Spécifications et analyse d'un pilote automatique embarqué de métro type V.A.L

Mahrez Azouni

THESE

présentée à

Institut National Polytechnique de Grenoble

pour obtenir le grade de

DOCTEUR INGENIEUR
(Génie Informatique)

par

Mahrez AZOUNI

SPECIFICATIONS ET ANALYSE

D'UN PILOTE AUTOMATIQUE EMBARQUE DE METRO TYPE V.A.L.

Thèse soutenue le 17 décembre 1979 devant la Commission d'Examen :

Mme	G. SAUCIER	Président
M.	J.F. LEMAÎTRE	Rapporteur
MM.	P. CASPI	Examinateurs
	M. CORAZZA	
	P. LESTAMPS	
	B. LETRUNG	

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Année universitaire 1977-1978

Président : M. Philippe TRAYNARD

Vice-présidents : M. René PAUTHENET

M. Georges LESPINARD

PROFESSEURS TITULAIRES

MM.	BENOIT Jean	Electronique - automatique
	BESSON Jean	Chimie minérale
	BLOCH Daniel	Physique du solide - cristallographie
	BONNETAIN Lucien	Génie chimique
	BONNIER Etienne	Métallurgie
*	BOUDOURIS Georges	Electronique - automatique
	BRISSONNEAU Pierre	Physique du solide - cristallographie
	BUYLE-BODIN Maurice	Electronique - automatique
	COUMES André	Electronique - automatique
	DURAND Francis	Métallurgie
	FELICI Noël	Electronique - automatique
	FOULARD Claude	Electronique - automatique
	LANCIA Roland	Electronique - automatique
	LONGEQUEUE Jean-Pierre	Physique nucléaire corpusculaire
	LESPINARD Georges	Mécanique
	MOREAU René	Mécanique
	PARIAUD Jean-Charles	Chimie - physique
	PAUTHENET René	Electronique - automatique
	PERRET René	Electronique - automatique
	POLOUJADOFF Michel	Electronique - automatique
	TRAYNARD Philippe	Chimie - physique
	VEILLON Gérard	Informatique fondamentale et appliquée

* en congé pour études

PROFESSEURS SANS CHAIRE

MM.	BLIMAN Samuël	Electronique - automatique
	BOUVARD Maurice	Génie mécanique
	COHEN Joseph	Electronique - automatique
	GUYOT Pierre	Métallurgie physique
	LACOUME Jean-Louis	Electronique - automatique
	JOUBERT Jean-Claude	Physique du solide - cristallographie

.../...

MM.	ROBERT André	Chimie appliquée et des matériaux
	ROBERT François	Analyse numérique
	ZADWORNY François	Electronique - automatique

MAITRES DE CONFERENCES

MM.	ANCEAU François	Informatique fondamentale et appliquée
	CHARTIER Germain	Electronique - automatique
	CHIAVERINA Jean	Biologie, biochimie, agronomie
	IVANES Marcel	Electronique - automatique
	LESIEUR Marcel	Mécanique
	MORET Roger	Physique nucléaire - corpusculaire
	PIAU Jean-Michel	Mécanique
	PIERRARD Jean-Marie	Mécanique
	SABONNADIERE Jean-Claude	Informatique fondamentale et appliquée
Mme	SAUCIER Gabrielle	Informatique fondamentale et appliquée
M.	SOHM Jean-Claude	Chimie Physique

CHERCHEURS DU C.N.R.S. (Directeur et Maîtres de Recherche)

M.	FRUCHART Robert	Directeur de Recherche
MM.	ANSARA Ibrahim	Maître de Recherche
	BRONOEL Guy	Maître de Recherche
	CARRE René	Maître de Recherche
	DAVID René	Maître de Recherche
	DRIOLE Jean	Maître de Recherche
	KLEITZ Michel	Maître de Recherche
	LANDAU Ioan-Doré	Maître de Recherche
	MATHIEU Jean-Claude	Maître de Recherche
	MERMET Jean	Maître de Recherche
	MUNIER Jacques	Maître de Recherche

Personnalités habilitées à diriger des travaux de recherche (décision du Conseil Scientifique) E.N.S.E.E.G.

MM.	BISCONDI Michel	Ecole des Mines St. Etienne (dépt. Métallurgie)
	BOOS Jean-Yves	Ecole des Mines St. Etienne (Métallurgie)
	DRIVER Julian	Ecole des Mines St. Etienne (Métallurgie)

.../...

MM.	KOBYLANSKI André	Ecole des Mines St. Etienne (Métallurgie)
	LE COZE Jean	Ecole des Mines St. Etienne (Métallurgie)
	LESBATS Pierre	Ecole des Mines St. Etienne (Métallurgie)
	LEVY Jacques	Ecole des Mines St. Etienne (Métallurgie)
	RIEU Jean	Ecole des Mines St. Etienne (Métallurgie)
	SAINFORT	C.E.N. Grenoble (Métallurgie)
	SOUQUET	U.S.M.G.
	CAILLET Marcel	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	COULON Michel	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	GUILHOT Bernard	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	LALAUZE René	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	LANCELOT Francis	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	SARRAZIN Pierre	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	SOUSTELLE Michel	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	THEVENOT François	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	THOMAS Gérard	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	TOUZAIN Philippe	Ecole des Mines St. Etienne (Chim. Min. Ph.)
	TRAN MINH Canh	Ecole des Mines St. Etienne (Chim. Min. Ph.)

E.N.S.E.R.G.

MM.	BOREL	Centre d'études nucléaires de Grenoble
	KAMARINOS	Centre national recherche scientifique

E.N.S.E.G.P.

M.	BORNARD	Centre national recherche scientifique
Mme	CHERUY	Centre national recherche scientifique
MM.	DAVID	Centre national recherche scientifique
	DESCHIZEAUX	Centre national recherche scientifique

Je remercie tous les membres du jury :

— Madame G. SAUCIER, Professeur à l'Institut National Polytechnique de Grenoble, qui préside ce jury.

— Monsieur J.F. LEHAÎTRE, Directeur au Centre d'Etudes et de Recherche de Toulouse (CERT / DERA), qui a suivi de près ce travail, et a accepté d'être rapporteur de cette thèse.

— Monsieur P. CASPI, Chargé de Recherche au C.N.R.S, qui m'a aidé à résoudre quelques points délicats,

— Monsieur M. CORAZZA, Professeur à l'Université de Rennes, qui s'est intéressé à mon travail, et a été d'une extrême gentillesse et disponibilité à mon égard

— Monsieur P. LESTAMPES, Directeur technique et responsable du Groupe "Sécurité - Disponibilité" du futur Métro de la ville de Lille, qui a accepté l'invitation de l'IRT afin d'assister à la soutenance de ma thèse

— Monsieur B. LETRUNG, Ingénieur de Recherche au Département "Métrologie - Automatismes" à l'Institut de Recherche des Transports et qui m'a toujours soutenu, conscient de la difficulté de ce travail.

J'ai effectué ce travail au :
- Laboratoire d'Informatique et de Mathématiques Appliquées de Grenoble Equipe "Conception et Sécurité des Systèmes Logiques", et au
- Département "Métrologie - Automatismes", à l'Institut de Recherche des Transports.

SOMMAIRE

N.B: Certains chapitres sont précédés d'un sommaire plus détaillé.

0 - INTRODUCTION

0.I - PRESENTATION GENERALE

0.II - PROBLEMES POSES

0.III - PROPOSITION D'UNE METHODOLOGIE DE CONCEPTION SURE

0.IV - ORGANISATION DE LA THESE

O.I - PRESENTATION GENERALE

Depuis quelques années, le développement de l'informatique et l'avènement sur le marché des composants monolithiques à très haute intégration ont amené, pour des raisons de fiabilité, de coût et de performance, les constructeurs d'automatismes à opter pour des réalisations programmées.

Devant un tel développement, les méthodes classiques de conception et d'analyse se sont avérées peu efficaces. Dans le domaine des transports (aviation, véhiculation en site propre) où la sécurité est un critère primordial, la nécessité de disposer de nouvelles méthodologies se fait de plus en plus sentir aussi bien pour le concepteur qui doit respecter un certain niveau de sécurité que pour l'organisme qui doit certifier le nouveau système conçu, et en autoriser la délivrance du visa d'exploitation.

C'est dans cette optique que le sujet de cette thèse m'a été proposé par l'Institut de Recherche des Transports :

Il s'agit d'étudier la sécurité du pilote automatique d'une nouvelle formule de métro, totalement automatisé, le V.A.L.

Une première version du V.A.L. constitue le futur métro de Lille, et a été réalisée par la Société "ENGINS MATRA" sur composants discrets : des modifications ont été apportées au brevet où sont stipulés les principes de base de fonctionnement, et cela afin de garantir une sécurité acceptable.

Pour nous, il s'agissait de considérer deux aspects :

- Proposer et décrire des réalisations possibles des différentes fonctions à élaborer par le système, tout en suivant de très près les principes de base décrits dans le brevet. Nous avons en fait tenu à exploiter la simplicité du brevet qui en fait l'originalité.
- Réfléchir sur une méthodologie de conception sûre de système de commande en temps réel en vue d'une réalisation programmée.

O.II- PROBLEMES POSES

II-1) Problèmes dûs à l'ambiguité de présentation d'un cahier des charges

D'habitude, un cahier des charges est présenté sous la forme d'un document informel ; la rédaction d'un tel document écrit dans un langage courant peut donner lieu à une mauvaise interprétation de la part des différentes personnes y ayant accès.

Par ailleurs, les spécifications fonctionnelles sont nées d'une intuition, d'une inspiration, ou d'une documentation : elles peuvent donc être fausses, ambigues ou incomplètes ; et souvent cela constitue des retards dans la conception (remise en cause des spécifications lorsque le système est déjà dans une phase de réalisation avancée).

II-2) Problèmes dûs à l'utilisation de composants monolithiques hautement intégrés.

. Les modèles de panne classiques s'avèrent inadéquats : ceux-ci sont fondés sur des hypothèses qui ne sont plus vérifiées. Au niveau de la porte logique, les hypothèses de collage à 0 ou à 1 se trouvent généralement mises en défaut, bien que dans certaines technologies, elles continuent d'être acceptées (certains défauts internes aux transistors en technologie MOS, ou les coupures de connexion en technologie TTL sont considérés comme des collages).

. La non connaissance parfaite de l'équivalent logique des circuits intégrés n'est pas suffisante pour décrire leur comportement en cas de panne.

. L'énumération des modes de panne est rendue impossible, leur nombre variant d'une manière exponentielle en fonction de la complexité du système.

. L'hypothèse de l'indépendance des pannes simples n'est plus vraie. Une panne simple peut affecter tout un ensemble de portes logiques dans le cas des technologies MSI et LSI.

. Aux problèmes matériels, s'ajoutent ceux relatifs au logiciel : notamment, la fiabilité du logiciel est encore mal connue, et il est actuellement difficile de prouver qu'un programme est correct.

II-3) Problèmes dûs à l'influence de l'environnement extérieur

Les évènements engendrés par l'environnement ont des fréquences aléatoires, des fréquences maximales très grandes ou très petites, et cela crée des difficultés lorsqu'on essaie de les décrire.

O.III - PROPOSITION DE METHODOLOGIE

La conception sûre d'un système de commande en temps réel doit donc se poser en termes nouveaux par rapport aux conceptions précédentes sur composants discrets.

De quoi a-t-on besoin ?

Pour une approche sûre, il est nécessaire de disposer :

a - d'un bon outil de spécification et d'analyse

Les caractéristiques d'un tel outil doivent être les suivantes :

- Il doit être d'un formalisme simple afin qu'il puisse être compris par tout lecteur, indépendant de toute technologie, et riche en concepts et primitives afin de pouvoir représenter une gamme de cahiers de charges assez étendue : pouvoir notamment exprimer la séquentialité, le parallélisme, l'exclusion mutuelle, la synchronisation entre deux processus indépendants.

- Il doit permettre la description d'un fonctionnement asynchrone, ainsi que celle de l'environnement extérieur.

- Il est intéressant qu'un tel outil puisse se présenter sous une forme de graphisme permettant d'avoir un aspect visuel du système.

- Il doit permettre de vérifier la cohérence du fonctionnement du système : (absence de blocages et de situations de conflits, d'incohérences des spéci-

b - d'une bonne méthode d'analyse de la sécurité :

Il est souhaitable qu'une telle méthode puisse exploiter toutes les caractéristiques offertes par l'outil de représentation. Une analyse de la sécurité ne peut être efficace et cohérente que si le fonctionnement du système est bien assimilé, ce qui n'est possible que si ce fonctionnement est correctement décrit.

L'approche que nous proposons, d'une manière générale, dans une conception sûre d'un système de commande en temps réel, peut se décomposer en trois phases principales : (fig.1)

Phase 1 : Modélisation

Phase 2 : Validation

Phase 3 : Réalisation matérielle

Remarque :

A la fin de la phase 2, l'analyse de la sécurité permet de déterminer les parties critiques du système, et par conséquent aide à la mise en place de moyens de vérification, auxquels nous avons consacré toute une étude [AZ077]

- Implantation de vérificateurs de propriétés invariantes
- Redondance algorithmique
- Redondance de données
- Implantation de vérificateurs homomorphes,....

Ces vérificateurs peuventêtre implantés soit sur le même matériel que le système, soit sur des matériels différents.

Dans cette thèse, on ne parlera ni de tels moyens de vérification ni de la réalisation matérielle du système.

L'accent est surtout mis sur les phases de modélisation et de validation lesquelles constituent une partie primordiale dans une étude de conception.

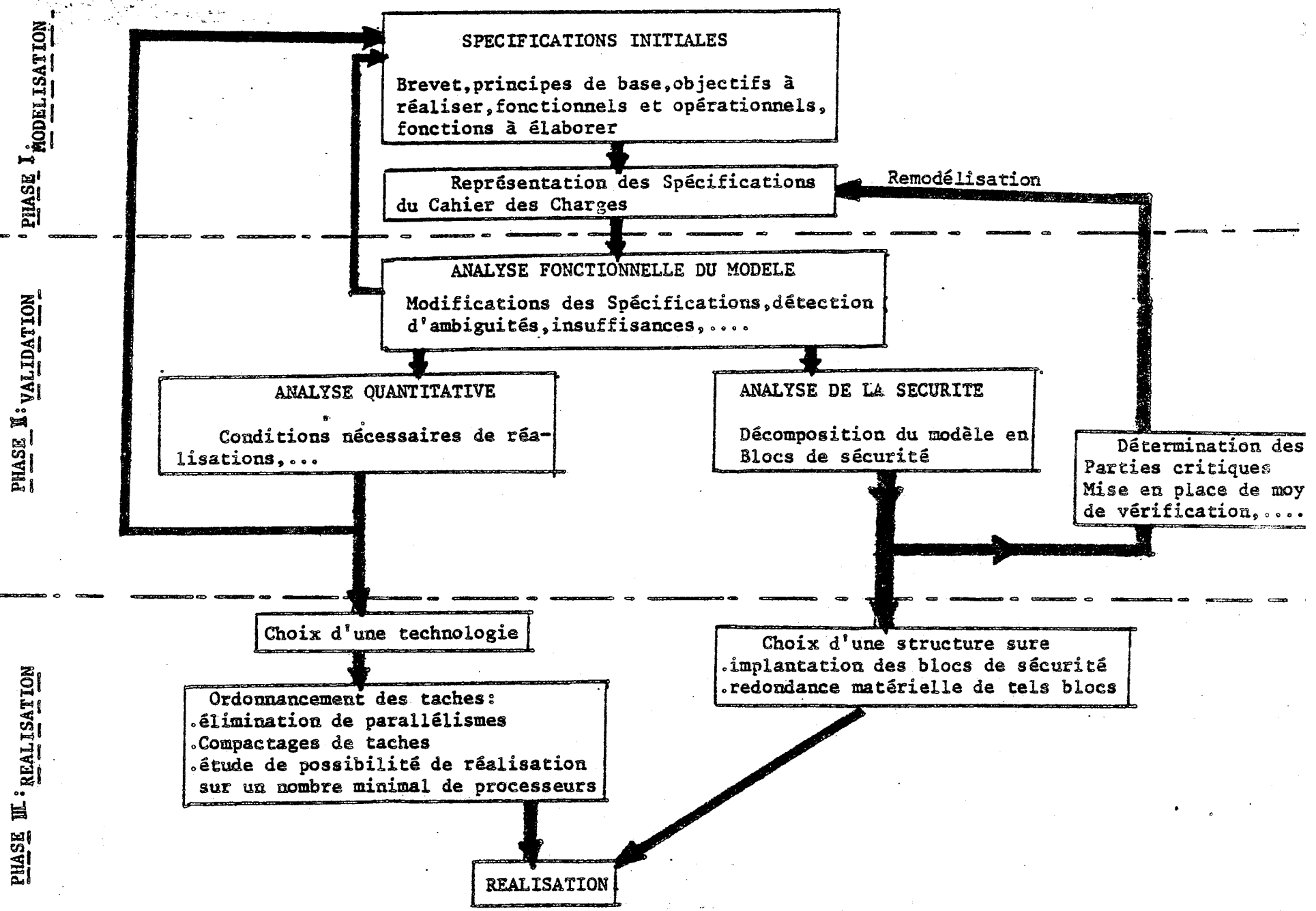

PHASE I : MODELISATION
PHASE II : VALIDATION
PHASE III : REALISATION
SPECIFICATIONS INITIALES
Brevet, principes de base, objectifs à réaliser, fonctionnels et opérationnels, fonctions à élaborer
Représentation des Spécifications du Cahier des Charges
Remodélisation
ANALYSE FONCTIONNELLE DU MODELE
Modifications des Spécifications, détection d'ambiguités, insuffisances, ...
ANALYSE QUANTITATIVE
Conditions nécessaires de réalisations, ...
ANALYSE DE LA SECURITE
Décomposition du modèle en Blocs de sécurité
Détermination des Parties critiques
Mise en place de moy de vérification, ...
Choix d'une technologie
Choix d'une structure sure
.implantation des blocs de sécurité
.redondance matérielle de tels blocs
Ordonnancement des taches:
.élimination de parallélismes
.Compactages de taches
.étude de possibilité de réalisation sur un nombre minimal de processeurs
REALISATION

Fig. 1

O.IV - ORGANISATION DE LA PRESENTE THESE

Le 1er chapitre présente les principes de base régissant le fonctionnement du V.A.L. Nous y proposons par ailleurs des réalisations possibles des différentes fonctions du système. Nous avons défini une nouvelle fonction de calcul de vitesse de consigne de sécurité permettant de corriger les défaillances du pilote automatique et le trainage de la vitesse réelle par rapport à la vitesse de commande, et avons introduit une nouvelle notion de "plots fictifs" dans le fonctionnement du système en station, afin de conserver au principe du canton temporel défini dans le brevet sa capacité d'assurer une sécurité propre d'anti-collision.

Dans ce chapitre, chaque fonction est décrite comme une "boîte noire" définie à partir de signaux d'entrée reçus par des capteurs, et des signaux logiques de sortie.

Le 2ème chapitre est consacré à l'évaluation des objectifs de fiabilité et de sécurité qui doivent être réalisés lors de la mise en exploitation du système.

Le 3ème chapitre traite de la représentation graphique des spécifications fonctionnelles décrites dans le premier chapitre. Après le rappel des Réseaux de Pétri, et de quelques modèles dérivés, nous donnons les règles d'évolution des Réseaux de Pétri Interprétés, c'est-à-dire auxquels on a donné une signification en précisant les liens du système avec l'Environnement extérieur (on explicite les évènements reçus de l'extérieur, et les actions envoyées vers l'extérieur).

Une comparaison est ensuite faite avec le GRAFCET dont nous avons pensé donner une extension à l'interprétation afin qu'il puisse spécifier les systèmes de commande en temps réel. Cette comparaison nous a amenés à utiliser le GRAFCET comme outil de description, et le Réseau de Pétri Interprété en tant qu'outil d'analyse et de conception.

Dans ce chapitre, on décrit alors chaque fonction séparément, et les GRAFCETS qui la représentent sont analysés en détail, ce qui nous permet de relever certaines ambiguités, incohérences ou insuffisances dans les spécifications initiales du cahier des charges.

Le 4ème chapitre montre comment on procède pour construire le modèle fonctionnel du pilote automatique. Le passage du GRAFCET au Réseau de Pétri Interprété se fait, tout en respectant les contraintes imposées lors de l'analyse précédente, par l'étude de la synchronisation des variables communes aux différents Grafcets décrits précédemment (étude d'un graphe de dépendance), et par celle des dépendances dues aux variables externes communes. A ce niveau, les spécifications concernant le fonctionnement global du système sont analysées.

Dans le 5ème chapitre, il s'agit de valider quantitativement le modèle fonctionnel obtenu, et de vérifier que le système ainsi spécifié peut être effectivement réalisé (prise en compte obligatoire de certains évènements, " sauvitude" de chaque place du Réseau obtenu").

Pour valider le modèle, on établit toutes les conditions nécessaires à la réalisation, reliant les fréquences des évènements et les durées des tâches à exécuter par le système. On démontre que de telles conditions sont nécessaires et suffisantes, en établissant des propriétés relatives aux compteurs.

Le 6ème chapitre est consacré à l'analyse de la sécurité du pilote automatique. Cette analyse utilise une méthode classique par "arbres de causes" ("Fault-Tree Analysis"), laquelle est rendue à la fois aisée et cohérente par un simple examen du modèle fonctionnel.

Une décomposition du modèle en blocs de sécurité est alors donnée, permettant dans une réalisation pratique une possibilité d'avoir des structures redondantes.

CHAPITRE I

SPECIFICATIONS FONCTIONNELLES DU CAHIER DES CHARGES

A. Principes de base de fonctionnement du V.A.L.
   1. Notion de canton temporel
   2. Equations de base
   3. Principe de l'arrêt du temps

B. Etude du pilote automatique (P.A.)
   1. Etude de la vitesse de régulation (Ve)
      1.1. Vitesse de programme (Vp)
      1.2. Vitesse (Ve)

   2. Sécurité anti-collision

   3. Etude de la vitesse limite (V_L)
      3.1. Mesure de la longueur d'interplot
      3.2. Décodage des balises

   4. Etude de la vitesse de consigne de sécurité (V_{CS})
      4.1. Etude de la répartition des plots en phase de décélération
      4.2. Etude de la vitesse (V_{CS}) non lissée
      4.3. Etude de la vitesse (V_{CS}) lissée

   5. Automatisation du stationnement et du départ des stations
      5.1. Phase d'arrêt
      5.2. Phase de stationnement
      5.3. Phase de démarrage
      5.4. Régulation en station. Notion de plots fictifs.

CONCLUSION

Présentation des objectifs à réaliser

Les objectifs fixés par le Cahier des Charges du V.A.L sont les suivants [RAL 73]

01. Automatisation totale :

Pas de personnel requis dans les rames ni dans les stations.

02. Régulation d'horaire :

Rattrapage des retards aléatoires dûs aux temps de stationnement

03. Régulation d'intervalle :

Respect d'un intervalle séparant deux rames successives .

04. Pilotage automatique :

Conduite respectant un diagramme de vitesses limites .

05. Sécurité anti-collision .

06. Précision d'arrêt en station.

07. Automatisation du stationnement et du départ des stations.

Un principe de base de fonctionnement du système et une description des fonctions réalisant de tels objectifs ont fait l'objet d'un brevet déposé au nom de l'E.P.A.L.E. (ANVAR n° 7125386).

Une première réalisation faite par la Société "Engins-MATRA" (1974) n'a pas retenu l'ensemble des spécifications définies dans le brevet.

C'est ainsi que les fonctions réalisant les objectifs 02, 03 et 05 ont été modifiées. En outre, il a été ajouté au système un dispositif de sécurité anti - collision, basé sur le principe bien connu du canton déformable mobile, consistant à faire calculer par chaque rame la distance qui la sépare de la rame qui la précède, et à maintenir constamment cette distance supérieure à une distance critique d'arrêt.

Dans le système que nous allons présenter ici, et qui va constituer le support de travail de cette thèse, nous avons cherché à rester le plus proche possible des spécifications décrites dans le brevet.

Nous avons respecté les principes des fonctions définies dans le brevet, et nous avons proposé des réalisations possibles qui rejoignent seulement en quelques points celles adoptées dans la réalisation initiale faite par MATRA. Nous avons, par ailleurs, défini une nouvelle fonction de sécurité intervenant notamment dans les phases critiques de décélération.

A. PRINCIPES DE BASE DE FONCTIONNEMENT DU V.A.L .

Ces principes sont présentés dans [GAB 73]; nous allons en rappeler l'essentie

A.1- Notion de canton temporel

A toute rame réelle est associée une rame fictive qui suit un programme de marche-type. La rame réelle doit suivre le plus près possible la marcl de la marche fictive.

Des plaques métalliques, dites plots ou balises (selon leur dimension), sont placées le long de la voie. Le programme de marche-type consiste à parcourir la distance séparant deux plaques successives en un temps constant To.

Notation :

On désignera par :

$H^R_p(n)$: l'heure de passage de la rame réelle p devant le nième plot

H^F_{np} : l'heure de passage de la rame fictive p devant le nième plot (c'est l'heure calculée par le programme de marche-type) .

$H^F_{n(p+1)}$: l'heure de passage de la rame fictive p +1,(c'est à dire la rame fictive suivante), devant le nième plot.

Considérons la double inégalité suivante :

(1) $H^F_{np} < H^R_{p(n)} < H^F_{n(p+1)}$

Si(1) est scrupuleusement respectée, aucun risque de collision n'est à craindre dans la marche des rames réelles.

Dans un diagramme (Temps, Distance), portons en abscisse l'axedu temps et en ordonnée l'axe des distances (fig.1).

La double inégalité (1) oblige la rame réelle p à rester dans un intervalle délimité par Hnp et Hn(p+1), appelé "canton temporel".

Sur le diagramme tracé sur la figure 1, on obtient une succession de cantons tempore glissant régulièrement le long de l'axe des temps.

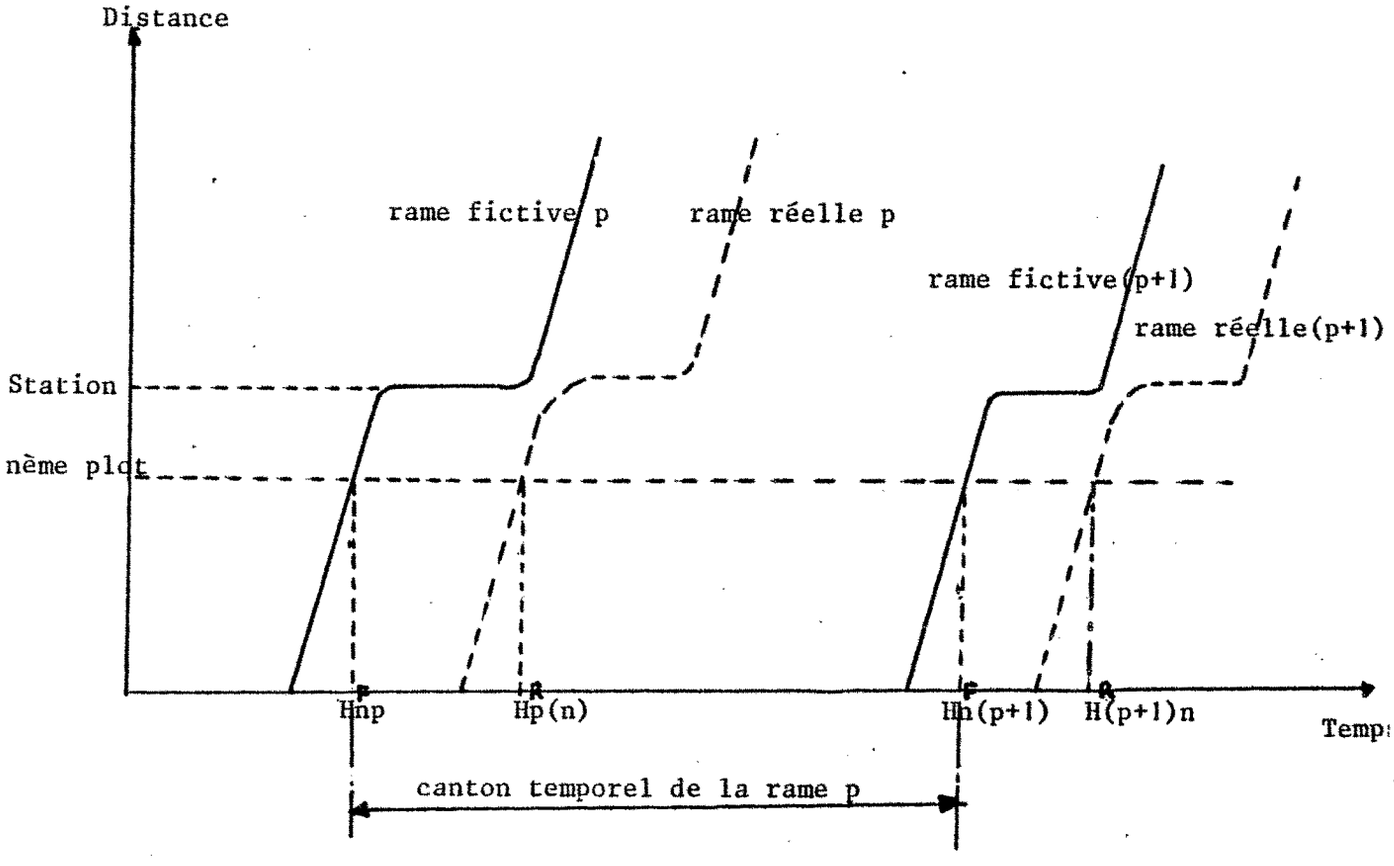


Fig.1 Principe du canton temporel

Remarque :

La sécurité anti-collision dans les systèmes classiques est basée sur le principe de l'exclusion mutuelle dans des cantons spatiaux (BLOCK SYSTEM).

Le principe du canton temporel apporte plus de souplesse.

A.2 - Equations de base

Désignons par To la période d'une horloge dont le signal est transmis à toutes les rames, à partir d'un Poste de Commande Centralisée (P.C.C.) soient :

ΔT : l'intervalle de temps séparant deux rames fictives successives

N : le nombre de périodes de l'horloge To, comptées depuis le départ de la première station jusqu'au passage de la rame réelle devant le nème plot.

Hop: l'heure de départ de la rame de la première station

On peut écrire les équations suivantes :

(2) $H^F_{n(p+1)} = H^F_{np} + \Delta T$

(3) $H^F_{n(p)} = Hop + n.To$

(4) $H^F_{n(p+1)} = Hop + n.To + \Delta T$

(5) $H^R_{p\ (n)} = Hop + N.To$

Dans la pratique, pour respecter la double inégalité (1), la rame réelle doit maintenir un écart minimum Tf par rapport à sa rame fictive, cet écar correspond à une distance minimum de freinage. On a la nouvelle inégalité

(6) $H^F_{np} + Tf \leqslant H^R_{p(n)}$

De façon symétrique, la rame réelle doit aussi tenir compte du temps d'arrêt aux stations. Ce temps est évalué à S périodes To, d'où :

(7) $H^R_{p(n)} + S.To \leqslant H^F_{n(p+1)}$

Si v désigne la vitesse de la rame, et γ_o une décélération limite à respecter (6) devient :

(6') $H^F_{np} + v/\gamma_o \leq H^R_{p(n)}$;

La combinaison de (3), (5) et (6') donne :

(8) $v/\gamma_o \cdot To \leq N-n$

La combinaison de (1), (4) et (5) donne :

(9) $N-n < \frac{\Delta T}{To}$;

et en tenant compte de (7) :

(9') $N-n + S < \frac{\Delta T}{To}$

Dans la réalisation que nous avons entreprise, et afin de mieux assurer la sécurité anti-collision, nous avons remplacé l'inégalité (8) par une inégalité plus restrictive en remplaçant v par la vitesse maximale V_M que peut prendre la rame réelle, soit en définitive

(10) $$\boxed{\frac{V_M}{\gamma_o \cdot To} < N-n < \frac{\Delta T}{To} - S}$$

Valeurs numériques :

Pour $\Delta T = 60$ s; $To = 1$s ; $S = 20$; $\gamma_o = 1{,}3$ m/s^2; $V_M = 22{,}1$ m/s(= 80 Km)

on obtient : $\boxed{18 < N - n < 40}$

Remarque :

Le choix de S = 20 est largement suffisant; pour le métro de Paris, S varie entre 13 et 20 selon les stations.

A.3- Principe de l'arrêt du temps

En fonctionnement normal, le pilotage automatique doit être capable de maintenir la rame réelle dans le canton temporel qui lui est associé, respectant ainsi le programme de marche-type. Cependant, il faut tenir compte des incidents imprévisibles qui peuvent occasionner un retard important de la rame : immobilisation par suite de panne, blocage des portes par les voyageurs dans une station... Si le retard accumulé dépass ΔT, la rame réelle viendra empiéter sur la marche de la rame fictive p+1 qui la suit.

Pour y remédier, on utilise le principe de "l'arrêt du temps" : chaque rame est munie d'un émetteur qui émet vers le P.C.C. un signal de "tranquillisation". De son côté, le P.C.C. émet un signal dont la réception par chaque rame conditionne la marche de son horloge.

Ainsi, si une rame accuse un grand retard qu'elle ne pourra plus rattraper, elle suspend l'émission de son signal de "tranquillisation" tout en continuant de rouler pour rattraper son retard.
Le P.C.C. cesse alors d'émettre les signaux d'horloge; les autres rames, ne recevant plus de signal du P.C.C., s'arrêtent si elles sont à l'heure, ou continuent de rouler si elles sont en retard.

Quand la rame ayant provoqué l'arrêt d'horloge aura rattrapé son retard elle en informe le P.C.C. en reprenant l'émission de son signal de tranquillisation.

B. ETUDE DU PILOTE AUTOMATIQUE (P.A.)

Pour la commande de la marche d'une rame, le P.A. élabore trois vitesses :

- une vitesse de régulation (Ve)
- une vitesse limite (V_L)
- une vitesse de consigne de sécurité (V_{cs}), intervenant essentiellement dans les phases de décélération.

Par ailleurs, une vitesse de télécommande (V_t) peut être élaborée et émise par le P.C.C. La plus petite des vitesses $\{V_e, V_L, V_t\}$ constitue la vitesse de commande (V_e), qui est une entrée de l'asservissement de vitesse de la rame.

La vitesse (V_{cs}) est régulièrement comparée à la vitesse réelle (V_R). L'ordre de freinage est donné dès que V_R dépasse V_{cs} (Fig.2)

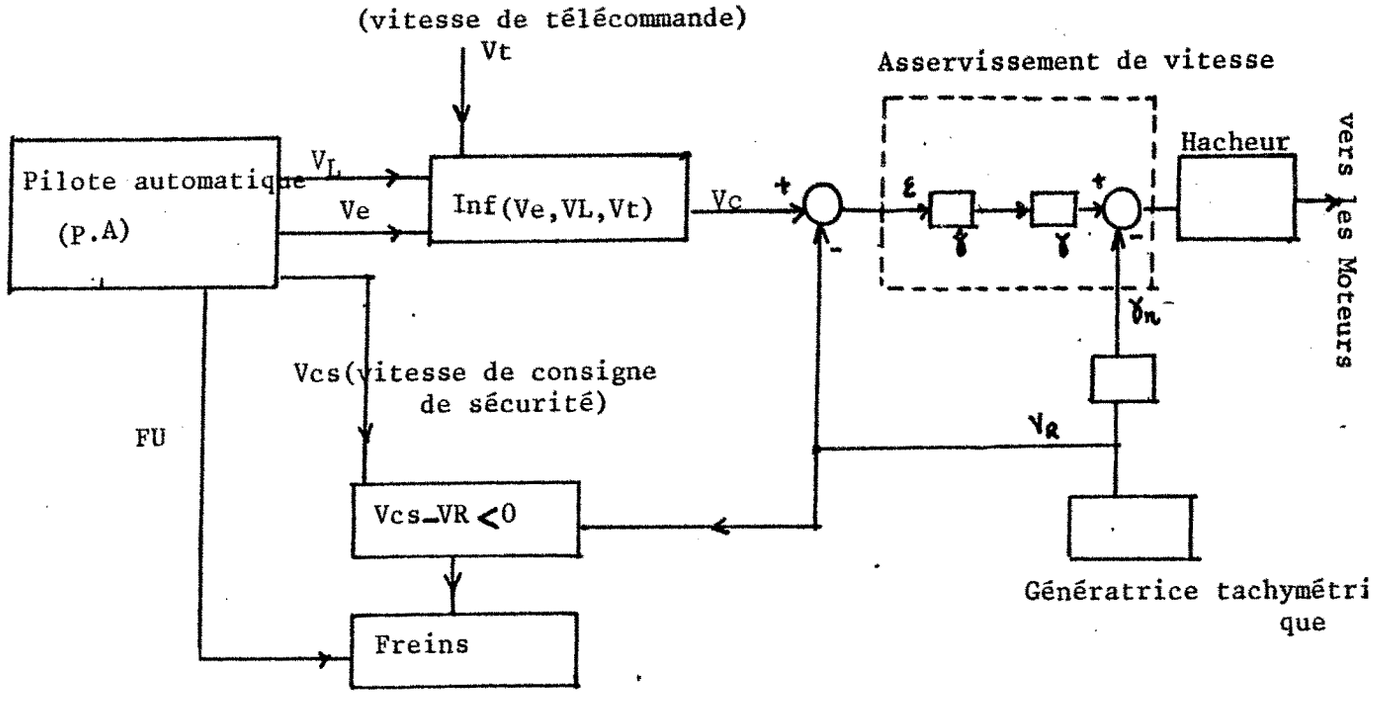


FIG. 2

De plus, le P.A. doit élaborer divers signaux logiques (ordre d'arrêt d'horloge, ordre de retour d'horloge, ordre de freinage, ...) et cela en fonction dès signaux d'entrée reçus par des capteurs (Fig.3).

Ces capteurs sont les suivants :

(P) - Un détecteur de plots qui, en présence de plot, émet un signal à niveau P.

(RP) - une roue phonique qui permet de mesurer la distance parcourue par une rame; cette roue phonique émet une impulsion RP chaque fois qu'une nouvelle distance égale au pas de la roue phonique est parcourue.

(V_R) - une génératrice tachymétrique entraînée par les roues porteuses du véhicule, et qui permet de mesurer en permanence la vitesse réelle de la rame.

(T_C) - un récepteur des signaux d'horloge T_C émanant du P.C.C.

(T_C') - un récepteur des signaux d'horloge T_C' émanant d'une horloge propre à la rame et indépendante de l'horloge centrale.

(PVS) - un détecteur qui élabore un signal à niveau PVS, lorsqu'une rame est présente dans une station ordinaire.

(VFU 1) - un détecteur de signal à niveau VFU1, validé par le système "Freins d'urgence" quand les freins d'urgence sont complètement enclenchés.

(VDFU 1) - un détecteur de signal à niveau VDFU1, validé par le système "Freins d'urgence" quand les freins d'urgence sont relâchés.

(VFU 2) - un détecteur de signal à niveau VFU2, validé par le système "Freins anti-survitesse" quand ces freins sont complètement enclenchés.

(VDFU2) - un détecteur de signal à niveau VDFU2, validé par le système "Freins anti-survitesse" quand ceux-ci sont relâchés.

(VFU3) - un détecteur de signal à niveau VFU3, validé par le système "Freins d'arrêt en station" quand ils sont complètement enclenchés.

(VDFU3) - un détecteur de signal à niveau VFU3, validé par le système "Freins d'arrêt en station" quand ceux-ci sont relâchés.

(PVO) - un détecteur de signal à niveau PVO, validé par le système-portes du véhicule quand les portes sont complètement ouvertes.

(PVF) - un détecteur de signal à niveau PVF validé par le système-portes du véhicule quand les portes sont complètement fermées.

(DEPTER) - un détecteur de signal impulsionnel DEPTER, ordre de départ de la rame de la station terminale, émis par le P.C.C. (toutes les minutes si l'on suppose l'intervalle des rames égal à ΔT = 1 mn).

(ARTER) - un détecteur qui élabore un signal à niveau ARTER, lorsqu'une rame est présente dans une station terminale.

(E) - un détecteur de signal à niveau E, validé par l'asservissement de vitesse quand la vitesse réelle de la rame devient inférieure ou égale à 1,3 m/s.

Quant aux signaux élaborés par le P.A., ils sont énumérés ci-dessous; leur signification apparaîtra clairement par la suite :

ARTO* - signal impulsionnel émis par une rame en retard pour demander au P.C.C. l'arrêt de l'émission des signaux d'horloge.

RETO* - signal impulsionnel de demande de reprise de l'émission des signaux d'horloge, émis par une rame qui a déjà lancé l'ordre ARTO, et qui a rattrapé son retard critique.

FU1 - signal à niveau de demande de freinage d'urgence, envoyé vers le système "freins d'urgence", remis à 0 dès la validation du signal VFU1.

FU2 - signal à niveau de demande de freinage anti-survitesse, envoyé vers le système "freins anti-survitesse", remis à 0 dès la validation du signal VFU2.

FU3 - signal à niveau de demande de freinage à l'arrivée en station, envoy vers le système "Freins d'arrêt en station", remis à 0 dès la validation du signal VFU3.

DFU1 - signal à niveau de défreinage envoyé vers le système "Freins d'urgence", remis à 0 dès la validation du signal VDFU1.

DFU2 - signal à niveau de défreinage envoyé vers le système "freins anti-survitesse", remis à 0 dès la validation du signal VDFU2.

DFU3 - signal à niveau de défreinage envoyé vers le système "freins d'arrêt en station", remis à 0 dès la validation du signal VDFU3.

COP* - signal impulsionnel de commande d'ouverture des portes du véhicule.

CFP* - signal impulsionnel de commande de fermeture des portes du véhicule.

DRR* - signal impulsionnel émis lorsque la rame démarre d'une station : ce signal est envoyé vers le système station pour initialiser la séquence de fermeture des portes de la station, et vers le P.C.C. pour localisation sur écran de visualisation.

GONG* - signal impulsionnel émis dès que le compteur d'arrêt en station CAS a la valeur 5; ce signal sert à prévenir les voyageurs de la fermeture imminente des portes du véhicule.

