes utilisant cette technologie.

L'aspect séquentiel d'un circuit se traduit par le fait que l'état d'une sortie à un instant donné est fonction à la fois de la configuration des entrées au même instant et d'informations internes liées aux état précédents du circuit. Ces circuits se révèlent donc sensibles en particulier aux parasites fugitifs car une information erronée aura un effet autoperturbateur sur la fonction du circuit.

- La complexité des circuits LSI et VLSI employés en logique programmée conduit souvent à un comportement imprévisible du système en cas de défaillance ou sous l'action de perturbations extérieures.

Les microprocesseurs du commerce que nous utilisons sont des composants qui intègrent un grand nombre de fonctions élémentaires dont les paramètres technologiques et fonctionnels ne sont pas tous accessibles à l'utilisateur. Ils ne peuvent être définis dans une optique de sécurité qu'au stade de la conception (projet BIST). La mise en sécurité des microprocesseurs consiste alors à proposer des méthodes de détection des pannes et une structure matérielle capables d'imposer au microprocesseur un état non contraire à la sécurité lorsqu'un défaut apparaît.

Devant la difficulté du problème, on ne peut à priori considérer que la détection des pannes est exhaustive ($\delta < 1$). De là la notion de sécurité probabiliste sur le matériel :

$$\lambda_s = \lambda (1 - \delta)$$

λ étant le taux de défaillance horaire du matériel

λ_s étant le taux résiduel de pannes non détectées et par conséquent contraires à la sécurité.

La sécurité de la composante logicielle peut être donnée sous forme d'un résultat de sécurité probabiliste car on peut envisager la fiabilité des logiciels par rapport aux deux sources d'erreurs possibles :

- Mauvaise spécification du logiciel
- Erreur résiduelle non débuggée

Les deux aspects (matériel et logiciel) sont donc homogènes dans leur aspect probabiliste et seront considérés comme tels dans ce qui va suivre. Toutefois, notre propos portera essentiellement sur la composante matérielle.

Donc, par rapport à une allocation de sécurité définie par une grandeur physique (probabilité horaire), il y a lieu de rechercher au moyen de tests (taux de couverture des pannes : δ) et si besoin par architecture, des structures dont l'indice de sécurité calculé peut être comparé à la valeur de l'objectif de sécurité (OS).

On aura deux types d'erreurs : les erreurs détectées et les erreurs non détectées. La sécurité de fonctionnement S(t) est définie comme la probabilité de survie à une panne non détectée, considérée en excès comme contraire à la sécurité, et de taux horaire I_s (notion "d'accident potentiel" |Réf. 10|). Une mesure de la sécurité de fonctionnement est le MTFMF temps moyen jusqu'à la première panne non détectée.

Le calcul de l'indice de sécurité du système est analogue à un calcul de fiabilité. La correspondance entre les termes utilisés est résumée dans le tableau I-2. Deux règles essentielles issues des théories probabilistes permettent de prendre en compte le mode d'assemblage des sous-systèmes. En termes de sécurité, les règles sont :

- Soit un ensemble comportant n sous-ensembles de sécurité respective $S_1(t)$, $S_2(t)$... $S_n(t)$ et tels que la défaillance catastrophique de l'un d'entre eux entraine la défaillance catastrophique de l'ensemble, alors :

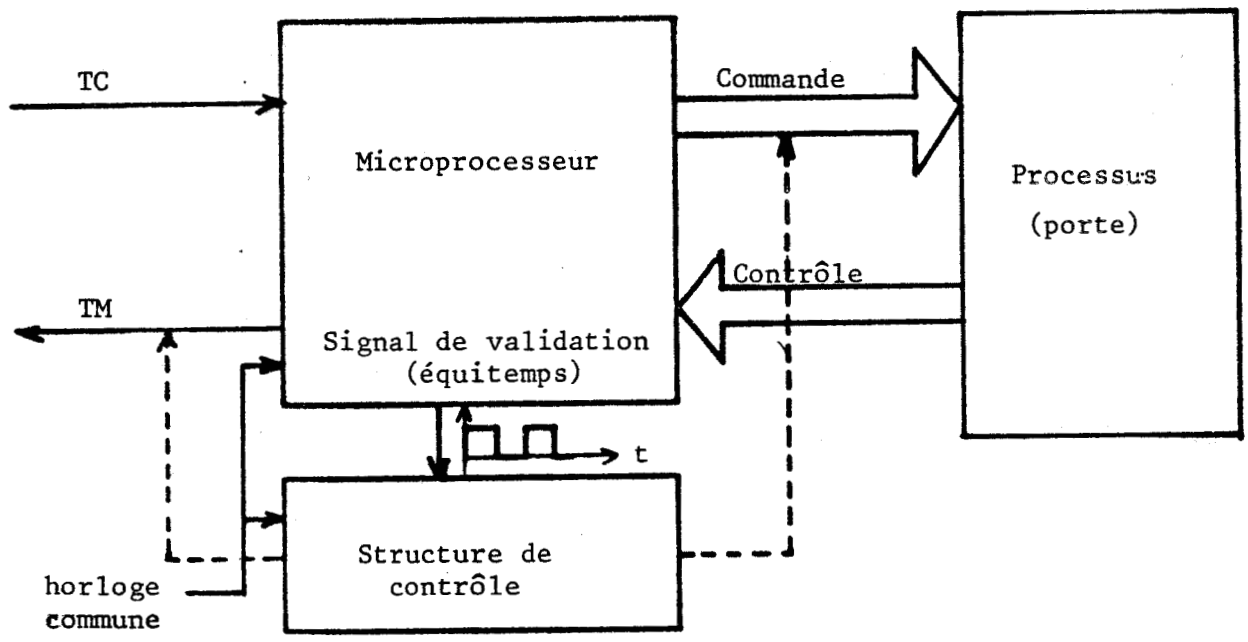
$$S(t) = S_1(t) \times S_2(t) \times \ldots \times S_n(t) \qquad (1)$$

- Soit un ensemble comportant n sous-ensembles et tel que la défaillance catastrophique de l'ensemble n'arrive que si les n sous-ensembles présentent une défaillance catastrophique, alors :

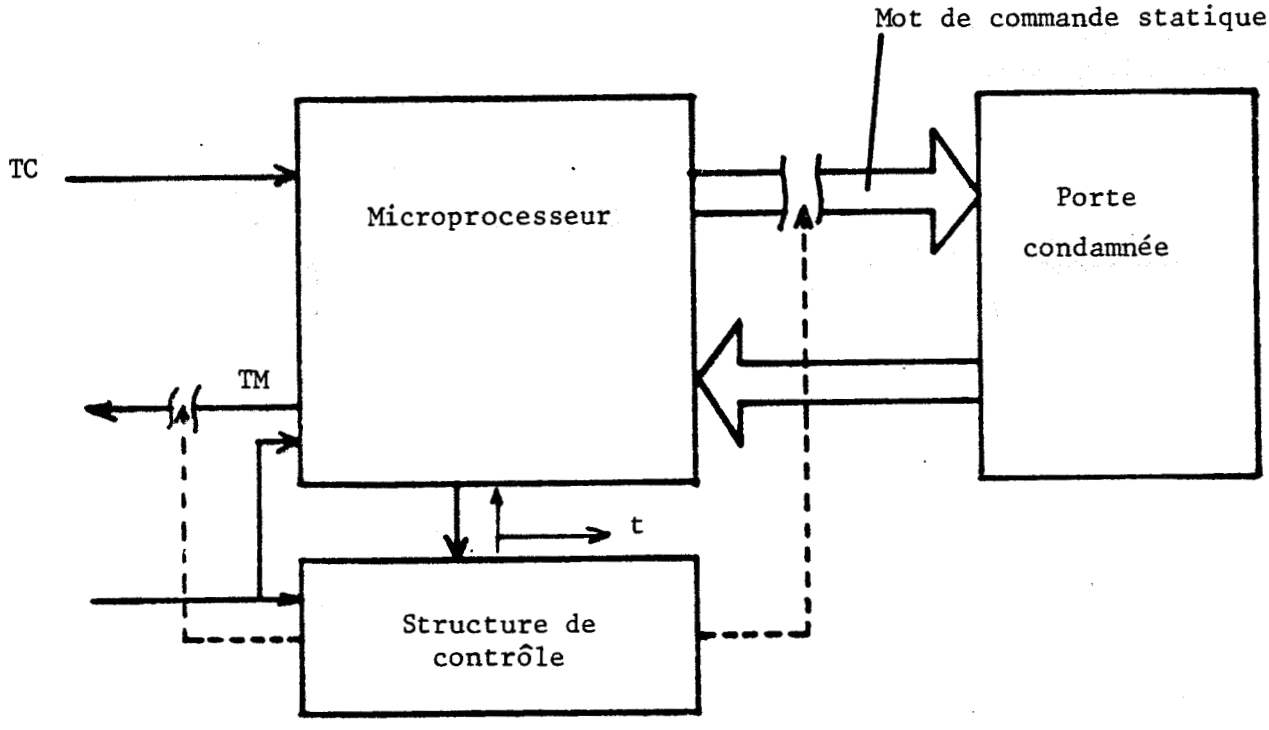
$$D(t) = 1 - R(t) = D_1(t) \times D_2(t) \times \ldots \times D_n(t) \qquad (2)$$

	Fiabilité	Sécurité
pour chaque sous-système	Taux de défaillance partiel : à λi	Taux résiduel de pannes contraires à la sécurité ou indices partiels de sécurité $\lambda_{Si} = \lambda_i (1 - \zeta_i)$
	Fiabilité = probabilité de survie au terme de la mission $\|o, t\|$ $Ri(t) = e^{-\lambda it}$	Sécurité = probabilité qu'aucun danger ne survienne durant la mission $\|o, t\|$ $S_i(t) = e^{-\lambda Sit}$
	Probabilité de défaillance entre o et t $F_i(t) = 1 - R_i(t)$	Probabilité d'apparition d'un danger entre o et t $D_i(t) = 1 - S_i(t)$
Système global	Taux de défaillance global du système $\lambda_T = - \frac{1}{R(t)} \frac{dR(t)}{dt}$	Indice de sécurité du système $I_S = - \frac{1}{S(t)} \frac{dS(t)}{dt}$

Tableau I. 2 : Analogie entre fiabilité et sécurité



Système en fonctionnement correct



Configuration de mise en sécurité du microprocesseur (état irréversible)

Figure I. 5 : Principe de mise en sécurité des satellites

La sécurité de fonctionnement ainsi définie est applicable à l'ensemble du système. Il faut pour celà déterminer la valeur des taux de défaillance λ_i et des taux de couverture de pannes δ_i des différents sous-systèmes qu'ils soient matériels ou logiciels.

I. 5. 1 - MISE EN SECURITE DES SATELLITES ET DU PROCESSUS

Pour notre application, la sécurité relative à la commande consiste à interdire une ouverture intempestive de la porte. A cet effet, la commande d'ouverture de porte s'effectue moyennant deux voies de commande indépendantes :

- une commande de déverrouillage (DEV)
- une commande d'ouverture (EVO).

La mise en sécurité des satellites est basée sur un principe combiné d'observation temporelle et de tests fonctionnels du fonctionnement du microprocesseur affecté à la commande. Une structure de contrôle en sécurité intrinsèque |Réf. 6|, valide le fonctionnement de cet ensemble. Le faible taux d'occupation du microprocesseur (processus lent) permet de traiter parallèlement à la tâche d'application des séquences de tests destinées à activer tous les blocs fonctionnels du microprocesseur et à réduire le temps de latence des pannes. L'ensemble du programme est décrit sous forme de modules équitemps |Réf. 2-3-4-5| qui permettent de générer un créneau de fréquence fixe représentatif du déroulement du programme. La structure de contrôle vérifie la conformité du signal et impose si nécessaire un état de sécurité au microprocesseur (lorsque le signal est modifié ou que la structure elle même est défaillante) (Figure I.5). L'état de sécurité consiste ici à déconnecter les sorties du microprocesseur et à imposer un mot de commande statique correspondant à l'état de sécurité (porte fermée verrouillée).

L'étude de sécurité du procédé est en cours, elle consiste à quantifier la valeur du taux de couverture des pannes. On peut à priori le considérer comme très proche de 1 par valeur inférieure. La difficulté de cette quanti-

fication réside d'une part parce que le phénomène de latence des pannes existe (durée d'une séquence complète de tests) et d'autre part parce que les modes de défaillance des microprocesseurs ne nous sont pas encore suffisamment connus pour affirmer l'exhaustivité des tests.

I. 5. 2 - MISE EN SECURITE DU RESEAU D'INTERCONNEXION

Les causes d'erreurs imputables au réseau sont :

- les défauts le liaisons (rupture, diaphonie, faux contacts)
- l'introduction d'erreurs dans les messages dues essentiellement aux parasites d'origine électromagnétique.

L'expérience nous montre que l'on peut à partir de précautions technologiques (isolement galvanique) établir un catalogue réduit de modes de défaillance et trouver durant l'exploitation tous les défauts.

Le second type de défauts, à caractère systématique, ne peut être que toléré. On peut rendre la probabilité d'insécurité due aux erreurs sur les messages compatible avec l'objectif de sécurité grâce à un codage efficace des informations |Réf. 19|.

I. 5. 3 - MISE EN SECURITE DU SYSTEME COORDONNATEUR

Le traitement à ce niveau se fait sur des messages dont le nombre et le contenu ont un caractère aléatoire et on ne peut plus envisager facilement le traitement d'une fonction équitemps. Pour assurer la sécurité, on utilisera plutôt une redondance des unités de traitement.

I. 6 - DÉFINITION D'UN INDICE DE DISPONIBILITÉ

La disponibilité s'exprime par la probabilité que le système soit dans l'état de bon fonctionnement au temps t |Réf. 11| indépendamment de sa vie antérieure.

Il faut au préalable définir la maintenabilité qui est la probabilité qu'après une défaillance, un système réparable soit remis en service en un temsp t. La relation générale exprimant la maintenabilité est :

$$M(t) = 1 - \exp\left|- \int_0^t \mu(t)\, dt\right|$$

Pour les systèmes à microprocesseurs, le taux de réparation $\mu(t)$ peut être considéré comme constant et ce pour les raisons suivantes :

- la maintenabilité consiste à faire un échange standard du sous-ensemble défaillant et à le remettre en service après les réglages et initialisations nécessaires.
- la localisation des défauts, qui est une des tâches du système, annule les temps de diagnostics qui conduiraient à une distribution "LOG" normale et non exponentielle (μ constant) |Réf. 11|.

D'autre part, compte tenu du fort rapport existant entre les taux de réparation μ et les taux de défaillance λ, la forme de la distribution (normale ou exponentielle) n'influe qu'au deuxième ordre sur les résultats. Le rapport μ/λ pour les systèmes à microprocesseurs étant largement supérieur à 100, on peut considérer les différents taux de réparation μ constants.

La disponibilité asymptotique A, est donnée pour un élément simple par :

$$A = \frac{MTBF}{MTBF + MTTR} = \frac{\mu}{\lambda + \mu}$$

MTBF = moyenne des temps de bon fonctionnement = $\frac{1}{\lambda}$

MTTR = moyenne des temps des tâches de réparation = $\frac{1}{\mu}$

La disponibilité asymptotique est celle correspondant au régime permanent. Après réparation, elle est, compte tenu des valeurs usuelles des taux d'échange standard μ du matériel, atteinte après quelques heures ou dizaines d'heures de service ; c'est donc un paramètre très représentatif et très usité pour caractériser les systèmes à microprocesseurs.

On peut définir le complément à 1 de la disponibilité A qui est l'indisponibilité U

$$U = \frac{\lambda}{\lambda + \mu} \neq \frac{\lambda}{\mu} = \lambda \text{ MTTR} \qquad (\lambda << \mu)$$

Le calcul de l'indice de disponibilité d'un ensemble utilise les règles suivantes :

soit un ensemble constitué de n sous-ensembles présentant des indisponibilités respectives U_1, U_2, ..., U_n et tels que :

- l'indisponibilité d'un sous-ensemble rend l'ensemble indisponible, alors :

$$U = 1 - A = U_1 + U_2 + ... + U_n \qquad (3)$$

- l'ensemble n'est indisponible que si chaque sous-ensemble est indisponible, alors :

$$U = 1 - A = U_1 \times U_2 \times .... \times U_n \qquad (4)$$

I. 6. 1 - AMELIORATION DE LA DISPONIBILITE

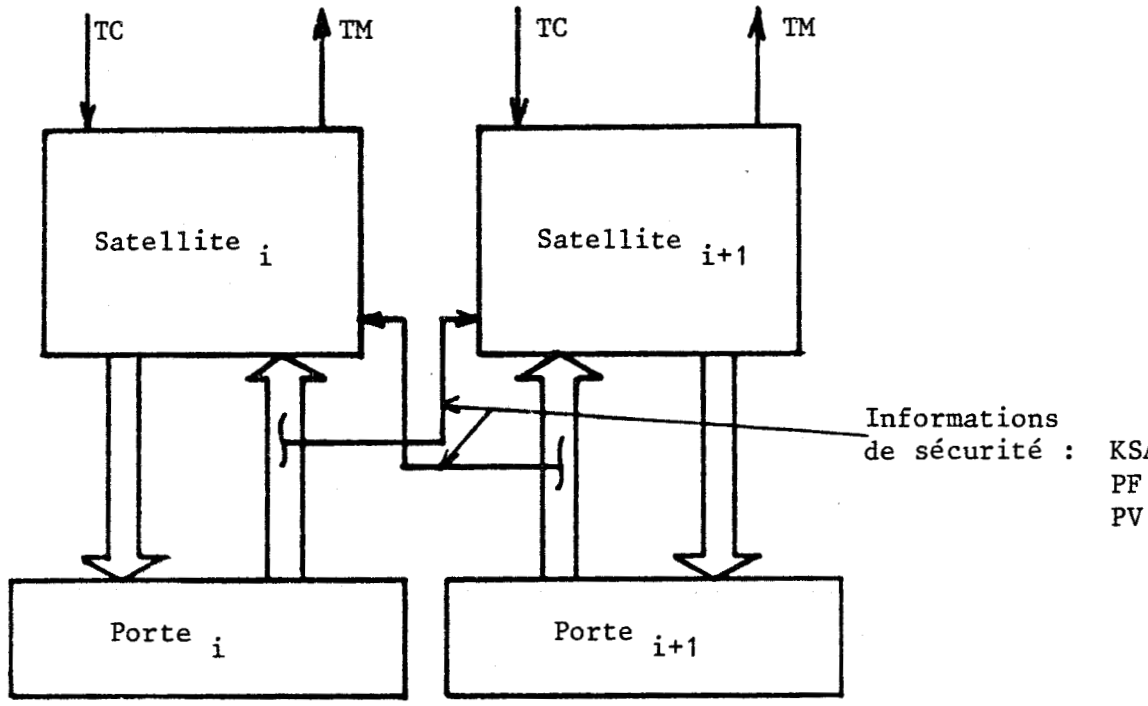
L'amélioration de la disponibilité de l'ensemble processus et système de commande contrôle hiérarchisé consiste à tolérer les défauts non contraires à la sécurité (conséquences mineures cf. § I.1.1).

Pour tolérer un défaut, il est nécessaire de prévoir une redondance suffisante au niveau de l'organe dont une défaillance veut être tolérée. L'amélioration de la disponibilité peut se faire à chaque niveau de la hiérarchie mais pas nécessairement à tous les niveaux. On cherchera en priorité à améliorer la disponibilité des organes qui présentent un taux de défaillance élevé.

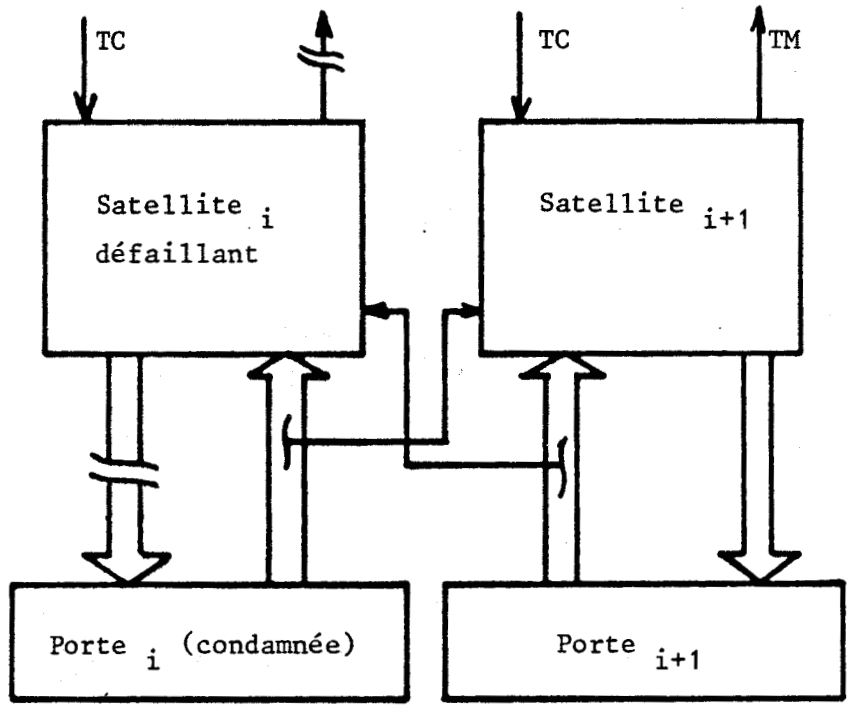
On peut tolérer les défauts affectant :

- le processus si le nombre de capteurs et la procédure de détection et de localisation des défauts permettent de détecter et de localiser toutes les pannes simples et que la présence d'un défaut quelconque ne remet pas en cause la validité du traitement des informations de sécurité. Pour un système de portes, ces informations sont fournies par les capteurs pV, pF et KSA et le traitement des informations s'apparente à un vote majoritaire (tests d'hypothèses).

- les satellites par une redondance totale ou partielle. Une redondance totale des satellites permet de poursuivre l'exploitation normale en présence d'un défaut alors qu'une redondance partielle dégrade les performances. Ce traitement par des unités différentes des informations de sécurité de chaque porte permet d'améliorer la disponibilité sans accroître le coût de la réalisation (Figure I.6). Cette redondance du traitement des informations de sécurité doit être prise en compte au niveau du logiciel de traitement du système coordonnateur qui doit être à même de détecter et de localiser tout satellite défaillant (la défaillance de deux satellites conjoints doit conduire à l'émission d'un message de danger et non plus de défaut).



fonctionnement normal



fonctionnement dégradé

les informations de sécurité permettent de déterminer si la porte se trouve dans un état de sécurité ou non.

Figure I.6 : Amélioration de la disponibilité par tolérance aux fautes d'un satellite - redondance du traitement des informations de sécurité

- le réseau grâce à une redondance des voies de transmission (maillage du réseau) et à une procédure de détection et de localisation des défauts de liaisons.

- le système coordonnateur en utilisant une redondance majoritaire (2 parmi 3) ou une redondance simple configurée en ET et commutable en OU. Cette deuxième solution nécessite une intervention extérieure afin de déterminer l'origine du défaut et commuter la redondance mais également une mise en sécurité de chaque unité.

CHAPITRE II

-o-o-o-o-o-o-o-o-o-o-

CHAPITRE II

-o-o-o-o-o-o-o-o-o-o-

SUPPORT DE COMMUNICATION

Le rôle du support de communication est de permettre aux différentes unités de traitement de pouvoir communiquer entre elles, ceci afin de traiter la tâche de commande-contrôle du processus sur un plan d'ensemble.

II. 1 - PROBLÈMES GÉNÉRAUX LIÉS AUX COMMUNICATIONS

Un problème important lié à la communication est sa relative lenteur qui est due non à la vitesse de transmission physique des signaux mais au temps nécessaire pour manipuler les informations échangées. Cette lenteur peut être particulièrement critique dans le domaine de la commande-contrôle de processus en temps réel où un retard excessif peut avoir des conséquences catastrophiques. L'environnement d'un réseau local de commande-contrôle étant le processus, les temps de réponse exigés du système d'interconnexion doivent être petits devant la plus petite constante de temps du processus (10 - 100 ms pour les systèmes électromécaniques à quelques secondes pour les systèmes industriels). Le temps de réponse total du système doit être borné, toute attente excessive pourrait en effet avoir comme conséquence la perte du contrôle du processus avec tout ce que celà implique.

Le contrôle de flux constitue un autre problème important. Ce terme recouvre les mécanismes d'asservissement d'un émetteur à un récepteur afin d'éviter les pertes d'informations dues à un débit excessif pour la capacité d'absorption du récepteur. Le contrôle de flux influence la taille des messages transmis et le volume des mémoires tampons.

Les contraintes particulières de sécurité et de disponibilité qui nous sont posées nous amènent à définir des contraintes supplémentaires propres au support de communication. Avant de définir ces contraintes particulières, il nous faut situer précisément le rôle du support de communication dans la hiérarchie globale du système de commande-contrôle.

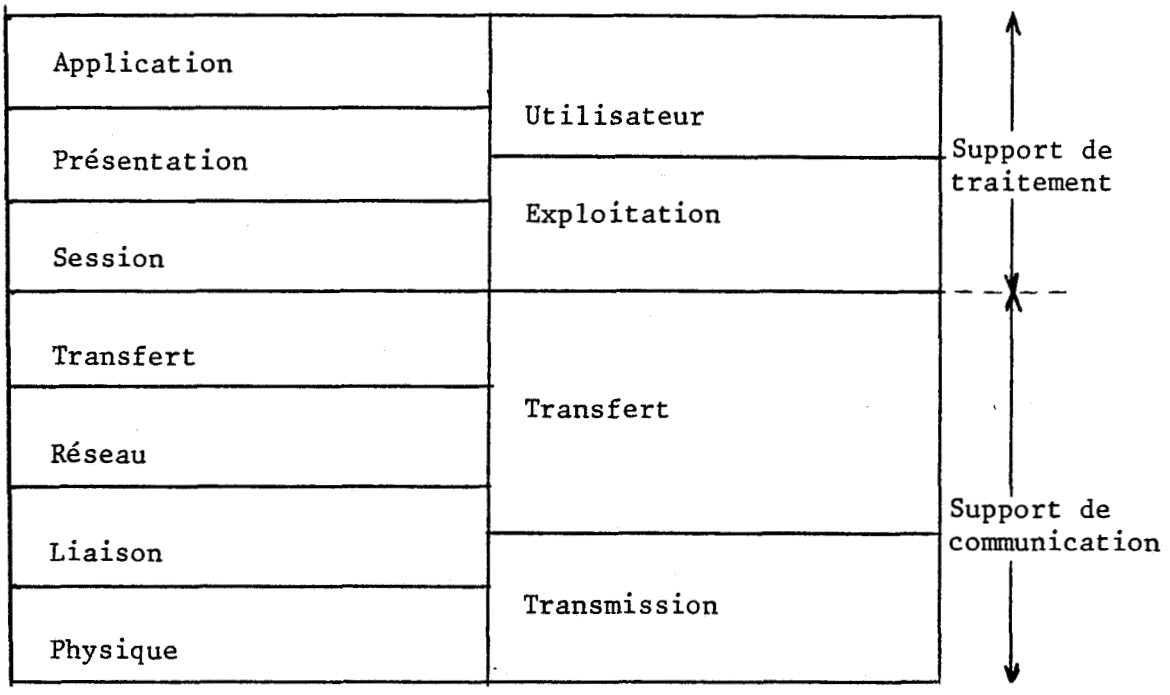
II. 1. 1 - RAPPELS DE QUELQUES CONCEPTS SUR LES RESEAUX LOCAUX

A partir d'une normalisation internationale (OSI) sur les concepts d'interconnexion des calculateurs hétérogènes dans les réseaux de type à commutation de paquets, a été élaborée une hiérarchie des tâches à réaliser dans l'optique de la commande-contrôle de processus répartis sur un réseau local |Réf. 8|. Cette hiérarchie plus restreinte (tableau II.1) distingue quatre niveaux :

- le niveau utilisateur ; le plus élevé dans la hiérarchie, c'est lui qui dialogue avec le processus commandé.

- le niveau exploitation ; il prend en compte les fonctions de gestion globale du processus en relation avec les contraintes définies par l'exploitant.

- le niveau transfert ; on définit à ce niveau des paquets de messages en relation avec le niveau exploitation. Les informations nécessaires à la synchronisation, au contrôle des erreurs et à l'acheminement des messages (adressage) sont traitées à ce niveau.



Couches correspondant au modèle ISO

Couches correspondant au modèle restreint

Tableau II.1 : Correspondance du modèle ISO et de la hiérarchie restreinte appliquée aux réseaux locaux de Commande-Contrôle

- le niveau transmission ; à ce dernier stade, on réalise l'interconnexion physique des différentes unités en incluant les problèmes de modulation.

Le rôle du support de communication est de gérer les couches transfert et transmission de la hiérarchie restreinte.

II. 1. 2 - SECURITE DE FONCTIONNEMENT

Pour le domaine d'application qui nous intéresse, la sécurité de fonctionnement de l'ensemble du système n'est pas liée à la sûreté de fonctionnement du réseau mais à sa mise en sécurité. Le concept traditionnel de sécurité positive n'est ici pas applicable car on transporte des informations sous forme de messages codés et non sous forme de signaux électriques où l'énergie est synonyme d'action. Le problème de sécurité est abordé sous forme probabiliste physiquement définie par une probabilité horaire d'insécurité.

La mise en sécurité du réseau consiste à imposer au processus l'état de sécurité physiquement défini (§ I-3). Cet état de sécurité est applicable par l'intermédiaire des niveaux supérieurs de la hiérarchie. La démarche permettant de mettre en sécurité le réseau consiste :

- à modéliser les défauts de manière à étudier leurs conséquences sur le système et sur un plan d'ensemble.

- à établir, à partir des conséquences des fautes sur les messages, des procédures de détection de pannes permettant de couvrir tous les modèles de fautes.

Les conséquences des pannes se traduisent au niveau des messages par un taux d'erreur par bit plus ou moins important (Figure II.1).

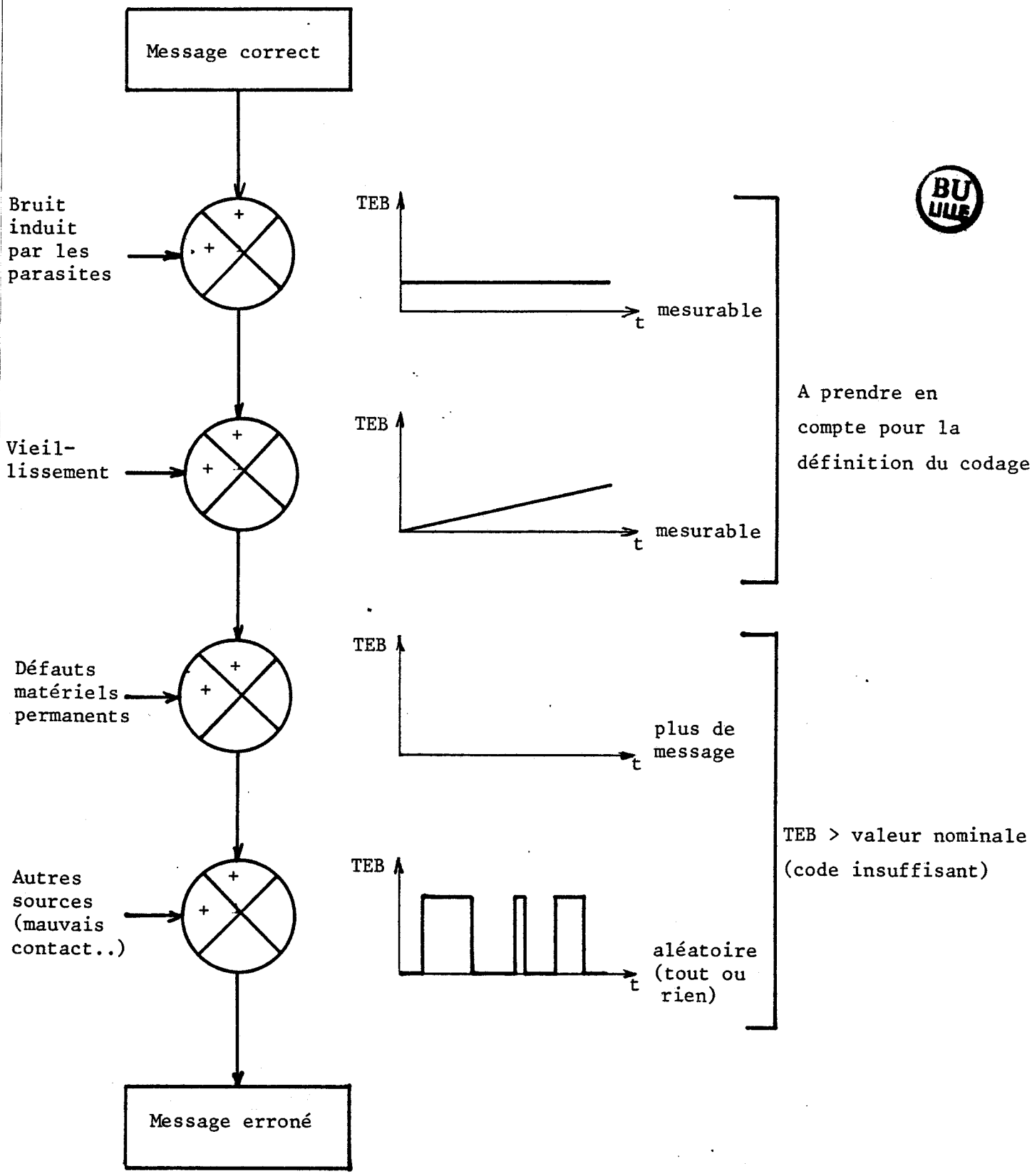


Figure II. 1 : Influence des différentes sources d'erreur sur le TEB

Il faut distinguer deux sources essentielles d'erreurs :

* les erreurs fugitives dues à l'environnement et au vieillissement des composants. Ces sources d'erreurs sont omniprésentes et doivent être tolérées. En fonction de la valeur nominale du TEB et du taux résiduel d'erreur par message que l'on désire obtenir, on définit les caractéristiques du code permettant de satisfaire de manière probabiliste l'objectif de sécurité |Réf. 19|.

