Conception d'un support de communication sûr de fonctionnement pour systèmes de surveillance et de sécurité : REBECCA

Jean-Paul Blanquart

N° d'ordre : 241

Année 1983

THÈSE

présentée

A L'INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE

pour l'obtention

du DIPLÔME de DOCTEUR INGÉNIEUR

Spécialité : Automatique-Informatique

par

Jean-Paul BLANQUART

Ingénieur des Mines de PARIS

CONCEPTION D'UN SUPPORT DE COMMUNICATION SÛR DE FONCTIONNEMENT POUR SYSTÈMES DE SURVEILLANCE ET DE SÉCURITÉ : REBECCA

Soutenue le 22 avril 1983, devant la Commission d'examen :

MM.	A. COSTES	*Président*
	M. BOURDÉ	*Examinateurs*
	A. DE FERRY	
	J.-C. GUILLANTON	
	J.-C. LAPRIE	
	M. PAVARD	
	J.-P. THOMESSE	

BLANQUART (Jean-Paul).

SUJET : Conception d'un support de communication sûr de fonctionnement pour systèmes de surveillance et de sécurité : REBECCA. - 120 pages.

Thèse de Docteur-Ingénieur, Automatique-Informatique, INP TOULOUSE 1983 n° 241.

RESUME : Ce mémoire est consacré à la conception d'un support de communication sûr de fonctionnement, à temps d'accès borné et faible, pour systèmes distribués de surveillance et sécurité. L'analyse effectuée conduit à une approche par double décomposition intégrant la validation progressive des choix : la conception est menée par affinements successifs, conjointement sur plusieurs niveaux d'abstraction afin de prendre en compte l'ensemble des contraintes et de leurs interactions. Pour l'application traitée dans ce mémoire : le système réparti de protection des postes à très haute tension du réseau électrique français, deux niveaux d'abstraction sont retenus : transmission et transfert. Les choix et leur validation reposent sur des critères adaptés à chaque étape, qualitatifs (décentralisation, latence minimale,...) et quantitatifs (durée d'acheminement de rafales de messages urgents, évaluation de la sûreté de fonctionnement et plus particulièrement de la sécurité). Cette méthode permet de retenir un support reconfigurable à deux boucles optiques contrarotatives indépendantes avec accès asynchrone par la technique d'insertion de registre.

MOTS CLES : - Sûreté de fonctionnement
- Systèmes distribués
- Réseau local
- Temps réel
- Architecture en boucle
- Insertion de registre

---

date de soutenance : 22 avril 1983

JURY : Président : A. COSTES
Membres : M. BOURDE
A. DE FERRY
J.C GUILLANTON
J.C LAPRIE (LAAS)
M. PAVARD
J.P THOMESSE

"Appelez moi Docteur!"

Jules ROMAINS, Knock ou le triomphe de la médecine, Acte II, Scène I.

- Mais... qui diable est-ce donc?
- Un de ces crâneurs d'ingénieurs des Mines.

Jack LONDON, Croc-Blanc, chap. 18

AVANT-PROPOS

Les travaux présentés dans ce mémoire ont été effectués au LABORATOIRE D'AUTOMATIQUE ET D'ANALYSE DES SYSTEMES (LAAS) du CNRS. Je tiens à exprimer ma profonde gratitude à Monsieur G. GRATELOUP qui m'a accueilli au LAAS alors qu'il en était le Directeur, et à Monsieur D. ESTEVE qui lui a succédé à ce poste, pour la confiance qu'ils m'ont toujours témoignée.

Je remercie également Monsieur J.C LAPRIE, Responsable de l'équipe "Conception et Validation de Systèmes Informatiques Sûrs de Fonctionnement (CV)" du LAAS, qui m'a accueilli dans cette équipe et a dirigé mes travaux.

Ces travaux n'auraient pas été possibles sans l'aide du CNRS et d'Electricité de France. Je tiens à remercier le personnel de ces organismes, et en particulier Messieurs J.L BOUSSIN et M. PAVARD pour leur fructueuse collaboration à l'ensemble de l'étude présentée ici.

Je remercie Monsieur A. COSTES, Directeur-Adjoint du LAAS, pour l'honneur qu'il me fait en acceptant de présider ce Jury de Thèse.

Ma reconnaissance va à :

- Monsieur M. BOURDÉ, Chef du Service "Equipements Automatismes et Téléconduite" à CGEE-ALSTHOM,
- Monsieur A. DE FERRY, Responsable du Laboratoire "Mathématiques et Numérique" au GIERS-SCHLUMBERGER,
- Monsieur J.C. GUILLANTON, Ingénieur en Chef à la Direction Technique d'Electronique Serge Dassault,
- Monsieur J.C. LAPRIE, Maître de Recherche au CNRS, Responsable de l'équipe CV au LAAS,
- Monsieur M. PAVARD, Chef de la Division "Fonctionnement Dynamique des Réseaux" à la Direction des Etudes et Recherches d'EDF,
- Monsieur J.P. THOMESSE, Professeur à l'Institut National Polytechnique de Lorraine,

qui ont accepté la charge de participer au Jury.

Enfin, je ne saurais commencer ce mémoire sans souligner la compétence et la gentillesse de tous ceux qui m'ont prodigué aide et conseils.

Tout d'abord, s'il existe une place privilégiée dans cet avant-propos, je tiens à la réserver à Alain COSTES et Jean-Claude LAPRIE, en témoignage de reconnaissance et d'amitié. Ils ont su guider mes travaux et me faire profiter de leur expérience sans jamais m'imposer leur point de vue. Je suis heureux de pouvoir leur dédier ce mémoire, concrétisation de notre collaboration qui fut toujours agréable et enrichissante.

Je tiens à exprimer mes remerciements et ma reconnaissance à tous ceux qui ont participé à cette étude : Messieurs Jean-Louis BOUSSIN, Christian BEOUNES et David POWELL, et surtout Madame Karama KANOUN pour sa précieuse collaboration.

Je remercie également ceux qui ont rendu possible ou facilité la réalisation de ce mémoire :

- Madame J. DAURAT, Monsieur et Madame BISSON, et Monsieur R. GOURDEAU, chargés du Standard et de la Réception,
- Madame J. PENAVAYRE, Secrétaire de la Division II,
- Mademoiselle M. CABANES, et Messieurs J. CATALA, D. DAURAT, E. LAPEYRE MESTRE, R. LORTAL, et R. ZITTEL, du Service de Documentation et Tirage,
- Monsieur J. LESTRADE et Madame E. MATHIEU, du Service de Gestion.

Enfin, je profite de ces pages pour adresser mes salutations amicales à tous mes camarades de l'équipe CV, Jean ARLAT, Christian BEOUNES, Yves CROUZET, Joni FRAGA, Paul JOLY, Karama KANOUN, Parthasaraty NARAYANAN, Daniel NOYES, Nicole MAZARS, David POWELL, Mauro RODRIGUES, Pascal TRAVERSE, et Jean-Charles VALADIER, sans oublier les "anciens" de l'équipe : Christian LANDRAULT, Anne-Marie LEGWINSKI, et Jorge MOREIRA

SOMMAIRE

INTRODUCTION

Un très grand nombre d'études, congrès, réunions de travail,... sont consacrés aux réseaux locaux, avec pour objectifs des réalisations commerciales ou expérimentales, des supports de recherche ou des projets de normes.

Parmi ces études, un nombre croissant est consacré à la sûreté de fonctionnement des réseaux locaux :

- soit de la part des concepteurs de systèmes distribués, lorsque la multiplicité des unités dans ces systèmes les empêchent de négliger l'occurrence de fautes dans au moins l'une d'entre elles,
- soit de la part des concepteurs de systèmes sûrs de fonctionnement, pour lesquels la distribution apparaît comme une solution-clé, mais à la condition que le support de communication qui les relie soit lui-même sûr de fonctionnement.

C'est dans cette dernière catégorie que se situe l'étude présentée dans ce mémoire, et plus particulièrement dans le domaine des supports de communication pour systèmes décentralisés de surveillance et sécurité. Il s'agit d'un domaine encore très peu exploré lorsqu'on le compare au domaine des réseaux locaux pour applications de bureautique, informatique, commande de processus, etc..., malgré l'aspect particulièrement critique de la sûreté de fonctionnement de ce type de système, et l'intérêt évident qu'il y a le plus souvent à les concevoir selon une architecture décentralisée.

Il apparaît toutefois que décentraliser les tâches, le contrôle et la commande, ne présente d'intérêt que si les différentes entités peuvent effectivement coopérer, se communiquer des informations, détecter les défaillances des autres entités et s'accorder sur la façon d'y remédier. Ceci suppose donc la présence d'un support d'échange d'informations dont la sûreté de fonctionnement et les performances fonctionnelles soient compatibles avec celles requises du système global.

Parmi les applications possibles de tels supports d'échange d'informations, nous nous intéressons plus particulièrement ici au système de surveillance et sécurité assurant les missions de protection dans les postes à très haute tension du réseau électrique français.

L'équipe "Conception et Validation de systèmes informatiques sûrs de fonctionnement" du LAAS-CNRS participe depuis 1978 au projet PAN (puis PANDOR) : Poste à Automatismes Numériques (Disjoncteur à Ouverture Rapide), mené par Electricité de France ; ce projet concerne l'introduction des techniques numériques dans le système "basse tension" des postes à très haute tension.

La contribution du LAAS à ce projet a d'abord consisté en l'évaluation (du point de vue de la sûreté de fonctionnement) de l'architecture du système de surveillance et sécurité, appelé système de protection, et à la définition de nouvelles architectures.

Dans le prolongement de ces travaux, l'étude que nous présentons dans ce mémoire concerne la définition d'un support de communication pour ce système de protection, dans le cas où l'on retient une architecture distribuée.

Ce mémoire se compose de deux parties. La première, intitulée **Buts et Méthodes**, concerne l'analyse de l'étude envisagée, et comporte deux chapitres.

Le premier chapitre est destiné à étudier le système dans son contexte, afin de dégager par une approche descendante les caractéristiques essentielles de sa mission, et les spécifications de base qui en découlent, puis à situer cette étude par rapport aux domaines dont elle se rapproche le plus : la **sûreté de fonctionnement**, et les **réseaux locaux**. Nous montrons en particulier que le système étudié présente des besoins de sûreté de fonctionnement et de performances fonctionnelles (très faible temps d'accès garanti), qui le différencient nettement des solutions existantes.

Le deuxième chapitre concerne l'étude de la méthode de conception applicable à un tel système. Nous examinons d'abord le principe d'étude par décomposition, ses possibilités et ses limitations, puis les notions de décomposition en points de vue ou couches permettant de compléter la technique d'affinements successifs, et l'importance du choix des critères de conception. Nous étudions ensuite l'expression de ces notions pour le support de communication considéré, en déterminant les points de vue à retenir, et les critères à utiliser pour guider la conception dans les différents points de vue et pour les différentes étapes d'affinements.

La deuxième partie, intitulée **Application**, se compose de trois chapitres constituant trois étapes successives du processus d'affinement.

Le troisième chapitre concerne les choix de base qu'il est possible d'effectuer entre les différentes structures et les différentes procédures d'accès possibles, en utilisant les critères qualitatifs définis au deuxième chapitre : décentralisation, latence minimale, simplicité, flexibilité, coût, normalisation (utilisation de composants standards).

Le quatrième chapitre consiste en un affinement de ces premiers choix, basé sur une étude plus détaillée faisant intervenir d'une part une évaluation comparative de sûreté de fonctionnement, reposant sur une modélisation par processus markoviens, et d'autre part une évaluation du temps d'acheminement d'une rafale de messages. Cette étape conduit à une double boucle contra-rotative, avec accès asynchrone basé sur la technique d'insertion de registre.

Dans le cinquième et dernier chapitre, nous précisons cette solution, jusqu'aux niveaux de détail nécessaires pour en vérifier la faisabilité et la conformité aux objectifs initiaux, ce qui permet de valider l'ensemble du processus de conception.

PREMIERE PARTIE: BUTS ET METHODES

Dans cette partie, nous effectuons une analyse du système objet de l'étude, et nous examinons les méthodes que nous pouvons appliquer à sa conception.

Le premier chapitre donne une description du système selon une approche descendante, permettant de dégager :

- les raisons qui conduisent à concevoir un support de communication pour le système de protection du poste à très haute tension,
- les spécifications que doit satisfaire ce support, pour que la mission globale soit remplie : fourniture de l'énergie à un coût acceptable, ces deux termes étant pris dans un sens large incluant les possibilités (éventuellement dégradées) de fourniture hors du fonctionnement normal, et l'ensemble des coûts entraînés par les défaillances éventuelles.

Le deuxième chapitre concerne l'étude de la méthode applicable à la conception de ce support. Nous dégageons dans un premier paragraphe (§II.1) les principes permettant de faciliter cette conception, et surtout de valider les choix effectués au cours même du processus de conception. Ceci permet d'acquérir confiance dans la solution obtenue, ce qui est particulièrement important pour une application devant satisfaire des contraintes de **sûreté de fonctionnement**.

Dans le paragraphe II.2, nous précisons comment peuvent s'exprimer ces principes généraux sur un exemple, en choisissant bien sûr l'application considérée. Nous définissons ainsi les couches de décomposition et les critères de base que nous analysons ensuite pour en tirer des guides de conception efficaces adaptés à chaque niveau de détail et à chaque couche.

CHAPITRE I : PRESENTATION GENERALE

Ce chapitre est plus particulièrement consacré, dans la présentation générale de l'étude constituée par cette première partie, à la définition de l'objet de l'étude : le système de communication d'un poste à très haute tension.

Nous allons tout d'abord, dans le paragraphe I.1, l'étudier dans son contexte, afin de faire apparaître les raisons qui conduisent à définir les besoins relatifs à un tel système. Ceci permettra de dégager, dans le paragraphe I.2, les principales caractéristiques du système à étudier.

I.1 PRESENTATION DU SYSTEME OBJET DE L'ETUDE

Nous suivons pour cette description une démarche descendante, du réseau de transport de l'énergie électrique et des principes de sa protection, jusqu'au système de protection du poste à très haute tension et à son support de communication. Cette description s'appuie sur des documents qui donnent une vue plus complète de ce sujet : /EDF'75,RGE'sp,BAR'79/.

I.1.1 Introduction

Les installations de gestion de l'énergie en France sont conçues selon une structure hiérarchisée constituée, du sommet vers la base, d'installations à vocation de plus en plus locale, assurant la répartition de quantités de moins en moins importantes d'énergie, sous des tensions de plus en plus faibles.

L'élément crucial de cette structure est son sommet constitué par le **réseau de grand transport**, chargé de la répartition à l'échelle nationale de l'énergie électrique -à partir des gros centres producteurs vers les gros centres consommateurs- et de l'interconnexion avec les pays voisins. Il englobe les installations à Très Haute Tension (THT) : 400 et 225 kV.

I.1.1.1 Réseau de grand transport

Ce réseau présente la particularité d'être maillé, c'est à dire d'être constitué de nœuds (les **postes**) reliés par des **lignes** assurant des chemins multiples entre les différentes paires de postes, comme indiqué sur la carte de la figure I.1. Ceci permet une gestion plus souple des transferts d'énergie, en diminuant la dépendance des centres consommateurs vis-à-vis de la disponibilité (voire de l'existence) des centres producteurs de la même région, et du bon fonctionnement des équipements qui les relient à ces centres.

I.1.1.2 Protection du réseau

Le réseau présente une redondance structurelle (due au maillage) permettant, lorsqu'il est affecté par un défaut (court-circuit, ligne tombée à terre, etc...) :

- d'isoler, par le jeu des interconnexions réalisées dans les différents postes, la partie défectueuse en perdant le minimum d'équipements,

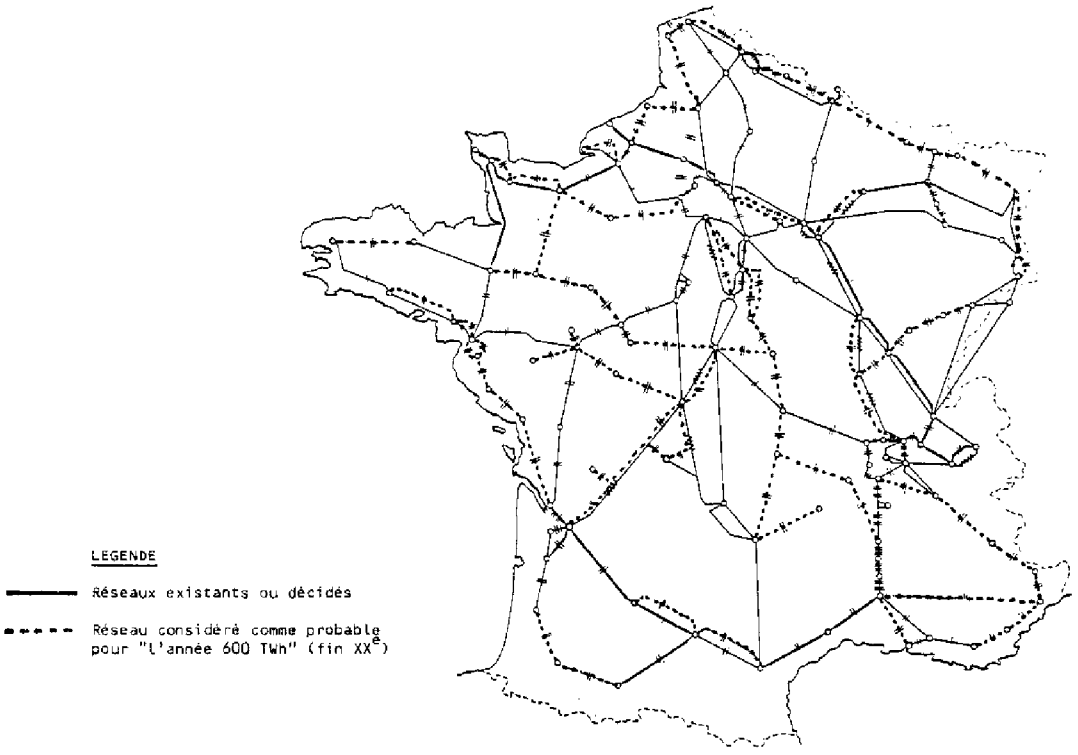


figure I.1 : structure maillée du réseau THT (extraite de /DEB'81/)

- de reporter la charge sur les parties encore saines du réseau, à condition de disposer dans ces parties de marges suffisantes de capacité, tant de transport que de production d'énergie.

Cette structure maillée entraîne cependant les inconvénients suivants :

- les effets d'un incident ont tendance à se propager sur l'ensemble du réseau. Il est donc **nécessaire** d'isoler rapidement la partie défectueuse, ce qui est **difficile**, car la propagation rend complexe la localisation du défaut,
- la mise en parallèle des sources d'énergie a pour conséquence l'augmentation de la puissance de court-circuit, et donc des dommages aux installations.

Remarquons enfin qu'il n'est pas toujours possible d'avoir un réseau bien équilibré, avec une répartition homogène des centres producteurs et consommateurs, et une réserve suffisante tant de production que de transport.

En résumé, il faut :

- isoler (et donc localiser) le plus rapidement possible la partie du réseau sur laquelle survient un défaut, afin de maintenir la stabilité du réseau (en tension et en fréquence),
- isoler la plus petite partie possible, pour éviter les réactions en chaîne dues aux transferts de charge en régime déséquilibré, ou fortement chargé.

Pour assurer un temps de réponse suffisamment court (pour fixer les idées, inférieur à un dixième de seconde) et pour accroître la sûreté de fonctionnement, la solution en France comme dans d'autres pays consiste à confier cette mission à un système de surveillance et sécurité (appelé **système de protection**) ; ce système est **distribué** : chaque nœud du réseau (c'est-à-dire chaque poste à très haute tension), est muni d'un système de protection de poste assurant de façon **autonome** la mission de sécurité, ou du moins la partie de cette mission concernant le poste considéré.

I.1.1.3 Poste à Très Haute Tension (THT)

Le poste THT est l'élément du réseau qui assure les interconnexions entre les lignes THT parvenant au point considéré. Pour cela, le poste est constitué d'un ou plusieurs **jeux de barres** (chaque jeu comprenant trois barres, une pour chaque phase, de même que chaque ligne est en fait triple, car le transport d'énergie se fait en régime triphasé). Ces jeux de barres sont des points de connexion, qui peuvent être reliés entre eux ou non, et à chacun desquels pourra être reliée chaque ligne parvenant au poste ; ces lignes sont appelées **départs** (quel que soit le sens du transfert d'énergie qui s'y effectue).

Les connexions sont réalisées par l'intermédiaire de **sectionneurs** et de **disjoncteurs** : les sectionneurs sont des organes mécaniques apparaissant à chaque connexion réalisable ; ils possèdent un pouvoir d'isolement très fort, mais un pouvoir de coupure nul : ils ne se commandent qu'à vide. Ils sont donc branchés en série avec les disjoncteurs, qui peuvent s'ouvrir ou se fermer en charge, mais avec un pouvoir d'isolement plus faible.
Remarque : il y a un disjoncteur et un sectionneur pour chaque couplage entre jeux de barres ; pour chaque départ, il faut autant de sectionneurs qu'il y a de jeux de barres auxquels ce départ peut être relié, mais un seul disjoncteur suffit pour protéger la ligne (voir la figure I.2).

La **conduite du poste** consiste à déterminer les connexions réalisant la structure désirée, et à effectuer ces connexions grâce au **système de commande** du poste, chargé, pour chaque connexion :

- d'ouvrir le disjoncteur associé au départ ou au couplage concerné,
- de manœuvrer le sectionneur associé à la connexion concernée (à réaliser, ou au contraire à supprimer),
- de fermer le disjoncteur.

La figure I.2 donne la structure d'un tel poste, représentée par son schéma **unifilaire** (les trois phases sont confondues). Pour simplifier ce schéma, nous n'avons pas fait apparaître le système de commande, ni le système de protection (qui fait l'objet du paragraphe suivant).

I.1.2 Système de protection

Rappelons que le système de protection **du poste** assure en fait la protection de **tout le réseau**, contre les défauts (courts-circuits, foudre, etc...).

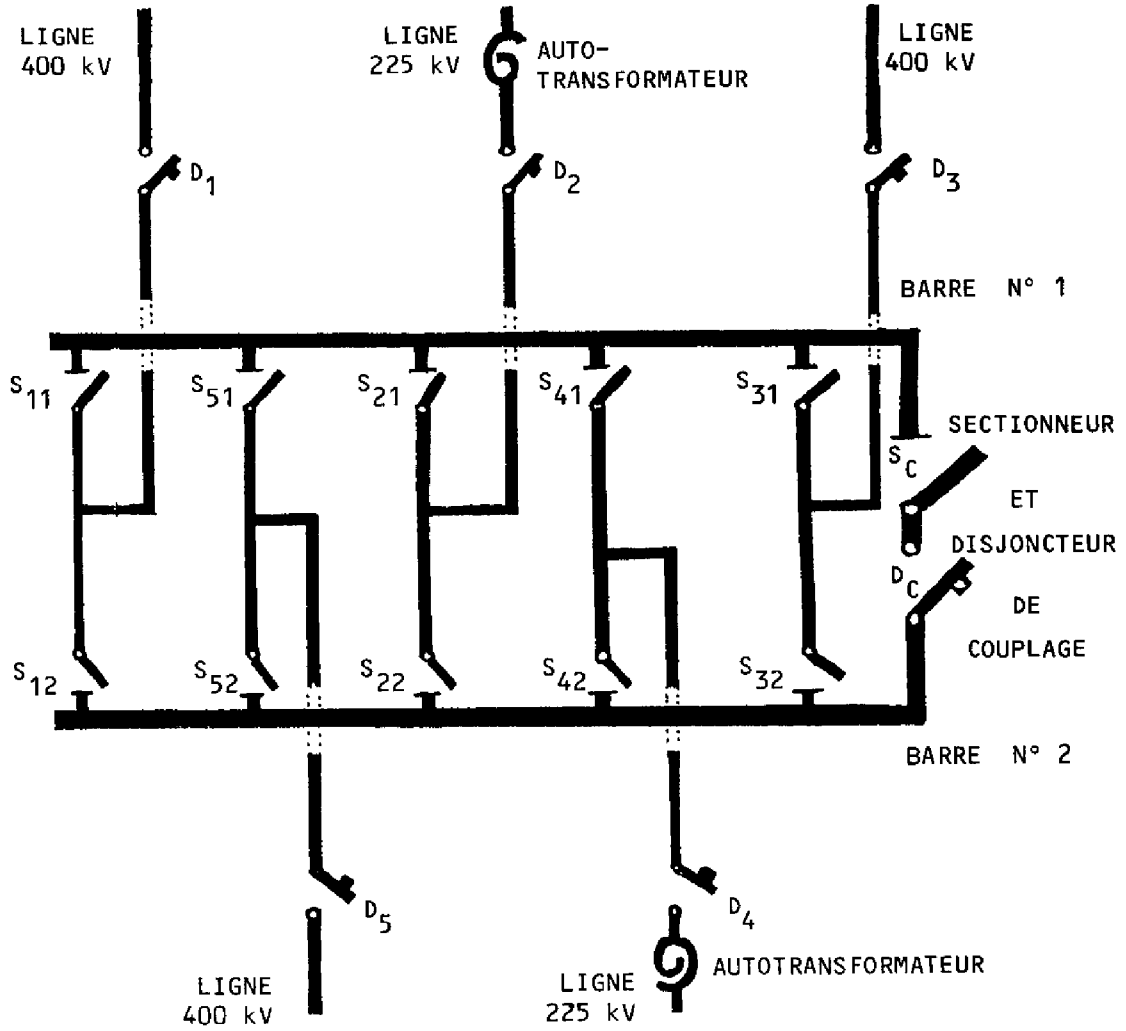


figure I.2 : schéma unifilaire d'un poste à très haute tension

I.1.2.1 Objectifs

La protection consiste à assurer l'**isolement** (rapide) de la partie en défaut, et à n'isoler que la partie **minimale**. Deux cas peuvent se présenter, selon que le défaut affecte une **ligne**, ou un **jeu de barres** :

- dans le cas d'un **défaut ligne** : il faut ouvrir, dans chacun des postes possédant cette ligne comme départ, le disjoncteur associé,
- dans le cas d'un **défaut barre** : il faut ouvrir, dans le poste auquel appartient ce jeu de barres, les disjoncteurs associés à tous les départs et à tous les couplages connectés à ce jeu de barres.

Remarque : comme pour tout système de protection, il faut inclure dans sa mission la nécessité de ne pas intervenir en l'absence de défaut. En toute rigueur, ceci fait d'ailleurs partie de l'exigence d'isolement minimal. Nous ne tiendrons pas compte, dans cette première description, de ce point qui sera abordé par la suite (paragraphes I.2.2.2, et II.2.2.4).

I.1.2.2 Moyens

Le principe de la protection du poste est basé sur le fait qu'il est possible, en mesurant sur chacun des conducteurs protégés par un disjoncteur, sa tension et le courant qui le traverse, de calculer **l'impédance**, et de déduire de cette valeur :

- l'occurrence d'un défaut sur le réseau,
- la direction de ce défaut par rapport au point de mesure.

Pour un disjoncteur associé à un départ, nous désignerons par :

- **amont** la direction des barres par rapport à ce disjoncteur,
- **aval** la direction opposée.

Dans le cas du **défaut ligne**, l'impédance calculée au disjoncteur du départ en défaut permet de **"voir le défaut en aval"**, alors que celles calculées aux autres disjoncteurs de départ (du moins ceux qui ne sont pas électriquement isolés du départ en défaut) permettent également de **"voir le défaut"**, mais **en amont**. Celles calculées aux disjoncteurs de couplage (non isolés du défaut) indiquent aussi le défaut, dans la direction du jeu de barres sur lequel est connecté le départ en défaut ; (la distinction amont-aval n'ayant pas de sens pour un tel disjoncteur).

Dans le cas du **défaut barre**, aucune impédance de départ ne permet de "voir le défaut en aval", et celles calculées pour les couplages non isolés du jeu de barres en défaut indiquent le défaut, dans la direction de ce jeu.

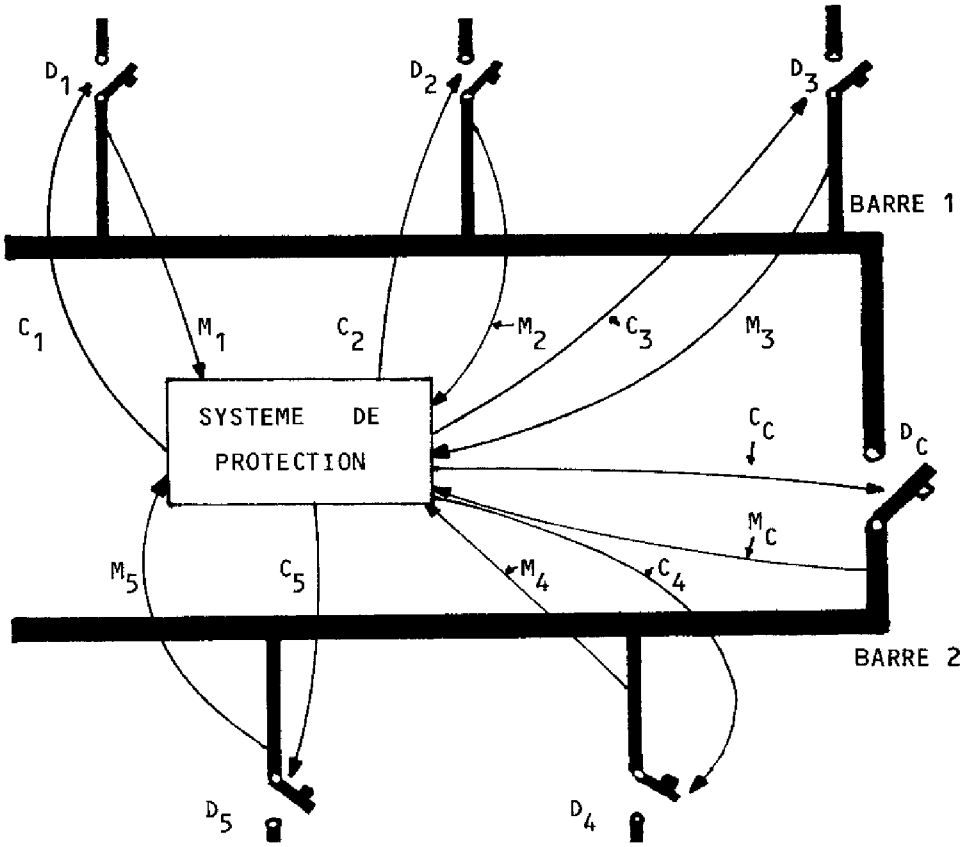
I.1.2.3 Actions

Les actions correctrices en cas de défaut (nous parlerons, selon la terminologie d'EDF, d'**élimination du défaut**), consistent à :

- dans le cas du défaut ligne, ouvrir le disjoncteur associé à cette ligne ; (le défaut ne sera correctement traité que si cette action est effectuée dans chacun des postes connectés à la ligne en défaut),
- dans le cas du défaut barre, ouvrir les disjoncteurs associés à tous les départs connectés sur cette barre, et ceux des couplages reliés à cette barre ; (le défaut est correctement traité sans intervention des autres postes).

Remarque : ceci montre qu'en toute rigueur, l'information de direction d'un défaut n'est pas suffisante, car il faut distinguer un défaut affectant une ligne d'un défaut affectant un poste voisin auquel est reliée cette ligne (dans ce deuxième cas, le poste considéré n'a pas à intervenir). Ceci est naturellement pris en compte dans la procédure complète, dont seule une description simplifiée est utile ici.

La figure I.3 donne un schéma fonctionnel des relations entre le système de protection et les installations du poste THT ; pour simplifier la lecture de cette figure, le système de commande et les sectionneurs n'y sont pas représentés.



M_i (M_c) : acquisition de mesure -détection de défaut, et direction- sur le départ i (ou couplage)

C_i (C_c) : commande du disjoncteur du départ i (ou couplage)

figure I.3 : schéma fonctionnel du système de protection

Remarque : il s'agit d'une description simplifiée des fonctions liées à l'élimination d'un incident. Une analyse complète devrait tenir compte des quatre points suivants :

Energie triphasée : les équipements électriques sont en fait triples, et leurs défauts peuvent concerner une, deux, ou les trois phases.

Réenclenchement : la plupart des défauts (en particulier les défauts ligne monophasés) sont fugitifs ; l'élimination de certains types de défauts est donc suivie d'une tentative de refermeture automatique des disjoncteurs concernés (ouverts de nouveau, et "définitivement" si le défaut est toujours présent après réenclenchement).

Gestion du neutre : lorsqu'un défaut oblige à isoler un équipement qui fixait le point neutre, il faut fixer ce point neutre dans un autre équipement (éventuellement plusieurs).

Elimination dégradée : lorsqu'un disjoncteur devant assurer l'isolement d'une partie en défaut est lui-même défaillant, le défaut se **propage**, en affectant d'autres parties, théoriquement saines. Il faut alors éliminer "en dégradé" le défaut en isolant les parties saines qui se révèlent indissociables de la

partie en défaut. Par exemple, un défaut ligne associé à une défaillance du disjoncteur du départ concerné oblige à ouvrir les disjoncteurs de tous les départs connectés sur le même jeu de barres que le départ (qui est alors doublement défaillant) : on parle alors de **faux défaut barre**. La même notion d'élimination dégradée apparaît lorsqu'un défaut se propage sur une barre saine (par défaillance du disjoncteur de couplage), ou sur une ligne saine (dont le disjoncteur est défaillant ; la propagation va alors jusqu'au poste à l'autre extrémité de la ligne).

I.1.3 Décentralisation de la protection

Le système de protection d'un poste THT est de nature centralisée, puisque les actions à prendre en chaque point dépendent de l'ensemble des informations disponibles dans le poste, et pas uniquement d'informations locales.

Cependant, EDF a préféré le réaliser selon une architecture décentralisée, ce qui substitue à la difficulté de concevoir un calculateur central de protection à très haute sûreté de fonctionnement (ce calculateur est en effet un "point dur" du système), la nécessité de doter chaque équipement local de capacités de traitement, et de moyens d'échanger des informations avec les autres équipements (avec naturellement, une sûreté de fonctionnement suffisante).

I.1.3.1 Principe

L'adoption d'une architecture décentralisée permet de détailler le schéma fonctionnel donné à la figure I.3 précédente. On peut en effet représenter le système de protection du poste selon le schéma de la figure I.4 dans lequel les **équipements** constituent des **stations**, notées S_i (ou S_c pour les stations de couplage).

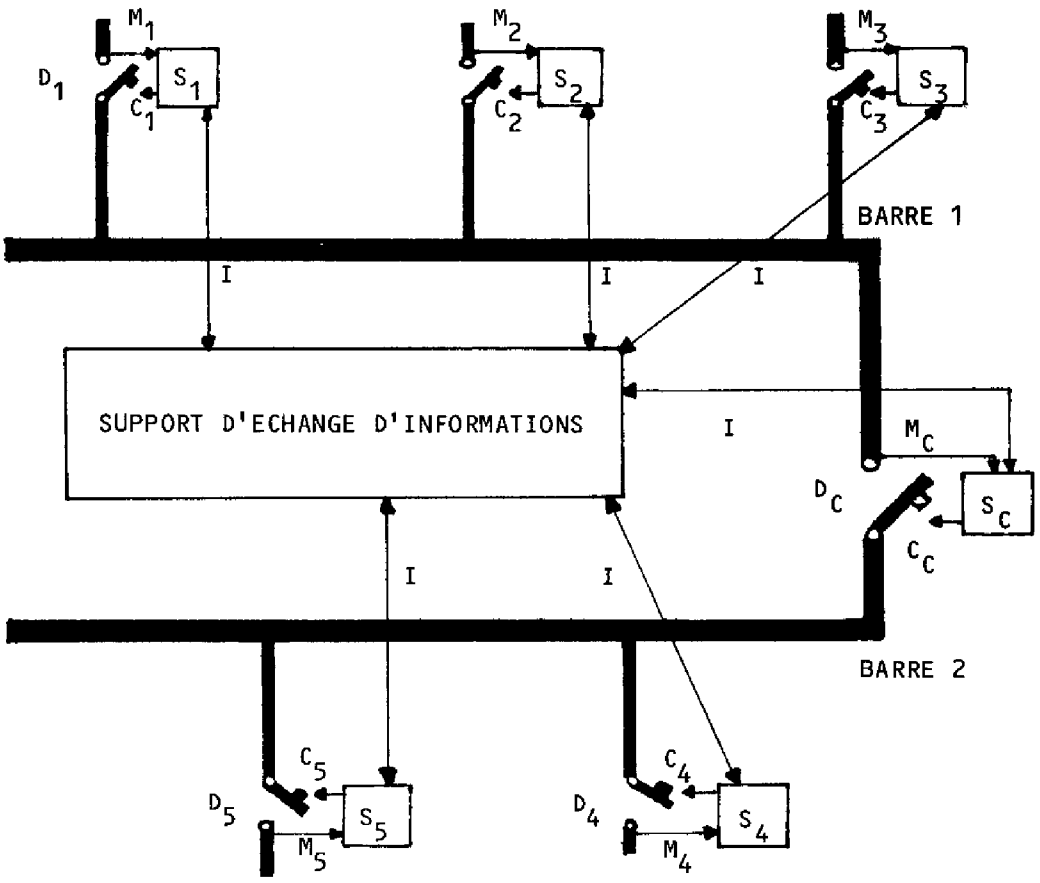
Ces stations acquièrent périodiquement des mesures, M_i (ou M_c), caractéristiques de l'état de la partie du réseau électrique qu'elles protègent. A partir de ces mesures, une procédure locale leur permet, après un premier traitement, d'envoyer éventuellement des informations I à d'autres stations, grâce à un **support d'échange d'informations**. Le traitement des informations reçues et des mesures locales permet alors à chaque station d'envoyer, le cas échéant, une commande C à son disjoncteur D_i (ou D_c).

Remarque : de la même façon que pour la figure I.3, le schéma de la figure I.4 ne fait pas apparaître le système de commande (pour la conduite du poste), ni les sectionneurs associés à chaque connexion.

I.1.3.2 Procédure locale

La procédure locale doit permettre à chaque équipement de déterminer, lorsqu'un défaut survient sur le réseau, s'il doit ou non ouvrir son disjoncteur.

Le cas d'un équipement de couplage et celui d'un équipement de départ sont différents ; nous allons donc les traiter séparément.



S_i (S_c) : Station de départ i (ou couplage) chargée :
- de l'acquisition et du traitement de la mesure locale,
- d'échanger éventuellement des informations de défaut (notées I) avec les autres stations,
- de commander éventuellement son disjoncteur.

figure I.4 : schéma de principe du système de protection distribué

Equipement de couplage

Un tel équipement peut déterminer la barre dans la direction de laquelle se trouve le défaut ; il sait alors que certains équipements n'ont pas à s'ouvrir, puisqu'il pourra les isoler du défaut par sa propre ouverture. Il enverra donc un **ordre de verrouillage** à tous les équipements connectés sur la barre d'où ne provient pas le défaut. Il devra de plus ouvrir son disjoncteur, mais seulement s'il s'agit d'un défaut affectant effectivement une des barres qu'il relie. Ce peut être un défaut affectant :

- une autre barre (ou un départ d'une telle barre) reliée par couplage à une de ses barres ; il recevra alors un ordre de verrouillage de la part d'un autre équipement de couplage,
- un départ relié à une de ses barres ; on verra dans la suite de ce paragraphe qu'il recevra un ordre de verrouillage de cet équipement de départ, qui seul doit s'ouvrir,
- une de ses barres : il ne reçoit pas d'ordre de verrouillage, et doit s'ouvrir.

Equipement de départ

Un tel équipement peut détecter un défaut :

- en **aval** : il s'agit alors d'un défaut ligne, et seul cet équipement le sait ; il doit donc :
  + **ouvrir** son propre disjoncteur,
  + envoyer un ordre de **verrouillage** à tous les autres équipements (de couplage et de départ) connectés sur la même barre que lui ; ces équipements ne peuvent en effet disposer d'aucune autre information distinguant ce cas d'un défaut sur la barre elle-même, pour lequel ils devraient s'ouvrir,
- en **amont** : il peut s'agir d'un défaut affectant :
  + une autre barre, ou un départ connecté sur une autre barre ; l'équipement doit alors recevoir un ordre de verrouillage provenant de l'équipement de couplage le reliant à la barre d'où provient le défaut,
  + un départ connecté sur la même barre que lui ; il doit alors recevoir un ordre de verrouillage de cet équipement de départ,
  + la barre même sur laquelle il est connecté ; il ne recevra alors aucun ordre de verrouillage, et devra s'ouvrir (ainsi que tous les équipements connectés sur cette barre).

I.1.3.3 Résumé

Ces différents aspects sont résumés dans le tableau de la figure I.5, pour un exemple de structure de poste.