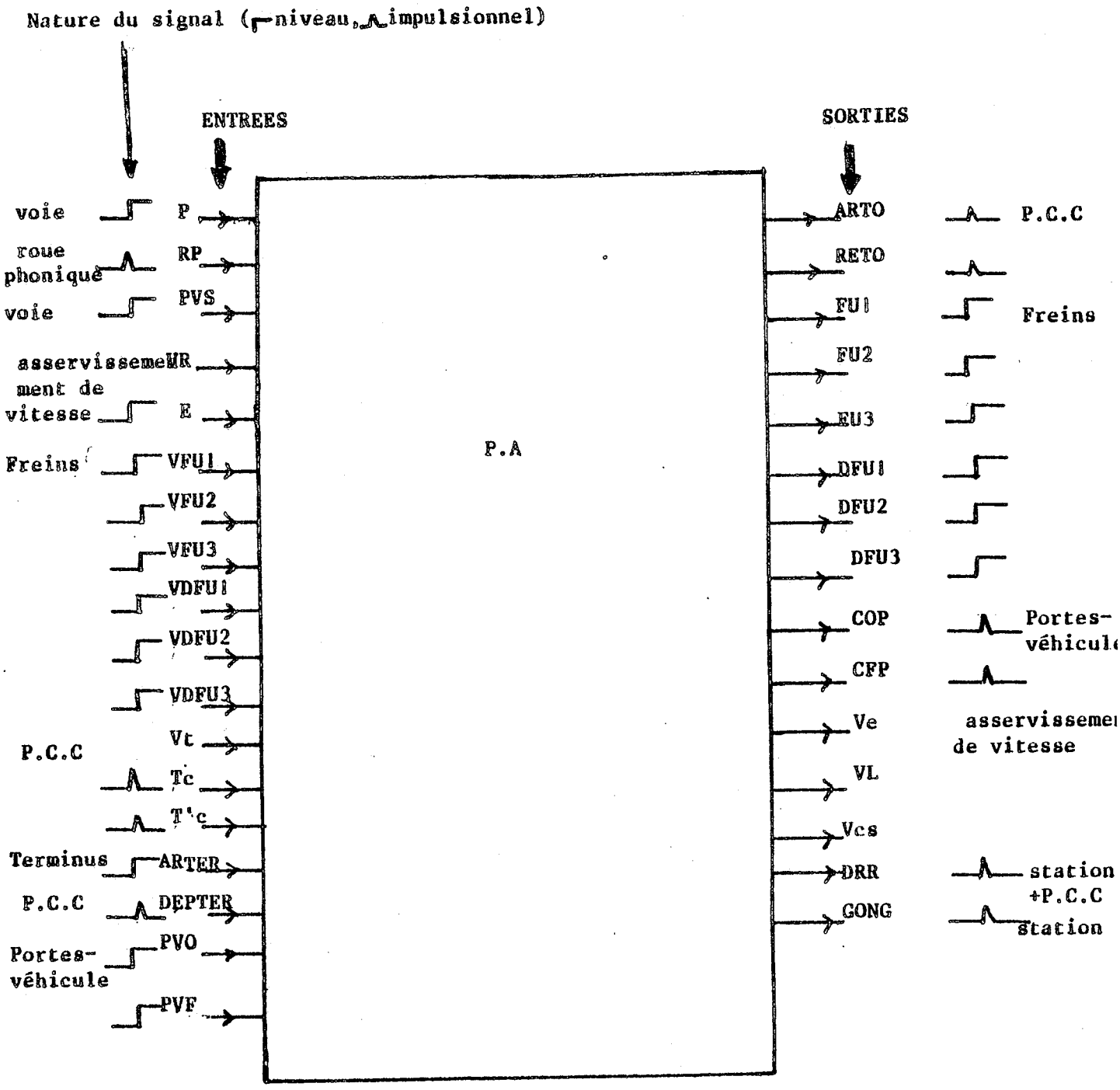

Nature du signal (niveau, impulsionnel)
ENTREES
SORTIES
voie
P
roue phonique
RP
voie
PVS
asservissement de vitesse
MR
E
Freins
VFU1
VFU2
VFU3
VDFU1
VDFU2
VDFU3
P.C.C
Vt
Tc
T'c
Terminus
ARTER
P.C.C
DEPTER
Portes-véhicule
PVO
PVF
P.A
ARTO
RETO
FU1
FU2
EU3
DFU1
DFU2
DFU3
COP
CFP
Ve
VL
Vcs
DRR
GONG
P.C.C
Freins
Portes-véhicul
asservissemer
de vitesse
station
+P.C.C
station

Fig.3

B.1 - Etude de la vitesse de régulation Ve

1.1 - Marche de la rame fictive. Vitesse de programme

Le programme de marche -type de la rame fictive consiste à parcourir un interplot en To seconde.

La vitesse de programme est : $V_P = \frac{\text{longueur-interplot}}{To}$

Pour To = 1 s, V_p = longueur interplot

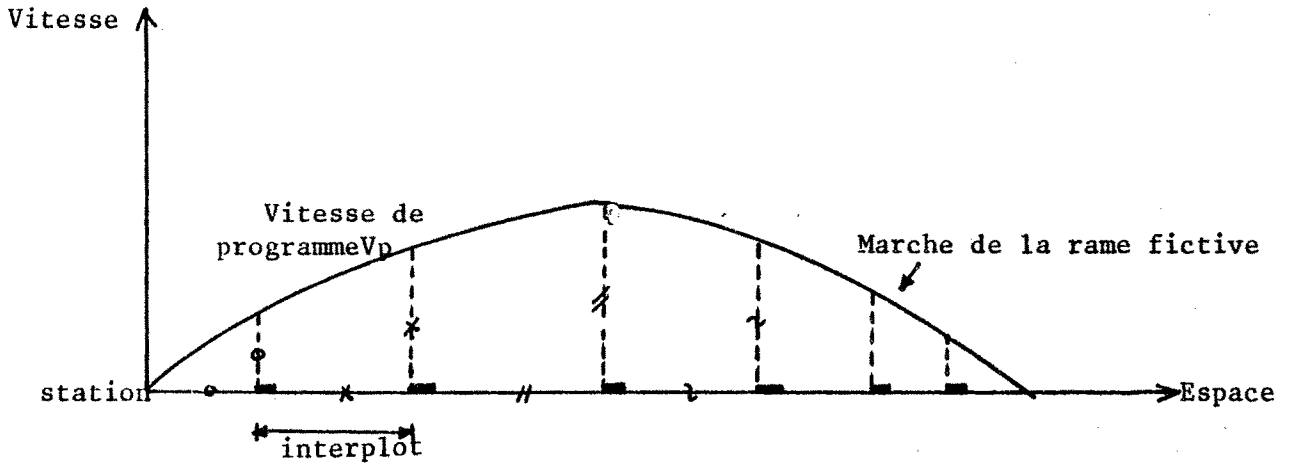


Fig.4

Plus l'interplot est grand, plus la vitesse de programme est grande (Fig.4)

1.2 - Vitesse de régulation (Ve)

Il s'agit d'asservir la rame réelle à la rame fictive de façon à respecter la double inégalité :

$18 < N-n < 40$

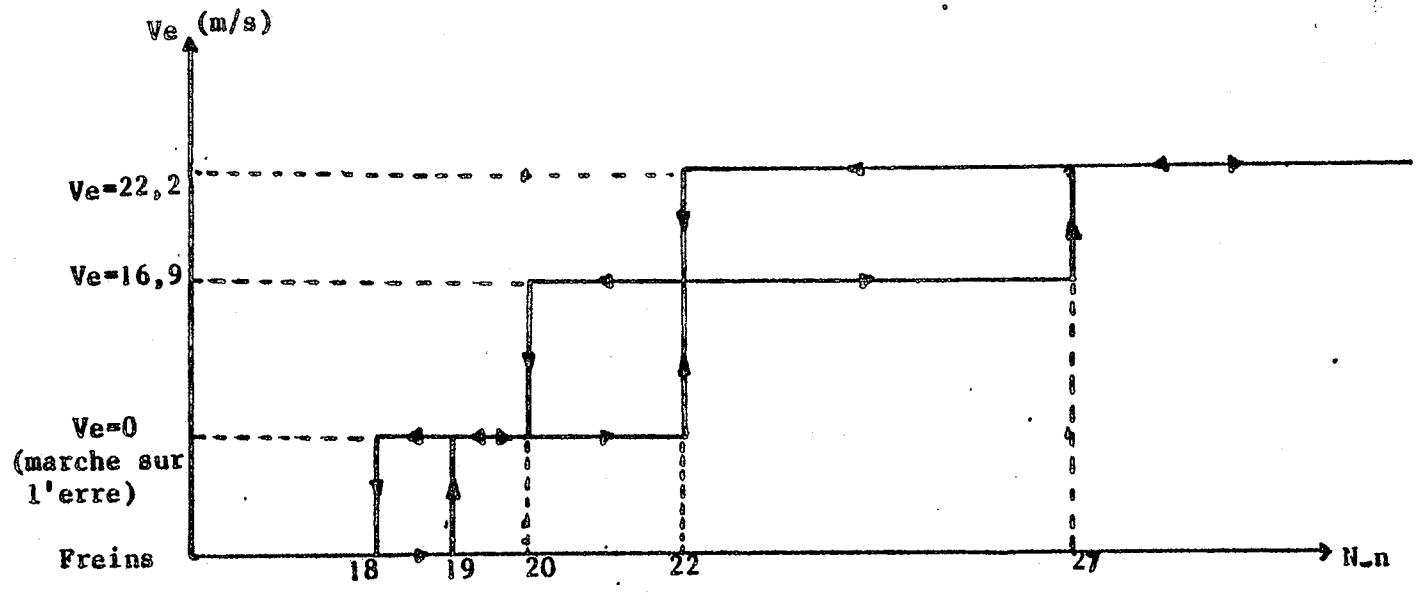
La vitesse Ve doit être filtrée de façon à obtenir un délai de rattrapage de retard minimum, tout en évitant des commutations traction-freinage intempestives. Pour cela, elle est réalisée à l'aide d'une fonction à seuil et à hystérésis de la grandeur d'écart (N - n).

$Ve = f(N-n)$

La fonction f est définie par le graphe de la figure 5.

Cette vitesse peut être calculée à l'aide d'un compteur REG qui est :

- initialisé à 18 dès la détection du signal DEPTER au départ de la station terminale.
- incrémenté de 1 à chaque impulsion d'horloge Tc reçue
- décrémenté de 1 à chaque signal de détection de plot P.



Si $N - n > 27$, la rame est considérée comme en retard,

$$V_e = V_M = 22,2 \text{ m/s} \quad \text{(vitesse maximum)}$$

Si $20 < N - n \leq 22$, la rame est considérée comme étant à l'heure

Si $18 < N - n \leq 20$, la rame est considérée comme étant relativement en avance : on a la marche sur l'erre (arrêt des moteurs)

$$V_e = 0$$

Si $N - n \leq 18$, on a freinage immédiat d'urgence.

Fig. 5

B.2 - Sécurité anti-collision

Le non respect de l'inégalité $18 < N-n < 40$ entraîne un risque de collision.

a) Si une rame accuse un retard important atteignant 39 s, elle lance l'ordre d'arrêt d'horloge (ARTO*) avec une hystérésis entre 37 et 39. Le retour d'horloge (RETO*) est donné dès que (N-n) redevient inférieur à 37 (Fig. 6)

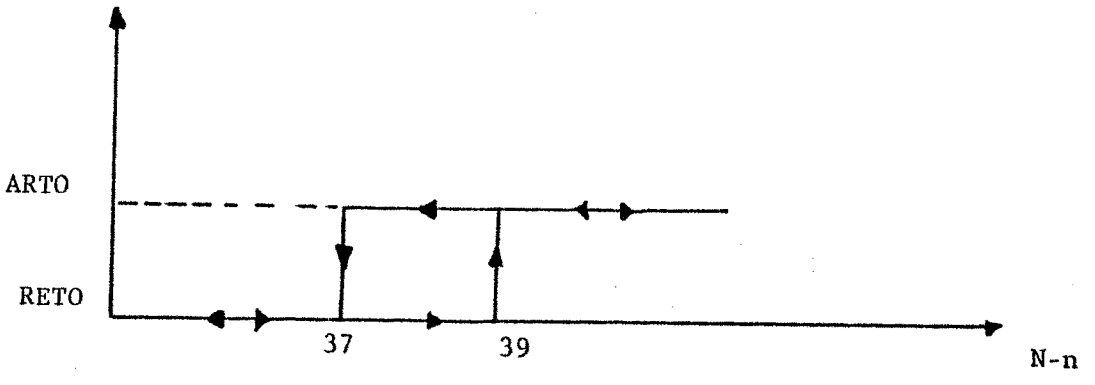
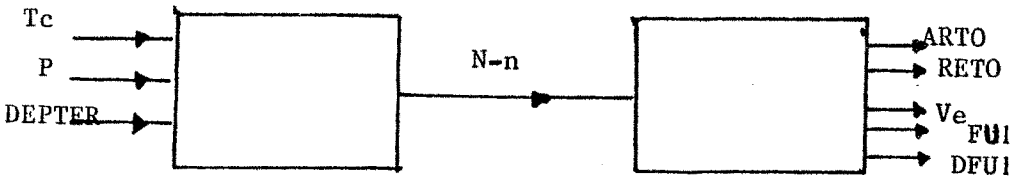


FIG. 6

b) Si (N-n) devient inférieur ou égal à 18, il y a freinage immédiat d'urgence (FU1). La rame immobilisée attend le retour d'horloge pour repartir. Pour redémarrer, la rame lance l'ordre de défreinage (DFU1).



Remarque :

La fonction réalisant la sécurité anti-collision joue aussi le rôle de régulation d'intervalle, puisque chaque rame en retard est ramenée à l'intérieur de son canton temporel.

La vitesse de régulation V_e asservit la rame réelle à la rame fictive. Cependant, elle ne tient pas compte directement des caractéristiques de la voie (courbes, approche en station, etc...)

Il convient dès lors de définir en tout point un domaine de vitesses acceptables délimité par la vitesse limite (V_L).

B.3 - Etude de la vitesse limite (V_L)

Le codage de la vitesse limite se fait à l'aide de balises et de la vitesse de programme selon la loi :

$$V_L = V_P + CA$$

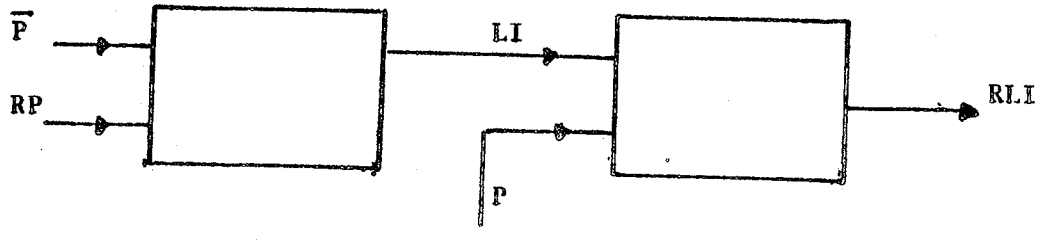
On a vu que la vitesse de programme V_P est égale à la longueur d'interplot. La valeur de CA est fonction de la dernière balise rencontrée. Elle est réinitialisée à 4 à chaque départ de station (sur condition DRR).

B.3.1 - Mesure de la longueur d'interplot (RLI)

Chaque rame est munie d'une roue phonique qui émet une impulsion RP chaque fois qu'une nouvelle distance égale au pas de la roue phonique est parcourue. Le comptage de ces impulsions entre deux plots donne la longueur d'interplot. Ceci peut être réalisé à l'aide d'un compteur LI qui est :

- initialisé à 0 dès la détection d'une fin de plot (signal $\bar{P}$)
- incrémenté de 1 à chaque impulsion (RP) de la roue phonique.

Le résultat du comptage est enregistré dans un registre RLI, dès que la rame détecte de nouveau la présence d'un plot (Fig.8).



B.3.2 - Décodage des balises

Les plots ou balises sont identifiés par leur longueur. Les plots ont une longueur minimum, les balises, plus longues que les plots, sont de quatre types (FIG 7).

Balise B1 : annonce une approche en station ou un ralentissement en ligne

Balise B2 : annonce une fin de zone d'accélération et le passage sur un palier de vitesse limite supérieur

Balise B3 : annonce la fin d'une zone de décélération et le passage sur un palier de vitesse limite inférieur

Balise B4 : annonce un alignement droit autorisant une vitesse maximum.

La mesure de la longueur d'une balise peut être réalisée à l'aide d'un compteur LP qui est :

- initialisé à 0 chaque fois que la rame détecte de nouveau la présence d'un plot
- incrémenté de 1 à chaque impulsion RP de la roue phonique (FIG.8)

Le résultat du comptage est enregistré dans un registre RLP, dès que la rame détecte la fin du plot

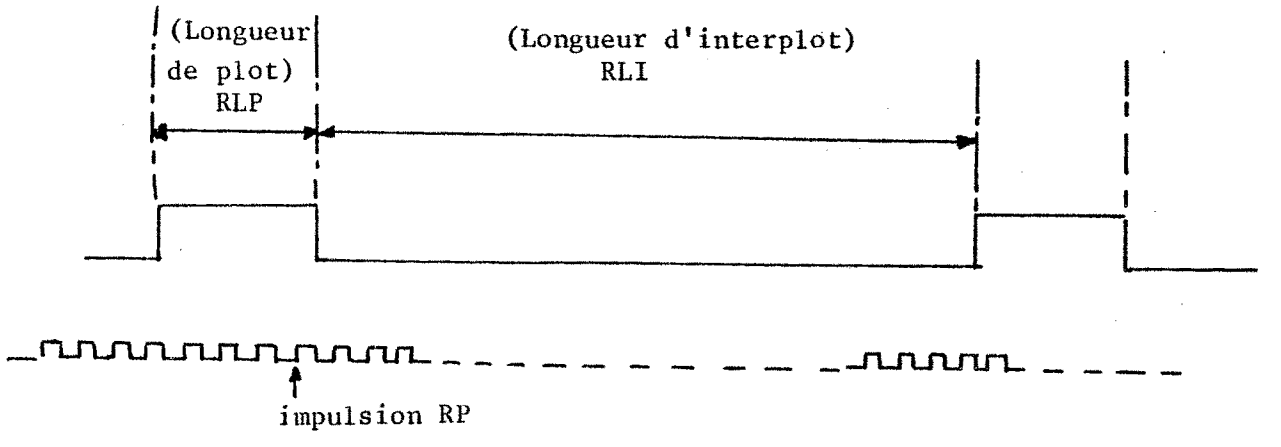
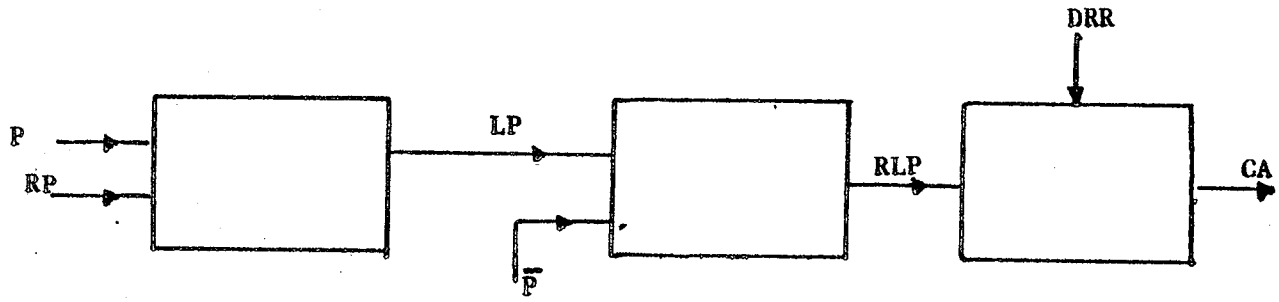


FIG. 8

Les valeurs de CA en fonction des balises sont données par les règles suivantes (FIG.7) :

- Si balise B2, CA est décrémenté de 1 à chaque détection d'un nouveau plot jusqu'à s'annuler.
- Si balise B4, CA est réinitialisé à 4
- Si balise B1, CA est mis à 0
- Si balise B3, aucun effet sur CA



Remarque :

A chaque état du compteur CA, on fait correspondre la Valeur To. To, soit 1,3m/s. Ainsi, les valeurs qui peuvent être ajoutée à la vitesse de programme sont les suivantes :

0 - 1,3 - 2,6 - 3,9 - 5,2 m/s.

On voit sur la figure (7) comment la loi V_p + CA permet de définir une vitesse limite supérieure ou égale à V_p.

D'autre part, on remarque que le rattrapage de la rame fictive n'est autorisé que dans la zone située entre les balises B4 et B1.

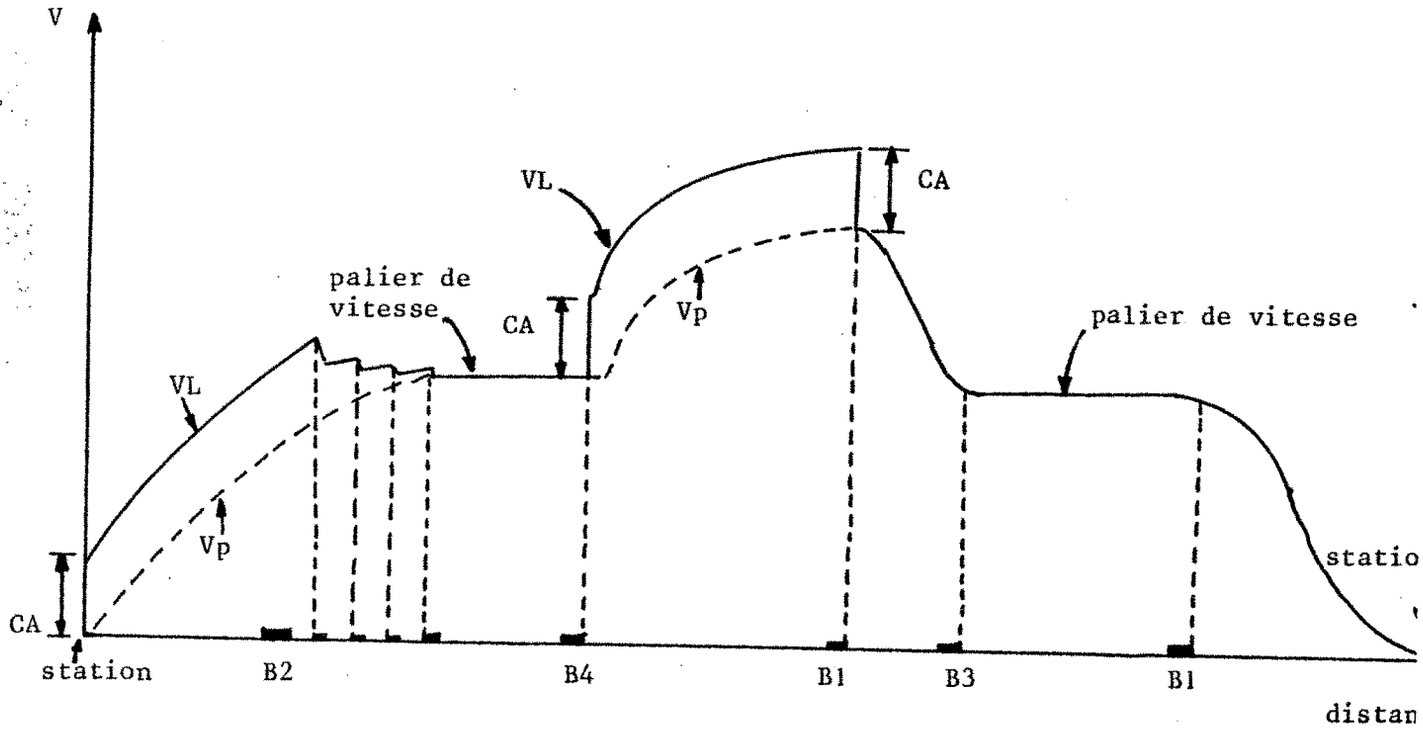
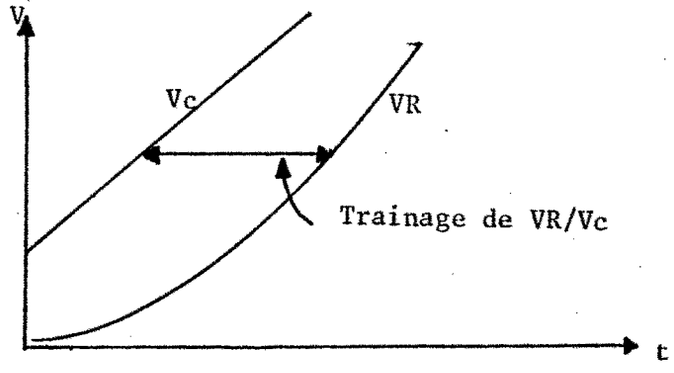


FIG. 7

Le compteur CA est mis à sa valeur maximale au départ de la station pour compenser le trainage de la vitesse réelle V_R par rapport à la vitesse de commande V_c.



On voit en effet que, si on prend $V_c = V_L$ on obtiendra une vitesse réelle V_R à peu près égale à la vitesse de programme V_p.

Données numériques :

Le pas de la roue phonique est supposé égal à δ = 3,5 cm

La mesure de la longueur de plot et de balise est entâchée d'une incertitude tenant compte de la vitesse réelle de la rame, de la constante de temps du détecteur de plots, et des différences de température.

Le tableau suivant donne les différents codages, en prenant une incertitude égale à 12,5 cm :

	PLOT	B1	B2	B3	B4
Longueur en cm	30	68	105	146	196
impulsions engendrées par la roue Phonique	6 à 14	15 à 25	26 à 36	37 à 49	50 à 62

B.4 - Etude de la vitesse de consigne de sécurité (V_{cs})

La vitesse de consigne de sécurité (V_{cs}) est une vitesse à laquelle on impose de ne jamais être dépassée par la vitesse réelle V_R de la rame; elle intervient dans la commande des freins, indépendamment de la commande des moteurs.

Elle permet de corriger :

- les défaillances du P.A. (calcul erroné de V_c,...), ou celles de l'asservissement de vitesse

- le trainage de la vitesse réelle par rapport à la vitesse de commande : En effet, si, en phase de décélération, on a : $V_C = V_L$ on aura $V_R > V_L$ du fait du trainage. Le freinage intervient alors pour limiter ce trainage. Par conséquent, dans les phases d'accélération ou celles dans lesquelles un palier de vitesse doit être respecté, on aura : $V_{CS} = V_L$.

En revanche, en phase de décélération, on devra élaborer une vitesse $V_{CS} > V_L$, sinon les freins interviendraient systématiquement.

D'autre part, si de forts paliers de la vitesse de commande V_C, en zone de décélération sont tolérables, puisqu'ils sont filtrés par l'asservissement (limitation des valeurs de la décélération à une valeur donnée) et par les éléments mécaniques de la rame (inertie du moteur, ...), cela n'est pas possible pour la vitesse V_{CS}, car on aurait alors un freinage brutal, d'où la nécessité d'une courbe de la vitesse V_{CS} lissée.

B.4.1 - Etude de la répartition des plots en phase de décélération

Dans la procédure de ralentissement, le mouvement de la rame est uniformément décéléré.

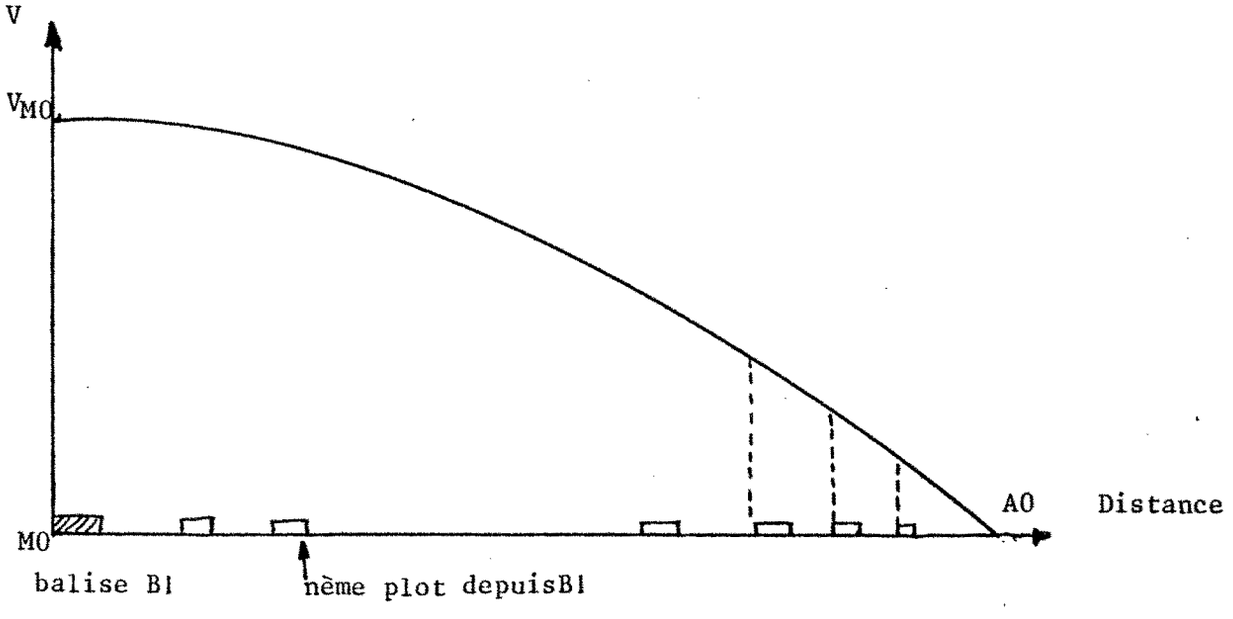


FIG. 9

En prenant Mo comme origine des axes (vitesse, distance), on a les équations suivantes pour un point quelconque entre Mo et Ao (Fig. 9) :

$$\begin{cases} x = -\frac{1}{2}\gamma t^2 + V_{M_0} t & (V_{Mo} \text{ étant la vitesse de la rame au point Mo}) \\ \frac{dx}{dt} = -\gamma t + V_{Mo} \end{cases}$$

Le temps mis pour parcourir un interplot étant égal à To, on a au passage sur le nième plot rencontré depuis B1 :

$$\begin{cases} x_n = -\frac{1}{2}\,\gamma_o (nTo)^2 + V_{Mo}\,(nTo) \\ v_n = -\gamma_o (nTo) + V_{Mo} \end{cases}$$

La vitesse au passage sur le $(n+1)^e$ plot est :

$v_{n+1} = -\gamma_o (n+1)\,To + V_{Mo}$;

et l'on a :

$v_n - v_{n+1} = \gamma_o To$

En appliquant ces formules, en partant de Mo avec une vitesse maximale V_{Mo} et une décélération limite γ_o, on obtient :

$v_n - v_{n+1} = \gamma_o . To$

- Si l_n désigne la longueur d'un interplot compris entre les plots n et n +1, on a ;

$l_n - l_{n+1} = (\gamma_o . To) . To$ soit $\gamma_o . To^2$

Donc, dans une zone de décélération limite, les plots doivent être placés en progression arithmétique de raison $\gamma_o . To^2$.

- La vitesse s'annule au plot n_o tel que $n_o = \frac{V_M}{\gamma_o . To}$

(Valeurs numériques) :

Pour $V_M = 22{,}1$ m/s, $\gamma_o = 1{,}3$ m/s^2, To = 1 s, on obtient $n_o = 18$)

.4.2 - Etude de la vitesse de consigne de sécurité non lissée

Au décodage de la balise B1, la vitesse V_L devient égale à la vitesse de programme V_p. Cependant, au cours de cette phase de décélération qui commence, la vitesse réelle V_R de la rame a tendance à rester constamment supérieure ou égale à la vitesse de programme V_p (à moins que la rame soit trop en avance). La courbe de vitesse V_{cs} suit la courbe V_p de manière à limiter l'écart de V_R par rapport à V_p. Si V_R dépasse V_{cs}, les freins mécaniques sont déclenchés systématiquement.

a) Pour tenir compte de la chute brutale due au passage de la vitesse limite V_L de la valeur $V_p + 4\,\gamma o.To$ à V_p, la vitesse de consigne a un profil en escalier tel qu'un pas de $\gamma o.To$ est retranché de la vitesse limite à chaque plot détecté. Pour cela, les 4 plots placés après la balise B1 sont équidistants (décélération de programme constante).

b) La phase de décélération de V_p commence à partir du 4ème plot situé après la balise B1. Les plots sont alors placés en progression arithmétique de raison $\gamma o.To^2$, comme il a été montré dans le paragraphe précédent; la décélération de programme est prise égale à la décélération limite γo.

Dans ce cas, la vitesse de consigne de sécurité (V_{cs}) suit V_p de façon à ce que la chute de vitesse qu'accuse V_p à chaque plot soit subie par V_{cs} au passage de la rame sur le plot suivant (Fig. 10).

Remarque :

Lorsqu'une balise B3 précède la balise B1, la vitesse limite V_L est égale à la vitesse de programme V_p calculée avant le décodage de B1. La valeur de CA est donc nulle, et il n'y a pas lieu dans ce cas de tenir compte de ce qui est dit en a). Les plots seront placés en progression arithmétique directement à partir de la balise B1 (FIG.11).

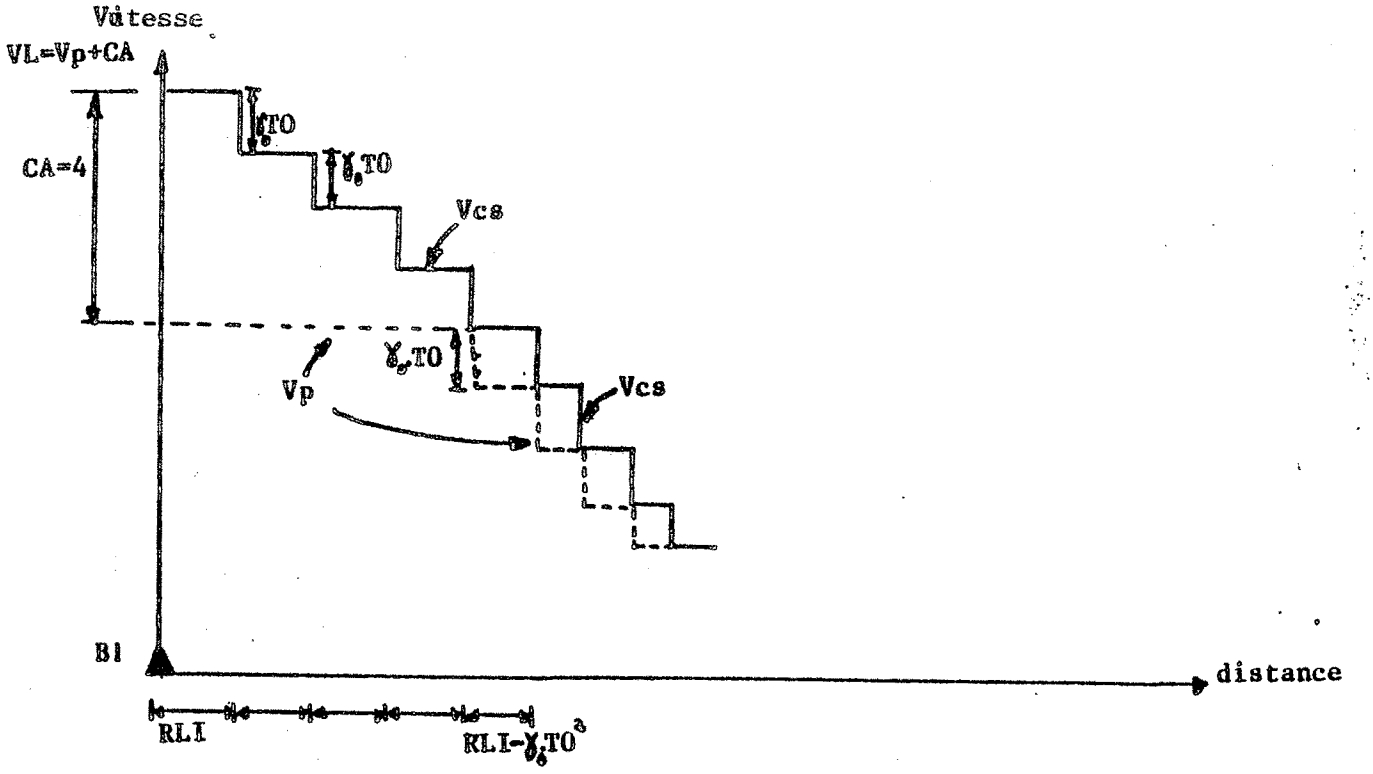


Fig.10

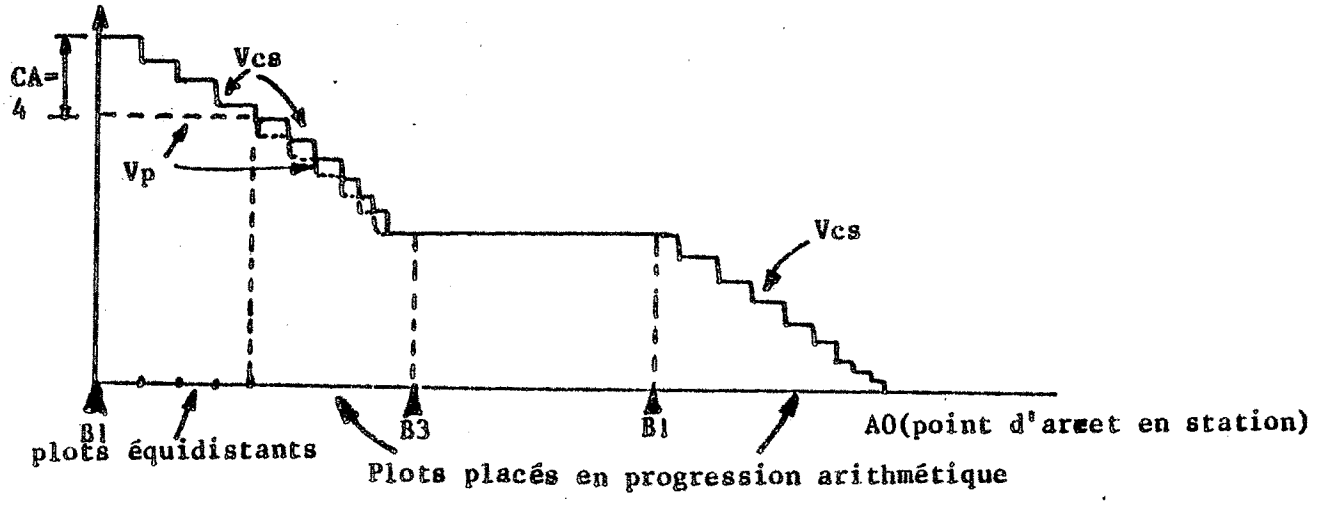


Fig.11

Cette vitesse V_{cs} peut être écrite sous la forme suivante :

$$V_{cs} = \begin{cases} (\delta \times RLI) + (CA' - n)\,\gamma_o.To & \text{si } CA' > o \\ (\delta \times RLI) - n'\gamma_o\,To & \text{si } CA' = o \end{cases}$$

où :

- δ est le pas de la roue phonique exprimé en mètres
- RLI est la longueur de l'interplot enregistrée à la détection de la balise B1.

- CA' = CA dans les zones comprises entre B1 et B3

  CA', égal à 4 au décodage de B1, est décrémenté de 1 à chaque plot détecté à partir de la balise B1.

- n est le nombre de plots comptés à partir du 4ème plot situé en aval de la balise B1, sachant que la balise précédente n'est pas B3.

- n' est le nombre de plots comptés à partir du décodage de la balise B1, sachant que la balise B3 a précédé cette balise B1.

B.4.3 - Lissage de la vitesse de consigne de sécurité (V_{cs})

- Afin d'éviter un freinage brutal, la vitesse de consigne ainsi obtenue est lissée : chaque interplot situé après la balise B1 est divisé en 16 sections égales. A la fin de chaque section, V_{cs} est diminuée de $\frac{\gamma_{oTo}}{16}$, ce qui permet d'affiner le profil précédent (FIG.12).

  A chaque mise à jour de V_{cs}, celle-ci est comparée à la vitesse réelle V_R de la rame. Si $V_{cs} < V_R$, les freins mécaniques sont déclenchés; le pilote automatique agit ainsi directement par "à coups" afin de maintenir $V_R \leqslant V_{cs}$. Ce fonctionnement permet en outre de contrôler la vitesse réelle de la rame d'une manière indépendante de l'asservissement de vitesse.

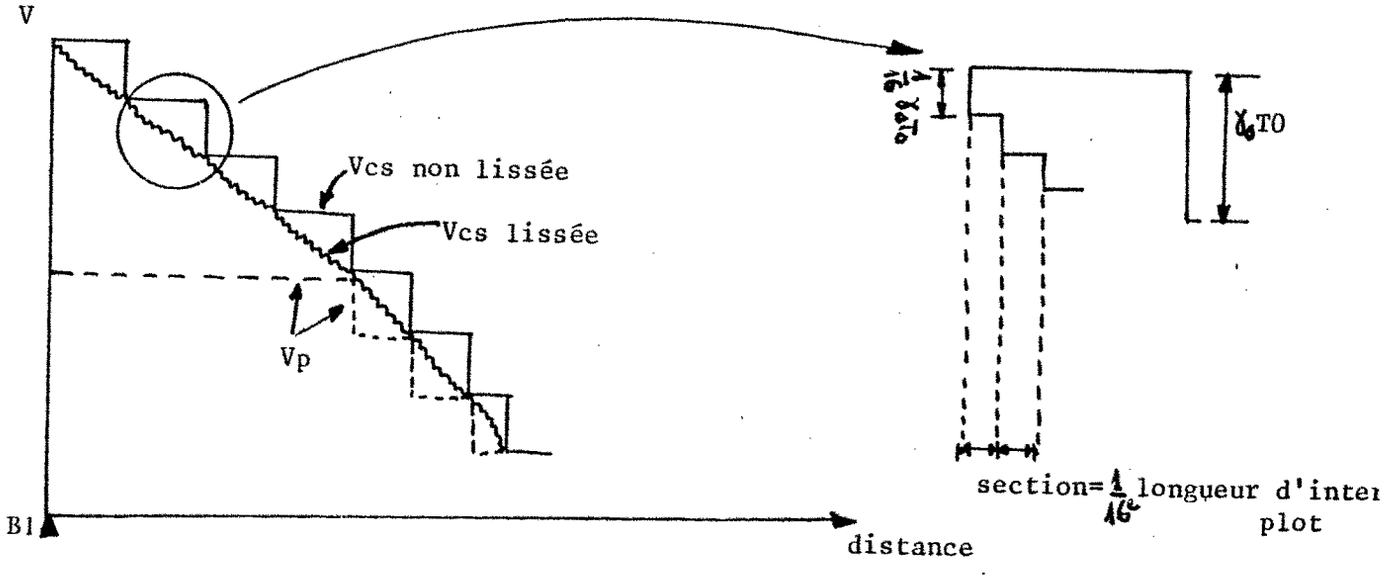


FIG. 12

- Réalisation de la vitesse V_{cs} lissée

. A partir du décodage de la balise B1, on sait comment sont placés les plots on peut donc connaître à l'avance la longueur d'un interplot suivant, et celle d'une section s de cet interplot ($= \frac{1}{16}$ de la longueur d'interplo

On considère alors un compteur LI' qui est :

* incrémenté de 1 à chaque impulsion RP reçue de la roue phonique
* initialisé à 0 à chaque détection de plot et à chaque fin de section parcourue.

La valeur courante de V_{cs} sera retranchée de $\frac{\gamma_o To}{16}$ chaque fois que la valeu du compteur LI' devient supérieure ou égale à s (préalablement calculée).

Il est à noter que la longueur d'une section s n'étant pas forcément multiple du nombre d'impulsions reçues de la roue phonique, on se contentera approximativement d'un seuil sur la valeur de s.

Remarque :

Le lissage que nous avons proposé est un lissage spatial, qui est appliqué sur la totalité d'un interplot.

On aurait pu proposer un lissage temporel obtenu de la manière suivante :

V_{cs} peut être réalisée par un compteur CLIS qui est :

* initialisé à 16 à chaque décodage de la balise B1 et à chaque nouvelle détection de plot situé en aval de la balise B1.
* décrémenté de 1, en l'absence de détection de plot, à chaque impulsion d'une horloge interne (H16) de fréquence 16 HZ.