Il faut au préalable déterminer le taux d'erreur moyen (TEB) et la loi d'évolution du rapport signal/bruit due au vieillissement des composants de manière à tolérer une certaine dégradation.

. Détermination de la valeur du TEB

$$TEB = \frac{\text{nombre de bits faux}}{\text{nombre de bits total}}$$

On peut avoir une valeur approchée du TEB en faisant le calcul sur les k derniers messages. Cette valeur sera d'autant plus juste que k sera grand.

Une méthode permettant de mesurer le TEB consiste à échanger des suites de messages prédéterminés et à comptabiliser les erreurs en comparant à la réception le message reçu et le message attendu.

$$TEB_i = \frac{n_{i-k} + n_{i-k+1} + \ldots\ldots + n_i}{kN}$$

$$TEB_{i+1} = \frac{n_{i-k+1} + \ldots\ldots + n_i + n_{i+1}}{kN} = TEB_i + \frac{n_{i-1} - n_{i-k}}{kN}$$

avec n_i = nombre d'erreurs sur le message i

N = nombre de bits/message.

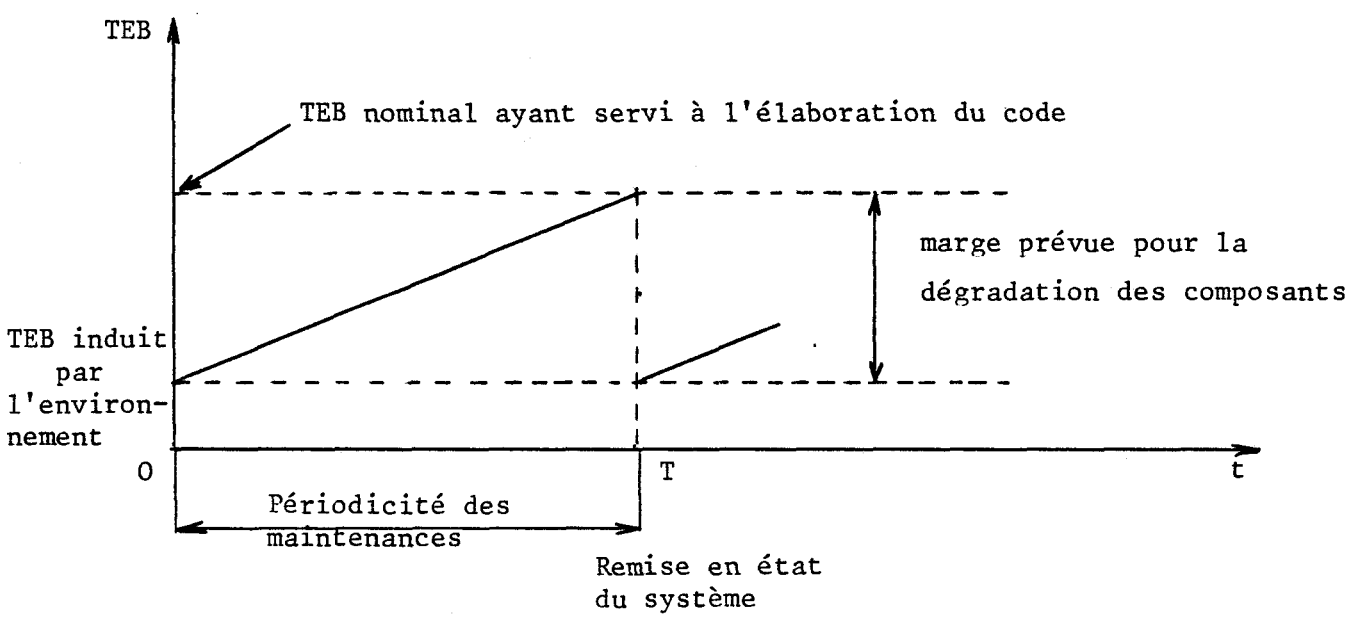
Cette opération nécessite de garder en mémoire les k dernières valeurs de n_i. Si le TEB est faible (ce qui est préférable), cette solution nécessite une grande capacité mémoire et un temps de calcul non négligeable (k très grand). On peut pallier à ces inconvénients en prenant n_{i-k} proportionnel au TEB précédent.

$$n_{i-k} = \overline{n_{i-k}} = N\ TEB_i$$

On obtient alors : $$\boxed{TEB_{i+1} = TEB_i + \frac{ni+1 - NTEB_i}{kN}}$$

Cette fonction représente l'évolution du TEB sur une moyenne de k messages.

Le vieillissement des composants pose un problème particulier au niveau de la sécurité : le rapport signal/bruit se dégrade dans le temps. Cette dégradation entraine une évolution du TEB qui peut remettre en cause l'efficacité du code. Pour satisfaire l'objectif de sécurité, il est nécessaire de remplacer systématiquement le matériel lorsque le TEB réel a atteint la valeur nominale qui a servi à l'établissement de la partition de messages codés. La périodicité des maintenances préventives dépend de la marge qui est prévue pour la dégradation du TEB ainsi que de la loi d'évolution de cette dégradation.



L'importance du phénomène de vieillissement est relative ; il faut la situer par rapport à la valeur du TEB induit par l'environnement qui peut aller de 10^{-9}/bit pour les fibres optiques à 10^{-3}/bit pour une liaison filaire. Ce phénomène est cependant à prendre en compte avant l'établissement des procédures de codage.

* Les erreurs permanentes qui sont la conséquence de défauts matériels. Les procédures de détection des défauts physiques des liaisons doivent être établies en fonction de la topologie du réseau. Ces procédures seront d'autant plus simples que le maillage est simple. La détection des défauts se faisant en ligne avec une périodicité aussi courte que possible, de manière à réduire le temps de latence des pannes.

II. 1. 3 - DISPONIBILITE DU RESEAU D'INTERCONNEXION

L'amélioration de la disponibilité nécessite de pouvoir tolérer certains défauts. Il faut pour celà faire appel à des redondances.

- Une redondance dans le maillage du réseau (cheminements multiples) permet de définir des modes de fonctionnement dégradés qui peuvent rester transparents pour l'utilisation mais néanmoins signalés. Il faut toutefois chercher à utiliser au mieux les possibilités de reconfiguration offertes par le maillage du réseau (Recherche de cheminements dégradés).

- Une redondance dans l'information utilisée à la détection des erreurs comme nous l'avons vu mais également à la correction.

II. 1. 4 - COMPROMIS SECURITE - DISPONIBILITE

Les contraintes apportées par la sécurité sont antagonistes à celles présentées par une haute disponibilité. En effet la complexité des protocoles d'échange d'informations et des procédures de détection de défauts est directement liée à la topologie du réseau par la multiplicité des chemins possibles entre deux abonnés. Plus le réseau sera maillé et plus il sera difficile de localiser un défaut voire de le détecter. Plus on cherchera à améliorer la disponibilité et plus il sera difficile d'avoir un haut niveau de sécurité. Il se dégage alors le fait que le concepteur doit satisfaire un compromis sécurité-disponibilité, c'est ce que nous avons cherché à résoudre dans notre application.

II. 2 - RAPPELS SUR DIFFÉRENTES TOPOLOGIES

Lorsqu'il s'agit d'interconnecter plusieurs entités numériques entre elles, on peut recourir à plusieurs topologies d'interconnexion différentes (Figure II.2) |Réf. 8|.

Deux voies de transmission sont utilisables :

- Voies point à point reliant seulement deux entités

- Voies multipoint reliant plus de deux entités.

Ensuite chaque entité peut être reliée à une ou plusieurs voies. On distingue alors deux types d'interconnexion :

- interconnexion régulière : il existe une relation de connexion constante entre les différentes entités voisines ; la régularité de l'interconnexion conduit à des algorithmes simples pour le cheminement des informations et va donc dans le sens de la sécurité.

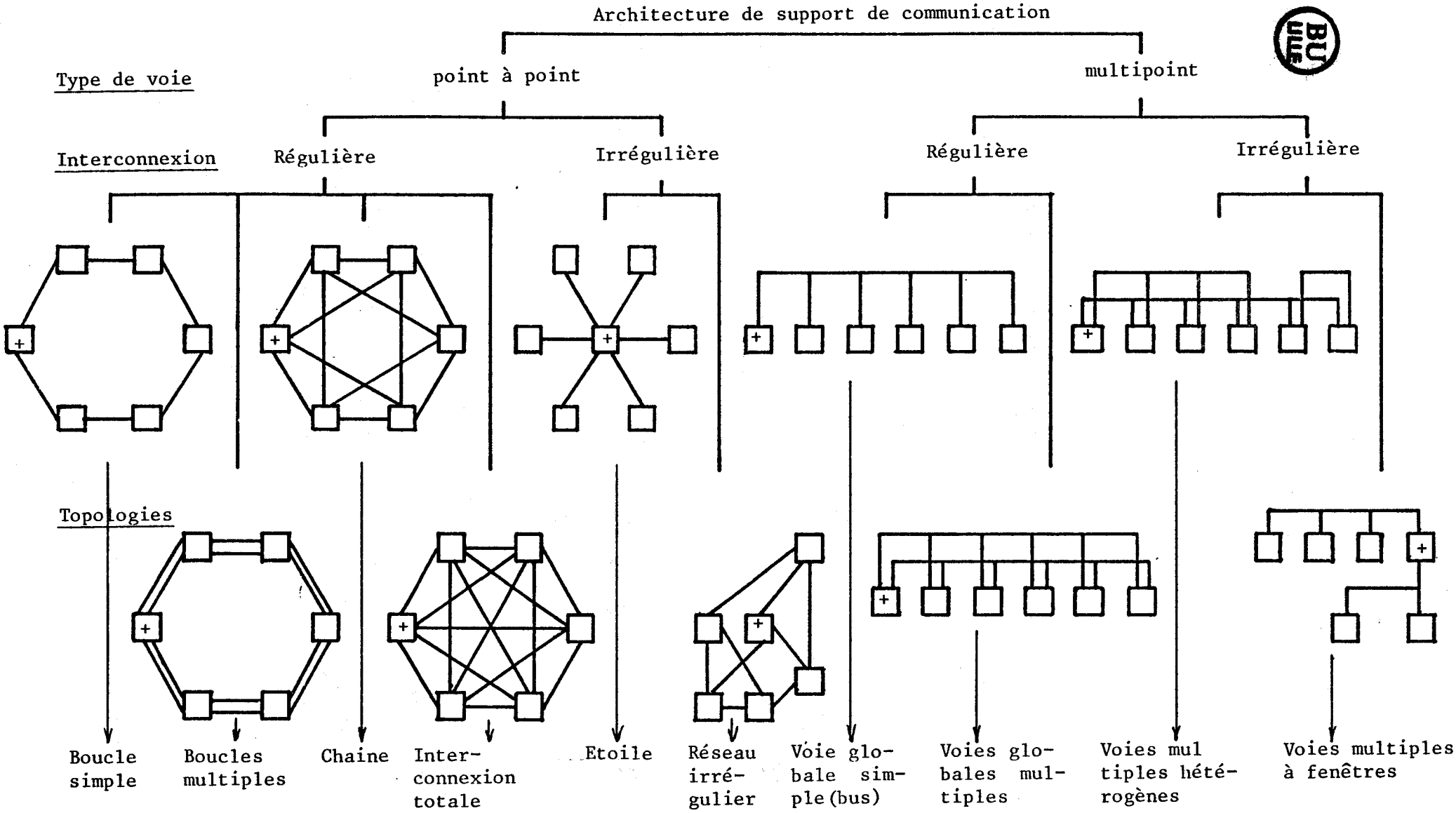


Figure II. 2 : Classification de topologies d'interconnexion

- interconnexion irrégulière : la relation de connexion entre entités voisines est arbitraire ; cette irrégularité d'interconnexion est habituellement la conséquence d'un besoin de spécialisation de la topologie en fonction de l'application.

Enfin chacune des voies peut être unidirectionnelle ou bidirectionnelle.

II. 3 - INCIDENCE DE L'EXIGENCE DE SÉCURITÉ SUR LE CHOIX À PRIORI D'UNE ARCHITECTURE DE RÉSEAU

Le recours à l'état de sécurité ne peut se faire que par le niveau le plus élevé de la hiérarchie du système de commande-contrôle, il est donc nécessaire de centraliser au niveau supérieur la tâche de détection des défauts propres au réseau d'interconnexion.

Pour que la routine de détection des défauts soit efficace ($\zeta \cong 1$), il est préférable de choisir un réseau simple c'est-à-dire ne présentant pas un niveau de redondance élevé ou des relations de connexion entre système coordonnateur et satellites irrégulières.

Ceci nous conduit à éliminer les solutions où il existe des liaisons qui ne vont pas vers le système coordonnateur car elles ne permettent pas une centralisation aisée de la détection des défauts.

Les architectures qui permettent à priori de satisfaire l'objectif de sécurité sont :

- le réseau en étoile qui n'est constitué que de liaisons directes entre chaque satellite et le système coordonnateur. Il se prête donc bien à une détection centralisée des défauts.

- le réseau en bus qui n'est constitué que d'une seule voie de transmission. Le nombre de défauts possibles est donc très limité et la détection de ces défauts peut également être centralisée.

II. 4 - CALCUL DES INDICES DE SÉCURITÉ POUR LES RÉSEAUX EN ÉTOILE ET EN BUS

II. 4. 1 - HYPOTHESES PRISES EN COMPTE POUR LE CALCUL DE L'INDICE DE SECURITE

* Hypothèses sur les erreurs de fonctionnement - Définition des sous-systèmes

- Hypothèses

Le fonctionnement incorrect des activités de communication peut résulter :

- des erreurs qui se produisent dans les processus frontaux. Les causes de ces erreurs sont des défauts de conception ou des pannes de matériel.

- de l'action des bruits d'environnement sur la transmission des messages.

- des pannes des ressources de la structure d'interconnexion : les liasions et les commutateurs.

Il peut également résulter de défauts de conception que nous ne prenons pas en compte dans notre étude :

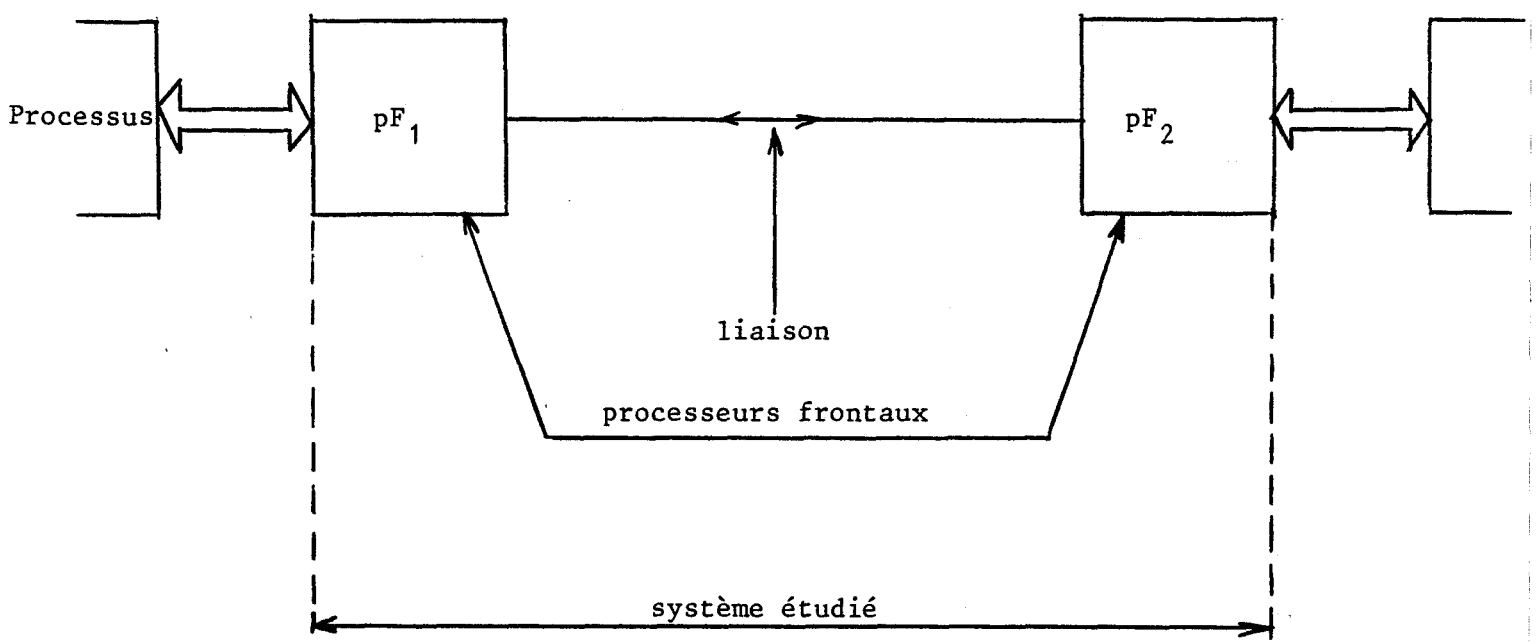
- définition insuffisante des protocoles qui peut amener à des situations dites de blocage (Dead lock).

- problèmes dits de congestion résultant de taux d'échange d'informations trop élevés.

- les sous-systèmes

L'analyse de sécurité sera faite en considérant les sous-systèmes suivants :

- les processeurs frontaux
- les liaisons
- les communications (la transmission de l'information).



* Les erreurs dans les processeurs frontaux

Etant donné le champ d'application de notre étude, nous considérons que la quantité d'informations à transmettre permet de définir des protocoles d'échange d'informations suffisamment simples pour être absolument sûrs où l'on aura eu la possibilité de réaliser des tests exhaustifs. Nous ne prendrons en compte que les pannes permanentes du matériel, ce qui nous conduit à adopter un taux de défaillance λ_c constant.

* Les erreurs dues aux pannes des liaisons

En ce qui concerne les pannes dans les liaisons (coupures ou court-circuit...), on peut utiliser les résultats de l'étude faite par Billington et Lee |Réf. 9| et adopter un taux de défaillance λ_L constant pour une liaison de longueur donnée

$$\lambda_L = x \lambda L_o$$

x = longueur totale des liaisons

λL_o = taux de défaillance d'une ligne de longueur unitaire.

A ce taux de panne λ_L, il convient d'ajouter les taux de défaillance des différents composants autres que la ligne et qui font partie de la liaison (connecteurs, coupleurs, émetteurs, récepteurs...).

Pour les liaisons, on aura un taux de défaillance global λ_1.

* Les erreurs de communication

La mesure de la valeur nominale du taux d'erreur par bit de la liaison et la connaissance du code utilisé permettent de quantifier la valeur du taux résiduel d'erreurs par bit (qui doit rester inférieur à l'objectif fixé pour l'élaboration du code cf. § II.1.2). Nous utiliserons pour la suite la nction de taux horaire d'erreurs résiduelles (ou de messages faux interprétés comme vrais) λ_1. Les notions relatives à ce taux d'erreurs sont précisées dans l'annexe 1.

Remarque :

On suppose la présence de procédures de détection de pannes dues aux défauts des processeurs frontaux et des liaisons. Toutes les pannes détectées le sont avant que leurs effets n'aient pu engendrer une situation dangereuse (hypothèse à vérifier lors de l'établissement des procédures).

Ces procédures sont caractérisées par les coefficients :

ζ_c : efficacité de la détection d'une panne d'un processeur frontal (taux de couverture des pannes)

ζ_1 : efficacité de la détection d'une panne d'une liaison.

* Sécurité de fonctionnement d'un support de communication non redondant composé de deux processeurs frontaux reliés par une voie point à point

Avant d'aborder le calcul de l'indice de sécurité d'un système complexe, nous allons traiter un exemple simple (Figure II.3) qui nous servira de base pour la suite.

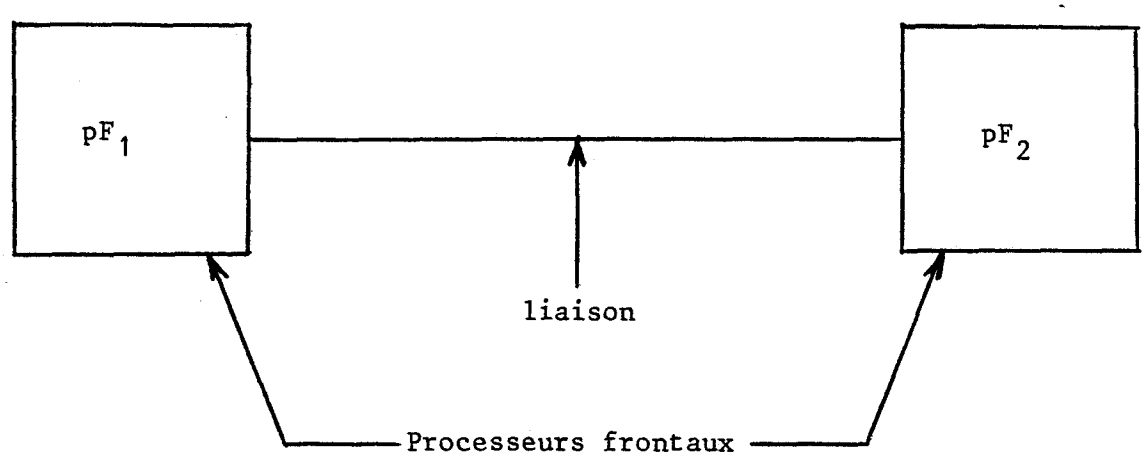


Figure II.3 : Schéma fonctionnel du support de communication pris en exemple

La première étape consiste à déterminer les indices partiels de sécurité. Cette étape est fondamentale car elle fixe les limites de chaque sous-système et par conséquent les interactions entre ces sous-systèmes.

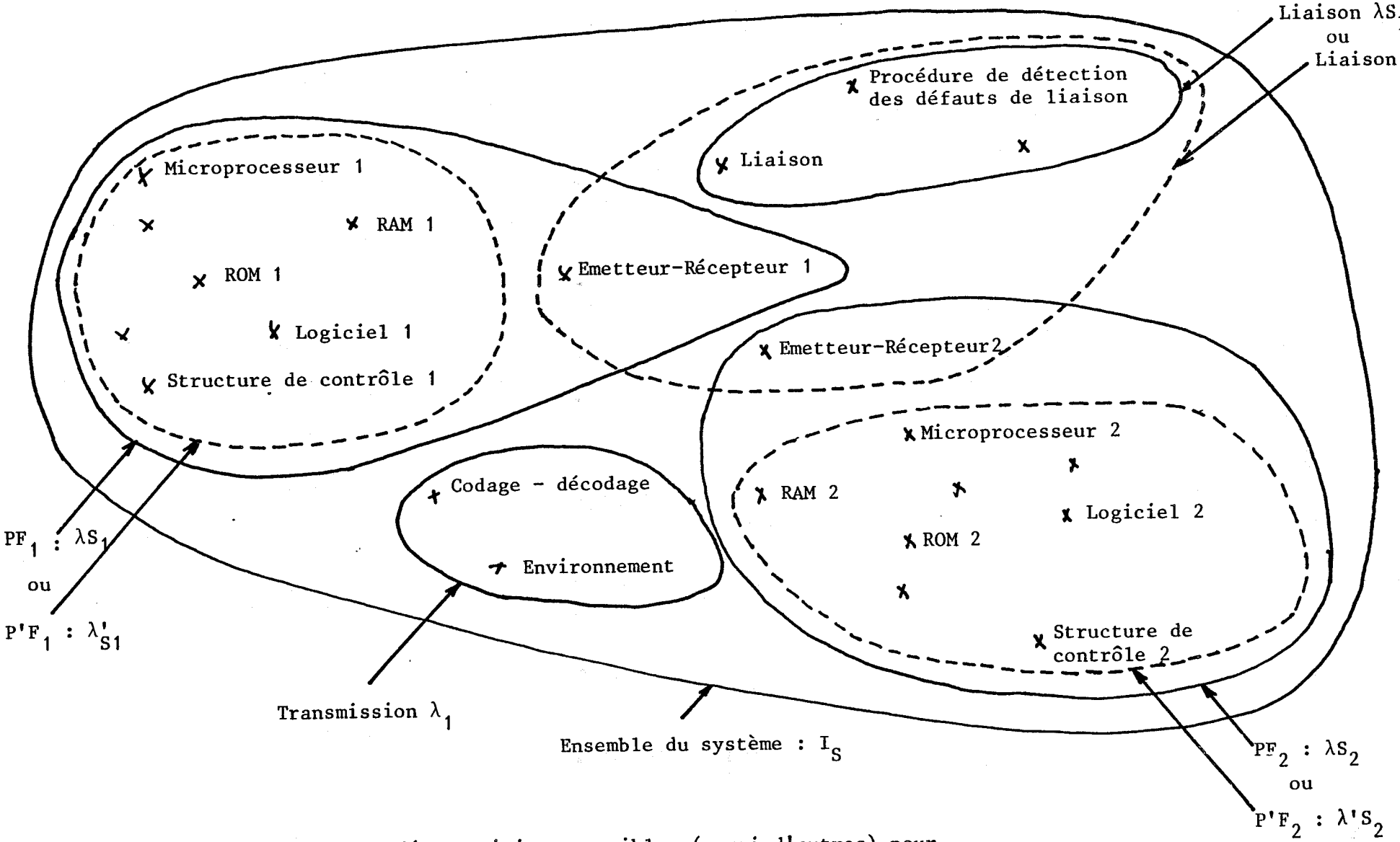


Figure II. 4 : Exemple de décompositions possibles (parmi d'autres) pour la détermination des indices partiels de sécurité

Le système étudié est décomposé en sous-ensembles disjoints, la réunion de ces sous-ensembles permettant de couvrir l'ensemble du matériel et du logiciel. La décomposition n'est pas unique (Figure II.4) mais doit s'inspirer de l'architecture du système tout en respectant les limites de couverture de pannes des différentes procédures de mise en sécurité. On ne peut, par exemple, réunir dans un même sous-ensemble un processeur frontal et une liaison qui utilisent des procédés différents de détection d'erreurs. Les sous-ensembles sont considérés comme disjoints dans la mesure où l'on considère qu'il n'y a pas de propagation d'erreurs entre les sous-ensembles.

Pour chaque sous-ensemble, on définit l'indice partiel de sécurité en fonction du taux de défaillance et du taux de couverture des pannes qui lui sont propres :

pF_1 : $\lambda S_1 = \lambda_1 (1 - \zeta c_1)$

pF_2 : $\lambda S_2 = \lambda_2 (1 - \zeta c_2)$

liaison : $\lambda s_1 = \lambda_1 (1 - \zeta_1)$

transmission : λ_1 = (voir Annexe 1).

Dans notre exemple, la défaillance catastrophique d'un seul sous-ensemble suffit à entrainer la défaillance catastrophique de l'ensemble. La sécurité du support de communication S(t) est donnée par :

$$S(t) = S_{1c}(t) \times S_{2c}(t) \times S_1(t) \times S_1(t)$$

$$S(t) = e^{-\frac{t}{MTFMF}} = \exp\left|-(\lambda S_1 + \lambda S_2 + \lambda S_1 + \lambda_1)\ t\right|$$

et la fiabilité R(t) par :

$$R(t) = e^{-\frac{t}{MTBF}} = \exp\left|-(\lambda_1 + \lambda_2 + \lambda_1)\ t\right|$$

L'indice de sécurité du système est :

$$I_S = \lambda_{S1} + \lambda_{S2} + \lambda_{S1} + \lambda_1$$

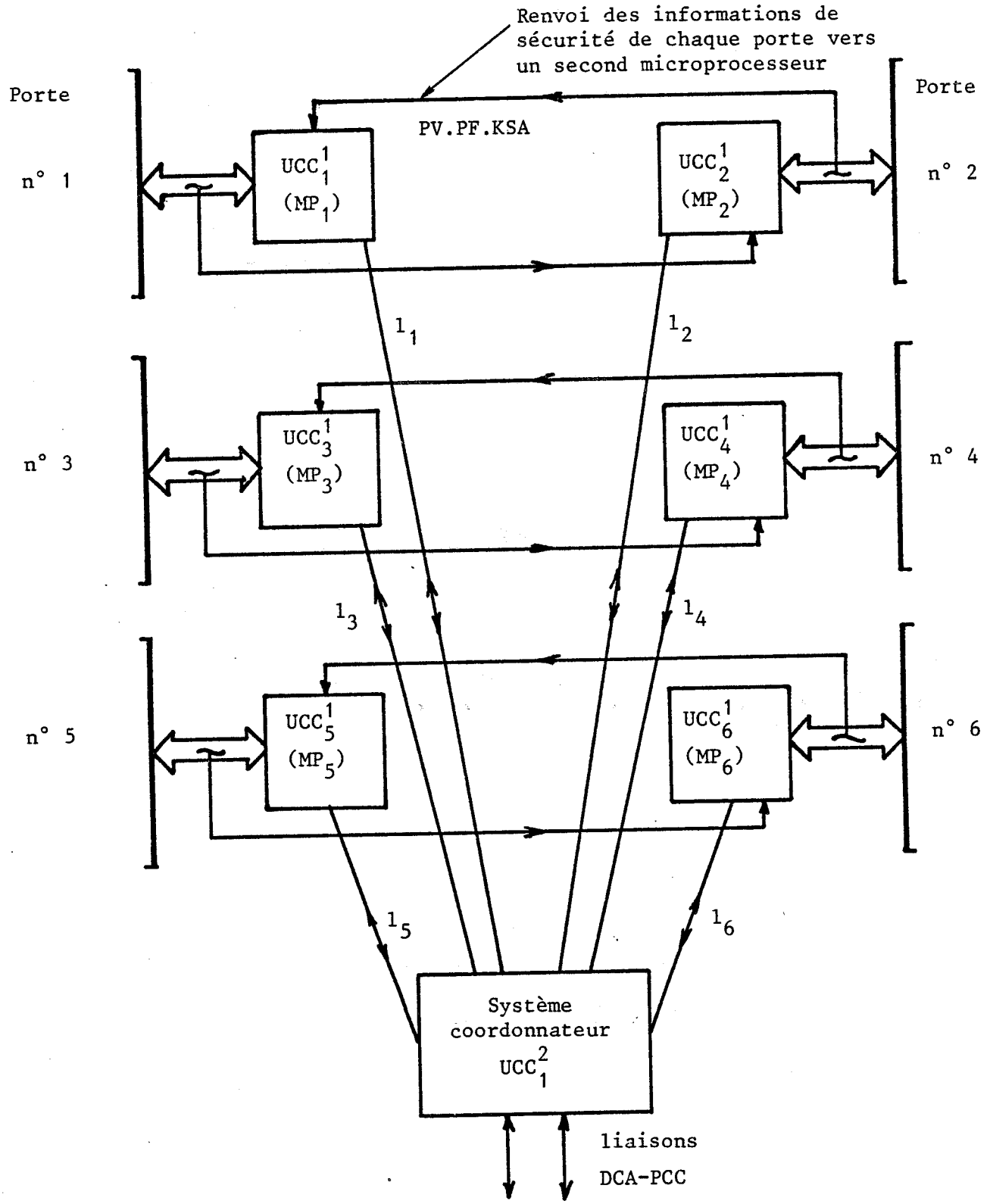


Figure II. 5 : Schéma de principe du réseau local de commande-contrôle de porte en sécurité - Bilan des liaisons

Remarque :

Dans l'expression de la fiabilité R(t), nous ne prenons pas en compte les erreurs de transmission alors qu'il existe un taux d'erreurs induites par l'environnement. La raison en est que ce type de fautes, pris en compte dans les traitements, n'entraîne aucune conséquence facheuse sur le système dans la mesure où elles sont détectées, à la différence des autres sous-ensembles pour lesquels la détection d'un défaut entraine un actionnement sécuritaire.