Remarque : Une description complète des fonctions d'élimination de défaut devrait tenir compte du nombre de phases concernées par le défaut, des possibilités de réenclenchement, de la gestion du neutre, et de la notion d'élimination dégradée (voir la remarque du paragraphe I.1.2.3). Précisons également que cette analyse repose sur le principe des protections dites "de distance". Les besoins de communication dans un poste protégé selon d'autres principes (protections "différentielles" par exemple) ne seraient pas nécessairement identiques.

I.1.4 Système de communication du poste

Les paragraphes précédents ont montré les raisons de la présence d'un système de communication dans le système de protection d'un poste THT. Il faut préciser que les équipements du poste sont également reliés entre eux et à une station centrale de commande, pour les fonctions relatives à la conduite du poste (cette station n'est centrale que pour ces fonctions, et n'a aucun rôle dans les fonctions de protection). Les impératifs de coût et la nécessité de s'adapter aux évolutions, de taille, de structure, mais aussi éventuellement de principe, des postes THT, conduisent à l'étude d'un **système de communication** assurant l'**ensemble** des fonctions de communication dans un poste.

Les spécifications d'un tel système, qui font l'objet de ce paragraphe,

	DEFAUT SUR LA LIGNE N° i-j (BARRE i, LIGNE j)						DEFAUT BARRE N°1				
	$D_{1\bar{j}}$	D_{1j}	C_{12}	$D_{2\bar{n}}$	D_{2n}	C_{23}	D_{3m}	D_{1i}	C_{12}	D_{2k}	C_{23}	D_{3m}
DIRECTION DE DETECTION DU DEFAUT	AMONT	AVAL	VERS B1	AMONT		VERS B2	AMONT	AMONT	VERS B1	AMONT	VERS B2	AMONT
ENVOI DE MESSAGE DE VERROUILLAGE	-	M1 VERS $D_{1\bar{j}}$ C_{12}	M2 VERS D_{2k} C_{23}			M3 VERS D_{3m}	-	-	M2 VERS D_{2k} C_{23}	-	M3 VERS D_{3m}	-
RECEPTION MESSAGE	M1	-	M1	M2		M2	M3	-	-	M2	M2	M3
OUVERTURE ?	-	OUI	-			-	-	OUI	OUI	-	-	-

	DEFAUT SUR LA LIGNE N° 2-n (BARRE 2, LIGNE n)						DEFAUT BARRE N°2				
DIRECTION DE DETECTION DU DEFAUT	AMONT		VERS B2	AMONT	AVAL	VERS B2	AMONT	AMONT	VERS B2	AMONT	VERS B2	AMONT
ENVOI DE MESSAGE DE VERROUILLAGE	-		M4 VERS D_{1i}	-	M5 VERS $D_{2\bar{n}}$ C_{12} C_{23}	M3 VERS D_{3m}	-	-	M4 VERS D_{1i}	-	M3 VERS D_{3m}	-
RECEPTION MESSAGE	M4		M5	M5	-	M5	M3	M4	-	-	-	M3
OUVERTURE ?			-	-	OUI	-	-	-	OUI	OUI	OUI	-

NOTATIONS :

C_{12}: EQUIPEMENT DE COUPLAGE ENTRE LES BARRES 1 ET 2

C_{23}: EQUIPEMENT DE COUPLAGE ENTRE LES BARRES 2 ET 3

D_{1i}: EQUIPEMENTS DE DEPART CONNECTES A LA BARRE 1

D_{2k}: EQUIPEMENTS DE DEPART CONNECTES A LA BARRE 2

D_{3l}: EQUIPEMENTS DE DEPART CONNECTES A LA BARRE 3

$D_{1\bar{j}}$: TOUS LES D_{1i} SAUF D_{1j}

$D_{2\bar{n}}$: TOUS LES D_{2k} SAUF D_{2n}

STRUCTURE DU POSTE SUPPORT DE L'EXEMPLE

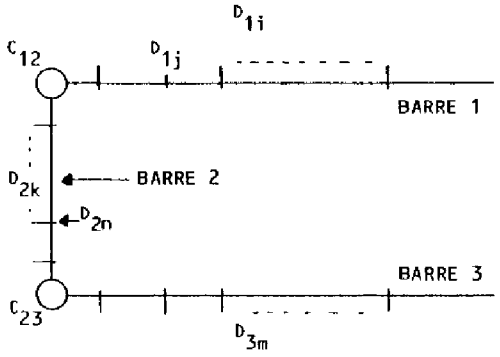


figure I.5 : algorithme de protection : tableau récapitulatif

peuvent se définir à partir de la connaissance de la **mission** de ce système, et de l'**environnement** dans lequel il doit l'accomplir.

La mission elle-même se décompose en une mission de **sécurité** (acheminement d'informations relatives à un défaut), et une mission de **service** (acheminement d'informations servant à la conduite du poste).

I.1.4.1 Mission de sécurité

Il s'agit de traiter les informations de défaut (direction de défaut, et gestion de neutre), qui doivent, lorsqu'un défaut survient sur le réseau THT, être communiquées par les équipements qui les possèdent à d'autres équipements du poste, qui en ont besoin pour assurer un traitement optimal du défaut.

D'après le principe de fonctionnement du système de protection (analysé au paragraphe I.1.3), nous voyons que le comportement des équipements dépend des informations qu'ils ont ou non reçues.

Pour des raisons de rapidité de traitement, et de quantité d'informations à traiter, il n'est pas question d'envoyer des messages spécifiques pour chaque information à transmettre. En fait, seuls les équipements de couplage, de départ voyant le défaut en aval, et ceux fixant le neutre auront des messages à transmettre. Les autres équipements possèderont aussi des informations (par exemple, détection d'un défaut en amont), mais qui seront supposées connues des autres équipements, **par défaut de message porteur d'information contraire.**

Compte tenu que :

- tous les équipements ne détectent pas le défaut au même instant,
- les messages ne peuvent pas être acheminés instantanément,
- tous les équipements n'ont pas de message à transmettre pour chaque occurrence de défaut,

on ne sait pas d'avance quel est le dernier message relatif à l'occurrence d'un défaut.

En conséquence, le seul critère dont peut disposer un équipement pour passer de l'état **information "x" non reçue** à l'état **information "non-x" vraie**, est un **délai maximal** au delà duquel il considère que tous les messages relatifs à un défaut ont été acheminés.

Ce délai doit être calculé en fonction de la durée du processus d'élimination de défaut et de la durée maximale pendant laquelle on peut tolérer la présence du défaut avant son élimination effective ; en effet, ce n'est qu'après expiration de ce délai que chaque équipement sera en mesure d'élaborer l'ordre d'ouverture de son disjoncteur.

Des études antérieures /BOU'80a/ du processus d'élimination d'un défaut ont conduit à retenir une valeur de **3 millisecondes**, pour le délai pendant lequel le support de communication devra pouvoir acheminer la **rafale** de messages relatifs à un défaut, sachant que dans le pire des cas, une telle rafale pourra contenir jusqu'à **7 messages.**

I.1.4.2 Mission de service

Si le système de protection est décentralisé, il n'en va pas de même du système de conduite du poste, régi par une station centrale envoyant des ordres (informations de **téléconduite**) aux différents équipements, et recevant des informations de **télémesure.**

Sur une longue période de temps, ces informations sont plus nombreuses que les informations de défaut, mais elles ne nécessitent pas un acheminement aussi rapide, ce qui conduit à un flux instantané plus faible. En conséquence, l'acheminement de ces informations n'induira pas directement de contrainte nouvelle.

Il n'y aura donc à prendre en compte que l'interaction entre ces deux types d'informations, c'est à dire dans ce cas, l'influence sur le traitement des informations de défaut de la présence simultanée d'informations de service.

Remarque : l'influence réciproque n'a pas d'intérêt, dans la mesure où les rafales de messages de défaut sont aussi rares que les défauts eux-mêmes, soit une dizaine par poste et par an, ce qui conduit à un taux d'occupation de seulement 10^{-10} pour les messages de défaut.

I.1.4.3 Environnement du système

Les spécifications du support de communication dépendent de l'environnement de ce support, au sens des mécanismes influant sur son comportement durant l'accomplissement de sa mission. Ce support de communication doit faire partie d'un **système de protection**, dans un **poste à très haute tension.**

Système de protection

Ce premier point permet de préciser l'importance de la mission du système à concevoir, et donc de fournir des critères significatifs pour élaborer une solution satisfaisante. En effet, on ne peut pas se contenter de choisir une solution présentant de bonnes performances fonctionnelles quand "tout marche bien". Au contraire, il faut étudier l'aptitude des solutions possibles à fournir des performances fonctionnelles suffisantes, non pas seulement dans les conditions optimales, mais dans les conditions réelles, c'est-à-dire en prenant en compte les différents cas possibles de mauvais fonctionnement.

Ce qui est vrai pour tout système prend donc encore plus d'importance pour un système de protection : le critère essentiel sera, non pas le service fourni par le système, mais la confiance que l'on peut avoir dans ce service. En conséquence, nous devons principalement mettre l'accent sur la **sûreté de fonctionnement** du système.

Précisons toutefois que les performances d'un système se définissent à partir de l'analyse de la mission de ce système. En l'occurrence, ce n'est donc pas tant la sûreté de fonctionnement du système de communication qui est significative, que l'influence de ce système sur la sûreté de fonctionnement du système de protection dans lequel il est inclus. De la même façon d'ailleurs, celle-ci se définit, en dernier recours par l'influence de ce système de protection sur la sûreté de fonctionnement du réseau électrique (disponibilité de l'énergie, non-dommage aux installations, à l'environnement, etc...).

Il faudra donc rechercher les critères à appliquer pour l'étude du système de communication en fonction de leur faculté à traduire la contribution de ce système aux performances escomptées du système de protection.

Poste à Très Haute Tension

Il s'agit ici de l'environnement physique proprement dit du système, qui influe directement sur les spécifications, dans la mesure où apparaissent :

- **des contraintes de dimensionnement** : ce système de communication doit interconnecter les équipements d'un poste ; tous les postes ne sont pas rigoureusement identiques, et de plus peuvent évoluer en taille comme en structure au cours de leur vie opérationnelle ; ceci entraîne pour le système de communication des spécifications :

+ de **capacité maximale** : les postes actuels comportent jusqu'à 4 jeux de barres et une quinzaine de départs (soit une vingtaine de **stations** pour le support de communication : 15 équipements de départ, 4 de couplage, et 1 pour le poste de conduite) ; nous adopterons en fait une valeur un peu plus élevée, conduisant à un support pouvant relier jusqu'à **30 stations** distantes de quelques centaines de mètres,

+ de **flexibilité** : ce terme recouvre la possibilité pour le système de fonctionner avec un nombre variable de stations, mais aussi la facilité avec laquelle on peut ajouter ou retrancher une station (si possible sans interrompre la communication entre les autres stations),

- **des contraintes de maintenance** :

+ pas de recours à des procédures manuelles régulières (inspection, maintenance préventive,...),

+ temps de réparation assez longs (à cause du délai avant intervention : jusqu'à 48 heures, sinon plus),

- **des contraintes technologiques**, dues à la très grande quantité de parasites électromagnétiques :

+ nécessité de protéger les systèmes électroniques et les liaisons de communication contre ces parasites,

+ nécessité de se limiter à des fréquences pas trop élevées (quelques Mégahertz), à cause de la mauvaise immunité aux parasites à haute fréquence.

I.2 CADRE DE L'ETUDE

Avant d'aborder l'étude proprement dite du système, il convient de préciser quelques points de terminologie, et de situer ce travail par rapport aux deux domaines essentiels auxquels il est lié :

- les **réseaux locaux**,
- la **sûreté de fonctionnement**.

I.2.1 Réseaux locaux

L'examen des spécifications détaillées au paragraphe I.1.4 permet de rattacher le support de communication à étudier au domaine des réseaux locaux. Il en possède en effet les caractéristiques essentielles :

- de dimensions : de l'ordre du kilomètre,
- de vitesse de transmission : de l'ordre du mégabit par seconde.

I.2.1.1 Normes et projets

Les réseaux locaux font l'objet, depuis quelques années, d'un très grand nombre d'études, de réalisations, mais aussi d'un effort de normalisation de la part de groupes internationaux réunissant des constructeurs, des utilisateurs et des chercheurs /ENJ'82,INF'82/.

Citons en particulier le "Projet 802" de l'IEEE /IEE'81/, le projet "PROWAY" de la CEI /AUG'81/, ainsi que les groupements de constructeurs : ECMA, et bien-sûr le système ETHERNET /MET'76/ promu par l'association entre DEC, INTEL, et XEROX (précisons que dans ce dernier cas, il ne s'agit pas d'une norme, mais d'une étude de système opérationnel).

D'une façon générale, il est essentiel de tenir compte des normes existantes ou en projet, même pour une application spécifique non couverte par ces normes, car :

- l'utilisation de tout ou partie d'une solution normalisée permet :
  + de réduire le coût, ainsi que le nombre de fautes de conception, par le recours à des composants (logiciels et matériels) normalisés (de tels composants subissent en effet par leur utilisation intensive dans des conditions variées et indépendantes des tests très efficaces),
  + d'accroître la modularité, et l'évolutivité par remplacement ou addition de composants de dernière génération,
- la conformité au moins partielle à une norme (ne serait-ce qu'à l'esprit d'une norme) peut transformer une étude spécifique en une contribution :
  + à l'étude ultérieure d'une norme couvrant le domaine considéré,
  + à la définition de nouveaux critères pour l'établissement de normes de réseaux standards universels.

Dans cet esprit, les principaux groupes d'étude des réseaux locaux ont retenu comme base de travail le modèle "**OSI**" défini par l'ISO. Il ne s'agit pas à proprement parler d'une norme, mais d'un **modèle de référence** pour "l'**interconnexion des systèmes ouverts**" /AFN'82/.

I.2.1.2 Relation avec le modèle OSI

En fait, ce modèle n'était pas initialement destiné aux réseaux locaux, mais aux moyens d'interconnexion de "gros" systèmes informatiques. le principe consiste à préconiser une structure en niveaux, ou **couches**. Ceci permet de regrouper certaines fonctions de communication de façon homogène. Chaque couche apparaît comme un **service** pour la couche immédiatement supérieure, exécuté de façon "transparente" pour cette couche :

- à l'aide des fonctions de la couche considérée, et
- en utilisant les services offerts par la couche inférieure.

Une telle approche ne s'applique naturellement pas uniquement aux systèmes de communication, mais elle présente dans ce cas un avantage, lié au fait qu'un tel système relie des abonnés distincts. Cette décomposition pourra alors être mise à profit pour autoriser l'interconnexion d'abonnés présentant des caractéristiques distinctes : il suffira de respecter les règles d'interconnexion pour chacune des couches considérées.

Ceci justifie la dénomination du modèle de référence : "Interconnexion des Systèmes **Ouverts**", dont le schéma est donné sur la figure I.6.

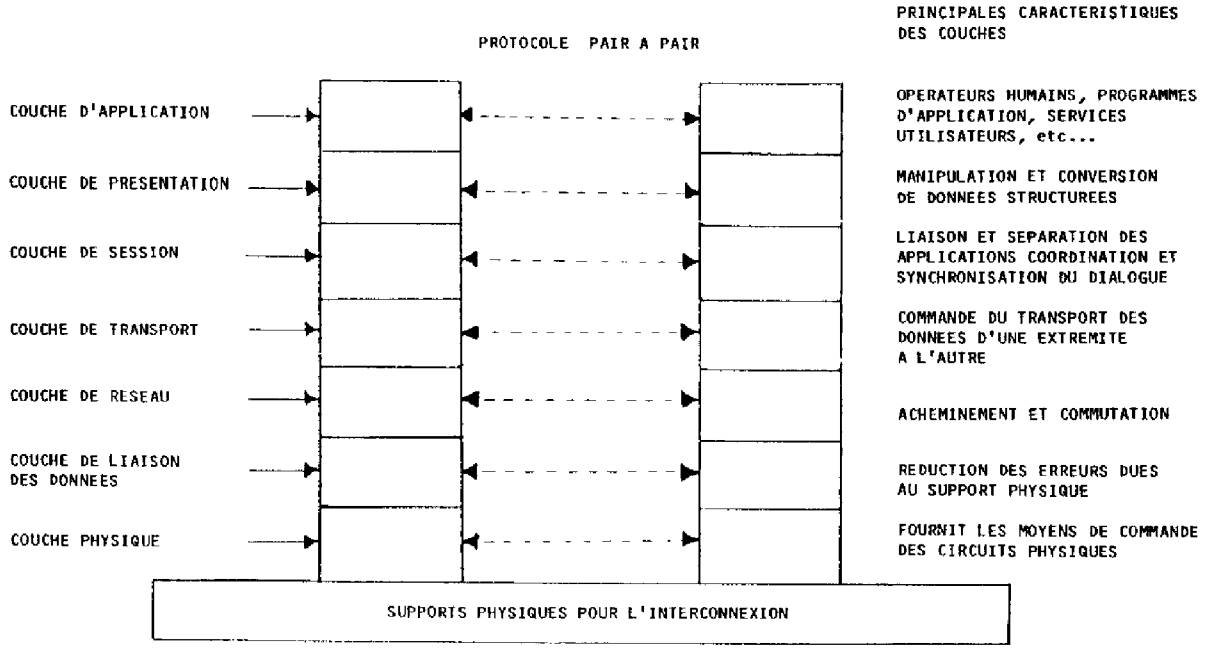


figure I.6 : modèle de référence OSI à sept couches /AFN'82/

I.2.1.3 Système de communication du poste

Ce système se caractérise, par rapport aux projets de réalisation ou de normalisation de réseaux locaux, par un nombre relativement faible d'abonnés - appelés ici **stations**- (quelques dizaines), des messages courts, mais surtout le besoin d'un temps d'accès très faible, et garanti (de l'ordre d'une milliseconde), à rapprocher d'une valeur de 10 à 30 ms pour PROWAY, et des temps non bornés des techniques de type ETHERNET.

Cette application se place donc dans un domaine non couvert par les projets actuels, caractérisé en particulier par le besoin d'un temps d'accès plus faible d'un ordre de grandeur au moins, et garanti. La prise en compte des besoins de sûreté de fonctionnement (qui seront vus plus en détail dans les paragraphes suivants) montre de la même façon qu'il s'agit d'un domaine spécifique, bien que son champ d'application paraisse extrèmement large : **réseaux locaux à haute sécurité et faible temps d'accès garanti.**

Conformément aux conclusions du paragraphe I.2.1.1, nous effectuerons donc une étude spécifique, mais en tenant compte des avantages apportés par le respect au moins partiel de certaines règles ou normes.

En particulier, nous adopterons le principe de la structure en couches du modèle OSI. Remarquons qu'en toute rigueur, il n'est pas nécessaire que le système de communication qui fait l'objet de la présente étude soit "ouvert". Une telle approche permet cependant non seulement de profiter au mieux d'une structure modulaire pour utiliser des composants standards, mais encore d'élargir le champ d'application des solutions obtenues, plus facilement adaptables à d'autres situations présentant des caractéristiques analogues.

Ce modèle n'est toutefois pas parfaitement adapté aux réseaux locaux, pour lesquels il est préférable de se limiter à une hiérarchie plus restreinte que les sept couches proposées /POW'81/.

En particulier dans ce cas, il n'y aura pas à considérer de protocoles de haut niveau, faisant intervenir des dialogues complexes entre abonnés. En effet, les spécifications concernent l'acheminement simple de messages, ce que l'on désigne par "envoi de **datagrammes**", par opposition à "l'établissement de **circuits virtuels**" /DAV'81/.

En fait, c'est le système de protection qui n'utilise que des datagrammes ; il n'en va pas nécessairement de même pour le système de commande et ses messages de service, mais ces éventuelles fonctions seront implantées à des niveaux supérieurs (couche "utilisateur"), en dehors du système de communication étudié ici.

Nous nous limitons donc à une hiérarchie restreinte, assimilant en une seule couche **Utilisateur** les couches 4, 5, 6, et 7 du modèle OSI ; cette couche correspond en fait aux abonnés qui utilisent le **support de communication** pour échanger des **messages** (porteurs d'**informations**). La figure I.7 indique la terminologie que nous pouvons associer à cette hiérarchie. Nous distinguerons dans le support de communication :

- la couche **transfert**, où les messages sont mis sous forme de **paquets**, et
- la couche **transmission**, où les paquets sont acheminés sous forme de **signaux** sur le **support de transmission** (liaison physique).

Il n'y a pas lieu de faire une distinction terminologique au sein de la couche transfert, entre les entités correspondant aux couches 2 et 3 du modèle OSI ; en effet dans les réseaux locaux, et en particulier ici, les fonctions relatives à la couche 3 (réseau : routage, commutation) sont réduites au minimum, voire inexistantes (nous nous y efforcerons d'ailleurs ici, pour rendre l'acheminement plus sûr et plus rapide).

I.2.2 Sûreté de fonctionnement

La sûreté de fonctionnement d'un système est la **crédibilité du service** qu'il fournit, c'est à dire la **qualité** de ce service permettant aux utilisateurs de lui accorder une **confiance justifiée** /CAR'82/.

I.2.2.1 Notions de base

Ce paragraphe sur les concepts de base de la sûreté de fonctionnement s'appuie sur les réflexions menées depuis plusieurs années dans l'équipe "Conception et Validation de systèmes informatiques sûrs de fonctionnement" du LAAS /LAP'79,LAP'82a/.

On convient d'appeler **défaillance** du système, l'événement caractérisé par la déviation du service effectivement fourni, par rapport au service requis.

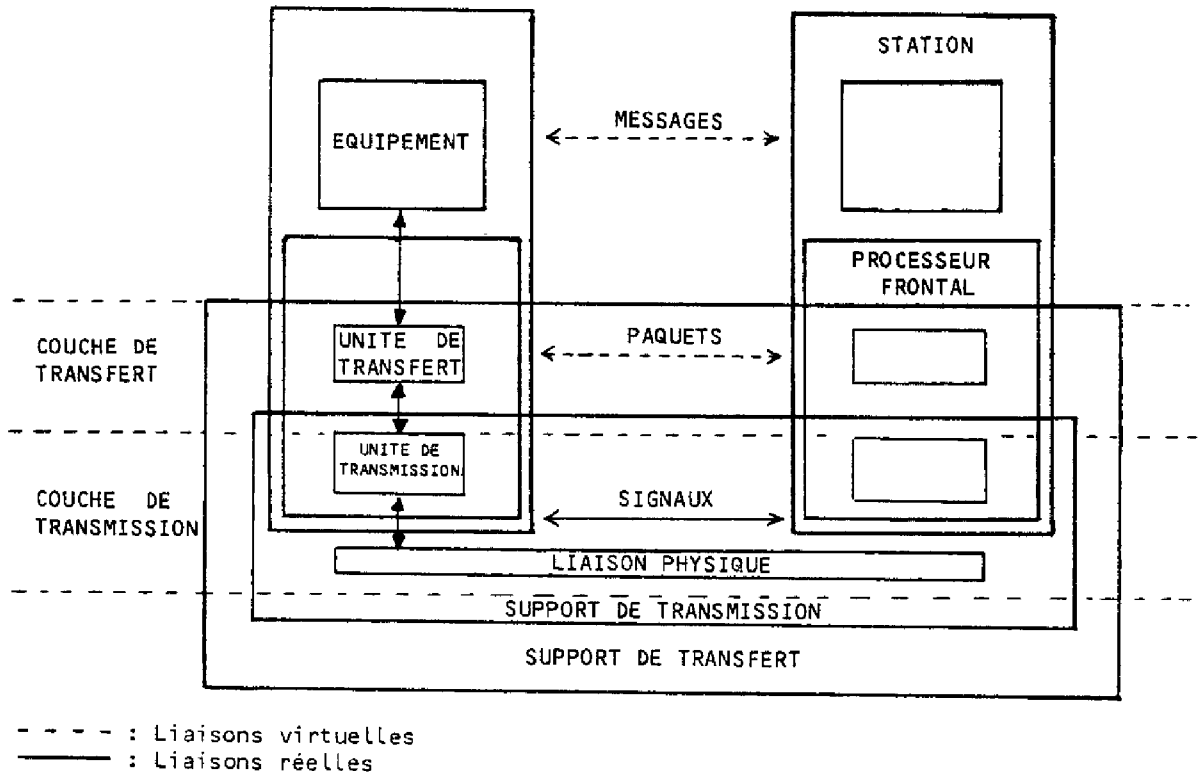


figure I.7 : hiérarchie restreinte ; terminologie

Le comportement du système est alors erroné : une **erreur** est la partie de l'état d'un système qui est différente de ce qu'elle devrait être pour qu'il soit à même de fournir le service requis.

La cause d'une erreur est une **faute**, physique ou humaine. Lorsqu'une faute survient, une erreur **latente** est créée, qui devient **effective** lorsqu'elle est activée. Une défaillance est donc l'événement constitué par le changement d'état de l'erreur, de latente à effective ; dit en termes équivalents, une défaillance est la **manifestation** d'une erreur.

La réalisation d'un système informatique sûr de fonctionnement passe par l'utilisation combinée de méthodes qui peuvent être classées en :

- **obtention** de la sûreté de fonctionnement : comment spécifier, concevoir, réaliser, et fournir les règles d'utilisation de manière à :
  + minimiser par construction l'occurrence de fautes : **évitement des fautes**,
  + assurer la continuité du service fourni malgré la présence d'erreur(s) effective(s) : **tolérance aux fautes**,
- **validation** de la sûreté de fonctionnement : comment acquérir la confiance dans la capacité du système à fournir le service requis :
  + en minimisant la présence d'erreurs latentes : **vérification**,
  + en prévoyant les conséquences des erreurs sur le service fourni : **évaluation**.

Il importe donc de préciser la nature des fautes qui peuvent affecter le système. Remarquons d'abord que toute faute peut être considérée comme humaine, en ce sens qu'elle résulte d'une incapacité à maîtriser la complexité des phénomènes qui gouvernent le comportement (y compris les interactions avec l'environnement) d'un système. L'usage consiste cependant à distinguer les fautes physiques et les fautes humaines :

- **fautes physiques** : phénomènes physiques adverses, qui peuvent être :
  + **internes** au système (désordres physico-chimiques),
  + **externes** au système (perturbations de l'environnement),
- **fautes humaines** : imperfections d'origine humaine, qui peuvent être :
  + des fautes de **conception** :
    * soit commises sur le système lui-même durant sa conception initiale (au sens large : des spécifications à la réalisation) ou durant des modifications ultérieures,
    * soit conduisant à des procédures d'interaction homme-machine ou de maintenance incorrectes,
  + des fautes d'**interaction** : violations des procédures, par inadvertance ou délibérément :
    * par des opérateurs,
    * par des équipes de maintenance, chargées d'améliorer, conserver, ou restituer le potentiel du système.

I.2.2.2 Cas d'un système de protection

Notre objectif est de concevoir un système de communication devant s'intégrer dans un **système de protection**, c'est à dire un système de surveillance et sécurité. La mission d'un tel système consiste à /MED'80/ :

- détecter les défaillances du **système surveillé**,
- intervenir pour éviter d'éventuelles conséquences catastrophiques des défaillances sur le système surveillé, et sur son environnement,
- ne pas intervenir en l'absence de défaillance du système surveillé.

La particularité d'un tel système, par rapport à la terminologie introduite dans le paragraphe précédent, est qu'il faut distinguer les défaillances du système surveillé de celles du système de sécurité lui-même. Les premières sont les événements "attendus" par le système de protection, pour le traitement desquels il est conçu.

Les défaillances du système de protection sont au contraire les événements tendant à l'empêcher d'accomplir sa mission. Ce sont donc ces dernières qui feront l'objet de l'étude de sûreté de fonctionnement, et le terme "défaillance" leur sera réservé.

Nous appelerons alors **défauts** les défaillances du système surveillé, conformément à la terminologie d'EDF, et d'**élimination de défaut** pour désigner la mission du système de protection.

Remarque : il n'y a pas à proprement parler, sauf dans le cas d'un défaut fugitif disparu après réenclenchement, d'élimination, ni de la **cause** du défaut (la "faute" : par exemple un court-circuit sur une ligne), ni de tous ses

effets : "l'erreur" initiale, matérialisée par une impédance anormale, est redevenue "latente", dans la mesure où cette impédance n'est plus mesurable (les tensions et les courants sont nuls). Mais d'autres effets sont apparus lors de la mise hors service de la partie en défaut : il y a effectivement restauration du système opérationnel, mais avec un potentiel dégradé. Le recouvrement du potentiel nominal nécessite d'autres actions correctrices, qui ne relèvent pas de la mission du système de protection, mais qui seules effectueront au sens strict "l'élimination du défaut".

I.3 CONCLUSION

Ce chapitre a permis de définir l'objet de l'étude présentée dans ce mémoire. Par une analyse descendante des besoins et des choix de principe, nous avons mis en évidence les spécifications du système à concevoir.

Il s'agit donc d'un réseau local sûr de fonctionnement, dans un domaine non couvert par les solutions existantes, ni même par les projets de réseaux locaux normalisés.

En continuité avec les travaux de l'équipe "Conception et Validation de systèmes informatiques sûrs de fonctionnement", nous appliquerons une **méthode rigoureuse de conception**, dans le but :

- d'**éviter** autant que possible les fautes de conception,
- de **valider** les solutions ainsi conçues,

sachant que ces solutions sont conçues de manière à **tolérer les fautes** (physiques, mais aussi de conception) qui pourraient les affecter.

En résumé, la conception d'un système sûr de fonctionnement nécessite :

- l'adjonction aux spécifications fonctionnelles "de base", de spécifications relatives à la sûreté de fonctionnement,
- l'utilisation de méthodes permettant, bien sûr de respecter ces spécifications, mais surtout de minimiser le nombre de fautes de conception (évitement) et d'acquérir confiance dans les résultats (validation).

Naturellement, il suffit en fait de se fixer comme objectif le respect des spécifications ; le deuxième point mentionné ci-dessus ne vise donc qu'à préciser les moyens à mettre en œuvre pour atteindre cet objectif.

Ces particularités de la conception d'un système sûr de fonctionnement entraînent les deux remarques suivantes :

(1) : l'accent nous paraît devoir être mis sur la méthode de conception, et en particulier sur l'intégration tout au long de cette méthode, de techniques de validation des choix ; ceci, sans exclure la nécessité de valider globalement la solution définitive, facilite cette validation.

(2) : notre conviction est que ces principes ne devraient pas être réservés à quelques systèmes devant satisfaire des contraintes particulières de sûreté de fonctionnement, ou plutôt qu'une proportion beaucoup plus élevée de systèmes devrait se voir imposer des spécifications de sûreté de fonctionnement.

CHAPITRE II : METHODE DE CONCEPTION

Ce chapitre est consacré à la méthode applicable à la conception du système décrit au chapitre I. Après une étude générale du principe de conception par décomposition, nous examinons comment une telle méthode peut s'exprimer dans le cas de l'application considérée.

II.1 PRESENTATION DE LA METHODE

Nous nous intéressons ici au principe d'étude des systèmes complexes par décomposition, à ses buts, à ses principales limitations et aux solutions qu'on peut apporter à ces dernières.

II.1.1 Décomposition d'un système

L'étude et la conception d'un système complexe nécessitent sa décomposition en sous-ensembles plus simples. L'efficacité d'une telle approche est basée sur l'hypothèse que l'expression, dans chaque sous-ensemble, des paramètres caractérisant le système, et de leurs liens avec les spécifications, est plus simple que celle obtenue sans décomposition.

Or un système complexe peut se caractériser par le fait qu'il n'est pas réductible à une réunion d'éléments simples indépendants. Toute décomposition doit donc faire apparaître, non seulement les sous-ensembles, mais encore les **interactions** entre les différents sous-ensembles. Ceci montre qu'une décomposition n'aboutira à une simplification que si les interactions peuvent être exprimées simplement.

II.1.1.1 Méthode par affinements

La notion de décomposition en sous ensembles est liée à l'idée de **hiérarchie**, c'est à dire à l'existence d'une **relation d'ordre**. Il est habituel de parler, pour une décomposition, de **niveaux de détail**, ce qui correspond à la relation "est composé de", ou dans l'autre sens, "fait partie de". On peut donc considérer des niveaux successifs en faisant abstraction, à chaque niveau, des éléments non cohérents avec le niveau de détail considéré.

Dans une telle décomposition, la simplification est alors obtenue par le maintien de la cohérence dans chaque niveau, ce qui permet de ne considérer que les interactions entre les sous-ensembles appartenant au même niveau, en faisant abstraction de celles avec les sous-ensembles des niveaux inférieurs.

II.1.1.2 Limites de la méthode

D'après ce qui précède, il est possible de déceler les limitations d'une étude basée uniquement sur des décompositions successives. On remarque en effet que cela consiste à faire abstraction des sous-ensembles des niveaux inférieurs (plus détaillés), et de leurs interactions avec ceux du niveau considéré. Or dans la pratique ceci conduit inévitablement -et c'est précisément là, la source des simplifications- à effectuer des choix de conception à

chaque niveau en ne prenant en compte l'impact de ces choix qu'au même niveau, c'est à dire de façon globale par rapport à l'ensemble du système.

On ne peut donc pas exclure, lorsque les choix ont été effectués à un niveau donné, la découverte d'une impossibilité après passage au niveau inférieur, cette impossibilité étant révélée par la prise en compte d'une quantité supplémentaire de détails.

II.1.1.3 Rebouclage

La méthode de **conception par affinements successifs** nécessite donc la **mémorisation des choix** effectués à chaque niveau, de façon à pouvoir éventuellement revenir sur ces choix à la lumière de leur impact réel découvert lors de l'étude sur les niveaux inférieurs /BEO'77/. Une solution pourrait consister après l'étude à chaque niveau, à réinjecter dans les niveaux supérieurs (et donc déjà étudiés) l'impact des choix qui y ont été effectués, afin de vérifier si ces choix restent corrects. Il est cependant clair qu'il faut trouver un meilleur compromis, en limitant la complexité des interactions que l'on veut considérer.

Dans la pratique, pour une méthode de conception descendante par affinements successifs, on pourra faire l'hypothèse que, si la décomposition en niveaux de détails successifs est correcte, l'impact des choix effectués à un niveau donné est également "descendant". Ces choix ne peuvent alors pas remettre en cause la validité des choix antérieurs, mais ils réduisent l'éventail des choix ultérieurs, éventuellement jusqu'à impliquer une incompatibilité.

Sous cette hypothèse, la méthode apparaît comme correcte, puisqu'il est alors justifié d'effectuer des choix de plus en plus détaillés en ne revenant sur ces choix que lorsqu'ils mènent à une impasse.

Remarque : une telle méthode permet, sous réserve que :

(1) : l'ensemble des niveaux considérés constitue une description complète du système et de ses spécifications, et que

(2) : les arguments sur lesquels sont basés les choix à chaque niveau sont corrects,

de trouver une solution correcte lorsqu'il en existe, mais ne permet pas de garantir que la solution trouvée est optimale. On admet en effet que des choix peuvent contenir des contradictions, soit internes, soit avec des choix antérieurs, non décelables au niveau considéré ; on doit bien admettre a fortiori que certains choix apparaissant comme optimaux au niveau considéré peuvent avoir des implications aux niveaux suivants remettant en cause, non pas la validité du choix, mais son caractère optimal.

II.1.2 Notion de point de vue

Une autre limitation de la méthode de conception par affinements apparaît du fait qu'il n'est généralement pas possible de décrire entièrement un système en n'utilisant qu'une décomposition en niveaux de détail successifs. A titre d'exemple, on voit qu'il n'est pas possible de passer de la description

du logiciel utilitaire d'un système à celle de sa structure matérielle sans faire appel à un mécanisme de décomposition supplémentaire ; ce mécanisme consiste en un **changement de point de vue**, et non en un accroissement du "pouvoir de résolution de l'observateur". Pour s'en convaincre, il suffit de remarquer par exemple que l'alimentation électrique -élément fondamental apparaissant à partir d'un certain niveau de détail dans la description matérielle d'un système informatique- n'a de "correspondant" à aucun niveau de détail de la description logicielle de ce même système.

Il est donc nécessaire de compléter la notion de **niveau de détail** par la notion de **point de vue**. L'étude d'un système complexe se fait alors par sélection d'un certain nombre de points de vue permettant d'isoler, non pas une partie mais un **aspect** du système. Celui-ci peut à son tour être étudié par décomposition en niveaux de détail de plus en plus fins ou, si le besoin s'en fait de nouveau sentir, par décomposition selon des points de vue distincts.

En résumé, la procédure de conception consiste à affiner de plus en plus la description du système, dans un certain nombre de points de vue représentatifs. Précisons que l'on ne procède pas par succession de niveaux de détail, qui seraient communs à tous les points de vue. Il s'agit en fait de succession d'**étapes d'affinement**, pour chacune desquelles il faut considérer chaque point de vue jusqu'à un certain niveau de détail.

Les points de vue apparaissent ainsi comme des directions privilégiées d'observation du système, permettant d'en obtenir une description plus simple (mais non complète), qui peut être considérée comme un autre système. Les niveaux de détail fournissent par contre une description plus ou moins grossière (d'où la simplification, qui n'est alors pas due à l'aspect incomplet de la description) du **même** système.

II.1.2.1 Hiérarchie des points de vue

Dans une décomposition selon des points de vue, une hiérarchie apparaît souvent, induite par une relation d'ordre qui pourrait s'exprimer par "fait appel à", ou "utilise le service de". (Nous désignerons de tels points de vue par le terme de "**couches**", pour traduire cette idée).

A titre d'exemple, un système informatique pourrait se décomposer selon le schéma :

Logiciel d'application —> Logiciel d'exploitation —> Matériel

Les entités qui composent chaque couche apparaissent comme des **machines abstraites** depuis les couches "inférieures". Ainsi, dans une décomposition classique de la couche "Matériel", un système pourra être décrit en termes de registres, de bascules, de portes, de transistors. Une bascule par exemple n'est pas simplement un assemblage de transistors, résistances, etc... mais une vue abstraite d'un tel assemblage, le munissant de significations nouvelles (en l'occurrence, la notion de mémorisation de valeur logique).

Toutefois cette hiérarchie, quand elle existe, n'offre pas les mêmes avantages que celle liée aux niveaux de détail. En effet, il n'est pas

possible d'affirmer que des choix effectués dans une couche particulière n'ont pas d'impact sur les choix déjà effectués dans d'autres couches apparaissant pourtant comme dominantes selon la relation "fait appel à".

Ceci provient du fait que chaque couche peut être décomposée selon des niveaux de détail successifs. En conséquence, il n'est pas incompatible avec l'hypothèse de "l'impact descendant" que des choix effectués dans une couche aient des conséquences dans d'autres couches, même dominantes ; en effet, ces choix n'ont certes des conséquences que dans les niveaux de détail inférieurs, mais éventuellement dans **toutes les couches.**

En conséquence, dans une décomposition en points de vue (structurés en couches ou non), la méthode de conception par affinements successifs peut s'appliquer au sein de chaque point de vue, décomposé en niveaux de détail successifs, mais à condition, après chaque affinement, de balayer l'ensemble des points de vue aux niveaux de détail nécessaires, pour :

- y examiner l'impact des choix effectués, afin de déceler les incompatibilités le plus tôt possible, avant d'affiner davantage, et
- y effectuer les choix adéquats ; en effet un choix trop tardif pourra avoir des implications dans d'autres points de vue éventuellement déjà plus affinés, et remettre ainsi en cause des choix antérieurs (qui n'auraient pas dû être antérieurs).

Remarque : Cette notion de couche est très générale. Elle se rattache par exemple aux notions de **services** et **couches** dans les protocoles de communication /AFN'82/, de **mécanisme** dans SADT /RIC'78/, et à la notion "d'**interface interprétante**" introduite par Anderson et Lee /AND'81/.

II.1.2.2 Ordonnancement des points de vue

L'ordonnancement entre les différents points de vue ne suit pas les mêmes règles que celui des niveaux de détail. En fait, il n'y a pas de règle générale permettant de fixer l'ordre de prise en compte des points de vue, pas plus qu'il n'y en a pour la prise en compte des différents éléments composant le système à un niveau de détail donné pour un point de vue donné. Cet ordre, qui pourra d'ailleurs varier avec les affinements successifs, dépendra essentiellement de la façon dont s'expriment, au niveau de détail correspondant à l'affinement considéré, les spécifications et contraintes à satisfaire.

En particulier, il est préférable d'examiner d'abord les éléments sur lesquels s'exercent les plus fortes contraintes, conduisant aux choix qui ont les conséquences les plus importantes. En fait, le processus d'affinement est souvent complexe et se décompose en "touches multiples" appliquées successivement à tous les éléments de tous les points de vue, avec de fréquents retours, au sein de la même étape d'affinement. On se ramène alors pratiquement à un processus "en parallèle" et continu, où l'ordre n'a plus de signification.