Avec les mêmes notations vues prédécemment, la vitesse de consigne de sécurité (V_{cs}) lissée peut être écrite sous la forme suivante:

$$V_{cs}\ \text{lissée} = \begin{cases} (\delta \times RLI) + \gamma_o.To\left[CA' - n - \frac{1}{16}(16 - CLIS)\right] & \text{si } CA' > o \\ (\delta \times RLI) - \gamma_o.To\left[n' + \frac{1}{16}(16 - CLIS)\right] & \text{si } CA' = o \end{cases}$$

Cependant, une telle réalisation supposerait qu'un interplot est parcouru exactement en une seconde. Comme une rame est généralement en retard sur son horaire, on peut avoir un profil où le lissage n'est pas appliqué sur la totalité de l'interplot (FIG. 13)

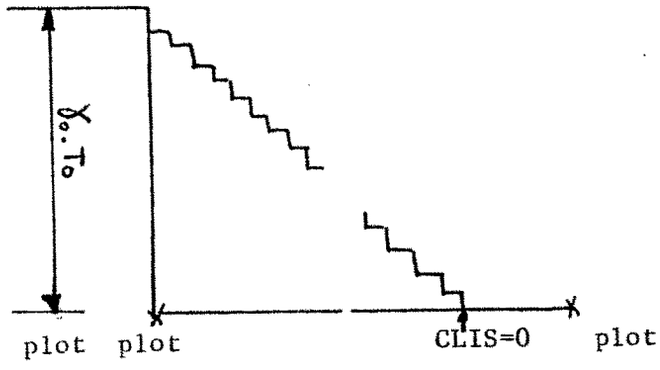


Fig .13

Dans le cas d'un ralentissement à l'approche d'une courbe, la consigne est annulée dès qu'une balise B3 est décodée (FIG.14).

Dans le cas d'un ralentissement à l'approche d'une station où un arrêt précis doit être préparé, le calcul de V_{cs} est effectué jusqu'à ce que la vitesse réelle V_R de la rame devienne $\leq$ 1,3m/s (FIG.15).

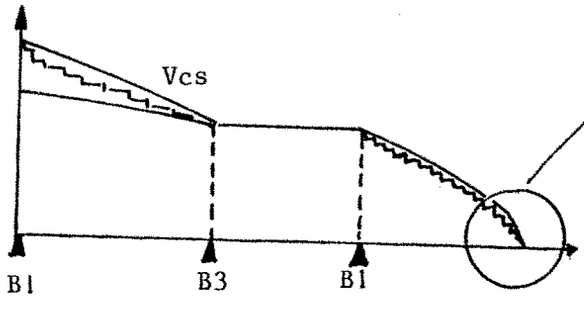


Fig.14

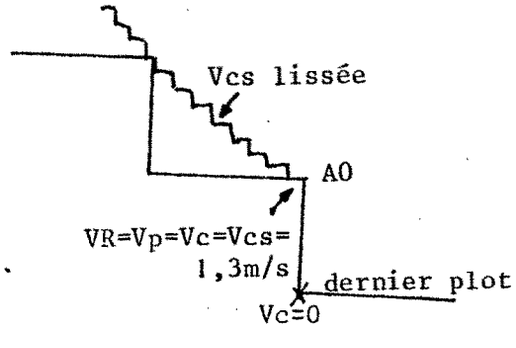


Fig.15

Le lissage nous assure que la vitesse réelle au point Ao (FIG.15) est $\leq$ 1,3 m/s (validation du signal E).

B.5 - Automatisation du stationnement et du départ des stations (FIG.17)

B.5.1 - Phase d'arrêt

a) A partir du point Ao, la rame est soumise à son inertie. Le temps mis pour que la vitesse réelle V_R passe de 1,3 m/s à 0 dépend du temps de réponse de l'asservissement de vitesse et des caractéristiques de la rame, qui sont des données connues, et peut donc être déterminé, si bien que le choix de l'emplacement des bobines de détection de présence de véhicule en station (PVS), et le déclenchement des freins dès détection du signal PVS permettent d'assurer un arrêt de précision (FIG.16).

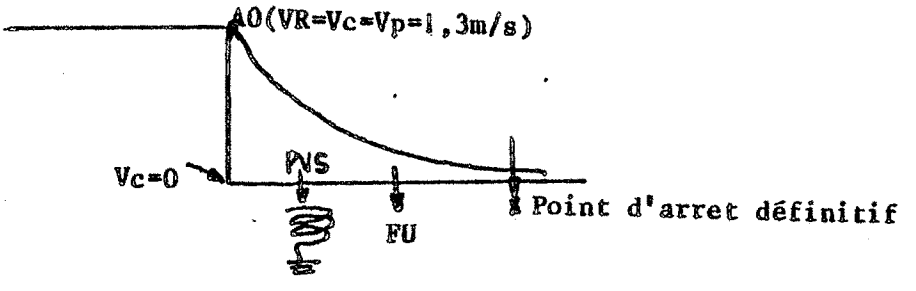


FIG. 16

Exemple :

Supposons que PVS soit détecté en Ao, la distance d'arrêt de la rame peut être donnée par la formule;

$$d_a = V_{(Mo)} \cdot \tau_1 + \frac{V(Mo)^2}{2\gamma_o} + L$$

où : - τ_1 est le retard de l'application de la décélération γ_o

- V(Mo) est la vitesse en Mo, au moment de la prise de décision de freinage.
- γ_o est la décélération limite préservant le confort des voyageurs
- L est la longueur de la rame.

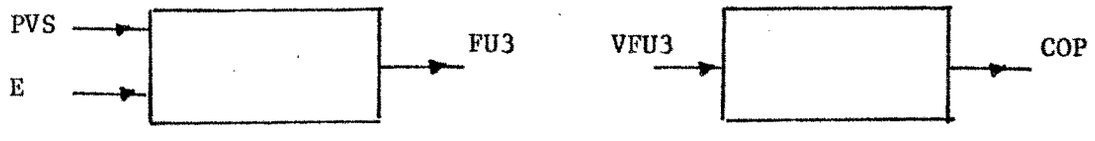
Valeurs numériques :

τ_1 = 1 s, V(Mo) = 1,3 m/s, γ_o = 1,3 m/s^2, L = 30 m;

ce qui donne : d_a = 31,95 m.

b) Après avoir lancé l'ordre de freinage (FU3), le PA attend la validation du signal VFU3 de vérification d'enclenchement des freins et envoie l'ordre COP* de commande d'ouverture des portes du véhicule.

Lorsque toutes les portes du véhicule sont complètement ouvertes, le système portes-véhicule valide le signal PVO.



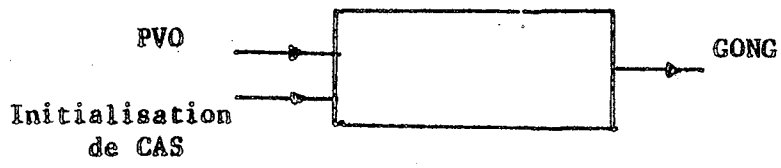
B.5.2 - Phase de stationnement

Elle est gérée par un compteur d'arrêt en station embarqué (CAS). Quand le signal PVO est validé, CAS initialisé à 20 est décrémenté de 1 à chaque signal d'une horloge T'_c, propre à la rame, de période égale à 1s, et indépendante de l'horloge centrale T_c.

Le choix d'une horloge T'_c différente de l'horloge centrale tient à la raison suivante :

Supposons que la rame, sur le point d'arriver dans une station, lance l'ordre ARTO* d'arrêt d'horloge centrale. Ne recevant plus de signaux T_c, la valeur de son compteur REG ne varie pas, et l'ordre RETO* de retour d'horloge ne pourra pas être émis : le décomptage du compteur CAS ne peut pas être effectué, et la rame reste immobilisée dans la station.

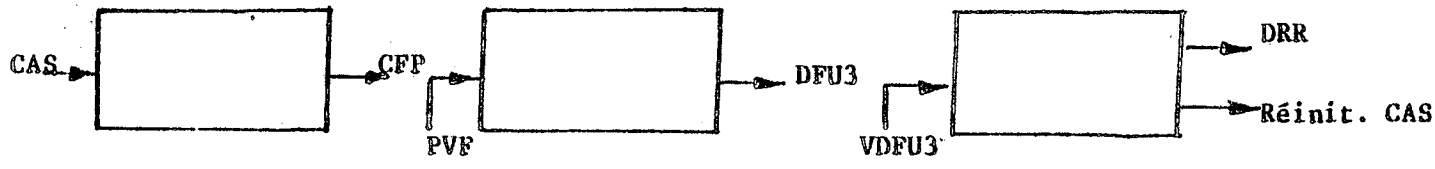
Le passage de CAS à 5 fait retentir un gong (émission d'un signal impulsionnel GONG*) prévenant les voyageurs de la fermeture imminente des portes.



B.5.3 - Phase de démarrage

Dès que la valeur de CAS devient nulle (fin du temps normal de stationnement), le PA émet le signal CFP* de commande de fermeture des portes du véhicule. Quand le signal PVF est validé, le PA lance l'ordre DFU3 de défreinage. Le PA attend la validation du signal VDFU3 avant d'émettre le signal DRR* de départ de la rame réelle. Ce signal DRR* est surtout destiné aux systèmes "station et P.C.C. ".

Le compteur CAS est ensuite réinitialisé à sa valeur maximale.



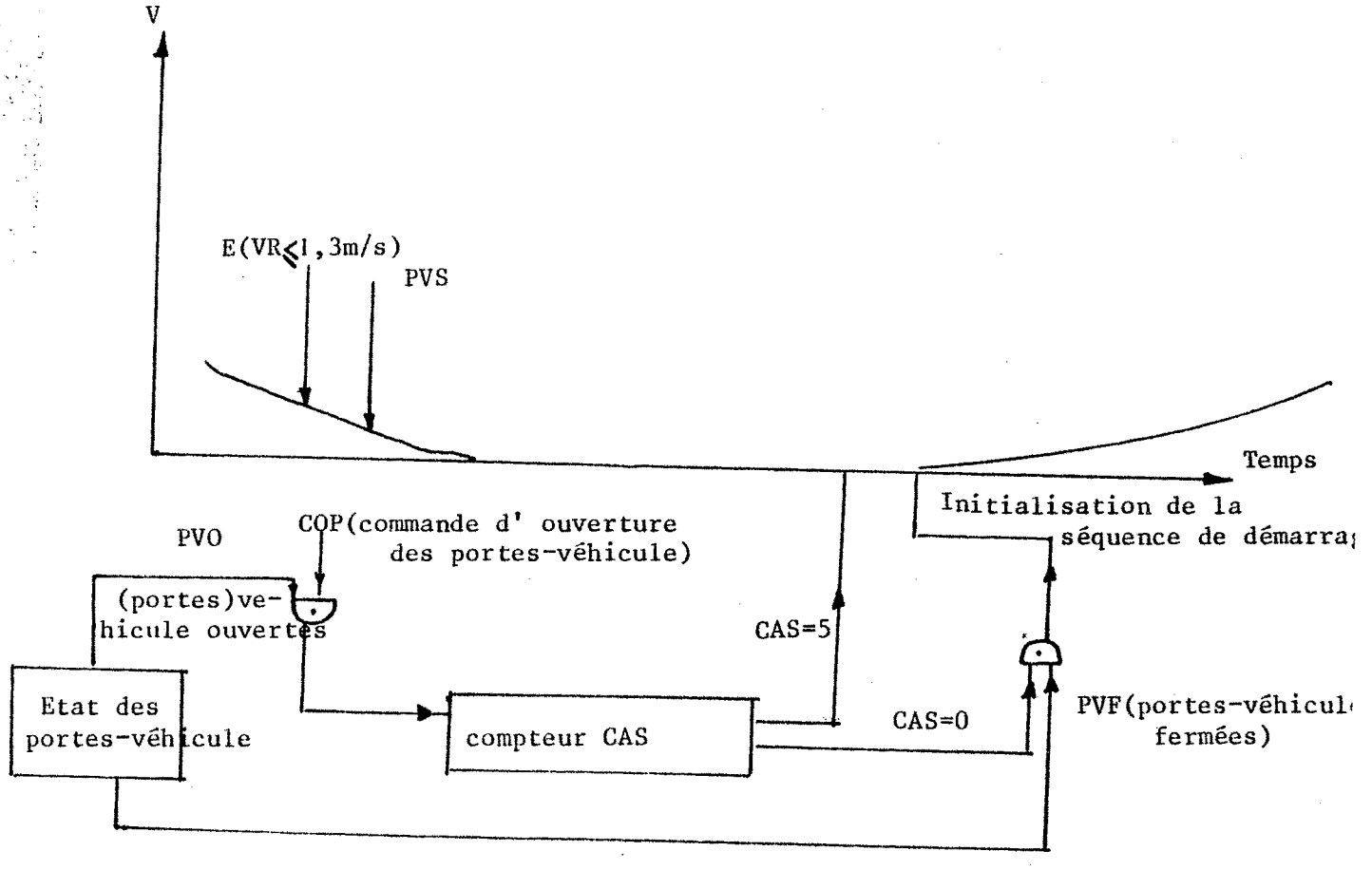


FIG.17

Remarques :

a) L'arrivée en station terminale s'effectue comme une arrivée en station ordinaire. La détection de la présence du véhicule en station terminale valide le signal ARTER. Ce signal est remis à 0 dès que la rame quitte la station terminale.

b) Au départ de la station terminale, la séquence d'initialisation de fermeture des portes et de démarrage se fait à partir de la réception du signal DEPTER émis par la P.C.C.

B.5.4 - Régulation en station. Notion de plots fictifs

La relation fondamentale du principe de base, (10) $V_M/\gamma_0 T_0 < N-n < \Delta T-S$ régissant le fonctionnement du V A L, et obligeant toute rame à rester à l'intérieur de son canton temporel, tient compte du temps de stationnement (S=20) d'une rame dans une station : on est alors tenté de verrouiller le compteur REG à l'arrivée de la rame dans la station, et de le déverrouiller au départ effectif de la rame de la station.

Mais le fait de ne pas prendre en compte les signaux T_c par la rame en station amènerait celle-là à n'avoir aucune connaissance d'éventuelle procédures d'arrêt et de retour d'horloge lancées par d'autres rames en ligne : d'où un risque d'empiètement de cantons temporels.

Il ne faut donc pas verrouiller le compteur REG, lorsque la rame arrive en station. Comme la quantité S est prise en compte dans la relation (10), la régulation en station peut être réalisée comme suit (FIG. 18).

* Compter les impulsions T_c dans le compteur REG
* Décompter, au moment du départ de la rame de la station, un nombre de plots fictifs, égal à S = 20.

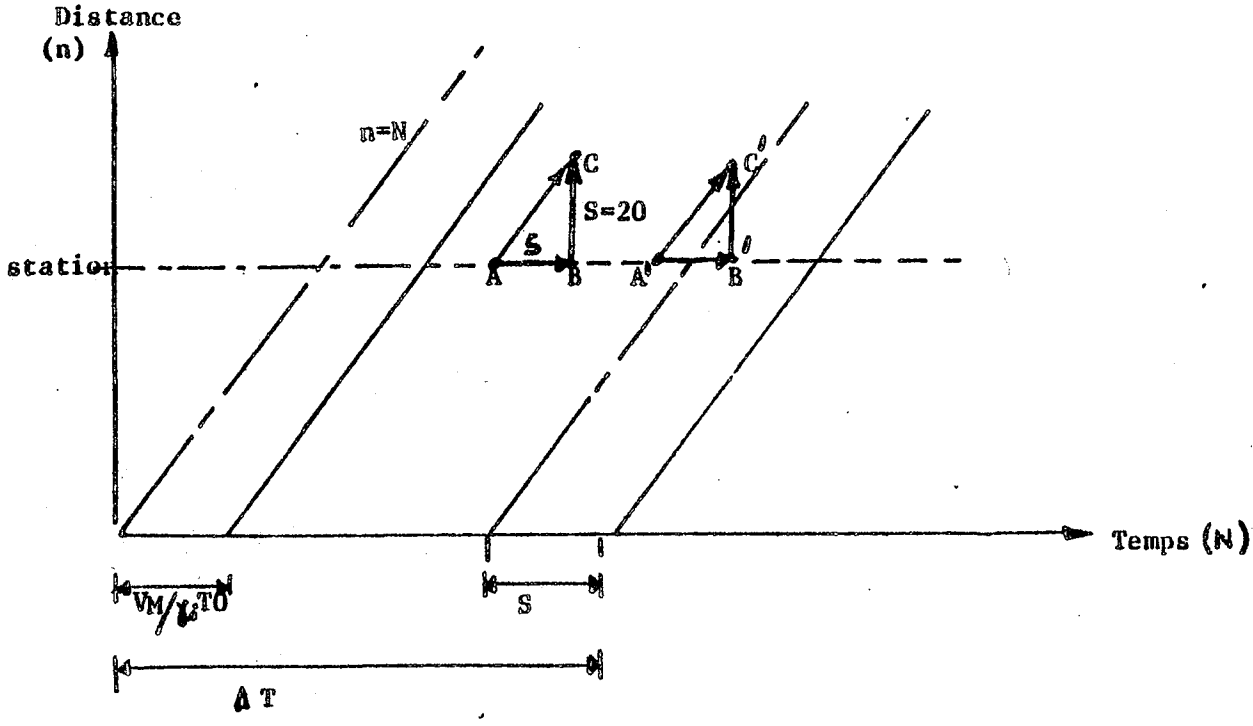


FIG.18

Toutefois, cette solution (chemin ABC, fig.18) peut amener la rame à sortir de son canton temporel (chemin A'B').

On peut par ailleurs, remarquer qu'une solution correspondant au chemin A (sans passer par B) est plus souple en ce qui concerne l'exploitation (pas d'arrêts fréquents des autres rames en ligne); ceci peut être réalisé de la manière suivante :

* Au lieu de décompter les 20 plots fictifs à la fin du stationnement, on les décomptera en décrémentant le compteur REG d'une unité à chaque impulsion T'_c reçue : tout se passe en fait comme si ces plots fictifs défilaient à la fréquence de l'horloge T'_c.

CONCLUSION :

La présentation des spécifications fonctionnelles que nous venons de faire peut être traduite par le schéma de la figure 19, sous la forme hiérarchisée de différents niveaux de spécification :

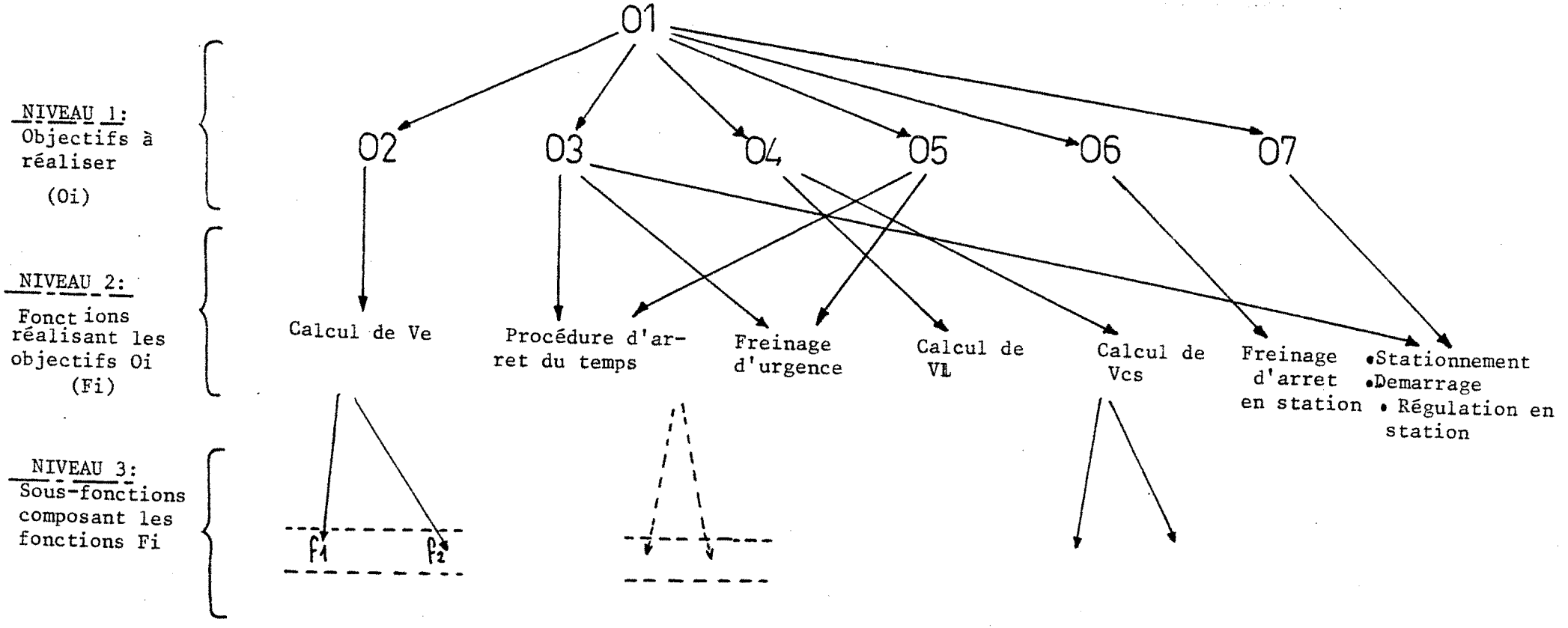
- un premier niveau constitue la spécification des objectifs (O_i) qui doivent être réalisés par le P.A.

- Un second niveau spécifie les diverses fonctions Fj (O_i) qui doivent être élaborées afin de réaliser les objectifs (O_i)

- Un troisième niveau constitue la description des sous-fonctions fj qui composent les fonctions Fj(O_i).

  etc....

Nous donnons un résumé de toutes ces fonctions sous la forme de "boîtes noires" en précisant les différentes informations d'entrée et de sortie (FIG.20).



* La réalisation de l'objectif O_1 équivaut à la réalisation des objectifs O_2, O_3, O_4, O_5, O_6 et O_7.

* Un objectif (O_i) est réalisé par un ensemble de fonctions (F_i).

* Une fonction (F_i) est composée de sous-fonctions (F_i),

etc...

FIG. 19

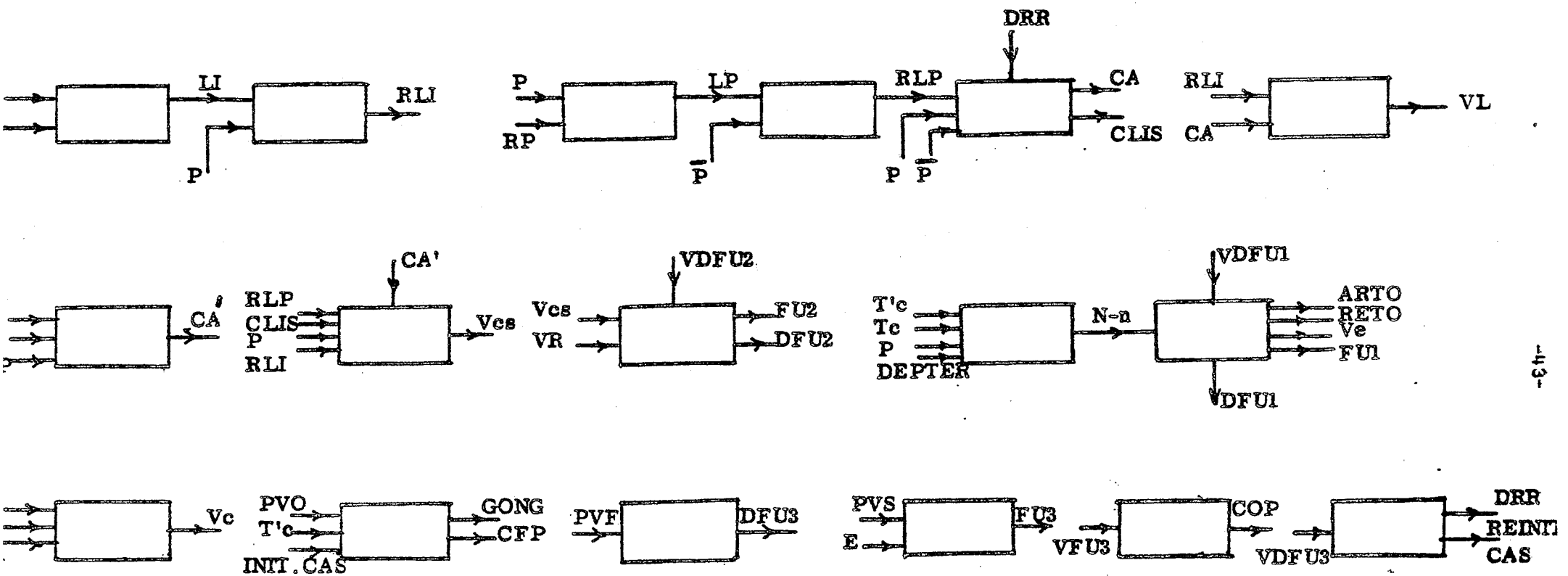


Figure 20 - Résumé des fonctions du système

CHAPITRE II

LES SPECIFICATIONS OPERATIONNELLES DU CAHIER DES CHARGES

A - Rappels sur la sûreté de fonctionnement

1 - Modèle général

2 - Composantes

B - Application à l'étude de notre système .

1_ Spécifications de l'exploitation

2_ Evaluation de l'objectif de fiabilité

3_ Evaluation de l'objectif de sécurité

Conclusion

Il s'agit dans cette partie des desiderata concernant le pilote automatique une fois implanté sur un matériel donné et mis en exploitation.

En général, plusieurs critères peuvent être considérés dans les spécifications opérationnelles d'un cahier des charges, par exemple :

- Goût de la réalisation
- Performances du système
- Spécifications du matériel d'implantation
- Qualité des interactions "Système-Environnement"
- Nature de la reprise en cas d'arrêt : manuelle, ou par télécommande,
- Sûreté de fonctionnement,...

Dans le cas qui nous intéresse, le P.A. sera étudié en vue d'une éventuelle réalisation sur microprocesseur ou sur réseau logique programmable (P.L.A.). Le critère auquel nous nous attacherons plus particulièrement est celui concernant la sûreté du fonctionnement du système, avec la condition suivante : Reprise manuelle non autorisée en cas d'arrêt en ligne.

A - RAPPELS SUR LA SURETE DE FONCTIONNEMENT D'UN SYSTEME

La sûreté de fonctionnement d'un système est une grandeur vectorielle complexe à plusieurs composantes : Fiabilité, disponibilité, sécurité, crédibilité, maintenabilité, réparabilité.

Dans tout ce qui suit, on définira une panne comme une défaillance matérielle du système, et une erreur comme une manifestation fonctionnelle de la pann

A.1) Modèle général de la sûreté de fonctionnement

D'une manière générale, l'ensemble des états que peut prendre un systéme peut être partitionné en trois sous-ensembles [LAPR75] :

- E_1 : sous-ensemble des états non défaillants
- E_2 : sous-ensemble des états défaillants tels que le système ne délivre pas de sorties erronées.
- E_3 : sous-ensemble des états défaillants tels que le système peut délivrer des sorties erronées.

a) Pour tous les états constituant le sous-ensemble (E_1), le système fonctionne correctement; on peut notamment avoir les états suivants :

. Il n'existe aucune panne dans le système (toutes les unités de la structure du système sont neuves ou complètement réparées).

. Il existe une panne, mais elle n'a pas encore provoqué d'erreurs (phénomène de latence).

. Certaines unités de la structure du système sont en réparation, mais le fonctionnement global est correct : cas des structures redondantes.

b) Pour le sous-ensemble (E_2), il s'agit d'une panne (simple ou multiple) qui a eu lieu.

Cette panne est détectée :

- soit en cours de fonctionnement correct ou incorrect par l'autodétection des erreurs manifestées,
- soit par une maintenance préventive.

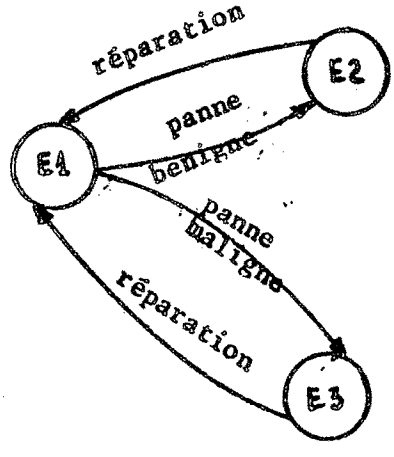
La réparation de la panne se fait alors soit par reconfiguration automatique du matériel, soit par intervention humaine.

c) Pour le sous-ensemble (E_3), il existe une panne (simple ou multiple) dans le système, qui a provoqué des erreurs, et qui n'ont pas été détectées.

Le système continue de fonctionner, mais peut délivrer des sorties erronées.

Les états du sous-ensemble (E_3) sont dits <u>contraires à la sécurité</u>.

On peut schématiser les sous-ensembles (E_1) ,(E2),et (E3) comme suit(Fig1)



- Le passage de (E_1) à (E_2) est dû à une "panne bénigne"
- Le passage de (E_1) à (E_3) est dû à une "panne maligne"
- Les passages de (E_2) à (E_1) et de (E_3) à (E_1) sont dûs à la réparation de la ou des unités dont la panne a provoqué la défaillance du système.
- Il n'y a pas de transition entre les états (E_2) et (E_3).

Fig.1

A.2) Composantes de la sûreté de fonctionnement

Nous rappelons ici la définition de certaines composantes de la sûreté de fonctionnement d'un système :

Fiabilité :

La fiabilité R(T) à l'instant T est égale à la probabilité que le système soit en état de bon fonctionnement, c'est-à-dire qu'aucune erreur ne se soit manifestée entre les instants 0 et T. La fiabilité à l'instant T d'un système est la probabilité que le système soit à un état $Q_1 \in (E_1)$, entre 0 et T.

$$R(T) = \text{Proba} \left\{ \text{état } (t) = Q_1 \in E1, \ \forall t \in [0,T] \right\}$$

Disponibilité :

La disponibilité A(T) à l'instant T est la probabilité que le système soit en état de bon fonctionnement à l'instant T, c'est-à-dire qu'il soit à un état $Q_1 \in (E_1)$ à l'instant T :

$$A(T) = \text{Proba} \left\{ \text{état } (T) = Q_1 \in (E_1) \right\}$$

Sécurité :

La sécurité S(T) à l'instant T est la probabilité que le système n'ait pas délivré des valeurs erronées au monde extérieur, c'est-à-dire qu'il n'y a pas eu d'erreurs non détectées de l'instant 0 à l'instant T.

La valeur de la sécurité est la probabilité que le système n'ait pas été dans un état $Q_3 \in (E_3)$, entre 0 et T.

$$S(T) = \text{Proba} \left\{ \text{état } (t) \neq Q3 \in (E_3), \ \forall t \in [0,T] \right\}$$

Crédibilité :

La crédibilité C(T) à l'instant T est la probabilité qu'il n'y ait pas d'erreurs non détectées à l'instant T. Sa valeur est donc égale à la probabilité que le système ne soit pas dans un état $Q_3 \in (E_3)$ à l'instant T.

$$C(T) = \text{Proba} \left\{ \text{état } (T) \neq Q_3 \in (E_3) \right\}$$

La disponibilité et la crédibilité n'ont une valeur différente, respectivement de la fiabilité et de la sécurité, que si le système est réparable.

Maintenabilité :

La maintenabilité M(T) est la probabilité que le système ne soit plus à un état $Q_2 \in (E_2)$ à l'instant T, sachant qu'il y était à l'instant 0.

La valeur de la maintenabilité est :

$$M(T) = 1 - \text{Proba}\left\{ \text{état } (t) = Q_2 \in (E2),\ \forall t \in [0,T] \right\}$$

L'état Q_2 considéré peut concerner soit le niveau matériel, soit le niveau logiciel, selon les conséquences de la panne produite :
la maintenabilité est un paramètre qui concernera, dans un cas, la maintenance curative du matériel, et dans l'autre cas, la remise en état du logiciel.

B. - APPLICATION A L'ETUDE DE NOTRE SYSTEME

Dans l'étude de notre système, nous ne nous intéresserons pas à la réparation de panne et à la reprise du système.

Les composantes de sûreté à considérer sont alors :

- la fiabilité
- la sécurité

Le graphe d'états du système peut être schématisé comme suit (fig. 2)

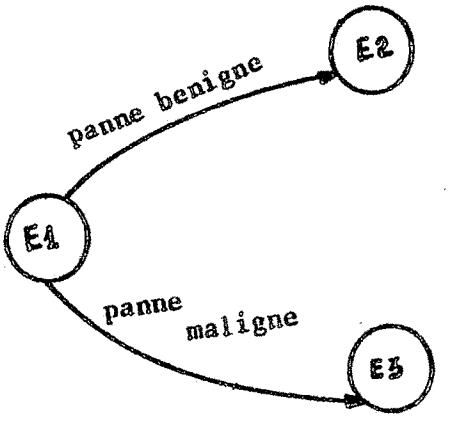


Fig.2

Les états entrant dans l'étude de sécurité sont les états du sous-ensemble $\{E1, E2\}$ puisque les états du sous-ensemble E_3 sont contraires à la sécurité.

Les états entrant dans l'étude de fiabilité sont ceux du sous-ensemble E_1. Pour tout état du sous-ensemble E_3, on dira qu'il y a risque d'accident.

En général, dans un système de transports terrestres, il existe deux grandes classes d'accidents :

. Les accidents non liés aù système de transports, et qui interviennent dans les accès des stations (accidents de circulation des piétons...)

. Les accidents liés au système de transport, dans lesquels les véhicules et l'infrastructure de transport sont impliqués.

Pour notre système particulier, on considérera :

- pour la fiabilité, les incidents bénins entraînant l'arrêt sûr de la rame,

- pour la sécurité, ceux des accidents qui sont dûs à un fonctionnement erroné du pilote automatique, notamment :

. Le risque de collision entre deux véhicules

. Le risque de survitesse, entraînant un déraillement d'une rame, dû à un dépassement de la vitesse limite autorisée

. Le risque de commande d'ouverture des portes du véhicule en ligne, ou de fermeture prématurée des portes dans une station.

B1) Evaluation des objectifs de fiabilité et de sécurité

L'évaluation de tels objectifs ne pourra se faire que par rapport à un modèle de référence : Nous choisirons celui du Métro de Paris (RATP), reconnu "sûr" et pour lequel nous disposons de données concernant les types d'accidents qui nous intéressent.

Les composantes de la sûreté de fonctionnement ont été définies comme des probabilités P (t) qui sont des fonctions décroissantes du temps t (à l'instant t = o, on a $P(0) = 1$).

On va spécifier ces probabilités par des fonctions exponentielles $e^{-\lambda t}$ qui correspondent à des taux de panne λ constants.

Soit λ_c la valeur de λ choisie .

La structure que nous nous proposons d'étudier sera déterminée par une fonction $\pi(t)$ telle que l'on ait, pour $t \in [0,T]$, T étant la durée d'exploitation pendant laquelle on se propose d'évaluer nos objectifs :

$$\pi(t) \geqslant e^{-\lambda_c \cdot T}$$

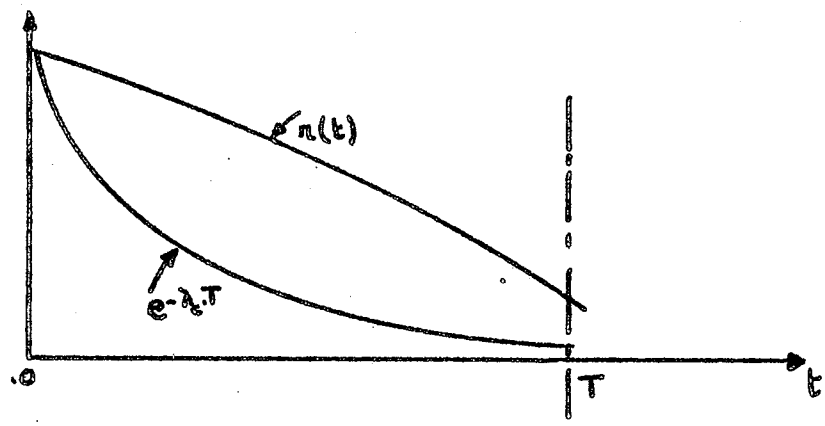


Fig. 3

B.1.1.) <u>Spécifications concernant l'exploitation</u>

On considérera les données suivantes :

Longueur de la ligne = 24 Km aller-retour

Fréquence des rames = 1 rame/minute aux heures de pointe

1 rame/2 minutes aux heures creuses

Vitesse commerciale = 40 Km/h

Durée de l'exploitation journalière = 20 heures

Répartition de cette durée = 4 heures de pointe et 16 heures creuses.

Désignons par v : la vitesse commerciale de l'exploitation

ΔT : l'intervalle entre les rames

L : la longueur de la ligne

La distance séparant deux rames successives est égale à : $v \times \Delta T$

Le nombre de rames en circulation est donc :

$$n_r = \frac{L}{v \times \Delta T}$$ soit aux heures creuses :

$$n_{r_1} = \frac{24}{40} \times \frac{1}{27/60} = 18 \text{ rames}$$

et aux heures de pointe :

$$n_{r_2} = \frac{24}{40} \times \frac{1}{17/60} = 36 \text{ rames}$$

Comme il y a 1 seul P.A par rame, on aura donc respectivement :

18 et 36 P.A

Calcul du nombre de P.A x heures actifs

Pendant 4 heures de pointe, on a : 36 x 4 = 144 P.A x heure

Pendant 16 heures creuses, on a : 18 x 16 = 288 P.A x heure

Pour une journée d'exploitation, on obtient :

144 + 288 = 432 P.A x heures actifs/jour

Pour une année d'exploitation, on a :

$N_1 = 432 \times 365$ soit $1,58 \times 10^5$ Heure x P.A actifs/an

Pour 20 années d'exploitation, on aura :

$N_{20} = 1,58 \times 10^5 \times 20$ soit $3,16 \times 10^6$ heure x P.A actifs/20 an

B.1.2.) Evaluation de l'objectif de fiabilité

L'objectif de fiabilité du modèle de référence (Métro de Paris) est de :

1 panne par pilote automatique et par an.

Il est cependant important de noter que, dans le cas du Métro de Paris comme dans celui de tous les métros à pilotage automatique en circulation dans le monde, la reprise manuelle, en cas d'arrêt, par un conducteur présent dans la cabine de pilotage est nécessaire.

Un tel objectif appliqué à notre système, où aucune reprise manuelle n'est autorisée, donnerait pour un ensemble de 36 rames, le chiffre de 36 incidents par an, soit 3 incidents par mois. Dans notre cas, cela se traduirait par 3 arrêts prolongés en ligne et par mois. Bien que de tels incidents n'entraînent pas d'accidents graves, ils constituent néanmoins une gêne certaine pour la qualité de service (Mécontentement de voyageurs, baisse de crédibilité à ce type nouveau d'exploitation...).

Il est par conséquent impératif pour nous de fixer un objectif de fiabilité encore plus sévère, soit :

Moins d'une panne par an

Evaluation du taux de panne correspondant

La durée à considérer pour l'objectif de fiabilité est :

$N_1 = 1{,}58 \times 10^5$ heures (durée d'exploitation pendant une année).

Le taux de panne s'en déduit :

$$\lambda_f = \frac{1}{N_1} \quad \text{soit} \quad \lambda_f = \frac{1}{1{,}58 \times 10^5} \quad , \text{ soit } \boxed{\lambda_f = 6{,}3 \times 10^{-6} \text{ panne/h}}$$

B.1.3) Evaluation de l'objectif de sécurité

Pour les différents types d'accidents à considérer, on dispose de données statistiques [GAB 74] qui nous conduisent au calcul des taux de panne suivants :

- Type d'accident : Risque de collision

Donnée :

Sur une période de 10 ans, il y a eu 4 collisions pour un nombre de rame x heures égal à $14{,}2 \times 10^6$.

Le taux de collision correspondant est :

$$\lambda_{col} = \frac{4}{14,2 \times 10^6} \quad \text{soit} \quad \lambda_{col} = 2,81 \times 10^{-7} \text{ panne/heure}$$

. Type d'accident : Risque de survitesse

Donnée :
Sur une période 10 ans, pour un nombre de rame x heure égal à $14,2 \times 10^6$, il y a eu 288 accidents.

Le taux de panne correspondant est :

$$\lambda_{sur} = \frac{288}{14,2 \times 10^6} \quad \text{soit} \quad \lambda_{sur} = 2,03 \times 10^{-5} \text{ panne/heure}$$

. Type d'accident : Risque de commandes intempestives des portes

Donnée :
On a enregistré 887 accidents sur une période de 10 ans correspondant à un nombre de rame x heure égal à $14,2 \times 10^6$.

Le taux de panne correspondant est :

$$\lambda_{por} = \frac{887}{14,2 \times 10^6} \quad \text{soit} \quad \lambda_{Por} = 6,2 \times 10^{-5} \text{ panne/heure}$$

Mais ces taux de panne sont des taux globaux, c'est-à-dire que pour chaque type d'accident, ils incluent le fonctionnement défectueux de plusieurs organes entrant en jeu dans la réalisation de la fonction désirée.

Comme dans ce travail, nous nous intéressons uniquement au pilote automatique, il convient de rapporter le fonctionnement du P.A à une fraction du fonctionnement global (c'est-à-dire celui de l'ensemble des organes d'une rame). Choisissons par exemple un tel rapport égal à $\frac{1}{10e}$.

Pour les trois types d'accidents considérés, nous prendrons alors comme objectifs de sécurité, les valeurs de taux de panne suivantes:

Taux de collision = $\lambda_{col/10}$ soit : $\lambda_c = 2,81 \times 10^{-8}$ panne/heure

Taux de survitesse = $\lambda_{sur/10}$ soit : $\lambda_s = 2,03 \times 10^{-6}$ panne/heure

Taux de panne des portes = $\lambda_{por/10}$ soit : $\lambda_p = 6,2 \times 10^{-6}$ panne/heure

En résumé, on demandera de l'ensemble du P.A :

. Une fiabilité $f_{PA}(t)$ correspondant à un taux de panne $\lambda f = 6,3 \times 10^{-6}$ panne sur une durée d'une année, soit :

$$f_{PA}(t) \geqslant e^{-(6,3 \times 10^{-6})t} \quad \text{pour } 0 \leqslant t \leqslant 1,58 \times 10^{8} \text{ heures}$$

. Pour la sécurité, on distinguera trois fonctions :

- Anti-collision
- Anti-survitesse
- Surveillance de la commande d'ouverture et de fermeture des portes

Pour chacune de ces fonctions réalisées par le P.A., on demandera des sécurités $s_1(t)$, $s_2(t)$ et $s_3(t)$ correspondant aux taux de panne respectifs λc, λs et λp sur une durée de 10 ans, soit :

$$\begin{cases} s_1(t) \geqslant e^{-2,81 \times 10^{-8} t} \\ s_2(t) \geqslant e^{-2,03 \times 10^{-6} t} \\ s_3(t) \geqslant e^{-6,2 \times 10^{-6} t} \end{cases}$$

pour $0 \leqslant t \leqslant 1,58 \times 10^{8}$ heures

CHAPITRE III

REPRESENTATION DU CAHIER DES CHARGES A L'AIDE DU GRAFCET

A - Rappel des Réseaux de Pétri

A.1 - Structure

A.2 - Représentation

A.3 - Marquage

A.4 - Règles d'évolution

A.5 - Définitions : Marquages borné et sauf, vivacité, conflit.

B - Décomposition Partie Opérative - Partie contrôle

C - Interprétation d'un Réseau de Pétri

C.1 - Réseau de Pétri Temporisé

C.2 - Réseau de Pétri Synchronisé

C.3 - Réseau de Pétri Temporisé Synchronisé

C.4 - Réseau de Pétri Interprété

D - GRAFCET

D.1 - Interprétation

D.2 - Extension

CONCLUSION

E - Représentation sous forme de Grafcets du Cahier des Charges

E.1 - Représentation de la vitesse V_e

E.2 - " de la vitesse V_L

E.3 - " de la vitesse V_{cs}

E.4 - " de la fonction "Contrôle de l'arrêt d'horloge"

E.5 - " des mécanismes de freins

5.1) Freins d'urgence

5.2 " anti survitesse

5.3 " d'arrêt en station

E.6 - Représentation de l'automatisme en station

E.7 - " de la régulation en station

E.8. " de la vitesse V_c

CONCLUSION

La description qui a été donnée du système, dans le chapitre I, est fastidieuse, et demande un effort de compréhension de la part du lecteur. La présentation sous forme rédigée peut en outre être mal interprétée.