* Exploitation des résultats

On cherchera à minimiser chacun des paramètres de manière à atteindre l'objectif de sécurité qui a été fixé pour le système. Le calcul de ces indices nous renseigne sur l'importance de chaque terme pour une application donnée et donc sur quelle partie du système il faut apporter des améliorations. Par exemple, pour un système comportant des liaisons de grande longueur, le terme λ_1 sera prépondérant et on augmentera beaucoup plus le niveau de sécurité en créant une procédure de détection et de correction des erreurs de transmission performante qu'en cherchant à améliorer la fiabilité des liaisons ou le taux de couverture des pannes.

II. 4. 2 - APPLICATION A NOTRE REALISATION

Le schéma de principe de notre réalisation (Figure II.5) peut sembler intuitif. Nous allons cependant justifier les choix effectués en traitant différents cas de figure :

- réseau en étoile sans redondance du traitement des informations de sécurité
- réseau en étoile avec redondance du traitement des informations de sécurité
- réseau en bus simple " " " " " "
- réseau en bus double " " " " " "

Il faut tenir compte de la disposition envisagée des cartes au sein du véhicule, qui donnent des longueurs de liaisons différentes et donc des taux de défaillance de ces liaisons différents. Afin de tirer tout le bénéfice de la redondance du traitement des informations de sécurité, nous ne considérons que le cas où chaque unité dispose de sa propre liaison vers le système coordonnateur.

Satellite	UCC_1^1	UCC_2^1	UCC_3^1	UCC_4^1	UCC_5^1	UCC_6^1
longueur de la liaison	l_1	l_1	l_2	l_2	l_3	l_3
taux de défaillance	$2xl_1x\lambda l_o$	$2xl_1x\lambda l_o$	$2xl_2x\lambda l_o$	$2xl_2x\lambda l_o$	$2xl_3x\lambda l_o$	$2xl_3x\lambda l_o$
	λl_1		λl_2		λl_3	

Les longueurs étant courtes (20 mètres), nous admettons que :

$$\lambda l = \max (\lambda l_1, \lambda l_2, \lambda l_3).$$

Pour permettre une comparaison entre les solutions, nous avons défini des indices partiels de sécurité pour les sous-ensembles suivants :

- Satellite + communications : ceci revient à considérer l'environnement parfait et à ramener cette source de danger au niveau de chaque satellite

$$\lambda S_i = \lambda_i(1 - \zeta_{ci}) + \lambda_1 \qquad (1 \leq i \leq 6)$$

- Liaisons : une liaison comprend l'ensemble du matériel destiné à transporter l'information (émetteurs, récepteurs, câble, connecteurs, photocoupleurs,...) hormis le matériel commun à d'autres liaisons

$$\lambda Sl_i = \lambda l_i \ (1 - \zeta l_i)$$

- Système coordonnateur qui englobe le matériel commun à plusieurs liaisons

$$\lambda S_c = \lambda_c \ (1 - \zeta_c)$$

- Réseau en étoile sans redondance du traitement des informations de sécurité (Figure II.6)

Pour le réseau en étoile, chaque satellite dispose d'une liaison qui lui est propre. Pour simplifier les expressions, considérons :

$$\lambda S_1 = \lambda s_i + \lambda s_1$$

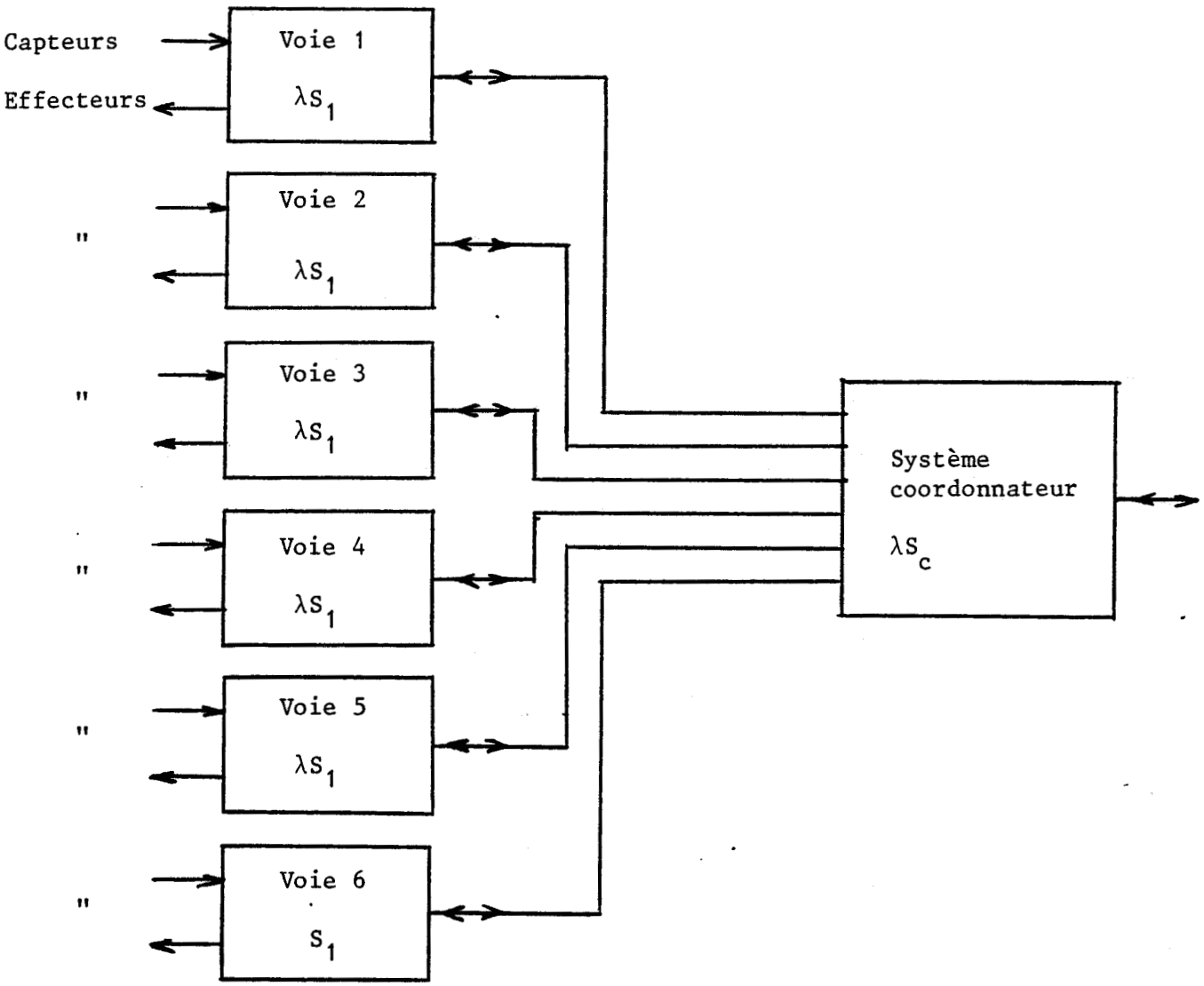


Figure II.6 : Schéma fonctionnel du système

Vu de la commande comme du contrôle, la défaillance d'un seul sous-ensemble entraine la défaillance de l'ensemble. La sécurité de l'ensemble S(t) est donnée par :

$$\underline{S(t)} = |S_1(t)|^6 \times S_c(t) = \underline{e^{-6\,\lambda S_1 t} \quad e^{-\lambda S_c t}}$$

$$I_S(t) = -\frac{1}{S(t)} \frac{dS(t)}{dt} = \lambda S_c + 6\,\lambda S_1$$

$$\boxed{I_S = \lambda S_c + 6\,(\lambda S_i + \lambda S_1)} \qquad (1)$$

- <u>Réseau en étoile avec redondance du traitement des informations de sécurité</u> (Figure II.7)

Pour la commande, le système est identique au système précédent et le niveau de sécurité n'est pas optimum. L'amélioration de la sécurité du contrôle ne permet pas d'empêcher l'apparition d'une situation dangereuse due à une commande intempestive. Pour augmenter le niveau de sécurité, il faudrait également redondancer la commande (voies de commande de deux satellites conjoints configurés en ET).

La sécurité pour ce qui concerne le traitement des informations de sécurité est donnée par :

$$S_2(t) = 1 - D_2(t) = 1 - |D_1(t)|^2$$

$$= 1 - |1 - S_1(t)|^2$$

$$S(t) = S_c(t) \times S_2(t)^3$$

$$\underline{S(t) = e^{-\lambda S_c t} \times (2\,e^{-\lambda S_1 t} - e^{-2\lambda S_1 t})^3}$$

On obtient l'indice de sécurité :

$$I_S(t) = \lambda S_c + 6\,\lambda S_1\,(1 - \frac{1}{2 - e^{-\lambda S_1 t}}) \qquad (2)$$

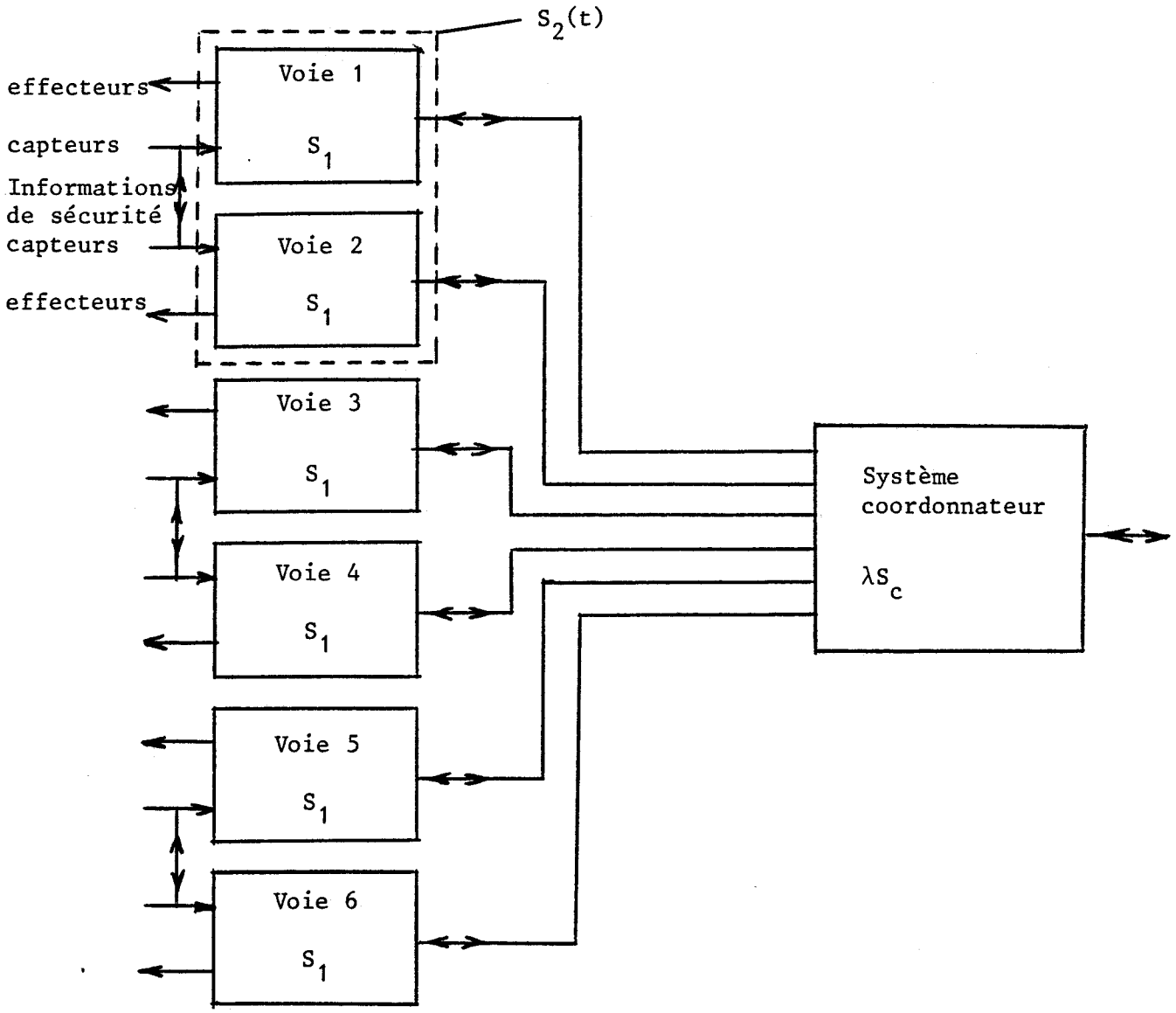


Figure II.7 : Schéma fonctionnel du système

- Réseau en bus simple avec redondance du traitement des informations de sécurité (Figure II.8)

Il faut prendre en compte la présence nécessaire de coupleurs de bus. Si un défaut au niveau d'un coupleur est susceptible de paralyser la voie de transmission (bus), les coupleurs font partie du sous-ensemble "liaison", nous avons alors

$$\lambda_{1i} = L \times \lambda_{1o} + 6 \times \lambda_{coupleur}$$

Dans le cas contraire, chaque coupleur fait partie d'un sous-ensemble "satellite".

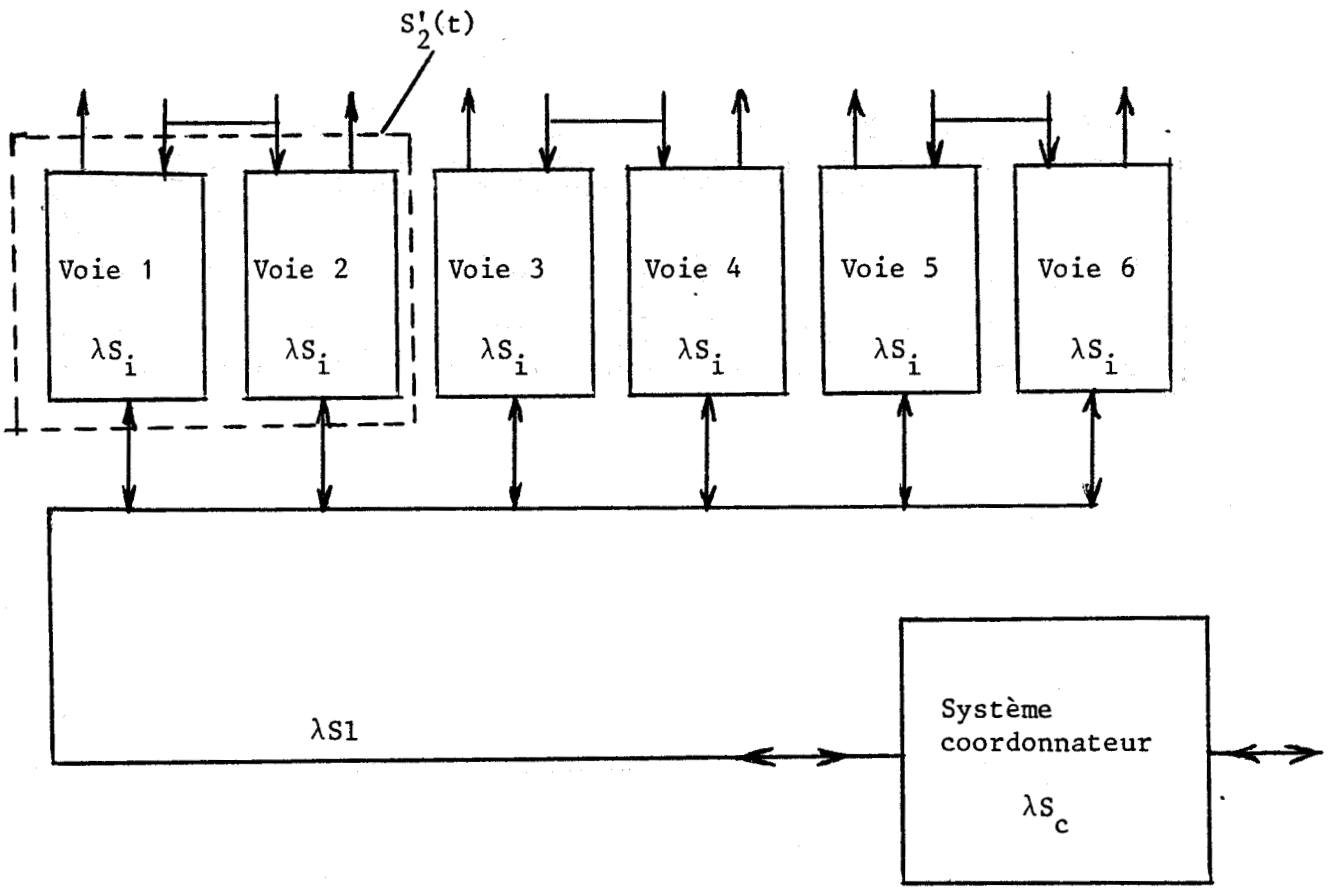


Figure II. 8 : Réseau en bus simple - schéma fonctionnel

La sécurité du système est donnée par :

$$S'_2(t) = 1 - D'_2(t) = 1 - \left|D_i(t)\right|^2$$

$$S(t) = S_c(t) \times S_1(t) \times \left|S'_2(t)\right|^3$$

$$S(t) = e^{-\lambda S_c t} \times e^{-\lambda S_1 t} \times \left|1 - (1 - e^{-\lambda S_i t})^2\right|^3$$

$$\underline{S(t) = e^{-\lambda S_c t} \times e^{-\lambda S_1 t} \times (2\, e^{-\lambda S_i t} - e^{-2\lambda S_i t})^3}$$

D'où l'indice de sécurité

$$I_S(t) = \lambda S_c + \lambda S_1 + 6\, \lambda S_i \frac{1 - e^{-\lambda S_i t}}{2 - e^{-\lambda S_i t}} \qquad (3)$$

- <u>Réseau en bus double avec redondance du traitement des informations de sécurité</u> (Figure II.9)

Dans cette configuration, il faut également prendre en compte la présence de coupleurs de bus

$$\lambda_{1i} = L \times \lambda_{1o} + 3 \times \lambda_{coupleur}$$

La sécurité du système est donnée par :

$$S(t) = \underbrace{S_c(t)}_{\text{Système coordonnateur}} \underbrace{\left|1 - D_i^2(t)\right|^3}_{\text{Défaillance de deux satellites conjoints}} \underbrace{\left|1 - D_1(t)^2\right|}_{\text{Défaillance des deux voies du bus}} \underbrace{\left|1 - D_1(t)(1-S_i(t)^3)\right|^2}_{\text{Défaillance d'une liaison et d'un satellite connecté à la seconde liaison}}$$

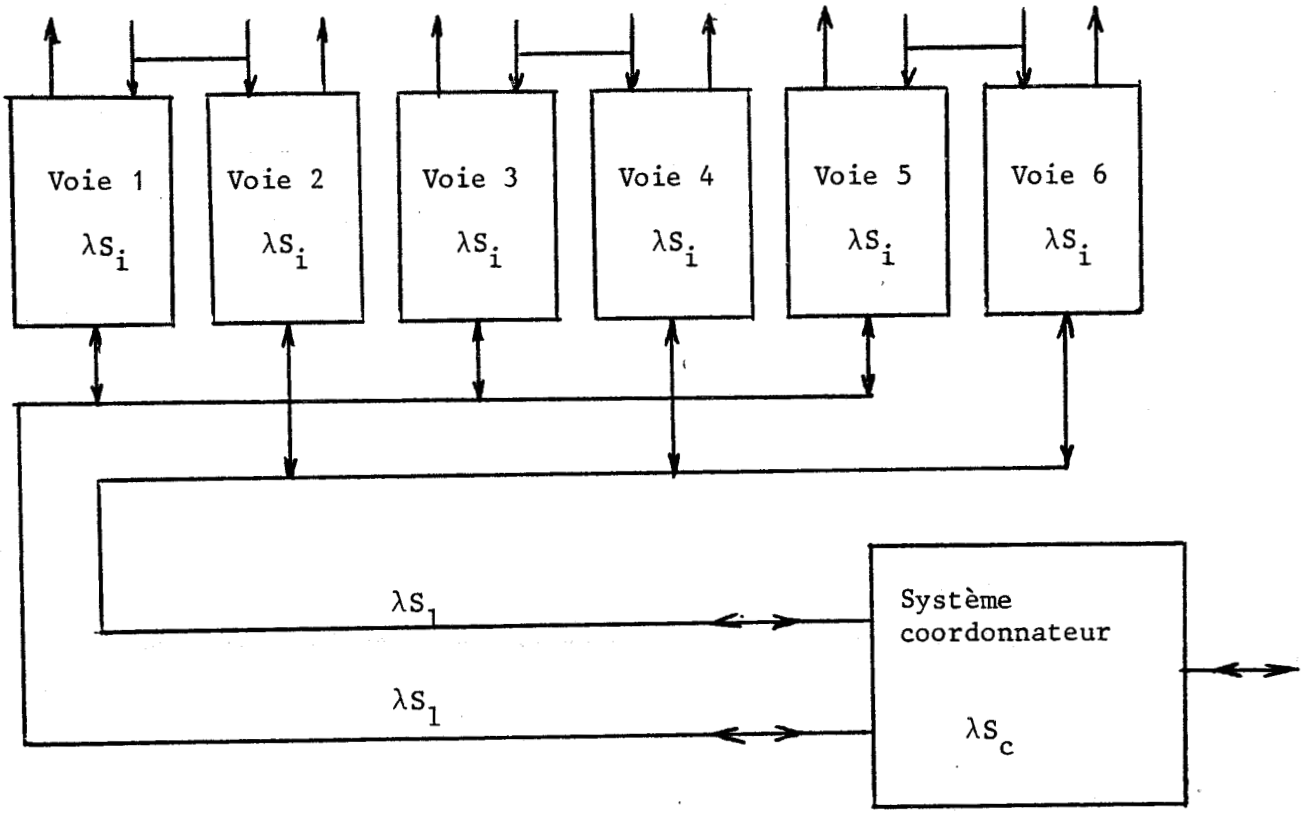


Figure II. 9 : Schéma fonctionnel du réseau en double bus

Après calculs, nous obtenons

$$S(t) = e^{-\lambda S_c t}\left(2e^{-\lambda S_i t} - e^{-2\lambda S_i t}\right)^3\left(2e^{-\lambda S_1 t} - e^{-2\lambda S_1 t}\right)\left|e^{-\lambda S_1 t} + e^{-3\lambda S_i t} - e^{-(\lambda S_1 - 3\lambda S_i)t}\right|^2$$

d'où l'indice de sécurité :

$$I_S(t) = \lambda S_c + 6\,\lambda S_i\left(\frac{1 - e^{-\lambda S_i t}}{2 - e^{-\lambda S_i t}}\right) + 2\,\lambda S_1\left(\frac{1 - e^{-\lambda S_1 t}}{2 - e^{-\lambda S_1 t}}\right) + 2\,\frac{\lambda S_1\, e^{-\lambda S_1 t} + 3\,\lambda S_i\, e^{-3\,\lambda S_i t} - (\lambda S_1 + 3\,\lambda S_i)\, e^{-(\lambda S_1 + 3\,\lambda S_i)t}}{e^{-\lambda S_1 t} + e^{-3\,\lambda S_i t} - e^{-(\lambda S_1 + 3\,\lambda S_i)\,t}} \qquad (4)$$

II. 4. 2. 1 - Comparaison entre les solutions

Le calcul que nous venons de développer ne permet pas une comparaison immédiate entre les résultats. Afin de simplifier les expressions, nous allons faire une hypothèse supplémentaire:

Pour chaque sous-ensemble, nous considérons que le taux de défaillance catastrophique λ_S est suffisamment petit pour que la probabilité d'apparition d'un "accident potentiel" durant la vie utile du système reste très faible.

Au niveau des expressions, ceci se traduit par :

$$\forall t \; : \; \lambda S_i t \ll 1$$

$$\lambda S_1 t \ll 1$$

Le fait qu'il existe des procédures de détection des pannes vient conforter cette hypothèse car il y a renouvellement du matériel lorsqu'une panne est détectée et donc retour aux conditions initiales (t = o).

Après simplification, nous obtenons, pour les cas envisagés, les indices de sécurité suivants :

$$(1) \quad I_S = \lambda S_c + 6 (\lambda S_i + \lambda S_1)$$

$$(2) \quad I_S = \lambda S_c + 6 (\lambda S_i + \lambda S_1)^2 t$$

$$(3) \quad I_S = \lambda S_c + 6 (\lambda S_i + \lambda S_1)^2 t + \lambda S_1 (1 - 6(\lambda S_1 + 2 \lambda S_i) t)$$

$$(4) \quad I_S = \lambda S_c + 6 (\lambda S_i + \lambda S_1)^2 t - 4 \lambda S_1{}^2 t$$

Le calcul de la valeur initiale (tableau II.2) de l'indice de sécurité pour différentes valeurs des indices partiels de sécurité nous permet de comparer les différentes solutions et de dégager l'importance de chaque élément.

$\lambda S_i/h$		10^{-8}				10^{-7}			
Type de réseau		1	2	3	4	1	2	3	4
0	0	610^{-8}	610^{-16}	610^{-16}	610^{-16}	610^{-7}	610^{-14}	610^{-14}	610^{-14}
	10^{-6}	$6,110^{-6}$	$6,110^{-12}$	10^{-6}	$2,110^{-12}$	$6,610^{-6}$	$7,310^{-12}$	10^{-6}	$3,310^{-12}$
	10^{-5}	610^{-5}	$6,10^{-10}$	10^{-5}	210^{-10}	$6,110^{-5}$	$6,110^{-10}$	10^{-5}	$2,110^{-10}$
10^{-8}	0	710^{-8}	10^{-8}	10^{-8}	10^{-8}	$6,110^{-7}$	10^{-8}	10^{-8}	10^{-8}
	10^{-6}	$6,110^{-6}$	10^{-8}	10^{-6}	10^{-8}	$6,610^{-6}$	10^{-8}	10^{-6}	10^{-8}
	10^{-5}	610^{-5}	$1,110^{-8}$	10^{-5}	10^{-8}	$6,110^{-5}$	$1,110^{-8}$	10^{-5}	10^{-8}
10^{-6}	0	$1,110^{-6}$	10^{-6}	10^{-6}	10^{-6}	$1,610^{-6}$	10^{-6}	10^{-6}	10^{-6}
	10^{-6}	$7,110^{-6}$	10^{-6}	210^{-6}	10^{-6}	$7,610^{-6}$	10^{-6}	210^{-6}	10^{-6}
	10^{-5}	$6,110^{-5}$	10^{-6}	$1,110^{-5}$	10^{-6}	$6,210^{-5}$	10^{-6}	$1,110^{-5}$	10^{-6}
10^{-5}	0	10^{-5}	10^{-5}	10^{-5}	10^{-5}	$1,110^{-5}$	10^{-5}	10^{-5}	10^{-5}
	10^{-6}	$1,610^{-5}$	10^{-5}	$1,110^{-5}$	10^{-5}	$1,710^{-5}$	10^{-5}	$1,110^{-5}$	10^{-5}
	10^{-5}	710^{-5}	10^{-5}	210^{-5}	10^{-5}	$7,110^{-5}$	10^{-5}	$2,10^{-5}$	10^{-5}
$\lambda S_c/h$	$\lambda S_1/h$								

Tableau II.2 : Indice de sécurité du système en fonction des taux de pannes non détectées des différents sous-ensembles au début de la vie du système (t = 1 heure).

$\lambda S_i/h$		10^{-6}				10^{-5}			
Type de réseau		1	2	3	4	1	2	3	4
0	0	610^{-6}	610^{-12}	610^{-12}	610^{-12}	610^{-5}	610^{-10}	610^{-10}	610^{-10}
	10^{-6}	$1,210^{-5}$	$2,410^{-11}$	10^{-6}	210^{-11}	$6,610^{-5}$	$7,310^{-10}$	10^{-6}	$7,210^{-10}$
	10^{-5}	$6,610^{-5}$	$7,310^{-10}$	10^{-5}	$3,310^{-10}$	$1,210^{-4}$	$2,410^{-9}$	10^{-5}	$2,10^{-9}$
10^{-8}	0	610^{-6}	10^{-8}	10^{-8}	10^{-8}	610^{-5}	$1,110^{-8}$	$1,110^{-8}$	$1,110^{-8}$
	10^{-6}	$1,210^{-5}$	10^{-8}	10^{-6}	10^{-8}	$6,610^{-5}$	$1,110^{-8}$	10^{-6}	$1,110^{-8}$
	10^{-5}	$6,610^{-5}$	$1,110^{-8}$	10^{-5}	10^{-8}	$1,210^{-4}$	$1,210^{-8}$	10^{-5}	$1,210^{-8}$
10^{-6}	0	710^{-6}	10^{-6}	10^{-6}	10^{-6}	610^{-5}	10^{-6}	10^{-6}	10^{-6}
	10^{-6}	$1,310^{-5}$	10^{-6}	210^{-6}	10^{-6}	$6,710^{-5}$	10^{-6}	210^{-6}	10^{-6}
	10^{-5}	$6,710^{-5}$	10^{-6}	$1,110^{-5}$	10^{-6}	$1,210^{-4}$	10^{-6}	$1,110^{-5}$	10^{-6}
10^{-5}	0	$1,610^{-5}$	10^{-5}	10^{-5}	10^{-5}	710^{-5}	10^{-5}	10^{-5}	10^{-5}
	10^{-6}	$2,210^{-5}$	10^{-5}	$1,110^{-5}$	10^{-5}	$7,610^{-5}$	10^{-5}	$1,110^{-5}$	10^{-5}
	10^{-5}	$7,610^{-5}$	10^{-5}	210^{-5}	10^{-5}	$1,310^{-4}$	10^{-5}	210^{-5}	10^{-5}
$\lambda S_c/h$	$\lambda S_1/h$								

Tableau II.2 : suite

- Un élément déterminant pour la sécurité est le système coordonnateur (λS_c). Lorsque ce système présente un niveau de sécurité médiocre, la mise en sécurité du reste du système est inutile (comparaison des valeurs pour $\lambda S_c = 10^{-5}/h$ à $10^{-6}/h$).

- Lorsque ce noeud est mis en sécurité (0 à $10^{-8}/h$), on remarque l'importance d'une redondance partielle des satellites (comparaison des colonnes 1 et 2) et des liaisons (colonnes 3 et 4) lorsque les pannes sur les satellites ou les liaisons ne sont pas ou peu détectables (taux de couverture faible).

- En comparant les colonnes 2 et 4 , on voit que les valeurs sont voisines et que le niveau de sécurité n'est pas directement lié à la topologie du réseau.

II. 4. 2. 2 - Conclusion sur l'étude de sécurité

Le but de notre étude est de fournir un moyen objectif de comparaison entre différentes architectures et à partir de cette comparaison, définir les points sensibles du système et les avantages et inconvénients des différentes solutions.

* Limite de validité du calcul

Le calcul développé permet de fournir une valeur numérique paramétrée par les taux de couverture de panne des différents éléments. Il ne permet pas, toutefois, de quantifier avec rigueur le niveau de sécurité global du système. Les raisons de cette limitation sont dues :

- à la non quantification du taux de couverture des pannes d'un microprocesseur. Actuellement, la mise en sécurité, par autotest, des satellites (tests fonctionnels et fonction équitemps) est basée sur un certain nombre d'hypothèses de pannes dont l'exhaustivité reste encore à démontrer. Les études en cours à ce sujet permettront, dans un avenir proche, d'apporter une solution à ce problème |Réf. 5-6-30-31|.
- aux hypothèses simplificatrices de départ.

Nous considérons que les taux de défaillance $\lambda(t)$ des différents éléments sont constants. Ceci constitue une approximation grossière pour les circuits LSI et VLSI [Réf. 13].

Nous ne faisons pas intervenir le fait que le système est réparable. En effet lorsqu'un défaut est détecté, le système est remis en état par substitution de l'organe défaillant. La variable temps que nous utilisons dans les calculs est donc réinitialisée pour cet organe.