On peut toutefois retenir que dans le cas de points de vue structurés en couches, il est généralement utile, sinon nécessaire, d'avoir une connaissance

déjà un peu plus approfondie des points de vue correspondant à des **services utilisés** par celui que l'on considère. Naturellement, ceci ne permet pas d'éviter l'obligation éventuelle de revenir sur les choix dans une couche à cause de leurs implications dans les autres couches, mais seulement de simplifier la conception. Pour donner un exemple schématique, il est souvent plus facile de concevoir un logiciel lorsque l'on connaît le matériel sur lequel il doit s'exécuter, que de faire la démarche inverse ; mais on peut être amené à revoir le matériel en fonction de l'étude du logiciel, comme on le serait, dans le cas de cette démarche inverse, à revoir le logiciel en fonction de l'étude du matériel.

II.1.3 Notion de critère

Chaque étape du processus de conception est constituée de choix, permettant l'élaboration progressive d'une solution satisfaisant les spécifications. Il faut donc disposer de **critères** permettant de guider les choix de conception vers une telle solution.

Le "respect des spécifications" ne constitue généralement pas directement un critère satisfaisant, car le plus souvent, il ne peut être évalué qu'à la fin du processus de conception. Il faut donc déterminer des critères pouvant synthétiser les propriétés caractéristiques du système dans un point de vue et à un niveau de détail donnés, en y fournissant :

- une "solution idéale de référence" (généralement fictive),
- les moyens de mesurer (quantitativement et qualitativement), l'écart entre les solutions envisageables et cette référence.

II.1.3.1 choix des critères

Le choix des critères est une phase fondamentale du processus de conception car c'est sur ces critères que l'on se base pour affiner les solutions, qui ne pourront être réellement validées qu'une fois entièrement définies.

Les critères "de base", issus directement des spécifications, font appel généralement à la connaissance de beaucoup trop de paramètres. Certains ne peuvent être connus qu'après définition des niveaux de détail les plus fins, ce qui ôte tout intérêt au critère comme guide de conception. D'autres paramètres ne peuvent pas être connus, sinon éventuellement par étude statistique sur la solution opérationnelle (probabilités de défaillance des équipements, temps de réparation, taux de couverture des mécanismes de tolérance aux fautes, etc...).

La solution consiste alors généralement à choisir des critères faisant intervenir moins de paramètres non connus. On peut pour cela adopter les deux techniques suivantes :

(1) Faire des hypothèses sur la valeur de certains paramètres, ou sur leur nature (par exemple, supposer que tel phénomène suit une loi de distribution donnée, ce qui revient à substituer à un "paramètre aléatoire" un petit nombre de paramètres suffisant à le caractériser : moyenne, écart-type, etc...).

Il peut cependant rester un certain nombre de paramètres non connus ; les critères restent alors utilisables (car on ne s'en sert pas comme mesure absolue, mais comme base de comparaison) :

- soit lorsque l'on peut faire l'hypothèse que l'**influence** de la valeur, ou de la loi de distribution des paramètres est la même pour les différentes solutions en concurrence,
- soit en effectuant une étude de sensibilité destinée à établir comment varient les critères -et donc les choix qu'ils induisent- lorsque l'on fait balayer aux paramètres non connus un domaine représentatif de valeurs ; on peut alors obtenir un ensemble de solutions, chacune correspondant à un domaine particulier de valeurs des paramètres ; toutefois, ceci n'est valable que s'il est possible d'isoler un **petit nombre** de paramètres inconnus, **indépendants** entre eux, et de **connaître leurs domaines** de valeurs possibles.

(2) Définir plusieurs critères, chacun ne faisant intervenir que certains des paramètres. Cette démarche relève en fait du même processus que la décomposition en points de vue : le choix d'un point de vue conduit à rechercher des critères adaptés à ce point de vue, permettant d'y effectuer des choix internes ; de la même façon, le choix d'un "critère partiel" revient à définir un point de vue particulier, permettant d'isoler l'effet de certains paramètres.

II.1.3.2 Critères et points de vue

Les critères que l'on définit ne sont pas indépendants des points de vue retenus, et en particulier certains critères peuvent ne pas avoir de signification dans tous les points de vue. Or, il arrive que certains critères présentent des antagonismes entre eux ; ceci résulte, soit de la décomposition d'une spécification complexe, soit de la coexistence de spécifications elles-mêmes antagonistes.

Lorsque des critères correspondant à des points de vue distincts présentent un tel antagonisme, l'efficacité de la méthode de conception risque d'en être considérablement réduite. En effet, il est alors à peu près certain que le processus d'affinement conduira, à chaque étape, à des conflits entre les différentes possibilités induites par la prise en compte de chaque critère dans chaque point de vue.

Pour améliorer cette efficacité, il faut essayer de résoudre ces conflits à l'intérieur d'un point de vue, plutôt que de mener, pour une étape donnée, l'affinement séparément dans les différents points de vue, et devoir résoudre ensuite les conflits apparus lors de la synthèse des résultats de l'étape. Pour cela, il est nécessaire, non seulement de rechercher un ensemble de critères représentatif de toutes les spécifications, mais encore d'effectuer une première analyse de ces critères, de façon à mettre en évidence leurs interactions. Ceci permet en particulier, par "projection" dans chaque point de vue des critères antagonistes liés plus spécifiquement à un autre point de vue, de ramener et résoudre les conflits à l'intérieur des points de vue.

Nous verrons dans le paragraphe II.2 consacré à l'application un exemple d'un tel antagonisme, entre les performances fonctionnelles du système et sa sûreté de fonctionnement. Ceci permettra de concrétiser cette notion, et la façon de mener la première analyse des critères de base.

II.1.4 Conclusion

L'analyse des paragraphes précédents montre que le processus de conception doit débuter par une "étape d'ordre zéro", destinée à traduire les spécifications en critères adaptés à chacun des points de vue et niveaux de détail retenus, sans négliger l'expression des antagonismes, et plus généralement des interactions, entre ces critères.

La notion de critère est donc essentielle dans la mesure où elle permet de matérialiser les interactions entre les différentes entités de décomposition du système : les points de vue et les niveaux de détail. Un choix judicieux de ces critères permettra donc de ramener au sein des entités de décomposition les contraintes induites par les spécifications sur les autres entités. Ceci facilite le processus de conception, en fournissant les moyens :

- d'orienter correctement les choix dès les premiers affinements (détermination de critères servant de guides de conception vers une solution satisfaisant les spécifications globales),
- de réduire le nombre d'itérations entre points de vue (détermination dans chaque point de vue, de critères prenant en compte les critères antagonistes liés aux autres points de vue).

Une fois les critères et points de vue définis, le processus de conception proprement dit peut être effectué, par affinements successifs, à partir d'une description grossière de base jusqu'à une ou plusieurs solutions, définie(s) jusqu'au niveau de détail souhaité. Chaque étape du processus consiste à affiner la conception dans les différents points de vue en fonction des critères retenus, déceler et résoudre les éventuels conflits internes à cette étape, et, en cas d'incompatibilité, revenir sur les choix de conception effectués lors des étapes précédentes.

II.2 APPLICATION

Dans ce paragraphe, nous appliquons au système de communication du poste THT les principes de conception étudiés au paragraphe II.1. Nous cherchons donc à déterminer un ensemble de points de vue représentatifs de ce système, ainsi que les critères susceptibles de conduire à une solution répondant aux spécifications détaillées au paragraphe I.1.4.

II.2.1 Choix des points de vue

D'après l'étude du paragraphe II.1, on peut distinguer deux catégories de points de vue, correspondant à deux démarches de décomposition différentes.

II.2.1.1 Types de points de vue

La première démarche, que l'on pourrait qualifier "d'horizontale", consiste à isoler certains aspects du système, en choisissant de l'examiner selon des points de vue déterminés : par exemple, le point de vue de l'utilisateur, du réparateur, etc...

La deuxième, démarche "verticale", consiste à introduire des couches hiérarchisées complétant la décomposition par affinements : par exemple, le logiciel d'application, le logiciel d'exploitation, etc...

C'est cette dernière qui semble la mieux adaptée pour aider à la conception d'un système, alors que la première est surtout utile pour comprendre un système existant, où les interactions ne sont pas à **découvrir** mais à **exprimer.**

II.2.1.2 Choix des couches

Nous recherchons donc une décomposition en couches du système de communication du poste. Compte tenu des résultats du paragraphe I.2 concernant le modèle OSI, la décomposition la plus naturelle et sans doute la plus efficace pour un réseau local, consiste à considérer, de façon analogue au clivage classique "logiciel-matériel" des systèmes informatiques :

- d'une part la couche de **transmission**, correspondant aux moyens physiques permettant aux stations de communiquer,
- d'autre part la couche de **transfert**, correspondant ici aux procédures permettant aux stations d'utiliser ces moyens physiques.

On pourrait être tenté de prendre en compte en tant que troisième point de vue, l'aspect **technologique** ; en effet, certaines spécifications (en particulier celles relatives à la résistance à l'environnement) ont des implications directes sur la technologie selon laquelle ce système doit être réalisé. Mais il s'agit en fait d'un point de vue induit par un type de spécification, qu'il est préférable de prendre en compte sous forme de critère particulier à l'intérieur des autres points de vue. En effet, l'aspect technologique n'est pas suffisamment dissocié des aspects liés aux couches de transfert et surtout de transmission, ce qui conduirait à de multiples itérations. Dans la mesure où pour diminuer le nombre de ces itérations, il faudrait projeter dans les points de vue transfert et transmission les implications des critères "technologiques", la prise en compte directe de ce point de vue devient peu efficace.

Il faudra donc prendre directement en compte dans les différents points de vue les spécifications influant sur la technologie, en choisissant les critères adéquats. En l'absence de telles spécifications, il ne serait pas utile d'effectuer des choix technologiques dès les premiers affinements ; on pourrait alors les retarder jusqu'à ce que les différents éléments constitutifs du système de communication soient suffisamment détaillés pour qu'il soit légitime d'étudier comment les réaliser. En effet, on ne risquerait pas dans ce cas d'aboutir à une incompatibilité due, non pas à des choix antérieurs uniquement, mais à la prise en compte à un certain niveau de détail de spécifications externes, non apparues auparavant.

II.2.2 Choix des critères

Il faut d'abord déterminer les critères de base, directement issus des spécifications du système.

II.2.2.1 Critères de base

Les spécifications essentielles concernent l'aptitude du système à acheminer une rafale de messages de défaut en moins de trois millisecondes. Cette aptitude se mesure en termes de probabilités, mais un tel critère n'est pas utilisable directement, car il fait appel à de trop nombreux paramètres, à des niveaux de détail très fins. Il faut donc chercher d'autres critères.

Pour l'application envisagée ici, une solution intéressante consiste à découpler les paramètres relatifs aux performances fonctionnelles de ceux relatifs aux défaillances. Il suffit pour cela de considérer le découpage, naturel pour un système de protection, en deux modes de fonctionnement :

- fonctionnement normal, regroupant outre l'état normal proprement dit, des états dont la probabilité n'est pas négligeable, mais pour lesquels l'acheminement d'une rafale devra pouvoir être assuré en moins de trois millisecondes,
- fonctionnement défaillant, regroupant des états où l'acheminement n'est pas garanti, mais dont on devra s'assurer que la probabilité est "suffisamment faible".

Nous retiendrons donc deux critères fondamentaux :

- **temps d'acheminement** d'une rafale en fonctionnement normal ; notons que nous ne rechercherons pas nécessairement le temps le plus court : il suffit que ce temps soit inférieur à trois millisecondes,
- **probabilité de défaillance** : nous examinerons dans le paragraphe suivant comment évaluer cette probabilité, c'est-à-dire mesurer la sûreté de fonctionnement du système.

L'examen des spécifications telles qu'elles ont été définies au paragraphe I.1.4, amène également à retenir les critères suivants :

- **débit moyen disponible pour les messages de service** : il n'y a pas pour ces messages de spécifications aussi rigoureuses que pour les messages de défaut ; ce critère apparaît toutefois comme la mesure la plus significative des performances relatives à ces messages, permettant de guider les choix entre solutions concurrentes (sans oublier qu'il ne s'agit que d'un critère secondaire).
- **flexibilité** : ce critère est destiné à mesurer la facilité de maintenance, mais surtout la facilité d'adaptation du système de communication aux modifications du poste (extensions en particulier).
- **coût** : ce critère n'est pas mentionné explicitement dans les spécifications. Il est cependant évident que la considération du coût permettra de guider les choix en vérifiant que les solutions proposées restent du même ordre de grandeur de coût, et en sélectionnant les améliorations les plus efficaces à coût comparable.

II.2.2.2 Mesures fondamentales de la sûreté de fonctionnement

La qualité du service fourni par un système comporte plusieurs aspects, ou attributs, différents. Parmi ceux-ci, citons les trois principaux :

- la **fiabilité** : aptitude du système à fournir continûment le service requis,
- la **maintenabilité** : aptitude du système à fournir de nouveau le service requis, après une défaillance,
- la **disponibilité** : aptitude du système à fournir le service requis.

L'évaluation de la sûreté de fonctionnement d'un système consiste à :

- choisir les attributs qui caractérisent le mieux le service que l'on attend de ce système, et
- déterminer des grandeurs représentatives de ces attributs pour l'application considérée.

Pour cela, on peut définir un certain nombre de grandeurs de type probabiliste /LAP'82a/. Appelons **Z** une variable discrète caractérisant le service fourni par le système. Dans un premier temps, nous pouvons considérer ce service comme indivisible : Z est alors une variable binaire dont les valeurs sont notées par commodité **f** et **i** (pour fourniture et interruption). La fourniture du service est alors l'événement probabiliste **(Z=f)**, et les grandeurs qui nous intéressent sont celles qui permettent de caractériser Z au cours du temps, par exemple entre un instant initial de référence, noté t_0, et l'instant d'observation t.

Nous pouvons ainsi définir :

- une fonction de **fiabilité**, F(t), donnant la probabilité que le système ait fonctionné sans interruption de t_0 à t :
  $F(t) = \text{Prob.}\ \{Z(x)=f \quad \forall\, x \in [t_0,t]\}$.
- une fonction de **maintenabilité**, M(t), caractérisant la durée de réparation, par exemple par la probabilité que le système, défaillant à t_0, ait été réparé avant t :
  $M(t) = \text{Prob.}\ \{\exists\, x \in]t_0,t],\ Z(x)=f \mid Z(t_0)=i\}$,
- une fonction de **disponibilité**, D(t), donnant la probabilité que le service soit fourni à t :
  $D(t) = \text{Prob.}\ \{Z(t)=f\}$.

II.2.2.3 Cas d'un système de protection

Dans le cas général, on peut enrichir les notions du paragraphe précédent en considérant plusieurs modes de fourniture ou d'interruption du service /LAP'82b/. En particulier pour un système de protection, c'est-à-dire assurant une mission de surveillance et de sécurité, on peut considérer :

- un mode de fourniture, noté f,
- deux modes d'interruption, se distinguant par les conséquences des défaillances causant l'interruption :
  - interruption **bénigne**, notée i_b,
  - interruption **maligne**, notée i_m.

Nous disposons alors de deux mesures de type "fiabilité" :

- $F(t) = \text{Prob.}\left\{Z(x)=f \quad \forall x \in [t_0,t]\right\}$,
- $S(t) = \text{Prob.}\left\{Z(x)\in\{f,i_b\} \quad \forall x \in [t_0,t]\right\}$: il s'agit alors de la **sécurité** (non-occurrence d'événement catastrophique).

La généralisation directe de la disponibilité, incluant l'événement $(Z=i_m)$ dans l'alternance fourniture-interruption, n'est pas très significative. En effet lorsqu'une défaillance catastrophique se produit, les conséquences sont généralement telles que la restauration du système n'est pas directement intéressante : d'une part elle peut passer au second plan par rapport à la réparation (au sens large, y compris juridique) des conséquences de la catastrophe, et d'autre part la durée très longue avant d'obtenir l'autorisation de sa remise en service (commissions d'enquête,..) conduirait à des valeurs numériques non significatives.

Par contre, une mesure hybride fiabilité-disponibilité est plus intéressante. Il s'agit d'une mesure de la fourniture du service par rapport à l'alternance fourniture-interruption bénigne, avant qu'une défaillance catastrophique ne se produise ; on peut donc la qualifier de **"disponibilité avant événement catastrophique"**.

II.2.2.4 Application

Rappelons que, comme indiqué au paragraphe I.1.4.3, nous cherchons ici à évaluer la contribution du support de communication du système de protection du poste, à la sûreté de fonctionnement du système surveillé.

Or en l'absence de toute communication entre les équipements du poste THT, un défaut sur le réseau peut quand même être éliminé, car les équipements qui le détectent ouvrent leur disjoncteur s'ils ne reçoivent pas d'ordre de verrouillage. Il n'y a donc pas de raison d'arrêter un équipement lorsque son processeur frontal est défaillant, ni le poste lorsque le support de communication est défaillant. Autrement dit, les défaillances du support de communication n'entraînent pas l'arrêt du système surveillé, ce qui ôte de son intérêt, pour cette application, à la mesure hybride définie précédemment.

Par contre, nous voyons que le système de communication sert à optimiser le processus d'élimination de défaut, c'est-à-dire que ses défaillances se traduisent par une **élimination dégradée**, caractérisée par l'ouverture de certains disjoncteurs supplémentaires. Le critère le plus pertinent pour mesurer l'accomplissement de la mission du support de communication apparaît donc comme un ensemble de mesures de type fiabilité pour un système comportant plusieurs modes d'interruption, chacun correspondant à un niveau de dégradation de la mission. Ceux-ci sont caractérisés par, en cas de défaut sur le réseau :

i_1 : l'ouverture d'un disjoncteur supplémentaire,

i_2 : l'ouverture de deux disjoncteurs supplémentaires,

etc...

Remarque : D'après les paragraphes I.1.2.1 et I.2.2.2, il faut également tenir compte des défaillances du système de protection entraînant l'ouverture de

disjoncteurs supplémentaires en l'absence de défaut . En ce qui concerne le support de communication, on voit que ce point n'intervient pas, puisque ses défaillances n'entraînent que la perte d'informations de **verrouillage.** L'ouverture d'un disjoncteur en l'absence de défaut ne peut donc être due qu'à une défaillance de son équipement ou du système de commande du poste, mais pas du support de communication.

II.2.3 Analyse des critères

Ce paragraphe est destiné à analyser les critères de base qui ont été définis, afin de déterminer les critères qui seront effectivement utilisés à chaque phase de la conception (points de vue et niveaux de détail).

Les critères secondaires : coût et flexibilité , peuvent être pris en compte à différents niveaux de détail, et dans tous les points de vue. Mais il faut analyser plus finement les critères essentiels : performances fonctionnelles pour messages de défaut, et sûreté de fonctionnement. En effet, ces critères restent trop complexes pour être pris en compte dès les premiers niveaux de détail, et ils recouvrent l'ensemble des points de vue ; de plus, l'expérience montre que la sûreté de fonctionnement et les performances fonctionnelles sont souvent antagonistes. Nous nous trouvons donc dans le cas où il faut, conformément à l'étude du paragraphe II.1.3 :

- rechercher des critères utilisables dès les premiers affinements,
- rechercher les "projections" des critères dans chaque point de vue,
- exprimer les interactions (en particulier les antagonismes) entre ces "projections", pour les prendre en compte à l'intérieur même des points de vue.

II.2.3.1 Performances fonctionnelles

La prise en compte du critère fonctionnel à haut niveau pourra se faire assez simplement, en considérant qualitativement :

- dans la couche de transmission : les possibilités de liaisons offertes par l'architecture du support de communication,
- dans la couche de transfert : la complexité des procédures de communication.

Pour les affinements suivants, on pourra utiliser des évaluations approchées des temps d'acheminement (de plus en plus précises). On peut cependant remarquer que de telles évaluations seront plus efficaces dans la couche de transfert que dans celle de transmission. Ceci est dû au fait que les paramètres de transmission intervenant dans ces évaluations semblent a priori moins nombreux et plus faciles à synthétiser que les paramètres de transfert. En conséquence, sauf peut-être pour les derniers affinements, nous nous limiterons dans la couche de transmission à la prise en compte des critères plus qualitatifs définis au début de ce paragraphe II.2.3.1.

Il faut toutefois noter que les critères retenus pour les premiers affinements dans chaque point de vue sont partiellement antagonistes. En effet, une architecture très "riche" en possibilités de liaisons obligera (généralement) à recourir à des procédures complexes pour exploiter cette richesse. Pour le premier affinement au moins nous commencerons par le point de vue "transmission", conformément aux résultats du paragraphe II.1.2.3. Il faudra donc évaluer dans ce point de vue l'incidence de chaque architecture sur les performances fonctionnelles des procédures qui pourront gérer la communication sur cette architecture.

II.2.3.2 Sûreté de fonctionnement

De la même façon qu'au paragraphe précédent, le critère de base retenu pour évaluer la sûreté de fonctionnement du système est difficilement utilisable pour les premiers affinements, ce qui conduit à rechercher des critères adaptés à ces premiers affinements, dans les deux couches.

Il faut donc essayer de synthétiser les paramètres de transmission pour les prendre en compte à haut niveau de détail dans des critères de sûreté de fonctionnement applicables à la couche de transfert, et réciproquement. Il apparaît toutefois que contrairement au cas des performances fonctionnelles, ce sont les paramètres de transfert qui seront les plus faciles à synthétiser.

Il faut cependant noter qu'il s'agit là d'une simplification. En effet, l'influence des procédures de transfert, et d'une façon plus générale du logiciel pour tout système informatique, sur la sûreté de fonctionnement du système complet est certainement très complexe, ce qui conduit à rechercher des expressions plus simples de cette influence :

- soit en négligeant les défaillances des procédures,
- soit en négligeant les conséquences de ces défaillances,
- soit en supposant que ces défaillances sont, par leurs conséquences et par leurs caractéristiques d'occurrence, assimilables à des défaillances du matériel.

Remarquons que la troisième solution, qui pourrait sembler la meilleure, suppose en outre que l'on est capable de chiffrer le logiciel en unités de "matériel-équivalent", ce qui n'est pas le cas actuellement. Nous nous efforcerons donc, dès les premières phases de la conception, de limiter autant que possible la **présence** de fautes dans les procédures, et les **conséquences** éventuelles de ces fautes, afin de rendre légitime la non-prise en compte de ces fautes dans une évaluation de sûreté de fonctionnement, possible à partir d'un certain niveau de détail.

Ces considérations nous conduisent à rechercher avec soin des critères permettant :

- d'une part de guider les choix dès les premières étapes dans les deux couches,
- d'autre part d'effectuer des choix dans la couche de transfert,

de façon à obtenir une solution finale conforme au critère de base.

Trois types d'actions concourent à améliorer la sûreté de fonctionnement du système considéré, consistant à minimiser :

- la probabilité d'**occurrence** de faute,
- la **présence** de faute non détectée lors d'un défaut à éliminer,
- les **conséquences** des fautes sur l'accomplissement de la mission.

En ce qui concerne le premier point, nous voyons que, si le même soin est apporté à la réalisation de toutes les solutions possibles, celles qui contiendront le moins de fautes de conception seront :

- les solutions les plus simples (moins de composants, matériels ou logiciels),
- les solutions pouvant bénéficier, par l'utilisation de composants (matériels et logiciels) standards, des travaux de conception et de tests des concepteurs et utilisateurs de ces composants.

De plus ces deux critères de **simplicité** et de **normalisation** permettent de minimiser le nombre de composants matériels, et donc la probabilité d'occurrence de fautes externes.

La présence de faute non détectée est liée au phénomène de **latence**, particulièrement important pour les systèmes de protection /MED'80,PIL'82/. Dans ces systèmes en effet, certaines parties matérielles et logicielles peuvent n'être que très rarement activées ; les fautes ne peuvent pas alors se manifester sous forme d'erreurs, ce qui empêche de prendre les mesures nécessaires pour y remédier avant occurrence de l'événement activant le système (défaut sur le réseau électrique, dans ce cas).

Nous retiendrons en conséquence, pour guider la conception dès le début et dans tous les points de vue vers une solution à haute sûreté de fonctionnement, le critère de **latence minimale** : nous nous efforcerons donc de réduire au minimum les parties qui ne sont actives que lors d'un défaut à traiter, c'est-à-dire les sièges éventuels d'erreurs latentes.

Le troisième point, concernant les conséquences des fautes, conduit à retenir comme critère, applicable dès les premiers affinements, et dans les deux points de vue choisis, la **décentralisation**, que nous prenons dans son sens le plus fort : "absence d'élément unique matériel ou logiciel, nécessaire au bon fonctionnement de l'ensemble". Cette notion va donc plus loin que le sens restreint de "répartition" qui lui est parfois attribué, en incluant la "non-vulnérabilité", ou robustesse (ce qui est à rapprocher de l'ensemble de propriétés que doit satisfaire un système réparti pour mériter, selon Enslow, le qualificatif de "système distribué" /ENS'78/).

II.2.4 Résumé et conclusion

Cette première analyse du système à concevoir a permis de déterminer, en accord avec le choix d'une structure compatible avec le modèle de référence

OSI, les points de vue à utiliser pour la décomposition :
- transmission,
- transfert.

Les spécifications ont conduit aux critères de base suivants :

- durée d'acheminement d'une rafale de sept messages, dans les cas normaux ou à probabilité non négligeable,
- probabilité d'ouverture de disjoncteur(s) supplémentaire(s) en cas de défaut, due au mauvais fonctionnement du support de communication,
- débit moyen disponible pour les messages de service,
- flexibilité,
- coût.

L'analyse de ces critères de base a ensuite permis de déterminer les critères à utiliser au cours du processus de conception, dans les différents points de vue et pour chaque étape d'affinement (en particulier pour les premières étapes) :
- pour favoriser dans les choix à haut niveau dans la couche de transmission, les solutions présentant de bonnes performances fonctionnelles :
  + possibilités d'interconnexion,
- pour guider les choix dans toutes les couches vers des solutions à haute sûreté de fonctionnement :
  + simplicité,
  + normalisation (utilisation de composants standards),
  + décentralisation (robustesse),
  + latence minimale.

L'antagonisme entre les possibilités de liaison offertes par un support de transmission et la simplicité des procédures de transfert permettant de le gérer, doit être résolu à chaque étape d'affinement, et en particulier dans la couche de transmission par la recherche d'un compromis entre les possibilités de liaison et la simplicité du support.

Pour conclure cette première analyse du système à concevoir, il convient de rappeler que la façon même d'aborder la conception, la sélection de la méthode et surtout des critères que l'on juge les plus représentatifs, constituent des choix de principe ; ceux-ci, pour justifiés qu'ils soient, n'en sont pas moins des "parti-pris" de conception, qui prédéterminent généralement la solution qui sera retenue à l'issue du processus de conception. En effet, le processus de conception lui-même est constitué de choix qui pour leur plus large part, découlent des choix initiaux.

Pour cette étude en particulier, le choix de la méthode ne soulève pas de difficulté en lui-même, mais les critères retenus méritent une certaine attention.

Si le "parti-pris" de simplicité et la préférence pour des solutions standards sont assez banals, il convient de remarquer que l'accroissement de sûreté de fonctionnement qui en résulte n'est généralement pas la raison essentielle qui a conduit à les adopter. Pour cette application au contraire, on a vu que c'était bien l'argument primordial.

La décentralisation est également un moyen (devenu) banal de concevoir un système sûr de fonctionnement. Précisons cependant que cela n'est pleinement justifié que lorsque ce terme inclut la notion de robustesse ; la simple répartition n'est en effet pas une condition suffisante d'obtention d'un système sûr de fonctionnement.

Le critère de latence minimale apparaît sans doute comme le choix de principe qui nous différencie le plus des systèmes classiques. Ce choix est imposé par les études générales antérieures des systèmes de sécurité et de protection, mais il est clair qu'il a des conséquences importantes sur le système, avant même tout affinement.

Pour notre application, cela se traduira en particulier par la nécessité :

- d'utiliser intensivement le support de communication en l'absence de défaut, en lui faisant acheminer des messages "de remplissage" (que nous appellerons messages de test, étant donné leur fonction), lorsqu'il n'y a pas de message de service ni bien-sûr de défaut,
- d'avoir le moins de différences possible entre le traitement des messages de défaut et celui des autres messages (de service et de test).

Remarque : Ainsi exprimé, le critère de latence fait apparaître, afin de le résoudre, l'antagonisme entre les performances fonctionnelles et la sûreté de fonctionnement, puisque :

- il devient impossible de négliger la présence de messages non urgents, qui risquent de ralentir l'acheminement des messages de défaut ;
- moins on peut privilégier le traitement d'une classe de messages, moins il est facile de leur faire satisfaire des contraintes données.

DEUXIEME PARTIE: APPLICATION

Après avoir dégagé les spécifications du support de communication pour le poste THT, et montré qu'elles n'étaient pas satisfaites par les solutions existantes, nous appliquons dans cette partie la méthode générale de conception exposée au chapitre II.

Le premier chapitre de cette partie (chapitre III) concerne les choix de base qu'il est possible d'effectuer, tant dans la couche de transmission que dans celle de transfert, à partir des critères qualitatifs définis au paragraphe II.2, à savoir essentiellement : décentralisation, latence, simplicité, flexibilité, coût, normalisation (utilisation de composants standards).

Les solutions qui se dégagent à l'issue de cette première étape sont ensuite affinées dans le chapitre IV, et une évaluation comparative de leurs performances est effectuée, en particulier par l'utilisation de processus markoviens pour modéliser et calculer leurs caractéristiques de sûreté de fonctionnement.

Le cinquième et dernier chapitre comporte une étude plus détaillée de la solution qui se dégage à l'issue de l'analyse des chapitres précédents : une double boucle contrarotative optique, avec accès asynchrone par insertion de registre. Cette étude permet de s'assurer de la faisabilité de cette solution, de sa conformité avec les spécifications de base, du maintien de la cohérence des choix et de la validité des hypothèses effectuées au cours du processus de conception.

CHAPITRE III : CHOIX DE BASE

Conformément aux résultats de la première partie, ce chapitre sera consacré aux premiers choix qu'il est possible d'effectuer, dans les couches de transmission et de transfert.

III.1 TRANSMISSION

A ce premier niveau de détail, nous analyserons, à l'aide des critères qualitatifs retenus au paragraphe II.2.3, ce point de vue "transmission" sous les deux aspects suivants :

- réalisation physique du support de transmission (aspects matériels),
- architecture du support de transmission (aspects structurels).

III.1.1 Aspects matériels

Les choix matériels au niveau de détail qui fait l'objet de ce chapitre ont une influence directe sur la probabilité d'acheminement correct des informations, ainsi que sur la flexibilité et le coût.

Pour des raisons de flexibilité et de coût, il n'est pas envisageable de transmettre les informations par "fil-à-fil" (chaque information étant alors matérialisée par l'état d'un support physique spécifique : tension électrique d'un conducteur, etc...). Pour les mêmes raisons, nous n'utiliserons pas un support physique partagé, possédant plusieurs états représentant chacun une information spécifique ("bus parallèle", logique multiniveaux, etc...).

Nous aurons donc recours à un support partagé par toutes les informations, qui seront transmises sous forme de **séquences d'états physiques** : transmission série.

La probabilité d'acheminement correct des informations dépend alors, surtout pour l'application considérée, de l'immunité du support contre les parasites électromagnétiques. La seule technologie offrant actuellement sans surcoût excessif une très bonne immunité contre ces parasites est la fibre optique. Ce domaine fait l'objet de nombreuses réalisations et études /KLE'78, ACT'79,DEG'82,RIC'83/ montrant que le coût et les performances de ce type d'équipements deviendront de plus en plus intéressants (existence de composants standards, de dérivateurs optiques passifs à faible atténuation, etc...).

Notre choix se porte donc sur l'utilisation de **fibres optiques** pour acheminer les messages sous forme de **séquences de signaux lumineux.**

III.1.2 Aspects structurels

La figure III.1 indique, à partir de la classification de /POW'81/, les structures de base qu'il est possible d'envisager a priori.

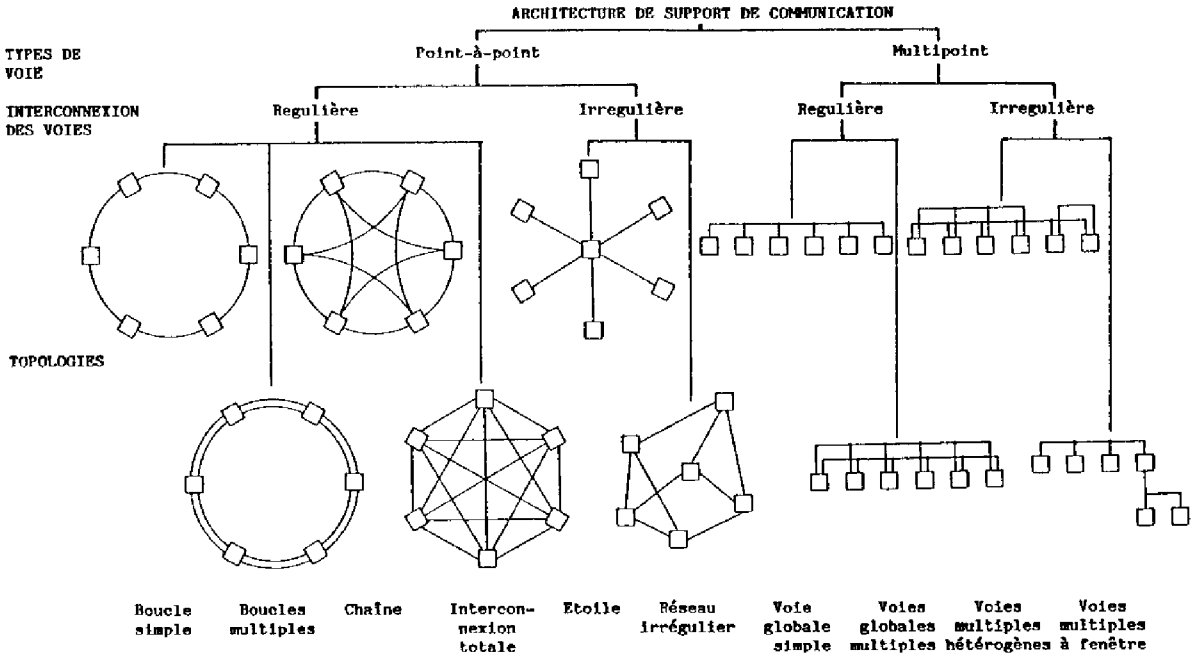


figure III.1 : Structures de base (d'après /POW'81/)

Un premier choix peut être effectué à l'aide des critères applicables à ce point de vue et ce niveau de détail : décentralisation, simplicité, coût et flexibilité.

III.1.2.1 Choix de structures

Le critère de **décentralisation** conduit à éliminer la boucle simple et l'étoile, où la défaillance d'un seul élément met hors service l'ensemble du système.

La structure en réseau totalement interconnecté ne satisfait pas les critères de **coût**, ni de **flexibilité**.

Le critère de **simplicité** conduit à rejeter les structures imposant des procédures complexes pour le routage des messages. Remarquons cependant qu'il peut y avoir découplage entre les procédures au niveau transfert, c'est-à-dire l'architecture apparente de transfert, et la structure physique assurant la transmission. Il n'y a toutefois ici aucune raison d'imposer un tel découplage, motivé généralement par la recherche d'un compromis entre une structure "complexe" (possédant des chemins multiples, par exemple) et une procédure simple.

Il est donc logique de retenir, au moins dans un premier temps, les structures les plus simples, et les mieux adaptées à la structure même du poste.

A priori, cet argument pourrait conduire à des structures où certaines stations auraient un rôle privilégié : les stations de couplage, qui

pourraient faire la jonction entre des voies locales interconnectant des stations de ligne.

Cela n'est cependant pas souhaitable, pour les raisons suivantes :

- chaque départ peut être relié à n'importe quelle barre. Il est difficile d'imaginer une structure analogue simple et décentralisée pouvant accueillir "dynamiquement" n'importe quelle station sur n'importe quelle voie locale,
- il est préférable d'adopter la structure la plus banalisée possible :
  - . pour faciliter la maintenance (modules interchangeables),
  - . pour améliorer la flexibilité : adaptation aux extensions du poste, et à ses changements éventuels de structure,
  - . pour accroître la décentralisation.

Ceci conduit donc à retenir une structure en voie globale ("bus"), simple ou multiple, ou une structure en boucle multiple, qui réduisent au minimum les fonctions de routage.

Les questions qui se posent alors sont :

- Comment s'expriment les implications des choix matériels (réalisation en fibres optiques) ?
- Quel degré de multiplicité faut-il choisir pour le bus et la boucle ?

III.1.2.2 Réalisation en fibres optiques

Par nature, les fibres optiques, associées à des éléments de conversion optique/électronique des signaux (émetteurs et récepteurs) permettent de réaliser des liaisons point-à-point monodirectionnelles /RAW'78/.

Nous pouvons donc réaliser une boucle optique selon le schéma de la figure III.2 où l'on voit que, ne pouvant pas disposer actuellement de dérivateurs passifs à faible atténuation, le signal lumineux est transformé en signal électrique dans chaque processeur frontal /MIR'81/.

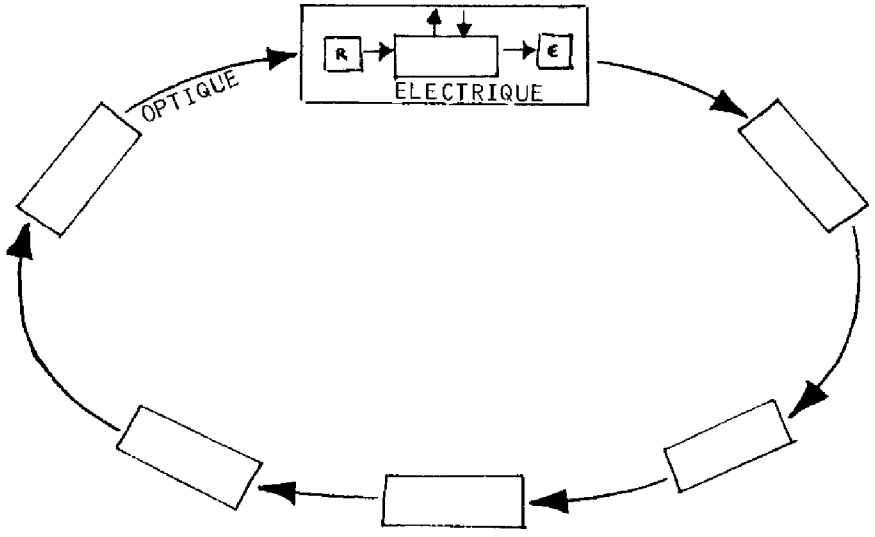
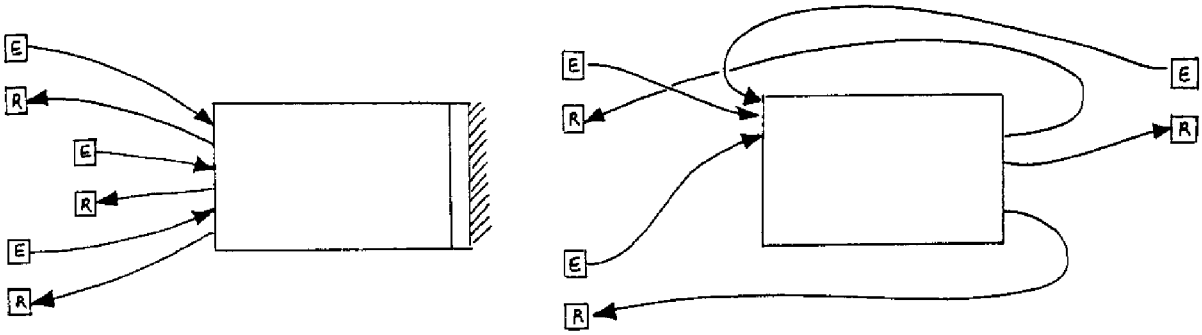


figure III.2 : schéma d'une boucle optique

La même difficulté apparaît pour le bus optique, mais on peut la résoudre sans élément actif, en utilisant un coupleur optique constitué d'un barreau mélangeur, soit par réflexion, soit par transmission (figures III.3.a et III.3.b) /KLE'78,RAW'78,RIC'83/.



a. coupleur par réflexion

b. coupleur par transmission

figure III.3 : coupleurs pour bus optique.

Le **bus optique** a donc une structure en étoile, mais l'élément central est entièrement passif ; sa probabilité de défaillance peut alors être considérée comme très faible. De tels coupleurs font l'objet d'études et de réalisations de la part de plusieurs industriels. La difficulté tient au nombre de voies (paires de fibres) que l'on peut brancher sur un tel coupleur. L'atténuation du signal est proportionnelle au nombre de voies, sans même tenir compte des inhomogénéités de répartition de la lumière, en particulier pour les fibres les plus externes /ACT'79/. L'état de l'art actuel consiste en des coupleurs par transmission d'une quarantaine de voies, avec une dispersion maximale de 2 à 3 dB /HOL'82/, ce qui est suffisant pour notre application.