Par ailleurs, une telle description demeure insuffisante :

. Le système a été décrit comme un ensemble de boîtes noires réalisant chacune une fonction spécifique. Cette description ne met pas en évidence les parallélisme , séquentialité et synchronisme entre les différentes variables et fonctions du système.

. L'analyse est difficile à faire : détection de situations de conflit ou de fonctionnement pouvant conduire à des blocages dans le système ; recherche d'éventuelles ambiguités et d'incohérences dans les spécifications du Cahier des Charges.

. Les interactions du P.A avec l'environnement extérieur (PCC, Station, Freins, Moteurs, Portes,...) sont mal représentées : en particulier, en ce qui concerne l'ordre de prise en compte des évènements engendrés par cet environnement.

Il est par conséquent nécessaire d'avoir à notre disposition un ou des outils adéquats :

- de description : qui puissent représenter les évolutions synchrones et asynchrones du système, et qui soient faciles à comprendre;
- et d'analyse : qui puissent mettre en évidence ces éventuelles ambiguités.

Nous avons choisi d'utiliser deux modèles dérivés des Réseaux de Pétri :

. Le Grafcet, en tant qu'outil de description

. Les Réseaux de Pétri Interprétés en tant qu'outil d'analyse et de conception.

A - RAPPEL DES RESEAUX DE PETRI

Définition formelle des Réseaux de Pétri [PET 77] [RAM 73] :

A.1 - Structure d'un Réseau de Pétri

Un Réseau de Pétri $\mathcal{P}$ est un triplet $< \mathcal{Q}, \mathcal{T}, \mathcal{A} >$ où :

$\mathcal{Q}$ désigne un ensemble non vide de places $\{Q1, Q2, \ldots Qn\}$

$\mathcal{T}$ désigne un ensemble non vide de transitions $\{t1, t2, \ldots, tm\}$

$\mathcal{A}$ est une relation ; c'est un ensemble d'arcs, joignant une place à une transition, ou joignant une transition à une place.

$$\mathcal{A} \subseteq (\mathcal{Q} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{Q})$$

Les 3 ensembles $\mathcal{Q}$, $\mathcal{T}$, $\mathcal{A}$ définissent la structure d'un Réseau de Pétri.

A.2 - Représentation de la structure d'un Réseau de Pétri

A la structure du Réseau, correspond un graphe biparti dont les noeuds sont des places ou des transitions.

Une place est représentée par un cercle, et une transition par un trait. Un arc est orienté d'une place Qi vers une transition tj si la place Qi est une place d'entrée de la transition tj ; de même, un arc est orienté d'une transition tj vers une place Qi si la place Qi est une sortie de la transition

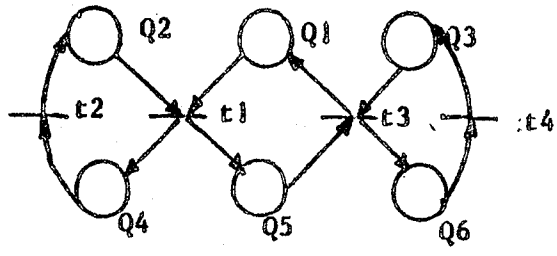
Notation :

Nous nous servirons dans la suite d'une notation qui nous paraît souple [RAM 73]. L'élément $(Q,t) \in \mathcal{A}$ s'écrit Q.t.

L'ensemble des éléments successeurs de a est $\{b \;/\; a.b\}$ et s'écrit $a^\bullet$

L'ensemble des éléments-prédécesseurs de a est $\{b \;/\; b.a\}$ et s'écrit $^\bullet a$

Exemple :



Ce graphe de Réseau de Pétri correspond à la structure suivante :

$\mathcal{Q} = \{Q1, Q2, Q3, Q4, Q5, Q6\}$

$= \{t1, t2, t3, t4\}$

$Q1. = \{t1\}$	$.t1 = \{Q1, Q2\}$	$t1. = \{Q4, Q5\}$
$Q2. = \{t1\}$	$.t2 = \{Q4\}$	$t2. = \{Q2\}$
$Q3. = \{t3\}$	$.t3 = \{Q3, Q5\}$	$t3. = \{Q1, Q6\}$
$Q4. = \{t2\}$	$.t4 = \{Q6\}$	$t4. = \{Q3\}$
$Q5. = \{t3\}$		
$Q6. = \{t4\}$		

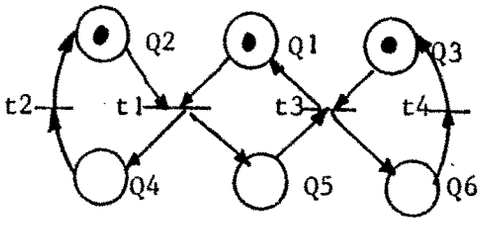
A.3) Définition d'un marquage

Un marquage M est une fonction telle que : $Qi \in \mathcal{Q} \longrightarrow M(Qi) \in N$

N étant l'ensemble des entiers naturels.

M (Qi) est appelé charge de la place Qi, et représente le nombre d'objets, appelés marques, pouvant se déplacer dans le graphe, et appartenant à la place Dans un graphe de Réseau de Pétri, une marque est représentée par un point.

Le réseau de Pétri $\mathcal{P} = < \mathcal{Q}, \mathcal{T}, \mathcal{A} >$ muni d'un marquage M devient un Réseau de Pétri marqué $\mathcal{P}_m = < \mathcal{Q}, \mathcal{T}, \mathcal{A}, M >$ /



M (Q1) = M (Q2) = M (Q3) = 1

M (Q4) = M (Q5) = M (Q6) = 0

Le marquage du Réseau peut être représenté par un vecteur M = (1,1,1,0,0,0)

Ce vecteur a pour dimension le nombre de places du Réseau ; ses composantes représentent les charges respectives des places.

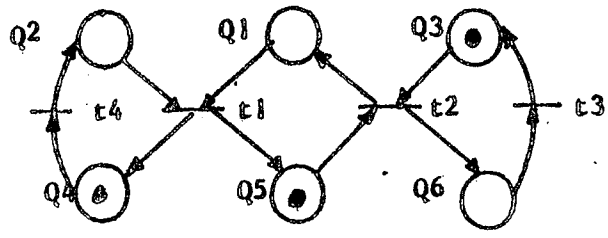
Remarque : *Dans tout ce qui suit, nous étudierons des graphes de Réseaux de Pétri marqués, mais par abus de langage, nous dirons simplement Réseau de Pétri.*

A.4) Règles d'exécution d'un Réseau de Pétri

. Une transition t_i est dite validée si et seulement si toutes ses places d'entrée possèdent chacune au moins une marque.

. Une transition validée peut être mise à feu : Une marque est alors enlevée de chaque place d'entrée, et une marque est placée dans chaque place de sortie.

Dans l'exemple précédent, la transition t_1 est validée, car M (Q1) = M (Q2)= La transition t3 n'est pas validée, car M (Q5) = 0.
La mise à feu de la transition t_1 donne :



Le vecteur marquage devient M1 = (0,0,1,1,1,0)

Maintenant, la transition t2 peut être mise à feu, car les places Q3 et Q5 possèdent chacune une marque. La transition t4 peut aussi être mise à feu.

Le vecteur marquage d'un Réseau de Pétri représente l'état du système.

A.5.) Définitions :

Définition 1 :

Séquences de tirs et classes de marquages

Soit M0 le marquage initial du Réseau de Petri.Soit M1 le marquage qui résul du tir d'une transition t1,à partir de M1;on note $M0 \xrightarrow{t_1} M1$.De même,soit M2 le marquage obtenu à partir de M1 après le tir d'une transition t2,c'est à dire $M1 \xrightarrow{t_2} M2$.Plus généralement,$M0 \xrightarrow{t_1} M1 \xrightarrow{t_2} M2 \rightarrow \ldots\ldots \xrightarrow{t_n} Mn$,et on note $M1 \xrightarrow{\sigma} Mn$; t1t2.....tn est appelée sequence de tirs des transitions t1,t2,....,tn qui engendre Mn à partir de M0.

L'ensemble des marquages accessibles à partir d'un marquage M est noté $[\vec{M}]$

Définition 2 :

Marquage borné, sauf

Un marquage M est borné pour une place Q_i, si et seulement si, il existe un entier n tel que $\forall M \in [\vec{M}], M(Q_i) \leq n$.

Si n = 1, le marquage est dit sauf pour Q_i.

Un marquage M est borné (ou sauf) pour un Réseau de Pétri $\mathcal{P}$ si et seulement si M est borné (ou sauf) pour toutes les places du Réseau.

Définition 3 :

Une transition tj est dite vivante pour un marquage M si pour tout marquage $M_i \in [\vec{M}]$, il existe une séquence σ qui peut mettre à feu tj.

Un réseau de Pétri est dit vivant si :

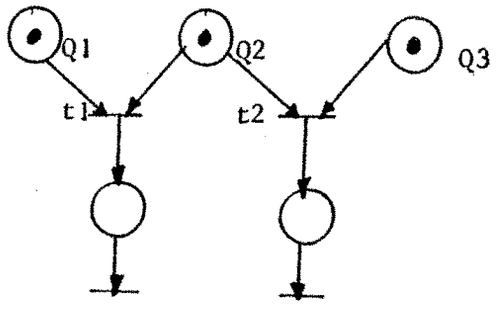
$\forall tj \in \mathcal{C}$, tj est vivante pour tout marquage $M_i \in [\vec{M}]$.

Définition 4 :

On dit qu'un Réseau de Pétri sauf est sans conflit s'il ne peut pas exister une situation où une place Qi se trouve partagée par deux ou plusieurs transitions distinctes pouvant être mises à feu simultanément.

Exemple de conflit :

$\bullet t1 \cap \bullet t2 = \{Q2\}$



B - DECOMPOSITION DU SYSTEME EN PARTIE CONTROLE - PARTIE OPERATIVE

Notre système peut être décomposé en deux parties : Une partie contrôle et une partie opérative.

a) La Partie opérative contient les données et les opérateurs utilisés pour effectuer des opérations sur ces données.

b) La Partie contrôle est un automate qui gère les activations des opérations. A chaque état de la Partie contrôle, un symbole de sortie est interprété par la Partie opérative comme l'ordre d'exécuter une action suivant un ou plusieurs opérateurs. La Partie contrôle évolue d'un état à un autre état, en fonction des changements de ses entrées, qui sont soit des valeurs de test calculées dans la Partie opérative, soit des évènements externes engendrés par l'environnement du système (fig.1)

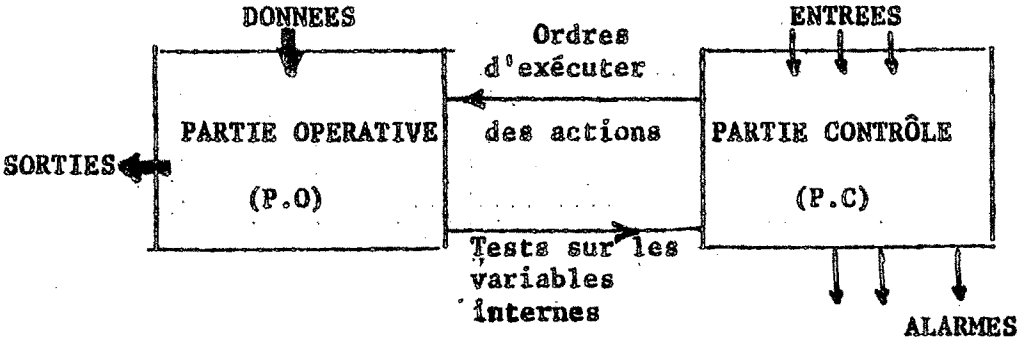


Fig.1 - DECOMPOSITION DU SYSTEME P.A

Le système P.A que nous venons de décomposer en Partie-contrôle et Partie opérative échange des informations avec les deux systèmes suivants :(Fi

1) le système "Processus physique à automatiser" * : (Freins, portes, Moteurs, Asservissement,...)
2) Le système "Environnement" : (P.C.C., voie, Roue phonique, détecteur de plot, Génératrice tachymétrique).

* Remarque : Certains auteurs utilisent le mot "Partie opérative" pour désigne le "Processus à automatiser" [GRA 77].

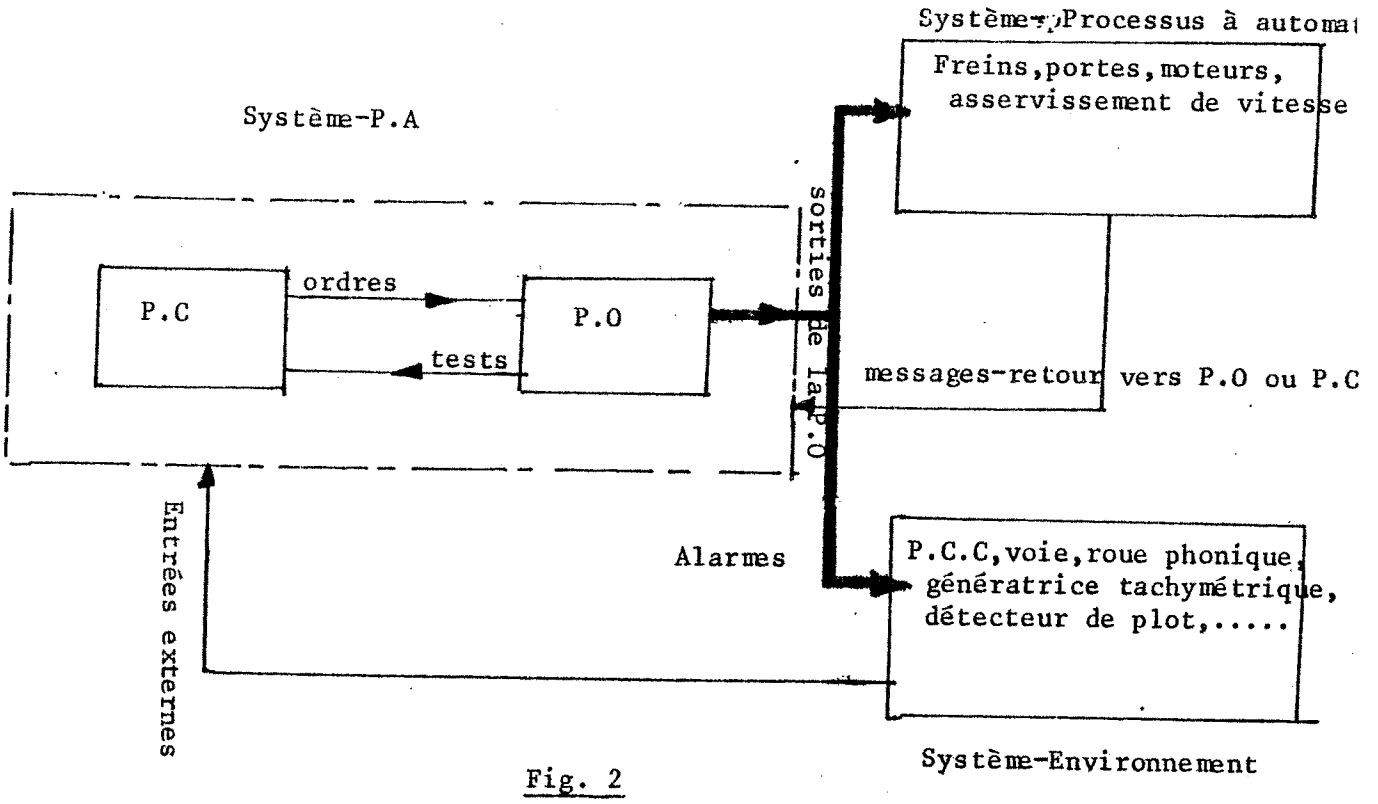


Fig. 2

C - INTERPRETATION DU RESEAU DE PETRI

Les Réseaux de Pétri que nous venons de présenter ont été surtout utilisés en tant que modèle mathématique : vérification de propriétés mathématiques, preuves de programmes, files d'attente, gestion des systèmes d'exploitation,...

Ils sont fondés sur l'hypothèse d'un fonctionnement asynchrone et autonome. Mais ils ne sont pas adaptés à la modélisation des systèmes de commande en temps réel, où l'environnement extérieur a une influence sur le système et où le facteur temps doit être pris en considération.

Des modèles dérivés des Réseaux de Pétri ont été définis afin de permettre la représentation d'une plus large gamme de systèmes réels.

Donner une interprétation à un Réseau de Pétri consiste à donner au Réseau une signification (une signification aux places, et une signification aux transitions), en précisant ses liens avec l'environnement extérieur, autrement dit en explicitant les évènements reçus de l'extérieur, et les actions engendrées et envoyées vers l'environnement [BLA 73] [AZO 76].

Un Réseau de Pétri muni d'une interprétation est dit Réseau de Pétri Interprété.

Nous allons rappeler quelques définitions formelles de modèles dérivés de Réseaux de Pétri, et nous expliquerons les règles d'évolution des Réseaux de Pétri Interprétés.

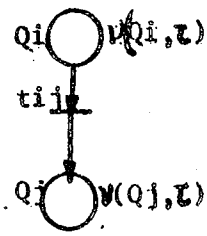
C.1) Réseau de Pétri temporisé : [RAM 73] [SIF 77]

Définition :

Un réseau de Pétri temporisé est défini par un sextuplet $(Q, \mathcal{C}, A, M, T, \nu)$ où

- $(Q, \mathcal{C}, A, M)$ est un Réseau de Pétri $\mathcal{R}_m$ marqué
- T est un sous-ensemble complètement ordonné de R, appelé base de temps ; (R = ensemble des réels).
- $\nu = Q \times T \longrightarrow T$ telle que si $\nu(Q, \tau_i) = \tau_j$ alors $\tau_j \geqslant \tau_i$

On représente un réseau de Pétri par le Réseau de Pétri associé en indiquant sur chaque place Q l'application $\nu(Q,\tau)$.



Règles d'évolution

- Une marque dans un réseau de Pétri temporisé peut se trouver dans l'un des deux états disponible ou indisponible.

  Initialement, si une place Q est marquée, elle contient M_0 (Q) marques disponibles.

- Une transition tj est validée si toutes ses places d'entrée contiennent au moins une marque disponible. Toute transition validée peut être mise à feu. La mise à feu d'une transition tj qui est validée consiste à enlever une marque disponible de chaque place d'entrée et à mettre une marque indisponible dans chaque place de sortie.

- Une marque reste indisponible dans une place Q durant l'intervalle de temps entre l'instant τ_o de son arrivée à la place et l'instant $\nu(Q,\tau_o)$, puis devient disponible.

Remarque :

Pour une place Q, la fonction $\nu(Q,\tau)$ n'est définie que pour les valeurs $\tau_j \in T$. Il se pose alors le problème de la durée de la mise à feu des transition toute mise à feu doit avoir une durée cadrée sur $[\tau, \tau_j]$ tel que $\tau_j \in T$.
Le problème se résoud de lui-même si $T = R$ (donc ν partout définie). Si $T \neq R$, on peut convenir de considérer que toute mise à feu est instantanée et qu'elle doit être effectuée dès la validation de la transition.

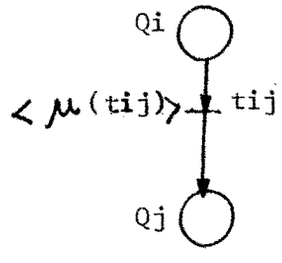
C.2 Réseau de Pétri synchronisé [MOA 78]

Définition

Un Réseau de Pétri synchronisé est défini par un sextuplet $(Q, \mathcal{T}, A, M, E, \mu)$ où :

- $(Q, \mathcal{T}, A, M)$ est un Réseau de Pétri marqué P_m
- $E = \{e1, e2, \ldots, e_s\}$ est un ensemble d'évènements externes
- $\mu: \mathcal{T} \longrightarrow E \cup \{e\}$ où e est l'élément neutre de E appelé "évènement toujours présent "

On représente un Réseau de Pétri synchronisé par le Réseau de Pétri associé en portant sur chaque transition tj le facteur $<\mu(tij)>$ où $\mu(tj)$ est l'évènemen associé à tj.



Règles d'évolution

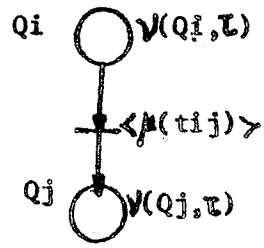
Les règles d'évolution sont les mêmes que dans un Réseau de Pétri à la différence que la mise à feu d'une transition validée tj ne peut avoir lieu qu'au moment de l'occurrence de $\mu(tj)$. Aussi, cette mise à feu est instantanée.

C.3) Réseau de Pétri Temporisé Synchronisé

Définition :

Un Réseau de Pétri Temporisé Synchronisé est la superposition d'un Réseau de Pétri Temporisé $(Q, \mathcal{E}, A, M, T, \nu)$, et d'un Réseau de Pétri Synchronisé $(Q, \mathcal{E}, A, M, E, \mu)$ construits à partir d'un même Réseau de Pétri marqué P_m $(Q, \mathcal{E}, A, M)$. De plus, les évènements de E sont tels que leur occurrence ne peut avoir lieu qu'à des instants $\tau j \in T$.

On représente un Réseau de Pétri Temporisé Synchronisé par le Réseau de Pétri marqué associé en indiquant sur chaque place Q l'application $\nu(Q, \tau)$ et sur chaque transition tj l'évènement $\mu(tj)$.



Règles d'évolution :

Les règles d'évolution sont obtenues en superposant celles définies pour le Réseau de Pétri Temporisé et le Réseau de Pétri Synchronisé.

- Une marque dans une place Q peut se trouver dans l'un des deux états disponible ou indisponible. Toute place Q marquée initialement contient M_0 (Q) marques disponibles.

- Une transition tj est validée si toutes ses places d'entrée contiennent au moins une marque disponible. Mais la mise à feu d'une transition validée ne peut avoir lieu qu'au moment de l'occurrence de l'évènement associé $\mu(tj)$.

- La mise à feu d'une transition tj est instantanée. Elle consiste à enlever de chaque place d'entrée une marque disponible et à mettre dans chaque place de sortie une marque indisponible.

- Une marque reste indisponible dans une place Q durant l'intervalle de temps entre l'instant τ_0 de son arrivée à la place et l'instant $\nu(Q, \tau_0)$.

C.4) Réseau de Pétri Interprété [MQA 76]

Définition

Un Réseau de Pétri Interprété est défini par la donnée :

- d'un sous-système opératif (D, oP, C) tel que :

. $D = \{ d_1, d_2, \ldots d_u \}$ est un ensemble fini de variables de données prenant leurs valeurs respectivement dans des espaces $D_1, D_2, \ldots D_u$;

. $oP = \{ oP1, oP_2, \ldots, oP_K \}$ est un ensemble fini d'opérateurs qui effectuent des transformations sur les données, ces opérateurs étant définis comme des applications internes dans D ;

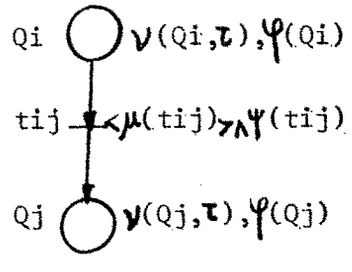
. $C = \{c1, c2, \ldots, C_n\}$ est un ensemble de conditions (prédicats) sur les valeurs des données d_u.

- d'un Réseau de Pétri Temporisé Synchronisé $(Q, \mathcal{E}, A, M, T, \nu, E, \mu)$;

- d'une application $\varphi : Q \rightarrow oP$;

et d'une application $\psi : \mathcal{E} \rightarrow C$.

On représentera un Réseau de Pétri Interprété par le Réseau de Pétri Temporisé Synchronisé associé en indiquant sur chaque place Qi l'opérateur $\varphi(Qi)$ et sur chaque transition tj la condition $\psi(tj)$.



Règles d'évolution :

L'interprétation définie par le sous-système opératif (D, oP, C) et les applications Ψ et Ψ introduit deux précisions supplémentaires aux règles d'évolution établies pour un Réseau de Pétri Temporisé Synchronisé.

- La mise à feu d'une transition validée tj n'est autorisée que si la condition $\Psi(tj)$ est vérifiée. En tout cas, cette mise à feu ne peut avoir lieu qu'au moment de l'occurrence de l'évènement $\mu(tj)$.

- L'arrivée d'une marque dans une place Q active l'opérateur $\Psi(Q)$. Cette marque reste indisponible durant l'intervalle de temps entre l'instant τ_0 de son arrivée à la place et l'instant $\Psi(Q, \tau_0)$, puis devient disponible.

D. - LE GRAFCET [GRA 77]

Le GRAFCET (Graphe de Commande Etape-Transition) est un outil de spécification défini par la Commission de Normalisation de la représentation du Cahier des Charges d'un automatisme logique. Cet outil est adapté à une approche hiérarchisée du Cahier des Charges selon 2 niveaux :

. Le niveau fonctionnel où l'on décrit le comportement de l'automatisme face aux différentes situations qui peuvent se présenter ;

. Le niveau technologique, où les éléments technologiques de l'automatisme sont précisés.

Le GRAFCET est un modèle largement inspiré des Réseaux de Pétri : Le mot "place" dans les Réseaux de Pétri est remplacé dans le Grafcet par "étape". Une étape peut être active ou inactive ;

D.1) L'interprétation du GRAFCET consiste à associer :

- à une place une ou plusieurs actions (éventuellement nulles)
- à une transition une réceptivité.

Une réceptivité est composée d'un évènement et d'une condition logique :

. L'évènement traduit le passage d'une variable d'une valeur à une autre valeur, ce qui peut être le fait de l'environnement ou d'une quelconque évolution interne au système.

. La condition peut porter sur les valeurs des variables internes au systèm sur celles des variables à niveau externes, ou sur les états d'activité ou d'inactivité des étapes.

Remarques :

. *Si la réceptivité comprend seulement un évènement, celui-ci est considéré comme associé à une condition toujours vérifiée.*

. *Si la réceptivité comprend seulement une condition, celle-ci est considérée comme associée à un évènement "toujours présent".*

. *Si la réceptivité n'est pas spécifiée, elle est considérée comprenant une condition toujours vérifiée, et un évènement toujours présent.*

. *Deux évènements distincts ne peuvent pas avoir lieu simultanément.*

Les règles d'évolution du GRAFCET sont les suivantes :

. Les étapes activées au début du fonctionnement représentent l'état initial du système (elles sont alors représentées par des double-cercles ◎).

. Une transition est validée lorsque toutes les étapes immédiatement précédentes sont actives.

. Une transition est franchie si elle est validée et si la réceptivité associée est vraie.

. Lorsqu'une transition est franchie, toutes les étapes immédiatement successeurs sont activées, et toutes les étapes immédiatement précédentes sont désactivées.

On peut noter qu'à une terminologie près, ces règles sont semblables à celles du Réseau de Pétri Interprété.

Cependant, des remarques doivent être faites :

- Dans le Grafcet, la réactivation d'une étape déjà activée n'a aucune influence (l'étape reste activée) : en d'autres termes, la notion d'accumulation de marques qui existe dans le Réseau de Pétri disparaît.

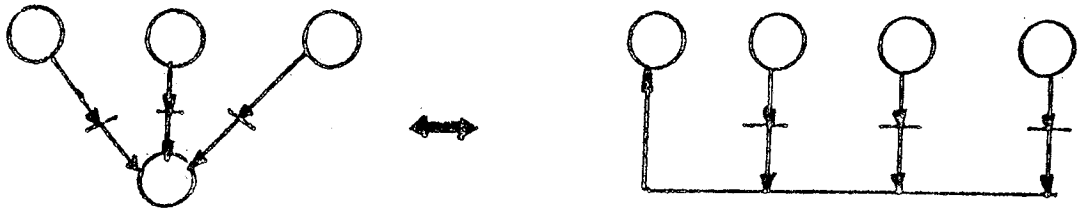
- Dans le Réseau de Pétri Interprété, l'association à une transition de l'état d'activité ou d'inactivité d'une place n'est pas permise.

Par ailleurs, les notations recommandées dans le Grafcet apportent beaucoup plus de simplification, de clarté et de précision dans la représentation du Cahier des Charges ; on peut notamment mentionner :

- l'introduction du temps associé à une étape ou à une réceptivité
- le fait de préciser la nature d'un signal : par exemple, une variable à niveau est notée X ou $\overline{X}$ selon que l'on s'intéresse à son état 1 ou 0.
  $\uparrow X$ représente le passage de X de l'état 0 à l'état 1
  $\downarrow X$ représente le passage de X de l'état 1 à l'état 0.
- ou le fait de préciser la nature d'une action qui peut être :
  - impulsionnelle (exécutée dès l'activation de l'étape associée, et qui dure un certain temps).
  - ou à niveau.

Si A est une action impulsionnelle, elle sera notée A^{*}.

- La simplification de graphisme afin de ne pas multiplier les arcs reliant des transitions à une même étape.



D.2) Extension de l'interprétation

L'interprétation donnée du GRAFCET spécifie en fait les automatismes logiques. Comme il s'agit dans notre étude d'un système de commande en temps réel, nous étendons l'interprétation précédente comme suit :

a) Définition

Un marquage instable est un marquage qui valide une transition non associée à un évènement explicite et dont la condition est vérifiée.

b) Règles :

b.1) *Toute occurrence d'un évènement explicite, c'est-à-dire différen de l'évènement toujours présent, doit trouver le Grafcet dans un état stable.*

b.2) *Dans une réalisation pratique, lorsque des calculs sont effectué nous considérons que leur durée devra être suffisamment courte pour que le système atteigne un état stable avant une nouvelle occurrence d'un évènement explicite.*

CONCLUSION

Que la Commission du Groupe Systèmes Logiques de l'AFCET ait proposé une normalisation des outils de représentation du Cahier des Charges d'un automatisme, lesquels devenaient de plus en plus nombreux d'autant qu'ils sont pour la plupart dérivés des Réseaux de Pétri, cela n'a pas empêché le déclenchement d'une polémique sur l'utilisation du GRAFCET et du Réseau de Pétri [VAL 78] [BLA 79].

En ce qui nous concerne, nous pensons que le GRAFCET et le Réseau de Pétri Interprété sont assez voisins l'un de l'autre, et que le passage d'un modèle à un autre peut se faire facilement.

Par ailleurs, tel que le GRAFCET est défini actuellement, il s'avère un bon outil de représentation d'automatismes logiques simples ; la normalisation de la représentation ne peut qu'aider à rendre plus compréhensible un Cahier des Charges par tout lecteur.

Cependant, pour le concepteur, la simple représentation du Cahier des Charges ne suffit pas :

Il lui faut analyser les spécifications du système, les vérifier afin qu'il n'y ait aucune ambiguité ni incohérence dans le fonctionnement étudié, avant de passer au stade de la réalisation matérielle. Or l'intérêt porté par les analystes aux Réseaux de Pétri est surtout dû à la notion de marque se déplaçant dans le Réseau.

Dans le GRAFCET, cette notion n'existe pas, et l'absence de considération de l'accumulation de marques dans une même étape exclut toute possibilité de vérifier que les actions associées aux étapes sont exécutées autant de fois que le fonctionnement le demande.

Aussi, dans une première étude, nous utiliserons le GRAFCET en tant qu'outil de représentation du Cahier des Charges : Cette étape constituera une aide considérable à tout lecteur pour mieux assimiler ce qui a été exposé sous une forme rédigée dans le premier chapitre.

Dans une seconde étude, nous utiliserons les Réseaux de Pétri Interprétés en tant qu'outil d'analyse et de conception.

Comme on le verra, nous pensons que cette approche constitue une solution cohérente dans la conception d'un modèle fonctionnel sûr.

E - REPRESENTATION SOUS FORME DE GRAFCET DU CAHIER DES CHARGES

Nous nous proposons dans cette partie d'utiliser le Grafcet en tant qu'outil de description et de spécification d'un Cahier des Charges.

La représentation graphique de chaque fonction sera faite séparément.

L'état initial considéré correspondra à celui où le système, étant au repos, est alors mis sous tension.

L'étude de chaque fonction se fera entre l'instant où le P.C.C. émet l'ordre DEPTER autorisant le départ de la rame de la station terminale et l'instant de détection du signal ARTER d'arrivée de la rame dans la station terminale.

Les fonctions qui seront étudiées sont représentées sur le schéma général de la figure 1 :

- fonction de calcul de la vitesse de régulation (V_e)
- fonction de calcul de la vitesse limite (V_L)
- fonction de calcul de la vitesse de consigne de sécurité (V_{cs})
- fonctions de contrôle des mécanismes de freins
- fonction de contrôle de l'arrêt d'horloge centrale
- fonction de calcul de la vitesse de commande (V_c)
- fonction d'automatisation du stationnement d'une rame
- fonction de régulation en station.

Pour chaque Grafcet décrit, on indiquera les entrées et les sorties du sous-système représenté, ainsi que l'état initial de ses variables.

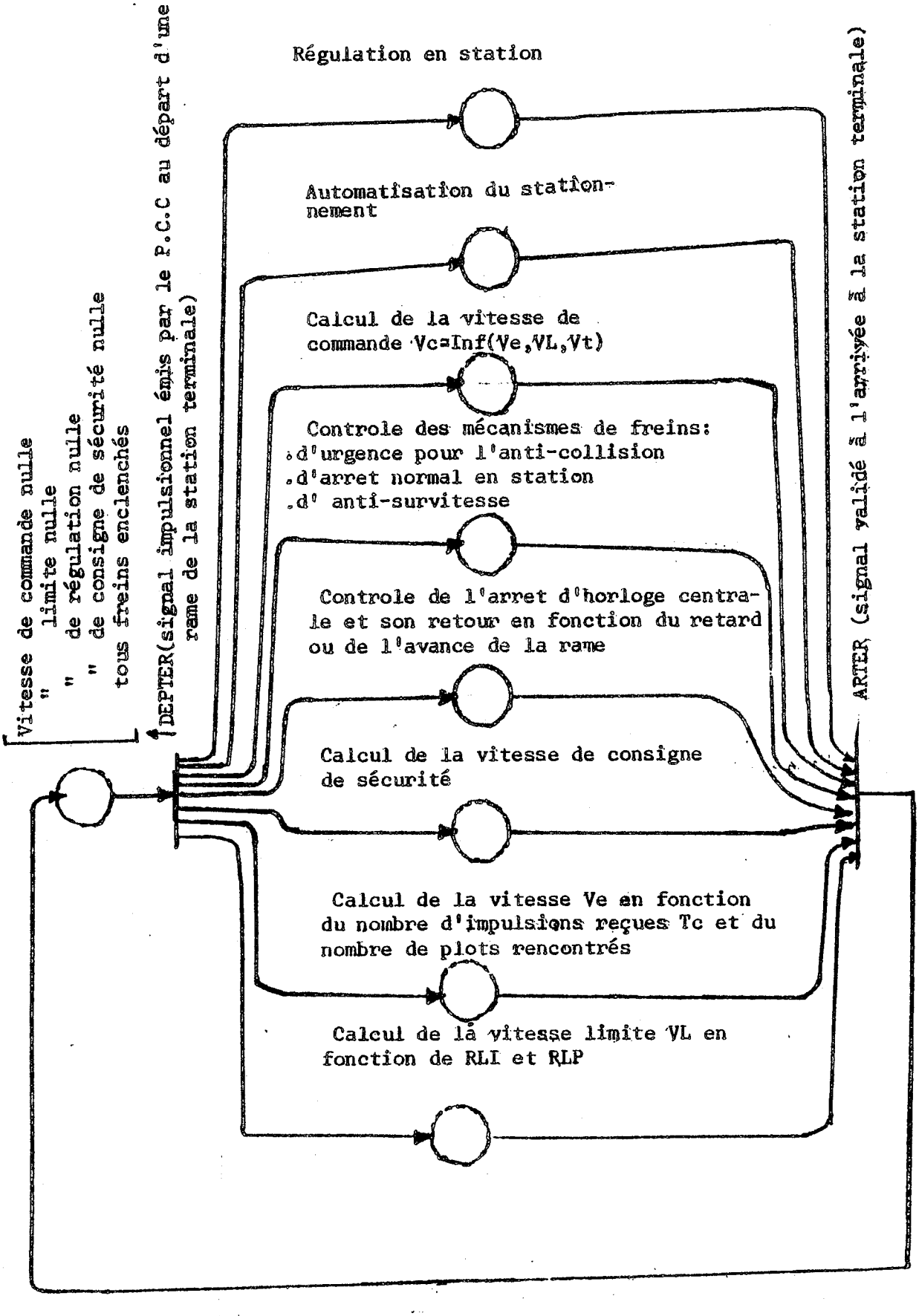


Fig.1 Schéma général des fonctions du P.A .

RAPPEL DE NOMENCLATURE

DEPTER = Signal impulsionnel émis par le P.C.C. pour ordonner le départ de la rame de la station terminale.

P = Signal à niveau de détection de plot

T_c = Impulsion d'horloge émise par le P.C.C. (période = 1 s)

T'_c = Impulsion d'une horloge interne de période 1 s, indépendante de l'horloge centrale, et utilisée pour la gestion du stationnement.

RP = Signal impulsionnel engendré par la roue phonique à chaque distance parcourue par rame, égale au pas de la roue phonique.

PVS = Signal à niveau validé quand la rame est présente dans une station ordinaire.

V_R = Valeur courante de la vitesse réelle de la rame, mesurée directement par une génératrice tachymétrique.

V_t = Vitesse de télécommande envoyée par le P.C.C. en cas d'incident.

E = Signal à niveau envoyé par l'asservissement de vitesse quand $V_R \leqslant 1{,}3$m/s

PVF = Signal à niveau validé par le système-portes quand les portes sont fermé

PVO = Signal à niveau validé par le système-portes quand les portes sont ouver

COP = Signal impulsionnel de commande d'ouverture des portes du véhicule.

CFP = Signal impulsionnel de commande de fermeture des portes du véhicule.

DRR = Signal impulsionnel émis lorsque la rame démarre au départ d'une station

GONG = Signal impulsionnel prévenant les voyageurs de la fermeture imminente des portes.

ARTO = Signal impulsionnel émis pour demander au P.C.C. l'arrêt de l'émission d'horloge.

RETO = Signal impulsionnel de demande de reprise de l'émission des signaux d'horloge.

Ve = Valeur courante de la vitesse de régulation

V_L = Valeur courante de la vitesse limite

CA = Dernière valeur modifiée de CA

Vcs = Valeur courante de la vitesse de consigne de sécurité

ARTER = Signal à niveau validé quand la rame est présente dans la station termina

RAPPEL DE NOMENCLATURE (Suite)

e = Valeur booléenne égale à 1 si $Vcs - V_R > 0$, égale à 0 si $Vcs - V_R \leq 0$.

Vc = Valeur courante de la vitesse de commande

FU1 = Signal à niveau envoyé vers les freins d'urgence

FU2 = " " " " " anti-survitesse

FU3 = " " " " " d'arrêt en station

VFU1 = " " " par le système - freins d'urgence -

VFU2 = " " " " " - freins anti-survitesse -

VFU3 = " " " " " - freins d'arrêt en station -

DFU1 = " " " vers les freins d'urgence pour défreinage

DFU2 = " " " " " anti-survitesse pour défreinage

DFU3 = " " " " " d'arrêt en station pour défreinage

VDFU1 = " " " par le système - freins d'urgence -

VDFU2 = " " " " " " " anti-survitesse

VDFU3 = " " " " " " " d'arrêt en station.

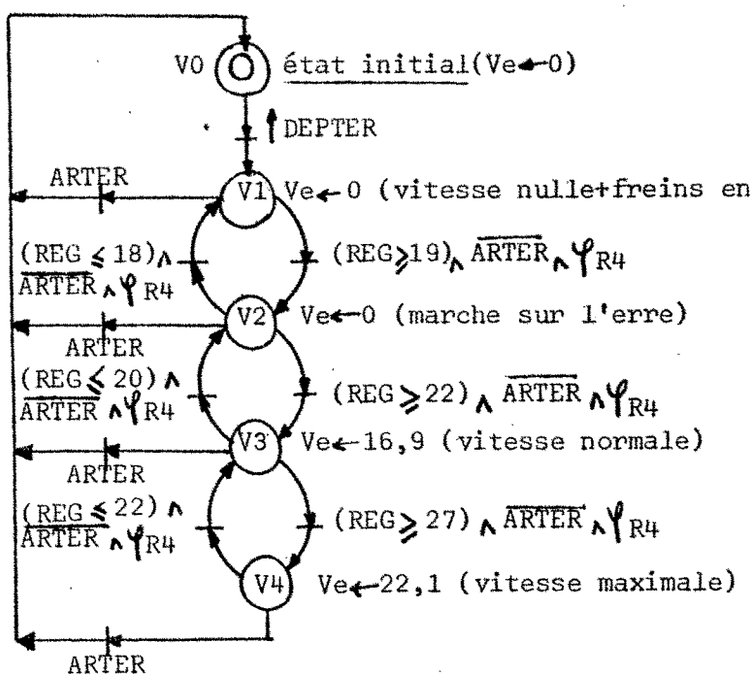
E.1) Représentation de la fonction de calcul de la vitesse de régulation \

Cette fonction a été décrite au paragraphe (B.1) du chapitre I.

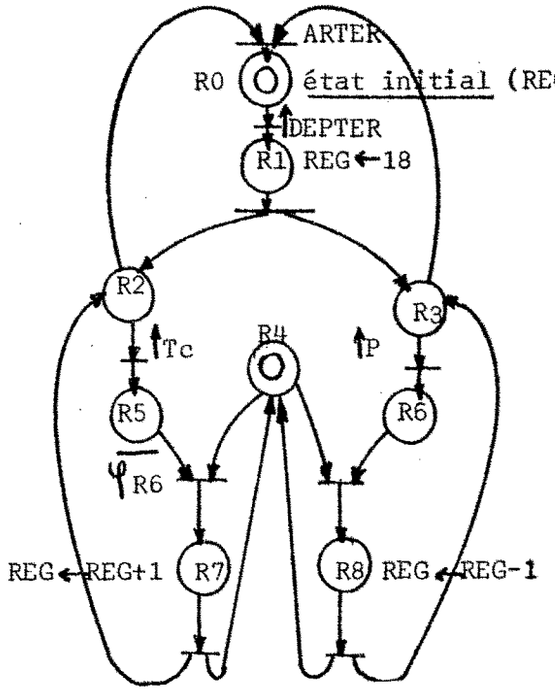
Elle est modélisée par les Grafcets (G1) et (G2) (Fig.1).

Entrées : ↑DEPTER ; ARTER ; ↑P; ↑T_c ; $\overline{\text{ARTER}}$;

Sortie : V_e



GRAFCET (G1)



GRAFCET (G2)

Fig.1

Commentaires :

Dans le GRAFCET (G1)

1 - Quand le signal ARTER est validé, l'une des étapes V_1, V_2, V_3 ou V_4 est active. Le retour à l'état initial doit donc pouvoir se faire à partir de chacune de ces étapes en la désactivant.

2 - Dans les réceptivités associées aux transitions entre les étapes V_1, V_2, V_3, V_4, nous avons ajouté les conditions suivantes :

. $\overline{\text{ARTER}}$ pour donner la priorité aux autres transitions issues de ces étapes, et dont la réceptivité porte sur la condition ARTER.