Par ailleurs, nous ne prenons pas en compte le temps de latence des pannes car les temps de balayage des procédures de détection d'erreurs sont courts.

Cette étude de sécurité présente tout de même un double intérêt :

- elle permet de justifier le choix intuitif d'une architecture du système
- elle met en évidence le fait que le niveau de sécurité se dégrade dans le temps.

II. 5 - CALCUL DE L'INDICE DE DISPONIBILITÉ POUR LES RÉSEAUX EN ÉTOILE ET EN BUS

A chaque sous-ensemble que nous avons défini pour le calcul des indices de sécurité, nous pouvons associer un taux de réparation $\mu = \frac{1}{MTTR}$ (cf. § I.5). Chaque sous-ensemble est défini par les variables suivantes :

- Satellite : λ_i, μ_i
- Liaison : λ_l, μ_l
- Système coordonnateur : λ_c, μ_c

Nous ne prenons pas en compte l'indisponibilité résultant des défauts propres aux systèmes de portes.

* Calcul de l'indice de disponibilité du réseau en étoile sans redondance du traitement des informations de sécurité

En se reportant au schéma fonctionnel (Figure II.6), on voit que toute panne au niveau d'un satellite, d'une liaison, ou du système coordonnateur nécessite un arrêt du système pour réparation. L'indisponibilité totale qui en résulte est la somme des indisponibilités partielles :

$$U_{total} = U_c + 6\,(U_i + U_L)$$

$$= \frac{\lambda_c}{\mu_c} + 6\,(\frac{\lambda_i}{\mu_i} + \frac{\lambda_1}{\mu_1})$$

La disponibilité asymptotique est donnée par

$$A = 1 - \left| \frac{\lambda_c}{\mu_c} + 6\,(\frac{\lambda_i}{\mu_i} + \frac{\lambda_1}{\mu_1}) \right|$$

* Calcul de l'indice de disponibilité du réseau en étoile avec redondance du traitement des informations de sécurité (Figure II.7)

Pour arrêter l'exploitation d'un véhicule, et compte tenu des modes de fonctionnement dégradés, il faut que deux voies en redondance soient indisponibles ou que le système coordonnateur ne puisse plus remplir sa fonction. L'indisponibilité de l'ensemble devient :

$$U_{total} = U_c + 3\,(U_i + U_1)^2$$

$$= \frac{\lambda_c}{\mu_c} + 3\,(\frac{\lambda_i}{\mu_i} + \frac{\lambda_1}{\mu_1})^2$$

La disponibilité asymptotique est donnée par

$$A = 1 - \left| \frac{\lambda_c}{\mu_c} + 3\,(\frac{\lambda_i}{\mu_i} + \frac{\lambda_1}{\mu_1})^2 \right|$$

* Calcul de l'indice de disponibilité du réseau en bus simple avec redondance du traitement des informations de sécurité

Pour ce réseau (Figure II.8), tout défaut affectant le fonctionnement du bus nécessite un arrêt de l'exploitation. L'indisponibilité de l'ensemble est

$$U_{total} = U_c + U_L + 3\ U_i^2$$

$$= \frac{\lambda_c}{\mu_c} + \frac{\lambda_1}{\mu_1} + 3\ \left(\frac{\lambda_i}{\mu_i}\right)^2$$

La disponibilité asymptotique est donnée par

$$\boxed{A = 1 - \left| \frac{\lambda_c}{\mu_c} + \frac{\lambda_1}{\mu_1} + 3\ \left(\frac{\lambda_i}{\mu_i}\right)^2 \right|}$$

* Calcul de l'indice de disponibilité du réseau en bus double avec redondance du traitement des informations de sécurité

Pour le réseau en bus double (Figure II.9), un défaut de liaison n'est pas tolérable car il signifie l'impossibilité de commander de 1 à 3 satellites connectés sur le même bus. Pour notre application, même si l'ensemble du processus reste observable grâce à une redondance partielle des satellites, il n'est pas tolérable que l'ensemble des portes situées du même côté d'un véhicule puissent être condamnées. L'indisponibilité de l'ensemble devient :

$$U_{total} = U_c + 2\ U_1 + 3\ U_i^2$$

$$= \frac{\lambda_c}{\mu_c} + 2\ \left(\frac{\lambda_1}{\mu_1}\right) + 3\ \left(\frac{\lambda_i}{\mu_i}\right)^2$$

La disponibilité asymptotique est donnée par

$$\boxed{A = 1 - \left| \frac{\lambda_c}{\mu_c} + 2\ \left(\frac{\lambda_1}{\mu_1}\right) + 3\ \left(\frac{\lambda_i}{\mu_i}\right)^2 \right|}$$

La comparaison des résultats obtenus pour les différentes architectures permet de justifier les remarques que nous avons formulées sur l'amélioration de la disponibilité (cf. § I.6).

D'une manière générale, pour que le système présente une bonne disponibilité, il est nécessaire à tous les niveaux d'envisager des modes de fonctionnement dégradés permettant de tolérer la présence d'un défaut.

Les résultats obtenus pour les réseaux en étoile montrent que la redondance du traitement des informations de sécurité améliore nettement la disponibilité du système. La comparaison des résultats obtenus pour les réseaux en bus fait apparaitre qu'il n'y a pas de différence notable entre les disponibilités offertes par le bus simple et le bus double. Ceci vient du fait que nous utilisons des modes de fonctionnement dégradés spécifiques de notre application. Pour que la comparaison soit juste, il faudrait non seulement redondancer le traitement des informations de sécurité mais également la commande des processus (disponibilité au sens large). Pour cette même raison, le réseau en bus double présente une disponibilité inférieure à celle du réseau en étoile avec redondance du traitement des informations de sécurité. Dans chaque cas, la disponibilité du système est fortement conditionnée par la disponibilité propre du système coordonnateur (redondance majoritaire).

Pour notre application, le réseau en étoile avec redondance du traitement des informations de sécurité représente le meilleur compromis sécurité-disponibilité.

La sécurité est avant tout liée :

- à la sécurité du système coordonnateur

- au rebouclage des informations de sécurité.

Le taux de couverture de panne des satellites est déterminant pour réduire la probabilité de commande intempestive :

$$I_S = \lambda S_c + 6\,(\lambda S_i + \lambda S_l)$$

Pour le contrôle de l'état du processus :

$$I_S = \lambda S_c + 6 (\lambda S_i + \lambda S_1)^2 t$$

On rappelle que l'on considère avoir traité en sécurité la commande et le contrôle d'un mécanisme de porte ($\tau = 1$) |Réf. 2|.

Le bon indice de disponibilité est obtenu de par le fait que chaque satellite est capable d'engendrer des modes de fonctionnement dégradés (condamnation de la porte) sans interrompre l'exploitation d'un véhicule.

II. 6 - DÉVELOPPEMENT DES PROTOCOLES D'ACCÈS AU RÉSEAU

Classiquement, la gestion des accès regroupe l'ensemble des moyens mis en oeuvre pour :

- gérer les flux de messages
- détecter les erreurs de transmission.

La spécificité de notre application nous conduit à inclure les procédures de détection des pannes.

La technique utilisée doit satisfaire à deux exigences particulières :

- la sécurité de fonctionnement
- les performances temporelles.

En accord avec notre choix consistant à réaliser un dispositif de commande-contrôle hiérarchisé, il est préférable d'utiliser une technique de gestion des accès par consultation qui suppose un élément centralisé de gestion et de synchronisation. Ceci nous a conduit à ne pas retenir les

techniques de gestion par compétition plus spécifiquement destinées aux solutions totalement décentralisées nécessitant l'utilisation de véritables processeurs frontaux pour chaque abonné. Nous avons estimé que cette tâche était disproportionnée par rapport à celle mise en oeuvre par nos satellites.

Les différentes techniques de gestion par consultation sont détaillées sur la Figure II.10.

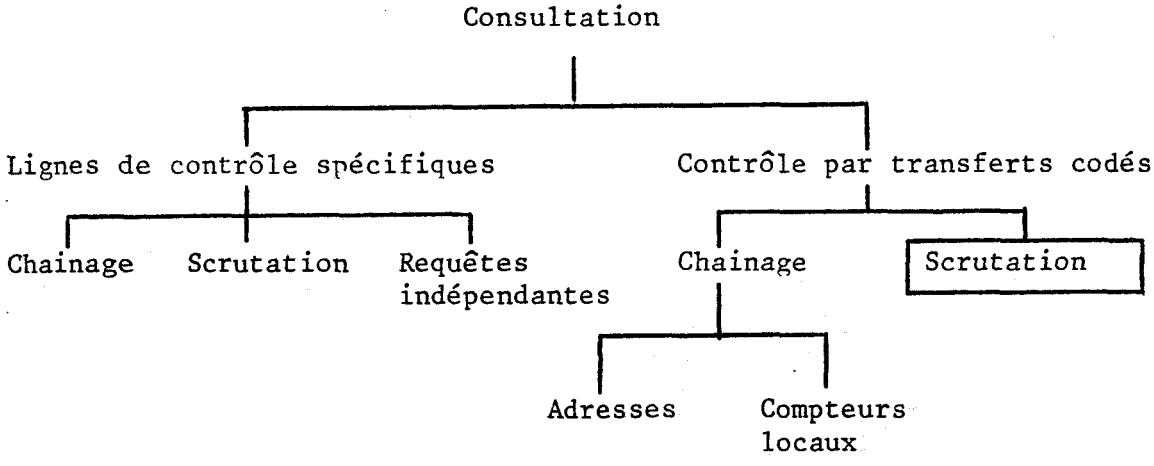


Figure II. 10 : Techniques de gestion par consultation

Le choix d'une de ces techniques se fait en fonction de la topologie du réseau. Pour un réseau en étoile, une gestion par chainage n'est pas envisageable, par contre, la consultation par chainage est particulièrement bien adaptée aux réseaux en anneau ou en bus.

Nous avons retenu le mode de gestion par scrutation pour plusieurs raisons :

- Cette technique, en laissant au système coordonnateur la charge d'organiser les échanges d'informations, répond parfaitement à la notion de système hiérarchisé.

- La détection de défauts au niveau du support de communication peut être confiée au seul système coordonnateur.

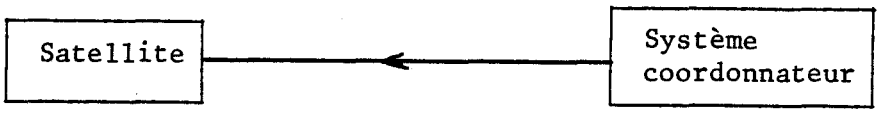
On garde ainsi l'aspect hiérarchique de l'organisation du système : chaque unité ne prend de décision que pour ce qui concerne les éléments hiérarchiquement moins élevés.

- Le logiciel à mettre en oeuvre au niveau des satellites est beaucoup moins important car on supprime à ce niveau la prise en compte des problèmes de détection de défauts et de conflits au niveau du réseau.

Ce mode de gestion n'est toutefois utilisable que lorsque le processus commandé est à évolution relativement lente. Il faut avoir le temps d'interroger chaque satellite et d'élaborer une commande en fonction de l'état du processus avant que celui-ci n'ait le temps d'évoluer de façon significative. Il est donc nécessaire dans notre cas de pouvoir majorer le temps d'une scrutation complète des satellites par le temps nécessaire à la prise en compte des défauts imputables au support de communication ainsi que celui nécessaire au traitement des informations recueillies et à l'élaboration d'une commande correspondante.

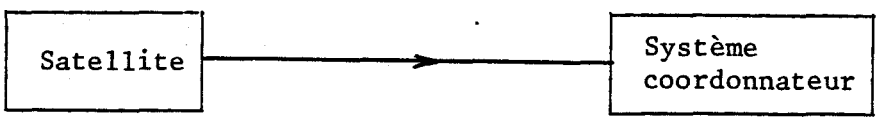
Avant de décrire la méthode utilisée, nous allons décrire précisément ce qui transite :

* Sens 1 :



Les informations échangées sont des messages de commandes.

* Sens 2 :



Les messages envoyés sont des télémesures d'état relatives :

- à l'exploitation
- à la sécurité
- à la maintenance.

Le transfert des informations de télémesure se fait suivant la méthode du polling en liste fermée (Figure II.11).

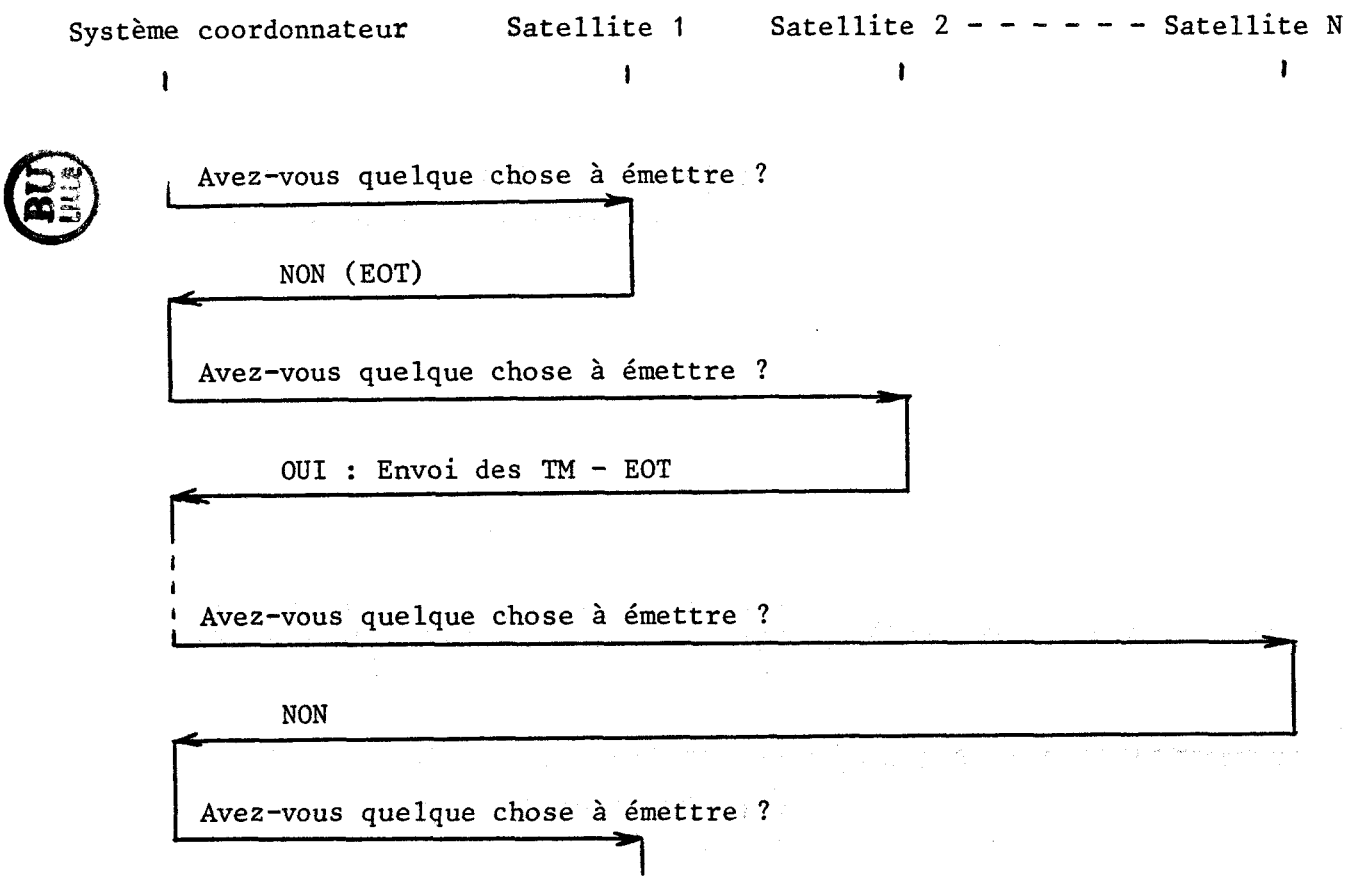


Figure II.11 : Polling en liste fermée à N abonnés

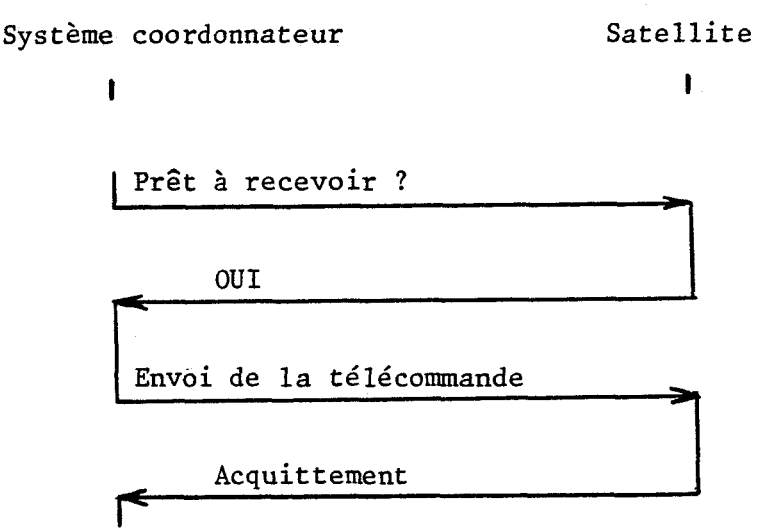


Figure II.12 : Méthode du polling selecting

Le système coordonnateur confie successivement aux satellites le statut maître. Le satellite qui dispose du statut maitre peut alors envoyer ses données vers le système coordonnateur, ou, s'il n'a rien à émettre, rendre le statut maître par l'envoi d'un caractère de procédure particulier (généralement EOT).

Le polling fait généralement référence à une table appelée liste de polling |Réf. 18|. On peut ainsi jouer sur les priorités en répétant plusieurs fois dans une même liste un satellite que l'on souhaite fréquemment interroger.

Le transfert des télécommandes peut se faire suivant la méthode du polling selecting (Figure II.12) lorsque le processus est très lent ou que la télécommande ne sera pas validée par l'émission de télémesures significatives de sa prise en compte. Pour notre application, chaque télécommande, lorsqu'elle est prise en compte par un satellite est validée par l'émission d'une télémesure représentative de l'état de la porte. Il n'est donc pas nécessaire d'avoir un acquittement immédiat de la prise en compte par chaque satellite d'une télécommande.

Ce protocole de gestion des flux de messages est utilisé pour procéder à la détection des défauts de liaisons car il permet une vérification des lignes en permanence, même en l'absence de trafic. En l'absence de messages réels, les procédures s'échangent des messages vides (passage du statut maitre) dont le bon acquittement par l'extrémité adverse permet de juger de l'état de la liaison.

La détection des défauts de liaison utilise le fait que chaque demande de télémesure doit être acquittée par chaque satellite (émission de EOT) dans un délai bien précis. En cas de non acquittement, au-delà d'un nombre de répétitions convenu, la ligne est déclarée hors service. Cette méthode n'est applicable que si on dispose d'un encadrement de la quantité de messages susceptibles d'être envoyés par un satellite. Dans le cas contraire, il est impossible de fixer un délai à l'issue duquel le satellite interrogé doit avoir acquitté la demande (émission des télémesures suives de EOT).

II. 6. 1 - DEFINITION D'UNE PROCEDURE DE DETECTION DES DEFAUTS DE LIAISONS

L'étude des modes de défaillance des composants constituant le réseau d'interconnexion et de leurs conséquences sur la transmission des messages |Réf. 27| permet de définir trois classes de défauts qui sont :

- les pannes franches, c'est-à-dire celles qui se traduisent par l'absence de message ou l'émission en continu. Cette classe prend en compte les pannes affectant un satellite et autodétectées par celui-ci. Ces pannes affectent la quantité de messages transmis.

- les défauts intermittents imputables au vieillissement des composants qui affectent le contenu des messages transmis et éventuellement la quantité (absence intermittente de transmission, faux contact...).

- les défauts naturels des liaisons qui affectent uniquement le contenu des messages en introduisant un taux d'erreur moyen (TEB).

Il faut chercher à établir des procédures particulières qui permettent de déceler tout défaut à partir de ses conséquences sur les messages. Chaque procédure particulière est destinée à contrôler un paramètre caractéristique de la transmission et permet de détecter tous les défauts qui modifient cette caractéristique. Pour obtenir un taux de couverture des pannes égal à 1, il faut que chaque défaut envisagé modifie au moins un des paramètres contrôlés. Les conséquences des défauts sont de deux ordres :

- modification de la quantité des messages
- modification du contenu des messages.

* Fautes affectant la quantité des messages

Pour détecter ce type de défauts, il est nécessaire de connaître, à priori, la quantité de messages qui doit être transmise.

Pour notre application, chaque satellite ne génère une télémesure que lorsqu'il y a :

- validation d'une télécommande
- présence d'un défaut
- présence d'un danger

Comme il ne peut y avoir validation d'une télécommande en présence d'un danger, chaque satellite n'est susceptible d'envoyer que deux télémesures au maximum à chaque demande. D'autre part, la méthode du polling que nous utilisons pour gérer les accès au réseau permet de fixer une borne inférieure à la quantité de messages.

Les paquets de messages transmis peuvent avoir les formats suivants :

EOT : pas de télémesure

TM , EOT : une seule télémesure

TM , TM , EOT : deux télémesures.

Le déterminisme des transferts de télémesures permet de contrôler trois paramètres :

- le nombre de messages est compris entre 1 et 3
- le dernier message est le mot de procédure EOT
- le temps de réponse d'un satellite est borné. Ce délai est calculé à partir du temps maximum que peut mettre le satellite interrogé pour prendre en compte l'ordre, et du temps d'émission d'un paquet de longueur maximale. Ce temps sera le temps de base de la routine de scrutation.

La seule discrimination temporelle des temps de transmission permet de contrôler les trois paramètres : à l'issue du délai fixé, on vérifie que le mot de procédure (EOT) a été reçu. S'il n'a pas été reçu, ceci indique que l'on a rien reçu ou qu'il n'a pas (encore) été envoyé et donc qu'il y a présence d'un défaut.

Cette procédure de détection des défauts permet de détecter les pannes franches du matériel ainsi que les défauts intermittents dont la durée est supérieure au temps de base de la routine de scrutation ou qui affectent le mot de procédure (EOT).

* Fautes affectant le contenu des messages

Ces défauts se manifestent de manière aléatoire et doivent pouvoir être considérés comme naturels durant toute la vie utile du système. La façon de détecter ces erreurs est, nous l'avons vu (§ II.1.2) le codage et la détection des erreurs de transmission. Le codage des informations doit permettre la correction des erreurs induites par l'environnement et le vieillissement des composants, de manière à tolérer ces erreurs, mais également la détection des erreurs dues aux défauts intermittents qui affectent le contenu des messages (faux contacts brefs induisant des paquets d'erreurs).

Ces deux procédures permettent de couvrir l'ensemble des pannes franches et des défauts naturels induits par l'environnement ainsi qu'une partie des défauts fugitifs. Pour couvrir une plus grande partie des défauts fugitifs, il faudrait normer la quantité de messages envoyés par les satellites en envoyant systématiquement trois messages. Ceci permettrait de détecter les défauts intermittents qui ont pour conséquence la suppression d'une télémesure dans un paquet. La probabilité d'apparition d'un tel défaut, bien que difficilement quantifiable, est à priori très faible et surtout ne présente pas un danger car il y a redondance du traitement des informations de sécurité.

II. 6. 2 - ORGANISATION DU LOGICIEL TRAITANT L'ENSEMBLE DES TACHES LIEES A LA COMMUNICATION

Les procédures que nous utilisons pour traiter l'ensemble des tâches liées à la communication répondent à la notion de couches de logiciel utilisée classiquement dans les réseaux locaux et rappelée au début de ce chapître

(couches ISO-modèle restreint). Les couches hiérarchiques des modèles ISO et restreint mettent l'accent sur les problèmes généraux liés aux communications mais ne proposent pas une couche caractéristique de notre problème de sécurité.

Dans le cadre de notre étude, nous pouvons proposer un modèle différent qui intègre dans sa définition les problèmes de sécurité du support de communication (Figure II.13). La couche supplémentaire qui est introduite par rapport au modèle restreint est destinée à spécifier les procédures de détection des défauts de liaisons (indissociables des protocoles de gestion du réseau).

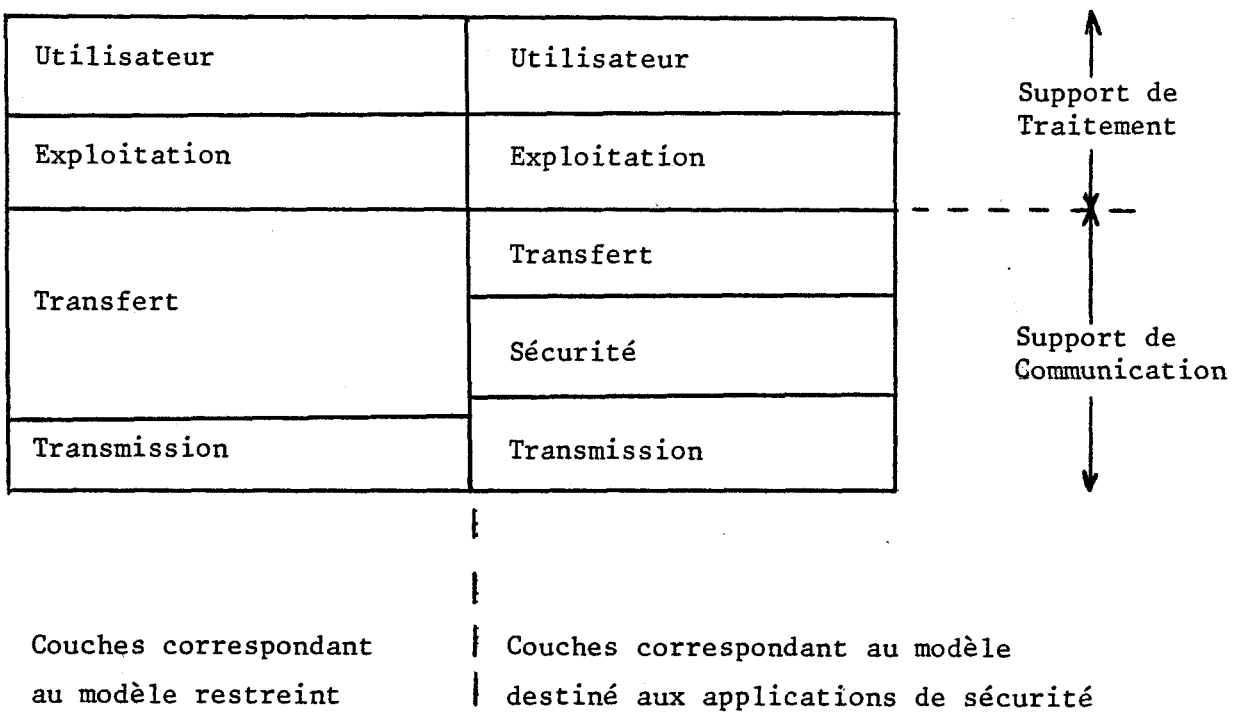


Figure II.13 : hiérarchie des tâches dans les applications de sécurité

Le niveau transmission est chargé de coder et décoder les informations et de réaliser l'interconnexion physique entre les abonnés.

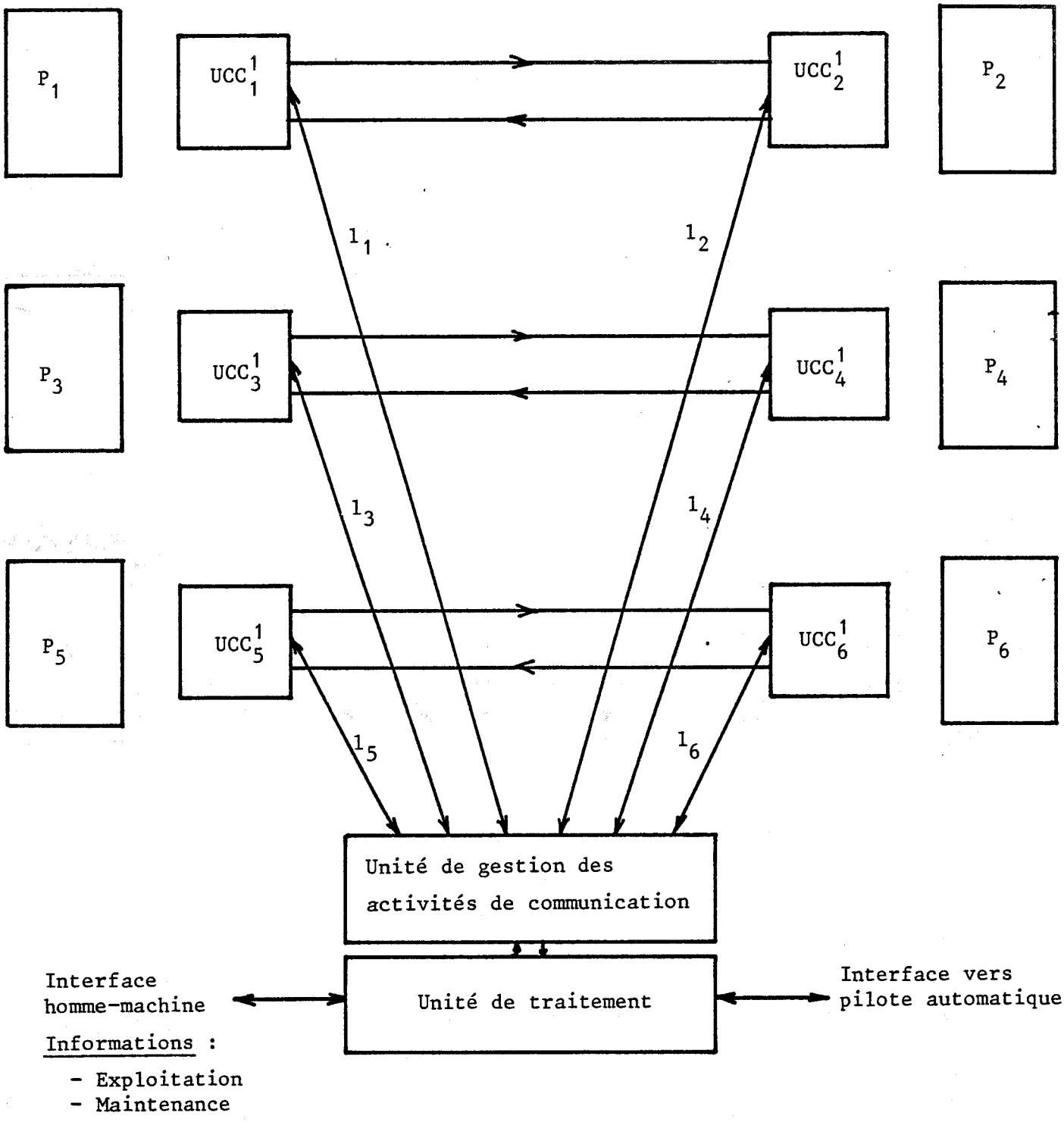


Figure II. 14 : Bilan fonctionnel des liaisons

Le niveau sécurité est chargé d'organiser les transferts d'informations entre abonnés (scrutation des satellites par la méthode du polling) et d'en extraire les deux types d'informations utiles pour le niveau transfert. Ces informations sont, d'une part, les messages de télémesures et d'autre part, les informations de pannes élaborées par les procédures de détection qui sont intimement liées à la procédure de gestion des flux d'informations.

Le niveau transfert est chargé d'organiser le transfert des télémesures vers le niveau exploitation du support de traitement (arrangement par paquets et par trames, protocole d'échange). Il est également chargé de recevoir les télécommandes et de les envoyer vers les satellites.

II. 7 - RÉALISATION DE LABORATOIRE - PERFORMANCES OBTENUES

BUT DE LA RÉALISATION

Le but de notre réalisation est la mise en oeuvre des procédés de contrôle de flux mais aussi de détection de défauts (reprise de toutes les particularités développées dans le chapître II). Toutes ces contraintes sont gérées dans un environnement proche de la réalité de par les processus à commander et la présence d'interfaces homme - machine à plusieurs niveaux, comme le montre le bilan fonctionnel des liaisons (Figure II.14).

Les mécanismes de porte sont constitués soit par un mécanisme réel ou par des simulateurs appelés portes fictives |Réf. 27| constitués par un microprocesseur dans lequel on a implémenté une tâche simulant le fonctionnement d'une porte. Les six mécanismes ou équivalents existent donc et leur fonctionnement est indépendant (décorrélation dans le temps).