Remarquons cependant que l'atténuation reste par principe très élevée ; ceci oblige à utiliser des fibres et connecteurs à très faible atténuation, et des émetteurs/récepteurs à hautes performances, ce qui augmente le coût.

Du point de vue purement structurel, la flexibilité est très bonne, tant qu'il reste des voies disponibles sur le coupleur.

La réalisation de la **structure en boucle** est tout à fait classique, du moins à ce niveau de détail. Remarquons toutefois que, par opposition à la structure en bus, le signal est régénéré à chaque station, ce qui donne un excellent rapport signal-sur-bruit avec des équipements optiques standards.

La flexibilité structurelle est par contre un peu moins bonne que celle du bus, puisque l'insertion ou l'extraction d'une station nécessite la coupure temporaire de la boucle. Toutefois, le nombre de stations n'est pas borné (du moins pas par des contraintes structurelles).

III.1.2.3 Degré de multiplicité

Nous avons vu que, quel que soit le coût supplémentaire, il fallait avoir recours à une boucle multiple plutôt qu'à une boucle simple, beaucoup trop

vulnérable.

Pour le bus par contre, nous pouvons négliger pour cette première approche la probabilité de défaillance du coupleur (entièrement passif). Les conséquences d'une défaillance sont alors limitées à une seule station. L'amélioration de sûreté de fonctionnement apportée par un bus double ne paraît donc pas compenser le doublement (au moins) du coût. De la même façon, tripler la boucle n'apporte pas une amélioration suffisamment significative, par rapport au doublement.

Ceci doit naturellement être complété par une comparaison du coût de ces deux solutions : bus simple et boucle double.

Or il apparaît que dans les deux cas, si N_s est le nombre de stations, il y a $4*N_s$ connecteurs. La longueur de fibre peut être estimée à $2*500*N_s$ dans le cas du bus où chaque station est approximativement à 500 mètres du coupleur, et à $2*200*N_s$ dans l'autre cas, 200 mètres représentant la distance approximative moyenne entre stations.

En conséquence, la différence de qualité des équipements optiques et le prix du coupleur sont en balance avec l'augmentation de coût des processeurs frontaux (doublés au moins partiellement pour gérer la double boucle). Il est donc légitime de retenir ces deux solutions, non départageables à ce niveau de détail : **bus simple**, et **double boucle.**

La deuxième solution est constituée de deux boucles monodirectionnelles. Cette redondance est introduite pour diminuer la vulnérabilité, en permettant de tolérer certaines fautes. Le sens de rotation respectif des boucles détermine les types de fautes qui peuvent être tolérées /ZAF'74/.

III.1.2.4 Sens de rotation

Du point de vue structurel, choisir des sens de rotation différents (boucles contrarotatives) présente l'avantage que les deux chemins qui relient une paire quelconque de stations ne passent par aucune autre station commune (figure III.4), ce qui permet de tolérer des fautes de mode commun, affectant les deux boucles en un endroit donné (isolement d'une station défaillante en particulier). C'est en particulier la solution retenue dans /IHA'82/, ainsi que dans /HAL'82/.

Par contre, nous voyons sur la figure III.5.a que les boucles isorotatives permettent de tolérer plusieurs fautes simples, mais aucune faute de mode commun.

Nous préférons donc la solution à boucles contrarotatives (figure III.5.b), plus conforme à l'objectif de sécurité : on peut supposer que l'on a le temps de réparer le support entre deux occurrences de fautes simples (ce qui ôte leur intérêt aux boucles isorotatives), alors que si une faute de mode commun affecte le support, le système de sécurité peut être sollicité par un défaut sur le réseau avant la réparation du support.

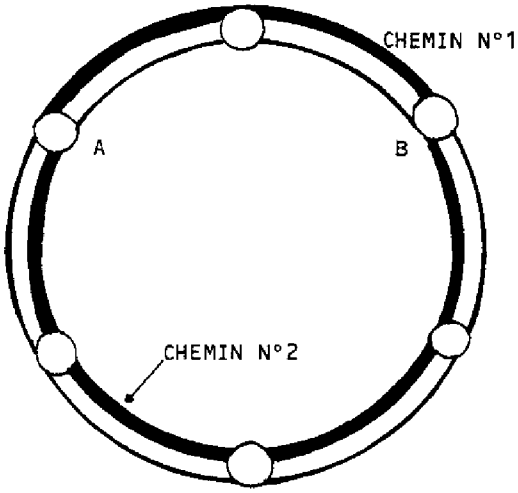
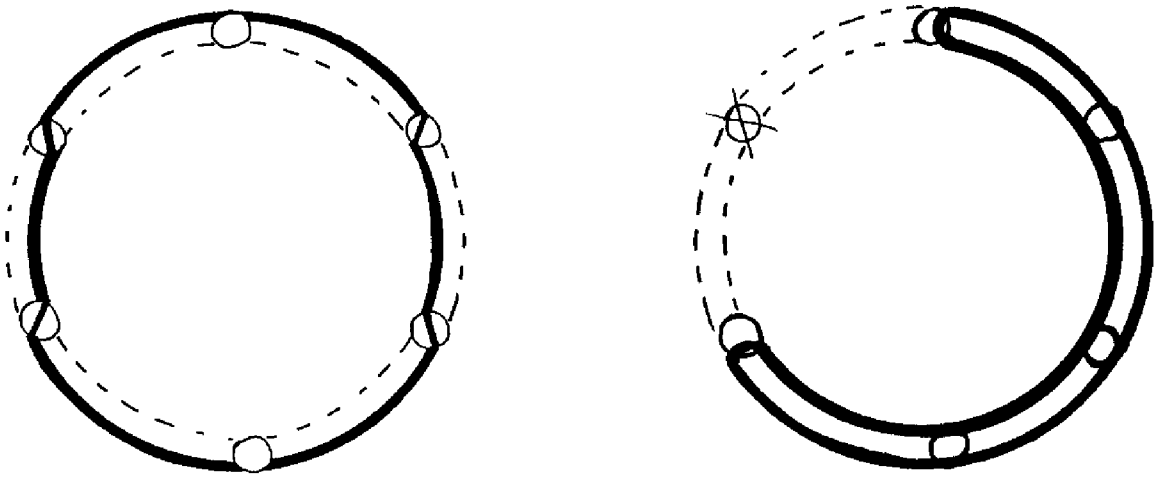


figure III.4 : boucles contrarotatives : chemins multiples



a : boucles isorotatives

b: boucles contrarotatives

figure III.5 : Possibilités de reconfiguration du support

III.1.2.5 Conclusion

Les premiers choix d'architecture de transmission conduisent donc à retenir :

- un bus simple, par coupleur optique passif,
- une double boucle contrarotative, avec conversion et régénération du signal optique dans chaque processeur frontal.

Ces deux solutions présentent des caractéristiques comparables de coût. Du point de vue de la flexibilité structurelle, le bus présente l'avantage d'une plus grande "souplesse", mais l'inconvénient d'une limitation matérielle. Du point de vue de la sûreté de fonctionnement, les caractéristiques de décentralisation sont analogues, à ce niveau de détail. Par contre, si la technique optique retenue interdit (actuellement) pour cette application le recours à une solution entièrement standard, le bus présente sur la boucle

l'inconvénient de requérir des composants plus spécifiques. Ce point ne pourra cependant être pris en considération qu'après l'étude des procédures de transfert, dans le paragraphe suivant, et de l'aspect plus ou moins spécifique des procédures applicables à ces structures.

III.2 TRANSFERT

Dans ce paragraphe, nous étudions un premier niveau de détail, du point de vue du transfert. Il s'agit donc :

- de déterminer l'objet traité par la procédure de transfert, c'est-à-dire préciser la constitution d'un paquet,
- d'examiner au moins dans ses grandes lignes le traitement de ces paquets.

III.2.1 Composition d'un paquet

Les paquets sont acheminés sous forme de séquences de signaux. Il s'agit de transmission série, ce qui oblige à utiliser des horloges permettant de synchroniser les instants d'émission des signaux successifs, ou les instants de réception (instants successifs d'échantillonnage du support).

Il n'est pas question, sur un support partagé par plusieurs dizaines de stations, d'utiliser une technique de transmission asynchrone, où la taille des paquets est limitée à une dizaine de bits : ce n'est même pas suffisant pour identifier l'expéditeur et le(s) destinataire(s).

Le choix se portera donc sur une technique synchrone, et conformément aux conclusions du paragraphe II.2.3.2, sur une technique normalisée qui permettra le recours à des fonctions et composants standards. La solution la plus couramment adoptée est le protocole HDLC /ECM'79/, recommandé par un ensemble d'instituts de normalisation (ISO, CCITT), et soutenu par les constructeurs de circuits. En fait, nous n'avons besoin ici que d'un sous-ensemble de ce protocole, la **trame** des informations caractérisée par :

- un indicateur de début et fin de paquet, appelé **fanion** : 01111110,
- deux octets de code de redondance cyclique (CRC) précédant le fanion de fin de paquet, destiné à la détection des erreurs de transmission,
- la transparence des données vis-à-vis du fanion, basée sur l'insertion systématique d'un "zéro" après cinq "un" à l'émission, et en réception, l'extraction du bit suivant le cinquième "un", si c'est un "zéro" (sinon, la séquence appartient à un fanion).

Le protocole HDLC est plus complet, mais la plupart des circuits de gestion de ce protocole possèdent un mode de fonctionnement simplifié, où seule la trame HDLC est traitée, c'est-à-dire les caractéristiques indiquées ci-dessus. Ceci suffira pour cette application, et surtout permettra d'envoyer des paquets à des groupes de stations, alors que le protocole HDLC n'offre que l'adressage individuel ou la diffusion.

Cette solution introduit un synchronisme entre les différentes stations, ce qui les oblige :

- soit à partager une horloge commune,
- soit à disposer de moyens d'ajuster leurs horloges locales.

La solution du partage d'horloge commune est à rejeter pour des raisons de sûreté de fonctionnement (très mauvaise décentralisation).

Pour ajuster les horloges locales, plutôt que d'utiliser un support séparé véhiculant un signal d'horloge (trop coûteux), il est préférable de faire appel à des techniques auto-synchrones, où l'horloge peut être reconstituée à partir du signal reçu lui-même.

Ces techniques reposent sur la synchronisation de l'horloge de la station réceptrice par les fronts détectés par le récepteur. Il suffit donc de garantir que pendant toute la période où la synchronisation doit être maintenue, c'est-à-dire la durée du paquet, les fronts se succèdent suffisamment rapidement par rapport à l'écart de fréquence entre les horloges d'émission et de réception.

La solution la plus simple consiste à utiliser un code de transmission garantissant un front par bit, tel que le code "Manchester Biphase" représenté sur la figure III.6.

Cependant, cette solution présente l'inconvénient de diviser par deux le débit de transfert à débit de transmission fixé (c'est-à-dire à bande passante fixée).

Une autre solution consiste à tirer parti du fait que le code de transfert utilisé (trame HDLC) interdit l'occurrence de plus de six "un" consécutifs. Il suffit donc de représenter les "un" par un changement de niveau logique, et les "zero" par un maintien au même niveau (code $NRZI_1$: Non Retour à Zero, Inversion pour 1), comme indiqué sur la figure III.6. Ceci offre deux avantages :

- le débit de transfert n'est pas diminué,
- la plupart des circuits de gestion de la trame HDLC sont conçus pour traiter ce code.

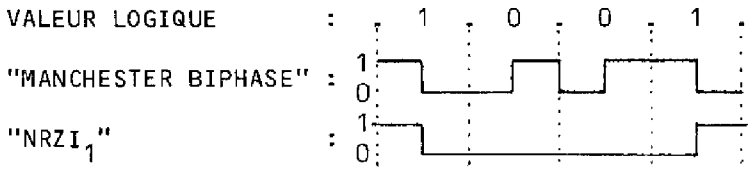


figure III.6 : codes auto-synchrones

A titre indicatif, le fonctionnement reste possible avec un rapport entre la fréquence de réception et celle d'émission compris entre :

- 0,75 et 1,25 avec le code Manchester biphase,
- 0,92 et 1,08 avec le code $NRZI_1$ associé à la trame HDLC.

III.2.2 Procédure de traitement

Dans ce paragraphe, nous allons étudier le **support de transfert** en faisant abstraction le plus possible de la couche de transmission, c'est-à-dire de l'architecture du **support de transmission.**

Le support de transfert est une entité partagée par toutes les stations, qui leur permet d'échanger des messages (sous forme de paquets). La procédure de traitement détermine l'architecture de ce support, c'est-à-dire **l'architecture de transfert**, qui peut ne pas coïncider avec l'architecture de transmission (par exemple RHEA /POW'81/ possède un support de transfert en voie multipoint -ou bus- réalisé par un support de transmission en réseau irrégulier).

Dans le cas général, toutes les stations ne pourront pas envoyer simultanément des paquets sur le support, qui apparaît alors effectivement comme une ressource commune. La caractéristique essentielle de la procédure sera alors, en première approche, la gestion du partage de cette ressource commune.

De nombreux auteurs ont proposé des études et classifications des méthodes d'accès à un support de communication partagé /AND'75,CLA'78,LUC'78,PEN'79, POW'81/. Ces classifications reposent principalement sur la distinction entre les méthodes :

- par **sélection** : gestion des accès dans le but d'éviter les conflits,
- par **compétition** : gestion des accès dans le but de détecter les **collisions** engendrées par les conflits, et de résoudre ces conflits.

III.2.2.1 Accès par sélection

Dans ce cas, une station au plus possède le **droit d'émettre** un paquet sur une liaison et à un instant donnés.

Pour assurer la gestion de ce droit d'émettre, on peut avoir recours à une procédure centralisée ou décentralisée :

GESTION CENTRALISEE : dans ce cas, le droit d'émettre est accordé à une "station-esclave" par une "station-maître". Cette procédure peut être effectuée à la seule initiative du maître (qui propose successivement le droit à toutes les autres stations), ou bien sur demande d'un esclave (le maître accorde alors le droit à la station la plus prioritaire qui en a fait la demande, ou bien s'il ne peut pas identifier les stations demandeuses, il les interroge successivement).

Le statut de maître peut être lié à une station particulière, ou bien circuler ; dans ce cas, c'est généralement la station en possession du droit d'émettre qui est le maître, c'est à dire qu'elle est également chargée de déterminer quelle station aura le droit d'émettre (et le statut de maître) à sa suite.

GESTION DECENTRALISEE : on peut classer les différentes techniques de gestion décentralisée selon qu'une station peut savoir indépendamment des autres ou non si elle peut émettre.

Dans les techniques relevant de la première catégorie, les stations sont placées en séquence sur un anneau ; cet anneau peut être **virtuel** -les stations déterminent si elles ont le droit d'émettre à l'aide d'un compteur local- ou **matérialisé**, soit par la voie de communication elle-même, soit par des lignes de gestion associées à la voie. Le droit d'émettre est alors lui-même matérialisé par un signal spécifique circulant sur l'anneau de station en station jusqu'à ce qu'une station décide de l'utiliser.

La deuxième catégorie correspond à des techniques où les différentes stations doivent se consulter pour déterminer, parmi celles qui demandent l'accès au support, quelle est la plus prioritaire (**élection**, ou **consultation**).

III.2.2.2 Accès par compétition

Ces procédures s'appliquent lorsqu'il ne doit pas y avoir plus d'une station qui émette à la fois sur une voie, afin de résoudre les conflits résultant d'émissions multiples. Elles se caractérisent donc par la méthode d'accès à la voie, ainsi que par la méthode de résolution des conflits. En ce qui concerne l'accès, on peut distinguer deux techniques :

EMISSION SOURDE : les stations émettent leur paquet dès qu'il est prêt, qu'il y ait ou non d'autres stations en cours d'émission. Les conflits peuvent alors être détectés, soit de façon centralisée par une station particulière capable d'écouter les signaux sur le support, soit par une procédure d'accusés de réception : tout paquet non acquitté est considéré comme perdu (collision ou erreur de transmission), et réémis.

ECOUTE AVANT EMISSION (technique "CSMA", utilisée dans ETHERNET /MET'76/) : dans ce cas, l'**acquisition** de la voie ne se fait que si la station ne détecte pas de signal indiquant l'occupation de la voie. Si la voie est occupée, la station **ajourne** son émission. La probabilité de conflit est alors réduite à la probabilité que deux stations tentent d'émettre à des instants séparés par une durée inférieure au temps de propagation des signaux entre ces deux stations.

Les collisions peuvent être détectées par les stations en conflit, par comparaison (au temps de propagation près) entre les signaux qu'elles émettent et ceux qu'elles détectent sur la voie : **détection d'interférence.**

En ce qui concerne la méthode de résolution de conflit, on pourra envisager, de la même façon que pour la procédure d'accès, des techniques par **sélection** ou par **compétition** :

- résolution de conflit par sélection : comme au paragraphe III.2.2.1, gestion centralisée, ou décentralisée avec "droit d'émettre" virtuel ou matérialisé.

- résolution de conflit par compétition : on utilise alors généralement la même technique de base que celle retenue pour l'acquisition de la voie (c'est-à-dire que si l'on a la possibilité d'écouter les signaux présents sur le support, on continue d'en profiter).

La résolution de conflit, et donc en particulier la procédure de réémission d'un paquet après collision, peut donc être différente de la procédure suivie pour une première émission, et même ne pas être une procédure par compétition, mais par sélection ; lorsque ce sera par compétition, il y aura également le plus souvent des différences, afin de diminuer la probabilité d'entrer de nouveau en collision (par exemple en modifiant le délai avant réémission).

III.2.3 Choix de base

Ce paragraphe est consacré à une première analyse des procédures possibles, à l'aide des critères de décentralisation, simplicité, coût, et flexibilité.

III.2.3.1 Décentralisation

Ce critère permet d'éliminer d'emblée les techniques centralisées : sélection à gestion centralisée, et compétition avec résolution par sélection centralisée. Il faut de plus rappeler que le critère de décentralisation que nous utilisons est pris dans son sens fort, incluant la notion de vulnérabilité -ou plutôt son opposée : la robustesse. A ce titre, les procédures d'accès (ou résolution de conflit) par sélection "décentralisée" avec droit d'émettre matérialisé par un signal spécifique ne sont pas très satisfaisantes. En effet, qu'il s'agisse d'une boucle avec jeton circulant, ou trame circulante, ou d'un bus avec passage de jeton, ces procédures reposent sur l'intégrité d'une entité spécifique (le jeton ou la trame) qui peut être "défaillante" (erreur de transmission, ou défaillance d'une station). Ces procédures, ainsi que les procédures purement centralisées, ne pourront donc pas être utilisées sans techniques complémentaires destinées à reconstituer l'entité défaillante. Ces techniques compliquent la procédure, et diminuent ses performances fonctionnelles (durée de recouvrement).

Nous préfèrerons donc, au moins pour cette première approche, les procédures purement décentralisées : **sélection décentralisée par droit virtuel**, et **compétition.**

III.2.3.2 Simplicité et coût

Ces critères ne sont pas très significatifs ici. En effet, la procédure de transfert pourrait être "artificiellement simple", en reportant la complexité et le coût sur la couche de transmission (et inversement). Nous pouvons toutefois remarquer que pour éviter un tel report de complexité, il sera préférable d'adopter une architecture de transfert (et donc la procédure qui la détermine) la plus proche possible de l'architecture de transmission retenue ; naturellement, ceci n'est vrai que pour ces critères, et l'ensemble des choix pourrait conduire à une solution différente.

La simplicité fournit de plus, comme indiqué au paragraphe précédent, un argument pour préférer une procédure purement décentralisée, à une procédure de nature centralisée munie de techniques de recouvrement pour pallier sa mauvaise robustesse. Il faut toutefois remarquer qu'il s'agit d'une simplification de conception, destinée à éviter les difficultés :

- de conception d'une procédure complexe à sûreté de fonctionnement suffisante,
- d'évaluation de la sûreté de fonctionnement propre de la procédure.

En fait, rien ne prouve qu'on ne rejette pas ainsi des solutions qui, bien que complexes, pourraient être rendues suffisamment sûres (voir par exemple le système REBUS /AYA'82/). Toutefois pour cette application nous nous en tiendrons, sans en faire cependant un choix de principe, à cette approche, ne serait-ce que parce que la durée d'une procédure de recouvrement est difficilement compatible avec la contrainte d'acheminement d'une rafale en un temps maximal de trois millisecondes.

III.2.3.3 Flexibilité

A priori, toutes les procédures proposées peuvent fonctionner avec un nombre **quelconque** de stations, et même, peut-être moyennant certaines précautions, avec un nombre **variable** de stations. Mais toutes n'offriront pas la même flexibilité. Ainsi les procédures par compétition seront très bonnes sous cet aspect, puisqu'il sera même possible (si la structure le permet) d'extraire ou d'ajouter, en cours de fonctionnement, une station.

Les procédures par sélection n'auront pas toutes le même avantage. En particulier, les techniques utilisant explicitement des adresses identifiant les stations (accès par forçage, anneau virtuel avec jeton), ou réservant un intervalle de temps pour chaque station (anneau virtuel sans jeton) imposeront un nombre maximal de stations. Il n'est en effet pas question de modifier à chaque fois dans chaque station, le nombre d'intervalles, ou la structure de l'anneau virtuel. De plus dans ce dernier cas, il faudra tenir compte de l'existence de "trous" dans l'anneau virtuel maximal, dus aux stations devenant actives ou inactives, c'est-à-dire d'adresses alternativement affectées et non affectées. Toutefois, ce dernier point était déjà imposé pour des raisons de décentralisation (non vulnérabilité à la défaillance d'une station, et donc a fortiori à sa suppression).

III.3 SYNTHESE DES CHOIX

A l'issue de cette première analyse, on a pu retenir :

- deux types d'architectures de transmission :
  - + bus simple,
  - + double boucle contrarotative,
- un mode de transmission (synchrone, selon la trame HDLC),
- deux codes de transmission auto-synchrones :
  - + "Manchester biphase"
  - + "$NRZI_1$" (auto-synchrone en association avec la trame HDLC).

Pour effectuer un premier choix de procédures de transfert il faut, à partir des résultats généraux de l'analyse du paragraphe III.2.2, prendre en compte les interactions avec la couche de transmission, et donc avec les choix du paragraphe III.1 rappelés ci-dessus. Nous allons donc étudier pour chaque structure de transmission possible : bus simple et double boucle contrarotative, les procédures de transfert les mieux adaptées pour gérer la communication sur ces structures.

III.3.1 Procédures pour bus

Comme la structure en bus retenue est entièrement passive, il s'agit d'une voie exclusivement multipoint, en ce sens qu'elle n'est, à aucun niveau de détail, composée fonctionnellement de liaisons individuelles pour chaque émetteur. On ne peut donc envisager sur une telle structure qu'un accès par compétition, ou par sélection basée sur un partage temporel.

III.3.1.1 Accès par compétition

C'est une méthode d'accès naturelle pour une telle voie, dont les architectures de transmission et de transfert sont alors en concordance. L'avantage essentiel de cette technique d'accès réside dans sa très bonne décentralisation ; il faut cependant tempérer cette autonomie apparente des stations, en considérant le fait qu'une station qui émet empêche toutes les autres de le faire. Nous devrons donc prévoir des procédures permettant aux stations de s'interdire de "polluer" le support de communication à la suite d'une défaillance (en particulier en détectant les émissions trop longues).

La détection de conflit se fera bien sûr par écoute et comparaison pendant l'émission (détection d'interférence). Pour la résolution des conflits comme pour l'ajournement (traitement des paquets dont l'occupation de la voie a empêché l'accès), on peut envisager une technique par compétition ou par sélection. Il n'est pas possible de trancher, à ce niveau de détail, mais on peut faire les constatations suivantes :

Ajournement par compétition :

- Si les stations qui ont ajourné un paquet tentent de l'émettre dès que la voie se libère (technique dite "persistante"), la probabilité de conflit devient égale à la probabilité que plusieurs stations aient eu un paquet prêt, non plus pendant la durée de propagation des signaux, mais pendant la durée de l'émission du précédent paquet. Ceci n'est généralement tolérable que si la résolution de conflit se fait par sélection.
- Si une station possède un délai moyen avant réémission plus long que les autres, elle peut être très défavorisée, surtout à forte charge. Il faut alors prévoir des techniques dites "adaptatives", qui compliquent généralement la procédure.

Ajournement ou résolution de conflit par compétition :

- Le temps d'accès n'est pas borné.

Ajournement et résolution de conflit par compétition :

- La procédure est alors plus simple, et satisfait le critère de latence minimale, tous les cas étant traités essentiellement de la même façon.

III.3.1.2 Accès par sélection

Sur une voie multipoint, les méthodes d'accès par anneau virtuel et signal réel ou virtuel ne paraissent pas très bien adaptées pour cette application.

Avec un signal réel, il faut prévoir des procédures de reconstitution de l'anneau virtuel, lorsque le signal identifiant la station qui a le droit d'émettre est affecté d'une erreur, ou lorsque cette station est défaillante (ou absente). La procédure consistant à confier à la dernière station qui a émis, l'envoi de "jetons" aux autres jusqu'à ce qu'une l'accepte, est en fait une procédure centralisée. L'élaboration d'une procédure décentralisée conduit à une solution plus complexe, et de durée de reconfiguration plus longue. Nous ne la retiendrons donc pas en première approche.

Avec un signal virtuel, la solution consiste à attribuer à chaque station un intervalle de temps pendant lequel elle est la seule à pouvoir émettre. Ceci oblige les stations à partager une base de temps, ce qui diminue la décentralisation. De plus, le système de priorités ainsi instauré entre les stations ne doit pas être fixe. Il faut donc élaborer une procédure, bien sûr décentralisée, de circulation des priorités (ce qui suppose que chaque station est capable de déterminer avec la plus grande autonomie possible, quelle est sa priorité) et de reconfiguration après erreur de circulation.

En première approche, on peut remarquer qu'une procédure par compétition présentera toujours l'avantage que les collisions y sont des événements normaux, résolus dans le cadre de la procédure courante, et non pas des défaillances nécessitant un traitement exceptionnel.

La deuxième technique d'accès par sélection, basée sur la notion d'élection, semble nécessiter une procédure complexe, et longue à exécuter. En fait, la structure particulière du support de transmission permet de recourir à une solution assez simple : l'accès par **forçage**.

En effet, si par exemple le "1 logique" est représenté par la présence d'un signal lumineux, et le "0" par son absence, la voie se comportera, au délai près, comme un "OU logique". Si donc deux stations sont en émission simultanée, celle qui émet un "0" voit son message perturbé, mais pas celle qui émet un "1". Ceci peut être mis à profit en attribuant à chaque station une valeur numérique binaire spécifique, à émettre en tête du paquet (poids fort en premier). On montre alors /POW'81/ que (sous réserve que chaque bit de l'en-tête dure au moins deux fois la durée maximale de propagation sur le bus) la station qui, parmi celles qui émettent, possède la valeur la plus élevée, peut seule continuer à émettre son paquet non perturbé, les autres cessant leur émission dès qu'elles détectent le conflit.

Cette méthode, basée sur des priorités, ne peut toutefois être utilisée qu'associée à une procédure décentralisée de circulation de ces priorités et de reconfiguration après erreur de circulation.
Remarque : comme toute méthode d'accès par sélection, celle-ci peut être utilisée pour résoudre les conflits résultant d'un accès par compétition. En l'occurrence, c'est très généralement le cas /MAR'78,POW'81/, car il n'y a aucune raison d'imposer un instant précis pour commencer d'émettre, plutôt que de laisser la possibilité d'émettre dès qu'un paquet est prêt, les conflits étant automatiquement résolus. Ceci permet même d'émettre un paquet ajourné dès que la voie se libère, sans qu'il soit nécessaire de chercher à diminuer la probabilité de conflit.

III.3.2 Procédures pour double boucle

Pour des raisons de simplicité et de sûreté de fonctionnement, les deux boucles doivent être gérées de la même façon, et de la même façon que serait gérée une seule boucle. En particulier, à la suite d'une défaillance sur une boucle, la même procédure doit être capable de gérer la boucle simple restante. A ce niveau de détail, nous n'aurons donc pas à étudier la gestion de la **double** boucle, et il suffira de considérer une seule boucle.

A la différence du bus, la boucle est constituée de liaisons point-à-point monodirectionnelles, comportant donc un émetteur unique. De plus, elle possède une structure en anneau.

En conséquence, il sera possible d'adopter :

- une technique d'accès par compétition, en considérant un support de transfert en voie multipoint, ou
- une technique par sélection, utilisant :
  + soit la structure d'anneau matériel,
  + soit un partage, non pas du temps comme pour le bus, mais des liaisons elles-mêmes.

Cette dernière technique (partage des liaisons) est basée sur le fait que les seuls conflits qui peuvent se produire apparaissent dans les stations, entre les paquets élaborés localement, et les paquets provenant des stations en amont. Ces deux types de paquets donnent en effet lieu à des signaux qu'il faut envoyer au même élément : l'émetteur de la station considérée. La sélection peut donc se faire de façon **décentralisée** et **asynchrone** dans chaque station ; il suffit pour cela que les stations disposent d'une capacité de mémorisation suffisante, pour stocker les signaux parvenant sur le récepteur pendant l'émission d'un paquet d'origine locale. Tout se passe alors comme si la station devait, pour émettre un paquet, le placer dans un registre à décalage, puis insérer ce registre entre le récepteur et l'émetteur ; l'opération de décalage fait alors entrer dans le registre les signaux atteignant le récepteur, en même temps que les signaux quittant le registre sont transférés vers l'émetteur, et le support de communication. C'est

pourquoi cette technique est connue sous le nom d'**insertion de registre** /HAF'74,REA'75,LIU'81/.

Sur le support en boucle, les inconvénients des techniques par sélection sont donc moindres que sur un support en bus, car la gestion décentralisée des priorités instaurées se fait de façon naturelle grâce à la structure même du support, qui favorise cette circulation. Cela est vrai pour l'insertion de registre, mais également pour les techniques utilisant un signal spécifique : jeton /FAR'69,BUX'82/, ou trame /PIE'72,BIN'82/.

Ces deux dernières solutions restent cependant vulnérables à la perte du signal spécifique, et présentent de ce fait une mauvaise décentralisation. Nous devons cependant tenir compte du fait qu'il y a deux boucles, ce qui améliore suffisamment la robustesse pour empêcher de rejeter ces solutions à ce niveau de détail.

III.3.3 Conclusion

La prise en compte des procédures de transfert n'a pas permis, à ce niveau de détail, de trancher entre les deux structures qui peuvent être retenues : bus simple et double boucle contrarotative.

D'une façon générale, nous pouvons remarquer que les procédures d'accès qui imposent la moins forte synchronisation entre les stations, présentent la meilleure décentralisation, du moins pour notre application où l'on ne dispose pas du temps nécessaire pour exécuter des procédures de recouvrement sûres de fonctionnement. Ceci conduit à préférer les méthodes d'accès asynchrones, c'est-à-dire par compétition, et par sélection lorsque cette sélection n'est pas basée sur un partage temporel, soit ici :

- pour le bus, une méthode d'accès par compétition avec écoute avant émission,
- pour la double boucle, une méthode d'accès asynchrone, soit par la technique d'insertion de registre, soit par compétition comme pour le bus, avec dans tous les cas une gestion séparée de chaque boucle.

Notons cependant que pour la double boucle, nous ne rejetons pas définitivement les techniques d'accès par sélection avec signal spécifique, car la redondance du support peut être utilisée pour gérer de façon "suffisamment indépendante" deux signaux spécifiques redondants. Nous approfondirons donc ces différentes solutions au chapitre IV, consacré à l'étape suivante d'affinement.

En ce qui concerne le bus, cette étape suivante doit prendre en compte les différentes possibilités pour les techniques de résolution de conflit et d'ajournement de paquet : méthode d'accès par compétition ou par sélection (y compris par forçage), en rappelant que si la première est a priori plus simple et moins vulnérable, elle conduit à des temps d'accès non bornés.

CHAPITRE IV : AFFINEMENT DES CHOIX

Dans ce chapitre, nous allons affiner les choix dans les couches de transmission et de transfert, en ajoutant des critères quantitatifs (performances fonctionnelles et sûreté de fonctionnement) à ceux déjà utilisés (latence minimale, décentralisation, simplicité,...).

Conformément à l'analyse du chapitre II, l'évaluation de la sûreté de fonctionnement est le critère principal de cette étape d'affinement dans la couche de transmission (§IV.1), avec les hypothèses adéquates simplifiant l'influence sur ce critère des procédures de transfert ; de façon analogue, l'affinement dans la couche de transfert (§IV.2) repose essentiellement sur l'évaluation des performances fonctionnelles.

IV.1 ARCHITECTURE DE TRANSMISSION

Dans ce paragraphe, nous affinons donc la conception de l'architecture de transmission. Pour cela, nous examinerons tout d'abord les différentes réalisations possibles pour les solutions retenues à l'issue du chapitre III, et nous aborderons ensuite l'évaluation comparative de leur sûreté de fonctionnement.

IV.1.1 Solutions en présence

Nous avons retenu au chapitre III une structure en bus, et une en double boucle contrarotative. Cette dernière peut être réalisée de plusieurs façons : la principale question qui se pose est en effet de savoir quelle est la structure du processeur frontal, c'est-à-dire la partie de la station qui permet à l'équipement d'utiliser le support de communication. Le support de communication en boucle étant doublé, alors que les stations ne le sont pas, on peut envisager plusieurs solutions, selon que la communication sur les deux boucles est gérée par la même unité ou par deux unités, ces unités pouvant être ou non munies de redondances permettant la tolérance aux fautes. Nous examinons dans les paragraphes suivants :

- la structure en boucles, avec processeurs frontaux :
  - * uniques, simplex ou tolérants aux fautes,
  - * doubles,
- la structure en bus, avec processeurs frontaux simplex.

IV.1.1.1 Boucles à processeurs simplex

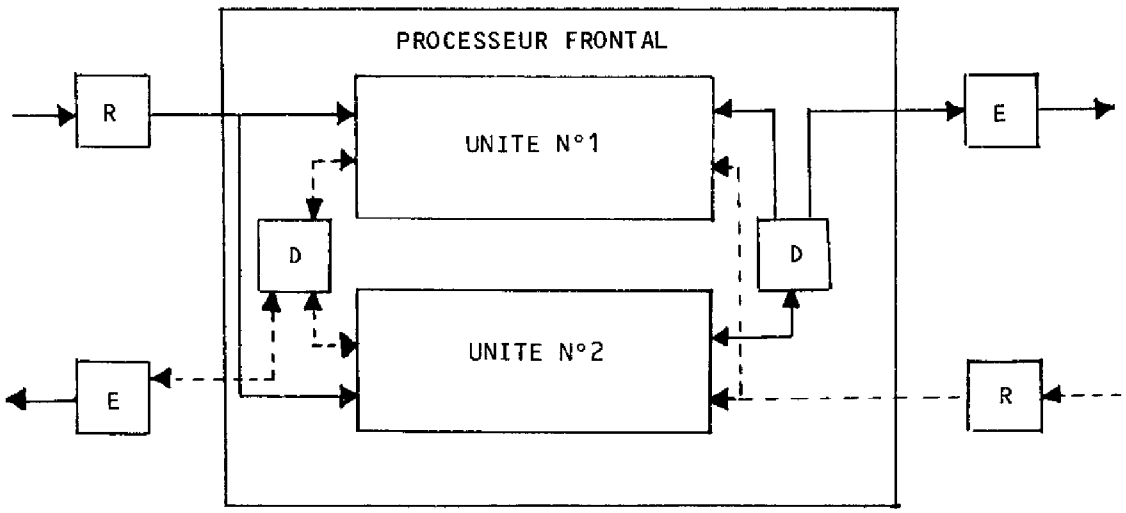
Une seule unité gère la communication sur les deux boucles, sans redondance. La seule redondance est donc celle du support physique, utilisée pour tolérer les fautes simples, mais également celles de mode commun, conformément à l'étude du paragraphe III.1.2.4, grâce à une reconfiguration du support.

Dans le cas de la structure à processeurs frontaux simplex, cette procédure de reconfiguration, qui permet de substituer à la structure en double boucle la structure indiquée sur le schéma de la figure IV.3 (page 64), doit être

effectuée après une défaillance double du support de communication, ou une défaillance simple d'un processeur frontal.

IV.1.1.2 Boucles à processeurs tolérants aux fautes

Le processeur frontal est alors lui-même doté de redondances. La figure IV.1 donne un schéma d'une telle structure, constituée de deux unités, chacune étant capable de gérer la communication sur les deux boucles, et d'équipements (notés D) permettant de détecter les erreurs dans ces unités.



E: sous-ensemble d'émission
R: sous-ensemble de réception
D: détection de faute et recouvrement
en cas de défaillance d'une unité

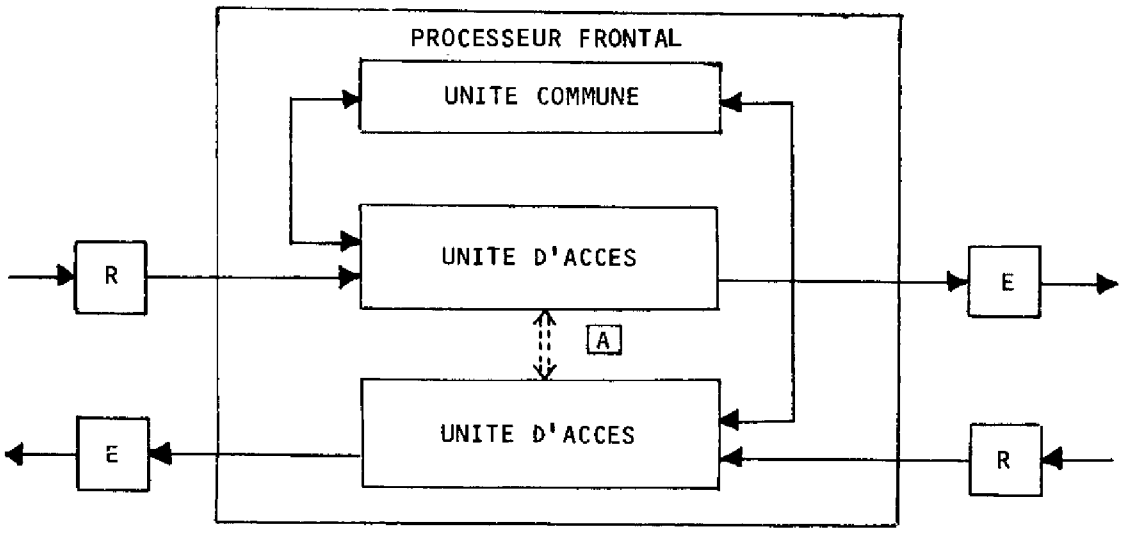
figure IV.1 : processeur frontal tolérant aux fautes

En cas de défaillance, une procédure de localisation est lancée et l'unité défaillante déconnectée ; l'avantage d'une telle structure est que la communication continue d' être entièrement assurée après une défaillance d'une unité (si la localisation et le recouvrement sont réussis). Il reste néanmoins nécessaire de disposer, comme pour la structure précédente, de moyens de reconfiguration destinés à modifier la structure du support après une défaillance double du support de communication lui-même, ou une défaillance non localisée d'une unité d'un processeur frontal.

IV.1.1.3 Boucles à processeurs doubles indépendants

Les processeurs frontaux sont alors composés, comme indiqué sur la figure IV.2, de **deux unités d'accès** gérant chacune la communication sur **une seule** boucle.

Toutefois, comme indiqué sur cette figure, il y a nécessairement une partie commune aux deux boucles, dans le processeur frontal car :



E: sous-ensemble d'émission
R: sous-ensemble de réception
A: organe permettant l'isolement d'une station

figure IV.2 : proceseur frontal double

- si les paquets sont envoyés en double (c'est-à-dire sur les deux boucles), il faut une unité en réception capable de réapparier les paquets pour n'en envoyer qu'un exemplaire à l'équipement,
- si les paquets ne sont envoyés que sur une boucle, il faut une unité en émission capable de choisir la boucle à utiliser,
- la fonction de reconfiguration du support, qui reste nécessaire en cas de double défaillance du support, ou des deux unités d'accès d'un processeur frontal, nécessite un lien de communication entre les deux boucles.

On ne considère pas, au moins en première approche, la possibilité de doter ces unités d'accès doubles de redondances propres permettant la tolérance aux fautes. En effet, les fautes simples et les fautes de mode commun sur les deux boucles sont déjà tolérées ; il ne faut donc pas espérer pour cette application de gain substantiel apporté par des techniques permettant de tolérer en plus la deuxième faute simple.