. $\Psi R4$, test d'activité de l'étape R_4 dans le GRAFCET (G2), pour attirer l'attention sur le fait que le test de la variable REG n'est autorisé que si la variable a une valeur stable (c'est-à-dire qu'elle n'est pas en cours de modification).

Dans le GRAFCET (G2)

1 - Quand le signal ARTER est validé, les étapes R2, R3 et R4 sont actives ; le retour à l'état initial se fait par la désactivation des étapes R2 et R3

2 - La simultanéité des évènements $\uparrow T_c$ et $\uparrow P$ ne peut pas exister. Toutefois, la variable REG pourrait être incrémentée et décrémentée à la fois : Aussi, l'étape R4 joue le rôle de ressource commune rendant exclusives les activations des étapes R7 et R8.

3 - Dans l'interprétation du GRAFCET (G2), en régime permanent, le seul marquage stable est (R2, R4, R3). Cela assure que l'on sera toujours réceptif aux évènements $\uparrow$Tc et $\uparrow$P, et donc qu'aucun de ces évènements ne sera per Dans la réalisation pratique, il faudra s'assurer que cela reste vérifié. Les durées des tâches de R7 et R8 devront être telles que l'on s'assure d'être toujours en R2 lorsque $\uparrow$Tc arrive, et en R3 lorsque $\uparrow$P arrive.

Deux indications importantes à cet effet sont les fréquences maximales instantanées des évènements ↑Tc et ↑P.

La fréquence de ↑Tc est inférieure ou égale à 1 Hz .

La fréquence maximale de ↑P est plus délicate à établir : A la vitesse de programme Vp, la fréquence des plots est de 1Hz . En un point x du diagramme Vitesse- Espace, la fréquence maximale de ↑P est :

$$f_{\uparrow P}(x) = \text{Max} \left\{ \frac{V_L(x),\ V_{cs}(x)}{Vp\ (x)} \right\}$$

La fréquence maximale instantanée de ↑P s'obtient donc en recherchant le maximum de cette quantité sur le diagramme de la ligne.

$$f_{\uparrow P\ \text{Max}} = \underset{(x)}{\text{Max}} \left(f_{\uparrow P}(x) \right)$$

E.2.) Représentation de la fonction de calcul de la vitesse limite V_L

Cette fonction a été décrite au paragraphe (B.3) du chapitre I. Elle est modélisée par les GRAFCETS (G3), (G4) et (G5) (Fig. 2).

Entrées : ↑DEPTER, ARTER, ↓P, ↑RP, ↑DRR, P, $\overline{P}$, ↑P

Sorties : CA, V_L

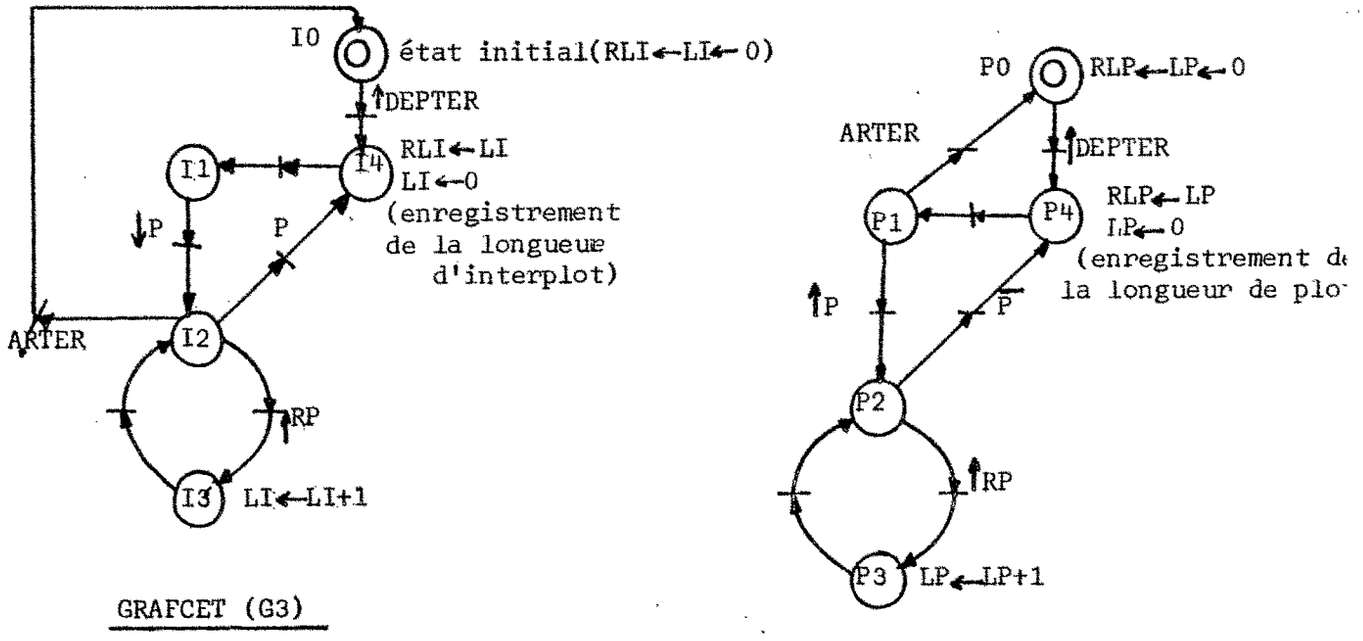
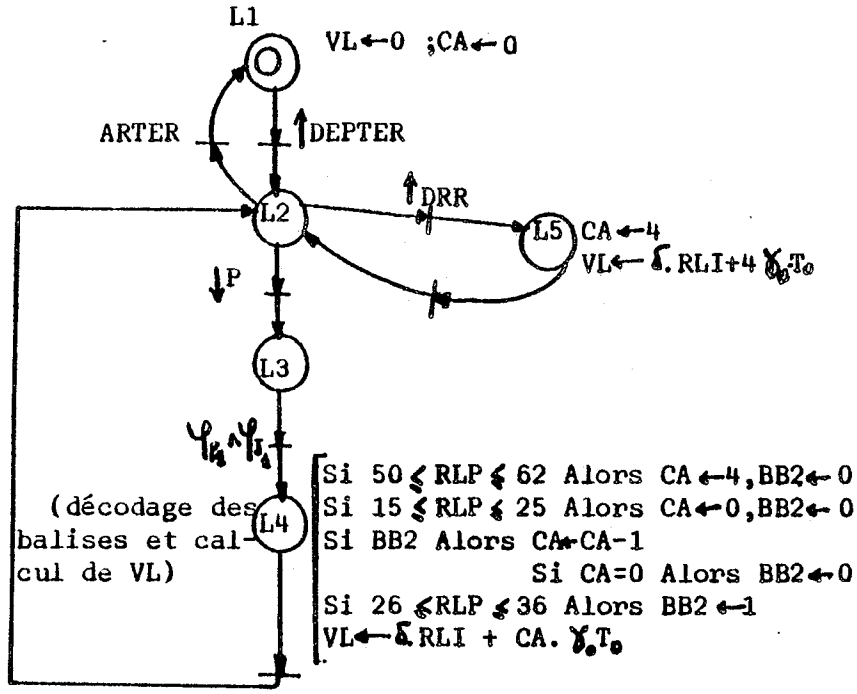


Fig.2



GRAFCET(G5)

Fig.2 (suite)

Commentaires :

Dans le GRAFCET (G3) :

1 - Quand le signal ARTER est validé , l'étape I_2 est active : Le retour à l'état initial doit donc se faire à partir de cette étape en la désactivant.

2 - L'introduction de l'étape I_2 entre les étapes I_2 et I_4 n'est pas indispensable ; cependant, elle nous permet de nous assurer qu'à l'occurrence de l'évènement ↓P, les variables RLI et LI ont des valeurs stables (étape I_4 désactivée).

3 - Ce GRAFCET impose que, dès que P↓ est arrivé et en l'absence de ARTER ou P, tous les évènements ↑RP doivent être pris en compte. Autrement dit, la durée de la tâche de l'étape I_3, devra être telle que l'on soit sûr d'être en I_2 lorsque ↑RP arrive.

Dans le GRAFCET (G4)

1 - Quand le signal ARTER est validé, l'étape P_1 est active : le retour à l'état initial doit donc se faire à partir de cette étape en la désactivant.

2 - L'introduction de l'étape P_1 permet de nous assurer qu'à l'occurrence de l'évènement $\uparrow P$, les variables RLP et LP ont des valeurs stables.

3 - Le GRAFCET (G4) impose que, dès que $\uparrow P$ arrive et en l'absence de P, tous les évènements $\uparrow RP$ doivent être pris en compte (c'est-à-dire que la durée de la tâche de l'étape P_3 doit être telle que l'on soit sûr dans une réalisation pratique d'être en P_2 lorsque $\uparrow RP$ arrive).

Dans les cas 3) et 3'), une indication importante est donnée par la fréquence maximale instantanée de $\uparrow RP$.

On rappelle que le signal $\uparrow RP$ est émis par la roue phonique chaque fois qu'une nouvelle distance égale au pas δ de la roue phonique est parcourue.

La fréquence maximale instantanée ($f_{\uparrow RP\,max}$) s'obtient en fonction de la vitesse maximale de la rame, soit :

$$f_{\uparrow RP}{}^{max} = \frac{V\ max}{\delta}$$

Dans le GRAFCET (G5)

1- Quand le signal ARTER est validé, l'étape L2 est active : Le retour à l'état initial doit donc se faire à partir de cette étape en la désactivant.

2- La valeur de V_L dépend de RLI et de CA. Une modification simultanée de ces variables donnerait un résultat erroné de V_L ; aussi, on conviendra de calculer V_L à l'occurrence de l'évènement $\downarrow P$.

3 - L'introduction de la réceptivité $\varphi_{P1} \wedge \varphi_{I1}$ dans la transition issue de l'étape L3 nous permet de nous assurer que le calcul de V_L (étape L_4 active) ne peut être effectué que si les conditions φ_{p1} et φ_{I1} sont toutes deux vérifiées, c'est-à-dire, d'après les remarques précédentes, lorsque les variables RLI et RLP ont des valeurs stables.

4 - BB_2 est une variable qui est positionnée à 1 pour mémoriser le fait que la dernière balise rencontrée est une balise de type B_2.

5 - Dans le GRAFCET (G5), le <u>seul marquage stable est</u> $\{L_2\}$:
Cela assure que l'on est réceptif à $\downarrow P$ et qu'aucun évènement $\downarrow P$ ne sera perdu. Dans la réalisation pratique, on s'assurera que cela reste vérifié (la durée de la tâche associée à l'étape L3 doit être telle que l'on soit toujours en L2 lorsque $\downarrow P$ arrive, et cela correspond à la détermination de $f_{\downarrow p}{}^{max}$).

E.3) <u>Représentation de la fonction de calcul de la vitesse de consigne de sécurité V_{cs}</u>

Cette fonction a été décrite au paragraphe (B.4) du chapitre I .Elle est modélisée par les GRAFCETS (G3), (G4) et (G6) (Fig. 3).

Entrées : ↑DEPTER, ARTER, P, ↑RP, V_R, E, V_L, CA, $\overline{P}$, ↓P

Sorties : e, Vcs

Les GRAFCETS (G3) et (G4) représentant respectivement les fonctions de calcul de la longueur d'interplot et de la longueur de plot ont déjà été étudiés (fig 2).

Le GRAFCET (G6) est représenté ci-dessous (fig 3).

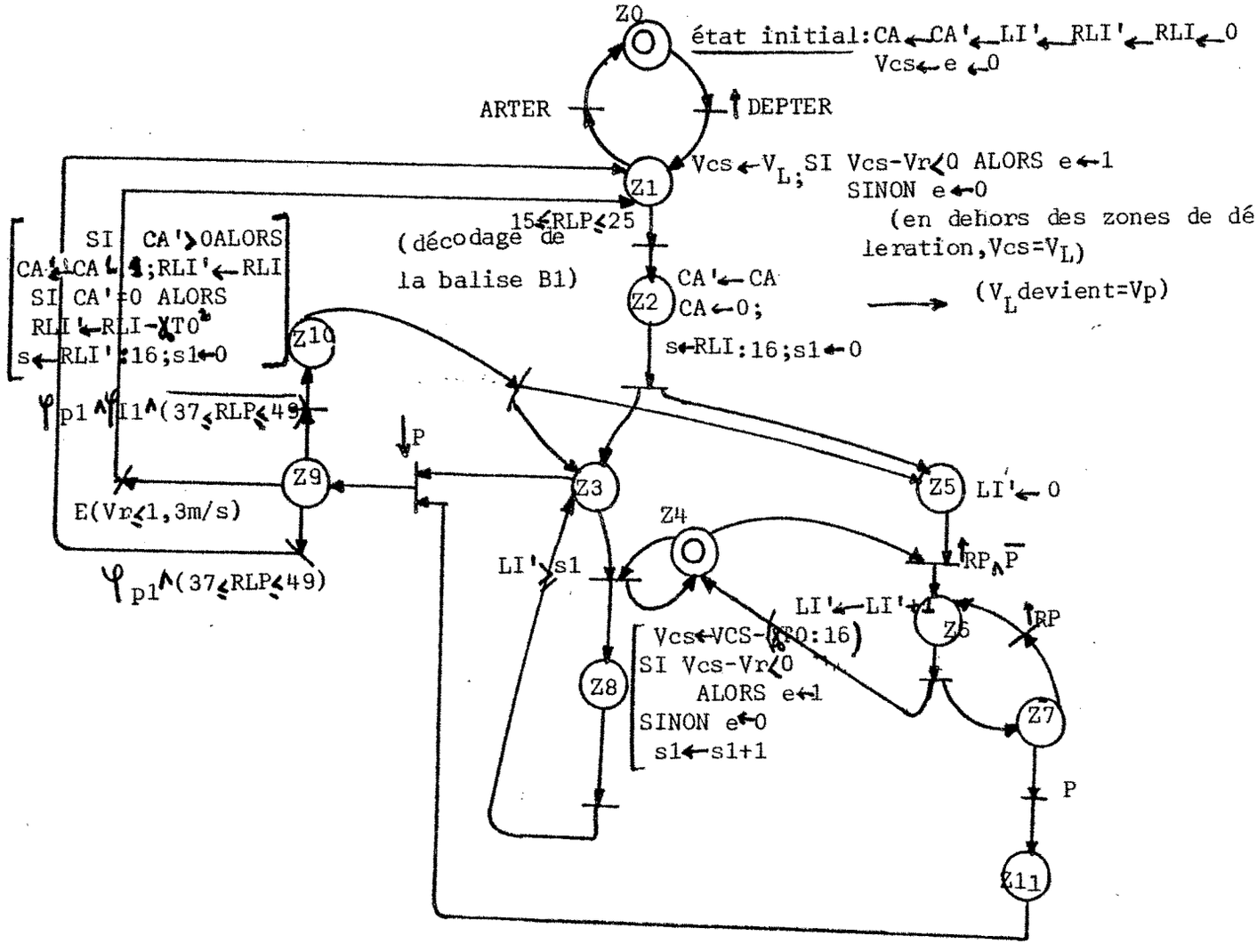


Fig.3 GRAFCET (G6)

Commentaires :

1 - D'après le modèle, on voit bien que Vcs est calculée à chaque nouvelle section mesurée

2 - L'introduction de l'étape S_4 indique que LI' n'est testée que lorsque LI' a une valeur stable (modification de LI' lors de l'activation de l'étape S_6)

3 - Quand le signal ARTER est validé, l'étape S_1 est active : le retour à l'état initial doit donc se faire à partir de cette étape en la désactivant.

4 - Dans les réceptivités associées aux transitions entre les étapes Z 9 et Z 10 et entre $^{Z}9$ et $^{Z}1$, nous avons ajouté respectivement les conditions $\varphi_{p1} \wedge \varphi_{I}$ et φ_{P1} pour montrer que les valeurs de RLI et de RLP doivent être stables afin qu'elles puissent être lues (lecture de RLI dans l'exécution de la tâche de l'étape Z 10, lecture de RLP dans les tests).

5 - On pourrait étudier de la même manière qu'on l'a fait pour les autres grafcets les contraintes imposées aux durées de certaines tâches, mais cela sera repris plus en détail ultérieurement (chapitre V).

6 - Comme il est impossible que les étapes Z 10 et Z 2 soient actives simultanément, il ne peut y avoir de simultaneité de lecture et écriture de la variable CA'.

E.4) Représentation de la fonction : Contrôle de l'arrêt d'horloge

Cette fonction a été décrite au paragraphe (B.2) du chapitre I. Elle est modélisée par les GRAFCETS (G2) et (G 9).

Le GRAFCET (G2) représentant le calcul du REG a déjà été étudié (fig 1

Le GRAFCET (G9) est représenté ci-dessous (fig. 4)

Entrées : ↑DEPTER, ARTER, ↑Tc, $\overline{\text{ARTER}}$, ↑P

Sorties : ARTO *, RETO *,

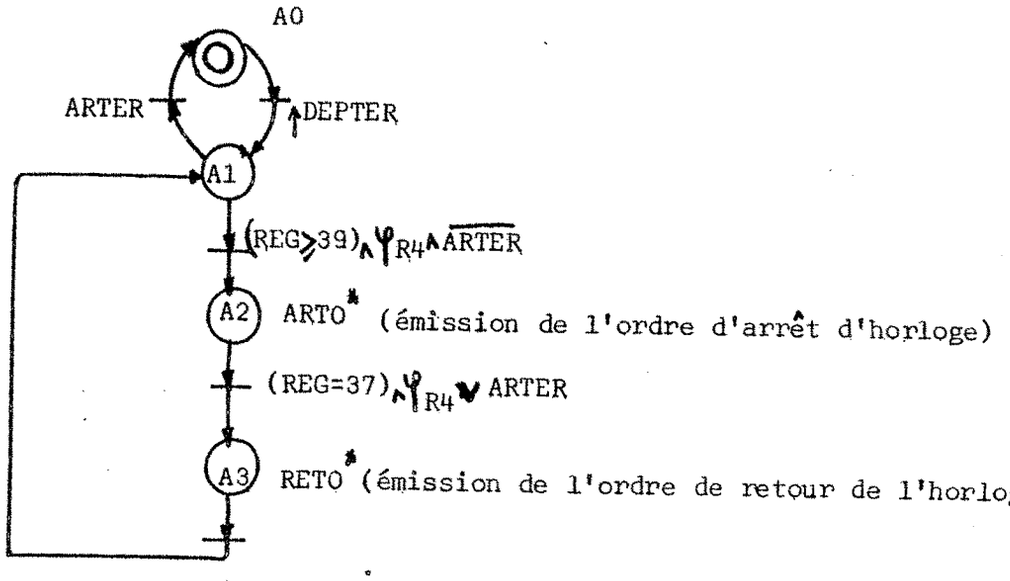


Fig.4 GRAFCET(G9)

Commentaires :

1 - Quand le signal ARTER est validé, l'une des étapes A1 ou A2 est active : le retour à l'état initial doit donc se faire à partir de chacune de ces étapes en la désactivant.

2 - Dans les réceptivités associées aux transitions issues des étapes A1 et A2, nous avons ajouté les conditions :

* $\overline{\text{ARTER}}$ pour donner la priorité aux autres transitions issues de ces étapes et dont la réceptivité porte sur la condition ARTER.

* Ψ R4 (test d'activité de l'étape R4 dans le Grafcet G2) pour montrer que le test sur la variable REG n'est autorisé que si la variable a une valeur stable (c'est-à-dire n'est pas en cours de modification).

3 - L'étude du modèle nous amène à étudier certains problèmes :

D'après la description faite au paragraphe (I.B.2) du chapitre I en ce qui concerne l'hystérésis utilisée pour le contrôle des arrêts d'horloge et dont nous rappelons le schéma de fonctionnement ci-dessous (fig. 5).

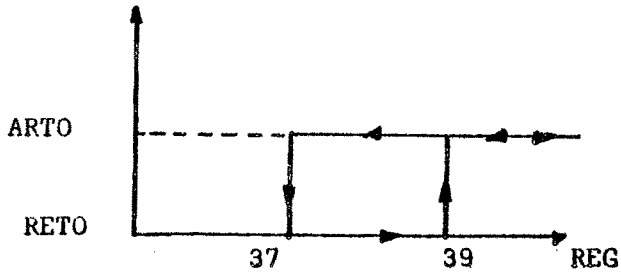


Fig.5

Le GRAFCET (G9) représente bien ce fonctionnement.

Cependant, un problème se pose au niveau du P.C.C. pour la gestion de l'horloge Tc.

Considérons en effet les configurations possibles suivantes des deux rames A et B, supposées en retard (fig. 6)

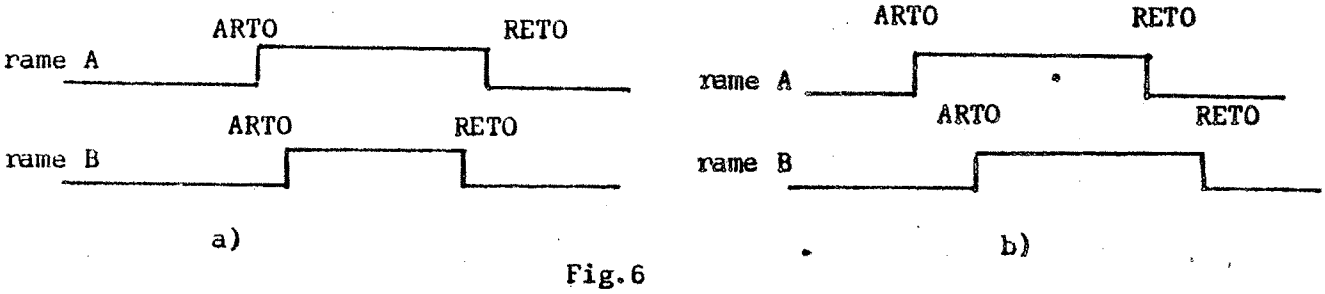


Fig.6

On voit que dans les cas a) et b), il peut arriver qu'une rame envoie l'ordre de retour d'horloge RETO, alors que l'autre rame qui avait déjà lancé l'ordre d'arrêt d'horloge ARTo n'a pas encore rattrapé une partie de son retard.

Il est évident que la rame qui a lancé l'ordre ARTO doit pouvoir être sûre que cet ordre sera maintenu tant que la valeur de son REG ne sera pas redevenue égale à 37, avant de relancer l'ordre RETO. Or, le signal ARTO est un signal impulsionnel.

Une solution est possible :

Pouvoir mémoriser l'ordre ARTO au P.C.C.

Dans ce cas, nous proposons la solution suivante :

On munit le P.C.C. d'un compteur COMP tel que :

il est initialisé à 0

Si ARTO reçu alors* $COMP \leftarrow COMP + 1$

*Si RETO * reçu alors* $COMP \leftarrow COMP - 1$

Si $COMP > 0$ *alors "Pas d'émission d'horloge".*

E.5) Représentation de la fonction = contrôle des mécanismes de freins

Cette fonction a été introduite implicitement lors de l'étude des fonctions de régulation (freins d'urgence), de calcul de la vitesse de consigne de sécurité (freins anti-survitesse), et de la procédure d'arrêt en station (freins d'arr en station).

Remarque :

La distinction entre 3 commandes de freins a été rendue nécessaire pour des raisons de sécurité : cela sera rappelé lors de l'analyse de la sécurité du système (chapitre VI).

5.1) Le contrôle des mécanisme de freins d'urgence est représenté par le GRAFCET (G'7) (fig. 7) et le GRAFCET (G2) qui a été étudié précédemment (fig1).

Entrées : ↑DEPTER, ARTER, VFU1, VDFU1, $\overline{\text{ARTER}}$, ↑P, ↑TC

Sorties : VFU1, DFU1

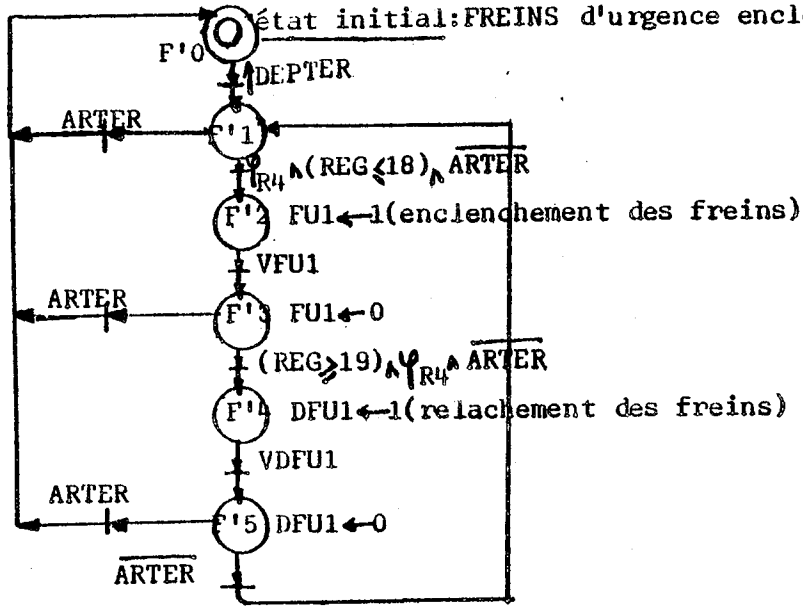


Fig.7

GRAFCET(G'7)

★ Quand le signal ARTER est validé, l'une des étapes F'1, F'3, ou F'5 est active. Le retour à l'état initial doit donc se faire à partir de chacune de ces étapes en la désactivant.

★ Les conditions $\overline{\text{ARTER}}$ et ↑R4 ont été ajoutées à certaines réceptivités pour les mêmes raisons vues dans l'étude du Grafcet (G1) (priorité, stabilité de valeur).

5.2) Le contrôle des mécanismes des freins pour l'anti-survitesse est représenté par le Grafcet (G7)(Fig. 8) et le Grafcet (G2).

Entrées : ↑DEPTER, ARTER, e, VFU2, ↓DFU2, ↑TC, ↑P, $\overline{\text{ARTER}}$

Sorties : FU2, DFU2

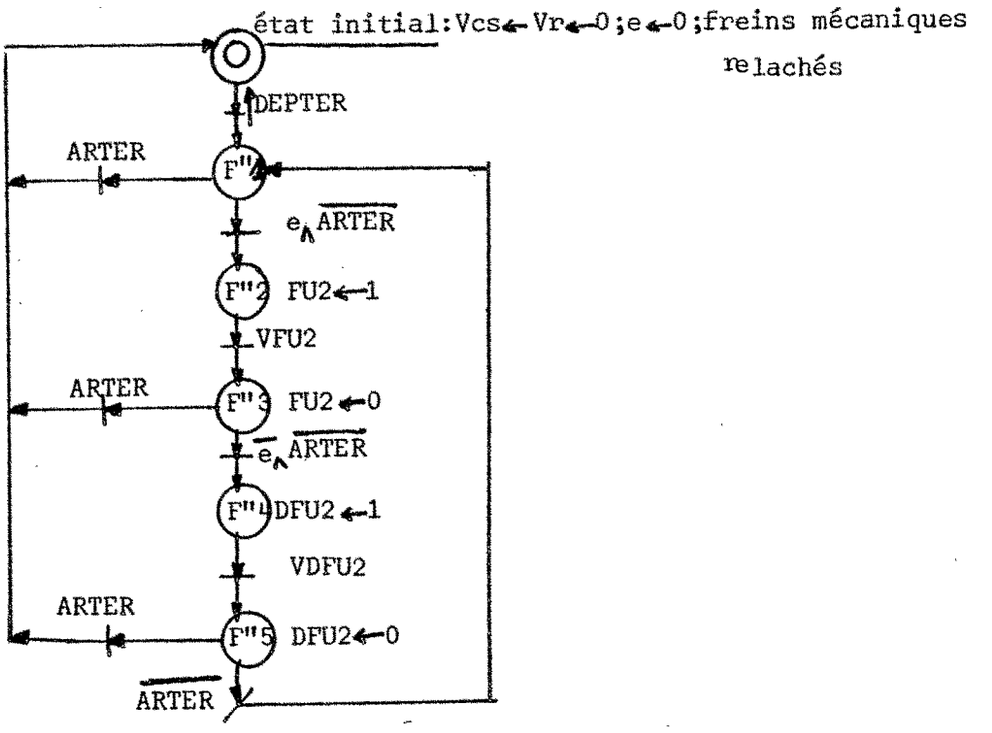


Fig.8 GRAFCET (G"7)

- Quand le signal ARTER est validé, l'une des étapes F"1, F"3 ou F"5 est active. Le retour à l'état initial doit donc se faire à partir de chacune de ces étapes en la désactivant.
- Pour les conditions ↓R4 et $\overline{\text{ARTER}}$, on a les mêmes commentaires que dans le cas précédent.

5.3) Le contrôle des mécanismes des freins d'arrêt en station est représenté par le Grafcet (G"'7) (Fig.9).

Entrées : PVS, ARTER, ↑DEPTER, E, VFU3, PVF, VDFU3

Sorties : FU3, DFU3

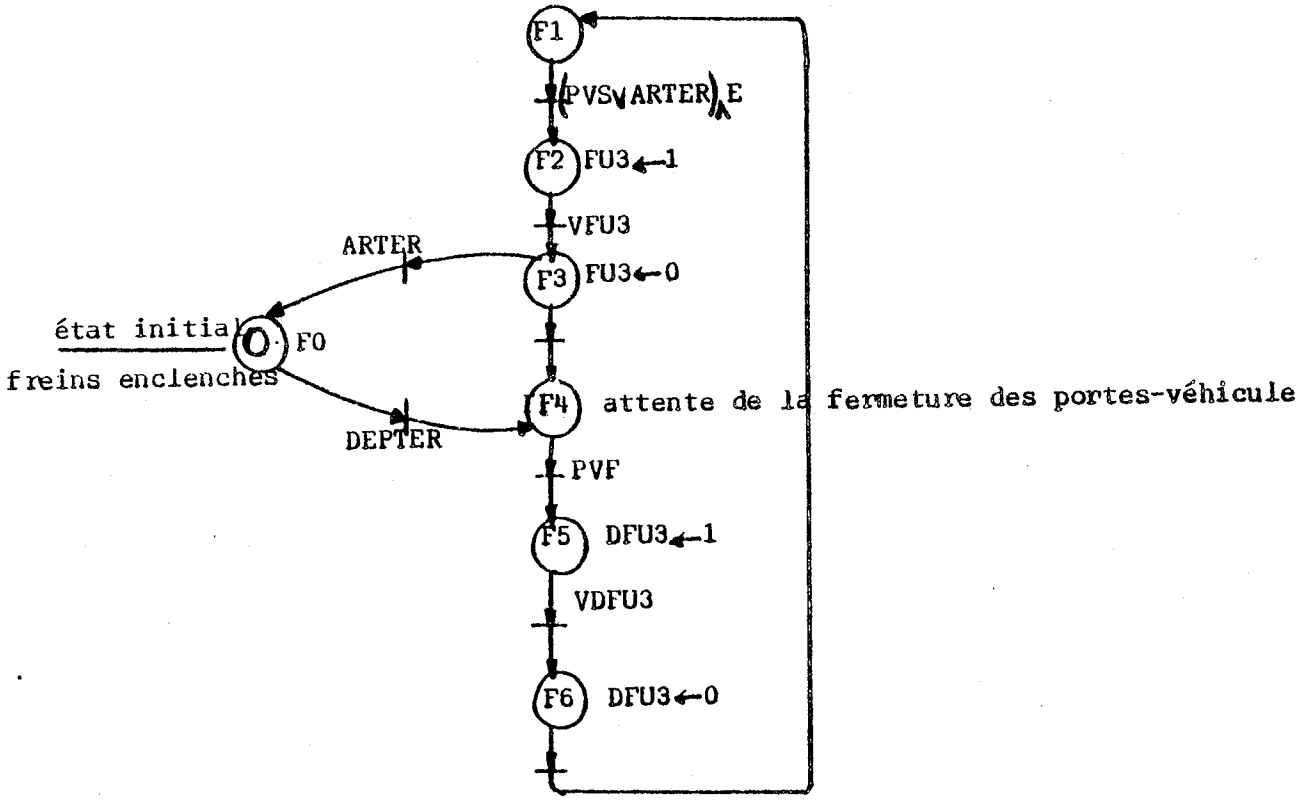


Fig.9 GRAFCET (G"'7)

Remarques :

* Quand le signal ARTER est validé, c'est l'étape F3 qui est active ;
  En effet, le freinage d'arrêt en station a été effectué.
* A l'état de repos, les portes du véhicule sont ouvertes en station terminale ; dès l'émission de ↑DEPTER, l'étape F_4 devient active : attente de fermeture des portes.

E.6) Représentation de la fonction : automatisation du stationnement d'une rame dans une station

Cette fonction a été décrite au paragraphe (B.5.3) du chapitre I et peut être modélisée par le Grafcet (G8) (Fig. 11).

Entrées : ↑DEPTER, ARTER, PVS, E, VFU3; ↑T'c, PVO, PVF, VDFU3

Sorties : COP*, CFP*, DRR*, GONG*

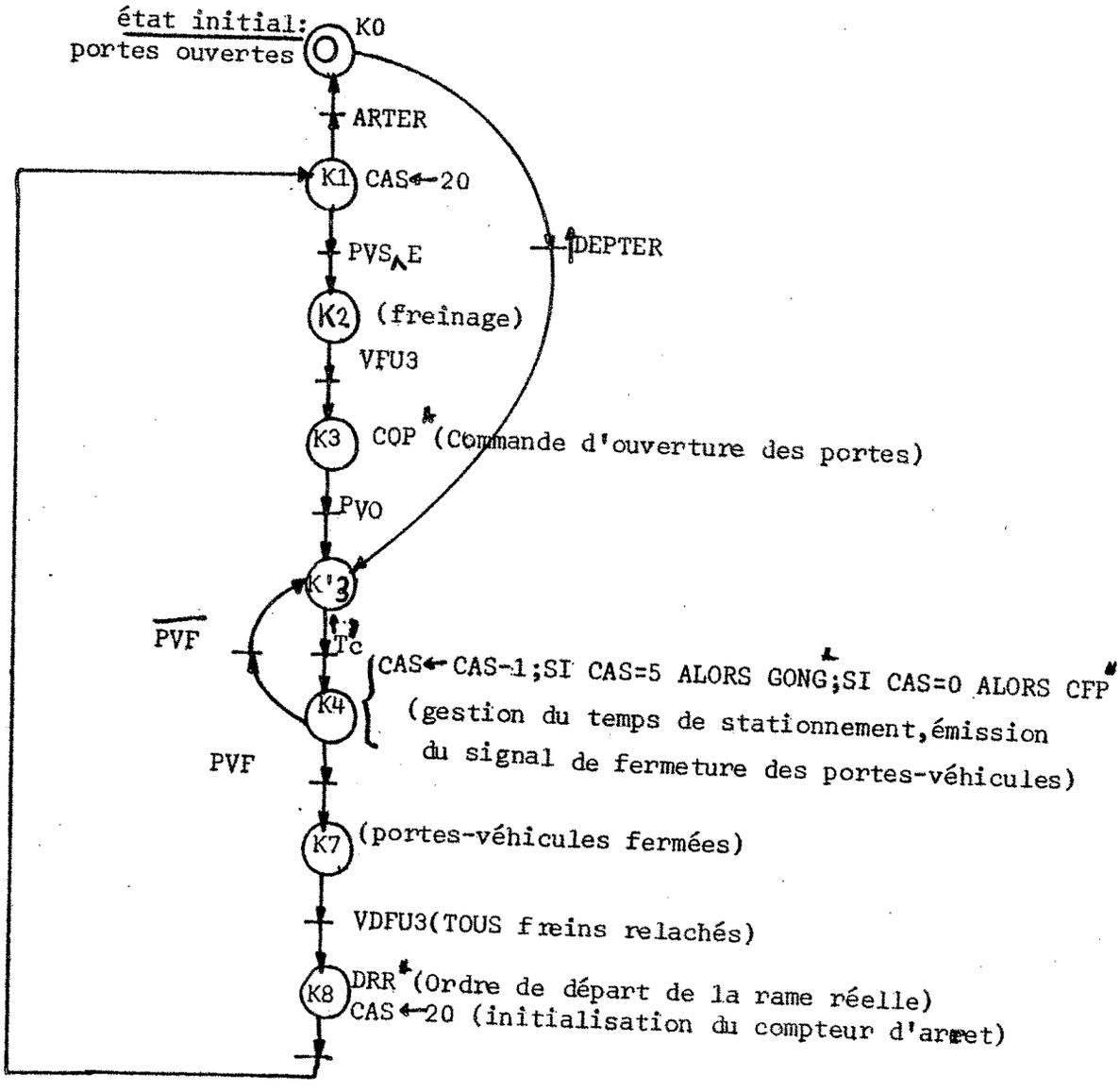


Fig.11 GRAFCET (G8)

Commentaires :

- Quand ARTER est validé, c'est l'étape K1 qui est active
- Dès émission de ↑DEPTER, c'est l'étape K'3 qui devient active : Initialisation de la séquence de stationnement, et de fermeture des portes.

E.7) Représentation de la fonction : Régulation en station

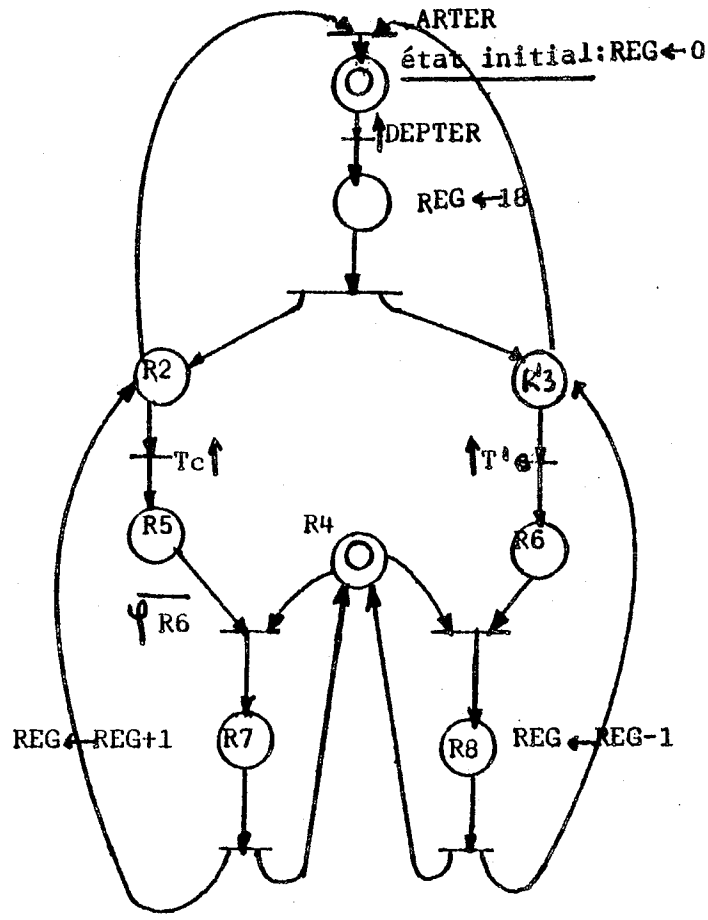
On a vu dans le paragraphe (B.5.4) du chapitre I que, pour la régulation en station, tout se passe comme si l'on décomptait des plots fictifs à la fréquence des impulsions d'horloge T'c.

Ceci peut être représenté par les Grafcets (G'2) et (G1) :

Le Grafcet (G1) a déjà été étudié ; le Grafcet (G'2) s'obtient en remplaçant dans (G2), l'évènement ↑P par ↑T'c. (Fig. 12)

Entrées : ↑Tc, ↑Tc', ↑DEPTER, ARTER, $\overline{\text{ARTER}}$

Sorties : Ve



E.8) Représentation de la fonction de calcul de la vitesse de commande V_c

Cette fonction peut être représentée simplement par le Grafcet (G10) (fig. 10).

Entrées : ↑DEPTER, ARTER, Ve, V_l, V_t

Sortie : Vc

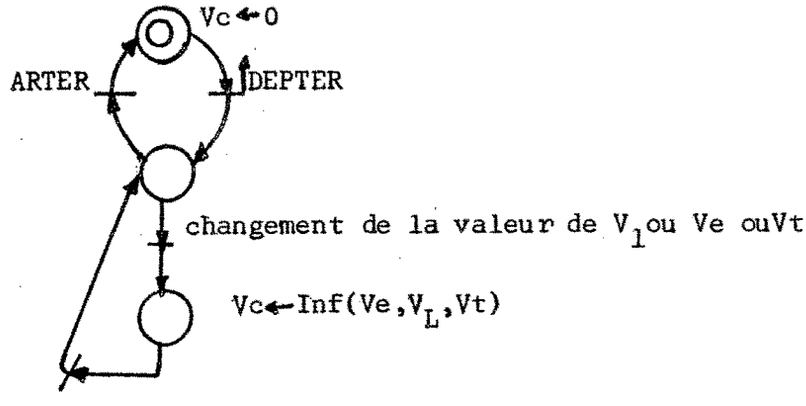


Fig.10
GRAFCET (G10)

Conclusion :

Nous avons montré dans cette partie comment on peut à partir d'une représentation par Grafcet décrire une fonction donnée, et l'analyser en détail.

Cela nous a permis de :

- mieux comprendre le système (clarté et simplicité de la représentation)
- compléter le Cahier des Charges par l'apport de précisions supplémentaires, notamment celles concernant :
  - ✱ les valeurs initiales des différentes variables
  - ✱ la manière dont sont calculées certaines variables
  - ✱ la nature des signaux (impulsion, niveau)
  - ✱ les échéances de début et de fin de chaque fonction et sous-fonction.

- résoudre pour chaque fonction étudiée des situations de conflit mises en évidence par une telle représentation (exclusion mutuelle, priorités, partage d'une même variable).

- relever certaines ambiguités dans les spécifications de certaines fonctions, ou des insuffisances dues à la non spécification de l'Environnement.

- Préciser l'ensemble des états stables dans lequel doit se trouver le système au cours de ses évolutions vis-à-vis de l'Environnement extérieur : de tels états stables doivent être respectés dans une réalisation pratique.

CHAPITRE IV

CONCEPTION DU MODELE FONCTIONNEL DU PILOTE AUTOMATIQUE

CONSTRUCTION DU MODELE FONCTIONNEL

Dans le chapitre III, nous avons étudié endétail toutes les fonctions réalisant les différents objectifs du système. Cela nous avait permis de compléter certaines spécifications du Cahier des Charges; cependant, la représentation sous forme de grafcets "séparés" ne permettait pas de mettre en évidence d'éventuelles situations de conflit, ambiguités ou incohérences dans les spécifications au niveau du fonctionnement global du système, parce que les interactions entre les différentes parties du système ne sont pas représentées.

Nous nous proposons dans cette partie de construire un modèle décrivant le fonctionnement général du système où toutes les formes de dépendance ou de parallélisme seront mises en valeur. Ce modèle doit être clair et aussi simple que possible afin qu'il puisse facilement être validé (analyse qualitative et quantitative).

D'après la représentation par grafcets du Cahier des Charges, on peut notamment remarquer que :

* certaines sous-fonctions du système apparaissent dans différents grafcets : cette redondance peut être utile lorsqu'il s'agit d'isoler des fonctions pour des raisons de sécurité.
  Néanmoins dans un premier temps, nous chercherons à identifier ces sous-fonctions et à les fusionner afin d'obtenir un modèle fonctionnel minimal.