De par le mode de traitement des graphes de Pétri sur les satellites, la vitesse maximale d'évolution du processus est de 10 ms entre deux changements d'état consécutifs.

Au niveau centralisé, nous avons un processeur chargé spécifiquement des accès au réseau (8085 à 4,84 MHz et deux USART 8251). Sa fonction est la suivante :

* Au niveau transfert :

  - elle élabore les trames d'informations destinées au support de traitement
  - elle envoie vers les satellites les télécommandes issues du support de traitement

* Au niveau sécurité :

  - elle gère la routine de scrutation des satellites
  - elle gère la procédure de détection des défauts

* Au niveau transmission :

  - elle code et décode les informations.

La vitesse de transmission est de 1200 bauds et chaque information est codée sur deux octets.

La période de scrutation des processus est de 360 ms soit, vu du système central, une période unitaire de scrutation de 60 ms.

Le nombre de changement d'état significatif, donnant lieu à des télésignalisations est de $4,5\ 10^{-2}$/seconde (4 sur 1 minute 30) si on se refère au cycle moyen de fonctionnement d'une porte |Réf. 1|. Une telle estimation qui peut s'avérer utile pour des processus parfaitement indépendants, est sans intérêt dans le cas des portes car les cycles de fonctionnement sont quasiment synchrones et par conséquent, la quantité de messages est très variable dans le temps.

Dans l'état actuel de son fonctionnement, le système coordonnateur est capable de recueillir 16 paquets d'informations par seconde soit, au maximum, 32 télémesures par seconde. Le nombre de mécanismes de portes que l'on pourrait traiter est fonction du temps maximum que l'on peut tolérer entre l'apparition d'un évènement significatif et sa prise en compte (par exemple, pour 15 mécanismes de portes, le délai maximum pour traiter une évacuation d'urgence (EVAC) sera de 1 seconde).

Les résultats que nous venons d'exposer amènent deux remarques :

- La méthode du polling que nous avons retenue dans un souci de sécurité ne permet pas d'accéder au domaine du traitement en temps réel. On aura toujours un décalage entre évènement et prise en compte de cet évènement au maximum égal à une période de scrutation des satellites.

- Nos résultats ne prennent en compte que l'acquisition des informations et non le traitement. Si on peut, au niveau de l'acquisition augmenter les performances en diminuant le temps unitaire de scrutation, il est par contre difficile de réduire le temps de traitement d'une information. Les performances du système coordonnateur seront donc essentiellement conditionnées par le traitement.

II. 8 - ASPECT TECHNOLOGIQUE DES TRANSMISSIONS

Une étude de la technologie optique en vue d'une réalisation du réseau d'interconnexion |Réf. 22-28| a permis de montrer qu'elle n'était pas adaptée à notre problème il y a encore quelques années. Cette technologie très performante présente les avantages suivants :

- immunité aux parasites électromagnétiques
- isolement galvanique

Par contre elle présentait les inconvénients suivants :

- coût très élevé
- composants mal adaptés à notre réalisation car il n'y a pas de composants peu performants (10 Kbaud max) mais très robustes
- technologie nouvelle et donc fiabilité peu connue.

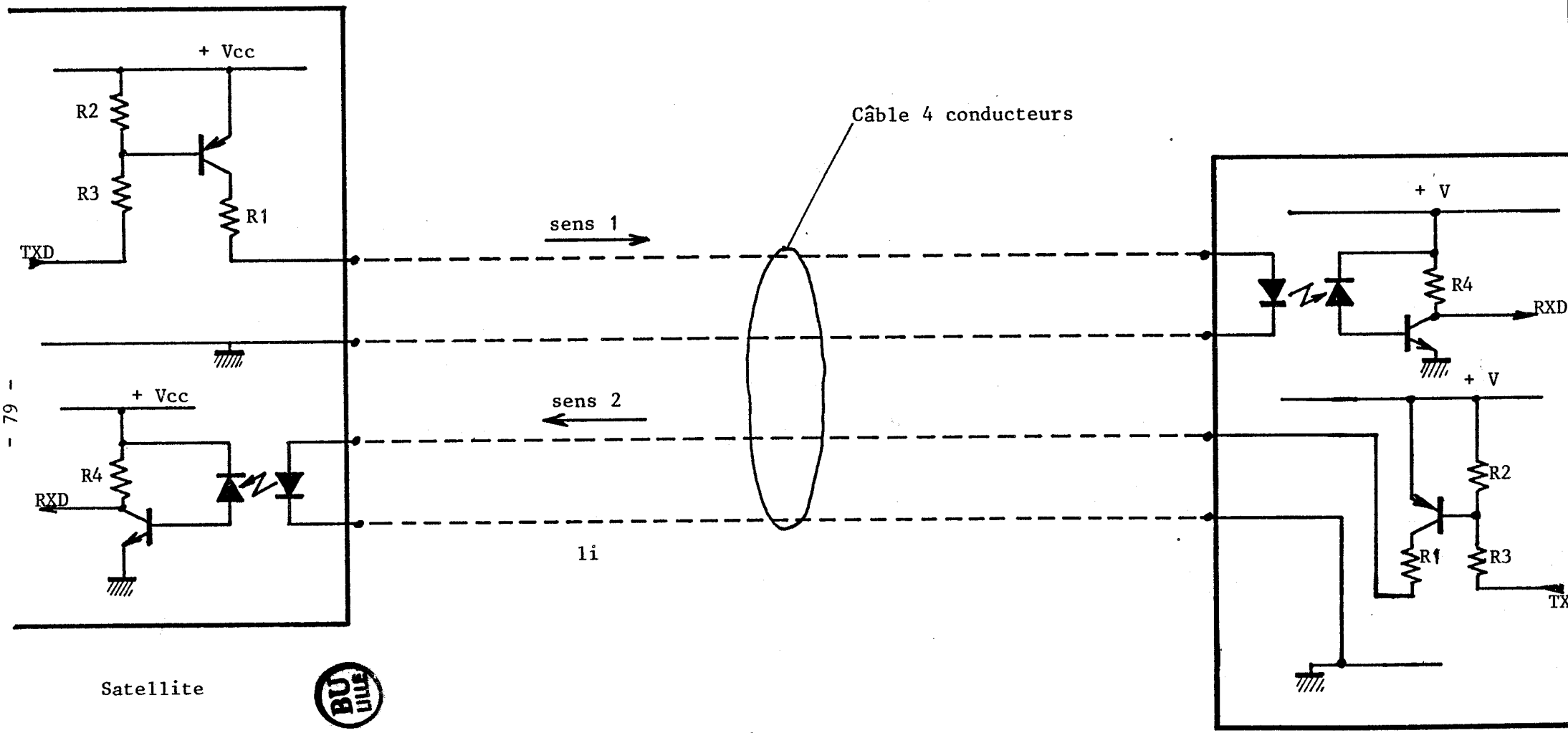


Figure II. 15 : Liaisons bifilaires en boucle de courant

Actuellement, l'arrivée sur le marché de fibres optiques plastique à faible coût remet en cause cette étude et on peut espérer dans quelques années utiliser avantageusement cette technologie.

Notre réalisation utilise des liaisons filaires classiques. La transmission des informations se fait par boucle de courant avec isolement galvanique (photocoupleurs) de manière à éviter les pannes de mode commun sur plusieurs liaisons, les diaphonies...

Le matériel utilisé pour réaliser chaque voie de transmission (Figure II.15) permet d'établir un catalogue des pannes à détecter et de leurs conséquences sur la transmission des messages |Réf. 27 - tableau II.3|. Il faut rappeler que les pannes intervenant sur les unités microprocesseurs sont traitées par ailleurs |Réf. 2|.

On pourra constater que, compte tenu des pannes considérées, les défauts se manifestent toujours par une absence de transmission dans un sens ou dans l'autre (pour les pannes franches). La routine de détection des défauts de liaisons que nous avons développée au paragraphe II.6.1 permet donc de détecter l'ensemble des défauts répertoriés ($\tau_1 = 1$).

* Taux de défaillance d'une liaison (cf. Annexe 3)

Pour une liaison filaire bidirectionnelle telle qu'elles sont réalisées (Figure II.15), nous avons un taux de défaillance horaire

$$\lambda_1 = 8{,}5\ 10^{-6}/h$$

Il faut noter que les photocoupleurs entrent pour 70 % dans le taux de défaillance global d'une liaison.

Composant	Pannes envisagées	Conséquences sur la carte correspondante
Photocoupleur	Court-circuit pour (diode photoémissive / diode photoréceptrice)	Messages non reçus par le microprocesseur correspondant
	Court-circuit du transistor photorécepteur	Messages non reçus par le microprocesseur correspondant
	Circuit ouvert pour : (- diode photoréceptrice / - diode photoémissive / - transistor photorécepteur)	Messages non reçus par le microprocesseur correspondant
	Diminution du taux de transmission entre l'entrée et la sortie	Inhibition de la transmission augmentation du TEB
Circuit d'attaque des branches émettrices	Circuit ouvert Court-circuit	Plus d'émission de messages
Liaisons par fil	Circuit ouvert	Plus de transmission de messages
	Court-circuit (unique)	Aucune incidence de par l'isolement galvanique
Connecteurs	Mauvais contact coupures	Transmission ou réception des messages impossible ou intermittente

Tableau II.3 : Bilan des pannes à détecter

CONCLUSION

Quelle que soit l'architecture du réseau de communication (bus ou étoile), la gestion des accès par la méthode du polling permet une détection de toutes les pannes de liaisons. Dans ces conditions, l'utilisation d'un réseau en bus simple peut s'avérer intéressante pour plusieurs raisons :

- le câblage est minimum
- l'extension du réseau est très facile
- la fiabilité d'une voie en bus, bien qu'inférieure à celle d'une voie point à point, permet d'espérer une disponibilité suffisante si les composants sont de bonne qualité et que des précautions sont prises pour éviter qu'un satellite défaillant ne puisse perturber le bus.

Le développement d'un réseau en bus simple, réalisé à partir de la technologie optique qui semble évoluer favorablement, paraît une perspective intéressante qui pourrait remplacer avantageusement un réseau en étoile.

CHAPITRE III

CHAPITRE III

-o-o-o-o-o-o-o-o-o-o-o-

SUPPORT DE TRAITEMENT

III - DESCRIPTION DU SUPPORT DE TRAITEMENT

Le support de traitement regroupe l'ensemble des moyens mis en oeuvre pour prélever les données, traiter les informations et activer les commandes. Le support de traitement est en relation directe avec le (les) processus à commander mais aussi avec une unité de traitement hiérarchiquement plus élevée, elle même en relation avec l'homme responsable de l'exploitation du système.

III. 1 - INSERTION DU SUPPORT DE TRAITEMENT DANS L'ENSEMBLE DU SYSTEME DE TRANSPORT

(Figure III.1)

Ce schéma permet de situer notre étude par rapport à l'ensemble du système de transport. Les niveaux 1 et 2 de la hiérarchie du système résultant du choix d'architecture de réseau vu au chapître précédent.

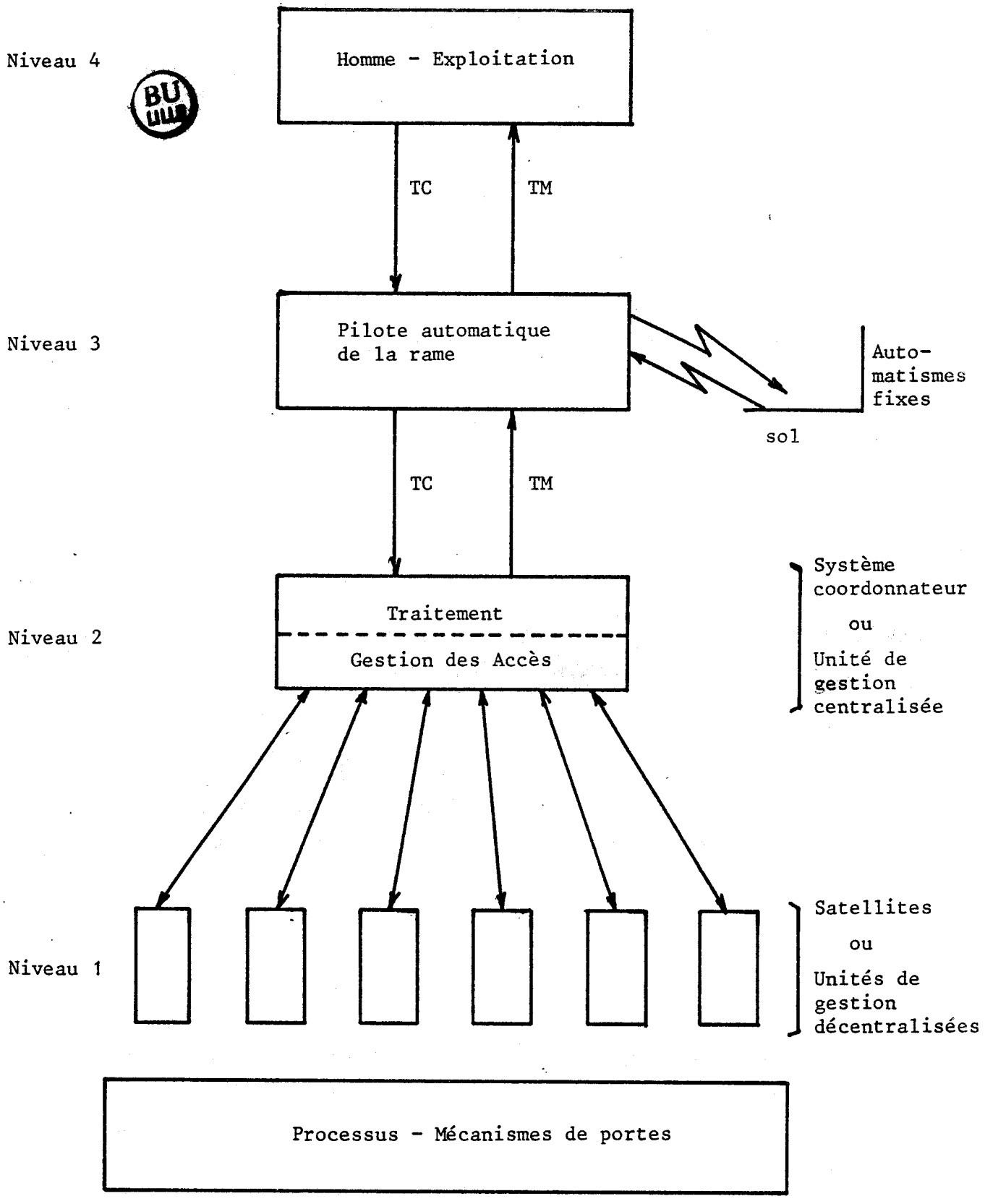


Figure III. 1 : Insertion du support de traitement dans l'ensemble du système de transport

III. 2 - SPECIFICATION GENERALE DES TRAITEMENTS A EFFECTUER

III. 2. 1 - Unités localisées ou satellites (niveau 1)

Le satellite est une entité capable de gérer seul la partie du processus dont il a la charge. Il n'a en aucun cas une vue globale du processus. Il peut tout au plus être informé par le niveau supérieur de la hiérarchie ou par une liaison horizontale de l'état des variables critiques dont il n'a pas la charge mais qui peuvent le concerner. Il gère en autonome le fonctionnement de plusieurs boucles de régulation (logiques dans notre cas). Philosophiquement, la finalité des satellites est d'assumer une tâche localisée, complète et autonome de commande-contrôle d'un processus.

Le dispositif est capable |Réf. 2-3| :

1 - d'effectuer la commande normale et simultanément de détecter des anomalies de fonctionnement

2 - si une anomalie est détectée, il y a analyse et localisation du défaut

3 - a l'issue de la reconnaissance d'un défaut, le système est capable (localement) de prendre une décision sur la nouvelle conduite à tenir vis à vis du processus

4 - enfin, il informe de ce qui se passe le niveau hiérarchiquement supérieur.

Sur le satellite sont traités électriquement tous les problèmes d'interfaçage entre le microprocesseur (unité de traitement niveau 1) et les capteurs ou effecteurs.

III. 2. 2 - Unité centralisée ou système coordonnateur (niveau 2)

Cette unité est chargée, par rapport à un contexte global, (exploitation de la ligne de transport) d'élaborer les commandes spécifiques à chaque satellite en fonction de l'état de fonctionnement du processus et de la consigne issue du niveau supérieur. Elle doit parallèlement élaborer une synthèse de l'état des divers sous-ensembles de manière à en informer le niveau supérieur. Le système coordonnateur a une vue globale du processus qui lui permet localement de prendre des décisions sur la conduite à adopter vis à vis des défauts imputables au réseau d'interconnexion ou aux satellites. Le cumul de différents défauts, qui font l'objet d'une prise de décision locale par les satellites, peut amener le système coordonnateur à prendre une décision plus globale vis à vis de l'exploitation du système (cas de la condamnation de plusieurs portes par exemple).

III. 3 - SPECIFICATION GENERALE DES TRAITEMENTS A EFFECTUER AU NIVEAU CENTRALISE

III. 3. 1 - Remarque préliminaire

Les contraintes posées par la sécurité de la commande des processus nous obligent, au niveau centralisé, à envisager le traitement d'une tâche relativement complexe pour plusieurs raisons :

- il faut d'abord gérer l'exploitation des équipements de façon satisfaisante pour la bonne marche du système. Cet aspect du problème nécessite le développement d'algorithmes de commande qui relèvent du traitement en temps réel.

- Il faut également gérer la sécurité de l'ensemble du système, ce qui nécessite de développer d'autres algorithmes d'analyse et de diagnostic de pannes. La particularité du traitement de cette tâche au niveau centralisé est que l'algorithme n'est plus temps réel, il doit en effet tenir compte de

l'histoire (à court terme) du système. Cette particularité permet de traiter des modèles de défauts fugitifs, et permet également, si nécessaire, d'obtenir à des fins d'exploitation et de maintenance un état détaillé du fonctionnement du système.

III. 3. 2 - Sécurité

L'aspect sécurité est à envisager suivant deux axes :

- Sécurité fonctionnelle du traitement des informations d'état du processus

Ces informations sont élaborées par les satellites et analysées par le système coordonnateur. Certaines configurations d'état peuvent se révéler dangereuses pour l'exploitation. La rapidité de traitement de l'analyse et de la synthèse des informations est primordiale. Elle se traduit, en fin de traitement, par un simple transfert vers le niveau supérieur d'un message indiquant la présence de danger en ne précisant pas toutefois la nature du danger. Ce transfert implique des contraintes de priorité sur l'acheminement des messages. Cette contrainte d'ailleurs étendue aux autres aspects (exploitation normale - disponibilité - aide à la maintenance) doit être analysée et spécifiée de façon rigoureuse.

- Sécurité de l'unité de traitement (logiciel et matériel)

La production d'un logiciel, conforme aux spécifications et fiable dans son exécution, se fait en plusieurs étapes |Réf. 29| (Figure III.2). Chaque étape doit donner lieu à l'établissement d'un document clair, exact et dont l'interprétation est unique. Il existe des outils d'aide à la spécification qui permettent de structurer et de formaliser la présentation du problème. On peut citer notamment pour la spécification des besoins SREM, ISDOS, HDM, SADT..., et pous la spécification fonctionnelle, les réseaux de Pétri (RDP), HOS,... Les documents, établis à partir de ces méthodes, permettent des échanges fiables entre les différentes équipes, chacune spécialisée dans une phase du développement.

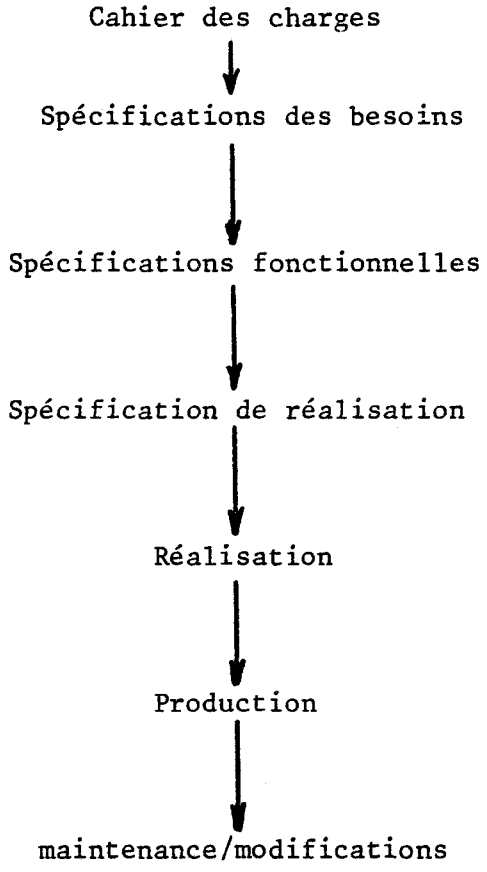


Figure III.2 : Cycle de vie d'un système informatique

Comme, d'une part, les outils d'aide à la spécification nécessitent un système support automatisé dont nous ne disposons pas et que, d'autre part, le but de notre étude n'est pas de maitriser ces méthodes, nous avons spécifié les besoins en langage naturel, la taille raisonnable du problème permettant une analyse rigoureuse des différents aspects du traitement.

La sécurité matérielle de l'unité de traitement est un problème complexe que nous n'avons pas traité ici.

III. 3. 3 - Disponibilité

La gestion de la disponibilité est conséquente du traitement de l'aspect sécurité, les données d'entrée sont en effet les défauts que l'on a diagnostiqué.

Pour améliorer la disponibilité, il est nécessaire de prévoir une possibilité de reconfiguration globale du système de manière à utiliser les ressources encore disponibles pour une exploitation en mode dégradé. Le traitement en mode dégradé tient compte de l'historique du processus afin d'estimer le niveau de dégradation global du système et son incidence sur la sécurité. Il prend notamment en compte les défauts fugitifs. A un niveau plus global, on tolère une partie des défauts de liaisons ou de satellites.

III. 3. 4 - Exploitation normale

Lorsqu'aucun défaut ne perturbe le fonctionnement du processus et du système de commande-contrôle, le traitement consiste à élaborer les télécommandes propres à chaque satellite en fonction des télécommandes émises par le niveau supérieur. Parallèlement, il s'agit d'élaborer une synthèse de l'état de l'ensemble du processus permettant de confirmer vers le niveau supérieur la prise en compte des télécommandes. Afin de limiter la quantité d'informations envoyées vers le niveau supérieur, on n'élaborera une information de synthèse que lorsque l'acquittement des fonctions demandées par l'exploitation aura été constaté . La gestion du transfert de ces informations de synthèse est confiée au niveau hiérarchiquement plus élevé (gestion des transferts par la méthode du polling cf. § II.6).

III. 3. 5 - Aide à la maintenance

La nécessité de détecter et de localiser les défauts peut être mise à profit pour une aide à la maintenance. Le dispositif d'aide à la maintenance (DAM) n'est pas dans notre esprit une finalité mais une conséquence de l'étude des problèmes de sécurité que l'on utilise à des fins économiques.

Le gain se concrétise de plusieurs façons :

- par une minimisation voire une suppression des maintenances préventives
- par une aide effective à la maintenance curative (connaissance des défauts diagnostiqués)

Ce dernier point implique sur la fonctionnalité du système central de mettre en forme toutes les informations d'erreur ou de panne de façon à faciliter au mieux les travaux des agents de maintenance.

III. 4 - OBSERVATION DU FONCTIONNEMENT DU PROCESSUS DEPUIS LE SYSTEME COORDONNATEUR

DIAGNOSTIC ET STOCKAGE DES INFORMATIONS D'ERREUR

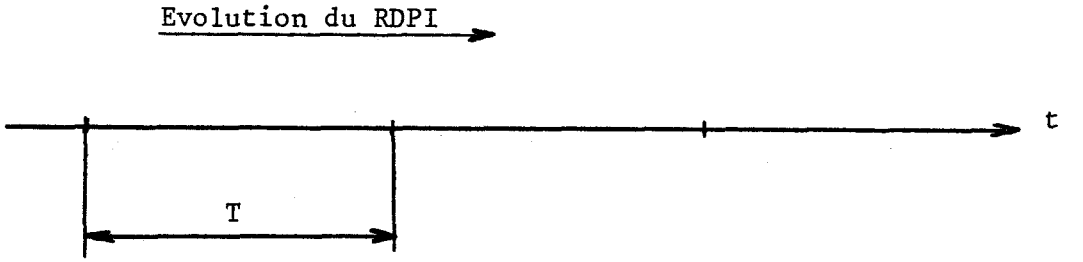
* Observation du processus

Le système coordonnateur est capable d'observer le fonctionnement des divers sous-ensembles formant le processus global à travers les satellites et les informations de télémesures qui y sont élaborées.

Si les RDPI (Réseau De Pétri Interprété) implémentés dans les satellites permettent de détecter des défauts de type collage et changements d'état intempestifs (Réf. 2-3), au niveau central, on traite un modèle d'erreur supplémentaire concernant leur aspect dynamique.

Le problème est dans notre cas le suivant :

- Au niveau des satellites



Le vecteur d'état du processus est échantillonné avec une périodicité T qui doit satisfaire la condition suivante :

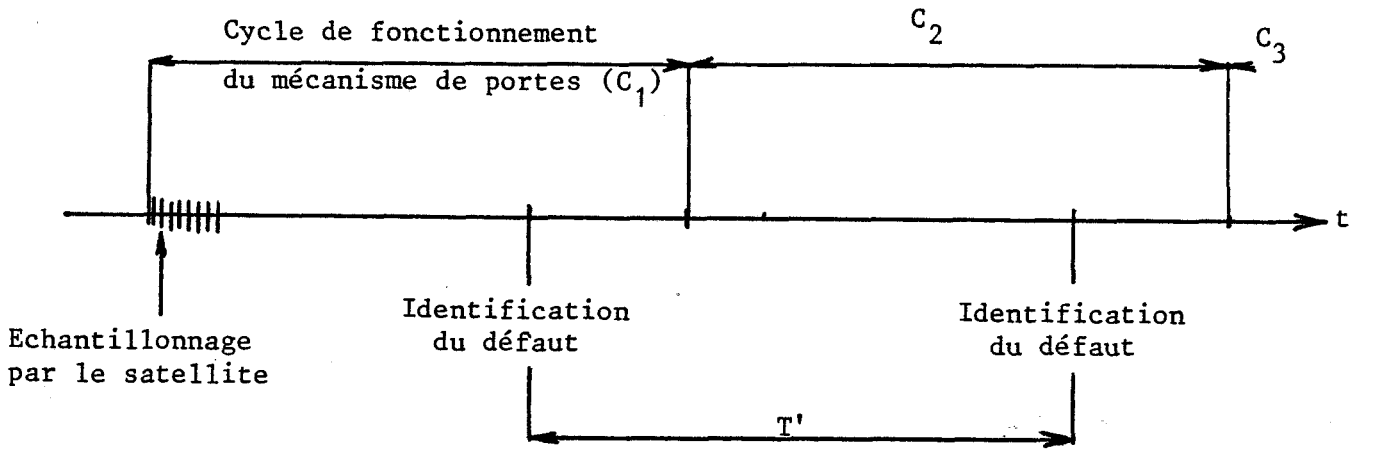
$$T \leq \frac{Tch}{2}$$

avec Tch = temps entre deux changements consécutifs des grandeurs du processus. Tch = 10^{-2} seconde selon les hypothèses.

- A l'échantillonnage, on s'assure de la stabilité du vecteur d'état (fonction antirebond)

- Entre deux échantillonnages, il peut y avoir des perturbations fugitives. Elles ne sont pas vues et ne sont pas gênantes (fautes tolérées naturellement par le dispositif).

- Au niveau central, on dispose d'une information supplémentaire sur la persistance du défaut identifié localement par le satellite.



T' est la période d'échantillonnage du défaut identifié par le satellite. Cette période correspond à la durée d'un cycle de fonctionnement du système. Dans notre application, T' équivaut à un cycle d'ouverture et de fermeture des mécanismes de portes accompagné du temps de circulation de la rame en interstation, soit dans nos hypothèses |Réf. 1| :

T' ≅ 1 mn 30

Un traitement statistique sur cette information permet de discerner les défauts fugitifs (perturbations) des défauts permanents.

* Problème du diagnostic au niveau central

Le rôle du système coordonnateur est d'abord de gérer en sécurité l'exploitation du système. Cette finalité nécessite une prise en compte immédiate des défauts, incompatible avec un traitement statistique destiné à confirmer la persistance de ces défauts. Le diagnostic au niveau central vise deux objectifs :

1 - permettre, grâce à une analyse en temps réel des informations de pannes, de poursuivre l'exploitation dégradée du système. Cette analyse permet de fournir à la maintenance une information de synthèse précisant le niveau de dégradation du système afin de planifier la remise en état.

2 - fournir à la maintenance des informations précises sur l'origine des défauts et leur persistance. Ces informations constituent une base de données pour un traitement statistique ultérieur.

* Analyse des informations de défaut

On distingue plusieurs types d'informations à traiter. Elles concernent :

1 - Les défauts précurseurs (obstacle à la fermeture, dur mécanique). Un traitement statistique de ces informations permet d'anticiper sur les procédures de maintenance périodique (nettoyage, graissage du mécanisme).

2 - Les défauts relatifs à des pannes sur le vecteur d'état du processus. Ces défauts sont entièrement identifiés et ne perturbent pas le fonctionnement du mécanisme de portes.

3 - Les défauts relatifs à des pannes sur le vecteur de commande du processus. Ces défauts sont entièrement identifiés mais ne permettent plus la commande du mécanisme de portes.

4 - Les défauts relatifs à des pannes de liaisons ou de satellites. Ces défauts ne permettent plus la commande ni le contrôle du mécanisme de portes. Seule la redondance du traitement des informations de sécurité permet de vérifier que le processus reste dans l'état de sécurité (portes fermées verrouillées).

Chaque type d'information est traité différemment en fonction de son incidence sur la sécurité et sur l'exploitation.

On utilise deux types de traitements :

- Une analyse combinatoire des défauts : elle permet d'estimer le niveau de dégradation global du système et d'analyser l'incidence des défauts sur la sécurité par une description des redondances. Cette analyse permet une exploitation dégradée du système en utilisant toutes les ressources offertes par la redondance des éléments à tous les niveaux.

- Une analyse séquentielle des informations : elle est utilisée pour traiter les défauts qui perturbent l'exploitation :

  . les défauts, qualifiés de précurseurs, qui persistent

  . les défauts qui affectent la commande et qui se produisent lorsque le processus n'est pas dans l'état de sécurité.

Ces défauts qui bloquent l'exploitation peuvent devenir tolérables grâce à une prise de décision locale par les satellites (réouverture, condamnation de la porte) ou par une requête, de la part du système coordonnateur, auprès d'une ressource extérieure. A chaque étape du traitement, on a recours à un niveau de plus en plus élevé de la hiérarchie (satellites, voyageurs, maintenance) pour résoudre le problème d'exploitation causé par le défaut. Lorsque le problème est solutionné, le défaut est alors analysé de manière combinatoire.

* Problème du stockage des informations

Les télémesures collectées auprès des satellites ou élaborées par le système coordonnateur sont stockées sous deux formes :

. Stockage des N dernières télémesures relatives à chaque sous-système. Cette forme de stockage permet de conserver la chronologie d'apparition des évènements. On dispose ainsi d'une source d'information qui permet de cerner l'origine des défauts (piège à défaut). Cette source permet, sur demande, de complèter par des informations sur la passé récent du système, l'information de synthèse envoyée à la maintenance.

. Stockage des télémesures avec datation de la première et de la dernière apparition et nombre d'occurences. Cette forme de stockage permet, avec une mémoire limitée, de garder une trace de tous les évènements apparus depuis la mise en service du système. Cette forme condensée de stockage se prête bien à un suivi statistique du fonctionnement de chaque sous-système.

* Problème du transfert des informations

En temps réel, on transmet à l'exploitant des informations synthétiques caractérisant l'état du système (exemple : 1 porte condamnée). Au besoin, en cas de blocage, on peut demander l'intervention d'un agent pour la poursuite de l'exploitation.

Les informations d'aide à la maintenance, stockées en mémoire, sont transférées en temps différé (au moment de la maintenance). La quantité d'informations peut être très variable selon les avaries rencontrées.

III. 5 - METHODE DE TRAITEMENT AU NIVEAU CENTRALISE PAR HIERARCHISATION DES TACHES

La hiérarchisation du traitement des informations permet la simplification du logiciel grâce à une décomposition du problème en sous-problèmes indépendants. Cette décomposition s'appuie sur la décomposition physique adoptée pour le système.