IV.1.1.4 Bus à processeurs simplex

L'architecture en bus n'étant pas redondante, il n'y a pas de raison de considérer pour ses processeurs frontaux les mêmes types de structures que pour le cas de l'architecture en double boucle. De plus, pour les mêmes raisons que celles qui ont conduit à ne pas retenir de bus redondant, nous ne considérerons pas de processeur frontal tolérant les fautes pour le bus. En fait, il n'est pas certain que cette approche soit tout à fait correcte, car s'il reste vrai que l'augmentation de sûreté de fonctionnement est plus significative en munissant de techniques de tolérance aux fautes les

processeurs frontaux de la structure en boucle plutôt que ceux de la structure en bus, la comparaison de coût ne permet plus nécessairement de conforter ce choix. En effet, on avait montré que la structure en bus simple était plutôt plus coûteuse que celle en double boucle, mais il n'en va pas forcément de même si les processeurs frontaux du support en boucle sont en fait équivalents à deux processeurs frontaux de la structure en bus (au moins).

Nous en resterons toutefois à ces choix en première approche. Naturellement, cet ensemble de possibilités peut, comme nous l'avons indiqué dans l'étude générale du paragraphe II.1.1.3, se révéler insuffisant à l'issue de cette étape d'affinement. Dans ce cas, il serait nécessaire d'effectuer un rebouclage pour recommencer cette étape avec un autre ensemble de choix.

Dans un premier temps, nous retenons donc :
- un bus simple avec processeurs frontaux simplexes,
- deux boucles contrarotatives avec procédure de reconfiguration et processeurs frontaux :
  * simplex,
  * tolérants aux fautes,
  * doubles "indépendants".

IV.1.2 Evaluation de la sûreté de fonctionnement

Nous utilisons les mesures définies au paragraphe II.2.2.4, c'est-à-dire des mesures de type fiabilité, donnant la probabilité de non-occurrence d'un événement redouté, celui-ci étant défini ici par l'ouverture, lors d'un défaut à éliminer sur le réseau, de disjoncteur(s) "en trop", à cause d'une défaillance du support de communication.

Nous disposons ainsi de plusieurs mesures, correspondant à autant de "niveaux de sûreté de fonctionnement". En fait, nous ne retenons que les deux premiers, à cause des risques entraînés, pour certains régimes fortement chargés ou déséquilibrés, par la perte de plusieurs lignes :

- **sûreté nominale** : l'événement redouté est l'ouverture d'**au moins un** disjoncteur qui n'aurait pas dû s'ouvrir,
- **sûreté dégradée** : l'événement redouté est l'ouverture de **plusieurs** disjoncteurs qui n'auraient pas dû s'ouvrir.

Pour évaluer ces grandeurs, nous allons déterminer l'évolution au cours du temps de la probabilité que l'événement redouté ne se soit pas produit. Ces calculs seront effectués sur un **modèle représentatif du comportement du système**.

Nous adopterons, dans le prolongement des travaux effectués dans l'équipe "Conception et Validation de systèmes informatiques sûrs de fonctionnement (CV)"/LAP'75,MED'80/, un modèle par **processus markoviens**, qui se prête bien aux traitements mathématiques, et en particulier par des programmes de calcul informatique tels que le programme **SURF** conçu dans l'équipe CV /COS'81/.

L'emploi d'un tel modèle revient à faire l'hypothèse que les différents événements suivent des lois de distribution exponentielles, c'est-à-dire avec des taux constants. Si cette hypothèse est bien vérifiée dans la pratique pour les événements "accidentels" tels que les défaillances, il n'en va pas tout à fait de même pour les événements liés à la réparation d'un système, ou à une maintenance périodique. Cependant, on montre /LAP'76/ que lorsque les durées de réparation ou des intervalles entre procédures de maintenance sont faibles devant l'intervalle moyen entre défaillances -ce qui est généralement le cas pour les systèmes sûrs de fonctionnement- l'utilisation de taux constants fournit des résultats très proches de ceux que pourraient fournir des modèles plus complexes.

IV.1.3 Modélisation des structures

Nous allons tout d'abord préciser les hypothèses sur lesquelles est basée la modélisation, avant d'aborder les modèles des différentes structures en présence.

IV.1.3.1 Hypothèses de modélisation

Outre l'hypothèse des taux constants, liée au principe même de la modélisation retenue, nous faisons les hypothèses simplificatrices suivantes :

- les défaillances des procédures de communication ne sont pas prises en compte, pas plus que les fautes de conception des processeurs frontaux,
- nous supposons que toute défaillance est immédiatement détectée, ceci résultant de l'application du principe de latence minimale à la conception du matériel et du logiciel du système,
- nous ne tenons pas compte, en application du principe de décentralisation, de défaillances des processeurs frontaux conduisant à la pollution du support ; il est ainsi possible après défaillance d'un nombre quelconque de processeurs frontaux d'utiliser le bus, et, sur les boucles, de lancer la procédure de reconfiguration.

Politique de réparation : Pour la modélisation, nous adoptons la politique de réparation consistant à réparer les éléments dans l'ordre où ils sont tombés en panne, quelles que soient les conséquences et les durées de réparation associées aux différentes défaillances successives.

Politique de reconfiguration : La procédure de reconfiguration n'est lancée qu'après une défaillance affectant **les deux** boucles. Il est inutile en effet d'exécuter une telle procédure, alors que la communication reste possible sans intervention. De plus, en accord avec les besoins de communication dans le poste, et avec les niveaux de sûreté définis, nous ne cherchons à reconfigurer le support que pour **isoler**, comme indiqué sur la figure IV.3, une station défaillante et non pas pour constituer des groupes disjoints de stations en communication. Nous nous limitons donc à une faute de mode commun (avec reconfiguration), ou deux fautes simples successives (sans reconfiguration,

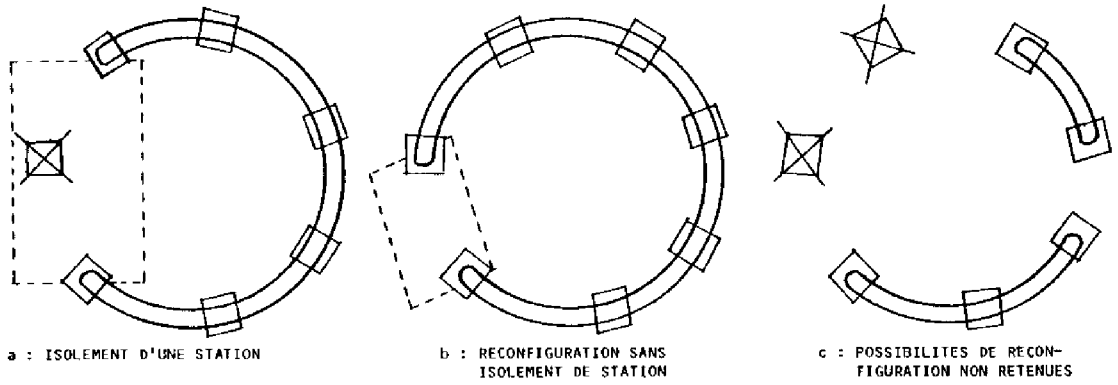


figure IV.3 : possibilités de reconfiguration

celle-ci n'étant de toutes façons possible que dans certaines configurations de fautes).

Dans une première étape, nous ferons également l'hypothèse que la reconfiguration est toujours réussie, puis nous examinerons l'influence de la prise en compte d'un **facteur de reconfiguration** différent de 1.

IV.1.3.2 Notations et principes généraux

Les modèles des différentes solutions envisageables représentent le comportement du système vis-à-vis des défaillances et des défauts, et vis-à-vis de la mesure de sûreté choisie. Nous regroupons ainsi tous les états correspondant à l'ouverture de plus d'un disjoncteur supplémentaire. Ceci correspond en fait aux modèles de sûreté dégradée. Pour la sûreté nominale, il faudrait regrouper, en les considérant comme absorbants, les états correspondant à l'ouverture d'un, ou de plusieurs, disjoncteur(s) supplémentaire(s). Ces modèles se déduisent donc très simplement de ceux de sûreté dégradée, que nous représentons sur les figures suivantes.

Précisons de plus que les modèles donnent le comportement d'une barre, qui apparaît en effet, avec ses équipements de couplage et de ligne, comme le "module" représentatif du poste.

NOTATIONS :

λ_E : taux de défaillance du sous-ensemble émission

λ_R : taux de défaillance du sous-ensemble réception

λ_F : taux de défaillance du processeur frontal "de base" (les processeurs doubles, et ceux tolérants les fautes en comportent deux)

λ_c : taux de défaillance d'organe commun : coupleur étoile pour le bus, ou unité commune pour la solution à processeurs doubles

μ : taux de réparation d'un élément quelconque

γ_1 : taux d'occurrence de défaut ligne

ξ : taux d'élimination d'un défaut ligne

n : nombre de départs sur une barre

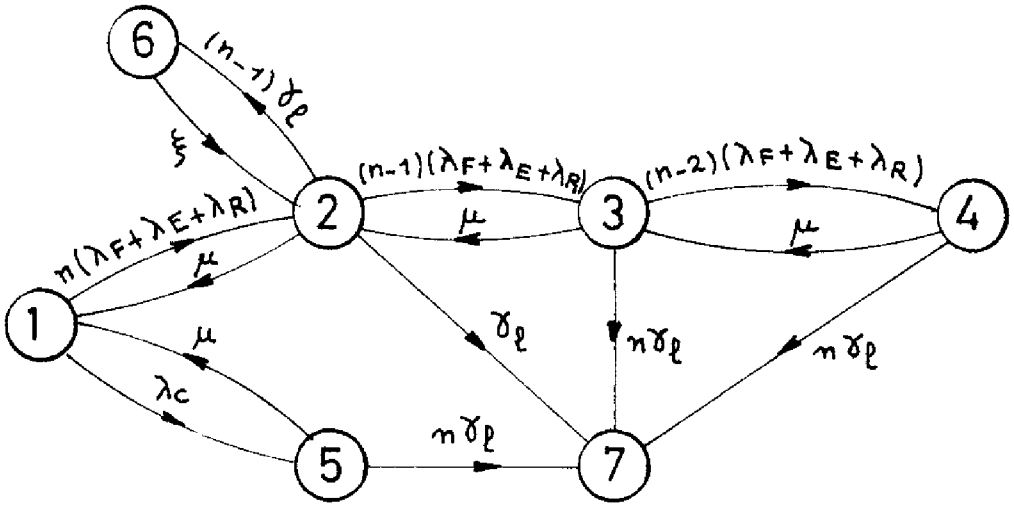
c_i : facteur de reconfiguration

c : facteur de couverture pour le processeur tolérant les fautes

IV.1.3.3 Modèle du bus

Ce modèle est donné sur la figure IV.4. Nous voyons que les défaillances des processeurs frontaux n'ont pas de conséquences sur les possibilités de communication entre les autres stations (d'après nos hypothèses, en particulier celle sur la "non-pollution" du bus par une station). Il n'y a donc pas de raison a priori pour limiter le nombre de défaillances successives à prendre en compte. Nous indiquons ici le modèle correspondant à trois défaillances successives.

Une étude de sensibilité, dont les conclusions sont données au paragraphe IV.1.4, a montré par comparaison entre les résultats fournis par des modèles prenant en compte différents nombres de défaillances, que le modèle proposé sur la figure IV.4 était suffisamment représentatif. En fait, on pourrait même se limiter aux deux premières défaillances.

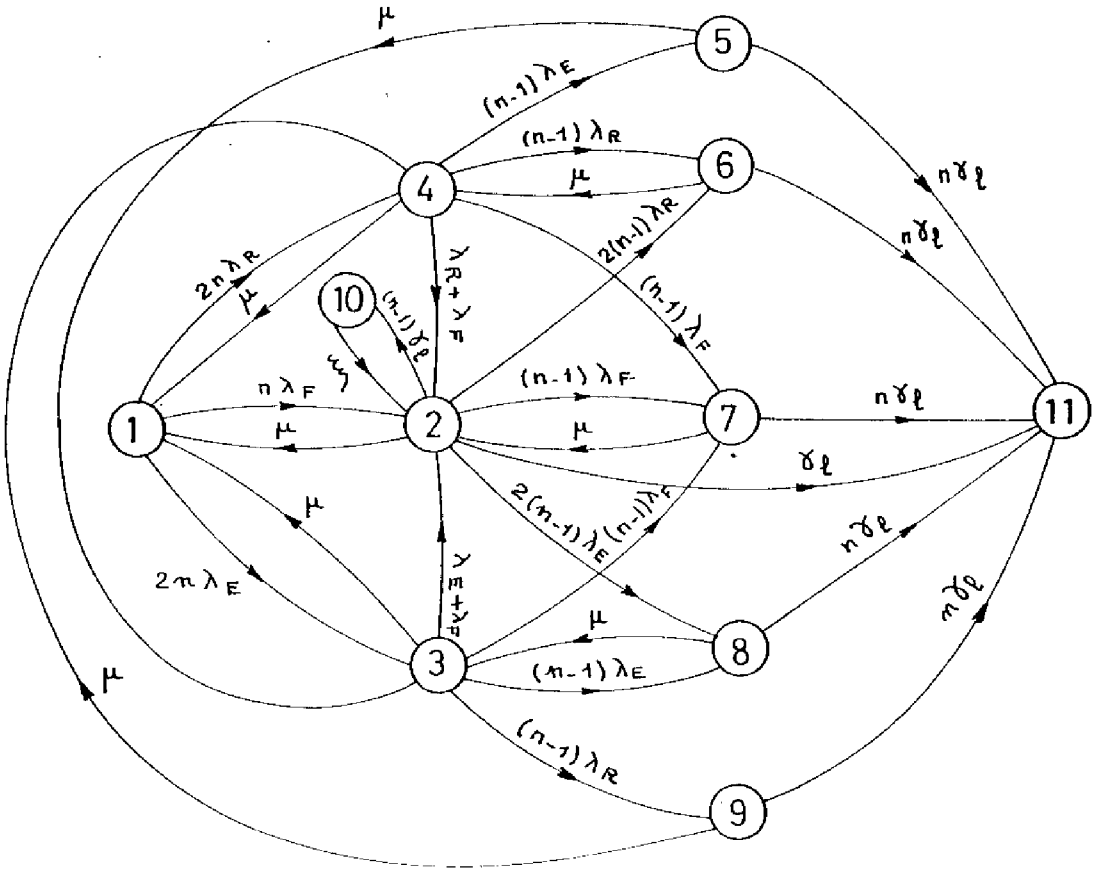


1. Etat de bon fonctionnement
2. Perte d'une station
3. Perte de 2 stations
4. Perte de 3 stations
5. Perte totale de la communication suite à la défaillance du coupleur étoile
6. Ouverture d'un disjoncteur supplémentaire
7. Ouverture de plusieurs disjoncteurs supplémentaires

figure IV.4 : modèle du bus

IV.1.3.4 Modèle des boucles à processeurs simplex

Ce modèle est représenté sur la figure IV.5. Remarquons qu'à la différence du bus, il n'y a pas à choisir un nombre maximal de défaillances. A la première, l'occurrence d'un défaut (ligne) entraîne l'ouverture d'un ou de n-1 disjoncteur(s) supplémentaires (selon que le défaut affecte une autre ligne, ou la ligne dont la station est isolée par la procédure de reconfiguration). A partir de la deuxième, il n'y a plus de communication possible.



1 Etat de bon fonctionnement

2 Perte d'une station après défaillance de son processeur frontal ou de ses deux émetteurs ou de ses deux récepteurs (état de reconfiguration)

3 Perte d'une boucle après défaillance d'un émetteur

4 Perte d'une boucle après défaillance d'un récepteur

5 à 9 Perte de la communication après défaillance de plusieurs stations

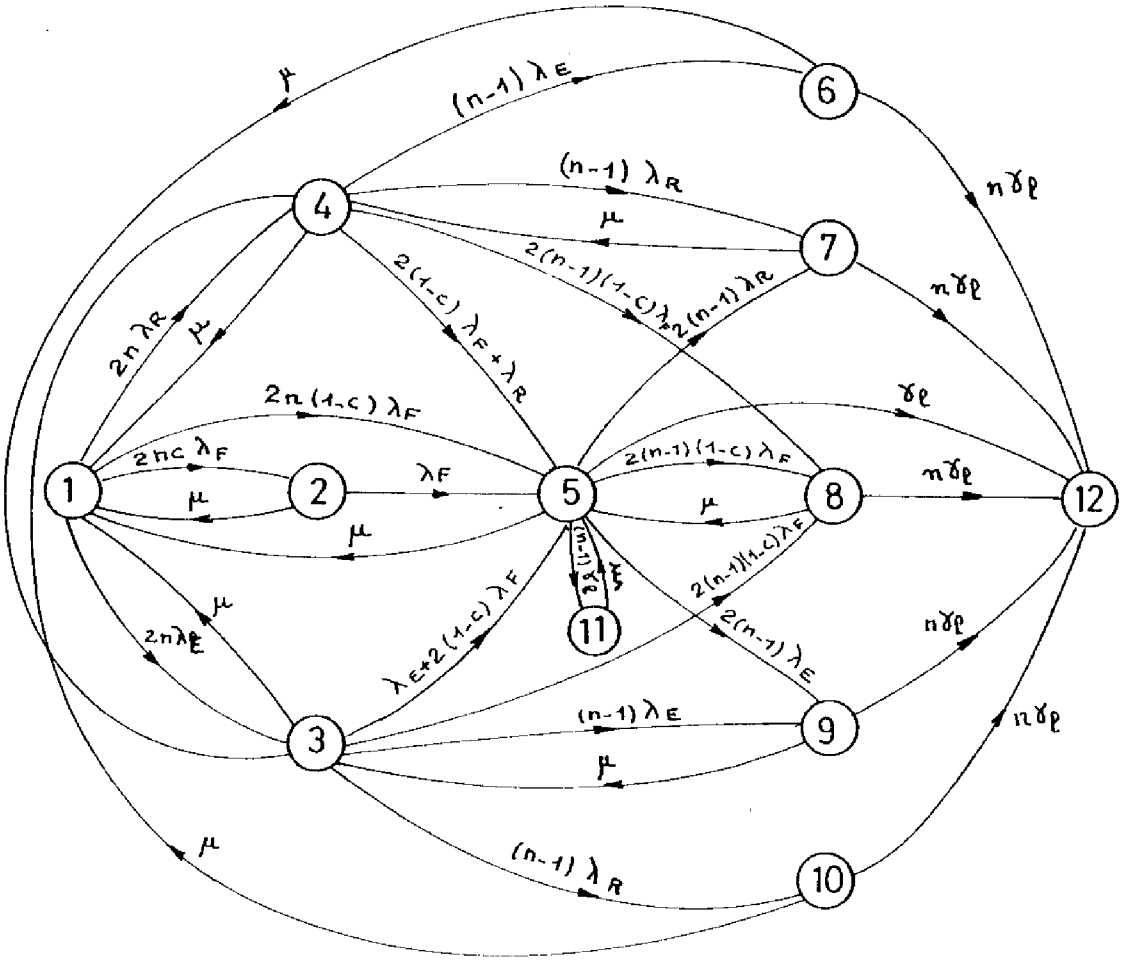
10 Ouverture d'un disjoncteur supplémentaire

11 Ouverture de plusieurs disjoncteurs supplémentaires

figure IV.5 : modèle des boucles à processeurs simplex

IV.1.3.5 Modèle des boucles à processeurs tolérants aux fautes

La différence entre ce modèle, représenté à la figure IV.6, et le précédent provient de l'existence de défaillances tolérées conduisant à l'état 2. Ces défaillances sont tolérées avec le facteur de couverture c, défini comme la probabilité que la communication continue d'être assurée sachant qu'une défaillance a eu lieu dans un processeur frontal. Ce terme intervient donc en facteur multiplicatif des taux de transition : c pour la transition de 1 vers 2, 1-c de 1 vers 5 (défaillance non tolérée).

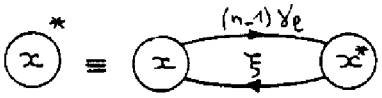


1 Etat de bon fonctionnement
2 Défaillance d'un processeur frontal avec recouvrement réussi
3 Perte d'une boucle après défaillance d'un émetteur
4 Perte d'une boucle après défaillance d'un récepteur
5 Perte d'une station (état de reconfiguration)
6 à 10 Perte de la communication après défaillance de plusieurs stations
11 Ouverture d'un disjoncteur supplémentaire
12 Ouverture de plusieurs disjoncteurs supplémentaires

figure IV.6 : modèle des boucles à processeurs tolérants aux fautes

IV.1.3.6 Modèle des boucles à processeurs doubles

Ce modèle, donné à la figure IV.7 ci-contre, comporte des états supplémentaires, dus à la défaillance de l'unité commune. Nous faisons l'hypothèse, conforme au principe de décentralisation, que cette unité commune ne sert qu'en réception, c'est-à-dire qu'au moins pour l'émission, l'indépendance entre les boucles est maximale. Dans ces conditions, les états 11 à 17 correspondent à des stations sourdes, qui peuvent quand-même envoyer des ordres de verrouillage. Pour faciliter la lecture de ce modèle, nous n'avons pas fait figurer pour les états 11 à 16 (où il n'y a qu'une station "sourde"), ni pour l'état 5 (une station isolée), les états notés 11* à 16* et 5*, correspondant à l'ouverture d'un disjoncteur supplémentaire lors d'un défaut sur un autre départ.



(1) Etat de bon fonctionnement

(2), (3) et (4) Perte d'une boucle suite à :

- (2) la défaillance d'une unité d'accès d'un processeur frontal
- (3) la défaillance d'un émetteur
- (4) la défaillance d'un récepteur

(5) Perte d'une station - reconfiguration réussie

(6) à (10) Perte de la communication suite à la défaillance de plusieurs stations

(11) à (17) Etats avec au moins une unité commune de réception défaillante

{x* = ouverture d'un disjoncteur supplémentaire}

(18) Ouverture de plusieurs disjoncteurs supplémentaires

Notations relatives à la figure IV.7

IV.1.4 Traitement des modèles

L'objectif étant de comparer les différentes solutions, nous devons nous assurer que les paramètres utilisés dans l'évaluation de chacune de ces solutions rendent légitime cette comparaison. Pour les modèles considérés, outre les différents paramètres introduits, il faut déterminer une base de comparaison pour les taux de défaillance des processeurs frontaux dans chaque solution. Pour cela, nous adoptons un processeur "de référence", celui des stations pour la solution en bus, dont nous notons le taux de défaillance λ_F'.

Nous admettons, en première approche, que les processeurs permettant de gérer la communication sur une boucle sont équivalents aux processeurs de référence. Il faut alors tenir compte de l'augmentation de matériel et de logiciel nécessaire pour la gestion de la **double** boucle. Nous définissons pour cela un facteur multiplicatif, noté **b** pour la structure à processeurs simplex (leur taux de défaillance est alors $b \cdot \lambda_F'$) et **d** pour les processeurs tolérants

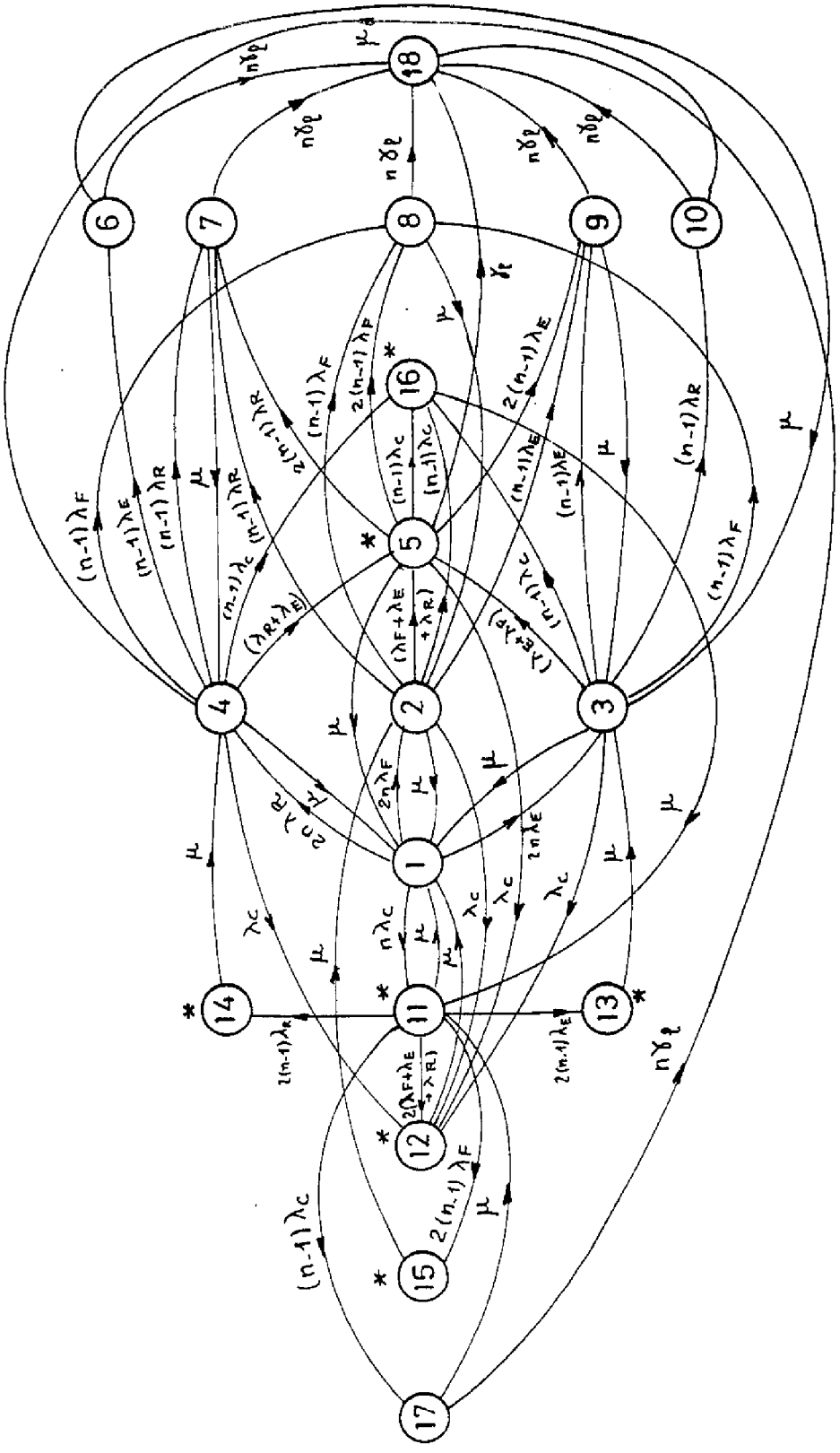


figure IV.7 : modèle des boucles à processeurs doubles

aux fautes (d tenant également compte dans ce cas des fonctions de détection et tolérance) ; le taux de défaillance de **chaque** unité d'un processeur tolérant aux fautes est alors $d \cdot \lambda_F'$.

Pour les processeurs doubles, nous pouvons retenir λ_F' pour chaque unité d'accès, les défaillances de la partie commune étant prises en compte dans λ_c.

Nous supposons de plus que les émetteurs et les récepteurs ont le même taux de défaillance, quelle que soit la structure, et nous le prenons, en première approche, dix fois plus faible que λ_F'.

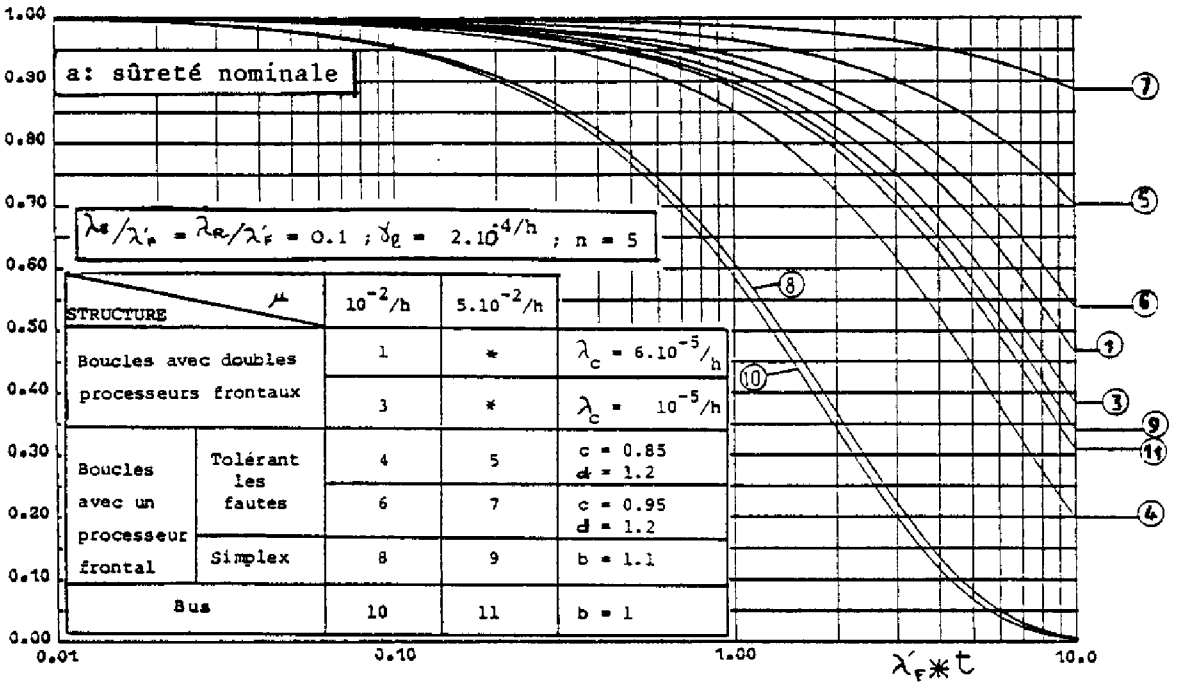
Avant de chercher à comparer les résultats fournis par le traitement numérique de ces modèles, nous avons effectué une étude de sensibilité permettant de dégager pour chaque structure les paramètres les plus influents. Une telle étude consiste à comparer les résultats obtenus en faisant varier un paramètre, les autres étant fixes. Il est ainsi possible, éventuellement après plusieurs affinements (le choix des valeurs des paramètres fixes pouvant provenir également d'une étude de sensibilité), de déterminer les paramètres à faire varier, et dans quelle gamme de valeurs, pour pouvoir comparer des solutions dont on ne connaît pas toutes les caractéristiques. Seules les conclusions de cette étude sont données ici, sous forme du tableau de la figure IV.8.

<table>
<tr><th colspan="2">STRUCTURES</th><th>PARAMETRES PREPONDERANTS</th><th></th></tr>
<tr><td rowspan="3">boucles à processeurs frontaux:</td><td>simplex</td><td>facteur multiplicatif du taux de défaillance λ_F' :b</td><td rowspan="4">taux de réparation</td></tr>
<tr><td>tolérants aux fautes</td><td>taux de couverture des mécanismes de tolérance : c</td></tr>
<tr><td>doubles</td><td>taux de défaillance de l'unité commune (pour la sûreté nominale) : λ_c</td></tr>
<tr><td colspan="2">bus à processeurs frontaux simplex</td><td>deux premières défaillances des processeurs frontaux
Non-influence des variations du taux de défaillance du coupleur (λ_c) pour des valeurs entre 10^{-2} et 10^{-3} fois lambda</td></tr>
</table>

figure IV.8 : influence des paramètres

IV.1.5 Comparaison des solutions

Les courbes des figures IV.9 (a et b) donnent la sûreté, respectivement nominale et dégradée, des solutions retenues en fonction du temps (en fait, de $\lambda_F' * t$), dans une gamme représentative de variation des paramètres.



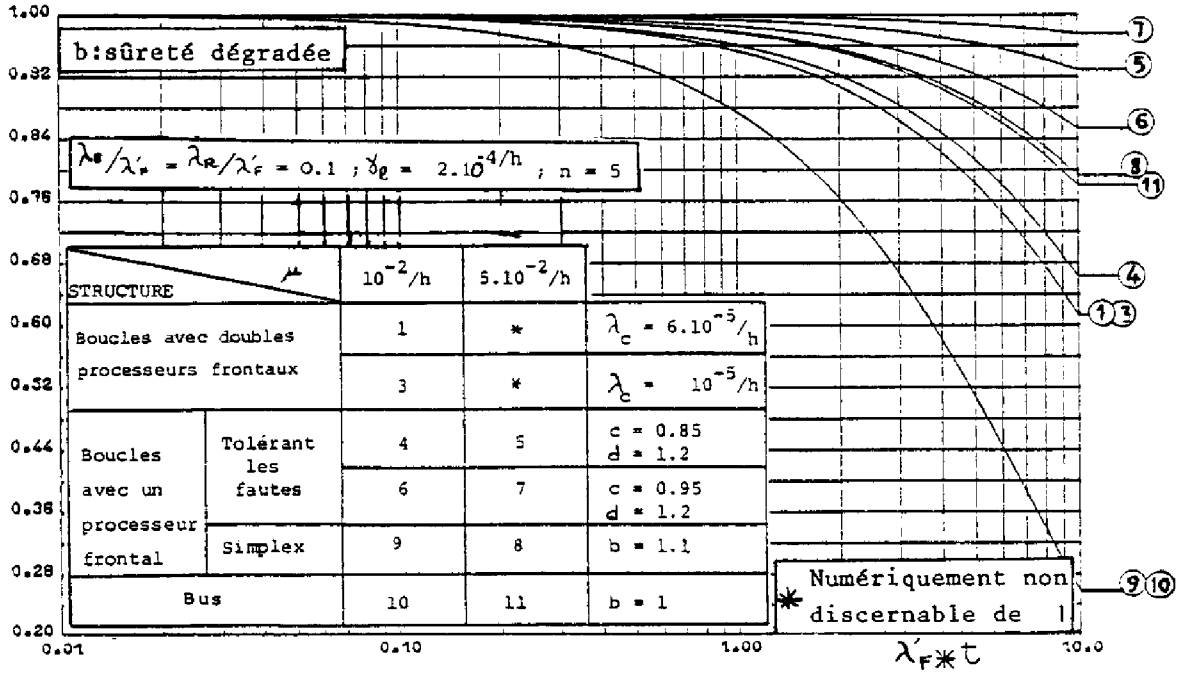


figure IV.9 : comparaison des solutions

La première conclusion que l'on peut tirer de ces courbes est que la solution du bus est comparable à la moins bonne des solutions en boucles, celle avec des processeurs simplex. Ceci conforte les hypothèses de choix des structures (§IV.1.1). En effet, doter la structure en bus de techniques de tolérance aux fautes est manifestement moins efficace que pour les boucles. Ces deux structures sans tolérance apparaissant comme équivalentes du point de

vue de la sûreté de fonctionnement (pour cette application du moins), on peut conclure qu'un bus à processeurs tolérants aux fautes n'atteindrait pas les performances de sûreté des deux autres solutions : boucles à processeurs tolérants aux fautes, et à proceseurs doubles.

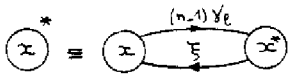
La comparaison entre ces deux dernières solutions montre que la structure à processeurs doubles est la meilleure lorsque le temps de réparation est de l'ordre de 20 heures. Pour des temps de 100 heures, la structure à processeurs tolérants l'emporte pour des facteurs de couverture supérieurs à 0,9 (à partir de 0,8 pour la sûreté dégradée).

Compte tenu de la plus grande importance de la sûreté nominale pour cette application, et de la difficulté de réalisation d'un processeur tolérant aux fautes avec un tel taux de couverture, nous pouvons donc retenir, à cette étape, la solution à processeurs doubles. Remarquons en particulier que cette solution va dans le sens du critère de simplicité, et facilite la mise en œuvre des procédures de gestion de la communication.

Il convient toutefois d'affiner cette analyse, en examinant l'influence du facteur de reconfiguration, c_i donnant la probabilité de réussite de la procédure de reconfiguration (prise égale à 1 dans le modèle précédent).

IV.1.6 Influence du facteur de reconfiguration

La prise en compte du facteur c_i conduit au modèle de la figure IV.10, qui diffère de celui de la figure IV.8 par la présence des états 3' et 4' et par la signification des transitions à partir des états 3 et 4 permettant de considérer l'échec de la reconfiguration, conduisant donc à la perte de la communication.



(1) Etat de bon fonctionnement

(2), (3) et (4) Perte d'une boucle suite à :

- (2) la défaillance d'une unité d'accès d'un processeur frontal
- (3) la défaillance d'un émetteur
- (4) la défaillance d'un récepteur

(5) Perte d'une station - reconfiguration réussie

(6) à (10) Perte de la communication suite à la défaillance de plusieurs stations

(11) à (17) Etats avec au moins une unité commune de réception défaillante

{x* = ouverture d'un disjoncteur supplémentaire}

(18) Ouverture de plusieurs disjoncteurs supplémentaires

(3') Défaillance d'un émetteur suivie de celle du récepteur de la même station sur l'autre boucle - reconfiguration réussie, aucune station n'est perdue

(4') Défaillance d'un récepteur suivie de celle de l'émetteur de la même station sur l'autre boucle

(Ces deux états peuvent être regroupés.)

Notations relatives à la figure IV.10

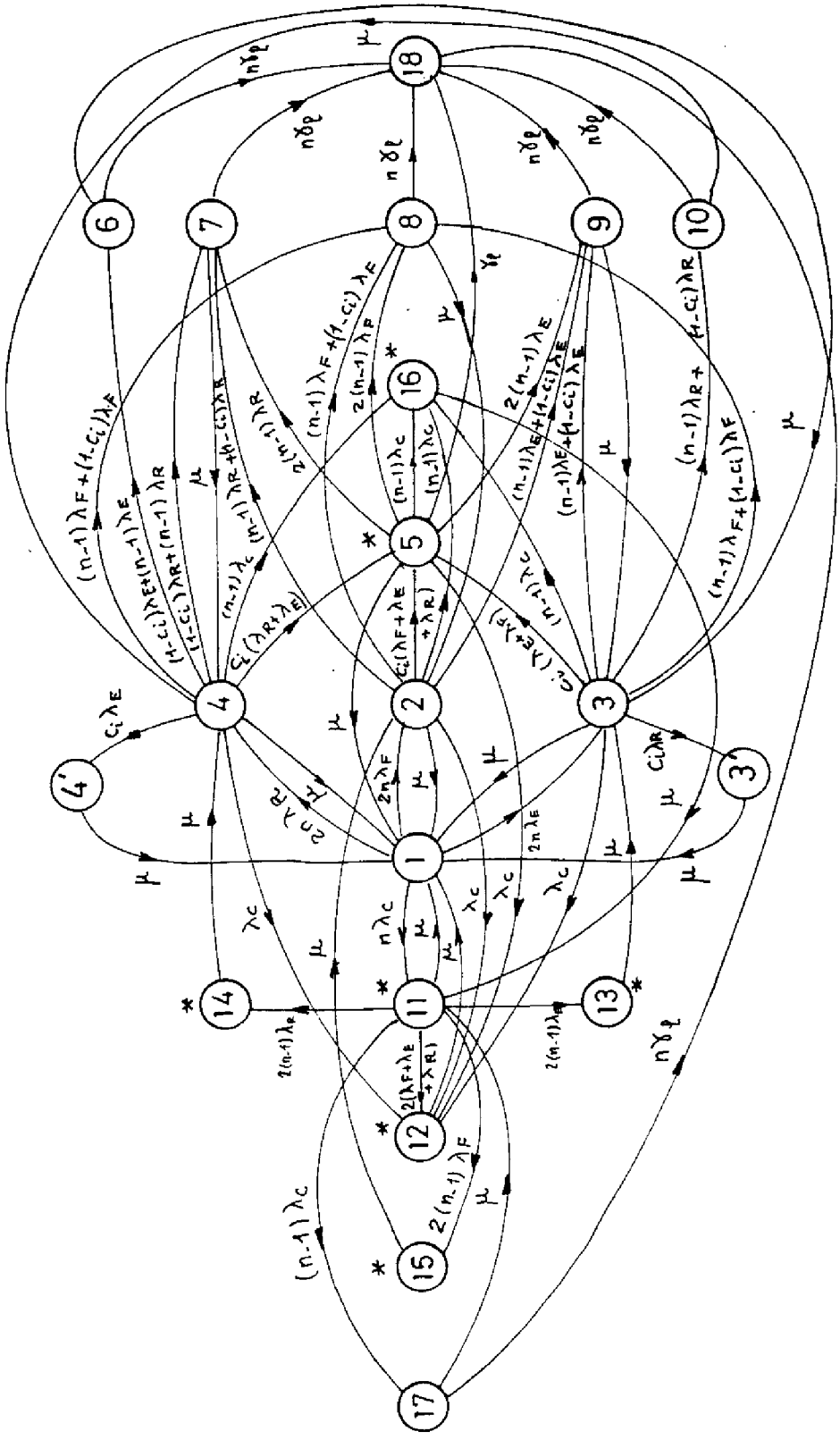


figure IV.10 : processeurs doubles ; influence du facteur de reconfiguration

Ce modèle permet d'obtenir les courbes de la figure IV.11 (a et b pour la sûreté nominale et dégradée).