* qu'il existe des dépendances entre les grafcets, dues notamment à l'utilisation de variables communes, à la réceptivité à des états ou communs d'activité d'étapes ou à des évènements externes communs.

Aussi, la construction du modèle consistera à relier les variables communes entre elles d'une manière adéquate, à supprimer les différents états d'activité de certaines étapes de grafcets, tout en respectant les contraintes imposées par l'analyse faite de ces grafcets.

On essaiera d'avoir un modèle décrivant, si possible un ordonnancement de tâches (qui peuvent par exemple être des sous-fonctions), en fonction des occurrences des différents évènements externes.

On procèdera selon les étapes suivantes :

Etape I :

Résumer sur un graphe les différentes relations entre les variables du système.

Etape II

Rechercher s'il est possible de fusionner certaines sous-fonctions afin de simplifier la représentation graphique de fonctions données, sans changer les spécifications fonctionnelles déjà établies.

Etape III

Etudier pour toutes les relations de dépendance les problèmes de synchronisation qui se posent : cette partie peut amener à établir de nouvelles spécifications, particulièrement en ce qui concerne les changements de valeurs prises par les différentes variables.

Etape IV

Mettre en valeur les différentes dépendances dues à la présence d'évènements externes communs à différents grafcets.

Dans une première étude, et dans un souci de clarté, nous étudierons un modèle représentant le fonctionnement du pilote automatique en ligne et dans une station ordinaire. Aussi, nous ferons abstraction des signaux ARTER et DEPTER lesquels interviennent uniquement dans l'activation de l'état initial du système et son retour à cet état initial (mises sous-tension et hors tension)

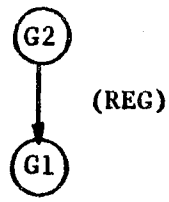
Etape I

Graphe de dépendance :

Le graphe de dépendance résume les différentes relations de dépendance existant entre les grafcets, dues à l'utilisation de variables communes, ou à la présence d'états d'activité relatifs à certaines étapes de ces grafcets.

Exemple :

* Dans le grafcet (G1), le calcul de V_e dépend de la variable REG; cette variable REG est calculée dans le grafcet (G2) : on dira alors que (G1) dépend de (G2), et on représentera cette relation de dépendance par :



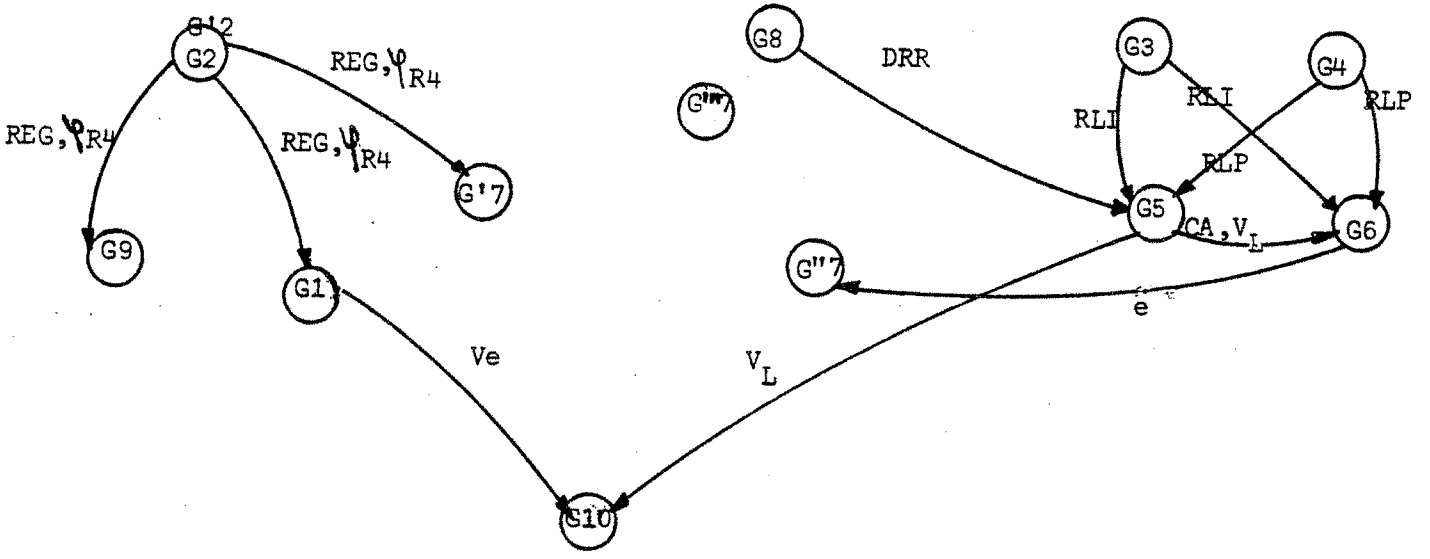
* Le test d'activité de l'étape R_4 (dans le grafcet G2) apparaît comme une condition associée aux réceptivités de certaines transitions dans le grafcet (G9):(G9) dépend alors de (G1), etc...

Les différentes relations de dépendance entre les différents grafcets représentant le système figurent sur le graphe de la figure 1 .

Etape II

On peut, d'ores et déjà, sur simple examen de ce graphe de dépendance, remarquer que les grafcets (G3), (G4) et (G6) ont plusieurs entrées et sorties communes, et qu'il serait intéressant d'essayer de les composer en un seul réseau.

1. Dans le paragraphe I.B.4.2.3, nous avons proposé la réalisation de la vitesse V_{cs} lissée à l'aide d'un compteur LI' (représentée dans le grafcet G6). On peut toutefois noter qu'on peut utiliser tout simplement le compteur LI : en effet, LI servant à la mesure de la longueur d'interplot, il suffira de lire la valeur de LI dernièrement modifiée, donc à chaque occurence de l'évènement RP, et de la comparer à celle de la valeur de la section d'interplot s préalablement calculée.



On rappelle que :

la fonction de calcul de V_e (Vitesse de régulation) est représentée par l'ensemble (G1, G2 ou G'2)

" " V_L (Vitesse limite) " " (G3, G4, G5)

" " V_{cs} (Vitesse de consigne de sécurité) " " (G3, G4, G6)

" " V_c (Vitesse de commande) " " (G10)

" des mécanismes de freins est représentée par " " (G2, G'7, G"7)

" d'arrêt d'horloge " " (G2, G9)

" d'automatisation du stationnement " " (G8)

FIG.1 - Graphe de dépendance

2_ Sur occurrence du signal P, les tâches suivantes doivent être exécutées :

a. [Enregistrement de la longueur d'interplot
Remise à 0 du compteur LI

b. [Calcul de la longueur de plot par incrémentation du compteur LP à chaque impulsion ↑RP

Les tâches a et b étant indépendantes, elles peuvent être exécutées en parallèle.

- Sur occurrence du signal $\bar{P}$, les tâches suivantes doivent être exécutées :

c. [Calcul de la longueur d'interplot par incrémentation du compteur LI à chaque impulsion ↑RP
Lecture de la valeur de LI, comparaison à s (d'après 1)
Modification de V_{cs}

d. [Enregistrement de la longueur de plot, et remise à 0 de LP
Lecture de RLP
Calcul de CA, en fonction de RLP
Lecture de CA', Modification de CA'
Calcul de V_L en fonction de RLI et CA
Calcul de RLI' et de s

Les tâches c et d étant indépendantes, elles peuvent être exécutées en parallèle.

L'ensemble des tâches a,b,c et d peut être décrit par le réseau suivant (fig.2).

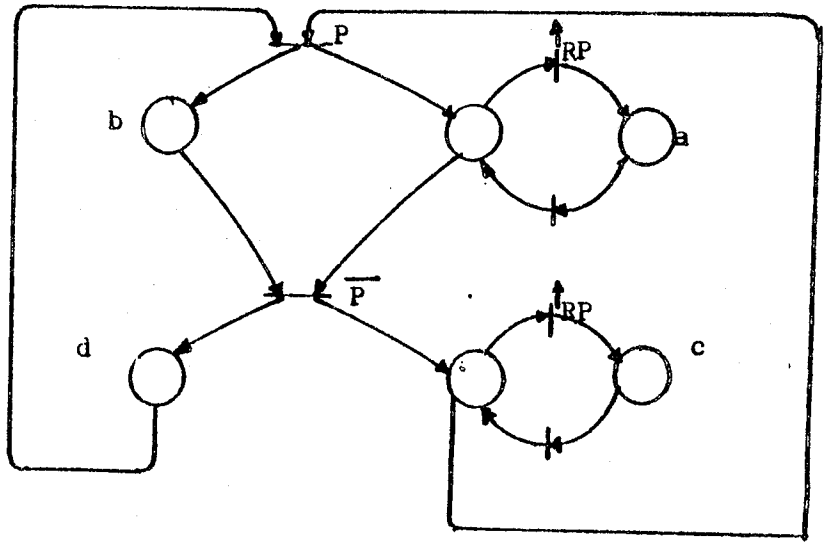


Fig.2

D'autre part, le calcul de V_{cs} ne doit se faire que pendant les phases de décél ration (entre les balises B1 et B3, et entre la balise B1 et l'arrivée en stat

Nous introduisons alors la variable X1 qui, positionnée à 1 indiquera que la dernière balise décodée était de type B1, et positionnée à 0 indiquera soit que la dernière balise détectée était de type B3, soit que la rame est arrivée en station.

D'après le réseau précédent (FIG.2), on note qu'on peut avoir une situation où la variable X1 est simultanément lue et écrite (présence simultanée de marques dans les places D et C.).

Pour éviter une telle situation, la solution la plus simple consiste à séquentialiser l'écriture de X1 et sa lecture, ce qui nous amène à proposer le modèle suivant :(FIG.3a) (Réseau $\mathfrak{R}$).

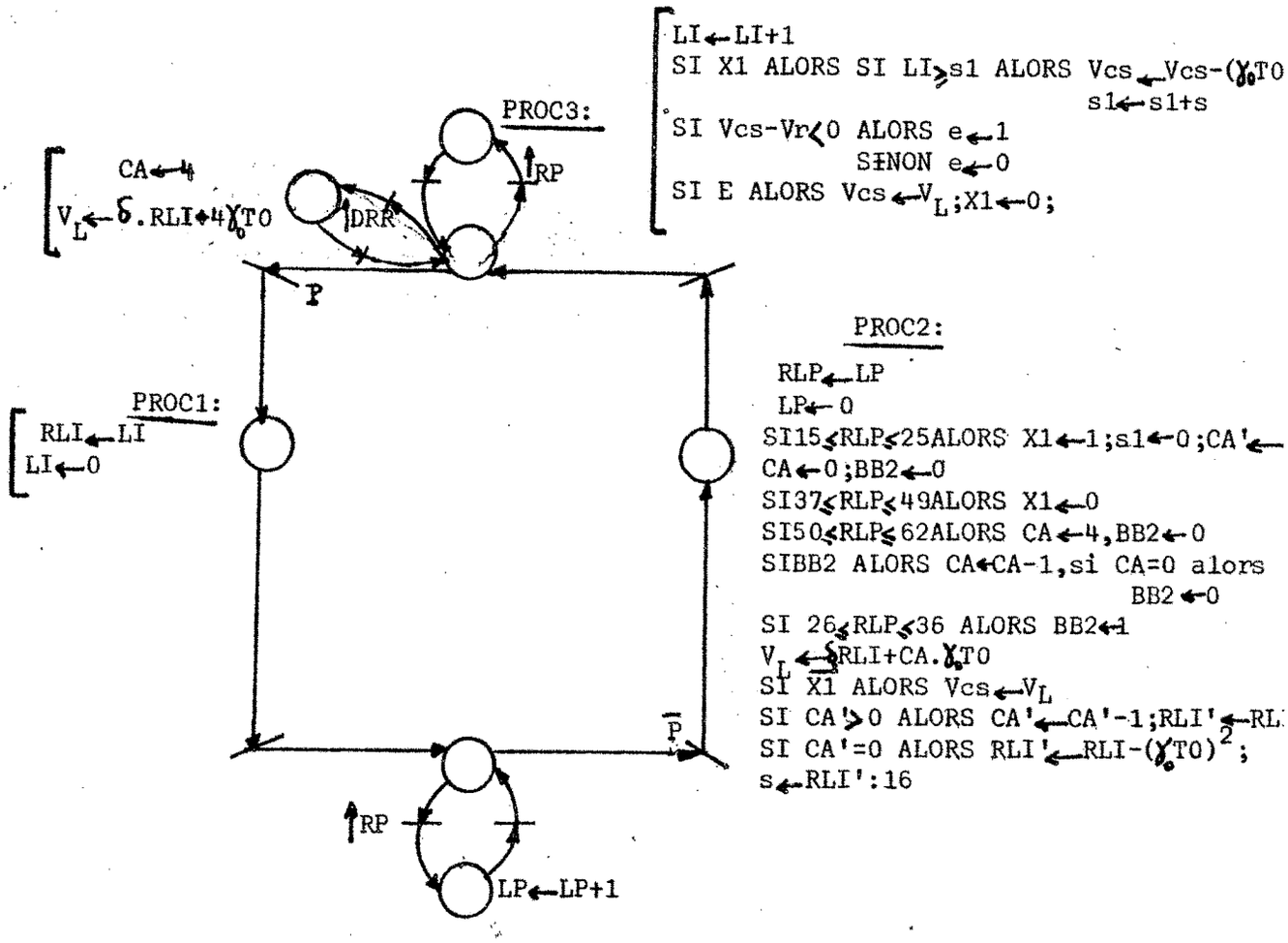


Fig.3_a Réseau $\mathfrak{R}$ (fusion des grafcets G3,G4,G5,G6)

Toutes les spécifications établies lors de l'analyse des grafcets G3, G4, G5 et G6 sont respectées, notamment :

- la séquentialité de lecture-Ecriture des différentes variables (LI, RLI, LP, RLP, CA, CA', V_L , V_{cs},...) : il n'existe pas de situation où une même variable est écrite et lue simultanément.

- Aucun évènement ne pouvant être perdu, ce modèle induit une contrainte qu'il faudra respecter lors d'une réalisation pratique :
  en effet, entre deux évènements ↑RP, on doit effectuer l'une des tâches suivantes :

  (LP←LP +1) et (PROC 2), ou (PROC3) et (PROC 1).

Toutefois, le réseau R qu'on vient de construire montre qu'on est seulement réceptif à l'évènement ↑RP.

Or, l'analyse qu'on a faite dans le chapitre précédent impose qu'on soit réceptif à ↓P, ↑P et ↑RP.

Aussi, nous proposons un modèle plus correct, où les évènements ↓P et ↑P sont mémorisés (fig.3b).

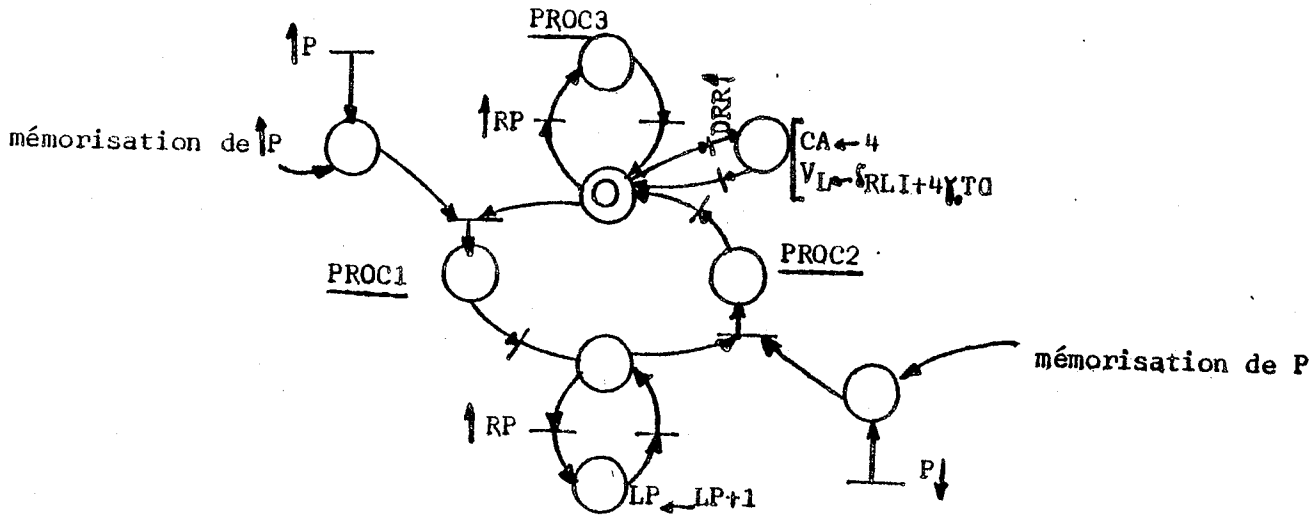


Fig .3b

REMARQUES :

* Dans la tâche PROC 3, E apparaît comme une condition et non comme évènement.

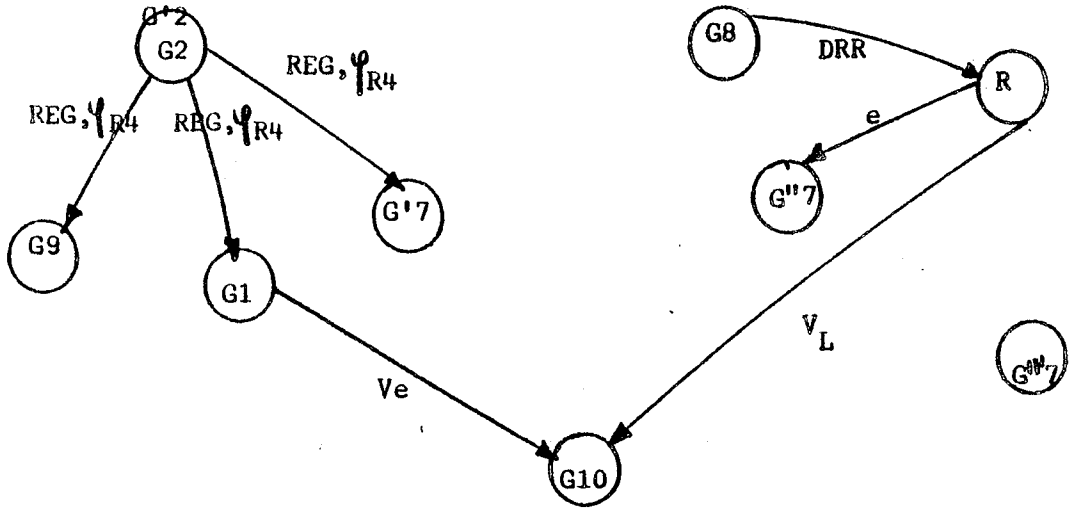
* Nous avons introduit dans le modèle l'initialisation de CA lors de l'émission du signal ↑DRR d'ordre de départ de la rame réelle d'une station ordinaire.

  Les signaux ↑DRR et ↑RP qui sont tous les deux impulsionnels ne peuvent pas arriver en même temps : lorsque ↑DRR est émis, la rame est à l'arrêt, et ↑RP n'existe pas.

* Dans la tâche PROC 3, le test sur $(V_{cs} - V_R)$ est effectué à chaque ↑RP, et cel quelle que soit la valeur de X1. Comme dans les zones d'accélération ou de palie la valeur courante de V_L est transférée dans V_{cs}, on effectue par la même un test sur $(V_L - V_R)$, ce qui constitue un moyen intéressant de surveillance anti-survitesse pour tout le fonctionnement en ligne.

Etape III

Le graphe de dépendance de la figure 1 devient :



Il s'agit maintenant de supprimer tous les états ψ utilisés dans les grafcets, en respectant les différentes contraintes imposées, et d'étudier les différents problèmes de synchronisation dûs surtout :

- à une lecture et une écriture simultanées d'une même variable
- à deux écritures simultanées d'une même variable.

La résolution de tels problèmes est étroitement liée à l'étude des spécifications concernant les différentes variables, et on est amené, si cela n'a pas été précisé dans le Cahier des Charges, à se poser la question suivante :

Quand telle variable doit - elle être modifiée ?

Une variable peut être modifiée de plusieurs manières, par exemple :

- périodiquement (toutes les x secondes)
- à l'occurrence d'un évènement donné
- chaque fois qu'une ou plusieurs variables sont modifiées.

L'analyse va être faite en détail pour toutes les relations de dépendance résumées dans le graphe de dépendance.

a) Etude de la relation (G2 ou G'2, G9)

Quand la fonction de contrôle de l'arrêt d'horloge doit elle être élaborée ?

D'après le grafcet (G9), on note que l'évolution d'un état à un autre dans (G9) dépend de la variable REG (stabilisation de la valeur de REG et test sur cette valeur); ceci nous amène à élaborer la fonction de contrôle de l'arrêt d'horloge chaque fois que REG est modifiée. Une telle spécification nous permet d'avoir une représentation explicite où la synchronisation entre les grafcets (G2) et (G9) est mise en évidence (Fig.4) :

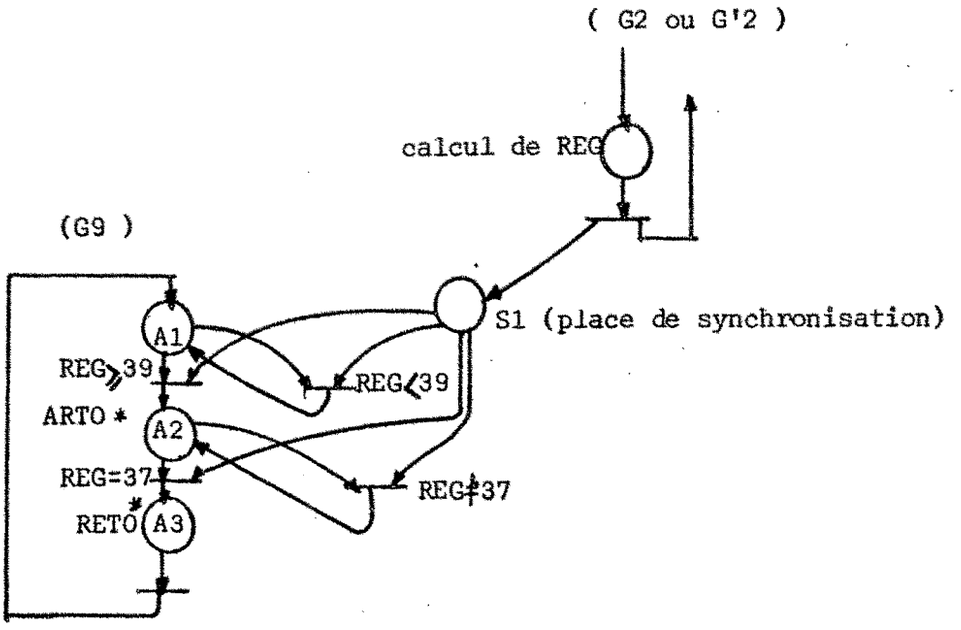
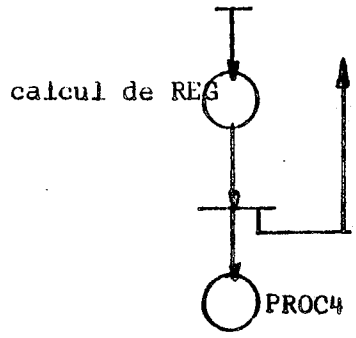


Fig.4

S1 est une place de synchronisation; chaque fois que la variable REG est calculée dans (G2), une marque est placée dans S1; la valeur de REG qui va être utilisée dans (G9) est certainement stable, on peut donc supprimer la condition φ_{R4}.
Par ailleurs, toute marque de S1 est immédiatement consommée, et cela quel que soit l'état où l'on se trouve dans le grafcet (G9).
On peut noter que dans le modèle précédent, il ne peut exister de situation de conflit (exclusivité des conditions).

Cette forme explicite peut par ailleurs être compactée : en effet, en introduisant les différents états pris par la fonction représentée par (G9), celle-ci peut être exprimée à l'aide d'un algorithme :

On notera par ETATA : = i l'état représenté par le marquage de la place A_i dans le grafcet (G9); on obtient :



avec : A l'état initial (mise sous tension), ETATA : = 1

PROC4 :

Si ETATA: = 1 ∧ REG ⩾ 39 Alors
ETATA: = 2
ARTO*

Si ETATAT: =2 ∧ REG ⩽ 37 Alors
RETO*
ETATA: = 1

Après chaque calcul de REG, la tâche PROC 4 est exécutée.
Toutefois, il faudra en outre s'assurer dans une réalisation pratique qu'une valeur de la variable REG venant d'être modifiée et stabilisée ne peut être utilisée que si le calcul de PROC.4, utilisant une valeur de REG précédemment calculée, est achevé. En d'autres termes, le Réseau doit être sauf.

b) Etude de la relation (G2 ou G'2, G1).

De la même manière, la fonction de calcul de la vitesse de régulation V_e, représentée par le grafcet (G1), doit être élaborée à chaque calcul de REG. Comme la fonction d'hystérésis décrivait toutes les évolutions possibles de V_e en fonction de la variable REG, on peut directement la traduire sous forme d'un algorithme, en notant par ETATV = i selon que l'une des places V_i dans le grafcet (G1), est marquée :

A l'état initial (mise sous tension), ETATV: = 1.

PROC.5:

Si ETATV: = 1 Alors $V_e \longrightarrow 0$

Si ETATV: = 1 $\wedge$ REG $\geqslant$ 19 Alors ETATV: = 2; $V_e \longleftarrow 0$

Si ETATV: = 2 $\wedge$ REG $\leqslant$ 18 Alors ETATV: = 1; $V_e \longleftarrow 0$

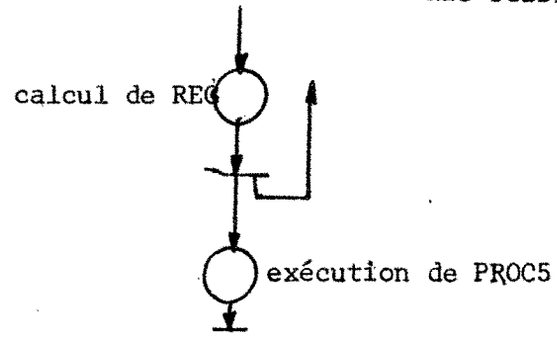
Si ETATV: = 2 $\wedge$ REG $\geqslant$ 22 Alors ETATV: = 3; $V_e \longleftarrow 16,9$

Si ETATV: = 3 $\wedge$ REG $\leqslant$ 20 Alors ETATV: = 2; $V_e \longleftarrow 0$

Si ETATV: = 3 $\wedge$ REG $\geqslant$ 27 Alors ETATV: = 4; $V_e \longleftarrow 22,1$

Si ETATV: = 4 $\wedge$ REG $\leqslant$ 22 Alors ETATV: = 3; $V_e \longleftarrow 16,9$

et on a la représentation en "pipe-line" suivante, qui induit d'ailleurs la suppression de la condition φ_{R4} (valeur c REG stable).



Comme dans le cas précédent, il faudra s'assurer, dans une réalisation pratique, que la place à laquelle est associée PROC 5 ne pourra posséder plus d'1 marque à la fois.

c) Etude de la relation (G2 ou G'2, G7) .

Dans les réceptivités associées aux transitions du grafcet (G'7), apparaissent soit des tests sur la variable REG, soit des états φ_{R4} d'activité relatifs à l'étape R_4, dans le grafcet (G2), soit des évènements externes (acquittements de freinage et de défreinage validés par le système "Freins") :

Reprenons la représentation du grafcet (G'7), décrivant le mécanisme de contrôle des freins d'urgence; pour simplifier le schéma, nous ne représentons pas les conditions φ_{R4} : leur suppression du modèle se fait comme dans les cas précédents (fig.5 a).

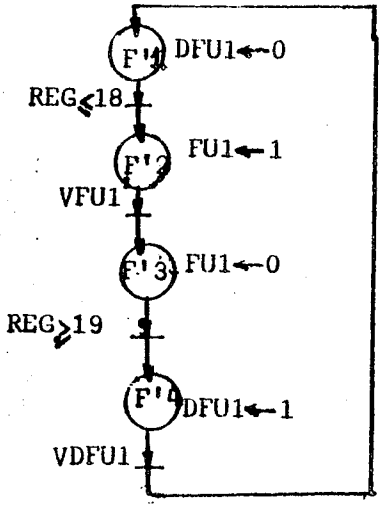


Fig.5a

a)Pour passer de l'Etat F'2 à l'état F'3, il faut attendre le signal VFU1 d'acquittement de freinage; or, entre l'instant où l'ordre de freinage est envoyé vers système-freins, et l'instant où l'acquittement est reçu il se passe un temps au moins égal au temps de réponse des freins d'urgence (de 1s à 1,5s).

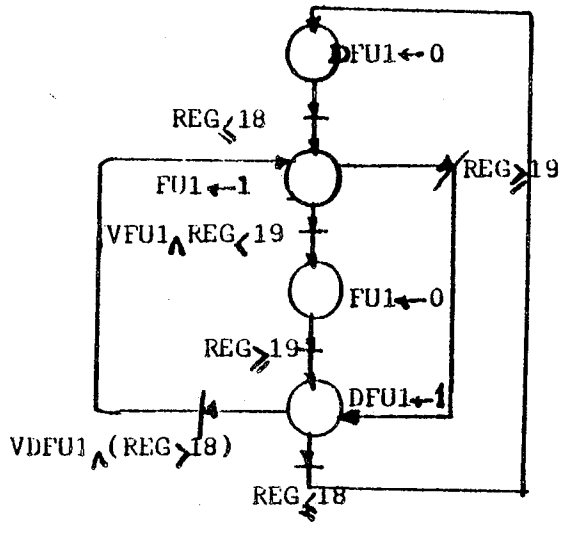
Pendant ce temps, la valeur de la variable REG peut avoir été modifiée. Deux cas se présentent alors :

* REG peut avoir augmenté (REG devient $\geq$19) : dans ce cas, il est inutile d'attendre VFU1; on donne directement l'ordre de défreinage (Etat F'_4).

* REG peut avoir diminué ou gardé son ancienne valeur : la commande de freinage est alors maintenue (état F'2).

b) Même raisonnement pour l'acquittement de défreinage VDFU1.

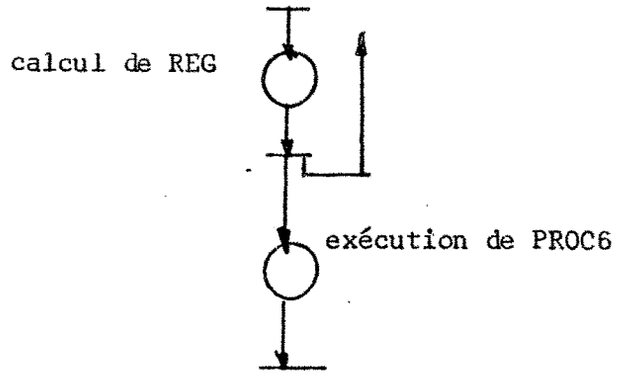
Avec ces remarques, on obtient un Réseau plus complet que le grafcet (G'7) (fig.5b) :



on note qu'il ne peut y avoir de conflit.

FIG. 5b

Remarquant par ailleurs que VFU1 et VDFU1 ne sont plus considérés comme des évènements, mais comme conditions, il est possible dès lors de traduire le Réseau précédent sous la forme d'un algorithme; en notant par ETAT F':= i l'état représenté par le marquage de la place F'i, on obtient :



A l'état initial(Mise sous tension), ETAT F':= 1

avec

PROC 6

Si ETAT F':= 1 ∧ REG ≤ 18 Alors

ETAT F': = 2

FU1 ← 1

Si ETAT F' :=2 ∧ VFU1 ∧ REG < 19 Alors

ETAT F': = 3; FU1 ← 0

Si ETAT F':= 2 ∧ REG ≥ 19 Alors

ETAT F': = 4

DFU1 ← 1

Si ETAT F': = 3 ∧ REG ≥ 19 Alors

ETAT F': = 4

DFU1 ← 1

Si ETAT F': = 4 ∧ VDFU1 ∧ REG > 18 Alors

ETAT F': = 1; DFU1 ← 0

Si ETAT F': = 4 ∧ REG ≤ 18 Alors

ETAT F' : = 2

FU1 ← 1

Remarque :

Les tâches PROC.4, PROC.5 et PROC.6 peuvent être exécutées en parallèle (étant indépendantes les unes des autres) (FIG.6) :

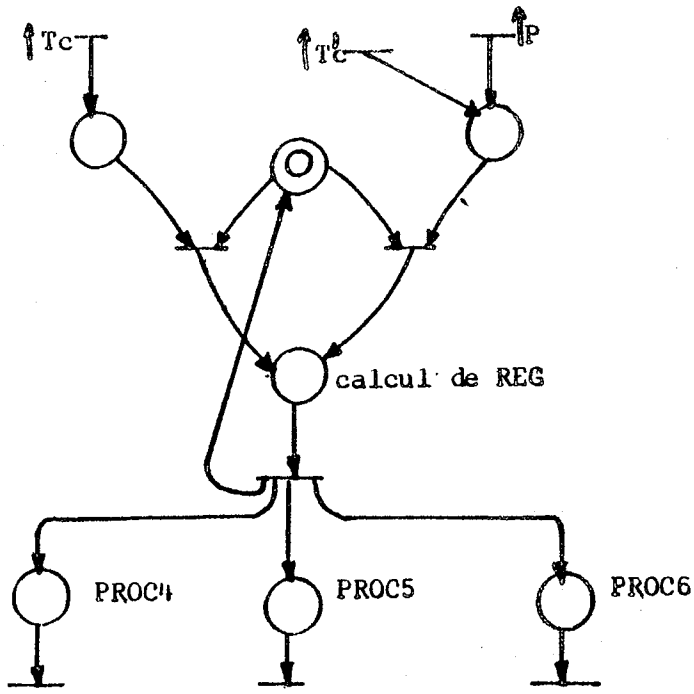


FIG. 6

d) Etude de la relation (G"7,R)

Le grafcet (G"7) est réceptif à e calculé dans (R).

Le même raisonnement que le cas c) nous amène à élaborer un fonctionnement total du contrôle des mécanismes des freins anti-survitesse, et donner une représentation plus complète que celle du grafcet (G"7) (FIG.7).

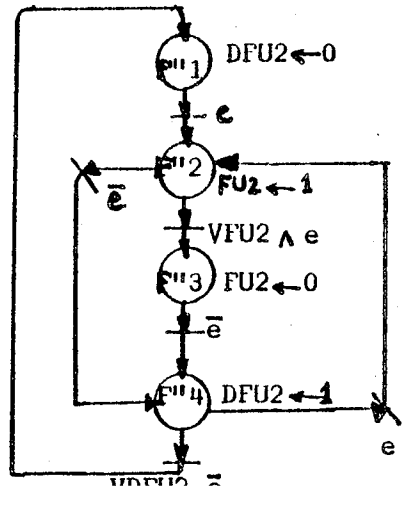


Fig.7

Entre l'instant de commande de freinage (état F"2) et celui où l'acquittement VFU2 est reçu, il se passe un temps au moins égal au temps de réponse des frein anti-survitesse, au cours duquel V_{cs} aura été plusieurs fois, modifiée (à chaqu $\frac{1}{16\tilde{e}}$ partie d'interplot parcourue).

e peut devenir égal à 0 ($\rightarrow \tilde{e}$), à l'état F"2 (freinage par récupération efficace Mais il est fort probable que e garde la valeur 1 (logiquement, e prend la valeu 0 dès l'acquittement de freinage : diminution de vitesse), et dans ce cas, V_{cs} aura été modifiée un assez grand nombre de fois sans que l'état du système change.

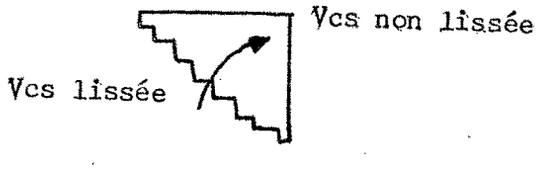
Aussi sommes-nous amenés à nous poser la question suivante :

Etait-il nécessaire de calculer V_{cs} à chaque section ($\frac{1}{16\tilde{e}}$ d'interplot), et est-que le lissage de V_{cs} était utile ?

Certes, comme on vient de le voir, il n'est pas nécessaire de calculer V_{cs} à chaque $\frac{1}{16\tilde{e}}$ partie d'interplot, puisque si $V_{cs} - V_R < 0$, la courbe de vitesse réelle de la rame ne descend pas instantanément en dessous de la courbe de lissage, tel qu'on l'avait spécifiée.

Toutefois, cela n'enlève rien à l'intérêt que nous avons porté à l'élaboration d'une vitesse V_{cs} lissée : le lissage constitue un bon moyen de surveillance presque continue, puisqu'elle se fait à des intervalles de temps assez fins (surveillance de V_R et de l'asservissement de vitesse du P.A.).

L'utilisation de V_{cs} lissée peut être considérée comme une "anticipation" à la commande de freinage :



Dans ce cas aussi, VDFU2 et VFU2 ne sont plus considérés comme des évènements mais comme des conditions, et le réseau précédent peut être traduit sous la forme d'un algorithme; on notera par ETAT F":= 1 l'état représenté par le marquage de la place F"i dans le grafcet (G"7).

A l'état initial (Mise sous tension, on a ETAT F":= 1

PROC 9 :

Si ETAT F": = 1 ∧ e Alors ETAT F':= 2
FU2 ← 1

Si ETAT F": = 2 ∧ $\bar{e}$ Alors ETAT F":= 4
DFU2 ← 1

Si ETAT F": = 2 ∧ VFU2 ∧ e Alors ETAT F":= 3; FU2 ← 0

Si ETAT F" := 3 ∧ $\bar{e}$ Alors ETAT F": = 4
DFU2 ← 1

Si ETAT F":= 4 ∧ VFU2 ∧ $\bar{e}$ Alors ETAT F":= 1; DFU2 ← 0

Si ETAT F":= 4 ∧ e Alors ETAT F" : = 2
FU2 ← 1

Comme le calcul de V_{cs} est effectuée dans PROC 3, c'est à dire à la fréquence de ↑RP, la tâche PROC 9 est activée à cette même fréquence (FIG 8)

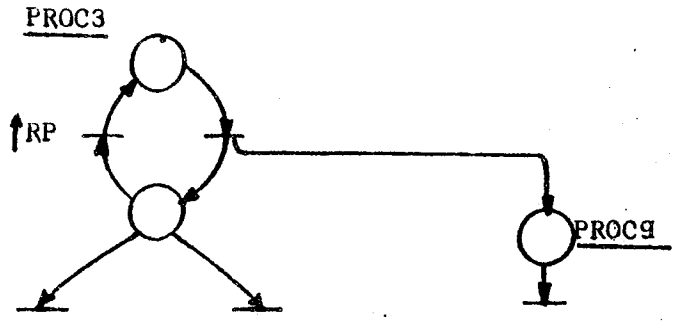


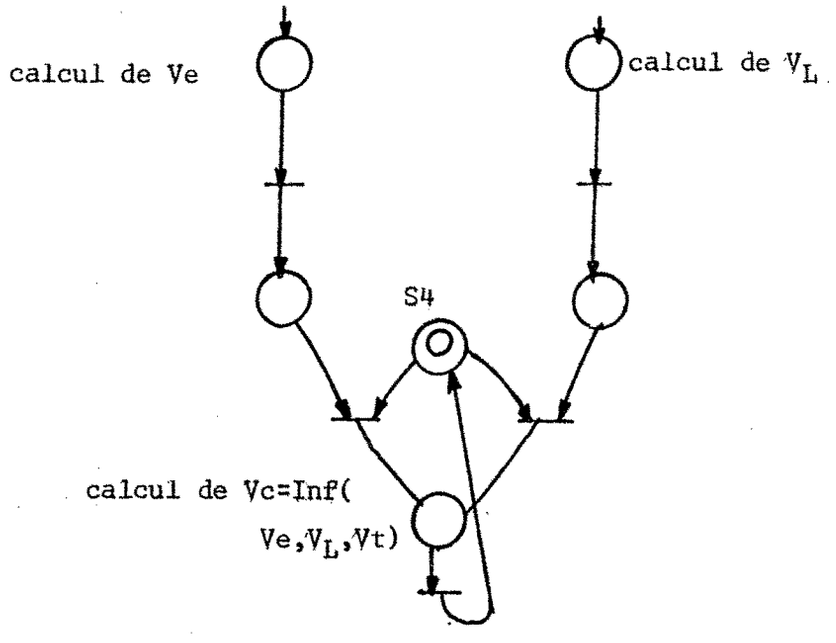
FIG. 8

Etude de la relation (G_1, G_{10}, R)

Il s'agit du calcul de la vitesse de commande V_c en fonction de V_L, V_e. On a vu que la vitesse V_e est calculée à chaque modification de la variable REG, et que la vitesse V_L est calculée à chaque occurrence du signal $\bar{P}$.

Cependant, les modifications de V_e et V_L peuvent être simultanées : ceci nous conduit à imposer une exclusion mutuelle entre les calculs de V_L et de V_e; la vitesse V_c sera calculée chaque fois que V_e ou V_L est modifiée, ce qui peut être représenté tout simplement par le modèle ci-dessous (FIG9).

Fig.9



S_4 joue le rôle d'une ressource commune; c'est une place initialement marquée.

Remarque :

L'étude de la relation (G8, R) ne pose aucun problème : le compteur CA est simplement initialisé à 4 lors de la séquence de démarrage au départ de la station (voir modèle Fig.13).

Etape IV

Etude des dépendances dues aux entrées externes communes.

L'examen des différents grafcets nous donne :

a) L'évènement ↑P est commun à (G2) et (R)

Lorsque ↑P arrive, la procédure PROC 1 (dans R) est activée, ainsi que le calcul de REG (dans G2 ou G'2): les deux calculs étant indépendants (ordre d'exécution indifférent), ils peuvent être exécutés en parallèle (Fig 10 a):

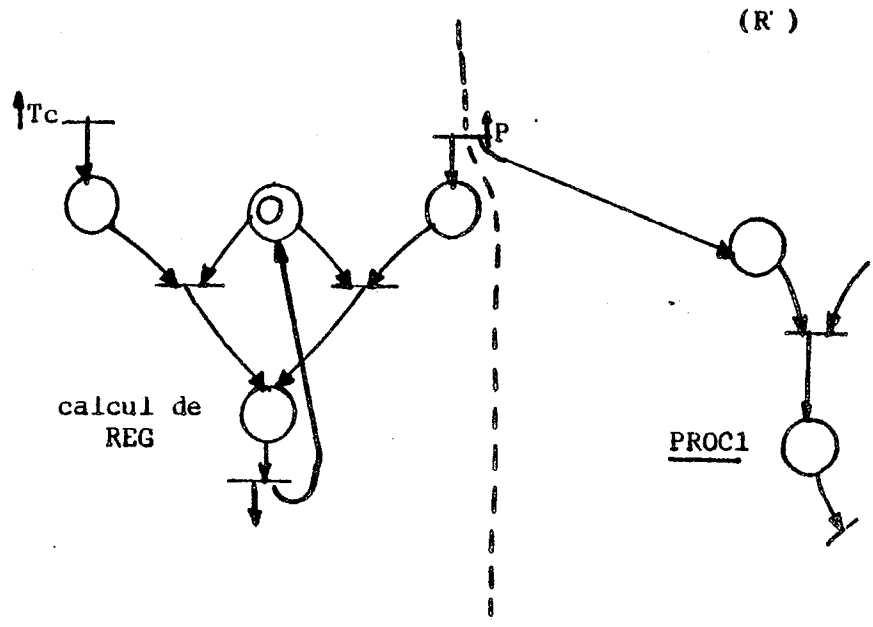


FIG. 10 a

b) L'évènement ↑TC' est commun à (G'2) et à (G8)

On a vu que (G'2) s'obtient à partir de (G2) en remplaçant l'évènement ↑P par ↑TC'.