De la même manière, nous allons hiérarchiser le traitement sur deux niveaux (figure III.3) :

- Un premier niveau référencé 2A (cf. Figure III.3) qui consiste à établir une synthèse des informations de télémesures relatives à chaque sous-système (indépendamment des autres). Cette synthèse, transmissible au niveau supérieur, tient compte de l'historique du sous-système.

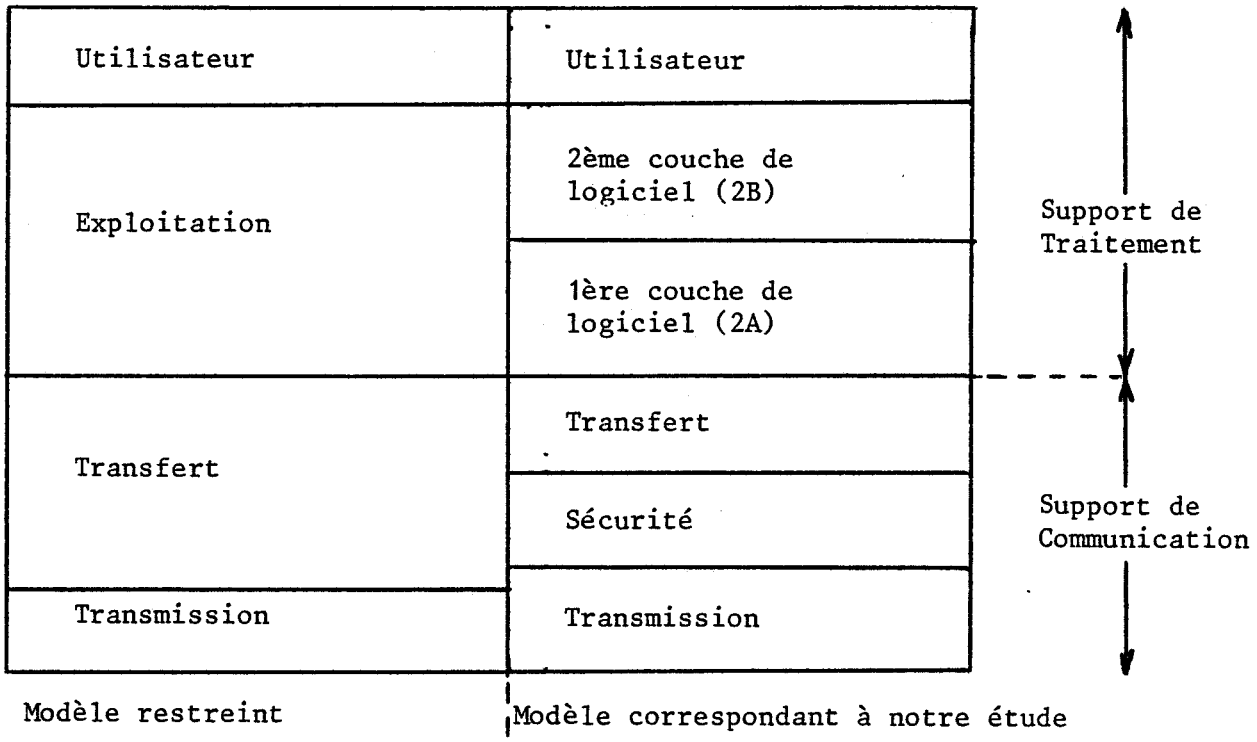
- Un second niveau référencé 2B (cf. Figure III.3) reprend les informations issues du niveau inférieur pour :

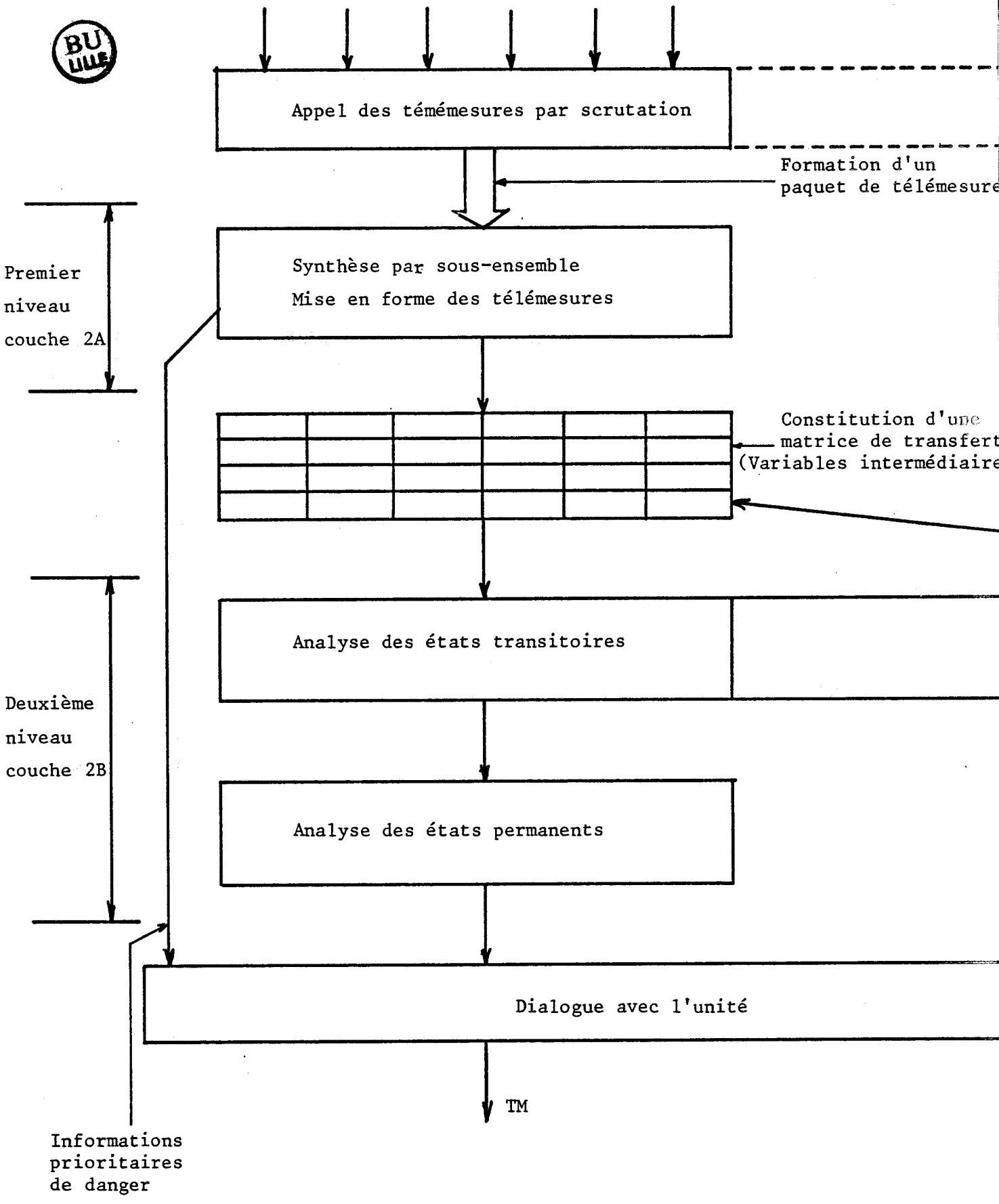
  . réaliser la coordination nécessaire entre les sous-systèmes (traitement des télécommandes)

  . définir les modes de fonctionnement dégradés

  . établir une synthèse globale du fonctionnement du système destinée à l'unité hiérarchiquement plus élevée.

L'ensemble du traitement des informations (couches 2A et 2B) se situe dans la couche exploitation de la hiérarchie restreinte appliquée aux réseaux locaux de commande-contrôle |Cf. Figure II.1|. La hiérarchisation du traitement revient à introduire une décomposition à l'intérieur de cette couche de logiciel. La hiérarchie des tâches à exécuter est définie de la manière suivante :




Appel des témémesures par scrutation
Formation d'un paquet de télémesure
Premier niveau couche 2A
Synthèse par sous-ensemble
Mise en forme des télémesures
Constitution d'une matrice de transfert (Variables intermédiaire
Deuxième niveau couche 2B
Analyse des états transitoires
Analyse des états permanents
Dialogue avec l'unité
TM
Informations prioritaires de danger

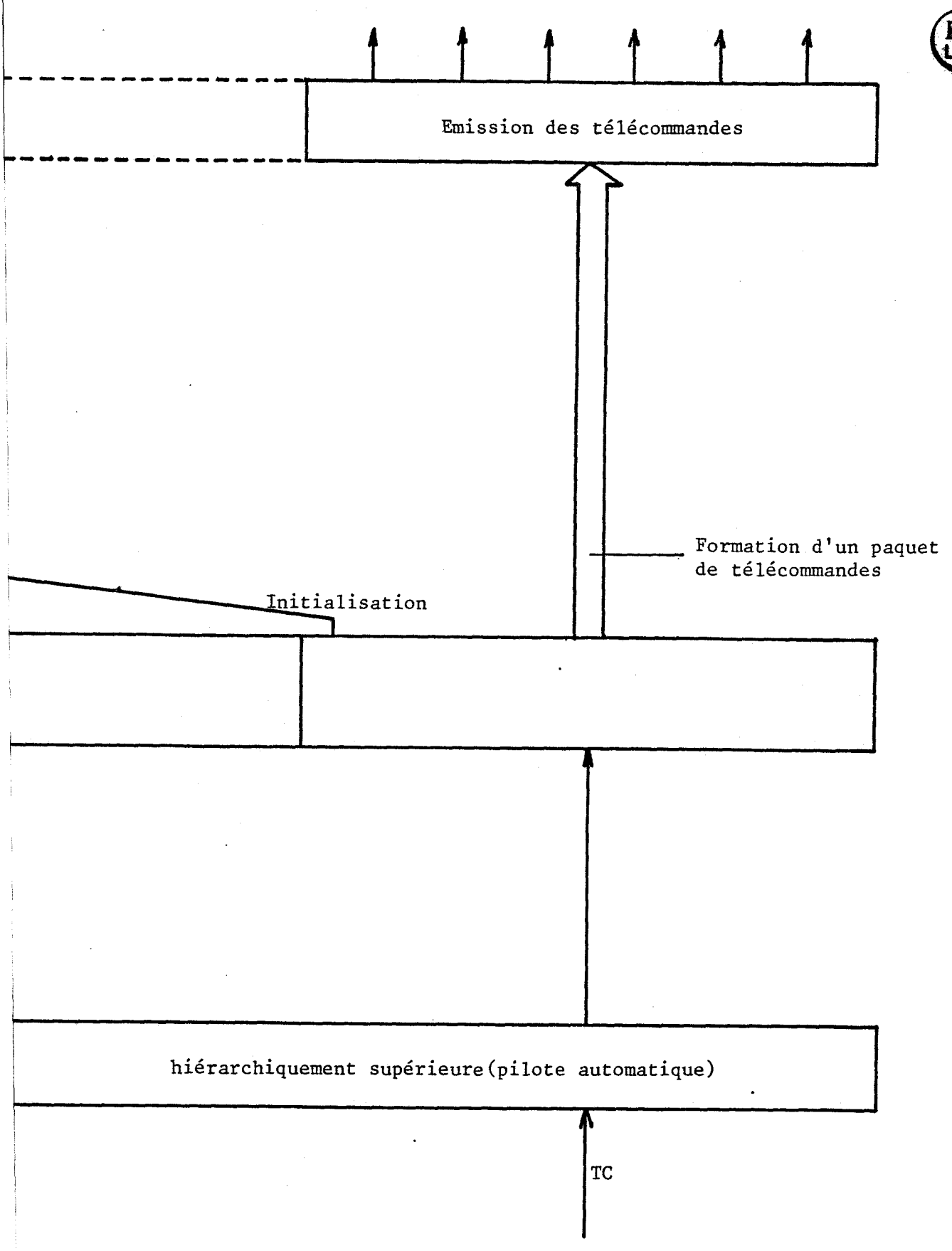


Figure III. 3 : Description de la hiérarchie des traitements effectués au niveau du système coordonnateur

La couche utilisateur n'apparaît pas dans notre description des traitements car elle ne peut être définie qu'en fonction de l'utilisateur final qui utilise ses services. Les services contenus dans cette couche de logiciel sont : le transfert des informations de télémesures destinées aux agents de maintenance (transfert d'un fichier) et la gestion des échanges d'informations avec le niveau supérieur.

Remarque :

La hiérarchisation du traitement permet de décomposer le problème mais ne résoud pas le problème de l'analyse à chaque niveau.

Pour analyser avec rigueur les tâches à développer à chaque niveau, nous aurions pu faire appel à un formalisme du type RDPI. Nous avons préféré analyser le problème différemment, comme le montre la suite de ce chapître, car, dans un premier temps, nous avons jugé le RDPI mal adapté à notre problème qui se caractérise par :

- un nombre important de variables (les différents télécommandes et télémesures)
- des contraintes de priorités
- de multiples modes de fonctionnement qui résultent des différentes combinaisons de défauts tolérables ; chaque sous-système pouvant tolérer un défaut simple.

Après avoir décrit la hiérarchie des traitements effectués au niveau du système coordonnateur, nous définissons ci-après la structure générale du programme de traitement au premier niveau (analyse organique des différentes tâches) puis nous développons le traitement spécifique à chaque module. Dans un deuxième temps, nous développons le traitement des tâches au second niveau.

III. 5. 1 - Description détaillée des traitements centralisés 1er Niveau (Couche 2A)

* Situation du problème

Le rôle de ce premier traitement est de déterminer, à partir des télémesures

relatives à chaque sous-système, leur état de fonctionnement, indépendamment des autres sous-systèmes.

On reçoit un flux d'informations qui est composé :

- d'un flux de télémesures connu : les télémesures d'acquittement des télécommandes

- d'un flux aléatoire de télémesures qui comporte :

  . les télémesures de danger
  . les télémesures signalant un défaut sur le processus commandé
  . les télémesures signalant un défaut sur le réseau d'interconnexion ou sur un satellite.

Les télémesures de danger sont reconnues immédiatement dès leur réception. Dès qu'une de ces télémesures est reçue, on la stocke puis on envoie un message de danger vers le niveau supérieur.

Les trois autres types de télémesures permettent de définir trois variables représentatives de l'état du système (notion de variables intermédiaires) :

- Une variable précisant l'état du sous-système indépendamment des défauts (Variable orientée exploitation)

- Une variable précisant le niveau de dégradation du sous-système (sous-processus, satellite et liaison) indépendamment de son état (Variable orientée maintenance du système)

- Une variable qui de manière générale sert à préciser l'état des paramètres utiles à d'autres sous-systèmes (Variable orientée maintenance du réseau). Elle permet au niveau supérieur du traitement de prendre en compte la redondance offerte par l'architecture du réseau, en vue d'une reconfiguration pour améliorer la disponibilité.

Remarque :

Nous avons cherché à définir un mode de traitement des informations qui

se base sur la connaissance de l'état antérieur du sous-système pour définir les nouvelles variables intermédiaires à partir des télémesures reçues, afin d'éviter un accroissement du temps de traitement de la mise en service jusqu'à l'arrêt de l'exploitation (conséquence de la quantité sans cesse croissante d'informations à prendre en compte).

A - Analyse organique du traitement d'un sous-ensemble

Nous avons cherché un moyen de permettre au programme de traitement d'acquérir au fur et à mesure des connaissances sur le système. Afin de définir un algorithme de traitement transposable à d'autres applications, nous avons cherché à sauvegarder les connaissances acquises sous une autre forme qu'une base de données. Cette information concernant le passé du système est contenue dans le choix d'un programme de traitement. Le programme de traitement choisi tient compte à priori des évènements antérieurs survenus sur le système.

Le passé du sous-système est ainsi contenu sous une forme implicite définie par le programme de traitement et sous une forme explicite par la variable définissant le module de programme choisi pour le traitement des télémesures.

Pour pouvoir exploiter cette méthode, il est nécessaire que le système ne puisse évoluer que dans le sens d'une dégradation croissante.

Exemple :

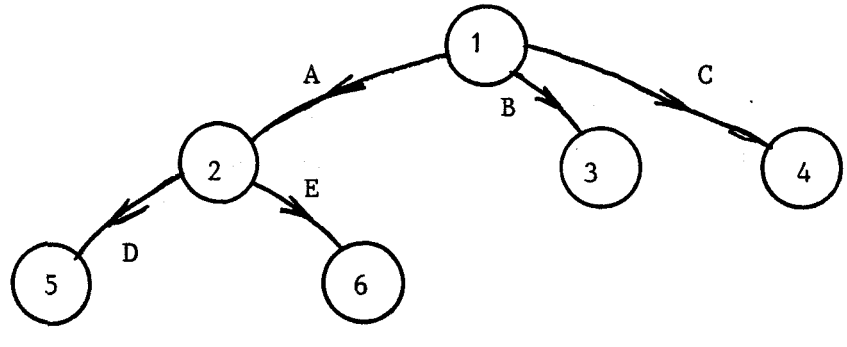


Figure III.4 : Graphe d'allocation des programmes de traitement en fonction de l'état du système

(1) : Programme de traitement initial - système en bon fonctionnement

(2) : Programme de traitement en mode dégradé tenant compte à priori du fait que l'évènement A est survenu

Le programme de traitement (1) est utilisé jusqu'à l'apparition d'un évènement A, B ou C (ce sont tous les évènements tolérables possibles).

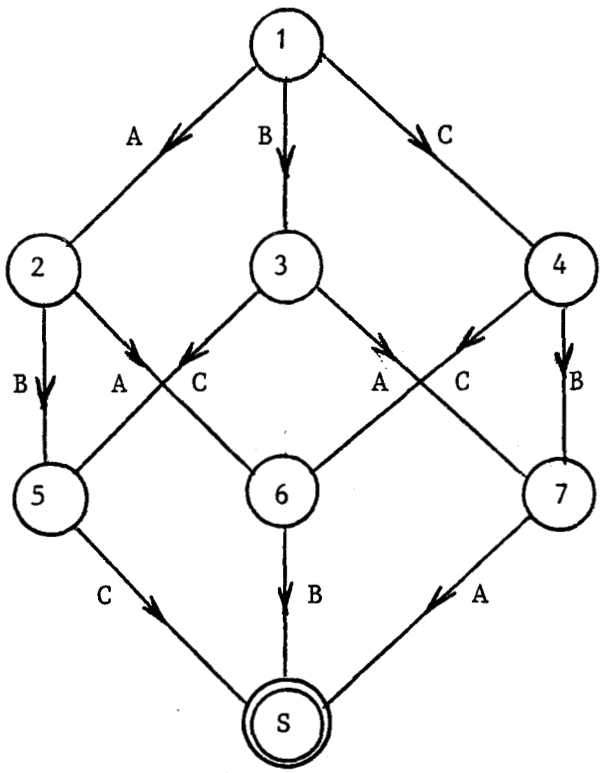
Lorsque par exemple l'évènement A apparaît, le programme utilisé pour le traitement des nouvelles télémesures devient le programme (2). Si un nouvel évènement D ou E survient le programme utilisé devient alors le (5) ou le (6). Chaque changement de programme correspond à une dégradation supplémentaire du système.

Le programme utilisé est bien porteur de l'historique du système car il n'a pu être choisi qu'à la suite d'un enchainement bien particulier d'évènements.

Cette méthode générale permet de traiter rapidement les informations lorsque le sous-système peut tolérer plusieurs dégradations successives (pas de manipulation d'informations sur le passé du système). De plus, cette méthode oblige le concepteur à analyser le contenu de chaque module ainsi que les conditons de passage d'un module à l'autre, ce qui constitue une analyse fonctionnelle structurée. En contrepartie, la taille du programme peut être disproportionnée par rapport à l'application car à chaque type de panne, ou de combinaison de pannes, on associe un module de programme particulier.

Cependant, dans la mesure où le vecteur de contrôle du processus est dimensionné de manière à détecter des pannes d'ordre supérieur à 1 (détection de plusieurs défauts), on peut utiliser un même programme de traitement pour des enchainements différents des mêmes évènements car l'ordre d'apparition des pannes n'est pas important en soi (de toute façon, il est aléatoire)(figure III.5).

La nature des pannes qui peuvent affecter le fonctionnement du processus ne permet pas dans tous les cas d'envisager une exploitation en mode dégradé, et le nombre de modules de programme à définir s'en trouve réduit.



Exploitation normale

1er Niveau de dégradation

2ème Niveau de dégradation

Système hors service

Processus à trois éléments A, B et C avec détection des pannes doubles.

Figure III.5 : Graphe d'allocation des programmes de traitement

On peut définir le nombre maximum de modules M qui peuvent être nécessaires pour traiter les informations relatives à un sous-système en exploitation normale ou dégradée :

$$M = \sum_{i=o}^{i=P} C_i^N$$

avec P = Niveau de redondance offert par le vecteur de contrôle (détection de pannes simples (p=1), doubles (p=2))

N = Nombre d'organes sous contrôle du satellite.

B - Analyse du traitement effectué par les différents modules

Un algorithme unique permet de définir le contenu de chaque module de traitement. Il considère le cas général d'un module correspondant à une exploitation en mode dégradé qui n'utilise pas encore toutes les ressources du système (Figure III.6).

Les variables d'entrée sont :

- les variables intermédiaires :
  1 - la variable orientée exploitation
  2 - " " " maintenance
  3 - " " précisant l'état de la liaison
- la variable précisant le module de traitement choisi
- une nouvelle télémesure

Les variables issues du traitement sont :

- les variables intermédiaires
- la variable précisant le module de traitement choisi.

Chaque module n'est constitué que d'une suite de comparaisons : chaque télémesure est comparée à toutes les valeurs possibles qu'elle peut prendre. Cette manière de procéder sous entend que le nombre de télémesures différentes qu'il est possible de recevoir est très limité ; ce qui restreint le domaine d'application de ce type de traitement qui, par contre présente un haut niveau de sécurité car on procède à une analyse exhaustive de tous les cas possibles.

L'organigramme général de traitement d'un module est composé de quatre tests principaux :

- le test 1 est destiné à confirmer le choix du module de traitement. Son rôle est de discriminer les défauts transitoires des défauts permanents.
- le test 2 est destiné à l'exploitation normale du système.

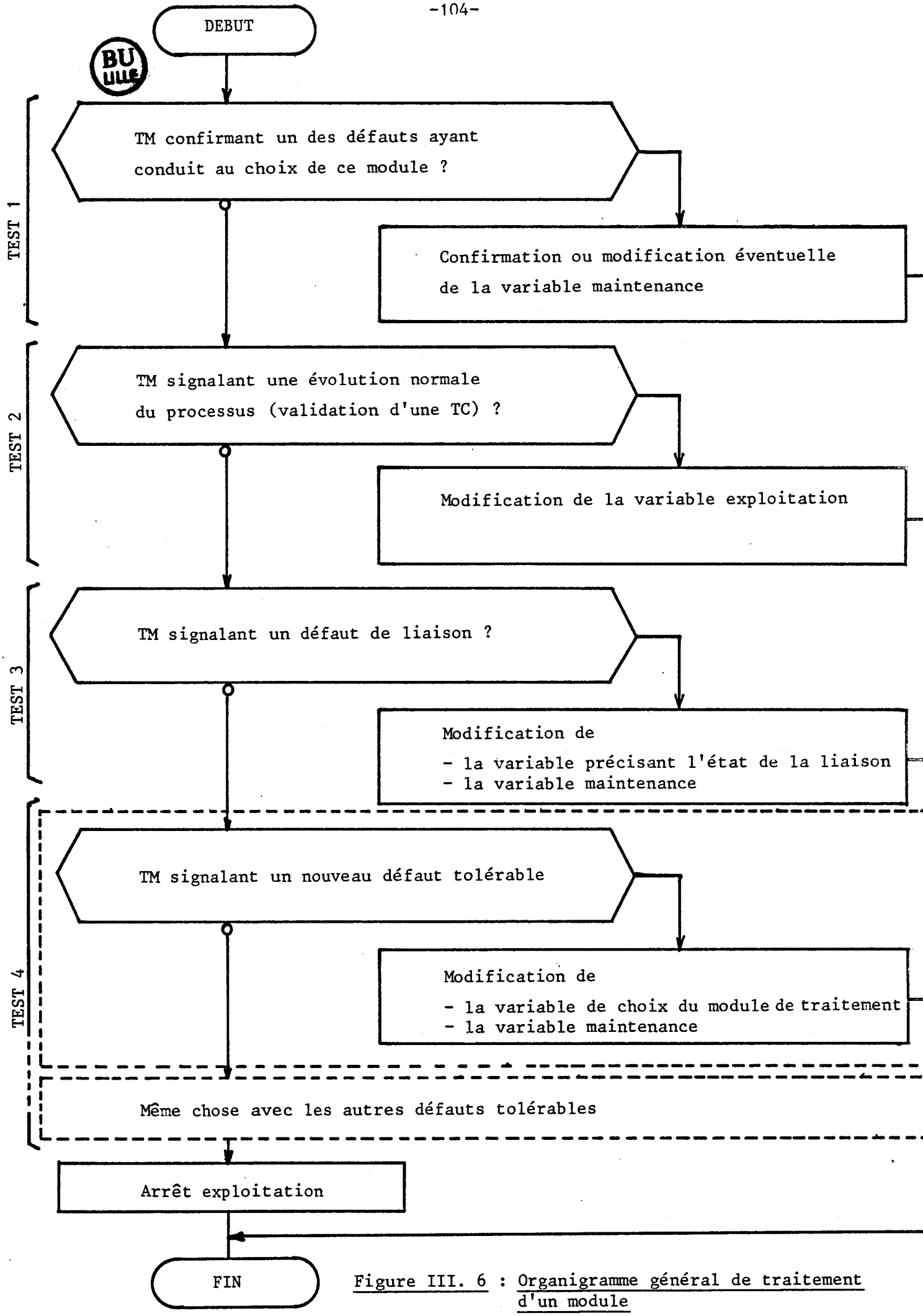


Figure III. 6 : Organigramme général de traitement d'un module

- le test 3 est destiné à l'exploitation dégradée par reconfiguration du système face aux défauts de liaison ou de satellite.
- le test 4 constitue l'analyse des conditions de passage d'un module de traitement vers un autre.

Le module de traitement initial ne comporte que les tests 2, 3 et 4. Un module de traitement en mode dégradé qui utilise déjà toutes les ressources du système, ne comporte que les tests 1, 2 et 3.

C - Analyse organique sur un plan d'ensemble

Le format d'une trame d'informations élaborée par le support de communication est le suivant :

. N TMI TM_J EOT M TM_k EOT O TM_L EOT ETX

. N, M, O : Identification de l'origine des télémesures (satellites)

. TMI, TM_J, TM_k, TM_L : Télémesures

. EOT : Indicateur de fin de paquet

. ETX : " " " " trame

La trame minimum est constituée par ETX. On reçoit cette trame lorsque chaque satellite ne fait qu'acquiter les demandes de télémesures par l'émission de EOT. Lorsqu'un satellite émet un paquet de télémesures suivi de EOT, ou lorsque le satellite ne répond pas et que le système coordonnateur en déduit qu'il y a un défaut de liaison, on stocke dans une pile l'adresse du satellite, les télémesures dans leur ordre d'arrivée suivies de EOT. Lorsqu'une scrutation complète est effectuée, on ajoute ETX et on émet la trame.

Le nombre de télémesures envoyées par un satellite est au maximum de deux étant donné l'intervalle de temps séparant deux demandes de télémesures (360 ms) :

- 1 TM de validation d'une télécommande
- 1 TM signalant un défaut (éventuellement).

Le format maximum d'une trame d'informations est de (4 x Nombre de satellites) + 1 (ETX) informations.

Cette estimation du nombre d'informations reçues n'est utile que pour justifier la capacité de traitement requise pour le système coordonnateur de manière à éviter un éventuel problème d'engorgement (saturation du système conduisant à un traitement en temps différé et éventuellement à une perte d'informations).

Le format de la trame d'informations et le mode de traitement utilisé ne sont pas, par contre, tributaires du nombre de satellites ni du nombre de télémesures par sous-système dans une trame d'informations.

Si on désire étendre le réseau à un nombre plus important de satellites, il suffit au niveau du programme d'ajouter autant de modules spécifiques (voir Annexe 2) à chaque sous-système qu'il y a de satellites en plus.

L'adjonction ou la suppression de voies de commande ou de mesure au niveau des sous-systèmes est prise en compte au niveau du programme par la création ou la suppression de modules de traitement en mode dégradé et la modification du module de traitement en mode normal.

Il est également possible de surveiller un dispositif entièrement différent ; il faut alors ajouter, à la fois un module spécifique, et des modules de traitement en mode normal et dégradé correspondant au fonctionnement de ce nouveau système.

A l'issue de ce premier traitement des informations, on dispose pour chaque sous-système de trois informations sur son état (quel que soit le nombre de télémesures reçues). On dispose pour l'ensemble du processus d'une matrice composée des variables intermédiaires et qui compte trois lignes et N colonnes (N étant le nombre de satellites).

Exploitation				
Maintenance				
Liaison				
	Σ1	Σ2 -		ΣN

Figure III. 7 : Forme matricielle du résultat du traitement (couche 2A)

III. 5. 2 - Traitement des tâches par la seconde couche de logiciel (2B)

La matrice d'informations, remplie des variables intermédiaires issues du premier niveau de traitement, est exploitée ligne par ligne pour traiter les informations relatives à l'exploitation ainsi que les informations destinées à caractériser l'état du système. Cette synthèse sur l'état du système est utilisée en temps réel pour constituer une aide à l'exploitation (tolérance aux fautes et reconfiguration).

Conformément aux spécifications que nous avons établies au paragraphe III.3, la fonction de traitement au deuxième niveau se décompose en trois tâches indépendantes et complémentaires :

1 - Une fonction de synthèse sur l'exploitation

2 - Une fonction de synthèse sur l'état de fonctionnement des processus sous contrôle, des satellites et du réseau d'interconnexion

3 - Une fonction de synthèse de l'état de fonctionnement des satellites et du réseau d'interconnexion.

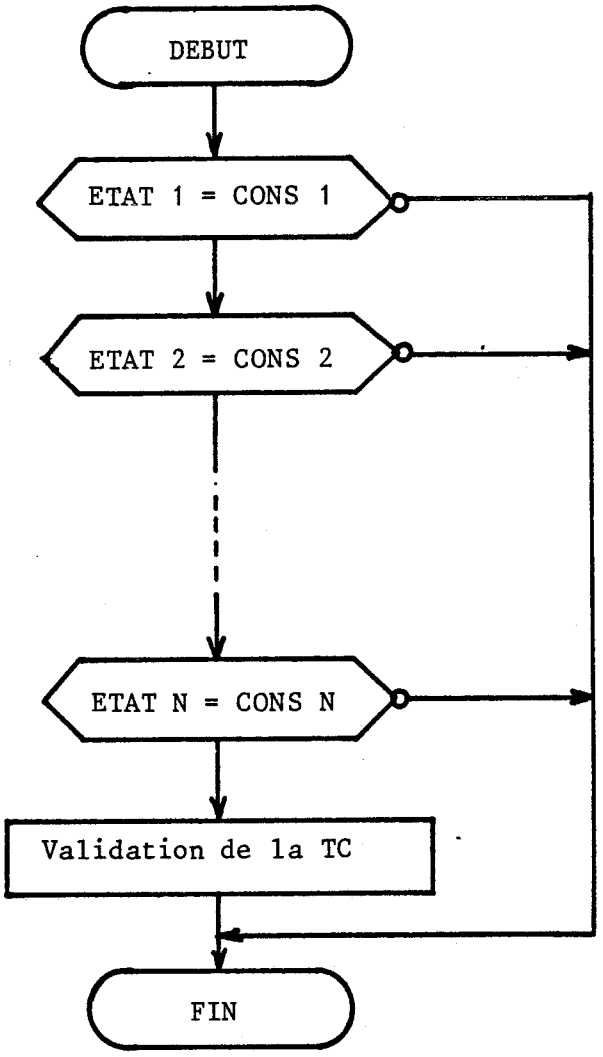
1-* - Synthèse des informations d'exploitation

Le but de cette synthèse est de fournir au système hiérarchiquement plus élevé, tel le pilote automatique de la rame, une information d'acquittement de la télécommande qu'il a envoyée. Le moyen le plus simple d'acquitter une télécommande consiste à vérifier que chaque sous-système se trouve dans l'état attendu correspondant à la télécommande globale.