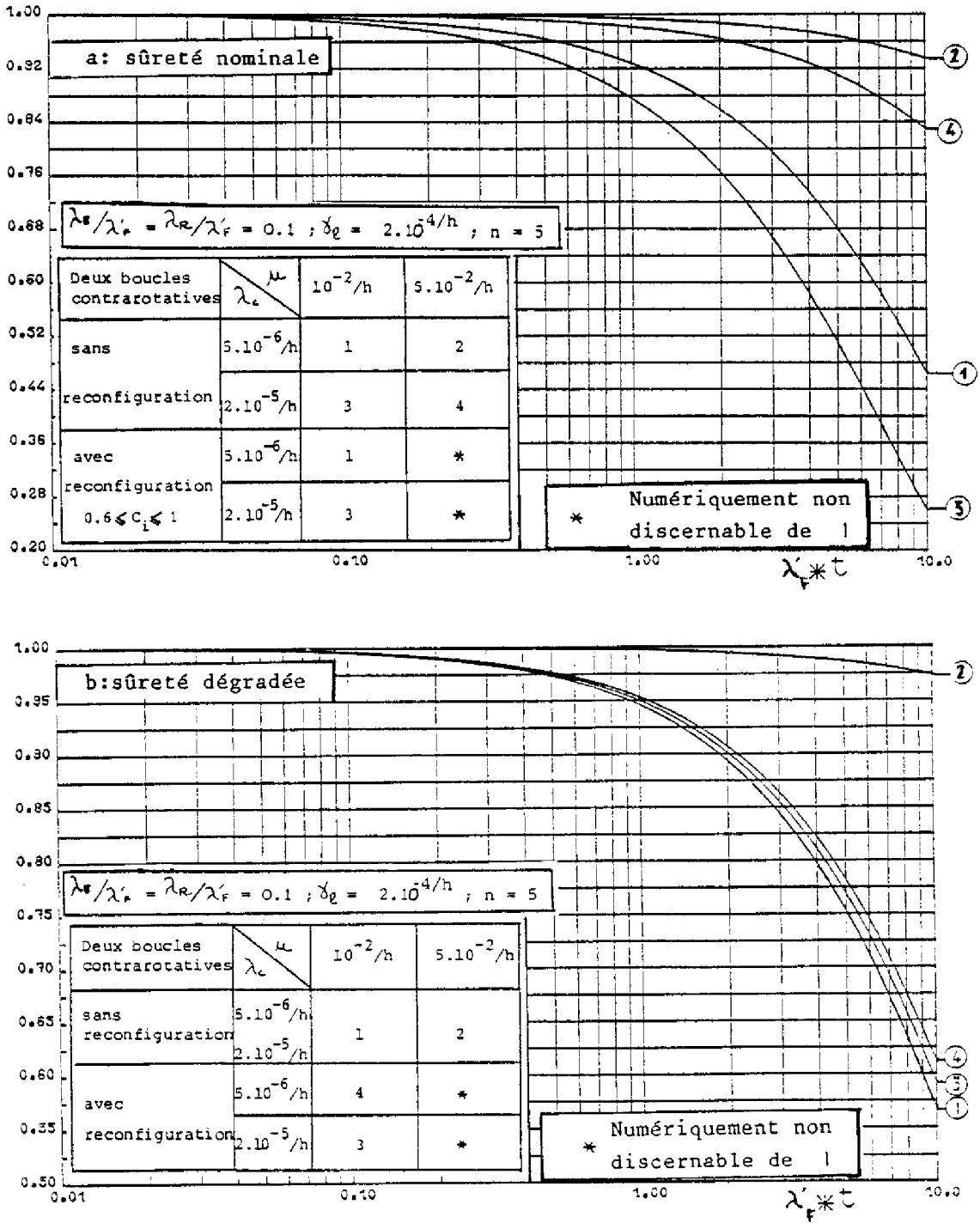


figure IV.11 : influence du facteur de reconfiguration

Il apparaît que la valeur exacte du facteur de reconfiguration a peu d'influence sur la sûreté, tant nominale que dégradée : les courbes obtenues

pour c_i variant entre 0,6 et 1 sont confondues, ce qui justifie a posteriori la comparaison du paragraphe précédent avec une valeur de 1.

Il serait tentant de conclure, au vu de ces courbes qu'en fait l'influence de la reconfiguration elle-même est assez faible, ce qui pourrait remettre en question l'adoption d'une telle procédure. Rappelons cependant qu'il s'agit d'une application de sécurité, pour laquelle il faut porter une attention particulière aux défaillances simples, même rares, entraînant l'événement catastrophique, ce qui est le cas des défaillances de mode commun qui avaient conduit à retenir le principe de la reconfiguration (§III.1.2.4). Les valeurs absolues fournies par le traitement des modèles n'est donc pas très significatif dans ce cas.

IV.1.7 Conclusion

L'évaluation de sûreté de fonctionnement conduit donc, d'une part à retenir, pour cette étape d'affinement, la solution en double boucle avec processeurs frontaux à deux unités d'accès indépendantes. Cette évaluation a permis d'autre part de justifier un certain nombre d'hypothèses préalables, la plus importante étant la non-prise en considération de processeurs tolérants aux fautes pour la structure en bus.

Naturellement, le choix définitif ne peut être effectué qu'après prise en compte de l'étude des procédures de transfert, en particulier à l'aide du critère retenu pour évaluer les performances fonctionnelles. Remarquons cependant que la solution obtenue est, au moins comparée aux autres solutions en boucles, celle qui est la moins susceptible d'être remise en cause, car elle permet une gestion indépendante par boucle, a priori plus simple qu'avec les autres structures. Néanmoins, il conviendra de vérifier la cohérence des choix, en s'assurant qu'il est effectivement possible, comme nous l'avons supposé dans ce paragraphe IV.1, de négliger les défaillances de l'unité commune en émission.

IV.2 PROCEDURES DE TRANSFERT

Dans ce paragraphe, nous étudions les procédures de transfert en affinant les choix effectués dans le chapitre III. A ce niveau de détail, nous pouvons effectuer une évaluation comparative des performances fonctionnelles significatives des solutions en présence. Cependant, nous utilisons également les critères qualitatifs relatifs à la sûreté de fonctionnement : essentiellement décentralisation et latence minimale ; ceci permet de se rapprocher le plus possible des hypothèses sur lesquelles est basée l'évaluation de sûreté de fonctionnement du paragraphe IV.1. En effet cette approche rend peu probable la présence de fautes non détectées au moment d'un défaut à traiter (en particulier de fautes de conception dans les procédures), et rend négligeables les conséquences de ces fautes sur l'ensemble du fonctionnement, comparées aux défaillances matérielles.

IV.2.1 Généralités

Le but est donc d'évaluer les performances fonctionnelles des solutions en présence, et en particulier la plus significative : l'aptitude à acheminer une rafale de messages de défaut en moins de trois millisecondes. Cette aptitude est liée aux quatre points suivants :

- composition d'une rafale de messages,
- "interface messages-paquets",
- traitement des paquets,
- acheminement des signaux sur le support de transmission.

Les deux derniers points relèvent directement de l'étude comparative des différentes procédures de transfert applicables sur les structures de transmission retenues. Cette étude nécessite donc :

- l'affinement préalable de la partie de la procédure de transfert commune à toutes les solutions : la constitution des paquets, ou interface messages-paquets,
- le choix d'hypothèses fixant l'utilisation du système (en particulier la composition des rafales), mais aussi les paramètres dont la connaissance exacte ne relève pas de ce niveau de détail (valeur du débit de transmission, des probabilités de défaillance ou d'erreurs de transmission, etc...).

IV.2.1.1 Constitution d'un paquet

Le choix s'est porté sur un format conforme à la trame HDLC (§III.2.1). Nous allons donc définir le contenu de cette trame, permettant d'identifier le(s) destinataire(s) du paquet, et éventuellement le paquet lui-même, et bien entendu de transporter les informations qui constituent l'essence du message : les **données.**

A priori, on a le choix entre des paquets de taille fixe ou variable. Bien qu'apportant une certaine souplesse, la deuxième solution ne sera pas retenue. En effet, l'adoption d'un format fixe rend beaucoup plus aisée et rapide la détection de certaines défaillances, et en particulier des défaillances les plus gênantes qui se traduisent par la pollution du support de communication. De plus, ceci va dans le sens d'une diminution de la latence : dans la mesure où moins de paramètres influent sur le comportement des différents éléments, il est plus facile d'activer toutes les parties de ces éléments.

Un paquet comporte un certain nombre d'octets d'identification et de données (nous raisonnons en octets -groupes de huit bits- conformément à la structure de la plupart des circuits de traitement de données, et de la trame HDLC elle-même).

Pour identifier une station parmi trente (hypothèse "maximale" retenue au chapitre I), cinq bits suffisent. Sur un octet, il reste alors plus de deux cents configurations, ce qui sera suffisant pour :

- autoriser une flexibilité suffisante sur le nombre de stations,
- permettre une identification plus précise, par exemple de la nature du paquet : défaut, service, éventuellement test,
- effectuer l'adressage de groupe et la diffusion.

Nous avons donc deux octets d'identification, auxquels nous en ajoutons un troisième destiné à identifier le paquet lui-même ; ceci permettra de mettre en place une procédure d'accusés de réception, et d'effectuer le diagnostic de certaines défaillances (pertes de paquets, duplications, paquets "parasites" en circulation permanente sur la boucle, etc...).

Le nombre d'octets de données est lié au nombre de paquets nécessaires pour transporter les informations d'un message, et à la quantité d'informations par message. Il est clair que ce dimensionnement doit essentiellement prendre en compte les caractéristiques des messages de défaut. Ceux-ci sont porteurs de très peu d'informations, qui peuvent être codées sur un seul octet ; nous retiendrons en fait une valeur de deux à trois octets, pour permettre une certaine flexibilité, et autoriser éventuellement un codage redondant de ces informations (en plus du CRC de la trame). Pour des raisons de rapidité, tant d'acheminement proprement dit que de traitement en émission et en réception, il est préférable de ne pas acheminer les messages de défaut sous forme de plusieurs paquets ; ceci étant compatible avec la faible quantité d'informations portées par ces messages, nous pouvons donc retenir des paquets comportant :

- quatre octets "de trame HDLC" : deux fanions, et deux octets de CRC,
- trois octets d'identification : identité de l'expéditeur, du ou des destinataire(s), et du paquet lui-même,
- deux à trois octets de données,

ce qui conduit à une dizaine d'octets.

Naturellement, ceci peut être assez pénalisant pour les messages de service, qui devront satisfaire le même format, et donc dans certains cas être répartis en plusieurs paquets émis à la suite, mais ce n'est pas gênant dans la mesure où les contraintes d'acheminement rapide ne concernent que les messages de défaut.

IV.2.1.2 Hypothèses de calcul

Le calcul des performances fonctionnelles nécessite la connaissance de la composition des rafales de messages à acheminer, élaborées à la suite de défauts à éliminer sur le réseau. Nous faisons l'hypothèse (pessimiste) que tous les messages d'une rafale sont prêts simultanément. Il s'agit d'une simplification, dans la mesure où n'est pas prise en compte la dispersion due aux instants différents de détection du défaut (période d'échantillonnage du réseau THT de 0,8 ms) et aux durées différentes de traitement.

Nous ne faisons pas d'hypothèse sur les messages (présence, nombre,...) de service ou de test en circulation au moment du défaut. Par contre nous admettons qu'il n'y a pas d'autre rafale ; nous ne tenons donc compte que d'un seul défaut pendant la durée retenue pour l'acheminement de la rafale.

Nous retenons donc des rafales de messages simultanés, composés d'au plus sept messages (§I.1.4.1) et nous faisons l'hypothèse -compatible avec la procédure actuelle d'élimination de défaut- que ces sept messages sont émis par sept stations distinctes.

Conformément au principe retenu au paragraphe II.2.2.1, nous ne tenons pas compte dans le calcul de performances des défaillances matérielles ou logicielles. Il n'en va pas de même pour les erreurs de transmission qui risquent de faire perdre des messages. L'objectif n'est cependant pas d'obtenir pour cette étape des mesures absolues des performances, mais de comparer des solutions en concurrence ; pour cela, il est suffisant de calculer dans un premier temps le temps d'acheminement sans tenir compte des erreurs de transmission, puis d'examiner ensuite leur influence sur les solutions qui restent en concurrence.

Le calcul nécessite la connaissance des possibilités d'acheminement offertes par les différentes structures de transmission retenues. En particulier, il faut déterminer le débit de transmission. Ce paramètre n'étant pas connu à ce niveau de détail, nous choisissons une valeur de référence, ce qui est suffisant pour comparer les solutions. D'après les contraintes examinées au paragraphe I.1.4.1, on peut retenir une valeur de 1 MHz, pour une première itération ; la valeur intervenant dans le calcul étant le débit de transfert, c'est à dire la fréquence des bits et non pas des transitions du signal physique, il faut tenir compte du code de transmission utilisé : en $NRZI_1$, le débit de transfert est de 1 Mbit/s, mais seulement 0,5 Mbit/s en "Manchester biphase". Dans un premier temps, nous adoptons donc la valeur la plus pessimiste, et nous supposons de plus qu'il est légitime de comparer les performances des différentes solutions avec la même valeur de débit de transmission, et le même code de transmission. Nous reviendrons sur cette hypothèse à l'issue de cette étape.

Dans ces conditions, la durée d'émission d'un paquet, notée $\mathbf{T_p}$, est donnée par le nombre de bits (10 octets, plus les bits de trame HDLC : au maximum un par groupe de 5 bits du paquet d'origine sans les fanions, soit 80 + 12) multiplié par la durée d'un bit (2.10^{-6}s), soit 184.10^{-6}s, valeur que nous majorons en prenant : $T_P = 200.\ 10^{-6}$ s.

Nous utiliserons de plus pour les calculs la notation N_s pour le nombre maximal de stations, que nous avons pris égal à 30, et N_d pour le nombre maximal de stations ayant un message de défaut à envoyer, c'est à dire 7.

IV.2.2 Procédures sur le bus

D'après l'étude générale du chapitre III, la caractéristique essentielle de la structure en voie multipoint est la durée maximale de propagation des signaux, que nous notons $\mathbf{T_{bus}}$. Sur le support retenu, cette valeur correspond

à deux fois le temps de parcours de la plus longue distance station-coupleur, que nous prenons égale à 500 mètres ; nous obtenons donc pour une vitesse de propagation des signaux optiques de 2.10^8 m/s (indice de réfraction de la fibre de 1,5) :

$$T_{bus} = 5.\ 10^{-6}\ s.$$

A l'issue du chapitre III, nous avons adopté le principe d'un accès par compétition, avec détection de conflit par écoute d'interférence. Il faut donc étudier la procédure d'ajournement, et celle de résolution de conflit.

En fait, la technique d'émission sourde ayant été rejetée, la résolution des conflits repose sur l'ajournement des paquets : en général, ajournement de tous les paquets (détection "multilatérale" de conflit), ou bien ajournement de tous les paquets sauf un, émis correctement (détection "unilatérale" de conflit, correspondant à la méthode d'accès par forçage). Nous allons donc commencer par étudier les différentes techniques utilisables pour ajourner un paquet, que cet ajournement soit dû à l'occupation de la voie ou à un conflit.

IV.2.2.1 Techniques d'ajournement

Nous avons vu (§III.2.2.2) que la procédure suivie par une station en ajournement de paquet pouvait, comme la procédure d'accès, reposer sur la sélection ou la compétition. Une étude plus détaillée conduit à distinguer les techniques "persistantes" et "non-persistantes" /LUC'78/.

On appelle **non-persistante** la technique consistant à renoncer provisoirement à émettre un paquet ajourné, pour faire une nouvelle tentative ultérieurement, généralement au bout d'un délai aléatoire. Il paut s'agir d'une technique **adaptative** (les délais d'ajournement tiennent compte de la charge du support), ou **non-adaptative**.

Par opposition, les techniques **persistantes** consistent à rester à l'écoute du support, pour détecter le moment où il se libère.

IV.2.2.2 Solutions possibles

D'après les conclusions du chapitre III, nous devons retenir une méthode d'accès par compétition, soit par forçage, soit avec ajournement de **tous** les paquets en conflit.

Avec la méthode par forçage, les conflits étant automatiquement résolus, on voit qu'il est inutile de chercher à diminuer la fréquence d'occurrence des conflits à la libération du support. La solution permettant de tirer le meilleur parti de la capacité du support consiste donc à utiliser une procédure d'ajournement **persistante**. Les paquets successifs ne sont alors séparés que par une durée au plus égale à T_{bus}.

Pour les méthodes basées sur l'ajournement de tous les paquets en conflit (**détection multilatérale**), on peut envisager a priori plusieurs possibilités. Les techniques persistantes ne sont applicables que lorsqu'il y a toujours un

paquet qui sort vainqueur du conflit (forçage), ou à très faible charge (la probabilité que plusieurs stations aient simultanément des paquets prêts est très faible, même après une période d'occupation du support). Ces solutions ne conviennent donc pas à un système destiné à acheminer des rafales de messages simultanés.

En conséquence, nous retenons, pour en étudier les performances dans la suite de ce paragraphe, les techniques suivantes :

- accès par forçage persistant,
- détection multilatérale avec ajournement :
  * non-persistant,
  * persistant à délais **déterministes** ou **aléatoires.**

IV.2.2.3 Accès par forçage

La figure IV.12 donne sur un chronogramme un exemple d'accès au support, dans lequel nous avons supposé pour le clarifier que le temps de propagation T_{bus} était très petit devant la durée d'un bit, notée T_{bit}.

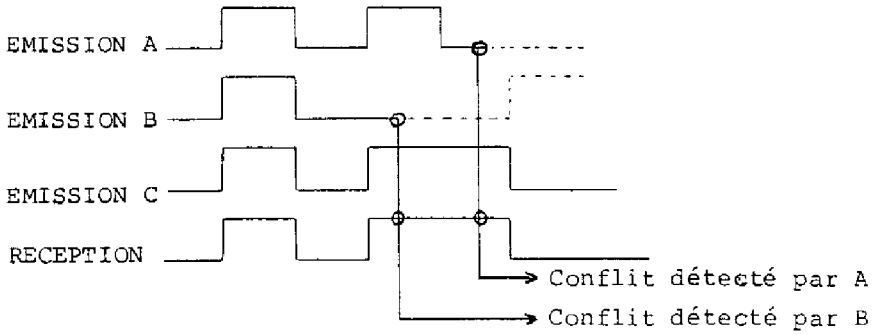


figure IV.12 : accès par forçage

On montre /POW'81/ que cette technique est applicable si T_{bit} est au moins deux fois plus grand que T_{bus}, ce qui donne ici une valeur minimale de 10 microsecondes soit un débit de transfert maximal de 100 kHz, cinq fois plus faible que celui que nous nous étions donné.

Précisons que, la technique de forçage reposant sur la priorité d'une valeur logique sur l'autre, on ne peut utiliser que des codes basés sur des niveaux et non sur des transitions. Ceci conduit donc à certains aménagements de la procédure, de façon à constituer un en-tête spécifique réalisant la configuration de forçage indépendamment du paquet lui-même qui peut utiliser le code Manchester biphase, éventuellement avec un débit différent de celui qui a servi à émettre l'en-tête.

Le plus simple serait naturellement d'utiliser le même débit, mais on ne peut alors émettre que 300 bits en 3 ms, soit moins de 4 paquets, ce qui est nettement insuffisant.

Il faut donc, malgré la plus grande complexité, utiliser deux fréquences d'horloge distinctes, une pour l'émission de l'en-tête et une autre pour le reste du paquet.

L'en-tête doit comporter, après un premier bit à 1 pour indiquer l'occupation du support, une configuration distincte pour chaque station et pour chaque classe de priorité. Si nous réservons une classe de priorité plus élevée pour les paquets de défaut, il nous faut 5 bits pour différencier les 30 stations, précédés par 1 bit de priorité, soit en tout au moins 7 bits.

Nous obtenons donc $7*T_{bit}+ T_P$ par paquet, valeur à laquelle il faut ajouter l'espacement entre paquets (qui peut atteindre T_{bus} : 5.10^{-6}s), ce qui donne un total de 275.10^{-6}s. En tenant compte de l'existence d'un paquet de service au moment de l'élaboration d'une rafale de défaut, le dernier paquet de cette rafale est émis au bout de $(N_d+ 1)* 275.10^{-6}$s, et reçu 5.10^{-6}s plus tard, soit en tout : 2205.10^{-6}s.

Nous pouvons donc retenir qu'une rafale de défaut est entièrement acheminée en moins de 2,3 ms, ce qui est conforme à la contrainte fixée.

En ce qui concerne les messages de service, le taux d'occupation utile maximal dont ils peuvent disposer en l'absence de défaut est de 200/275 (durée théorique du paquet / occupation effective), soit 70%.

IV.2.2.4 Ajournement persistant à délais déterministes

Pour éviter les conflits à la libération du support, on oblige alors chaque station en ajournement à attendre un certain temps avant de faire un nouvel essai. Il n'y a pas de conflit si le premier délai qui vient à expiration précède le suivant d'au moins T_{bus}, ce qui conduit à affecter à chaque station un délai propre, tous ces délais différant au moins de T_{bus}. (Il faudrait naturellement faire circuler ces délais de façon à éviter l'instauration d'une priorité fixe entre les stations).

Il faut remarquer que cette technique s'apparente à l'accès par gestion d'anneau virtuel vue au paragraphe III.2.2.1, la seule différence étant que si le support est libre, toutes les stations peuvent essayer d'émettre indépendamment des autres, ou d'un quelconque droit, matérialisé ou non.

Pour calculer le temps d'acheminement d'une rafale, il faut considérer que dans le pire des cas, nous avons l'espacement maximal entre paquets, soit $N_s* T_{bus}$ (théoriquement, on pourrait considérer des valeurs un peu plus faibles, puisque tous les paquets de la rafale sont prêts simultanément). En tenant compte des N_d paquets de défaut, d'un paquet de service en cours de circulation, le dernier paquet de la rafale est entièrement émis au bout de $T_P+ N_d* (N_s* T_{bus}+ T_P)$, et acheminé en même temps que la rafale complète, T_{bus} après, soit au total : 2555.10^{-6}s.

Avec cette méthode, il est donc possible d'acheminer une rafale de défaut en moins de 2,6 ms.

En l'absence de défaut, les paquets de service sont au moins séparés par $N_s * T_{bus}$ ($=150.10^{-6}$s), correspondant aux intervalles réservés aux paquets de défaut, soit un taux d'occupation maximal de l'ordre de 200/350 = 57%.

Il faut cependant tenir compte, de même d'ailleurs que pour la méthode par forçage (§IV.2.2.3), de la difficulté de réaliser un algorithme permettant à chaque station de déterminer de façon autonome quel est l'intervalle qui lui est alloué.

Pour cela, il existe des solutions basées par exemple sur l'utilisation de N_s^2 classes de priorités, c'est à dire N_s classes constituées de N_s sous-classes. Chaque station possède une priorité (éventuellement fixe) dans chaque sous-classe, et utilise une classe de priorité d'autant plus élevée que le paquet à émettre a subi un grand nombre d'ajournements. On montre /POW'81/ que l'on obtient ainsi, avec un algorithme n'utilisant que des variables locales, un système de priorités circulantes garantissant un temps d'accès borné... mais long : avec l'ajournement par délais déterministes, l'espacement moyen entre paquets est alors de $(N_s^2 * T_{bus})/2$, soit plus de 2 ms. (La perte de temps est moins considérable pour la méthode par forçage, où la longueur de l'en-tête est proportionnelle au logarithme du nombre de classes de priorités).

IV.2.2.5 Ajournement à délais aléatoires

On peut envisager un ajournement persistant, ou non, mais on ne retiendra a priori que la possibilité d'utiliser la même technique pour tous les paquets ajournés, que ce soit à la suite d'un conflit ou de l'occupation du support ; ceci permet en effet de simplifier la procédure, et de diminuer la latence.

Avec une technique persistante, le délai aléatoire est armé par chaque station en ajournement au moment de la libération du support, alors qu'avec la technique non-persistante, il est armé à chaque essai échoué, indépendamment de l'instant d'observation de la libération du support. Ces deux solutions sont donc assez semblables, et l'on voit qu'en jouant sur la loi de probabilité des délais, on pourra obtenir des comportements analogues. La solution persistante, qui est en général choisie (Ethernet, par exemple), permet, grâce à la synchronisation du lancement de la procédure d'accès après ajournement, de mettre plus facilement en œuvre diverses stratégies adaptatives.

Avec la technique non-persistante, le délai entre la libération du support et le nouvel essai d'une station en ajournement dépend de l'instant auquel l'essai précédent avait été effectué, et donc des résultats des tirages antérieurs du délai aléatoire. Par exemple, avec une loi uniformément distribuée entre 0 et une valeur notée TM, la probabilité de faire une nouvelle tentative au bout d'un temps t après la libération du support n'est pas uniformément distribuée, mais décroît quand t varie de 0 à TM. Cette décroissance est d'autant plus marquée que le paquet ajourné est prêt depuis plus longtemps : une station a donc d'autant plus de chances de pouvoir émettre son paquet

qu'elle a dû l'ajourner souvent, puisqu'alors son délai moyen est plus court que celui des stations ayant effectué moins de tentatives.

Cette procédure a donc de façon naturelle un comportement adaptatif. Mais il faut noter que dans le cas général ce comportement est globalement plutôt néfaste, car il conduit à diminuer la valeur moyenne des délais à forte charge, et donc à augmenter la probabilité de conflit. Cette solution est cependant bien adaptée à notre application, car on peut considérer que le nombre de stations en compétition (en faisant abstraction des messages de service) décroît au fur et à mesure que la rafale s'écoule.

Nous pouvons donc retenir, pour cette application précise, cette solution. Pour garantir un passage privilégié aux messages de défaut, le plus simple est de leur accorder un délai aléatoire, par exemple uniformément distribué entre 0 et une valeur notée T_D, les messages de service disposant d'un délai entre T_D et une valeur supérieure, notée T_S. Il n'est bien-sûr pas possible de calculer la valeur maximale du temps de passage d'une rafale de N_D messages de défaut, ce temps n'étant pas borné. Ce non-déterminisme n'est cependant pas rédhibitoire, si l'on peut montrer que la probabilité que ce temps soit supérieur à 3 ms est, par exemple, du même ordre de grandeur que la probabilité de défaillance pour une autre solution, apparemment déterministe.

Une étude par simulation de cette procédure /BOU'80b/ a permis de montrer que la valeur optimale pour T_D était de l'ordre de 100.10^{-6}s (avec des valeurs de 5.10^{-6}s et 200.10^{-6}s pour T_{bus} et T_P), conduisant alors à un temps d'écoulement moyen de rafale de 1,72 ms avec un faible écart-type (0,12 ms). En ajoutant la durée d'un éventuel message de service en cours au moment du défaut, on peut donc retenir, à ce niveau de détail, une valeur de l'ordre de 2,2 ms (en ajoutant deux fois l'écart-type).

Seule une étude plus approfondie pourrait fournir le paramètre réellement significatif, qui est la probabilité de dépasser la valeur limite de 3 ms, mais une telle étude ne se justifie pas au niveau de détail considéré dans ce chapitre. Nous pouvons donc, à cette étape, retenir cette solution, en particulier pour sa simplicité, et ses caractéristiques de décentralisation. Il faut toutefois remarquer que :

- une station possédant un délai (déréglé) trop court acquiert une priorité de fait,
- l'existence d'un double délai augmente la latence,
- les performances relatives aux messages de services sont médiocres, puisqu'il y a un délai d'au moins T_D entre ces messages, sans même tenir compte de la valeur exacte des délais et des possibilités de conflit (soit un taux d'occupation inférieur à 67%).

IV.2.3 Procédures sur les boucles

Pour les mêmes raisons que dans le chapitre III, nous nous limitons ici à l'étude de la procédure sur une seule boucle. Nous prenons pour cette

structure un espacement moyen entre stations de 200 mètres, ce qui donne un temps de parcours des liaisons, noté T_L, de 10^{-6}s. Le temps de parcours de la boucle dépend aussi du temps de traversée des processeurs frontaux dans chaque station, noté T_{pf}. Ce temps n'est pas nécessairement très long, car les stations n'ont pas de traitement autre que la régénération à effectuer sur les signaux qui les traversent. En effet les paquets, du fait qu'ils peuvent avoir plusieurs destinataires, ne peuvent être extraits de la boucle que par la station qui les a émis, après un tour complet (on suppose que cette station possède le moyen de reconnaître son propre paquet dès son arrivée). Il n'y a donc pas de raison de stocker les signaux reçus un certain temps avant de les réémettre, et T_{pf} sera limité à la durée nécessaire pour détecter un bit, le régénérer et l'émettre. Nous prenons donc $T_{pf} = T_{bit}$.

Le temps total de parcours d'une boucle est alors $T_{bou} = N_s * (T_L + T_{pf})$, soit 90.10^{-6}s.

IV.2.3.1 Accès par compétition

Comme nous l'avons vu au chapitre III, il est tout à fait possible d'envisager, a priori, un accès par compétition sur une boucle. C'est en particulier la solution adoptée dans /HAL'82/, où une station qui désire émettre envoie un signal distinctif (son adresse) sur le support si celui-ci lui paraît libre. Si le signal accomplit le tour complet et lui revient, c'est qu'aucune autre station ne tente une émisssion. Elle peut alors envoyer son message.

Cependant il faut tenir compte du fait que le délai de propagation est dans notre cas près de 20 fois supérieur à celui caractérisant le bus étudié au paragraphe IV.2.2. La transposition des résultats précédents montre alors que la procédure d'accès par compétition n'est pas utilisable sur la structure en boucle pour cette application.

Nous nous limitons donc aux autres possibilités retenues dans les conclusions du chapitre III : solutions par sélection, avec droit d'émettre, et sélection asynchrone par insertion de registre.

IV.2.3.2 Accès par droit d'émettre

Deux techniques relèvent de cette approche : jeton et trame circulant(e).

jeton circulant : Si nous supposons par exemple qu'après chaque émission de paquet, on laisse le jeton faire un tour complet où il n'est utilisable que pour des paquets de défaut, une station quelconque voit passer le "jeton de défaut" ou un paquet de défaut, au maximum au bout de $T_p + T_{bou}$. La dernière station qui peut émettre son paquet de défaut commence donc au plus tard au bout de $(N_d - 1) * T_p + T_p + T_{bou}$, et termine T_p après, ce paquet étant reçu par toutes les stations T_{bou} après (en négligeant la durée du signal matérialisant le jeton). Le temps d'acheminement de la rafale est donc au maximum $(N_d + 1) * T_p + 2 * T_{bou}$, soit : 1880.10^{-6}s. Nous pouvons donc retenir une valeur inférieure à 2 ms. L'espacement entre paquets de service est de l'ordre de T_{bou} (plus exactement $T_{bou} + (1/N_s) * T_{bou}$), soit un taux d'occupation de $200/(200+90+3) = 68\%$.

trame circulante : Si l'on réserve q_d tranches, sur un total de q_s, pour des paquets de défaut, une station voit passer une "tranche de défaut" libre au maximum au bout de $(N_d/q_d) * T_T$, si l'on note T_T la durée totale d'un tour qui vaut ici $q_s * T_p$. Les N_d stations ont alors pu commencer à émettre, et la rafale est entièrement acheminée au bout de $(N_d/q_d) * T_T + T_p + T_T$, ce qui donne $(N_d*(q_s/q_d) + q_s + 1) * T_p$, dont la valeur minimale est obtenue, si nous imposons $q_s > q_d$, pour $q_s=4$ et $q_d=3$: $((4/3)*N_d + 5) * T_p = 2867.10^{-6}$s. Nous avons donc une valeur un peu élevée, de 2,9 ms, avec un taux d'occupation de 25% (une tranche de service sur quatre). Il faut ajouter à cela la nécessité de ralentir les signaux dans chaque station pour faire tenir la trame dans la durée du tour ($T_p > T_{bou}$), ce qui accroît encore la vulnérabilité intrinsèque de cette procédure, due à la nécessité de maintenir la synchronisation de trame.

IV.2.3.4 Accès asynchrone par insertion de registre

Cette méthode offre une meilleure décentralisation que le jeton circulant, et a fortiori que la trame circulante, les stations ayant une entière autonomie à l'émission. Cependant à forte charge, toutes les stations peuvent être en phase d'émission, et un paquet doit alors traverser dans chaque station le registre que celle-ci a inséré. Il faut donc ajouter la longueur de ce registre, T_p (durée d'un paquet), à T_{pf}, ce qui porte la durée maximale du tour à $N_s * (T_L + T_{pf} + T_p)$, soit 6 ms.

Pour satisfaire la contrainte d'acheminement de rafale de défaut, on peut soit augmenter le débit, soit diminuer le nombre de paquets de service en circulation simultanée. C'est cette dernière solution que nous retenons ici, au moins dans un premier temps, afin de conserver les éléments de comparaison avec les autres techniques.

Il faut donc utiliser un accès par sélection pour les paquets de service, la solution la plus simple étant un jeton circulant. Dans ces conditions, moyennant certaines précautions dans la gestion du jeton /BLA'81/, on peut garantir qu'un paquet de défaut ne traverse pas plus d'une station émettrice d'un paquet de service. Le temps de passage de la rafale est alors $T_{bou} + (N_d + 2) * T_p$, soit 1890.10^{-6}s.

Cette méthode permet donc d'acheminer une rafale en 1,9 ms, avec un excellent taux d'occupation, puisqu'en l'absence de défaut, les paquets peuvent se succéder au temps près de passage du jeton d'une station à sa voisine. Nous pouvons adopter, en première approximation pour ce taux, une valeur de l'ordre de 90%, ce qui correspond à une durée de 20 microsecondes pour le passage du jeton. Il faut de plus remarquer que les paquets de défaut ne sont pas ralentis par la perte éventuelle du jeton, et que s'il y a une double procédure -ce qui nuit à la simplicité et à la latence- les deux parties de la procédure sont très semblables : tous les paquets utilisent la même technique d'insertion du même registre ; seul le mécanisme de détection du droit d'insérer est spécifique du type de paquet.

Remarques : Nous avons effectué une étude plus détaillée de cette solution dans /BLA'81/, dont seuls les résultats essentiels relèvent du niveau de détail considéré dans ce chapitre IV. Nous montrons en particulier que la valeur maximale du temps d'acheminement d'un paquet n'est pas obtenue pour une station déjà en émission d'un paquet de service au moment du défaut, bien qu'alors il lui faille attendre la libération de son registre avant de pouvoir émettre le paquet de défaut.

En ce qui concerne les précautions relatives à la gestion du jeton, il s'agit en fait d'empêcher qu'un paquet de défaut, qui se trouve toujours derrière le jeton, ne soit retardé par toutes les stations qui reçoivent ce jeton et émettent un paquet de service. Il est possible ici d'inhiber le passage du jeton en présence de défaut, car la durée du tour est plus faible que celle du paquet, ce qui fait qu'en l'absence de défaut, une station qui émet un paquet de service en voit revenir le début avant d'avoir fini de l'émettre entièrement, et donc avant d'avoir décidé de réémettre le jeton.

IV.2.4 Comparaison

Les principaux résultats de cette étude sont résumés dans le tableau de la figure IV.13.

TAUX D'OCCUPATION (MESSAGES DE SERVICE) / TEMPS D'ACHEMINEMENT D'UNE RAFALE (ms)					OBSERVATIONS (PRINCIPAUX INCONVENIENTS)
BUS	ajournement unilatéral (forçage)		2,3	70%	double fréquence d'émission
					gestion des priorités
	ajournement à délais	déterministes	2,6	57%	synchronisme
		aléatoires	2,2	<60%	valeurs non déterministes
BOUCLES	signal circulant	jeton	1,9	68%	vulnérabilité (synchronisme)
		trame	2,9	25%	
	accès asynchrone	insertion de registre	1,9	90%	double procédure

figure IV.13 : tableau comparatif des procédures

On voit donc que deux solutions se dégagent :
- bus avec accès par compétition, non-persistant à délais aléatoires,
- boucles avec accès asynchrone par insertion de registre.

A l'issue de cette étape, il est tentant de comparer entre elles ces deux

solutions. On peut en particulier noter que si les temps d'acheminement de rafales sont équivalents, il ne s'agit pas d'une valeur déterministe dans le cas du bus. Toutefois, le déterminisme n'est qu'apparent pour les boucles, la probabilité de défaillance n'étant jamais nulle. Nous nous gardons donc d'utiliser un tel argument à ce niveau de détail.

Si la procédure pour les boucles offre un meilleur taux d'occupation pour les paquets de service, elle paraît conduire à une latence un peu plus élevée (quoique, en toute rigueur, la technique d'accès sur le bus est également double).

Les performances de flexibilité et de décentralisation -au moins pour les paquets de défaut- sont équivalentes, et la complexité logicielle de la solution sur boucles est à mettre en balance avec la complexité prévisible de réalisation matérielle de la solution en bus (en particulier, détection des conflits avec un mauvais rapport signal sur bruit).

Il faut de plus revenir sur les hypothèses faites au début de cette étape : influence des erreurs de transmission, valeur du débit, et composition des rafales. (La prise en compte des autres types de défaillances, et en particulier le fait que sur le bus les stations interviennent moins dans l'ensemble de la communication, ne relève pas de cette analyse ; ceci a été considéré dans le paragraphe IV.2).

Erreurs de transmission : la structure en boucles permet à la station expéditrice d'en détecter la plupart, par comparaison entre le paquet qu'elle reçoit au bout d'un tour et celui qu'elle avait émis, ce qui est l'équivalent d'un accusé de réception au niveau transmission. Il est ainsi possible de prévoir une procédure de réémission des paquets erronés beaucoup plus facilement sur cette structure que sur le bus. Cet argument doit cependant être pondéré par :

- la fréquence d'occurrence des erreurs de transmission : elles devraient être plus nombreuses sur le bus, à cause du rapport signal sur bruit, mais il faut tenir compte du matériel traversé :
  - * bus : N_s*(récepteur + liaison de 500m), plus un émetteur et une liaison, plus le coupleur et les connecteurs qui y sont raccordés,
  - * boucle : N_s*(récepteur + processeur frontal + émetteur + liaison de 200m),
- la prise en compte de leurs conséquences : dans le cas de la boucle, une erreur rend le paquet inutilisable pour toutes les stations situées en aval, soit un nombre quelconque de valeur moyenne $N_s/2$; sur le bus, une erreur en amont du (ou dans le) coupleur affectera toutes les stations, alors que les autres erreurs (les plus probables car le rapport signal sur bruit n'est mauvais qu'en aval) n'affecteront qu'une station.

Débit : le recours à un code tel que le "Manchester biphase" est surtout justifié pour le bus, à cause de la faible intensité des signaux et de la

nécessité de détecter les conflits d'accès. Il en va de même pour la fréquence de transmission, et on considère généralement qu'à débit égal, la réalisation technologique d'un bus géré par compétition est plus complexe qu'une boucle (gérée par sélection) /SAL'81/, ou à l'inverse qu'il est légitime de comparer, par exemple, un bus à 3 MHz et une boucle à 10 MHz /BLA'82/. Ceci montre que l'on dispose d'une certaine marge sur le débit applicable à la structure en boucles (au moins un facteur 2 en adoptant le code $NRZI_1$) sans remettre en cause fondamentalement le principe de la comparaison de ces deux solutions. Cette marge de débit peut en particulier être exploitée pour éviter l'utilisation d'un jeton circulant pour les paquets de service, ainsi qu'il était suggéré au paragraphe IV.2.3.3.

Composition des rafales : une augmentation du nombre de paquets par rafale est plus néfaste pour l'accès par compétition que pour l'insertion de registre. En effet, l'augmentation des temps de passage n'est pas linéaire pour le premier, à cause de l'augmentation de la probabilité de conflit. Par contre la possibilité qu'une station ait plusieurs paquets distincts à émettre dans la même rafale ne change rien pour la procédure par compétition (seul le nombre de paquets intervient), alors qu'il faudrait reprendre partiellement l'étude pour la solution par insertion de registre.

IV.3 CONCLUSION

Il ressort de cette étape d'affinement que l'ensemble des critères retenus permet de converger vers une solution à deux boucles contrarotatives. La communication est gérée de façon asynchrone dans chaque processeur frontal par insertion de registre, indépendamment sur chaque boucle par une unité d'accès spécifique (il y a donc deux unités d'accès dans chaque processeur frontal, une pour chaque boucle).