On obtient aisément le Réseau suivant (FIG 10b) :

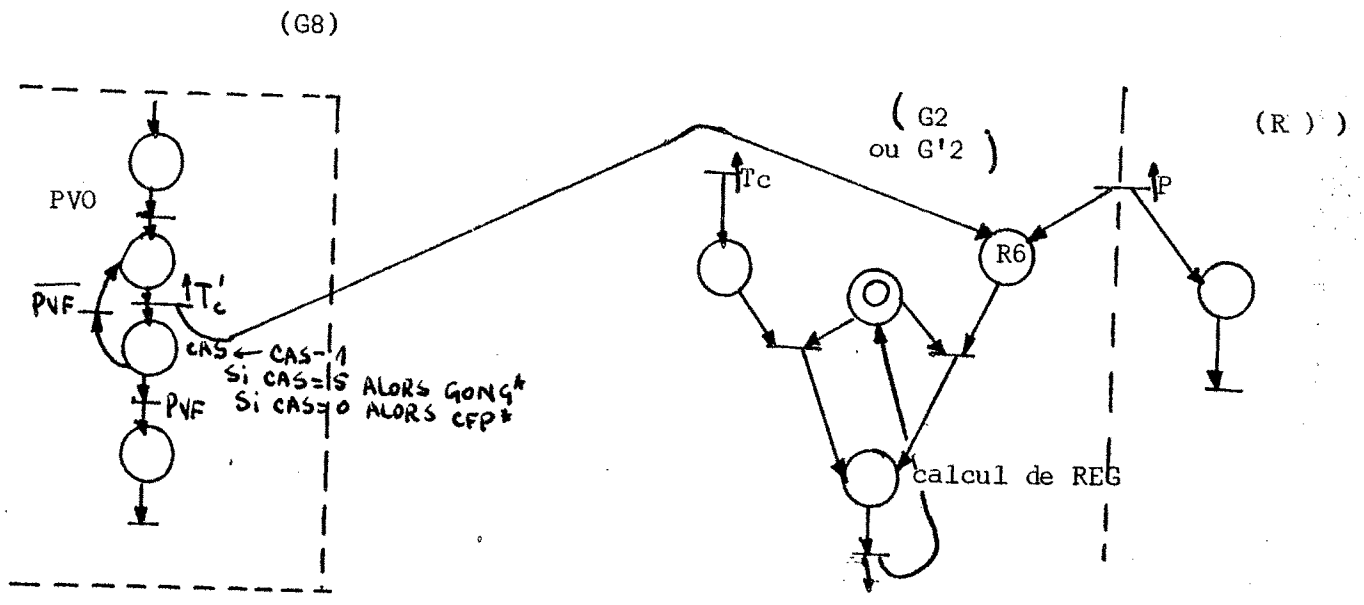


FIG 10 b

D'après ce modèle, on voit bien que les impulsions ↑TC' ne sont plus décomptées dans le compteur REG à partir de la fermeture des portes du véhicule (validation du signal PVF).

Remarque :

Comme il n'y a pas d'occurrence d'évènements ↑P pendant que les ↑TC' arrivent , la place R6 ne peut pas avoir plus d'une marque à la fois (FIG. 10 b)

c) Les évènements PVS, VFU3, PVF et VDFU3 sont communs à (G8) et à (G'''7)

En les regroupant comme il est montré sur la figure 11, on remarque que certaines places sont redondantes et qu'on peut donc les supprimer; c'est le cas des places K2, et K7.

Un réseau équivalent est représenté sur la figure 12.

Afin d'avoir un modèle encore plus simple, on pourrait compacter certains calculs dont l'ordre d'exécution est indifférent, tout en ne perdant pas de vue que le parallélisme précédent pourrait être exploité dans le cas où l'on voudrait utiliser des structures parallèles.

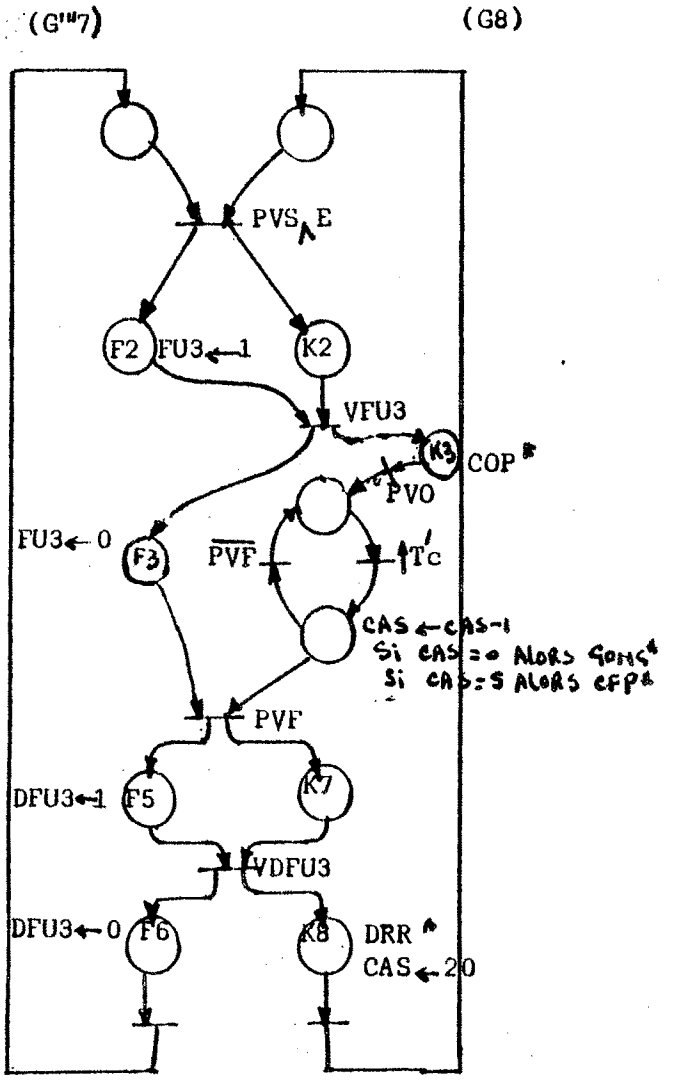


FIG. 11

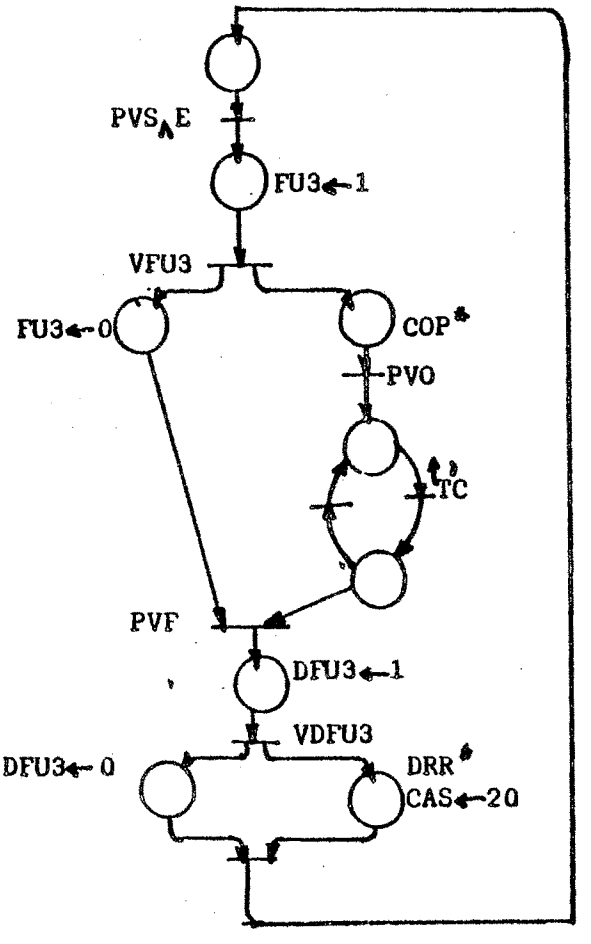


FIG 12

Sur le modèle de la figure 13, on a compacté les actions (FU3←0 et COP*) les actions (DFU3 ← 0, DRR* , CAS←20, et CA ←4).

En définitive, en regroupant tous les résultats trouvés dans les étapes II, III et IV, et complétant certains sous-Réseaux par leur marquage initial, on obtient le modèle de la figure 13, représentant le fonctionnement du système en ligne et dans une station ordinaire.

On note que ce fonctionnement est ramené à un algorithme simple.

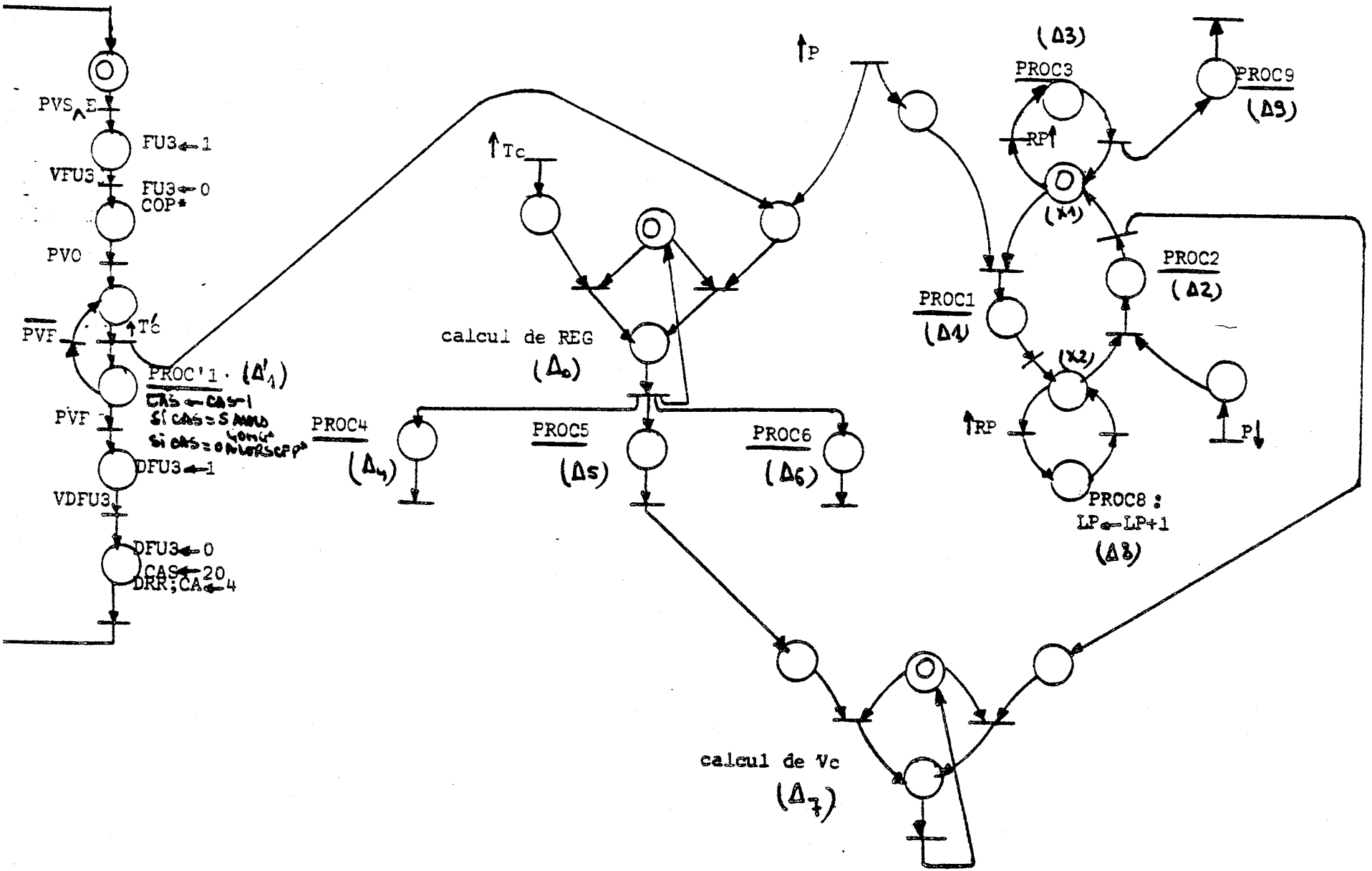

PVS
E
FU3←1
VFU3
FU3←0
COP*
PVO
PVF
Tc
PROC'1 · (Δ'1)
CAS←CAS+1
Si CAS=S alors
Si CAS=0 lorsque
PVF
DFU3←1
VDFU3
DFU3←0
CAS←20
DRR;CA←4
PROC4
(Δ4)
↑Tc
calcul de REG
(Δ0)
PROC5
(Δ5)
PROC6
(Δ6)
↑P
(Δ3)
PROC3
RP↑
(X1)
PROC9
(Δ9)
PROC1
(Δ1)
PROC2
(Δ2)
(X2)
↑RP
P↓
PROC8 :
LP←LP+1
(Δ8)
calcul de Vc
(Δ7)

Fig.13

L'approche suivie dans ce chapitre nous a permis non seulement de déceler certaines ambiguités dans le Cahier des Charges, qui étaient impossibles à montrer dans la représentation par grafcets, et cela parce que maintenant toutes les interactions et les dépendances fonctionnelles existant entre les différentes parties du système ont été étudiées, mais aussi d'obtenir un modèle représentant tout le fonctionnement du système d'une manière cohérente. La simplicité d'un tel modèle fait que toute analyse qu'on voudrait effectuer sur le système s'en trouve largement simplifiée (vérification, validation, décomposition, ...).

C H A P I T R E V

ANALYSE QUANTITATIVE DU MODELE

Il s'agit maintenant de savoir si le modèle que nous avons conçu peut être réalisé dans la pratique.

Notre système étant un système temps réel, sa réalisation consiste à choisir une implantation (matérielle et logicielle) satisfaisant aux contraintes temps réel.

A certaines entrées externes, ayant une fréquence maximale indiquée, une certaine charge de travail doit être exécutée par le système dans un délai donné

Pour permettre d'étudier l'aptitude d'une réalisation du système à "tenir" le temps réel, des paramètres temporels liés à l'implantation doivent apparaître dans le modèle.

Dans notre modèle, nous prenons comme paramètre le temps d'exécution Δi d'une procédure PROCi associée à une place Qi du modèle, et cela dans un souci de simplification de l'étude.

L'étude du modèle fonctionnel impose que, dans une réalisation pratique,

* certains évènements doivent être absolument pris en compte
* chaque place du Réseau ne peut posséder plus d'une marque à la fois.

I. - CONDITIONS NECESSAIRES DE REALISATION

Le nombre maximal de processeurs qu'on peut utiliser est égal au nombre de tâches à exécuter (1 processeur par tâche).

- Le nombre minimal de processeurs est égal à:

$$W = \lceil \Sigma fi \Delta_i \rceil$$

où : fi est la fréquence maximale d'activation de la tâche PROCi

Δi est la durée d'exécution de cette tâche

$\lceil X \rceil$ est la partie entière supérieure de X.

Notations :

f_{Tc} = fréquence maximale instantanée des impulsions $\uparrow Tc$

f_{Rp} = " " " " $\uparrow Rp$

f_p = " " " des évènements P

$f_{\overline{p}}$ = " " " " $\overline{P}$ (= f_p)

$f_{T'_c}$ = " " " des impulsions $\uparrow T'_c$

Δi = durée d'exécution de la procédure PROCI

$X i$ = durée indéterminée d'attente d'une marque dans une place Q_i.

Si le modèle fonctionnel proposé correspond aux spécifications (Réseau sauf) et si l'on suppose que l'on a 1 processeur par tâche, alors les conditions (nécessaires) suivantes doivent être vérifiées :

C1. $\frac{1}{\Delta_0} \geqslant f_{Tc} + f_p$

C2. $\frac{1}{\Delta_0} \geqslant f_{T'_c} + f_{Tc}$

(Les occurrences de $\uparrow T'_c$ et $\uparrow P$ sont exclusives)

C3. $\frac{1}{\Delta 5} \geqslant \frac{1}{\Delta_0}$

C4. $\frac{1}{\Delta 4} \geqslant \frac{1}{\Delta_0}$

C5. $\frac{1}{\Delta_6} \geqslant \frac{1}{\Delta_0}$

C6. $\frac{1}{\Delta_7} \geqslant \frac{1}{\Delta_5} + f_{\overline{p}}$

C7. $\frac{1}{\Delta_8 + \Delta_2} \geqslant f_{RP}$

C8. $\frac{1}{\Delta_4 + \Delta_3} \geqslant f_{Rp}$

C9. $\frac{1}{\Delta 9} \geqslant \frac{1}{\Delta_3}$

C10. $\frac{1}{\Delta 1} \geqslant f_p$

C11. $\frac{1}{\Delta_2} \geqslant f_{\overline{p}}$

C12. $\frac{1}{\Delta'_1} \geqslant f_{T'_c}$

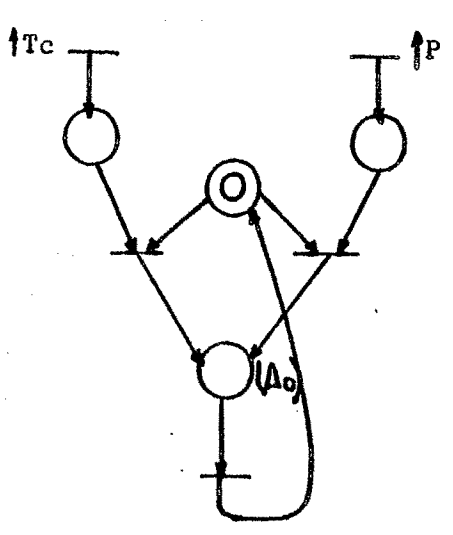
C13. $\frac{1}{\Delta 3 + X1 + \Delta 1} \geqslant f_{Rp}$

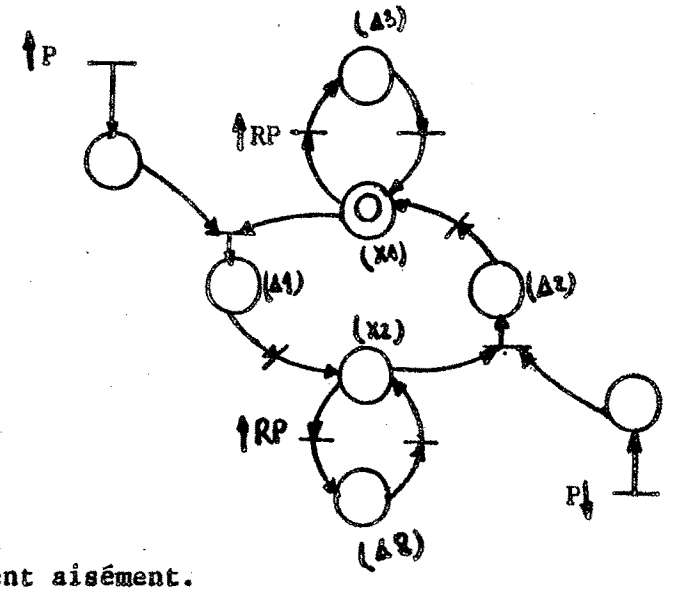
C14. $\frac{1}{\Delta 8 + X2 + \Delta 2} \geqslant f_{Rp}$

Chacune de ces relations exprime que la durée d'exécution d'une procédure PROCi associée à une place Qi est inférieure ou égale à la période d'activation de cette place.

Nous allons montrer que ces conditions sont nécessaires et suffisantes.

Il suffit, pour cela, d'étudier les conditions c_i relatives aux 2 réseaux suivants :





Tous les autres cas s'en déduisent aisément.

II. - ETUDE 1

Considérons le Réseau $(\mathcal{R}_1^*)$ (fig.1)

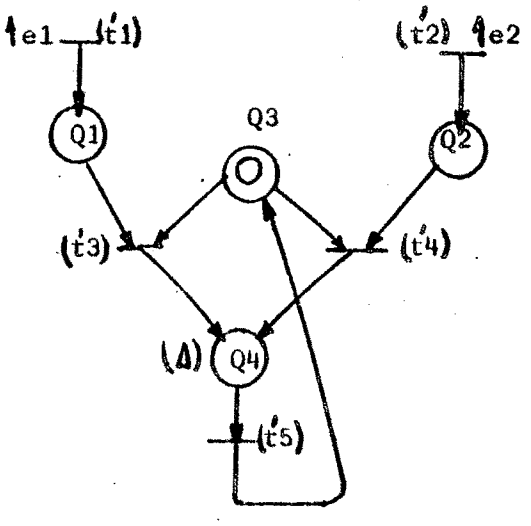


Fig.1

e_1 et e_2 sont 2 évènements ayant pour fréquences maximales instantanées respectives f_{e1} et f_{e2}. = $\frac{1}{T_2}$

Posons : $fe_1 = \frac{1}{T1}$ et $f_{e2} = \frac{1}{T_2}$

V.1 - THEOREME 1

> $\Delta \leq \frac{T_1 \cdot T_2}{T_1 + T_2}$ est une condition nécessaire et suffisante pour que R* soit sauf.

En remarquant que les places Q3 et Q4 sont exclusives et ne peuvent jamais contenir chacune plus d'une marque (trivial), il suffit de démontrer que :

$\Delta \leq \frac{T_1 \cdot T_2}{T_1+T_2}$ est une CNS pour que Q_1 et Q_2 ne puissent posséder plus d'une marque à la fois.

La condition nécessaire est évidente.

1) Préambule :

Définition :

Un compteur n (t) est une fonction à valeurs entières, semi-continue à gauche, non décroissante sur $[o, +\infty[= R^+$:

$$n(t) = n(t^+)$$

Un compteur a de période α vérifie : $(\forall t)\ n(t+\alpha) = n(t) + 1$

Soit T un intervalle fermé $[to, t1]$ et soit q (t,a) le nombre de réalisations du compteur a dans T.

Par définition : $q(T,a) = n_a(t1) - n_a(t_o^-)$

avec :

$$n_a(t-) = \begin{cases} n_a(t) \text{ si } n_a \text{ est continue à droite en t} \\ n_a(t) - 1 \text{ si } n_a \text{ n'est pas continue en t} \end{cases}$$

Lemme 1 :

Si le compteur a est périodique de période α, on a :

$$\left\lfloor \frac{t_1-t_0}{\alpha} \right\rfloor \leqslant q(T,a) \leqslant \left\lceil \frac{t_1-t_0}{\alpha} \right\rceil$$

Où $\left\lfloor \frac{t_1-t_0}{\alpha} \right\rfloor$ désigne la partie entière inférieure de $\frac{t_1-t_0}{\alpha}$

et $\left\lceil \frac{t_1-t_0}{\alpha} \right\rceil$ " " " supérieure de $\frac{t_1-t_0}{\alpha}$

Démonstration :

Posons : $\left\lfloor \frac{t_1-t_0}{\alpha} \right\rfloor = p$

a) Par définition du compteur n_a, on a :

$$n_a (t_0+p\alpha) - n(t_0) = p$$

Soit un instant t_1 tel que :

$$t_0 + p\alpha \leqslant t_1 < t_0 + (p+1)\alpha$$

Comme n (t) est non décroissante, on a:

$$n(t_0+p\alpha) - n(t_0) \leqslant n(t_0+p\alpha) - n(t_0^-) \leqslant n(t_1)-n(t_0^-) \leqslant n(t_0+(p+1)\alpha)-n(t_0^-)$$

$$\Downarrow$$

$$p \leqslant q(T,a)$$

b) Pour démontrer l'inégalité de droite, on considère 2 cas :

Cas 1 : t_0 n'est pas un point de discontinuité (pas d'évènement apparaissant à cet instant),

On a alors : $n(t_0) = n(t_0^-)$

et $n(t_1) - n(t_0^-) \leqslant n\left[t_0+(p+1)\alpha\right] - n(t_0^-)$

$q(T,a) = n(t_1)-n(t_0^-) \leqslant n\left[t_0+(p+1)\alpha\right] - n(t_0)$

Soit

$$q(T,a) \leqslant p+1$$

Cas 2 :

t_o est un point de discontinuité

$$t1 < t_o + (p+1)\alpha \Longrightarrow t1 \leqslant \left((t_o + (p+1)\alpha\right)^-$$

et :

$$n(t1) \leqslant n(t_o + (p+1)\alpha) = n\ (t_o^- + (p+1)\alpha\ )$$

D'après la définition de n (t), :

$$n\ (t_o^- + (p+1)\alpha) \qquad = n(t_o + (p+1)\alpha) \ -1$$

D'où :

$$n(t1) \leqslant n(t_o + (p+1)\alpha) \ - 1$$

et :

$$q(T,a) = n(t1) - n(t_o^-) \leqslant n(t_o + (p+1)\alpha) - 1 - n\ (t_o^-)$$

Soit :

$$q(T,a) \leqslant n(t_o + (p+1)\alpha) - 1 - \left(n(t_o) - 1\right)$$
$$\leqslant n(t_o + (p+1)\alpha) \ - n(t_o)$$
$$\leqslant p+1$$

Lemme :2 :

Si $\begin{cases} n_a(t_o) = n_a\ (t_o^-) + 1 \\ \text{ou} \\ n_a(t1) = n_a\ (t_1^-) + 1 \end{cases}$

Alors : $q(T,a) = \left\lceil \frac{t1-t_o}{\alpha} \right\rceil$

Démonstration :

Posons : $\left\lfloor \frac{(t1-t_o)}{\alpha} \right\rfloor = p$

Par définition : $q(T,a) = n_a(t1) - n_a(t_o^-)$

Soit : $q(T,a) = \left(n_a\ (t1) - n_a\ (t_o)\right) + 1$ (par hypothèse)

Pour $t_1 \geqslant t_o + p\alpha$, on a :

$$n_a(t_1) - n_a\ (t_o) + 1 \geqslant \left(n_a\ (t_o + p\alpha\ ) \ - n_a\ (t_o)\right) + 1$$

soit :

$$q(T,a) \geqslant p+1 \qquad \text{(par définition de } n_a(t)\text{)}$$

or d'après le lemme 1, $q(T,a) \leq p+1$, on en déduit :

$$q(T,a) = p+1 = \left\lceil \left(\frac{t_A - t_o}{\alpha} \right) \right\rceil$$

Lemme 3 :

$$\lceil A + B \rceil \leq \lceil A \rceil + \lceil B \rceil \leq \lceil A + B \rceil + 1$$

Démonstration :

* $A \in \mathbb{N}$, $B \in \mathbb{N}$, cela est vrai

* $A \in \mathbb{N}$, $B \notin \mathbb{N}$, $B = b + \beta$ avec $0 < \beta < 1$ et $b \in \mathbb{N}$

$$\lceil A \rceil + \lceil B \rceil = A + b + 1$$

et

$$\lceil A + B \rceil + 1 = A + b + 2 \qquad \text{(vrai)}$$

* $A \notin \mathbb{N}$, $B \notin \mathbb{N}$

$A = a + \alpha$ $\quad 0 < \alpha < 1$

$B = b + \beta$ $\quad 0 < \beta < 1$

et a, b $\in \mathbb{N}$

$$\lceil A \rceil + \lceil B \rceil = a + b + 2$$

$$\lceil A + B \rceil + 1 = \lceil (a + b + \alpha + \beta) \rceil + 1$$

$$= a + b + (\alpha + \beta) + 1 \leqslant a + b + 2 + 1$$

(vrai)

2. Reprenons le réseau R_1^* de la figure 1

Désignons par $q(t) = q_1(t) + q_2(t)$ le nombre de marques présentes dans Q_1 et Q_2 à l'instant t.

D'après le fonctionnement du Réseau R_1^*, on a, dans un intervalle $[t_1, t_2[$:

$$\begin{cases} n_1(t+T_1) = n_1(t) + 1 \\ n_2(t+T_2) = n_2(t) + 1 \\ n_3(t) + n_4(t) = \min\left[n_1(t) + n_2(t),\ n_5(t) + 1\right] \\ n_5(t+\Delta) = n_3(t) + n_4(t) \end{cases}$$

soit :

$$(1)\quad n_3(t) + n_4(t) = \min\left[n_1(t) + n_2(t),\ n_3(t-\Delta) + n_4(t-\Delta) + 1\right]$$

on peut écrire par ailleurs :

$$q(t) = n_1(t) + n_2(t) - n_3(t) - n_4(t)$$

Supposons qu'il existe un instant t_2 tel que :

$$q(t_2) \geqslant 2$$

Soit t1 l'instant tel que:

$$t_1 = \operatorname{Sup}_{t \in [0,t_2[} t \quad \text{tel que} \begin{cases} t \in [0,t_2[\\ (2)\ n_1(t) + n_2(t) = n_3(t) + n_4(t) \\ \qquad\qquad\quad = n_5(t) \\ \qquad\qquad\quad = n_3(t-\Delta) + n_4(t-\Delta) \end{cases}$$

L'instant t_1 existe :

En effet, à l'instant 0, (2) est vérifiée; en outre, l'intervalle $[0,t_2[$ étant borné, possède une borne supérieure qui est: $\operatorname{Sup} t = t_1$.

t_1 est le premier instant tel qu'aucune marque n'est en attente.

D'après (1), on a, sur $[t_1\ t_2[= T$,

$$n_3(t) + n_4(t) = n_3(t-\Delta) + n_4(t-\Delta) + 1$$

Ce qui signifie que : $q(T_{,3,4})$ est un compteur périodique de période égale à Δ,

On peut donc utiliser le lemme 2 :

(3) $q(T_{,3,4}) = \left\lceil \left(\frac{t_2 - t_1}{\Delta} \right) \right\rceil$

D'autre part, on a :

$$q(t_2) = q(T_{,1}) + q(T_{,2}) - q(T_{,3,4})$$

D'après le lemme 1, :

(4) $q(T_{,1}) \leq \left\lceil \frac{t_2 - t_1}{T_1} \right\rceil$

et (5) $q(T_{,2}) \leq \left\lceil \frac{t_2 - t_1}{T_2} \right\rceil$

(3), (4) et (5) donnent :

$$q(t_2) \leq \left\lceil \frac{t_2 - t_1}{T_1} \right\rceil + \left\lceil \frac{t_2 - t_1}{T_2} \right\rceil - \left\lceil \frac{t_2 - t_1}{\Delta} \right\rceil$$

D'après le lemme 3 :

$$q(t_2) \leq \left\lceil \frac{t_2 - t_1}{T_1} + \frac{t_2 - t_1}{T_2} \right\rceil + 1 - \left\lceil \frac{t_2 - t_1}{\Delta} \right\rceil$$

$$\Delta \leq \frac{T_1 \cdot T_2}{T_1 + T_2} \Longrightarrow q(t_2) \leq 1 - \varepsilon, \qquad (0 < \varepsilon < 1)$$

SOIT : $\boxed{q(t_2) \leq 1}$

Donc, les places q1 et q2 ne peuvent jamais être marquées les deux à la fois, et ne peuvent avoir plus d'une marque chacune.

Le Réseau (R_1^*) est donc sauf.

III ETUDE 2.

Soit le Réseau (R_2^*) (Fig. 2)

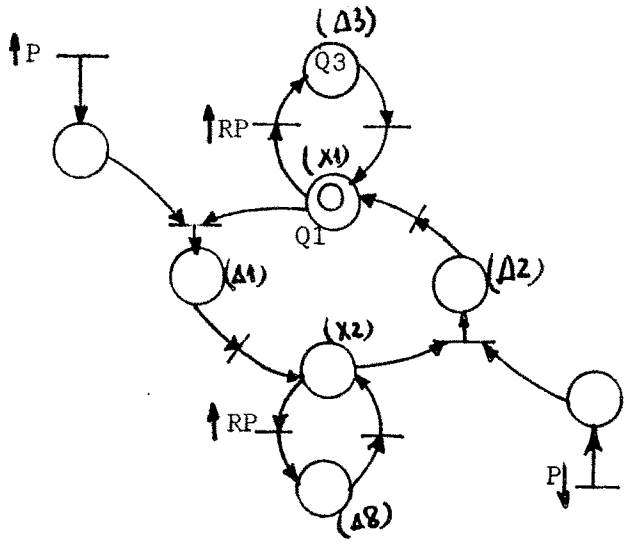


FIG. 2 Réseau R_2^*

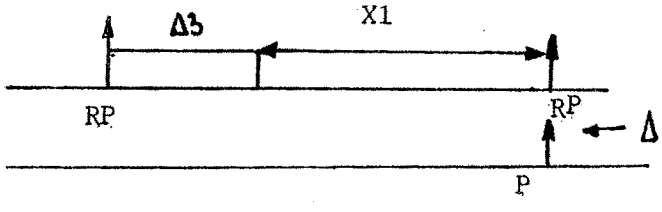
On a vu que les conditions nécessaires relatives à une telle machine sont :

C13) $\Delta_3 + X_1 + \Delta_1 \leq \frac{1}{f_{RP}}$ C14) $\Delta_8 + X_2 + \Delta_2 \leq \frac{1}{f_{RP}}$

C10) $\frac{1}{\Delta_1} \geq f_P$ C11) $\frac{1}{\Delta_2} \geq f_{\bar{P}}$

Etude de la condition C13.

Dès occurrence de l'évènement ↑RP, la marque vient en q_3 où elle reste pendant une durée égale à Δ_3. Ensuite, elle se déplace en q_1 où son temps d'attente est indéterminé (FIG.3). Mais supposons que l'évènement ↑P arrive en même temps que ↑RP, cela signifie que Δ_1 peut être nul.



On en déduit que le modèle (R^*2) ne peut pas être réalisé dans la pratique (bien qu'il soit conforme aux spécifications, donc correct).

Il en est de même de la condition C14 (Δ_2 peut être nul).

Cette étude nous montre l'intérêt d'une analyse fine afin de prouver l'applicabilité d'une spécification.

Deux possibilités nous sont alors offertes :

1ère Possibilité :

La contrainte imposée à ↑RP est un peu sévère : l'étude précédente nous a montré qu'on peut perdre des évènements ↑RP.

On peut donc les mémoriser (Fig. 3)

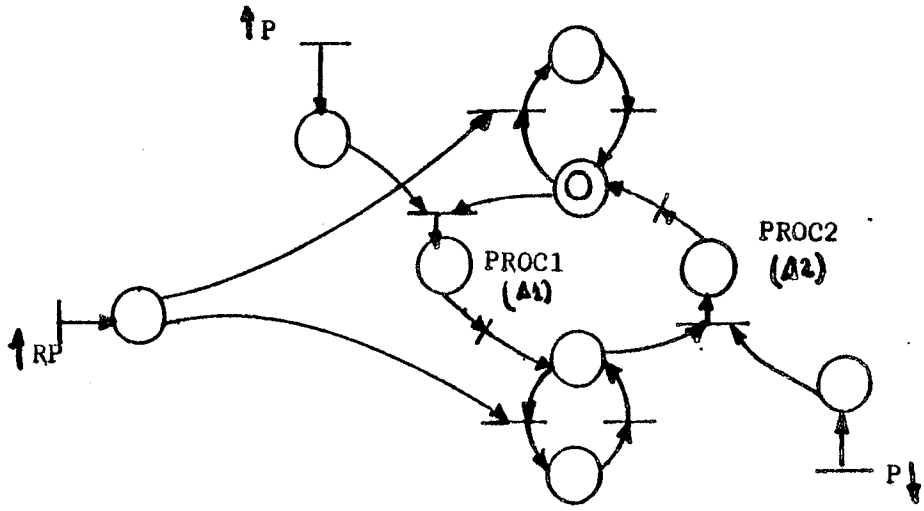


FIG. 3

Toutefois, cela nous amène à établir de nouvelles conditions, et à les vérifier, ce qui peut nous donner des calculs fastidieux.

2ème possibilité :

Elle nous paraît plus simple :

Ne pas exécuter les tâches PROC 1 et PROC 2 entre $\uparrow P$ et $\uparrow RP$ (ou $\downarrow P$ et $\uparrow RP$), ce qui équivaut à ajouter des branches parallèles comme le montre le modèle suivant (FIG 4a):

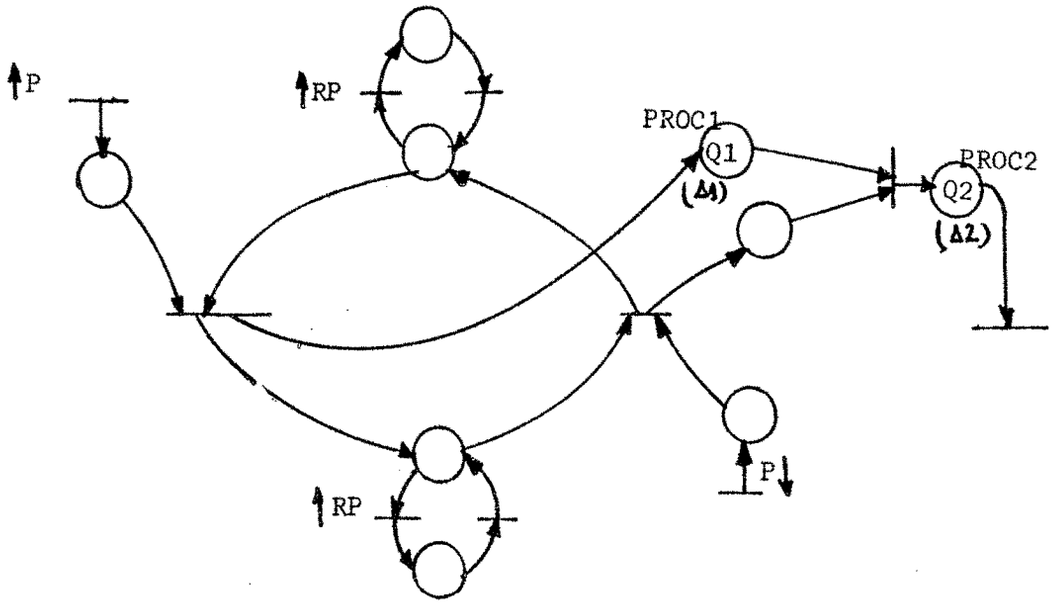


FIG. 4a

Remarque :

Dans ce modèle, on voit qu'il ne peut pas y avoir de possibilité de lecture et écriture simultanées de la variable RLI (écrite dans PROC 1, et lue dans PROC 2 pour le calcul de V_L).

L'analyse du problème se réduit à celle du réseau R_3^* (FIG. 4b):

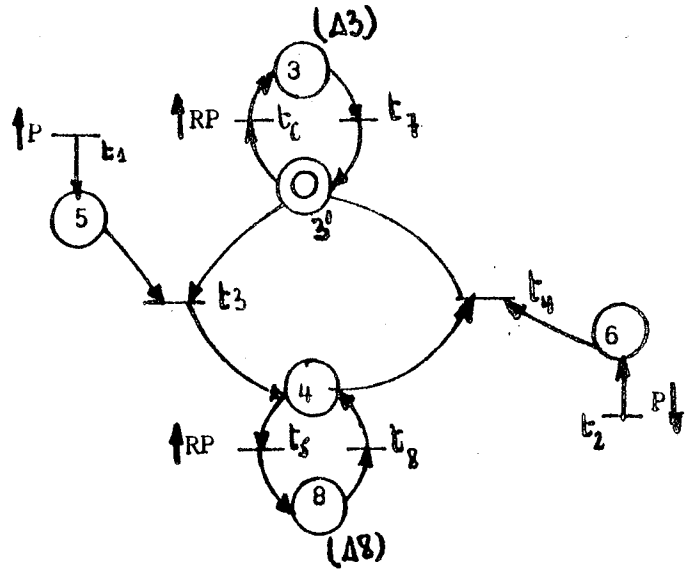


Fig. 3b Réseau (R_3^*)

THEOREME II

$\max(\Delta_3, \Delta_8) \leq \min\left(\frac{1}{f_P}, \frac{1}{f_{RP}}\right)$	est une CNS pour que le réseau R_3^* soit sauf.

Posons : $\frac{1}{f_P} = \tau_P$, $\frac{1}{f_{RP}} = \tau_{RP}$

Préambule :

En utilisant les notations de compteurs comme dans l'étude 1, le fonctionnement du réseau (R^*3) nous donne les relations suivantes :

(1) $n_1(t+\tau_p) = n_1(t) + 1$

(2) $n_2(t+\tau_p) = n_2(t) + 1$

(3) $n_6(t+\tau_{RP}) + n_5(t+\tau_{RP}) = n_6(t) + n_5(t) + 1$

(4) $n_7(t+\Delta_3) = n_6(t)$

(5) $n_8(t+\Delta_8) = n_5(t)$

(6) $n_3(t) = \min\left(n_1(t),\ 1 + n_4(t) + n_7(t) - n_6(t) \right)$

(7) $n_4(t) = \min\left(n_2(t),\ n_8(t) + n_3(t) - n_5(t) \right)$

Démonstration

a) Lemme 1 :

α) $n_7 \leq n_6 \leq n_7 + 1$

β) $n_8 \leq n_5 \leq n_8 + 1$ (les places Q3, et Q8 sont sauves)

γ) $n_4 \leq n_3 \leq n_4 + 1$

Preuve :

On a :

$$n_6 = n_7 (t + \Delta_3) \geq n_7(t)$$

$$n_5 = n_8(t + \Delta_8) \geq n_8(t)$$

(6) $\Longrightarrow n_3 \leq n_4 + 1$

(7) $\Longrightarrow n_4 \leq n_3$

(8) $\Longrightarrow n_6 \leq n_7 + 1$

(9) $\Longrightarrow n_5 \leq n_8 + 1$

b) Lemme 2 :

Les places Q_3, Q_8, Q_5, et Q_4 sont sauves .

En effet :

$\beta) \Longrightarrow 0 \leq n_5 - n_8 \leq 1$

$\alpha) \Longrightarrow 0 \leq n_6 - n_7 \leq 1$

La charge de Q_4 est : $q_4 = n_8 + n_3 - n_4 - n_5$

$(\beta, \gamma) \Longrightarrow q_4 \leq n_3 - n_4 \leq 1$ et

$(\beta, \gamma) \Longrightarrow q_4 \geq n_3 - n_4 - 1 \geq 0$

De la même façon :

$$q_3 = n_7 + n_4 - n_3 - n_6$$

et $0 \leq q_3 \leq 1$

c) Une condition nécessaire et suffisante pour respecter (3) est

$$\begin{cases} \Delta 3 \leq \tau_{RP} \\ \Delta 8 \leq \tau_{RP} \end{cases} \qquad \text{soit } \max(\Delta_3, \Delta_8) \leq \tau_{RP}$$

Preuve :

Condition suffisante :

soit t la date d'un évènement $\uparrow_{RP}$. A l'instant t^-, il y a une marque dans Q_3 ou Q_4, soit :

$$q_3(t^-) + q_4(t^-) = 1$$

Alors si la condition est vérifiée, il y en aura une à l'instant $t^- + \tau_{RP}$

Condition nécessaire :

Evident

d) Une condition nécessaire et suffisante pour que les places Q_5 et Q_6 soient sauves est :

$$\max(\Delta_3, \Delta_8) \leq \tau_p$$

Condition nécessaire : Evident.

En effet, si la marque arrive dans Q_3 juste avant le tir de la transition t_1, et y reste un temps supérieur à la période de franchissement de t_1, il y aura 2 marques dans la place Q_5.
(De même pour la place Q_6).