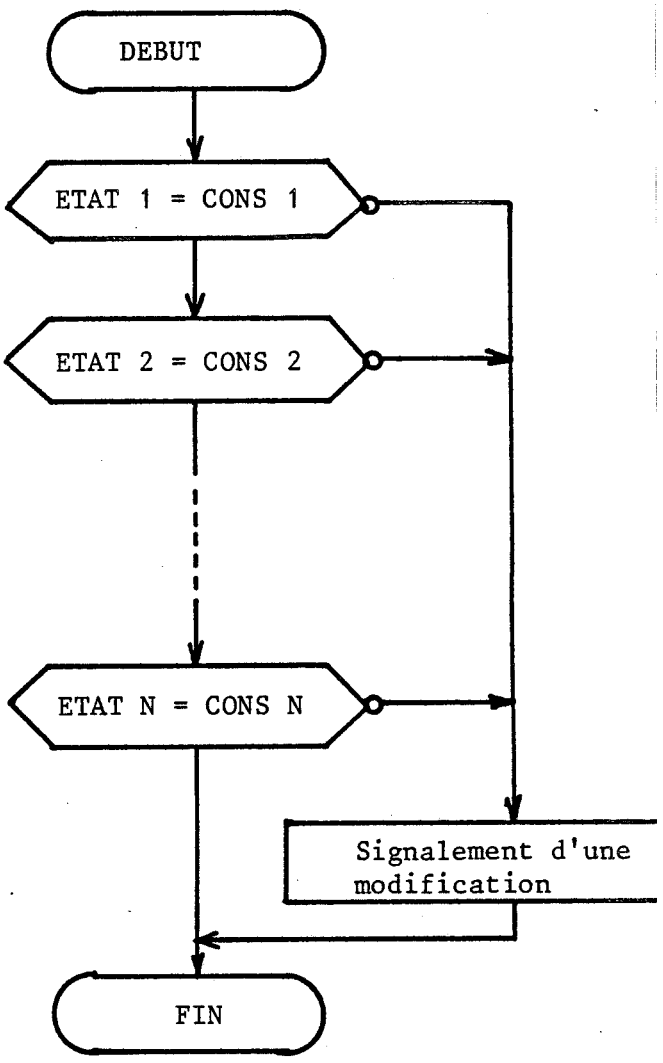
A chaque télécommande correspond une configuration particulière de l'état de chaque sous-processus et donc du satellite correspondant. On associe à chaque télécommande un module de programme qui consiste à vérifier que l'état de chaque sous-système correspond bien à la consigne imposée et qu'il ne s'écarte pas de cet état.

En fait, il faut pour chaque télécommande deux modules de programme qui vérifient que l'état réel du système correspond à l'état imposé par la télécommande, mais dont la finalité est différente (Figure III.8) :

a) le premier module consiste à attendre que le système évolue d'un état initial connu, correspondant à la dernière télécommande envoyée, vers



Premier module associé à la TC
Phase transitoire



2ème module associé à la TC
Phase permanente

Figure III. 8 : Finalité des deux modules de traitement des variables exploitation associés à chaque télécommande

l'état attendu imposé par la nouvelle télécommande. On n'émet un message de validation de la télécommande que lorsque la consigne imposée est atteinte.

b) lorsque la télécommande est validée, on utilise ensuite le second module dont le rôle est de vérifier que le processus ne s'écarte pas de son état nominal.

On analyse ainsi, séparément, la phase transitoire correspondant au changement d'état, puis la phase permanente ou statique entre deux changements imposés par télécommande. On traite deux modèles d'erreur employés lors des diagnostics de panne sur le processus lui-même :

- collage ou non changement d'état (absence de transitoire)
- changement d'état intempestif.

A ce 2ème niveau de la hiérarchie du traitement, on effectue la tâche effective de commande-contrôle de l'ensemble des processus, la tâche de premier niveau s'apparente davantage à une mise en forme des variables intermédiaires.

En créant une véritable tâche de commande-contrôle, on peut réaliser la coordination entre les différents satellites afin de faire évoluer les processus vers un état défini par une télécommande globale. Cette démarche est homogène avec celle entreprise lors de l'établissement des procédures de commande-contrôle des processus. On introduit dans la fonction de commande-contrôle des possibilités de détection de défauts et de génération de modes dégradés par suppresion de télécommandes vers un sous-système incapable de les prendre en compte. La détection de défauts se base sur la compatibilité entre les différentes variables exploitation élaborées pour chaque sous-système. Une description de cette tâche de commande-contrôle est donnée en Annexe.

2-* - Synthèse des informations d'état de fonctionnement du système

Elle a pour but d'établir l'état de fonctionnement global de l'ensemble du processus. Cette synthèse réagit sur l'exploitation en donnant à l'exploitant les moyens de planifier la remise en état du système en fonction des temps de tolérance aux pannes.

Pour celà, on signale l'apparition de tout nouveau défaut et lors de la validation d'une télécommande, on signale parmi tous les défauts l'incidence la plus grave.

Cette synthèse, consituée par un module de programme unique, est effectuée en alternance avec la tâche de commande-contrôle. Elle utilise les variables intermédiaires orientées maintenance et fournit donc à la fois :

- une synthèse de l'état du processus
- une synthèse du fonctionnement du réseau et des satellites.

3-* - Gestion des ressources du réseau dans l'optique disponibilité

L'utilisation des informations de défauts relatifs aux liaisons et aux satellites doit permettre :

- le choix des voies de transmission en fonction des défauts présents et des possibilités de reconfiguration offertes par le réseau.

- une poursuite de l'exploitation en mode dégradé lorsque le processus reste observable (Etat de sécurité observé sans ambiguïté).

- un recours à l'état de sécurité par émission vers le niveau supérieur d'un message de danger lorsque le réseau d'interconnexion ne permet plus de connaître l'état de l'ensemble du processus.

Il est bien entendu nécessaire que l'ensemble des liaisons (liaisons utilisées et voies redondantes) soit testé en permancence pour permettre d'envisager une exploitation dégradée.

Remarque :

Les tâches 1, 2 et 3 s'effectuent en temps réel avec les contraintes propres à la conduite de processus. Elles contribuent globalement à ce que l'on peut appeler de l'aide à l'exploitation.

III. 5. 3 - Aide à la maintenance

En temps différé, ce logiciel peut, sur appel, fournir aux agents de maintenance la liste des défauts détectés. Les télémesures sont transférées

sous forme d'un fichier qui regroupe l'ensemble des informations stockées en mémoire :

- nature du défaut
- origine du défaut
- date de la première apparition
- " " " dernière apparition
- nombre d'occurences.

III. 6 - APPLICATION DES PRINCIPES DECRITS CI-DESSUS AU SYSTEME DE PORTES

Le système est composé de six portes identiques et nous n'avons donc à définir des modules de traitement des informations relatives à un fonctionnement normal ou dégradé que pour une seule porte. Le vecteur de contrôle et la procédure mise en oeuvre pour localiser les pannes permettent à chaque microprocesseur affecté à la commande et au contrôle d'une porte de détecter toutes les pannes simples qui peuvent affecter les trois effecteurs et les septs capteurs |Réf. 2-3|.

A - Niveau localisé (satellites)

Pratiquement toutes les pannes simples détectées peuvent conduire à une exploitation en mode dégradé de la rame. Ce mode peut être, soit la poursuite de l'exploitation avec tolérance du défaut, soit la condamnation de la porte. Seuls quelques défauts de très faible occurence peuvent bloquer la rame en station. L'apparition d'un second défaut n'est pas tolérable et les hypothèses de travail ont conduit à un temps de tolérance aux fautes limité |Réf. 2|.

B - Niveau centralisé - traitement 1er niveau (couche 2A)

Le nombre de modules de programme à définir pour le traitement au premier niveau est

$$\sum_{i=o}^{i=1} C_9^i = 10 \text{ modules} \qquad \text{(Réf. § III.5.1-A)}$$

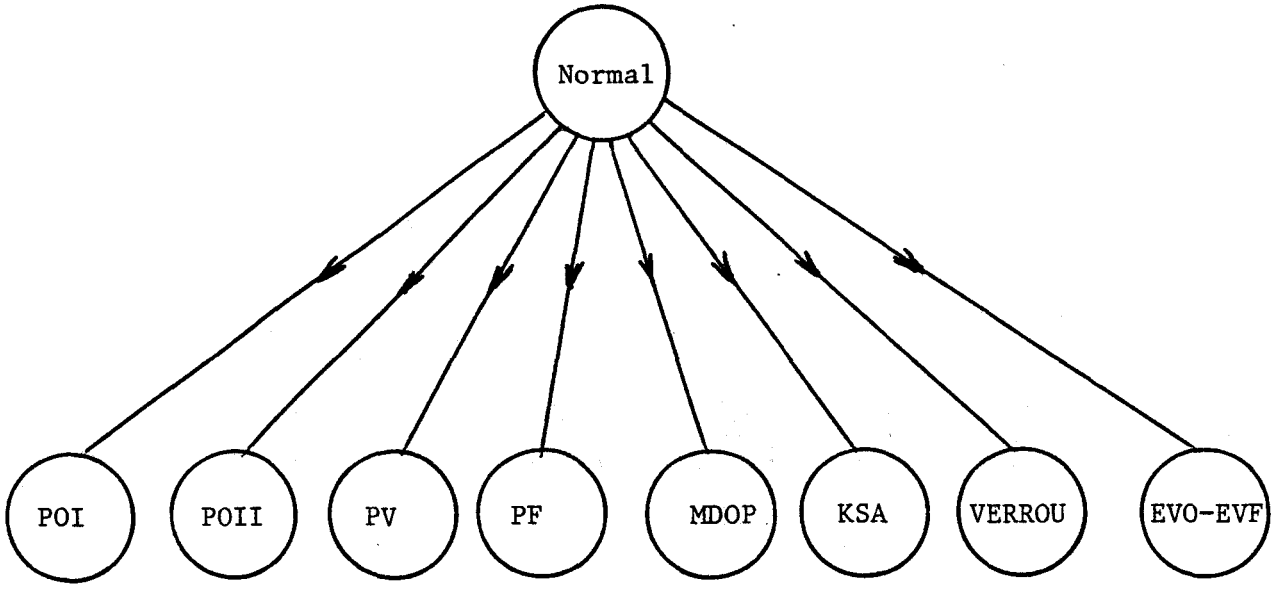
1 module correspondant à un fonctionnement normal

9 modules correspondant aux 9 éléments sous contrôle sur lesquels on diagnostique les défauts.

On rappelle que les 10 modules sont identiques, seules les variables utilisées sont spécifiques.

* Graphe d'allocation des programmes de traitement au 1er niveau de la hiérarchie

L'allocation des modules s'organise de la façon suivante :



Les conditions de passage du module "Normal" à un autre module sont données dans l'annexe 2 (seconde partie du module "Normal").

Nous avons défini un module unique pour EVO et EVF car dans les deux cas, il y a condamnation de la porte.

A l'issue du traitement au premier niveau, on dispose des informations ou variables intermédiaires, que l'on peut représenter de la façon suivante :

module	"	"	"	"	"	Choix du module de traitement
TM11	TM21	TM31	TM41	TM51	TM61	Maintenance
TM12	TM22	TM32	TM42	TM52	TM62	Exploitation
TM13	TM23	TM33	TM43	TM53	TM63	Réseau
Porte1	Porte2	Porte3	Porte4	Porte5	Porte6	Repérage des divers sous-ensembles

Les différentes variables peuvent prendre les valeurs suivantes :

Maintenance (TMi1) : - Rien : fonctionnement normal
- Défaut : défaut sans incidence sur l'exploitation
- App maint : " nécessitant une intervention

Exploitation (TMi2): - Rien : on ne connait pas l'état de la porte
- Ouverte : porte ouverte
- fermée : porte fermée
- Pcond : porte condamnée

Réseau (TMi3) : - Rien : les échanges d'informations sont normaux
- Ruptli : rupture de liaison.

C - Traitement 2ème niveau (couche 2B)

Les télécommandes, envoyées depuis le niveau supérieur (pilote automatique) et destinées aux commandes de portes, sont particulièrement simples |Réf. 3| :

- TCI : Initialisation de l'ensemble du système
- TCP : Préparation du système

} Mise en service

- TCO PD : Ouverture de portes droites (2, 4, 6)
- TCO PG : " " " gauches (1, 3, 5)
- TCF PD : Fermeture des portes droites
- TCF PG : " " " gauches

} Exploitation

Comme nous l'avons vu, à chaque télécommande correspond un module de traitement 2ème niveau. Ce module est composé de deux modules distincts comme décrit au § III.5.2.

La synthèse des informations d'état de fonctionnement du système et la gestion des ressources du réseau sont deux modules supplémentaires exécutés en alternance avec la synthèse exploitation.

III. 7 - CONSTITUTION MATERIELLE DU SYSTEME COORDONNATEUR

Nous avons abordé séparément les problèmes liés aux communications et ceux liés au traitement des informations. La constitution matérielle du système coordonnateur ne fait pas nécessairement appel à cette même distinction et plusieurs architectures sont possibles.

Nous avons vu au chapître II les fortes contraintes de sécurité à respecter pour le système central.

Nous avons vu également que la disponibilité était liée étroitement au système central (goulot d'étranglement).

On peut développer deux solutions :

- Une seule unité de traitement
- Deux unités de traitement spécialisées pour
  - . la gestion des accès au réseau
  - . le traitement des informations.

Le choix d'une de ces solutions conditionne les performances et les difficultés de la tâche à traiter. Lorsqu'une solution est choisie, il faut alors trouver un procédé de sécurité et une architecture satisfaisant les contraintes de sécurité et de disponibilité.

CONCLUSION

La conception hiérarchisée du logiciel permet une décomposition de la complexité du problème et une analyse structurée qui vont dans le sens de :

- la sûreté de l'analyse fonctionnelle
- la sûreté des logiciels

La méthode développée, qui consiste à décrire l'ensemble des configurations possibles du système par autant de modules de programme, nous permet d'envisager ultérieurement une description des tâches grâce à des outils formels (RDPI).

Les algorithmes que nous avons définis au niveau central sont généralisables ; en effet :

- nous n'avons pas fait de restriction quant à l'homogénéité des processus ni au nombre de satellites raccordés au système coordonnateur (cf. § III.5.1.c)

- le nombre de télécommandes et leur nature sont indifférents.

Le traitement peut donc être étendu à l'ensemble des matériels embarqués bien que ce mode traitement soit surtout intéressant lorsque tous les sous-systèmes sont identiques.

CONCLUSION

CONCLUSION

-o-o-o-o-o-o-o-o-o-

L'objectif de notre étude était d'apporter une solution aux problèmes posés par la sécurité et la disponibilité d'un ensemble d'unités micro-informatiques réunies au sein d'un réseau local de commande - contrôle de processus.

Notre étude a permis sur un plan d'ensemble de faire des choix rationnels au niveau de l'architecture du système. Pour notre application, le calcul d'un indice de sécurité global, paramétré par les taux de couverture de pannes des différents éléments, met en évidence le fait que le niveau de sécurité de l'ensemble du système est très lié à la sécurité propre du système coordonnateur et à la redondance des satellites, mais qu'il dépend peu de l'architecture du réseau de communication puisque nous avons un taux de couverture des pannes de liaisons égal à 1. La disponibilité de l'ensemble nécessite par contre des redondances à tous les niveaux et le meilleur compromis sécurité-disponibilité est obtenu pour un réseau en étoile. La définition d'une hiérarchie des tâches à exécuter, propres aux applications de sécurité, permet de situer les différentes couches de logiciel par rapport à la norme existante. Ce modèle spécifique met l'accent sur les particularités de notre application en proposant une décomposition particulière permettant de structurer l'étude.

L'analyse du logiciel de traitement des informations au niveau central est orientée vers une gestion des défauts à des fins de sécurité et de disponibilité. L'intérêt de ce type de traitement réside dans sa modularité qui permet notamment d'appliquer les résultats de notre étude à l'ensemble du matériel embarqué à bord d'une rame de métro. Un autre avantage est de prendre en compte implicitement le passé des sous-systèmes par le choix de modules de programme adaptés, réduisant ainsi le temps de traitement.

Pour compléter cette étude, des travaux restent à effectuer, notamment en ce qui concerne la détermination des taux de couverture de pannes des microprocesseurs et la conception matérielle du système coordonnateur.

Dans le cadre d'une maintenance informatisée au niveau des ateliers de réparation, notre dispositif permet d'alimenter une base de données sur la "vie" des matériels, il serait également intéressant de développer le traitement statistique de ces informations de défauts en vue de fournir aux agents de maintenance et à la société d'exploitation des éléments supplémentaires.

RÉFÉRENCES BIBLIOGRAPHIQUES

|1| M. CARTIER
"Sécurité des portes d'accès véhicule"
Note Sécurité MATRA - CIMT - Octobre 1980

|2| J.F. DHALLUIN
"Commande contrôle de processus en sécurité - application à la commande d'un ensemble de portes véhicule d'une rame de métro de type VAL"
Thèse Docteur Ingénieur - USTL - Décembre 1983

|3| E. KOURSI
"Une méthode sûre de développement des logiciels destinés à la commande de processus en sécurité"
Thèse - USTL - Mai 1985

|4| Ph. DELANGHE
"Contribution à la mise en sécurité d'un système de commande à micro-processeurs"
Rapport DEA - USTL - Juin 1983

|5| S. MAGNIEZ
"Test fonctionnel de la partie opérative du microcontrôleur 8051"
Rapport DEA - USTL - Juillet 1985

|6| F. BARANOWSKI
"Utilisation des circuits câblés SSI pour la conception de fonctions logiques en sécurité intrinsèque"
Rapport DEA - USTL - Juin 1984

|7| A. OUADGHIRI
"Application de la théorie des codages en traitement d'information de sécurité analysées par microprocesseurs"
Rapport DEA - USTL - Juillet 1983

|8| D. POWELL
"Réseaux locaux de commande-contrôle de processus sûrs de fonctionnement"
Thèse d'Etat - Institut National Polytechnique de Toulouse - Octobre 1981

|9| R. BILLINGTON, S. LEE
"Unavailability analysis of underwater cable systems"
I.E.E.E. Transactions on power apparatus and systems,
Vol. PAS-96, n° 1, January - February 1977

|10| R. GABILLARD
"Tentative de vérification de vraisemblance de l'affirmation de sécurité reposant sur le recours au concept de la sécurité positive"
Note USTL - Diffusion MATRA - EPALE - Mars 1978

|11| R. BOMM
"Quelle sûreté de fonctionnement ?"
Electronique industrielle - n° 66 - 1-3-1984

|12| J.P. JAGUIN
"Propriétés mécaniques et vieillissement des fibres optiques"
Thèse Docteur-Ingénieur - Université de Rennes - 1980

|13| Documentation CNET
"Recueil de données de fiabilité"
Edition 1976 - remise à jour Janvier 1979

|14| Documentation CNET
"Recueil de données de fiabilité : circuits intégrés"
Remise à jour Janvier 1982

|15| "Fiabilité et maintenabilité"
Electronique professionnelle n° 1303 - pages 40-47 - Avril 1971

|16| P. BEHAGHE
"Le transport de l'information - application aux réseaux"
Téléinformatique - Octobre 1976

|17| A. TITLI
"Contribution à l'étude des structures de commande hiérarchisées en vue de l'optimisation des processus complexes
Thèse Docteur Ingénieur - TOULOUSE - 1972

|18| J. CLAVIER, M. NIQUIL, G. COFFINET, F. BEHR
"Théorie et technique de la transmission des données"
Ed. MASSON

|19| A. OUADGHIRI
"Transmission de messages en sécurité. Etablissement d'une partition de messages codés à distance maximum et de procédures de détection d'erreurs s'y rapportant"
Note USTL - LRPE - 1984

|20| E. KOURSI, C. MAGNIEZ, J.F. DHALLUIN
"Commande des portes VAL - rapport d'avancement au 01.03.1984"
Note USTL - LRPE

|21| M. SCHWOB, G. PEYRACHE
"Traité de fiabilité"
Ed. MASSON - 1969

|22| "Etude de faisabilité d'un réseau d'interconnexions à fibres optiques selon les spécifications données par l'USTL"
Document de la Compagnie Lyonnaise de Transmissions Optiques (CLTO) - Janvier 1983

|23| J.C. LAPRIE
Journées "Sécurité des applications des automatismes numériques dans les transports"
Villeneuve d'Ascq, 24-25 Octobre 1984
"L'informatique dans le système de sécurité problème et approche"

|24| A. SCHWEITZER, J.P. GERARDIN
"Méthode permettant d'améliorer le niveau de sécurité des systèmes à logique programmée"
Electronique, technique et industrie (Paris) - n° 12 - Novembre - n° 13 - Décembre - 1984

|25| C. LIEVENS
"Sécurité des systèmes"
Ed. CEPADUES - 1976

|26| G. JUANOLE
"Prévision de la sûreté de fonctionnement des communications entre calculateurs"
Thèse d'Etat - Université Paul Sabatier - TOULOUSE - Juin 1978

|27| M. SZELAG, J.F. DHALLUIN
"Conception et réalisation d'un réseau local microinformatique de commande de portes véhicule d'une rame de métro"
Rapport G.R.R.T. - Juillet 1984

|28| C. MAGNIEZ
"Etude d'un réseau local par fibres optiques"
Note USTL - LRPE - Mai 1983

|29| C. BEOUNES
"Spécification du logiciel"
Sûreté de fonctionnement des systèmes informatiques - Toulouse - 14 - 15 Mai 1984

|30| J.F. DHALLUIN - F. BARANOWSKI
"Dispositif de contrôle de bon fonctionnement d'un microprocesseur mis en sécurité par observation temporelle"
Conception et étude de sécurité
Note USTL - LRPE - Juin 1985

|31| A. MAHMALGI
"Conception et réalisation d'un outil de test et de mesure de la sûreté de fonctionnement de systèmes à microprocesseurs, mis en sécurité par un signal équitemps"
Rapport DEA - USTL - Juillet 1985

|32| M. TIMOULALI
"Modélisation graphique et simulation des systèmes de production"
Thèse Docteur-Ingénieur - LYON - Avril 1981

ANNEXES

-o-o-o-o-o-o-

ANNEXE 1

-o-o-o-o-o-o-o-

DÉTERMINATION DU TAUX HORAIRE D'INSÉCURITÉ DÛ AUX ERREURS SUR LES MESSAGES (λ_1)

Dans l'hypothèse d'un bruit blanc gaussien et d'un canal binaire symétrique, la loi de distribution des erreurs sur un mot de n bits est la loi binominale de moyenne n_{Pe}, Pe étant la probabilité d'erreur par bit, ou encore, lorsque cette probabilité Pe est faible, la loi de Poisson. Ceci conduit à des taux d'erreurs constants.

Symboles utilisés :

n = nombre de bits/message (n = m + k)

m = " " " d'information

k = " " " de redondance

τ = taux d'erreurs brut/message

E = efficacité du code = $\frac{\text{nombre de messages faux et détectés}}{\text{nombre total de messages faux}}$

ζ = taux résiduel d'erreurs/message

d = distance minimale entre les mots du code

N = nombre moyen de messages échangés avec chaque satellite en une heure de fonctionnement.

Le taux horaire d'insécurité λ_1 est donné par :

$$\lambda_1 = N\zeta$$

avec $\zeta = \tau(1-E) = n_{Pe}(1-E)$

Estimation de N :

Par cycle de fonctionnement d'une porte, sont échangées en moyenne :

- 2 télécommandes
- 4 télémesures : * 3 télémesures d'exploitation
  * 1 télémesure de défaut.

Il faut ajouter à ces messages, les messages échangés du fait de la seule interrogation des satellites :

- une demande de TM toutes les 360 ms
- une validation de la demande : EOT

La somme de ces messages est :

$$N = 6 \times \frac{60}{1,5} + 2 \times \frac{3600}{0,36}$$

$$N = 240 + 2\ 10^4 \cong 2\ 10^4 \text{ messages/heure}$$

Calcul de λ_1 :

$$\lambda_1 = 2\ 10^4 \times n \times {}_{Pe}(1-E)$$

Pe est mesurée

n et E sont définis par les caractéristiques du code.

Le code qui a été choisi est un code linéaire de distance minimale d = 6. Le nombre de bits de redondance est k = 10. Chaque mot du code est codé sur 16 bits. Ce code permet de détecter 5 erreurs indépendantes ou des paquets d'erreurs de longueur L < 9 |Réf. 19|.

* Efficacité du code :

avec $P_e = 10^{-3}$/bit

$$E \cong 1 - 5\ 10^{-13}$$

Nous obtenons un taux horaire d'insécurité :

$$\lambda_1 = 2\ 10^4 \times 16 \times 10^{-3}\ (5 \times 10^{-13}) \cong \underline{1{,}6\ 10^{-10}/h = \lambda_1}$$

ANNEXE 2

-o-o-o-o-o-o-o-

I - TRAITEMENT DES INFORMATIONS AU 1er NIVEAU (Couche 2A du logiciel)

ASPECT GENERAL DE L'ACQUISITION ET DU TRAITEMENT D'UNE TRAME D'INFORMATIONS

La première étape de l'acquisition des informations consiste à reconnaître dans chaque paquet la première information qui définit l'origine des télémesures. Lorsque cette origine est reconnue, on utilise un programme spécifique à chaque sous-système dans lequel on procède à l'acquisition et au traitement proprement dit des télémesures. Lorsqu'on arrive à un séparateur (EOT), on sort du programme propre au sous-système pour recommencer l'opération avec le paquet suivant. L'acquisition et le traitement au premier niveau sont terminés lorsque le paquet suivant est ETX. Cette organisation générale est décrite par l'organigramme de la Figure A-1.

Ayant défini l'organisation générale du programme de traitement d'une trame d'informations, nous pouvons maintenant définir plus précisément le rôle des programmes d'acquisition et de traitement des télémesures, spécifiques à chaque sous-système. C'est à ce niveau que doivent être pris en compte le traitement prioritaire des informations de danger et le stockage de l'ensemble des informations (aide à la maintenance).

La définition d'un programme spécifique à chaque sous-système résulte du fait que le stockage des informations occupe une zone mémoire réservée et que le traitement utilise et modifie les variables propres à ce sous-système. Les différents pointeurs et variables sont définis dans ce programme.

Le traitement proprement dit n'est pas spécifique car il utilise un des modules de programme définis en fonction du niveau de dégradation d'un sous-système et peut être utilisé par un autre sous-système identique.

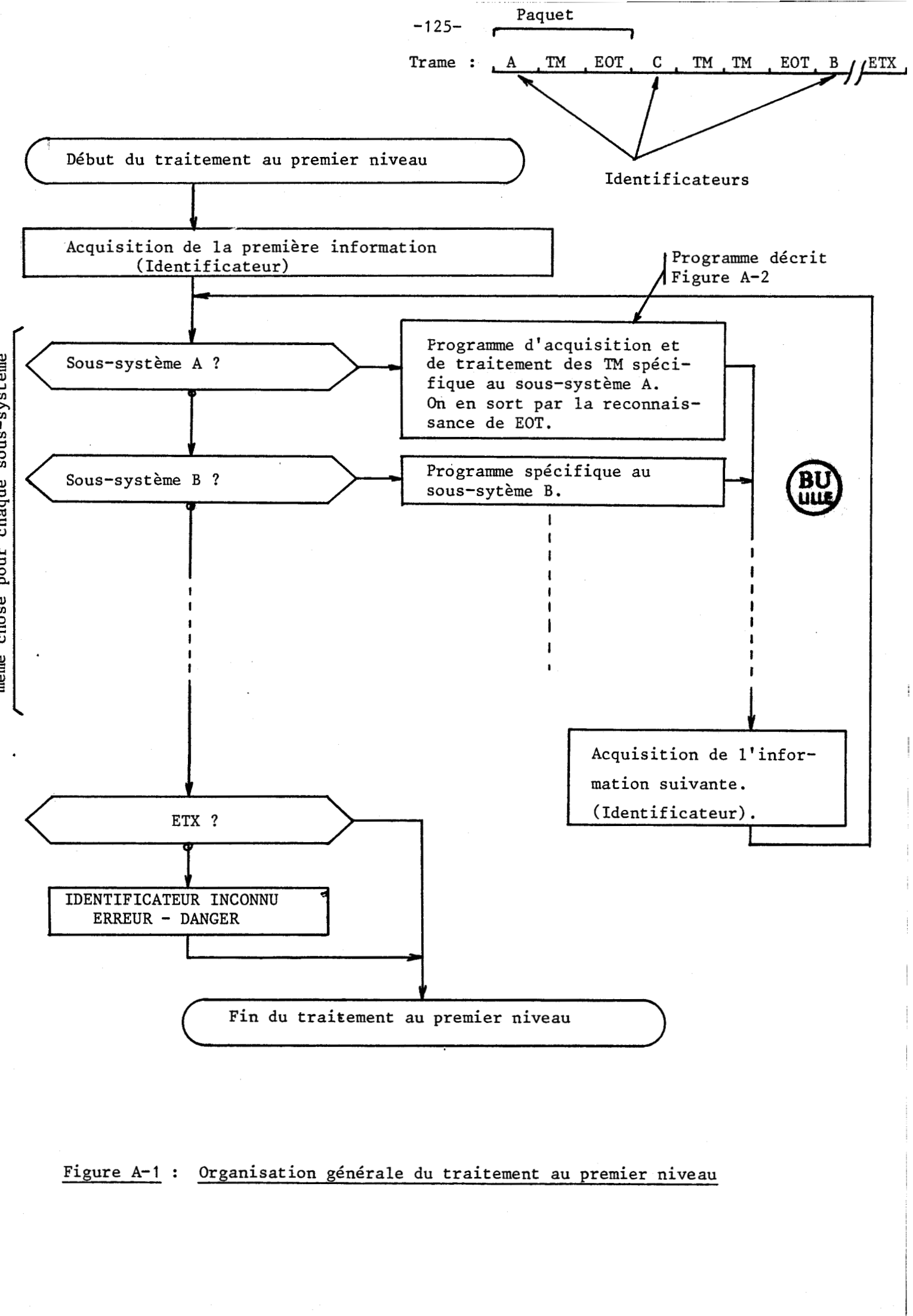


Figure A-1 : Organisation générale du traitement au premier niveau

La Figure A-2 montre l'organigramme de traitement d'un paquet de télémesures. Il est à remarquer que l'acquisition des télémesures et le traitement des informations de danger n'a rien de spécifique et peut être réalisé sous la forme d'un sous-programme utilisable par chaque programme spécifique.

Les variables spécifiques au sous-système sont :

- la variable précisant le module de traitement choisi
- " " " l'état de la liaison
- " " orientée exploitation
- " " orientée maintenance
- le pointeur de pile destiné au stockage des N dernières TM
- l'adresse de la zone mémoire destinée au stockage des TM avec datation et nombre d'occurences.

Les cinq premières variables sont susceptibles d'être modifiées à chaque nouvelle témémesure.

On remarque immédiatement la modularité du programme qui permet de l'adapter à d'autres processus. L'enchainement des modules permettant le traitement des télémesures (Figure A-3) permet de voir facilement la correspondance qui existe entre les différents modules et le processus à contrôler.