La synthèse des choix de transmission et de transfert permet ainsi de retenir cette structure :

- offrant une meilleure sûreté (d'après la mesure de sûreté retenue comme significative pour notre application) que la structure en bus pour un coût, une simplicité et une flexibilité comparables,
- pouvant être gérée par une procédure de transfert aux performances fonctionnelles satisfaisantes, caractérisée en particulier par la simplicité de l'accès au support, et surtout l'indépendance des stations dans leur accès au support.

Le chapitre suivant est consacré à un affinement supplémentaire destiné en particulier à vérifier la faisabilité de la solution proposée : **REBECCA** (**RE**seau en **B**oucl**E**s **C**ontrarotatives pour la **C**ommande d'**A**utomatismes), qui se révèle mieux adaptée que les solutions plus traditionnelles (essentiellement les solutions par compétition sur un bus, ou par jeton sur un bus ou une boucle) pour cette application, ou plus généralement tous les systèmes caractérisés par un régime de rafales très rares, mais nécessitant un traitement "immédiat", superposé à un régime permanent beaucoup moins contraignant.

CHAPITRE V : SOLUTION RETENUE : REBECCA

Dans ce chapitre, nous effectuons un dernier affinement de la solution retenue. L'objectif n'étant pas de définir un cahier des charges pour la réalisation d'un tel système, nous nous limitons aux niveaux de détail suffisants pour se convaincre de sa faisabilité, et de sa conformité aux objectifs initiaux.

V.1 PRINCIPES GENERAUX

La solution retenue consiste en une double boucle contrarotative en fibres optiques, selon le schéma de la figure V.1. Les processeurs frontaux comprennent deux unités d'accès assurant indépendamment l'une de l'autre la gestion de la communication sur une boucle, selon une méthode d'accès asynchrone, utilisant la technique de l'insertion de registre.

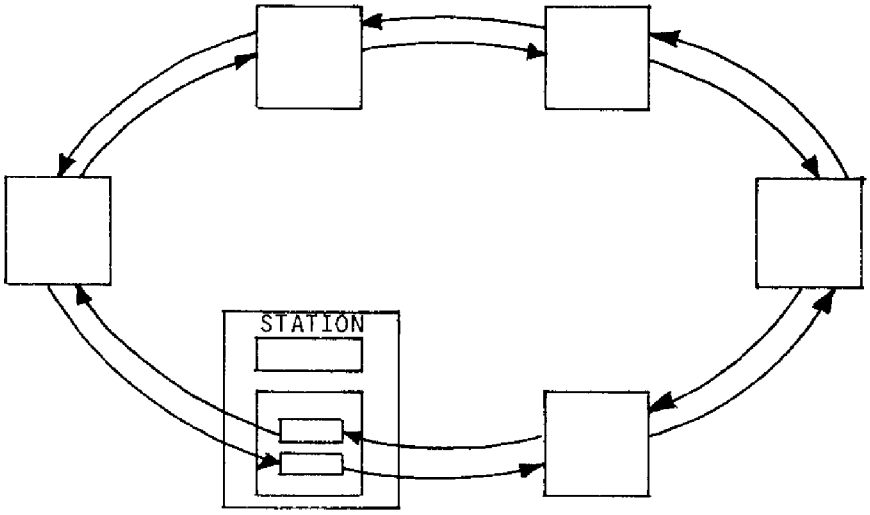


figure V.1 : structure du support

V.1.1 Accès asynchrone par insertion de registre

L'accès à une boucle repose sur la possibilité d'éviter les conflits en stockant les éventuels signaux reçus pendant l'émission d'un paquet d'origine locale. Il suffit donc de pouvoir :

- détecter un instant opportun (fin de paquet) pour interrompre la transmission directe,
- insérer dans la boucle une capacité de mémorisation au moins égale à la longueur du paquet à émettre.

Il convient de détailler l'utilisation que nous faisons de cette technique, proposée par Hafner et al. en 1974 /HAF'74/, et en particulier de souligner les différences fondamentales par rapport aux utilisations habituelles de cette technique (la plus connue étant celle de l'Université d'Ohio : DLCN

/REA'75,LIU'81/). Les choix de principe -et donc les différences fondamentales éventuelles- tiennent essentiellement dans la taille des registres, et dans l'extraction des signaux.

V.1.1.1 Taille des registres

Nous utilisons ici des registres de la taille d'un seul paquet. Il n'est donc pas possible d'émettre des paquets de taille variable, ni d'émettre un nouveau paquet avant que le registre n'ait été libéré.

Les raisons de ce choix sont liées :

- à la simplicité (objectif de sûreté de fonctionnement) : un registre de taille fixe est plus facile à réaliser, à gérer, et à surveiller,
- à la décentralisation : l'intervention d'une station dans l'ensemble de la communication est beaucoup plus faible,
- au temps d'acheminement : le temps d'accès est en moyenne plus long qu'avec un registre de taille variable, puisqu'il faut attendre plus souvent la libération du registre, mais le temps d'acheminement peut être borné par une valeur beaucoup plus faible (de l'ordre de la durée de traversée des registres multipliée par le nombre de stations).

Remarque : Dans ce cas, les deux types de priorité que l'on peut envisager pour cette méthode /BUX'83/ :

- émission de paquet si et seulement si le registre n'est pas plein,
- émission de paquet si et seulement si le registre est vide,

sont équivalentes.

V.1.1.2 Extraction des signaux

Le support étant rebouclé, les signaux qui ont été placés sur ce support doivent être extraits. Cette extraction peut être confiée à l'expéditeur ou au destinataire du paquet. Comme nous l'avons vu dans les chapitres précédents, nous utilisons la technique de l'extraction par l'expéditeur, qui permet, par opposition à l'extraction par le destinataire :

- d'envoyer des paquets à plusieurs destinataires,
- de disposer de l'équivalent d'un accusé de réception (au niveau "transmission").

Avec la technique d'insertion de registre, l'extraction par l'expéditeur offre de plus l'avantage :

- d'accroître l'autonomie des stations, qui ne dépendent pas du bon fonctionnement du destinataire de leur paquet pour la libération de leur registre et leurs possibilités ultérieures d'émission,
- d'augmenter la décentralisation en diminuant l'intervention de chaque station dans la communication.

En particulier pour ce dernier point, on peut utiliser le fait que la station expéditrice a nécessairement inséré son registre ; ceci permet d'éviter de devoir systématiquement stocker les paquets reçus pour en lire les identificateurs avant de les réémettre (conformément à l'hypothèse du paragraphe IV.2.3). En effet, quand des signaux parviennent à une station en phase d'émission, celle-ci dispose de toute la durée de traversée de ce

registre, c'est-à-dire la durée de son paquet, avant de devoir décider de réémettre ou non ces signaux. Elle peut donc extraire les signaux qui correspondent à son propre paquet au bout d'un tour, en extrayant son registre une fois que celui-ci contient le paquet entier, c'est-à-dire en rétablissant le trajet direct entre son récepteur et son émetteur.

Nous voyons que de cette façon, il est possible de rendre très faible l'intervention des stations en établissant un trajet minimal :

Récepteur —> Dispositif de régénération —> Emetteur,

correspondant aux stations qui ne sont pas en phase d'émission. Ce trajet permet de contourner la majeure partie de la station, et l'on peut doter le processeur frontal de mécanismes de surveillance permettant de forcer le passage par ce trajet (en cas de détection de défaillance, ou de durée d'insertion trop longue, puisque grâce à la petite taille des registres, la durée du tour est bornée par une valeur peu élevée).

La figure V.2 permet de visualiser les différentes phases de la procédure, sur un schéma comportant six états successifs d'une boucle avec trois stations, notées A, B et C, matérialisées par leur registre.

V.1.2 Utilisation de la double boucle

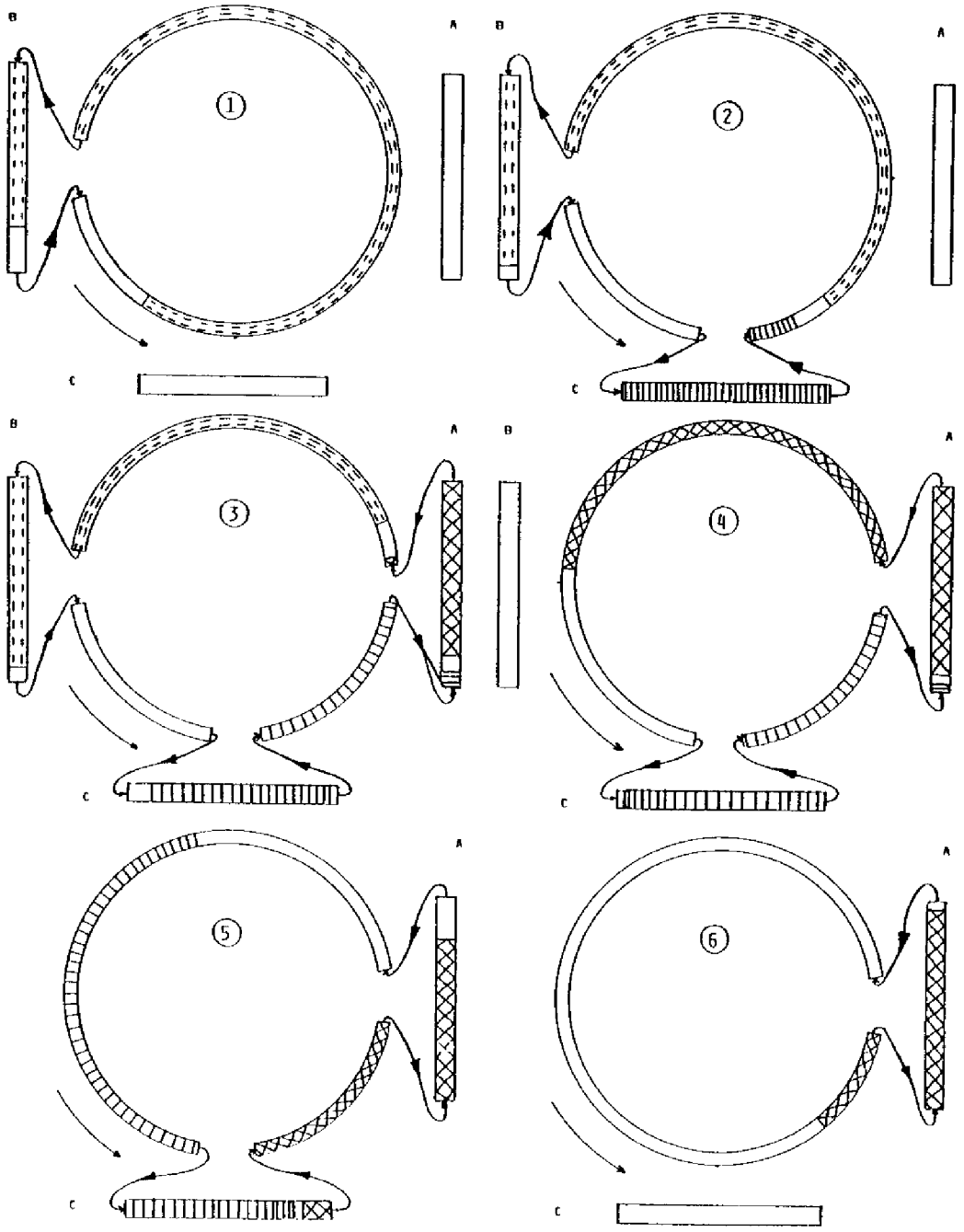
Le chapitre IV ayant conduit à retenir une structure à deux unités d'accès indépendantes pour les processeurs frontaux, nous allons chercher à maintenir le plus possible cette indépendance dans la procédure de communication.

Pour des raisons de latence, il n'est pas envisageable de n'utiliser qu'une boucle et garder l'autre en secours. On peut donc penser, soit envoyer systématiquement les paquets sur les deux boucles, soit ne les envoyer que sur une, en essayant de répartir équitablement la charge.

Cette dernière solution conduit à des procédures plus complexes, qui remettent en cause la décentralisation de la gestion des accès (le droit d'accès est alors lié à un paramètre non local : la charge), et surtout l'indépendance des deux boucles.

Nous préférons donc l'envoi simultané sur les deux boucles, d'autant plus que ceci augmente la probabilité d'acheminement correct qui est, pour cette application, un critère beaucoup plus important que la durée **moyenne** d'acheminement (la durée maximale est plus significative... mais elle est identique pour les deux possibilités envisagées ici).

Remarquons enfin que cette solution permet de diminuer l'impact des défaillances de mode commun, et de justifier l'hypothèse faite au paragraphe IV.1.3.6. En effet, la partie commune en émission dans le processeur frontal peut être considérée comme nulle, puisqu'il ne s'agit que de distribuer les informations en provenance de l'équipement vers les unités d'accès qui les traitent alors indépendamment.



PHASE \ STATION	A	B	C
1	Attente d'une fin de paquet	Emission terminée Ecoute avant extraction	Attente d'une fin de paquet
2	Attente d'une fin de paquet	Ecoute avant extraction	Début d'émission
3	Début émission	Ecoute avant extraction	Suite d'émission
4	Suite d'émission	Extraction du registre	Suite d'émission
5	Ecoute avant extraction	(Registre extrait)	Ecoute avant extraction
6	Ecoute avant extraction	(Registre extrait)	Extraction du registre

paquet envoyé par A
paquet envoyé par B
paquet envoyé par C

figure V.2 : insertion de registre ; exemple de fonctionnement

La partie commune est en revanche plus importante en réception, puisqu'il faut réapparier les paquets reçus sur chaque boucle pour n'en envoyer qu'un exemplaire à l'équipement (lorsqu'il est destinataire).

Néanmoins les défaillances en réception conduisent au pire à rendre "sourde" une station et au risque d'ouverture d'un disjoncteur supplémentaire seulement (en cas de défaut sur une ligne connectée sur la même barre que cette station). Par contre, une station muette peut entraîner l'ouverture de N_b-1 disjoncteurs supplémentaires en cas de défaut sur la ligne surveillée par cette station, ou de N_b disjoncteurs supplémentaires s'il s'agit d'une station de couplage avec une barre sur laquelle survient un défaut (N_b : nombre maximal de disjoncteurs par barre).

La structure d'un tel processeur frontal est représentée sur le schéma de la figure V.3.

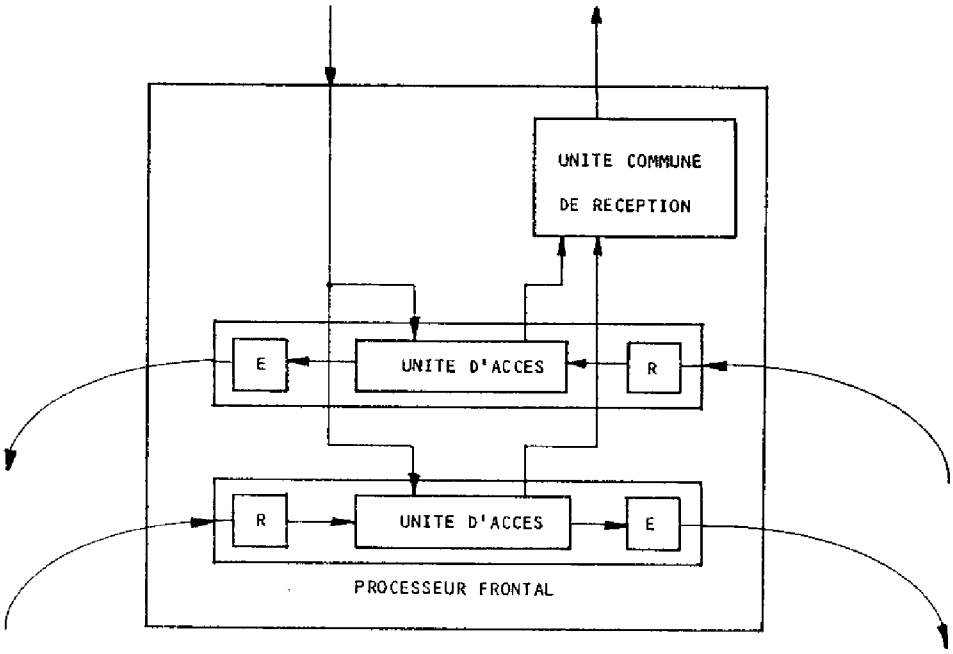


figure V.3 : Schéma d'un processeur frontal

La double boucle peut également être utilisée pour reconfigurer le support en isolant une station, conformément à l'étude des chapitres précédents. Nous n'étudions pas ici le déroulement de cette procédure de reconfiguration ni les fonctions supplémentaires qu'elle entraîne dans les processeurs frontaux, ce qui déborderait du cadre de ce mémoire. Par contre nous examinerons comment la procédure de communication peut s'adapter à la structure du support une fois la reconfiguration effectuée.

V.2 FONCTIONNEMENT NOMINAL : ETUDE DETAILLEE

Les résultats du chapitre IV permettent d'adopter une solution à débit relativement faible (de l'ordre de 500 kbit/s), basée sur la limitation du nombre de paquets de service en circulation simultanée grâce à un jeton.

Il est cependant préférable du point de vue de la simplicité et surtout de la latence, de traiter tous les paquets, de service comme de défaut, selon la même procédure. Disposant, comme nous l'avons vu, d'une certaine marge sur le débit, nous adoptons donc la méthode de l'**accès asynchrone par insertion de registre** pour **tous** les paquets sans distinction de type. L'étude détaillée des paragraphes suivants permettra de déterminer le débit nécessaire pour satisfaire les contraintes d'acheminement de rafales, et de vérifier que ce débit reste acceptable.

V.2.1 Composition d'un paquet

Pour identifier les deux paquets correspondant au même message, nous utilisons un octet donnant un numéro d'ordre aux **messages** émis par une station. Les deux paquets correspondant à ce message portent donc le même numéro, qui ne sera utilisé de nouveau qu'après émission par la même station de 255 autres messages.

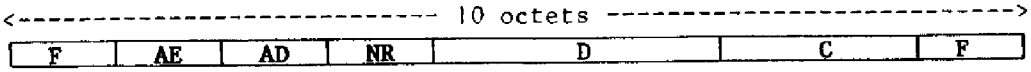
Cette solution permet, en réception, de réapparier les paquets, mais aussi de détecter des pertes de paquets, par comparaison avec les numéros des précédents paquets reçus de la même station.

Remarques :

(1) : Il s'agit de numéros propres à chaque station émettrice ; deux paquets émis par des stations distinctes portent des numéros indépendants.

(2) : On pourrait utiliser un cycle de numérotation plus court que 256, mais le découpage par mots de 8 bits et les facilités de traitement de ces mots justifient ce choix.

Ces choix ainsi que ceux exprimés aux paragraphes III.2.1 et IV.2.1.1 permettent de définir la composition d'un paquet, détaillée sur le schéma de la figure V.4.



F : 2 fois 1 octet de fanion de trame HDLC (01111110),

AE : 1 octet d'identification de l'expéditeur (5 bits d'adresse, 3 bits restant disponibles pour préciser le type du paquet (défaut, service, test, ...),

AD : 1 octet d'adressage (possibilité d'adressage individuel (sur 5 bits), par groupe, ou de diffusion),

NR : 1 octet de numérotation permettant d'identifier le message auquel correspond ce paquet parmi les 256 derniers émis par la même station expéditrice,

D : 3 octets de données,

C : 2 octets de CRC

figure V.4 : composition d'un paquet

Ces paquets sont acheminés sous forme de signaux optiques selon le code $NRZI_1$, conformément aux choix des chapitres précédents.

V.2.2 Emission

Pour émettre un message, une station doit le mettre sous forme d'un paquet dont elle envoie deux copies identiques -une à chacune des deux unités d'accès de son processeur frontal- qui réalisent ensuite la fonction d'émission de façon entièrement indépendante l'une de l'autre.

Ces paquets doivent présenter le format indiqué au paragraphe V.2.1, c'est-à-dire être munis des identificateurs d'expédition et de destination, de deux octets de CRC, de fanions, et des "0" éventuels de "transparence de trame HDLC". L'unité d'accès peut alors exécuter la procédure permettant de transmettre les signaux correspondants (en code $NRZI_1$) sur sa boucle.

V.2.2.1 Insertion

Une unité d'accès peut émettre un paquet sur sa boucle entre deux paquets déjà en circulation sur cette boucle, ou bien lorsqu'il n'y a aucun paquet en circulation (du moins vu de son récepteur : état de repos du récepteur).

Pour simplifier la fonction de détection des états où l'insertion est autorisée, nous choisissons de nous ramener toujours au second cas, en ménageant un espacement suffisant entre les paquets consécutifs sur la boucle. Avec le code $NRZI_1$ associé à la trame HDLC, la durée maximale sans transition est de $7*T_{bit}$ (§III.2.1) ; c'est donc aussi la durée minimale nécessaire pour détecter l'état de repos, que nous notons T_E.

Cette solution semble introduire une contrainte supplémentaire sur les paquets en circulation, mais en contrepartie le mécanisme d'insertion est beaucoup plus simple (pas de traitement des paquets ni de reconnaissance de la trame, et utilisation d'un mécanisme asynchrone). Précisons toutefois qu'il serait possible de mettre en œuvre cette procédure de communication sans recourir à cet espacement. Il faut également remarquer que nous disposerons d'un mécanisme, décrit au paragraphe V.3.1.1, permettant d'insérer le registre même si l'espacement n'est pas respecté. (Un tel mécanisme serait d'ailleurs indispensable quel que soit le principe retenu pour détecter les états où l'insertion est autorisée).

Il suffit donc, pour avoir le droit d'insérer son registre, de vérifier qu'aucun signal n'est parvenu au récepteur depuis un certain intervalle de temps T_E, ce qui est représenté par le réseau de Petri de la figure V.5', donnant un détail du principe général d'accès représenté (également par réseau de Petri) sur la figure V.5.

Remarque : nous utilisons ici les réseaux de Petri essentiellement dans un but descriptif. Pour simplifier la représentation, nous associons à certaines transitions :

- des **conditions C** devant être vérifiées (en plus du marquage des places

précédentes) pour que la transition puisse être tirée,
- des **actions A** exécutées au moment du tirage.

Ceci est noté **(C ;A)** à côté du trait matérialisant la transition.

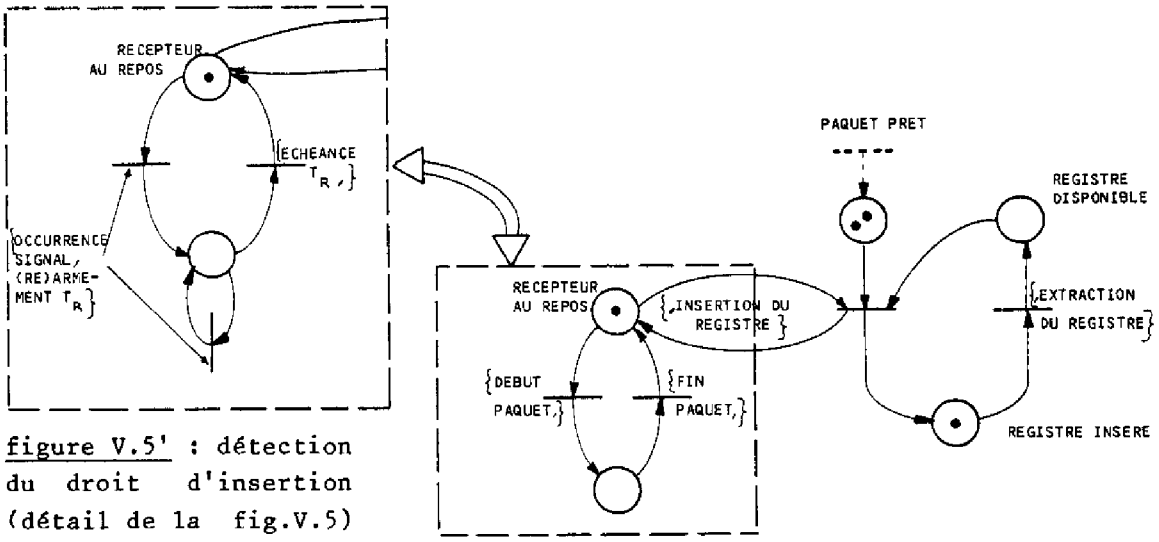


figure V.5' : détection du droit d'insertion (détail de la fig.V.5)

figure V.5 : émission d'un paquet ; fonctionnement normal

V.2.2.2 Fin d'émission

La procédure d'émission se termine par l'extraction du registre qui est ainsi libéré pour une émission ultérieure. Le registre est extrait quand le dernier bit du paquet est revenu, après avoir effectué un tour. Dans la procédure normale, c'est-à-dire lorsque tout s'est déroulé correctement, l'unité d'accès peut reconnaître son paquet, soit par comparaison du deuxième octet avec son adresse propre, soit par comparaison bit à bit avec une copie du paquet émis (cette technique étant ici utilisable sans complication excessive, du fait qu'une unité d'accès ne peut avoir qu'un paquet en attente à la fois). L'extraction consiste alors à rétablir la liaison directe entre le récepteur et l'émetteur. Le paragraphe V.3.1.3 est consacré à l'étude des mécanismes destinés à mettre fin à la procédure d'émission en cas de fonctionnement anormal.

V.2.3 Réception

En réception, le traitement comporte des fonctions effectuées dans chaque unité d'accès, et des fonctions effectuées dans l'unité commune de réception, que nous allons étudier successivement.

V.2.3.1 Unités d'accès

Pour diminuer la latence, et améliorer l'observabilité et donc la connaissance que chaque station peut avoir de l'ensemble du système, tous les paquets sont systématiquement traités dans les unités d'accès de toutes les

stations, destinataires du paquet ou non.

Ce traitement consiste à prélever une copie du paquet, en même temps que les signaux qui le composent sont transférés vers l'émetteur, soit directement, soit à travers le registre si cette unité est engagée en parallèle dans une procédure d'émission.

Les fanions de début et fin de paquet, les "0" insérés à l'émission, ainsi que les deux octets de CRC sont supprimés, et le CRC vérifié (fonctions classiques des circuits de gestion de la procédure HDLC).

Dans le cas où le CRC est incorrect, le traitement est achevé (en ce qui concerne bien sûr uniquement les fonctions de réception). Sinon, les six octets qui restent sont soumis à la deuxième phase du traitement, qui se déroule dans l'unité commune à laquelle ces octets sont fournis.

De plus pendant cette première phase, dans le cas où l'unité d'accès considérée est également engagée dans une procédure d'émission, le paquet est comparé avec celui qui avait été émis, de façon à déterminer s'il faut ou non extraire le registre, comme indiqué au paragraphe V.2.2.

V.2.3.2 Unité commune de réception

Dans cette unité, on tient à jour un tableau indiquant, pour chaque station du système, le numéro du dernier message envoyé par cette station et reçu correctement (par l'une ou l'autre des unités d'accès, ou les deux) dans la station où se fait le traitement.

Ainsi, chaque station peut :

- vérifier si elle n'a pas perdu de message,
- identifier les éventuels messages perdus,
- sélectionner pour l'envoyer à l'équipement un seul des deux paquets correspondant au même message.

Notons que cette mise à jour est effectuée même dans les stations non destinatrices. Les tableaux des stations actives ne sont cependant pas identiques même en l'absence d'erreurs, car le système ne possède pas d'état global observable par toutes les stations /LEL'79/.

A la réception d'un paquet reconnu correct par le processeur HDLC, son numéro (noté NR) est confronté avec celui (noté NM) qui est mémorisé dans le tableau pour la même station expéditrice. Les deux cas suivants peuvent alors se présenter :

(a) le numéro reçu NR est supérieur au numéro mémorisé NM,

(b) le numéro reçu NR est inférieur ou égal au numéro mémorisé NM.

Dans le cas (a), l'autre exemplaire du paquet considéré a déjà été reçu correctement. Le traitement est alors achevé.

Dans le cas (b), il faut :

- mettre à jour le tableau : NR —> NM,
- transmettre ce paquet à l'équipement, s'il en est destinataire (et s'il n'en est pas l'expéditeur).

Remarques :
(1) Comme il s'agit d'une numérotation cyclique, les mots "inférieur" et "supérieur" ne correspondent pas à la relation d'ordre habituelle. Nous disons que n est inférieur à m si "(m-n) modulo N" est inférieur à N/2 (N étant le cycle, soit ici 256).
(2) Si NR>NM, les messages NM+1, NM+2, ... NR-1 sont considérés comme perdus ; outre une simple fonction d'alarme, on pourra prévoir de mémoriser cette liste (jointe à l'identité de la station expéditrice), pour une procédure éventuelle de demande de réémission.
(3) Nous avons donné ici l'ensemble minimal des fonctions de réception. Il est évident que la prise en compte des fonctions de diagnostic /KAN'82/ amène à implanter des mécanismes supplémentaires tant dans l'unité commune de réception que dans les unités d'accès.
(4) Une procédure complète (dont l'étude ne relève pas du présent mémoire) nécessite un minimum de traitement sur les séquences de signaux à format incorrect, ou CRC incorrect.

V.3 CAS DE FONCTIONNEMENT DEGRADE

Ce paragraphe recouvre les défaillances de type :
- fonctionnel :
  + comment une station peut émettre lorsqu'elle ne détecte, pour une raison ou pour une autre, aucun espacement lui permettant d'effectuer l'insertion de registre,
  + ce que doit faire une station engagée dans une procédure d'émission, qui ne reconnaît pas son paquet au bout d'un tour,
- structurel : comment continuer à communiquer sur le support dégradé, c'est-à-dire en cas :
  + de perte d'une boucle,
  + d'isolement d'une station.

V.3.1 Défaillances fonctionnelles

Etant donné l'importance de l'accès au support, pour les messages de défaut, le premier point à examiner concerne les défaillances risquant d'empêcher cet accès.

V.3.1.1 Insertion en l'absence d'espacement

En fonctionnement normal, il ne peut s'écouler plus de la durée d'un paquet sans que le récepteur d'une unité d'accès ne retourne à l'état de repos. La présence d'une séquence anormalement longue de signaux peut donc être détectée par chaque unité d'accès, lorsque son récepteur reste sollicité au-delà d'une durée notée T_0 (qu'il suffit de prendre légèrement supérieure à T_p). Nous autorisons dans ce cas cette unité d'accès, si elle a un paquet prêt, à effectuer l'insertion exactement comme si son récepteur était au repos (nous parlerons alors d'**insertion forcée**).

En résumé, pour émettre un paquet, une unité d'accès doit, comme indiqué sur le réseau de Petri de la figure V.6, attendre de détecter :

- soit l'état de repos : échéance de la temporisation T_R sans réception de signal,
- soit l'état "d'occupation excessive" : échéance d'une temporisation de durée T_O réarmée à chaque fois que le récepteur retourne à l'état de repos (c'est à dire réarmée par l'échéance de T_R).

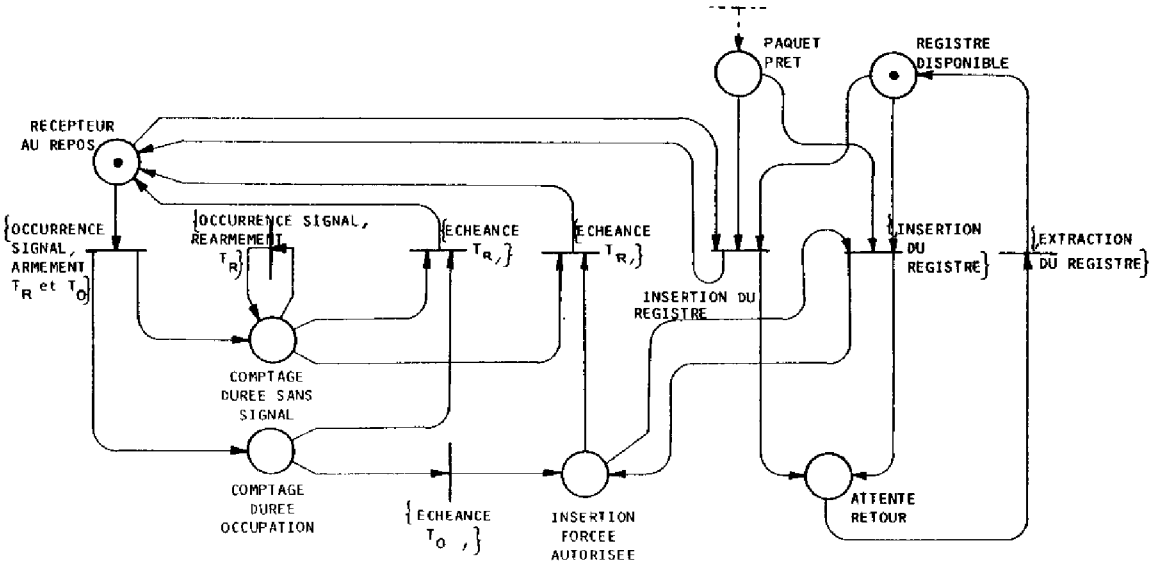


figure V.6 : insertion forcée : principe de détection

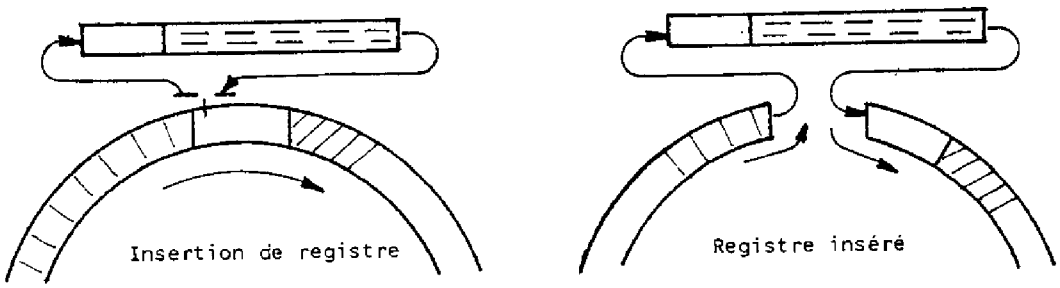
Le paquet ne peut cependant pas être émis exactement selon la même procédure dans les deux cas. En effet, en cas d'insertion forcée, pour éviter que le paquet ne soit coupé par une station en aval qui aurait aussi détecté la séquence trop longue, il est nécessaire de le faire précéder par une "absence de signal" pendant la durée correspondant à l'espacement entre paquets : T_E.

L'insertion forcée comprend donc un paquet et deux espacements, alors qu'en mode normal il suffit d'insérer un paquet et un espacement. On peut alors envisager les trois possibilités représentées sur la figure V.7 :

- première solution : insérer tous les paquets avec deux espacements,

- deuxième solution : concevoir un système mixte capable d'insérer un paquet accompagné dans certains cas de deux espacements, et dans les autres, d'un seul,

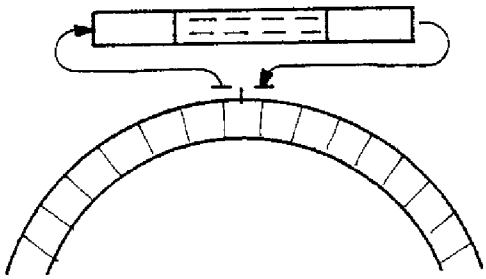
- troisième solution : créer, dans le cas de l'insertion forcée, l'espacement du début par superposition sur les signaux en circulation, avant l'insertion (inhibition de ces signaux pendant une temporisation T_I de durée au moins égale à T_E).

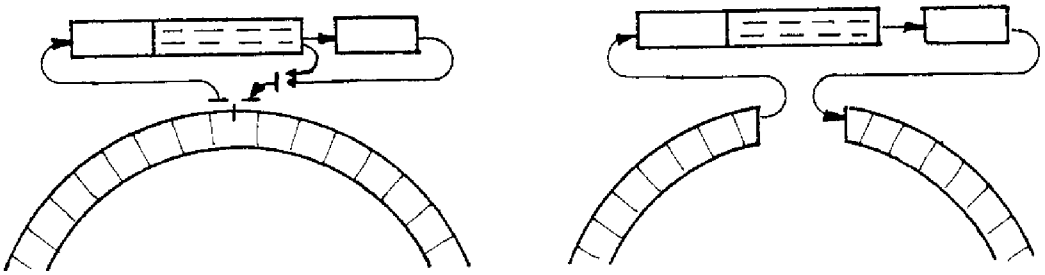


a. Fonctionnement normal

Prise en compte de l'insertion forcée :

b. (Solution n°1)
Insertion systématique d'un paquet et 2 espacements





c. (Solution n°2). Insertion mixte, d'un paquet avec 1 ou 2 espacements (1 en mode normal, 2 pour insertion forcée).

d. (Solution n°3)
Superposition d'un espacement sur les signaux incorrects, en insertion forcée.

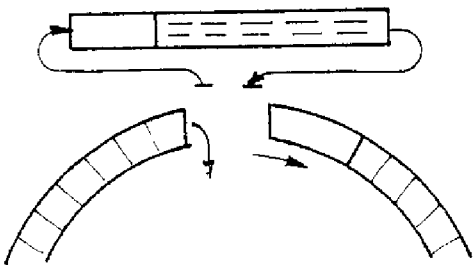


figure V.7 : insertion d'espacement

En tenant compte du fait qu'à l'extraction il faut laisser au moins un espacement pour que l'insertion normale soit possible entre les paquets restants, nous retenons la troisième solution. C'est en effet celle qui permet le plus facilement d'insérer un paquet avec un ou deux espacements, tout en l'extrayant toujours avec un seul.

Remarque : il est légitime de détruire ces signaux, qui ne peuvent plus être porteurs d'informations après l'insertion forcée par l'unité d'accès, que cette insertion forcée soit justifiée (séquence trop longue : les signaux concernés n'étaient déjà plus porteurs d'informations) ou non (défaillance de l'unité d'accès entraînant l'insertion au milieu d'un paquet correct).

V.3.1.2 Nettoyage d'une boucle

La procédure d'insertion forcée permet donc de tolérer les fautes se traduisant par la pollution d'une boucle, soit à cause d'une accumulation de signaux intempestifs ou de portions de paquets non ou mal extraits, soit à cause d'une "génération spontanée" de signaux de la part d'une unité d'accès. Il n'est donc pas nécessaire de nettoyer une boucle ainsi polluée. Cependant une telle procédure de nettoyage est incontestablement utile pour éviter, d'une part de se trouver toujours dans l'obligation d'utiliser l'insertion forcée, et d'autre part d'obtenir des paquets d'apparence correcte à partir des signaux parasites au bout d'un certain nombre de tours.

La procédure d'insertion forcée participe en fait au nettoyage, car après extraction il reste un espacement dans la séquence initialement trop longue. Compte tenu du fait que les signaux qui suivent l'insertion, jusqu'au prochain espacement, ne sont plus utilisables, on peut accélérer le processus de nettoyage.

Pour cela, il suffit de maintenir l'inhibition des signaux reçus, non seulement pendant la durée d'un espacement, mais jusqu'à l'espacement suivant, ou à défaut pendant une certaine durée maximale. On peut pour cela utiliser le même mécanisme, avec les mêmes temporisations, que celui qui sert à décider d'effectuer une insertion forcée. Ceci est représenté sur la figure V.8 sur laquelle on peut noter la présence d'un mécanisme permettant de maintenir l'inhibition des signaux jusqu'à l'insertion, ce qui évite de devoir régler finement les valeurs relatives de T_E et T_I.

Cette procédure permet, si la cause de la défaillance a disparu, de supprimer les trop longs paquets et de rendre la boucle utilisable par les procédures normales sans insertion forcée. En toute rigueur, il n'est pas nécessaire de supprimer les séquences courtes de signaux parasites. Toutefois pour éviter que, les altérations se succédant, ils ne prennent la forme d'un paquet correct, on peut prévoir de les supprimer après concertation entre les stations. La procédure correspondante peut être engagée par n'importe quelle unité d'accès après détection d'un certain nombre de paquets mal formés, qui envoie alors, sur sa boucle, un message spécifique.