II - DESCRIPTION DES TRAITEMENTS EFFECTUES PAR LA SECONDE COUCHE DU LOGICIEL (2B)

* Traitement des télécommandes

Il est effectué à partir d'une véritable tâche de commande-contrôle qui consiste à décomposer une télécommande globale en plusieurs séries de télécommandes correspondant aux étapes successives qui permettent d'amener le processus vers l'état attendu. L'émission d'une série de télécommandes est conditionnée par la validation de la série précédente |Figure A-4|. Lorsqu'une

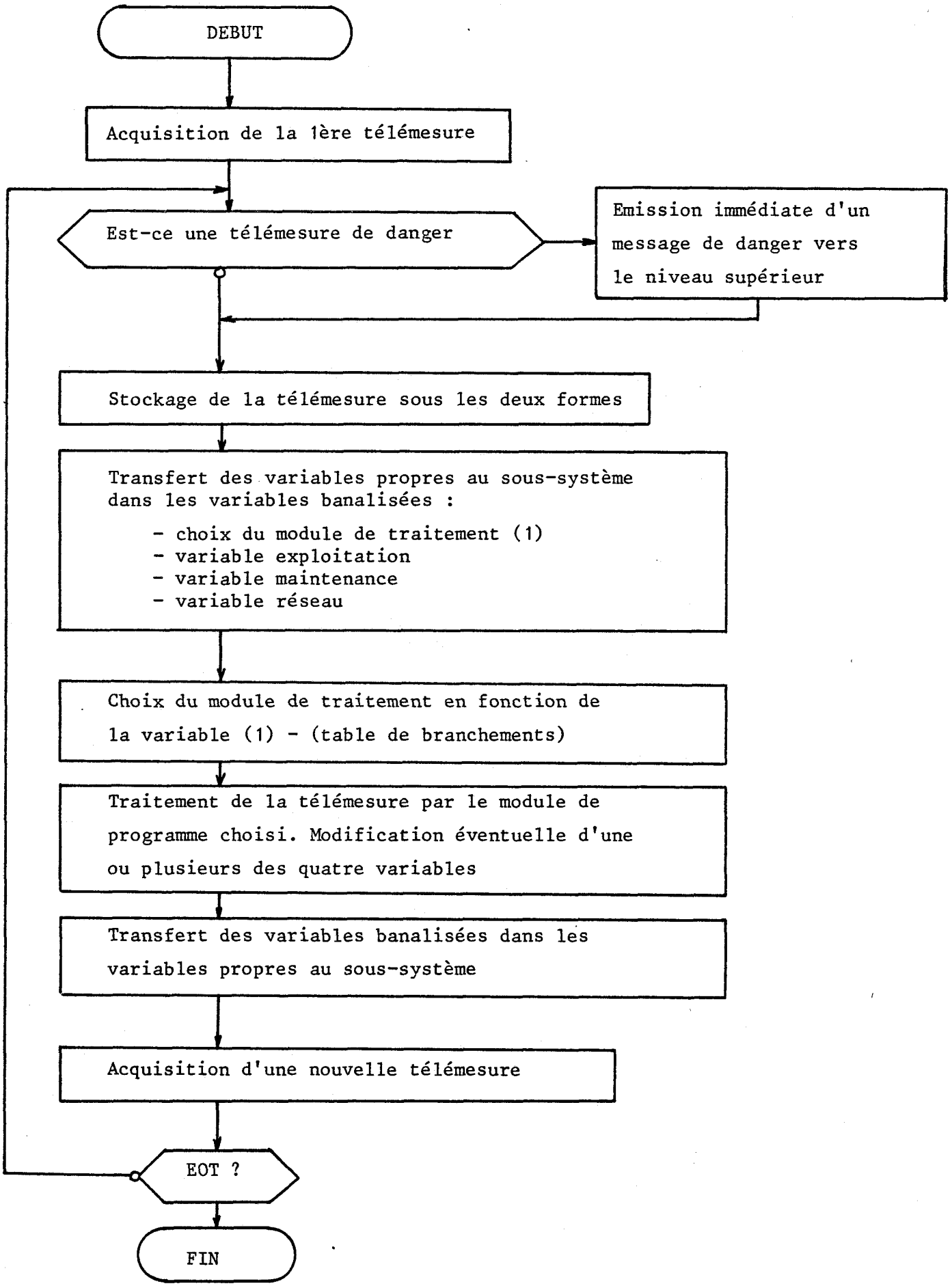


Figure A-2 : Organigramme de traitement d'un paquet de télémesures.

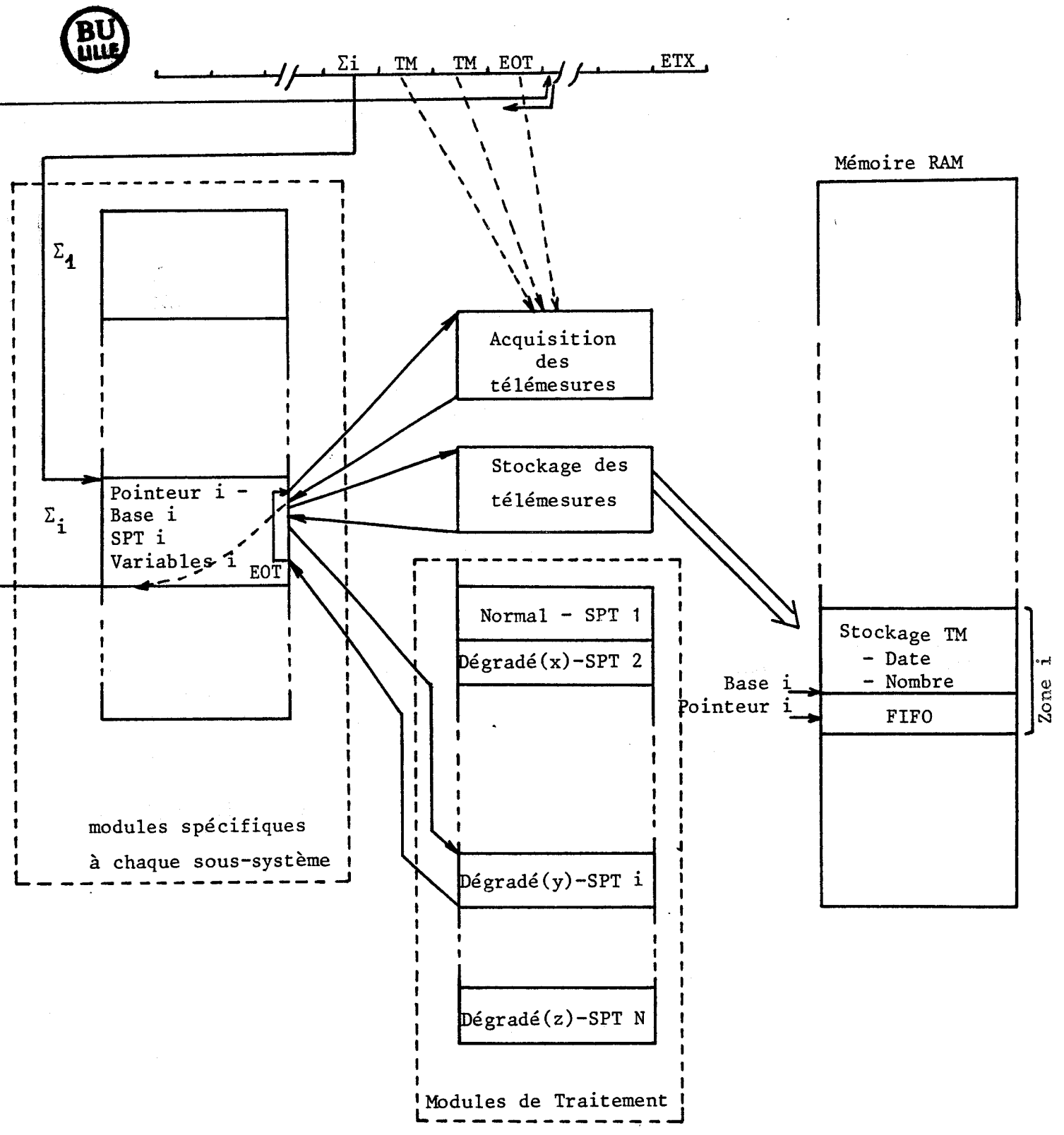


Figure A-3 : Séquencement des tâches effectuées par la 1ère couche de logiciel (2A)

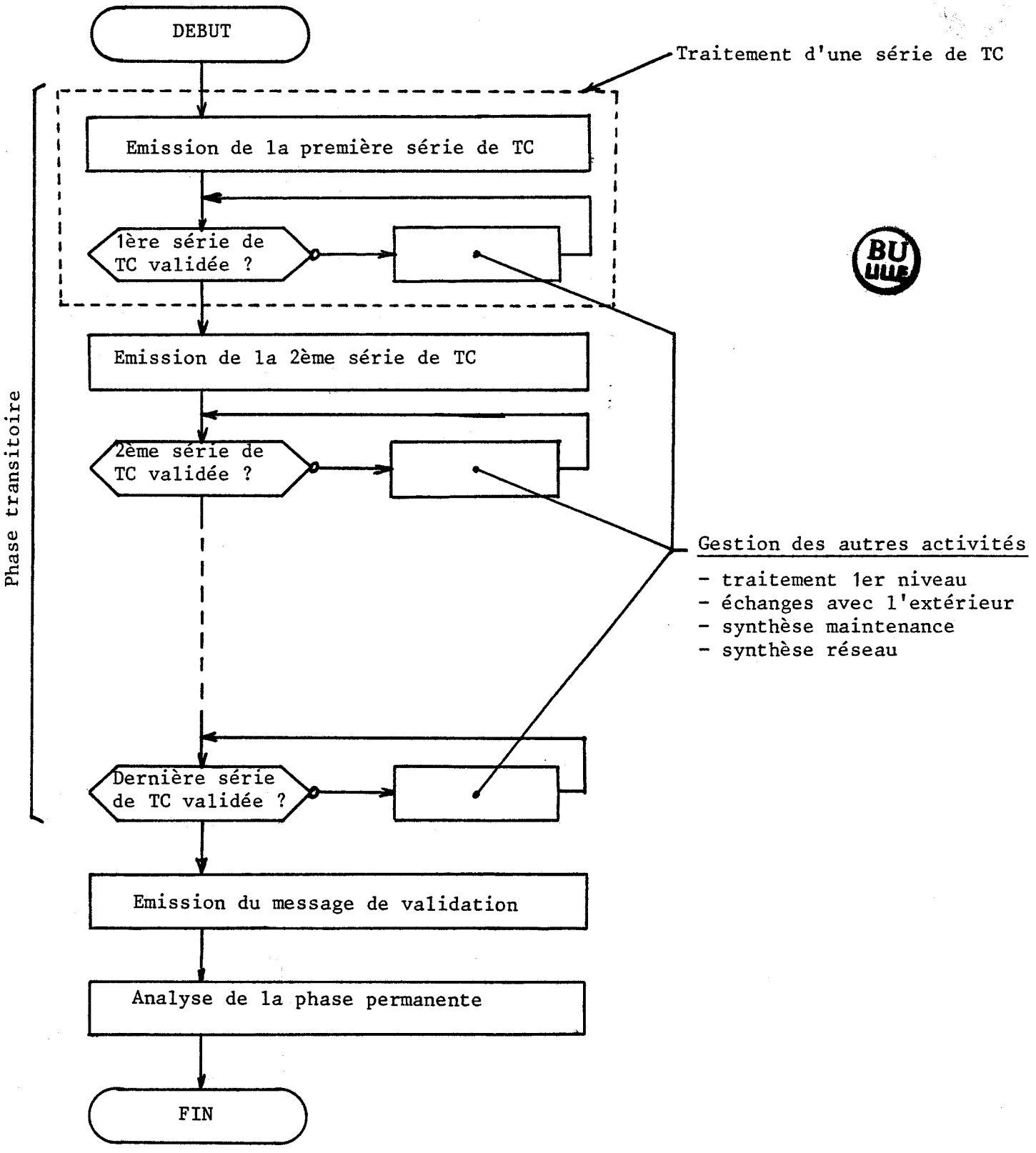


Figure A-4 : Organisation générale du traitement d'une télécommande

télécommande n'est pas validée, ou ne correspond pas à l'état attendu, on peut réemettre la télécommande, puis à l'issue d'un délai, diagnostiquer un défaut dont on ne peut toutefois préciser la nature. Le traitement d'une série de télécommandes est représenté par l'organigramme de la Figure A-5.

* Gestion des ressources du réseau

Le traitement des défauts de liaisons ou de satellites consiste à vérifier que lorsqu'un défaut se présente, l'état du processus reste observable grâce à une redondance totale ou partielle qui reste opérationnelle (Figure A-6).

* Synthèse des informations d'état de fonctionnement du système

Elle consiste à signaler tout nouveau défaut (Figure A-7). Lorsqu'un défaut a été signalé, il est dit validé, c'est-à-dire qu'il n'est plus signalé ultérieurement, bien que sa présence reste prise en compte par le programme.

Lorsqu'il y a validation d'une télécommande, on signale, parmi tous les défauts, celui qui est le plus perturbant. Les messages qui sont envoyés ne précisent que la gravité des défauts et non la nature. Dans notre application seuls deux types de messages peuvent être envoyés :

- défaut tolérable
- appel maintenance.

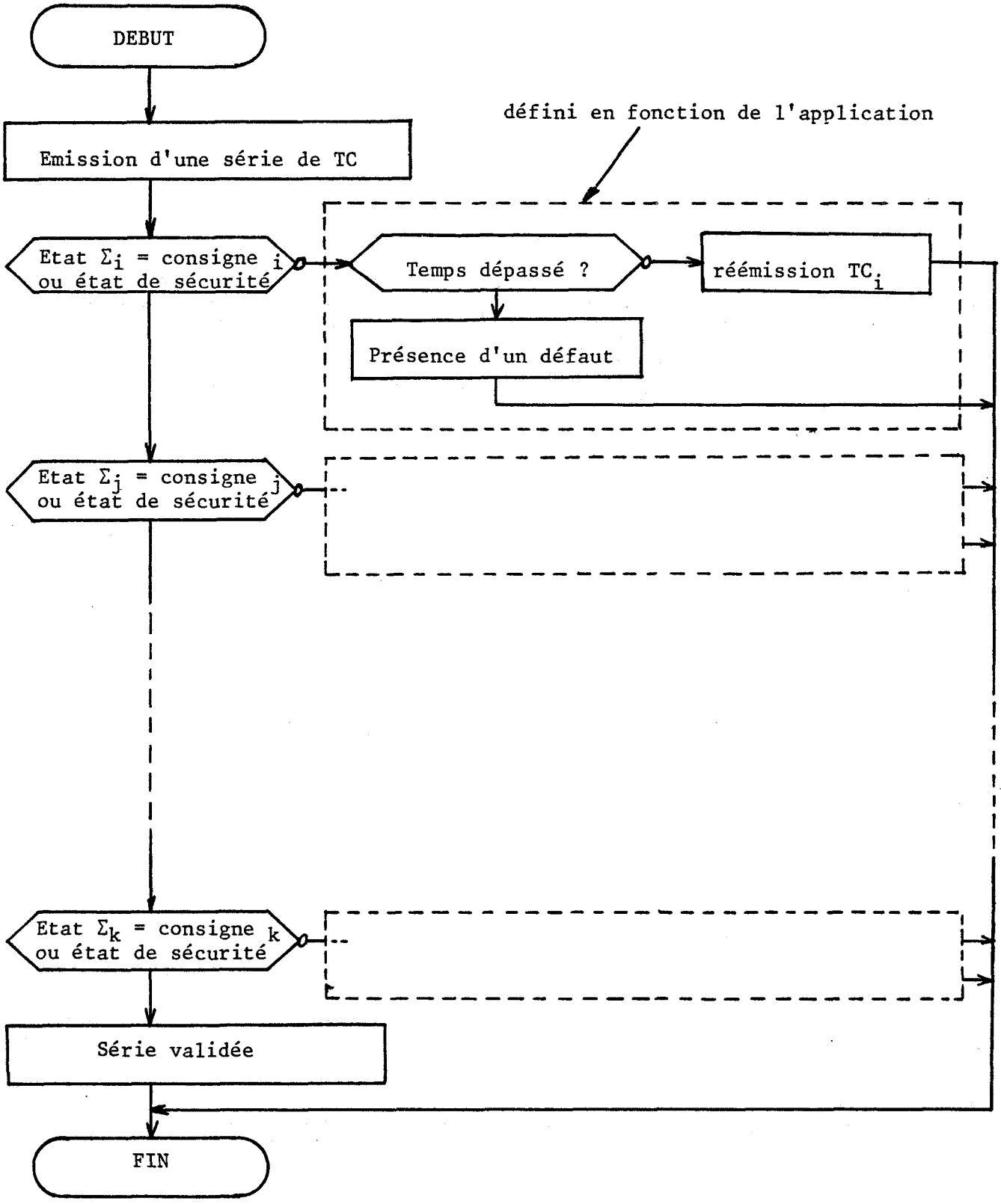


Figure A-5 : Traitement d'une série de télécommandes

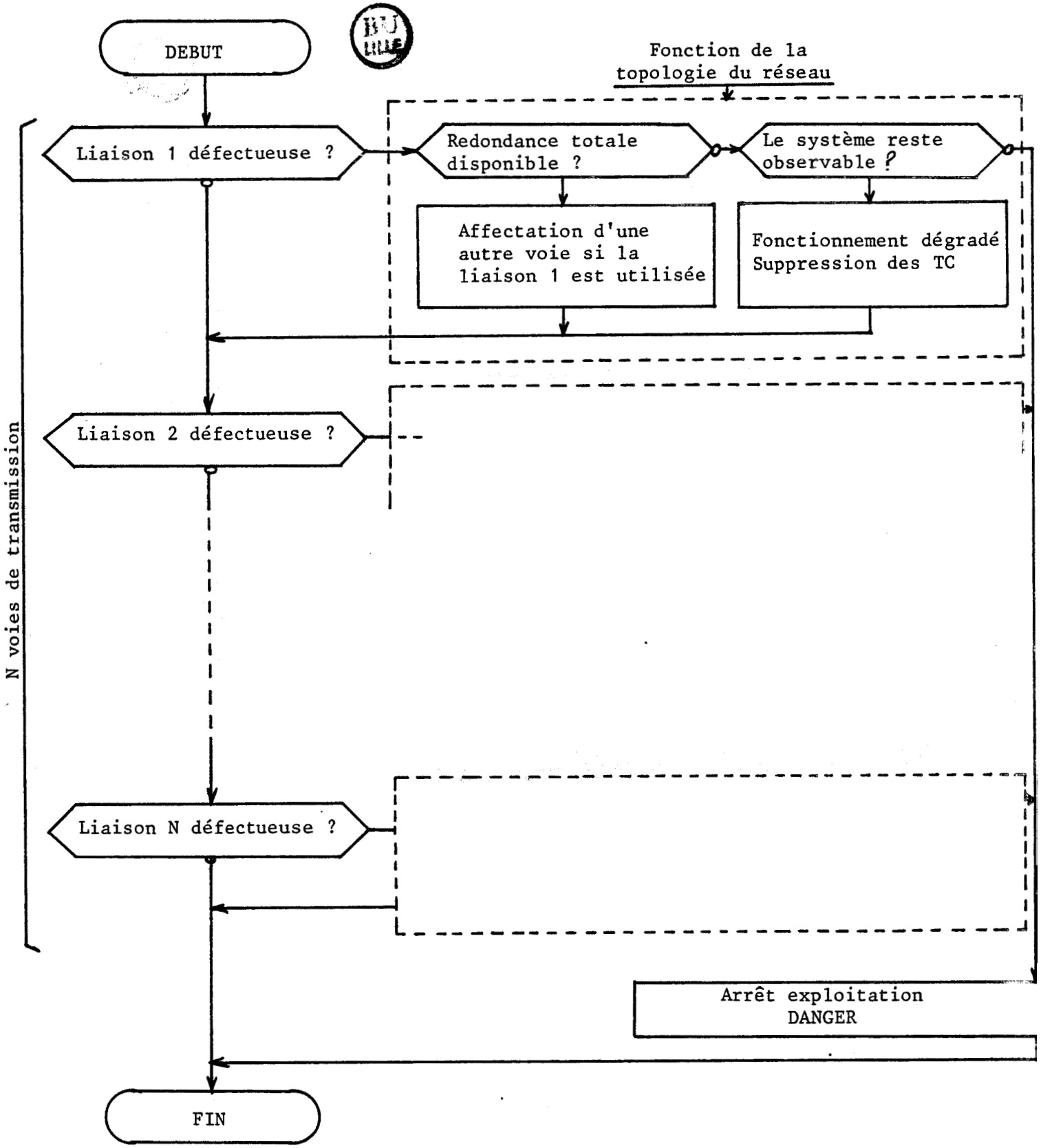


Figure A-6 : Algorithme de traitement des défauts de liaisons

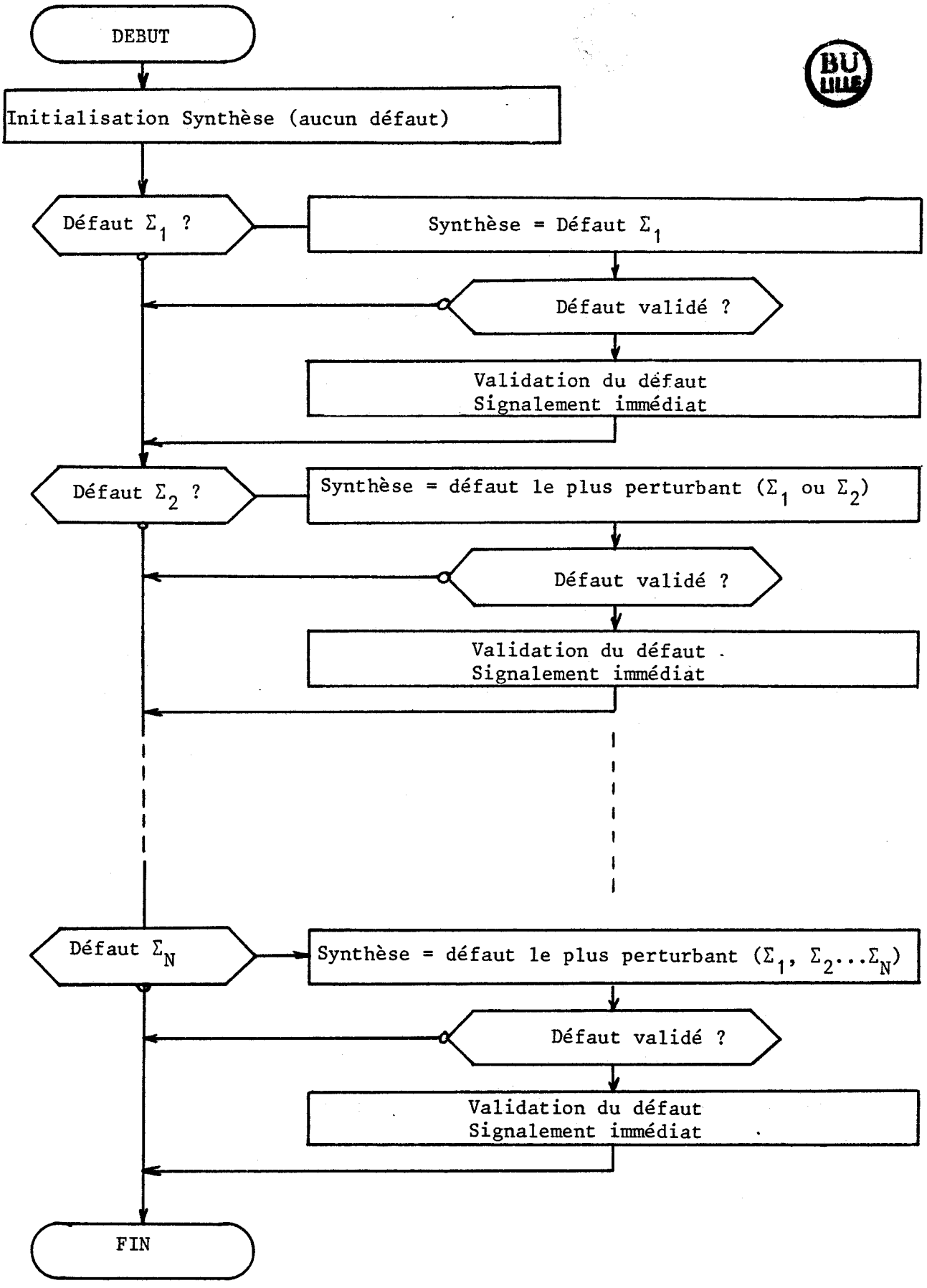


Figure A-7 : Synthèse des informations d'état de fonctionnement du système

TM 1	PORTE OUVERTE
TM 2	PORTE FERMEE VERROUILLEE
TM 3	FERMETURE EN MODE DEGRADE
TM 4	OBSTACLE A LA FERMETURE
TM 5	COMMANDE DE DEVERROUILLAGE IMPOSSIBLE
TM 6	CONTACT PORTE VERROUILLEE DEFECTUEUX COLLE EN POSITION FERME
TM 7	CONTACT PORTE FERMEE NC1 DEFECTUEUX COLLE EN POSITION FERME
TM 8	COMMANDE IMPOSSIBLE DE L'ELECTROVALVE D'OUVERTURE
TM 9	MDOP DEFECTUEUX COLLE EN POSITION BASSE PRESSION
TM 10	CONTACT PORTE OUVERTE NC1 DEFECTUEUX COLLE EN POSITION OUVERT
TM 11	COUPURE IMPOSSIBLE DE L'ELECTROVALVE DE FERMETURE
TM 12	GRIPPAGE DU MECANISME DE PORTE OUVERTURE COMPLETE IMPOSSIBLE
TM 13	CONTACT PORTE OUVERTE NC2 DEFECTUEUX COLLE EN POSITION OUVERT
TM 14	OUVERTURE DE LA PORTE PAR UN AGENT ITINERANT
TM 15	CONTACT PORTE OUVERTE NC2 DEFECTUEUX COLLE EN POSITION FERME
TM 16	COUPURE IMPOSSIBLE DE L'ELECTROVALVE D'OUVERTURE
TM 17	COMMANDE IMPOSSIBLE DE L'ELECTROVALVE DE FERMETURE
TM 18	CONTACT PORTE OUVERTE NC1 DEFECTUEUX COLLE EN POSITION FERME
TM 19	CONTACT PORTE OUVERTE NC1 DEFECTUEUX COLLE EN POSITION OUVERT
TM 20	FERMETURE IMPOSSIBLE DE LA PORTE APPEL D'UN AGENT
TM 21	PORTE CONDAMNEE PAR UN AGENT ITINERANT
TM 22	COUPURE IMPOSSIBLE DE L'ELECTROVALVE DE DEVERROUILLAGE
TM 23	CONTACT PORTE VERROUILLEE DEFECTUEUX COLLE EN POSITION OUVERT
TM 24	MDOP DEFECTUEUX COLLE EN POSITION HAUTE PRESSION
TM 25	PORTE NON ENTRAINANTE
TM 26	PORTE CONDAMNEE
TM 27	CONTACT PORTE OUVERTE NC1 DEFECTUEUX CHANGEMENT D'ETAT INTEMPESTIF
TM 28	CONTACT PORTE OUVERTE NC2 DEFECTUEUX CHANGEMENT D'ETAT INTEMPESTIF
TM 29	COMMANDE INTEMPESTIVE DU VERROU SYSTEME DE VERROUILLAGE DEFECTUEUX
TM 30	CONTACT PORTE VERROUILLEE DEFECTUEUX CHANGEMENT D'ETAT INTEMPESTIF
TM 31	OUVERTURE EN LIGNE DE LA PORTE DANGER COUPURE FS/HT
TM 32	CONTACT PORTE FERMEE DEFECTUEUX CHANGEMENT D'ETAT INTEMPESTIF
TM 33	MDOP DEFECTUEUX CHANGEMENT D'ETAT INTEMPESTIF
TM 34	CETTE TELEMESURE N'EXISTE PAS
TM 35	DEVERROUILLAGE INTEMPESTIF.PORTE FERMEE.VEHICULE EN LIGNE
TM 36	CONTACT D'EVACUATION D'URGENCE DEFECTUEUX
TM 37	DEMANDE D'EVACUATION D'URGENCE .DANGER COUPURE FS/HT
TM 38	CETTE TELEMESURE N'EXISTE PAS
TM 39	NE VOUS OPPOSEZ PAS A LA FERMETURE DE LA PORTE S.V.P
TM 40	POUVEZ VOUS AIDER A LA FERMETURE DE LA PORTE S.V.P
TM 41	CETTE TELEMESURE N'EXISTE PAS
TM 42	DEMANDE D'EVACUATION D'URGENCE SUR LA PORTE OPPOSEE.DANGER COUPURE FS/HT
TM 43	CONTACT DE DEMANDE D'EVACUATION D'URGENCE SUR L'AUTRE PORTE DEFECTUEUX
TM 44	OUVERTURE EN LIGNE DE LA PORTE OPPOSEE.DANGER COUPURE FS/HT
TM 45	CONTACT PORTE VERROUILLEE DE LA PORTE OPPOSEE DEFECTUEUX
TM 46	CONTACT PORTE FERMEE DE LA PORTE OPPOSEE DEFECTUEUX
TM 47	CETTE TELEMESURE N'EXISTE PAS
TM 48	LE MICROPROCESSEUR NE REPOND PLUS AUX DEMANDES DE TELEMESURES

Code et signification des différentes télémesures qui peuvent être élaborées par les satellites ou le système coordonnateur.

Exemple de transfert d'informations destinées aux agents de maintenance :

NB : Nombre d'occurences

DATP : Date de la 1ère apparition

DATD : Date de la dernière apparition

	PORTE 1			PORTE 2			PORTE 3			PORTE 4			PORTE 5			PORTE 6		
TM	NB	DATP	DATD	NB	DATP	DATD	NB	DATP	DATD	NB	DATP	DATD	NB	DATP	DATD	NB	DATP	DATD
1	8	9: 6	11:30				9	9: 6	11:30				9	9: 6	11:30			
2	18	9: 5	11:31	12	9: 5	11:31	20	9: 5	11:31	12	9: 5	11:31	20	9: 5	11:31	12	9: 5	11:31
3																		
4	13	10:50	10:51															
5																		
6	4	9: 6	10:54															
7																		
8	1	11:29	11:29															
9																		
10																		
11																		
12																		
13																		
14																		
15																		
16																		
17	1	11:30	11:30															
18																		
19																		
20	1	10:51	10:51															
21	1	10:51	10:51															
22																		
23																		
24																		
25	6	9: 6	10:54				9	9: 6	11:30				9	9: 6	11:30			
26	3	10:51	11:30															
27																		
28	1	11:12	11:12															
29																		
30																		
31																		
32																		
33																		
35																		
36																		
37																		
39	1	10:50	10:50															
40	1	10:50	10:50															
42																		
43																		
44																		
45																		
46																		
48																		

NOMBRE DE MANOEUVRE DES PORTES GAUCHES: 9

NOMBRE DE MANOEUVRE DES PORTES DROITES: 0

ANNEXE 3

-o-o-o-o-o-o-o-

EVALUATION DU TAUX DE DÉFAILLANCE D'UNE LIAISON

Pour déterminer les taux de défaillance horaire des composants |Réf. 13-14|, nous avons retenu les conditions suivantes :

- feuilles de données simplifiées
- composants agréés PTT sans contrôle de qualité
- température ambiante : 40°C
- Environnement : au sol mais mobile.

Taux de défaillance :

Transistor bipolaire $\lambda_T = 21\ 10^{-8}/h$

Résistance (R < 100 kΩ) : $\lambda_R = 3\ 10^{-8}/h$

Photocoupleur : $\lambda_p = 3\ 10^{-6}/h$

Connecteur : $\lambda_c = (36 + 2N)\ 10^{-9}/h$

N = nombre de contacts actifs $\lambda_c = 4{,}4\ 10^{-8}/h$

Câble (100 m) : $\lambda_{lo} = 10^{-6}/h$

Pour une liaison bidirectionnelle, le taux de défaillance est donné par :

$\lambda_1 = 4 \times \lambda_T + 8\ \lambda_R + 2\ \lambda_P + 2\ \lambda_c + 4 \times 1 \times \lambda_{lo}$

1 = longueur de la liaison/100 m ≠ 0,3

$$\boxed{\lambda_1 \cong 8{,}5\ 10^{-6}/h}$$

RESUME

La thèse présente les résultats d'une recherche sur le problème de commande en sécurité de processus géographiquement répartis à bord d'un véhicule de transport tel une rame de métro. La mise en oeuvre de dispositifs microinformatiques pour traiter ce genre de problème nécessite une approche différente de l'étude de la sécurité.

Dans un premier chapitre, après avoir rappelé les différents concepts de sécurité, appliqués aux transports guidés sécurité intrinsèque,puis avec l'avènement des microprocesseurs, sécurité probabiliste, nous posons de façon générale les calculs d'indice de sécurité des sous-ensembles par analogie avec les calculs classiques de fiabilité. Sur un plan architectural nous développons les avantages d'une structure de commande de processus décentralisée dont le traitement est hiérarchisé sur plusieurs niveaux. Outre la sécurité, les objectifs attendus sont l'aide à l'exploitation par tolérance à certains défauts, et l'aide à la maintenance.

En nous appuyant sur une maquette de laboratoire, nous présentons dans les chapitres 2 et 3, les études relatives au réseau de communication entre les différentes unités de traitement, où nous montrons par le calcul des indices de sécurité et de disponibilité qu'un réseau du type étoile apporte un bon compromis, puis enfin nous exposons de façon détaillée les traitements hiérarchisés effectués par le dispositif situé au coeur de l'étoile.

Les tâches particulières propres à notre étude et traitées par logiciel sont présentées sous forme classique de couches de logiciel, que nous situons par rapport à la classification restreinte du modèle ISO appliquée aux réseaux locaux de commande-contrôle de processus.

MOTS CLES :

- Sécurité - Disponibilité - Transports urbains
- Commande-Contrôle - Réseau local
- Traitement hiérarchisé