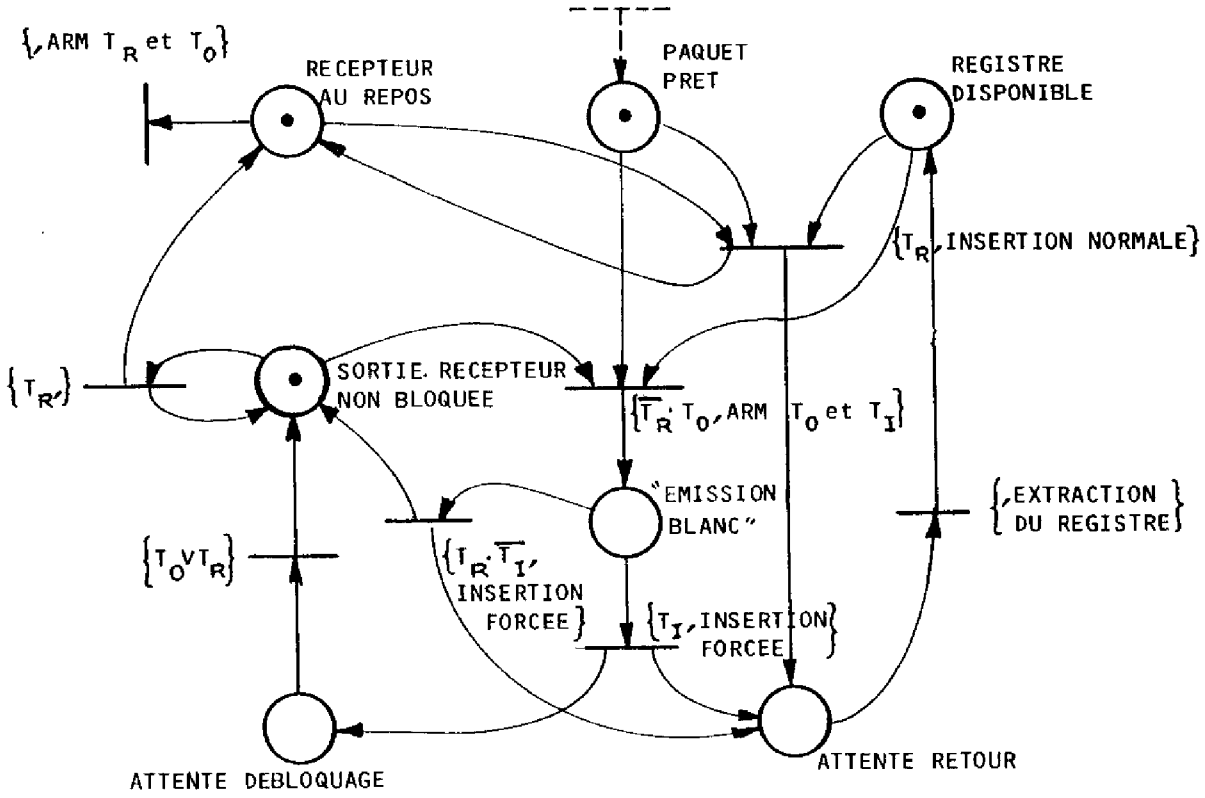


figure V.8 : insertion forcée et nettoyage partiel

Toute unité d'accès qui reçoit au moins un nombre préalablement fixé de tels messages (d'expéditeurs différents) exécute la phase de nettoyage : il s'agit alors de ne plus transmettre aucun signal sur la boucle pendant une durée au moins égale au temps maximal de parcours de la boucle (les signaux reçus pendant cette période ne sont pas mémorisés pour une transmission ultérieure, mais détruits).

V.3.1.3 Extraction après anomalie

En fonctionnement normal, la procédure d'extraction prend fin pour une unité d'accès quand elle extrait son registre après avoir reconnu son propre paquet qui a effectué un tour.

Si pour une raison ou pour une autre l'unité d'accès ne retrouve plus son paquet, nous autorisons cette unité à extraire son registre à l'échéance d'une temporisation, ce qui permet de surveiller, et de limiter l'intervention des unités défaillantes dans la boucle. Toutefois cette solution se traduit par une cascade de telles extractions, la première unité extrayant une partie du paquet d'une autre unité qui ne le reconnaît plus, etc... Nous adoptons donc, pour limiter cet effet, une procédure à deux niveaux de dégradation :

- au bout d'une première temporisation T_{X1} après le début de l'émission, l'unité d'accès est autorisée à extraire son registre dès qu'il contient un paquet à CRC incorrect,

- à l'échéance d'une deuxième temporisation T_{X2}, elle est autorisée à extraire son registre sans autre condition ; il lui est alors interdit de réutiliser ce registre avant au moins N_s fois T_{X2}, ceci afin de permettre à la réaction en chaîne d'extractions de s'achever (N_s étant le nombre maximal de stations).

V.3.2 Défaillance du support

Les défaillances qui sont étudiées dans ce paragraphe sont celles qui laissent la possibilité de communiquer : perte d'une boucle, et défaillances conduisant à l'isolement d'une station.

V.3.2.1 Perte d'une boucle

D'après la description de la procédure, il apparaît qu'aucun traitement particulier n'est nécessaire, et la procédure de base fonctionne sans modification qu'il y ait une ou deux boucles, ce qui est conforme aux principes de latence et de simplicité.

La seule différence tient dans le fait que sur la boucle défaillante, les registres ne peuvent pas être extraits par la procédure normale puisque les paquets ne peuvent pas achever leur tour. C'est donc systématiquement la procédure d'extraction forcée qui sera effectuée. Il ne s'agit toutefois pas d'une procédure d'exception à très forte latence puisque, d'après le paragraphe V.3.1.3 elle est basée uniquement sur le non-retour du paquet attendu : le traitement est semblable quelle que soit la cause de ce non-retour (erreur de transmission, extraction erronée par une autre station, boucle "coupée", mécanisme de reconnaissance défaillant).

V.3.2.2 Isolement d'une station

Nous ne traitons pas le cas des stations des extrémités, c'est-à-dire celles qui sont les plus proches de la partie isolée et qui effectuent le transfert des paquets d'une boucle sur l'autre. Ceci relève en effet beaucoup plus de l'étude du processus de reconfiguration que du système de communication proprement dit, auquel ce mémoire est consacré.

En ce qui concerne la façon dont les autres stations peuvent communiquer sur le support une fois celui-ci reconfiguré, nous adoptons la même procédure que sur le support original, dans le but d'augmenter la simplicité et la décentralisation, et de diminuer la latence.

L'examen de la procédure normale montre en effet qu'elle peut s'adapter sans modification à cette nouvelle structure du support (à condition toutefois que la temporisation T_{X1} gérant l'extraction forcée (§V.3.1.3) tienne compte du temps de parcours maximal sur le support reconfiguré, plus long que sur une boucle d'origine). Les stations n'ont donc pas besoin de savoir s'il y a eu ou non reconfiguration, ni d'adopter un comportement spécifique. Chaque unité d'accès continue à gérer sa propre boucle comme si elle était indépendante de l'autre, et chaque station envoie une copie du message à émettre à ses deux unités d'accès. Il importe peu qu'en fait :

- les paquets "homologues" se suivent sur le même support,
- le paquet émis par une unité d'accès soit en général extrait par l'unité d'accès du même processeur frontal mais sur l'autre boucle.

V.4 PERFORMANCES. DETERMINATION DU DEBIT

Dans ce paragraphe, nous étudions les caractéristiques fonctionnelles de la solution ainsi détaillée, afin de déterminer quel est le débit de transfert nécessaire pour satisfaire la contrainte d'acheminement de rafale de défaut, et de vérifier si cette valeur est admissible.

V.4.1 Notations et valeurs typiques

* durée d'un bit	: T_{bit}	: valeur à déterminer
* traversée d'une unité d'accès n'ayant pas inséré son registre	: T_{pf}	: $T_{pf} = T_{bit}$ (§IV.2.3)
* parcours d'une liaison	: T_L	: $T_L = 10^{-6}$s (§IV.2.3)
* durée de parcours entre deux stations voisines	: T_s	: $T_s = T_L + T_{pf}$
* durée d'un paquet	: T_P	: $T_P = 92 * T_{bit}$ (voir ci-dessous)
* durée d'un espacement	: T_E	: $T_E = 10 * T_{bit}$ (voir ci-dessous)
* nombre de stations	: N_s	: $N_s = 30$ (§I.1.4.3)

valeur de T_P : un paquet fait 10 octets, ce qui peut faire après insertion des "0" de trame HDLC jusqu'à 92 bits. Nous prenons donc la valeur maximale, soit : $T_P = 92 * T_{bit}$.
valeur de T_E : elle doit être strictement supérieure à la durée de détection de repos, $7 * T_{bit}$, augmentée des durées d'insertion et d'extraction. Etant donné les principes retenus (§V.1.1) ces opérations peuvent se limiter à l'aiguillage des signaux selon deux chemins possibles. Nous pouvons donc retenir, avec une marge suffisante, une valeur de $10 * T_{bit}$.

V.4.2 Temps d'acheminement maximal sur une seule boucle

Le temps maximal est obtenu pour l'émission d'un paquet dans une unité d'accès qui vient de commencer à émettre son paquet précédent (temps d'accès maximal), et lorsque toutes les autres unités d'accès sont en phase d'émission (temps de parcours maximal). Le temps d'acheminement du nouveau paquet est alors obtenu en faisant la somme :

* du temps d'émission du précédent paquet..	: T_P
* du temps jusqu'au retour dans le registre	: $(N_s-1)*(T_s+T_P+T_E) + T_s + T_E$
* du temps nécessaire pour faire un nouvel accès (en supposant l'espacement insuffisant pour extraire l'ancien et insérer le nouveau paquet à la fois).....	: $T_P + T_E$
* du temps d'émission du nouveau paquet ...	: T_P
* du temps d'acheminement aux N_s-1 autres stations	: $(N_s-2)*(T_s+T_P+T_E) + T_s$

On obtient au total le temps, noté T_{B1}, au bout duquel le nouveau paquet est acheminé à tous ses destinataires, ainsi donc que tous les autres paquets de la même rafale :

$T_{B1} = (2N_s - 1)*(T_s + T_P + T_E) + T_P$, soit en fonction de T_{bit} :

$\mathbf{T_{B1} = 6169 * T_{bit} + 59}$ (en microsecondes).

V.4.3 Temps d'acheminement maximal avec deux boucles

Dans ce cas, le dernier terme de l'expression précédente se ramène à l'acheminement à $\lceil (N_s - 1)/2 \rceil$ stations ($\lceil x \rceil$ désignant le plus petit entier supérieur ou égal à x), puisque les autres sont servies dans le même temps sur l'autre boucle.

On obtient alors la valeur notée T_{B2} donnée par l'expression :

$T_{B2} = (N_s + \lceil (N_s - 1)/2 \rceil)*(T_s + T_P + T_E) + T_P$, soit en fonction de T_{bit} :

$\mathbf{T_{B2} = 4727 * T_{bit} + 45}$ (en microsecondes).

V.4.4 Boucle reconfigurée

Il est plus difficile de faire une évaluation précise du temps d'acheminement maximal lorsque le support est reconfiguré, car il faut faire intervenir les durées nécessaires pour que les stations d'extrémité effectuent le transfert des signaux d'une boucle sur l'autre.

En négligeant cette durée supplémentaire, la libération du registre exige le parcours complet du support, c'est-à-dire l'équivalent de deux fois une boucle d'origine. L'acheminement prend ensuite le temps nécessaire pour que chaque paquet atteigne "sur sa boucle" la station d'extrémité. Ceci peut nécessiter jusqu'à la durée de parcours d'une boucle d'origine, pour les stations proches des extrémités.

Nous pouvons donc borner le temps d'acheminement d'une rafale sur le support reconfiguré par une valeur de l'ordre de trois fois la durée maximale de parcours sur une boucle d'origine, soit environ 9000 * T_{bit}.

Remarquons cependant qu'il s'agit d'une valeur rarement atteinte car généralement, lorsqu'un paquet aura été retardé par la traversée d'un registre dans une unité d'accès, le paquet correspondant à ce registre aura été extrait par l'unité homologue ; il paraît improbable (mais non impossible) que cette station réémette immédiatement un autre paquet, et qu'il en soit ainsi pour toutes les stations. Ceci conduit donc à une valeur de l'ordre de 6000 * T_{bit}, sans même tenir compte de la charge effective du support, ce qui fait l'objet

du paragraphe suivant.

V.4.5 Influence de la charge du support

Les valeurs précédentes sont calculées pour la charge maximale : toutes les stations ont des paquets à émettre. Si les conditions d'utilisation sont telles que la charge puisse être considérée comme plus faible, ces valeurs deviennent pessimistes.

En notant N_a le nombre de stations qui peuvent effectivement être considérées comme actives et en émission simultanée, on peut retrancher du temps d'acheminement :

* sur une seule boucle : $(N_s-N_a)*(T_P+T_E)+(N_s-N_a-1)*(T_P+T_E)$
* avec les deux boucles : $(N_s-N_a)*(T_P+T_E)+(\lceil(N_s-1)/2\rceil-\lceil(N_a-1)/2\rceil)*(T_P+T_E)$

Les résultats les plus caractéristiques sont donnés sous forme de courbes sur la figure V.9, indiquant pour différents cas de charge et les différents états du support le temps d'acheminement d'un paquet à tous ses destinataires ; les stations travaillant en parallèle, ce temps est le même que celui correspondant à l'acheminement d'une rafale de N_d paquets, sous réserve que :

- les N_d paquets sont émis par N_d stations distinctes,
- N_d augmenté du nombre de stations en émission de paquets autres que ceux de la rafale, reste inférieur au nombre N_a considéré.

V.4.6 Compatibilité avec les traitements à effectuer

Nous étudions ici les contraintes limitant le débit, dues aux traitements à effectuer pendant le passage des signaux.

Mécanisme d'insertion/extraction : les durées correspondantes ont été prises en compte dans la détermination de la valeur de T_E (§V.4.1).

Traitement des signaux : l'extraction des informations de la trame HDLC et le traitement du CRC peuvent être effectués avec les circuits intégrés spécialisés actuels jusqu'à un débit d'au moins 2 Mbit/s.

Traitement des paquets en réception : En utilisant par exemple dans chaque unité commune de réception, un processeur du type Z80 (Zilog, version 4 MHz), le traitement d'un paquet selon la procédure détaillée au paragraphe V.2.3.2, nécessite moins de 100 cycles d'horloge, soit 50.10^{-6}s pour les deux paquets (provenant de chaque boucle) que peut recevoir chaque unité pendant une durée de T_P+T_E.

Il va sans dire qu'il ne s'agit pas là de l'architecture idéale, mais uniquement d'une étude destinée à s'assurer de la faisabilité de la solution.

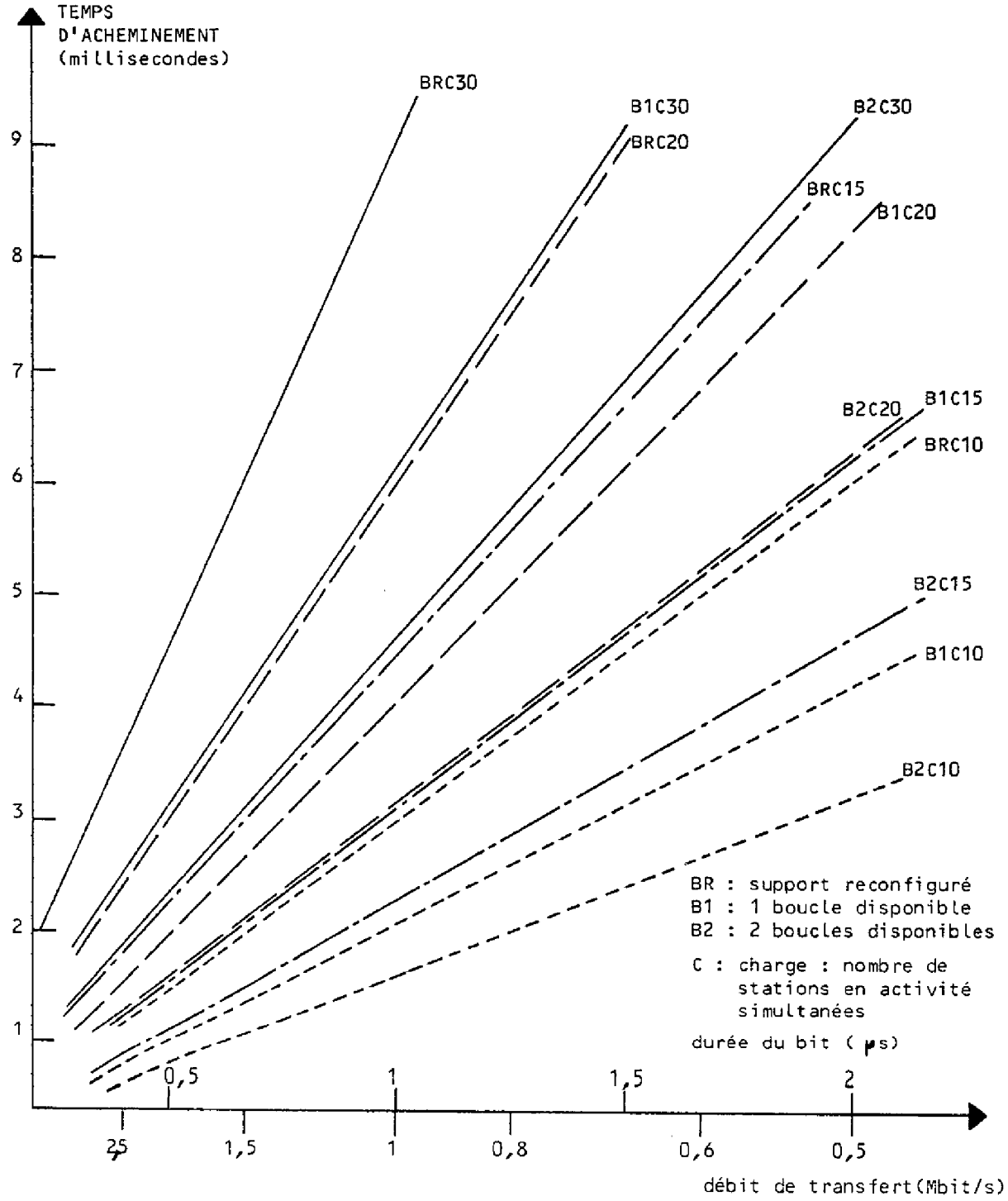


figure V.9 : temps d'acheminement de rafale

V.4.7 Choix du débit de transfert

Ce choix doit tenir compte :

- des contraintes technologiques sur le débit de transmission, dues aux

interférences électromagnétiques qui limitent la bande passante à environ 3 à 4 MHz, soit avec le code $NRZI_1$, 3 à 4 Mbit/s,
- de la capacité de traitement des paquets en réception,
- du temps maximal autorisé pour l'acheminement des rafales de défaut.

D'après le paragraphe V.4.6, il existe une solution satisfaisant la deuxième contrainte si $T_p + T_E$ est supérieur à 50.10^{-6}s, ce qui correspond à un débit de transfert inférieur à 2 Mbit/s.

La troisième contrainte impose l'acheminement d'une rafale de défaut en moins de trois millisecondes. Avec un débit de transfert de 1,5 Mbit/s, nous obtenons un temps d'acheminement d'environ 3 ms dans le pire cas lorsque les deux boucles sont disponibles (respectivement 4 et 6 ms en fonctionnement dégradé sur une seule boucle et sur le support reconfiguré), ces valeurs correspondant à la charge maximale.

Ces valeurs deviennent respectivement 1,6 ms, 2 ms, et 3 ms à mi-charge, alors qu'en fait la charge effective ne semble pas devoir dépasser 1/3 (7 stations en possession d'un message de défaut, plus 2 ou 3 stations émettant divers messages de service et de test. Dans ce cas, les valeurs du temps d'acheminement sont 1,1 ms, 1,4 ms, et 2 ms).

V.5 CONCLUSION

Un débit de 1,5 Mbit/s permet donc de satisfaire l'ensemble des contraintes à charge maximale lorsque les deux boucles sont disponibles, et à mi-charge pour les cas de dégradation du support.

Si nous tenons compte du fait qu'actuellement le nombre de stations réel est beaucoup plus faible que 30, ce qui constitue une limite physique à la charge effective du support étudié, cette valeur du débit peut être adoptée.

Nous voyons alors, en se référant au paragraphe IV.2.4, que cette valeur n'est pas susceptible de remettre en cause la validité des choix antérieurs, et en particulier ceux du chapitre IV concernant la comparaison des performances fonctionnelles sur une base de 0,5 Mbit/s. L'étude de ce chapitre V permet de plus de constater qu'avec cette valeur de débit, la solution proposée est tout à fait compatible avec les possibilités de réalisation technologiques, sans remettre en cause le principe de simplicité.

La cohérence avec l'ensemble des choix successifs de conception a donc pu être maintenue, en particulier dans le domaine de la sûreté de fonctionnement. Il n'est donc pas nécessaire d'affiner davantage cette étude pour pouvoir affirmer que la solution la mieux adaptée pour interconnecter les équipements du système de protection d'un poste THT se compose de deux boucles contrarotatives en fibres optiques et de processeurs frontaux à deux unités d'accès indépendantes, avec sur chaque boucle accès asynchrone par insertion de registre.

CONCLUSION

L'étude présentée dans ce mémoire concerne la définition et l'application d'une méthode rigoureuse de conception, pour un support de communication destiné à un système décentralisé de surveillance et sécurité (système de protection). On peut tirer de cette étude deux types de conclusions : celles relatives à la méthode elle-même appliquée au cas considéré, et celles relatives aux résultats auxquels elle a permis d'aboutir concernant le système de communication objet de cette étude.

En ce qui concerne la méthode elle-même, les principaux résultats consistent en :

- l'utilisation d'une décomposition en **couches** (ou plus généralement, points de vue) complétant l'approche par niveaux de détails successifs,
- l'étude de la façon de choisir des guides de conception ou **critères** en fonction des spécifications bien sûr, mais aussi du niveau de détail et du point de vue considérés,
- l'**analyse préalable** de ces critères de manière à exprimer leurs interactions pour les prendre en compte le plus tôt possible, pendant l'application même de ces critères dans le processus de conception.

Appliquée au support de communication du système de surveillance et sécurité du poste à Très Haute Tension, cette méthode a permis d'aboutir :

- à une décomposition en deux couches, **transfert** et **transmission**, dérivées du modèle OSI,
- aux choix de critères qualitatifs mettant l'accent sur la **latence** et la **décentralisation**, ainsi que sur la **simplicité**, la **normalisation** (choix de composants standards), la **flexibilité** et le **coût**,
- à la définition des critères d'évaluation des solutions envisageables : le temps d'acheminement de rafales de messages en fonctionnement normal, et en ce qui concerne la sûreté de fonctionnement, la probabilité d'ouverture de disjoncteur(s) supplémentaire(s) due à une défaillance du support.

Nous avons pu ainsi :

- définir un support constitué de deux boucles contrarotatives en fibres optiques à gestion indépendante, l'accès étant effectué de façon asynchrone par insertion de registre,
- montrer que cette solution était conforme aux spécifications.

Bien qu'en toute rigueur, ceci prouve que nous avons atteint les objectifs initiaux, il convient de se poser les deux questions suivantes :

- La méthode suivie est-elle la meilleure, c'est-à-dire concrètement, y a-t-il une meilleure solution que REBECCA pour notre application, et/ou pouvait-on aboutir plus rapidement au résultat ?
- Les résultats obtenus se limitent-t-ils à la présente application ?

Il est en fait extrèmement difficile de répondre à la première question. Nous pouvons cependant remarquer que, sans chercher à résoudre un débat général sur la découverte et l'invention, ou la méthode et l'imagination, l'utilisation d'une méthode rigoureuse de conception offre a priori plus de garanties, en particulier si l'on tient compte de l'importance de la sûreté de fonctionnement, et donc de la validation des résultats obtenus.

Mais il ne faut pas se cacher que si la solution obtenue présente un certain nombre de caractères originaux, il ne s'agit en aucune façon de création. Nous avons déjà indiqué que l'approche suivie ne garantit pas "l'optimalité" de la solution (§II.1.1.3). Cette remarque prend encore plus de poids si l'on considère que :

- d'une part il est difficile d'être exhaustif et de prendre en compte toutes les possibilités envisageables par un esprit méthodique,
- d'autre part il est impossible de prendre en compte toutes celles envisageables par un esprit créatif (en notant que ces possibilités pourraient être suffisamment simples pour se révéler très faciles à valider).

La deuxième question, concernant les extensions des résultats, est heureusement plus facile à traiter, et permet de conclure ce mémoire sur une note plus optimiste. Nous envisagerons, comme au début de cette conclusion, les extensions de la méthode elle-même, puis ceux des résultats qu'elle a permis d'obtenir pour cette application.

S'il est clair que la méthode utilisée peut s'appliquer à tout type de système, les résultats obtenus ici pourraient paraître plus spécifiques. Il faut toutefois remarquer que tout réseau local peut se décomposer en couches, et comporte en particulier des couches de transmission et de transfert ; de même, les critères choisis sont ceux qui correspondent à tout système de protection.

La solution obtenue, REBECCA, est donc susceptible de convenir à un domaine très large de systèmes, caractérisés par un fonctionnement en régime permanent auquel se superposent des rafales de messages très urgents. De plus, nous pouvons constater que, outre l'importance des contraintes de sûreté de fonctionnement, les spécifications étaient ici particulièrement sévères (environnement très perturbé, limitation du débit possible, difficultés de maintenance, performances fonctionnelles nécessaires,...). C'est pour cela que le recours à une solution spécifique était, comme nous l'avons vu, nécessaire, mais c'est également pour cela que cette solution spécifique peut convenir à de nombreuses autres applications, dans le domaine du contrôle-commande de processus par exemple.

Enfin, il nous paraît important de préciser qu'au-delà des applications directes, la solution proposée apporte une ouverture, en montrant qu'il est tout à fait possible de concilier les avantages d'une procédure d'accès

asynchrone avec les avantages intrinsèques d'un support en boucle (simplicité technologique du support, en liaisons point-à-point, et des équipements des processeurs frontaux, possibilités de diffusion de messages **avec** accusé de réception,...). En effet, l'accès asynchrone n'est pas réservé aux méthodes d'accès par compétition sur une voie multipoint, et l'insertion de registre dans une boucle présente des caractéristiques analogues, avec en plus un temps d'accès borné (qu'il est possible de rendre très faible en limitant la taille des registres).

L'augmentation constante des besoins en vitesse de transmission et distances d'interconnexion conduisent à un regain d'intérêt pour les boucles, dû aux diminutions de performances des bus dans ce domaine (qui d'une façon assez inattendue se rapprochent des systèmes à émission sourde -de type ALOHA- la durée du bit, voire du paquet devenant de plus en plus faible par rapport au délai de propagation). Il est donc essentiel de rappeler et de souligner qu'il n'est pas nécessaire d'utiliser un jeton sur une boucle, et qu'en conséquence, si l'argument du **déterminisme** ne favorise en fait pas réellement la boucle (car la probabilité de défaillance n'est jamais nulle), celui de l'**accès asynchrone** n'est pas non plus le monopole du bus.

BIBLIOGRAPHIE

ACT'79 ACTA ELECTRONICA : **"Numéro spécial sur les transmissions par fibres optiques : Composants et dispositifs"**, vol.22 n°4, 1979.

AFN'82 AFNOR : **"Systèmes de traitement de l'information : modèle de référence pour l'interconnexion de systèmes ouverts"**, Document AFNOR n°Z 70-001, Paris La Défense (France), juin 1982.

AND'75 G.A. ANDERSON et E.D. JENSEN : **"Computer interconnection structures: taxonomy, characteristics, and examples"**, Computing Surveys, vol.7 n°4, décembre 1975, pp.197-213.

AND'81 T. ANDERSON et P.A. LEE : **"Fault-tolerance, principles and practice"**, (en particulier chapitre 2, pp.29-36), Prentice-Hall Int., 1981.

AUG'81 M.AUGER : **"Présentation de PROWAY"**, note n°HN 231, EDF Service Normalisation et Brevets, Clamart (France), novembre 1981.

AYA'82 J.M. AYACHE, J.P. COURTIAT, et M. DIAZ : **"REBUS, A fault-tolerant distributed system for industrial real-time control"**, IEEE Trans. on Comp. vol. C-31 n°7, juillet 1982, pp.637-647.

BAR'79 M. BARRERE : **"La protection des réseaux"**, Mémoire de diplôme d'ingénieur CNAM. Conservatoire National des Arts et Métiers, Centre Associé de Pau (France), mai 1979.

BEO'77 C.BEOUNES : **"Automate Sûr et Modulaire Adapté aux Régulations Avioniques : ASMARA"**, Thèse de Docteur Ingénieur, Institut National Polytechnique de Toulouse (France), novembre 1977.

BIN'82 S.E. BINNS, I.N. DALLAS, et E.B. SPRATT : **"Further developments on the Cambridge ring network at the University of Kent"**, Proc. of the IFIP Symposium on Local Computer Networks, Florence (Italie), 19-21 avril 1982, pp.183-204.

BLA'81 J.P. BLANQUART, K.KANOUN, et J.C. LAPRIE : **"Sûreté de fonctionnement des automatismes des postes THT : définition du support d'échange des informations"**, Contrat EDF n°47836. Note technique LAAS n°81T25, Toulouse (France), juillet 1981.

BLA'82 G.S. BLAIR et W.D. SHEPHERD : **"A performance comparison of Ethernet and the Cambridge Digital Communication Ring"**, Computer Networks vol.6, 1982, pp.105-113.

BOU'80a J.L. BOUSSIN et P. ERHARD : **"Projet PANDOR. Architecture cible. Temps d'élimination des défauts"**, note manuscrite EDF, Département FORCAM, Clamart (France), 1980.

BOU'80b J.L. BOUSSIN : **"Projet PANDOR. Système de transmission par bus dans un poste THT"**, note manuscrite EDF, Département FORCAM, Clamart (France), 1980.

BUX'82 W. BUX, F. CLOSS, P.A. JANSON, K. KÜMMERLE, H.R. MÜLLER, et E.H. ROTHAUSER : **"A local-area communication network based on a reliable token-ring system"**, Proc. of the IFIP Symposium on Local Computer Networks, Florence (Italie), 19-21 avril 1982, pp.69-82.

BUX'83 W. BUX et M. SCHLATTER : "**An approximate method for the performance analysis of buffer insertion rings**", IEEE Trans. on Comm. vol COM-31 n°1, janvier 1983, pp.50-55.

CAR'82 W.C. CARTER : "**A time for reflection**", Proc. of the 12th Symposium on Fault-Tolerant Computing, Santa-Monica (Californie), 22-24 juin 1982, p.41.

CLA'78 D.D. CLARK, K.T. POGRAN, D.P. REED : "**An introduction to local area networks**", Proc. of IEEE, vol.66 n°11, novembre 1978, pp.1497-1517.

COS'81 A. COSTES, J.E. DOUCET, C. LANDRAULT, et J.C. LAPRIE : "**SURF, a program for dependability evaluation of complex fault-tolerant computing systems**", Proc. of the 11th symposium on Fault-Tolerant Computing, Portland (Maine), 24-26 juin 1981, pp.72-78.

DAV'81 D.W. DAVIES et R.W. WATSON : chapitre 6 (en particulier section 6.6, pp.109-118) de "**Distributed systems- Architecture and implementation (an advanced course)**", Lecture Notes in Computer Science, vol.105, 1981.

DEB'81 S. DE BATZ, A. MERLIN, et G. SANTUCCI : "**Les méthodes de détermination du schéma directeur du réseau de transport**", Revue Générale d'Electricité, Tome 90 n°6, juin 1981, pp.479-485.

DEG'82 G. DE GRANDI et G.P. ROSSI : "**Design issues for a fibre optic local network**", Computer Communications vol.5 n°2 avril 1982, pp.65-70.

DIC'78 M.E. DICKOVER, C.L. McGOWAN, et D.T. ROSS : "**Software design using SADT**", Structured analysis and design, state of the art report, pp.99-114, Maidenhead (Angleterre), Infotech Int., 1978.

EDF'75 ELECTRICITE DE FRANCE : "**Le plan de protection "Palier technique 1975", ses principes**", note n°D.63/328 EDF Département Exploitation, Paris (France), novembre 1975.

ECM'79 ECMA : "**HDLC: Elements of procedure**", document TC9-ECMA-49, mai 1979.

ENJ'82 ENJEUX : "**Dossier Réseaux informatiques, les normes-clés de la communication**", Enjeux (AFNOR) n°28, septembre 1982, pp.28-70.

ENS'78 P.H. ENSLOW Jr : "**What is a "distributed" data processing system?**", IEEE Computer vol.11 n°1, janvier 1978, pp.13-21.

FAR'69 W.D. FARMER et E.E. NEWHALL : "**An experimental distributed switching system to handle bursty computer traffic**", Proc. of the ACM Symposium on the Problems in the Optimization of Data Communication Systems, Pine Mountain (Géorgie), octobre 1969, pp.1-33.

HAL'82 A.P.B. HALLEY et H. DAVIE : "**A fault-tolerant communications ring for on-line distributed control systems**", 4th International Conference on Trends in On-line Computer Control Systems, 5-8 avril 1982, publication IEE n°208, pp.30-33.

HAF'74 E.R. HAFNER, Z. NENADAL, et M. TSCHANZ : "**A digital loop communication system**", IEEE Trans. on Comm. vol. COM-22 n°6, juin 1974, pp.877-881.

HOL'82 C. HOLWECK : **"Les systèmes de transmissions numériques associés aux protections : Transmission entre tranches"**, Communication présentée par la Société ENERTEC à la journée SEE "Numérisation des protections et des fonctions connexes dans les postes THT", Gif-sur-Yvette (France), 17 juin 1982.

IEE'81 IEEE Project 802. **Local Networks Standards Committee- A Status report. Draft B**, octobre 1981.

IHA'82 H. IHARA et K. MORI : **"Highly reliable computer network system based on autonomous decentralization concept"**, Proc. of the 12th Symposium on Fault-Tolerant Computing, Santa-Monica (Californie), 22-24 juin 1982, pp.187-194.

INF'82 INFOREP/BNI : **"Le point sur la normalisation des réseaux informatiques"**, document INFOREP/BNI diffusé par C.X.P, PARIS (France), juin 1982.

KAN'82 K. KANOUN et M. RODRIGUES : **"Sûreté de fonctionnement des automatismes des postes THT : Tolérance aux fautes dans REBECCA, support d'échange des informations"**, Contrat EDF n°47836, note LAAS n°82041, Toulouse (France), juillet 1982.

KLE'78 C. KLEEKAMP et B. METCALFE : **"Designer's guide to fiber optics"**, présenté par EDN Magazine, 5 mars 1978.

LAP'75 J.C. LAPRIE : **"Prévision de la sûreté de fonctionnement et architecture de structures numériques temps réel réparables"**, Thèse de Doctorat d'Etat, Université Paul Sabatier, Toulouse (France), juin 1975.

LAP'76 J.C. LAPRIE : **"On reliability prediction of repairable redundant digital structures when neglecting repair times"**, IEEE Trans. on Reliability, vol.R-20 n°4, octobre 1976, pp.256-258.

LAP'79 J.C. LAPRIE, A. COSTES, et R. TROY : **"La sûreté de fonctionnement : besoins et solutions"**, Congrès SEE sur la Sûreté des Systèmes Electriques et Electroniques, Toulouse (France), octobre 1979.

LAP'82a J.C. LAPRIE et A. COSTES : **"Dependability: a unified concept for reliable computing"**, Proc. of the 12th Symposium on Fault-Tolerant Computing, Santa-Monica (Californie), 22-24 juin 1982, pp.18-21.

LAP'82b J.C. LAPRIE : **"Systèmes de sécurité et sécurité des systèmes"**, Journées Rail et Recherche, Paris (France), 1-3 décembre 1982.

LEL'79 G. LE LANN : **"Le contrôle dans les systèmes informatiques répartis : nature du problème et quelques solutions"**, Cours IRIA sur les Systèmes Informatiques Localement Répartis, Rocquencourt (France), 4-7 décembre 1979, pp.1-22.

LIU'81 M.T. LIU, D.P. TSAY, C.P. CHOU, et C.M. LI : **"Design of the Distributed Double-Loop Computer Network (DDLCN)"**, Journal of Digital Systems, vol.5 n°1/2, 1981, pp.3-37.

LUC'78 E.C. LUCZAK : **"Global bus computer communication techniques"**, Proc. of 1978 Computer Networking Symposium, Gaithersburg (Maryland), 13 décembre 1978, pp.58-71.

MIR'81 V.L. MIRTICH : "**Fiber optics offers promise in data network design**", EDN, 4 mars 1981.

MAR'78 M. MARINESCU : "**Mécanisme de communication par bus série pour des réseaux informatiques locaux**", Thèse de troisième cycle, Institut National Polytechnique de Grenoble (France), septembre 1978.

MED'80 K.MEDHAFFER-KANOUN : "**Evaluation de la sûreté de fonctionnement des systèmes de sécurité. Application à la commande des postes à très haute tension**", Thèse de Docteur-Ingénieur, Institut National Polytechnique de Toulouse (France), juillet 1980.

MET'76 R.M METCALFE et D.R. BOGGS : "**Ethernet: distributed packet switching for local computer networks**", Communications of the ACM vol.19 n°7, juillet 1976, pp.395-404.

PEN'79 B.K. PENNEY et A.A. BAGHDADI : "**Survey of computer communications loop networks**" (en 2 parties), Computer Communications vol.2 n°4, août 1979, pp.165-180, et vol.2 n°5 octobre 1979, pp.224-241.

PIE'72 J.R. PIERCE : "**Network for block switching of data**", Bell System Technical Journal vol.51 n°6, juillet-août 1972, pp.1133-1145.

PIL'82 E. PILAUD : "**Conception et validation de systèmes informatiques à haute sûreté de fonctionnement**", Thèse de Docteur-Ingénieur, Institut National Polytechnique de Grenoble (France), novembre 1982.

POW'81 D.R. POWELL : "**Réseaux locaux de commande-contrôle sûrs de fonctionnement**", Thèse de Doctorat d'Etat, Institut National Polytechnique de Toulouse (France), octobre 1981.

RAW'78 E.G. RAWSON, et R.M. METCALFE : "**Fibernet: multimode optical fibers for local computer networks**", IEEE Trans. on Comm. vol. COM-26 n°7, juillet 1978, pp.983-990.

REA'75 C.C REAMES et M.T. LIU : "**A loop network for simultaneous transmission of variable length messages**", Proc. of the 2nd Annual Symposium on Computer Architecture, Houston (Texas), 20-22 janvier 1975, pp.7-12.

RIC'83 J. RICHARD JONES : "**Consider fiber optics for local-network designs**", EDN, 3 mars 1983.

RGE'sp REVUE GENERALE D'ELECTRICITE : **Numéros spéciaux sur le réseau de transport, les postes THT et leur protection**, Tome 83 n°2, février 1974 ; tome 88 n°10, octobre 1979 ; tome 90 n°6, juin 1981 ; tome 90 n°7/8, juillet/août 1981.

SAL'81 J.H. SALTZER et D.D. CLARK : "**Why a ring?**", Proc. of the 7th Data Communications Symposium, Mexico, 27-29 octobre 1981, pp.211-217.

ZAF'74 P. ZAFIROPULO : "**Performance evaluation of reliability improvement techniques for single-loop communications systems**", IEEE Trans. on Comm. vol. COM-22 n°6, juin 1974, pp.742-751.

TABLE DES MATIERES

Thèse de Monsieur Jean-Paul BLANQUART

« Conception d'un support de communication sûr de fonctionnement pour systèmes de surveillance et de sécurité : REBECCA »

RÉSUMÉ :

Ce mémoire est consacré à la conception d'un support de communication sûr de fonctionnement, à temps d'accès borné et faible, pour systèmes distribués de surveillance et sécurité. L'analyse effectuée conduit à une approche par double décomposition intégrant la validation progressive des choix : la conception est menée par **affinements successifs,** conjointement sur plusieurs **niveaux d'abstraction** afin de prendre en compte l'ensemble des contraintes et de leurs interactions. Pour l'application traitée dans ce mémoire : le système réparti de protection des postes à très haute tension du réseau électrique français, deux niveaux d'abstraction sont retenus : transmission et transfert. Les choix et leur validation reposent sur des critères adaptés à chaque étape, qualitatifs (décentralisation, latence minimale...) et quantitatifs (durée d'acheminement de rafales de messages urgents, évaluation de la sûreté de fonctionnement et plus particulièrement de la **sécurité**). Cette méthode permet de retenir un support reconfigurable à deux boucles optiques contrarotatives indépendantes avec accès asynchrone par la technique d'insertion de registre.

MOTS CLÉS : Sûreté de fonctionnement, Systèmes distribués, Réseau local, Temps réel, Architecture en boucle, Insertion de registre.

« Design of a dependable communication subsystem for monitoring and safety systems : REBECCA »

ABSTRACT :

This dissertation reports the methodology and the results concerning the definition of a dependable communication subsystem with low bounded access time for distributed monitoring and safety systems. Analysis leads to a double decomposition approach with progressive validation of the various design decisions : **successive refinements** are processed simultaneously at several **abstract levels.** This approach allows all the relevant requirements and their interactions to be taken into account at each step. This methodology is applied to the distributed protection system of the extra-high voltage substations of the French electricity distribution network. Two abstract levels are defined : the transmission and transfer levels. Design decisions are validated using criteria adapted to each step : qualitative ones (decentralisation, latency...) and quantitative ones (time needed for processing bursts of messages, dependability evaluation and in particular **safety** evaluation). The resulting system consists of a reconfigurable optical counter-rotating double loop. Each loop is independently accessed in a asynchronous way using the register insertion technique.

KEY WORDS : Dependability, Distributed computing, Local area network, Real-time, Loop architecture, Register-insertion.