Condition suffisante :

On pose : $q_5 = n_1 - n_3$

$q_6 = n_2 - n_4$

α) On ne peut avoir simultanément : $q_5 > 1$ et $q_6 = 0$

(resp. $q_6 > 1$ et $q_5 = 0$)

$q_6 = 0 \longrightarrow n_4 = n_2$

$1 < n_1 - n_3 \leq n_1 - n_4 = n_1 - n_2$

soit $n_1 > n_2 + 1$ Ce qui est impossible

. De même pour :

$q_5 = 0$, et $q_6 > 1$

On a :

$1 < n_2 - n_4 \leq n_2 - n_3 + 1 = n_2 - n_1 + 1$

d'après (γ)

$0 < n_2 - n_1$ et $n_1 < n_2$ ce qui est impossible

β) soit t le premier instant tel que $q_5(t) = 2$, et $q_6(t) = 1$

Alors :

$q_5 = n_1 - 1 - n_4 - n_7 + n_6 = 2$

$q_6 = n_2 - n_8 - n_3 + n_5 = 1$

$n_1 = n_4 + 2$

$n_2 = n_3 + 1$

Il vient :

$$\begin{cases} n_5 - n_8 = 0 \\ n_6 - n_7 = 1 \end{cases}$$

Soit :

$n_6(t) = n_7(t) + 1$ ou encore

$n_6(t) = n_6(t - \Delta_3) + 1$

Dans l'intervalle de temps semi-ouvert $]\, t-\Delta_3,\ t\,]$, il y a un franchissement de la transition t_6. Soit t' cette date :

à t'^-, on a : $Q_5(t'^-) = 0$, sinon on n'aurait pas franchi la transition t_6 mais t_3. Donc, 2 marques sont arrivées en Q_5 entre $]\, t-\Delta_3$ et $t\,]$. Cela n'est pas possible si $\Delta_3 \leq \tau_p$

Valeurs numériques :

Calcul des fréquences maximales instantanées :

$f_{T'_c} = f_{T_c} = 1$ Hz

Calcul de f_{RP}: pour un pas de la roue phonique $\delta = 3{,}5$ cm, et une vitesse maximale de 22,1 m/s, on a $\tau_{RP} = 1{,}58$ ms, soit $f_{RP} = 632$ Hz

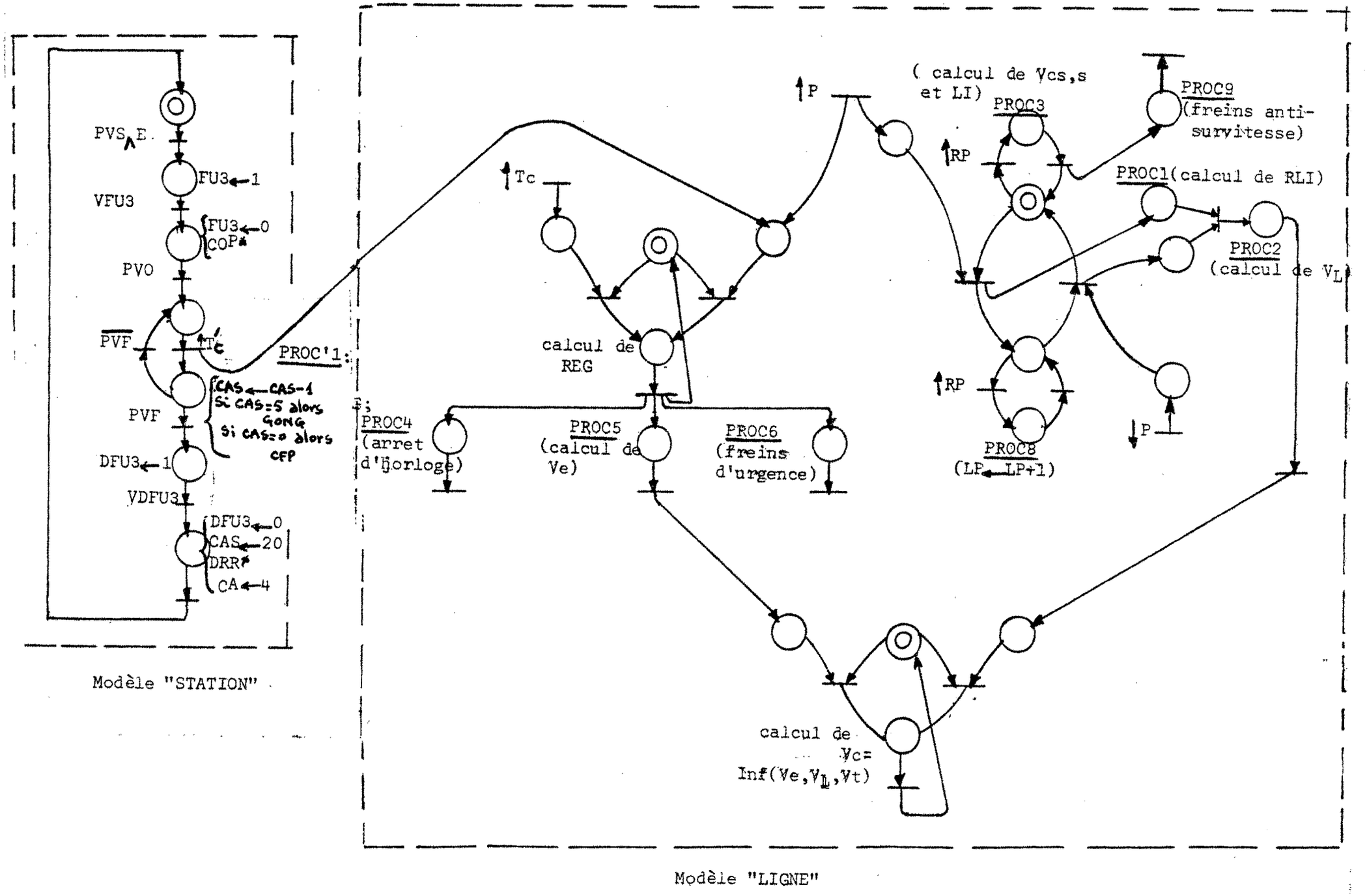
Calcul de $f_p = \frac{1}{\tau_p}$: $\tau_p = \frac{16{,}9}{22{,}1}$, soit $f_p = 1{,}4$ Hz

CONCLUSION :

L'analyse que nous venons de faire nous a permis de corriger le modèle fonctionnel du P.A.

Par ailleurs, le modèle définitif (FIG 5) ne peut être réalisable dans la pratique que si et seulement si les caractéristiques du matériel d'implantation vérifient les conditions $(C_1, C_2, \ldots, C_{14})$.

Toutefois, insistons sur le fait que cette analyse quantitative est faite en considérant un nombre maximal de processeurs, soit 1 processeur par tâche. Auss au stade de l'implantation, le réalisateur n'aura pas à implanter une tâch par processeur; il aura en outre à étudier un ordonnancement des tâches, éliminer certains parallélismes (compactage de tâches), et examiner s'il est possible de réduire le nombre de processeurs à réaliser.


PVS
E
FU3←1
VFU3
FU3←0
COP#
PVO
PVF
↑Tc
PROC'1;
CAS←CAS-1
Si CAS=5 alors GONG
si CAS=0 alors CFP
PVF
DFU3←1
VDFU3
DFU3←0
CAS←20
DRR#
CA←4
Modèle "STATION"
↑P
(calcul de Vcs,s et LI)
PROC3
PROC9 (freins anti-survitesse)
↑RP
PROC1(calcul de RLI)
PROC2 (calcul de VL)
↑Tc
calcul de REG
PROC4 (arret d'horloge)
PROC5 (calcul de Ve)
PROC6 (freins d'urgence)
↑RP
PROC8 (LP←LP+1)
↓P
calcul de Vc= Inf(Ve,VL,Vt)
Modèle "LIGNE"

CHAPITRE VI

ANALYSE DE LA SECURITE

I. Approche déductive

I.1 Analyse par arbre des causes

I.2 Insuffisances de l'analyse par arbres des Causes

II. Analyse de la Sécurité

II.1 Analyse du risque de collision

II.2 Analyse du risque de survitesse

II.3 Analyse du risque de mauvaises commandes d'ouverture ou de fermeture des portes

Conclusion

Il est intéressant d'avoir, à partir du modèle fonctionnel construit, une décomposition du système en blocs de sécurité : chaque bloc assurant une fonction entrant en jeu dans l'évaluation des objectifs de sécurité, établis dans les spécifications opérationnelles du Cahier des Charges.

Nous rappelons que les fonctions à considérer dans l'étude de la sécurité son celles assurant l'anti-collision, l'anti-survitesse, et les commandes d'ouverture et de fermeture des portes.

Pour déterminer ces blocs, une analyse des différents risques d'accidents, nous permettant de déterminer les causes de ces accidents, s'avère nécessaire. Pour cela, nous allons utiliser une analyse par arbre de causes .

I. Approche déductive. Arbres de Causes [CHA74]

Dans l'analyse de la sécurité d'un système, l'approche déductive est la techni que exigée :

- lorsqu'on dispose d'une liste d'évènements critiques
- lorsque les pannes n'ayant aucun effet sur le système peuvent être négligées

Une telle approche est optimale pour les pannes multiples.

L'analyse par arbres de causes ("Fault Tree Analysis") est la méthode utilisa une telle approche. En outre, elle ne s'intéresse pas seulement aux défaillanc matérielles du système.

I.1 Analyse par arbres des causes

Elle est aussi appelée "Arbres de Défauts" par les fiabilistes.

Dans cette méthode, l'évènement d'intérêt est dit "Evènement Indésirable", dont l'occurrencepeut conduire à un incident ou un accident (fig 1). La structure utilisée par cette méthode est l'arbre des causes. C'est un modèle graphique qui représente les relations logiques au sens de l'Algèbre de Boole, c'est-à-dire qu'elles font appel aux opérateurs tels que l'opérateur intersection ET, et l'opérateur réunion OU, liant l'évènement indésirable à des évènements de base, souvent dits indépendants ou primaires, car on admet qu'on ne peut plus développer l'arbre au delà de ce niveau. La construction de l'Art consiste à déterminer les conditions minimales nécessaires et suffisantes pour qu'un évènement indésirable ait lieu. Le procédé se répète avec les conditions trouvées jusqu'à ce qu'on arrive aux éléments de base (fig. 2).

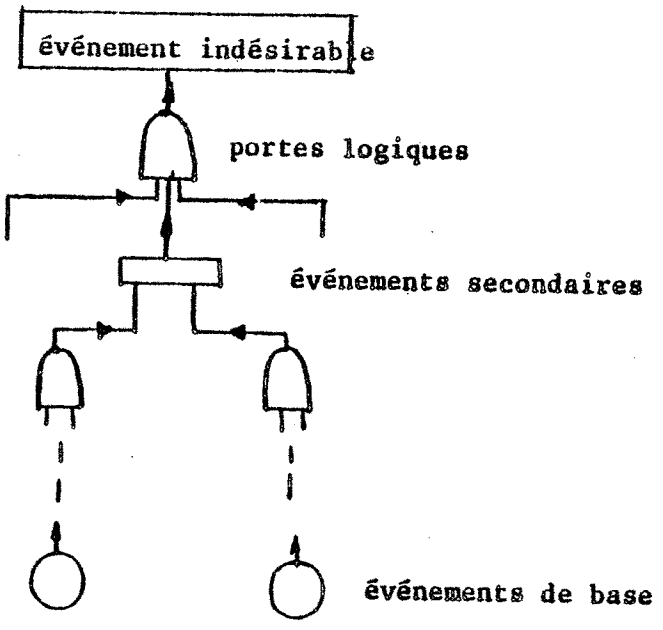


Fig.1 - Structure d'un Arbre des Causes

Les relations logiques permettent d'obtenir la fonction booléenne du système, qui exprime l'évènement indésirable en fonction des évènements de base. L'analyse du système est effectuée à partir de la forme réduitede la fonction booléenn obtenue.

L'Analyse qualitative consiste à déterminer les chemins critiques de l'Arbre. On appelle chemin critique la succession des évènements liés par des portes logiques OU aboutissant à un ou plusieurs évènements de base. Un seul évènement de base suffit à entraîner la défaillance du système. L'étude des évènements du chemin critique est primordiale dans une analyse par arbre des causes.

L'Analyse quantitative consiste à déterminer la probabilité d'occurrence des évènements de l'arbre, ainsi que celle de l'évènement indésirable.

L'Analyse qualitative ne permet pas de détecter facilement les défauts de mode commun [CAR 73] ,de tels défauts résultant de la combinaison ou de l'enchaînement d'évènements situés en aval des portes ET (donc a priori non situés sur le chemin critique).

.../...

I.2 Insuffisances de l'analyse par Arbres des Causes

L'analyse par arbres des causes est, sans aucun doute, la méthode d'analyse qui a trouvé le plus de succès chez les spécialistes de sécurité. Cette méthode fait l'objet de nombreux travaux universitaires aux Etats-Unis, et depuis quelques années, regagne de plus en plus de l'intérêt dans les milieux industriels français.

Les avantages de la méthode sont indéniables [FUS 74] ;le raisonnement d'approche tel que "Qu'est-ce qui pourrait causer ceci? est très simple.

Cependant ,certaines insuffisances lui sont reprochées :

** L'analyse par arbres des causes est une méthode statique qui ne tient pas compte des contraintes temporelles, et n'est pas applicable aux systèmes parallèles [GOL 75].

** Elle est fondée sur certaines hypothèses qui ne sont pas réalistes de nos jours, dont la plus importante est celle de l'indépendance statistique des évènements [1YEL 75] Cette hypothèse d'indépendance est systématiquement utilisée dans la plupart des modèles de fiabilité et de sécurité. Il est vrai que les approximations qui en découlent donnent des résultats satisfaisants dans certains cas réels, mais il existe un grande classe de systèmes où cela n'est plus acceptable [2YEL 75]. Dans l'analyse par Arbres de causes, l'approche s'arrête dès qu'on arrive aux évènements de base; l'idée même de dire que de tels évènements sont indépendants ou primaires montre bien qu'on se contente de ne pas chercher à en déterminer les causes.

** La méthode ne permet pas de mettre en évidence des évènements mutuellement exclusifs.

** La détermination des pannes de mode commun n'est pas évidente.

** La plus grande partie des travaux traitant de la méthode est surtout consacrée à l'analyse quantitative. De très nombreux algorithmes sont de plus en plus développés [GAR77, CAM78]. Ces algorithmes ne diffèrent que par leur rapidité, l'espace mémoire utilisé pour leur implantation, et par la taille de l'Arbre des Causes qu'ils peuvent traiter.

L'analyse qualitative a été souvent négligée :

** La construction de l'Arbre des causes est reconnue comme étant l'étape la plus fastidieuse dans l'étude d'un projet. Cette construction est souvent subjective, et la plupart des arbres des causes sont alors pourvus d'oublis [FUS74].

** Les incorrections dans un arbre des causes sont dues à la difficulté de comprendre le système étudié, parce que celui-ci est mal défini ou mal décrit.

** Pour un même système et pour la même mission, il a été relevé que différents analystes construisent des arbres différents.

En réalité, la plupart des insuffisances de cette méthode sont dues au manque de modèle de description convenable du sytème à étudier [LAP77] [AZ078].

Un tel modèle de description doit :

** être simple, et peut être compris par d'autres analystes.
** tenir compte de la dépendance des évènements, sous une forme plus claire.de CAUSE-EFFET [HEN76] [2YEL75] et s'adapter à la complexité du système (présence de boucles)
** décrire le comportement du système en fonction du temps (séquentialité, parallèlisme, exclusivité mutuelle des évènements, ...).

Le Réseau de Pétri Interprété peut répondre à la question.
Indépendamment de toute réalisation matérielle, le modèle fonctionnel que nous avons élaboré est assez clair et simple pour nous permettre la construction aisée des arbres *de causes relatifs aux divers accidents considérés.*

Par ailleurs, l'analyse et la validation du modèle fonctionnel rendent petit le nombre d'omissions qu'on pourrait commettre et des ambiguités qui constituent la majeure partie des sources d'erreurs de conception : et cela ne peut que garantir la cohérence et l'efficacité de l'analyse de la sécurité.

II Analyse des différents risques d'accidents

Le modèle fonctionnel du P.A. met en évidence 2 parties représentant respectivement les fonctionnements du P.A. en ligne et en station. Entre ces 2 parties, il existe une relation de dépendance traduisant la régulation en station sur occurrence des impulsions d'horloge $T'c$ dès la fermeture des portes du véhicule.

Le décomptage des impulsions $T'c$ dans le compteur REG ne peut pas avoir lieu correctement si le fonctionnement du P.A. en station est incorrect.

En première analyse, nous supposerons le fonctionnement du P.A. en station correct. Nous y reviendrons ultérieurement et confirmerons cette hypothèse.

II. 1- Analyse du risque d'accident : Type collision entre deux rames

a) Le risque de collision en ligne a lieu si l'une des conditions suivantes est vérifiée :

1- La commande de freinage d'urgence (FU1) n'a pas été donnée sachant que la valeur de la variable REG est $\leqslant 18$.

2- La valeur réelle de REG est inexacte : elle aurait dû être égale à 18, la commande FU1 ne pourraît donc être donnée.

3- La valeur de REG est bien inférieure ou égale à 18, la commande FU1 a été correctement émise mais par suite d'une panne quelconque, la commande de défreinage DFU1 est donnée intempestivement, ce qui annule l'ordre de freinage.

4- La valeur de REG est égale ou supérieure à 39, mais l'ordre ARTO * d'arrêt d'horloge n'a pas été émis vers le P.C.C.

5- La valeur réelle de REG est inexacte : elle aurait dû être égale ou supérieure à39 ; l'ordre ARTO * ne pourrait alors être émis.

6- La valeur réelle de REG est bien supérieure ou égale à 39, l'ordre ARTO * a été correctement émis, mais par suite d'une panne quelconque l'ordre RETO* est émis intempestivement, ce qui fait reprendre l'émission des signaux d'horloge.

Cette analyse serait insuffisante si l'on ne considérait pas les éléments de l'environnement dont la défaillance pourrait entraîner un risque de collision, sachant que le P.A. fonctionne correctement.

En effet, le risque de collision peut avoir lieu si :

7- Le P.C.C., ayant reçu l'ordre ARTO *, n'arrête pas l'émission des signaux d'horloge, ou remet intempestivement l'ordre RETO *

8- Les freins d'urgence sont défaillants, sachant que l'ordre FU! a été correctement émis (par freins, on entend l'ensemble "compresseur - vérin hydraulique - pistons - sabots ou disques")

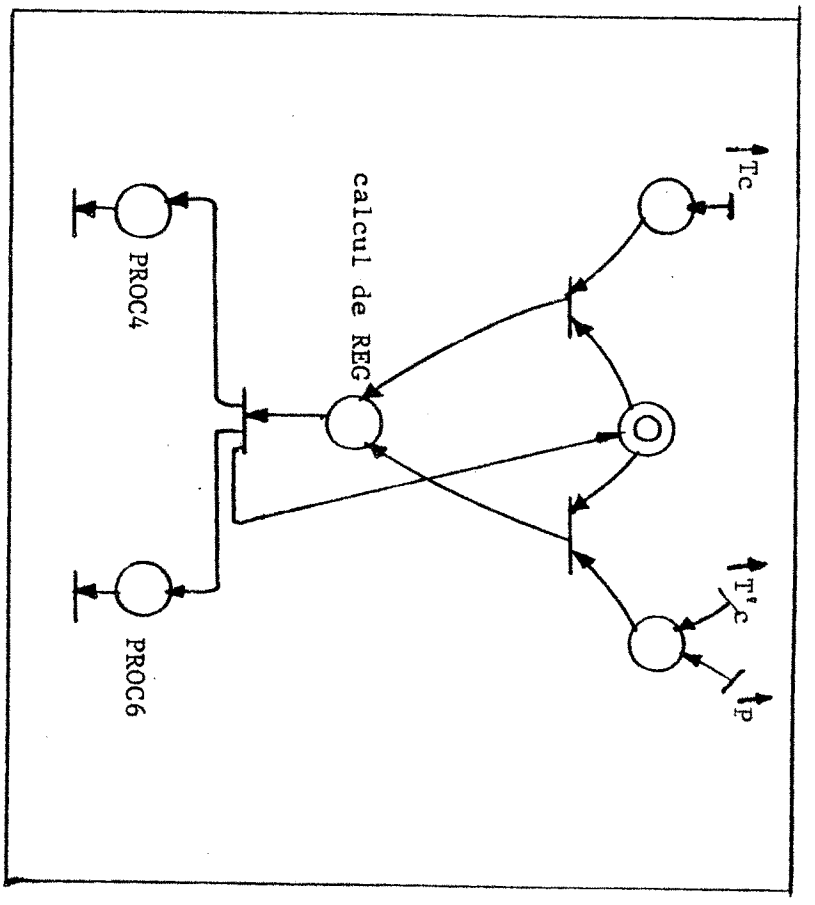
9- Les détecteurs des signaux Tc, Tc' et des signaux de détection de plot P sont défaillants : ce qui entraîne des erreurs dans les valeurs de REG.

Remarque :

Les détecteurs de signaux VFU! et VDFU! d'acquittement de freinage et de défreinage d'urgence n'entrent pas dans l'analyse de sécurité. En effet, en supposant que les défaillances de tels détecteurs sont du type collage, on peut remarquer d'après le fonctionnement des mécanismes de freins d'urgence (voir réseau;fig 5b Chap. IV) que :

* Quelle que soit la valeur de VFU!, on reste soit à l'état sûr (place F'2 marquée) : maintien de la commande de freinage, soit à l'état représenté par le marquage de F'4 (fonctionnement normal).

.../...



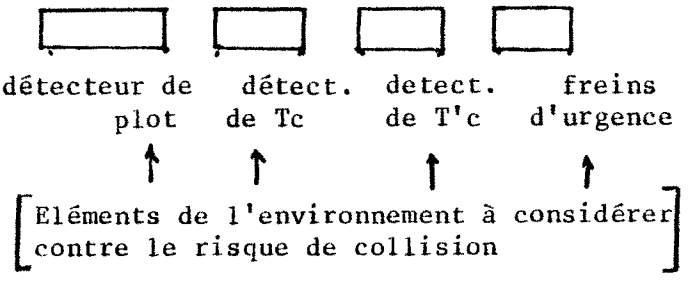


Fig.3 Bloc anti-collision

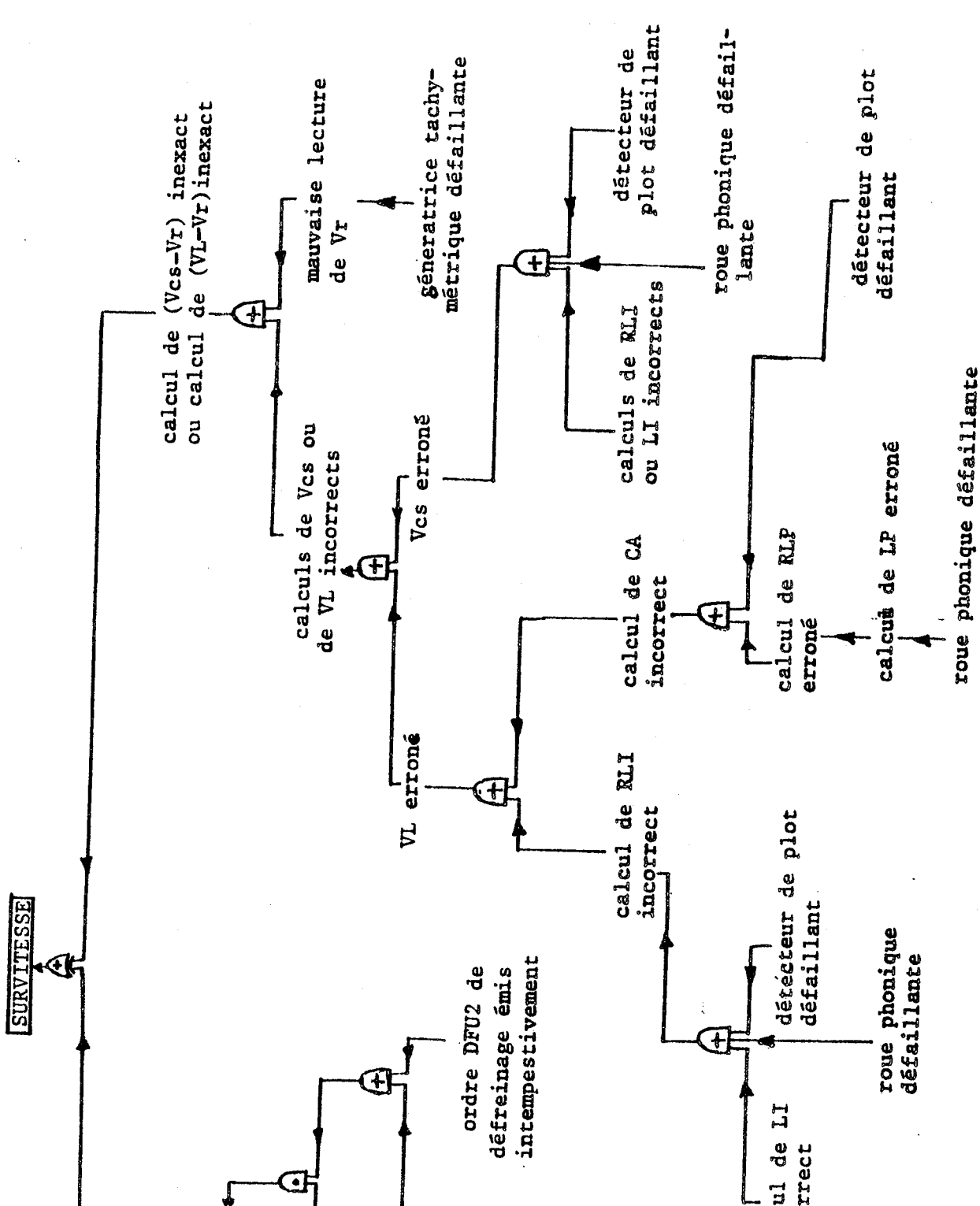


Fig 4 Arbre ASUR (Risque de survitesse)

* Dans le cas critique où REG $\leq$ 18, quelle que soit la valeur de VDFU1, on va vers les états sûrs (représentés par les marquages de F'1 ou F'2).

Tous ces résultats sont représentés sur l'arbre des causes ACOL (fig 2). Le bloc fonctionnel correspondant comprend tous les éléments entrant dans l'analyse (fig 3).

II. 2- Etude du risque de survitesse en ligne.

Ce risque a lieu si l'une des conditions suivantes est vérifiée:

1- La commande de freinage d'anti-survitesse (FU2) n'a pas été donnée, sachant que le calcul de (Vcs - Vr) est correct (pour une phase de décélération), ou le calcul de (V_L - Vr) correct (pour une phase d'accélération ou de palier).

2- La commande FU2 est correctement émise, mais par suite d'une panne quelconque, la commande de défreinage DFU2 est donnée intempestivement ce qui annule la commande de freinage FU2.

3- Les calculs de Vcs ou V_L sont erronés.

L'examen du modèle fonctionnel nous donne facilement la liste des causes possibles d'un calcul erroné de Vcs, Vr, ou V_L.

Comme dans le cas précédent, le risque de survitesse peut avoir lieu si les éléments suivants de l'Environnement sont défaillants :

- Roue phonique
- Détecteur de signal de plot
- Génératrice tachymétrique
- Freins anti-survitesse

Ces résultats sont représentés sur l'arbre des causes (ASUR) (fig 4).

.../...

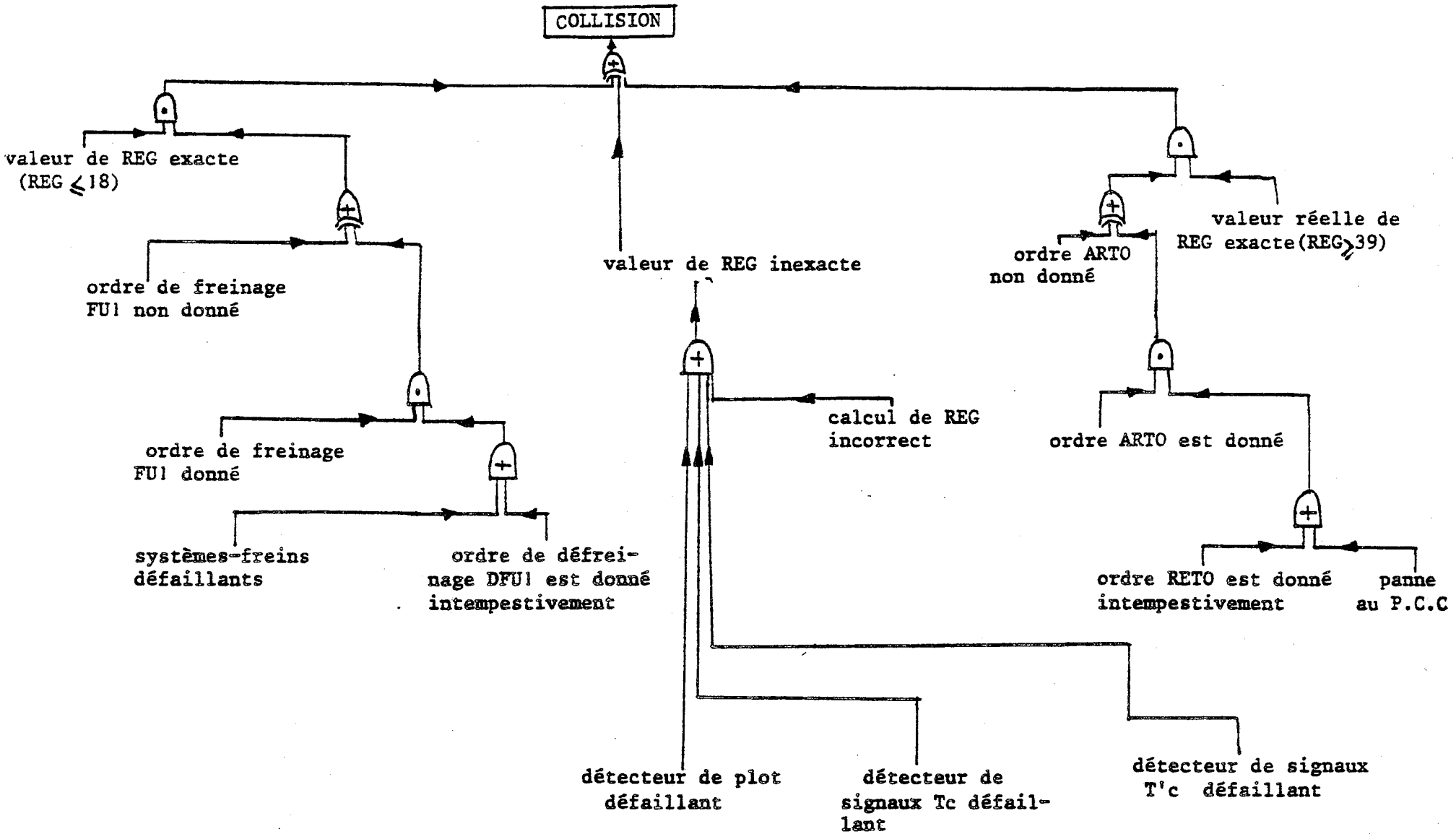


Fig 2. Arbre ACOL (risque de collision)

Le bloc fonctionnel correspondant doit comprendre tous les éléments intervenant dans l'analyse de ce risque (fig 5) :

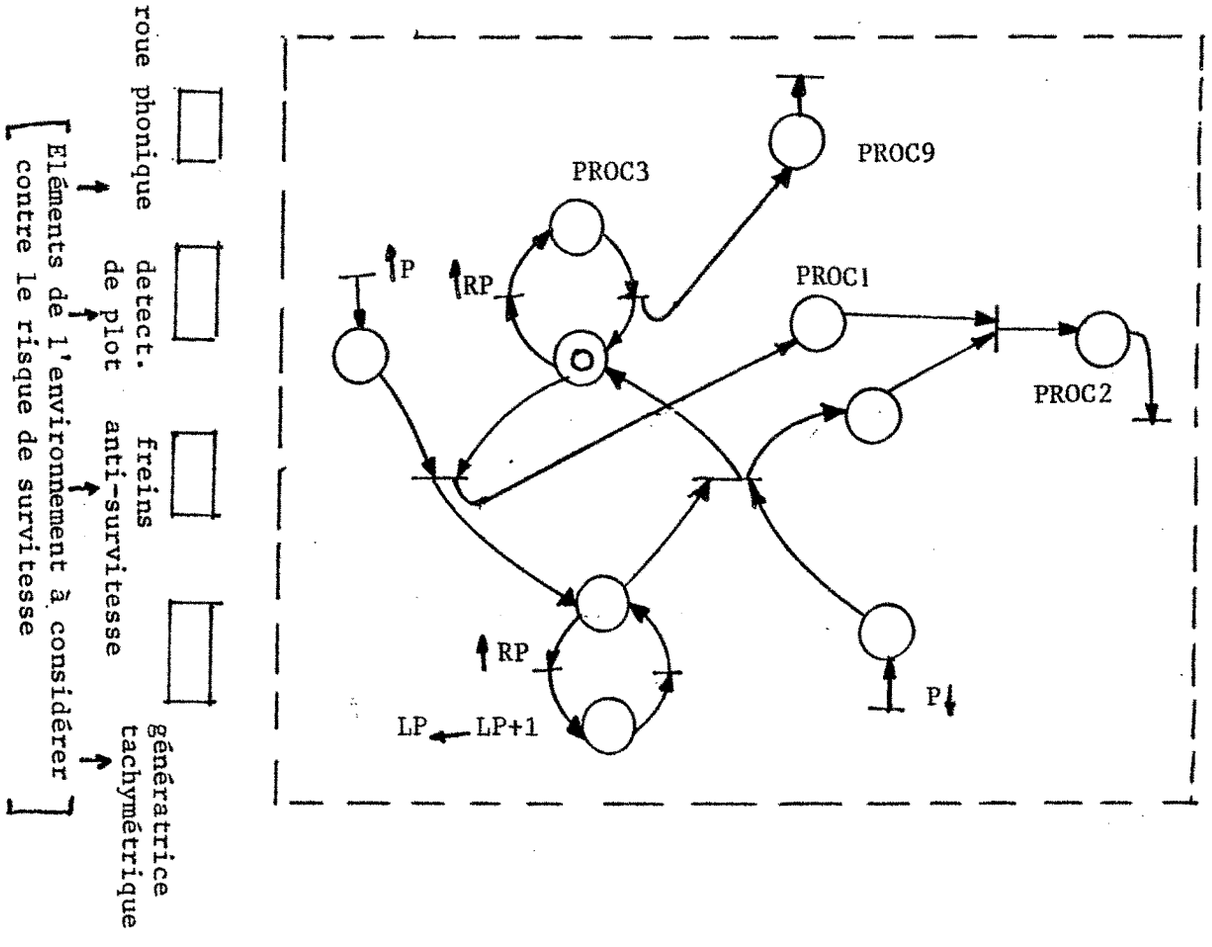


Fig.5 Bloc anti-survitesse

Remarque :

Comme il a été dit pour les détecteurs de signaux VFU1 et VDFU1, les détecteurs de signaux VFU2 et VDFU2 n'entrent pas dans l'analyse de sécurité (on se trouve toujours soit dans un état sûr, soit dans un état correspondant au fonctionnement normal du système).

II.3) Etude du risque de mauvaises commandes d'ouverture et de fermeture des portes.

Le risque de commande d'ouverture des portes du véhicule en ligne peut être dû à une commande intempestive de COP *

Une fermeture prématurée des portes du véhicule alors que celui-ci se trouve en station peut être due soit à une commande intempestive de CFP *, soit à un mauvais comptage de la variable CAS, soit à une panne de l'horloge de gestion de stationnement (T_c').

Par ailleurs, par suite d'une panne quelconque, il est possible que l'ordre de défreinage soit donné d'une manière intempestive : on pourrait se trouver alors dans une situation où la rame partirait les portes ouvertes.
L'analyse du risque d'ouverture intempestive des portes du véhicule fait donc intervenir le mauvais fonctionnement des commandes de défreinage; ceci nous amène à considérer comme bloc correspondant le bloc représentant le fonctionneme du P.A en station (confirme l'hypothèse du § II.I). On prendra alors comme objectif de sécurité du fonctionnement en station, celui correspondant à λ_p (taux de panne des portes):

$$s_3'(t)=s_3(t) \geqslant e^{-6,2\times10^{-6}t} \quad \text{pour } 0 \leqslant t \leqslant 1,58\times10^{6} \text{ heures}$$

De la même manière qu'on l'a fait pour l'analyse des risques de collision en ligne, et de survitesse, l'analyse précédente ne peut être complète que si l'on étudie aussi l'influence de l'état incorrect du fonctionnement des éléments de l'environnement, intervenant dans le fonctionnement du P.A en station. On suppose le fonctionnement du P.A correct.

* Détecteur du signal d'arrivée en station PVS :

Supposons qu'il existe une panne du détecteur de PVS (par exemple une panne de type collage); on peut se trouver alors dans la situation suivante : la rame arrive à vitesse lente, mais ne détecte pas la station.

Par ailleurs, comme l'ordre de freinage ne peut être donné, la rame reprend sa marche sans s'arrêter en station, sans pour autant causer un risque d'un accident.(L'incident à considérer correspond à la non ouverture des portes et au non débarquement des voyageurs).

On peut donc ne pas considérer le détecteur de PVS dans une analyse de sécurité.

* Il en est de même du détecteur du signal E (réponse de l'asservissement)

* Détecteur du signal de vérification d'ouverture des portes PVO :

Pour une panne du détecteur du signal PVO, on voît d'après le modèle fonctionnel du système que la rame reste bloquée et ne pourra pas reprendre sa marche. Or dans le système V.A.L tel que nous l'avions considéré, l'état d'arrêt d'une rame en station pendant un temps dépassant son temps de stationnement normal n'est pas sûr (risque de collision avec une autre rame arrivant à la station).

Le détecteur de PVO est donc à considérer dans une analyse de sécurité.

* Il en est de même du détecteur de signal PVF de vérification de fermeture des portes du véhicule, du détecteur de VFU3 et celui de VDFU3, et aussi du détecteur de l'horloge T'_c . (fig 6)

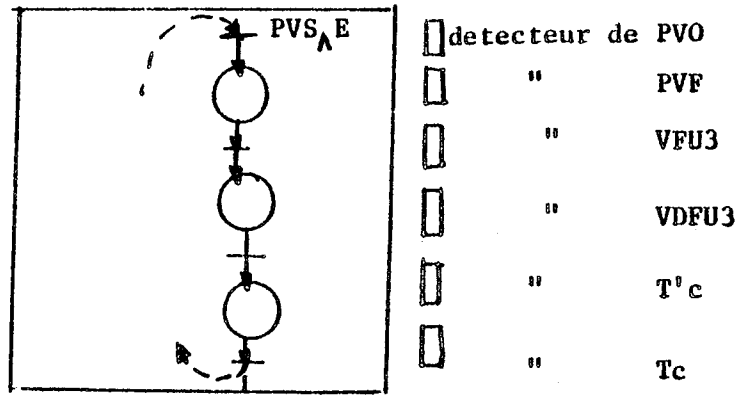


Fig. Bloc station

Conclusion :

Cette analyse de la sécurité du système met en évidence une décomposition en blocs de sécurité :

- Un bloc-station assurant le bon fonctionnement du P.A en station, et une surveillance des commandes d'ouverture ou de fermeture des portes
- Un bloc anti-collision en ligne et en station
- Un bloc anti-survitesse

Inversement, quel que soit le fonctionnement (correct ou incorrect) des parties réalisant le calcul de Ve ou de Vc, et si les blocs de sécurité cités ci-dessus sont supposés implantés sur un ou plusieurs matériels suffisamment fiables, alors les sécurités demandées par les spécifications opérationnelles du Cahier des Charges peuvent être obtenues à condition que les différents éléments de l'environnement ayant intervenu dans l'analyse de sécurité soient fiables : pour ces éléments, on pourrait par exemple utiliser une méthode classique de redondance matérielle.

En tout cas, cette étude montre l'influence de l'environnement sur la sécurité d'un système.

VII - CONCLUSION GENERALE

La complexité du système étudié nous a montré à quels points sont difficiles :

- une description exacte d'un système de commande en temps réel, et
- une analyse détaillée de ses spécifications

L'étude a par ailleurs mis en valeur une méthodologie d'analyse, laquelle peut être appliquée à une grande gamme de systèmes de commande en temps réel; les différentes étapes en sont :

1. Décrire le système dans un langage courant, en spécifiant les différentes fonctions à réaliser.

2. Représenter chaque fonction séparément à l'aide de GRAFCETS, avec l'interprétation étendue aux systèmes de commande en temps réel, sans se soucier des problèmes de synchronisation avec les autres fonctions du système. Une telle représentation est relativement simple, puisqu'il s'agit de fonctions peu complexes.

   Les étapes 1 et 2 sont complémentaires : elles permettent une bonne assimilation du fonctionnement du système.

3. Analyser chaque GRAFCET obtenu :

   . en précisant les valeurs initiales des différentes variables, la nature des signaux, ainsi que les échéances de début et de fin de chaque fonction ou sous-fonction

   . en mettant en évidence les situations de conflit ou de blocage : étudier alors l'exclusion mutuelle, les priorités, le partage d'une même variable par deux processus; vérifier la non simultanéité de lecture et écriture d'une même variable
   Cette analyse permet de retourner maintes fois vers les spécifications initiales.

   . et en distinguant les divers évènements externes qui doivent être pris en compte : doit-on considérer toutes leurs occurrences ou peut-on en tolérer la perte de quelques-unes ?

.../...

4. Passer du GRAFCET au Réseau de Pétri Interprété en étudiant :

   . les relations de dépendance dues à la présence de variables communes dans les différents grafcets (variables internes, états φ d'activité d'étapes), ces relations pouvant être résumées sur un graphe de dépendance. Cette étude doit se faire en posant pour chaque variable la question suivante : Quand doit-on la modifier ? Est-ce qu'une telle modification a été précisée dans les spécifications initiales ?

   Pour chaque variable, la synchronisation doit en outre en vérifier la séquentialité "Ecriture-lecture".

   Il est bien entendu que dans cette étude, on doit respecter les contrain imposées par l'analyse faite sur les Grafcets séparés (évènements à pren dre en compte). Cette partie permet de compléter les spécifications du Cahier des charges au niveau du fonctionnement global du système.

   . Les dépendances dues aux entrées externes communes :

   Le compactage de certaines fonctions permet d'obtenir un modèle fonction relativement simple où les tâches sont ordonnancées, et où l'influence d l'Environnement extérieur est mise en évidence.

5. Etablir toutes les conditions nécessaires, caractérisant les fréquences maximales instantanées des divers évènements et les durées des différentes tâches à exécuter par le système, et nécessaires pour que le modèle fonctionnel obtenu soit effectivement réalisable : l'étude des différentes relations permet de dire si la réalisation est compatible avec les spécifications ou non. La démonstration des propriétés que nous avons établie peut être utilisée dans une grande gamme de primitives compliquées.

6. A partir de là, une analyse de la sécurité peut être entamée afin de mettr en évidence les parties critiques du système.

   La phase de la réalisation matérielle peut alors commencer.

Bibliographie

(AZO 76)

M. AZOUNI, "Modélisation du pilote automatique d'un mode de transport en site propre", Rapport D.E.A., Sep. 1976, INP, Grenoble.

(AZO77)

M. AZOUNI, A. VERDILLON, "Description, Simulation and Safety of a Subway automatic control system", RR, ENSIMAG, n° 109, Oct. 1977

(AZO78)

M. AZOUNI, "Méthode d'Analyse de la sécurité d'un pilote automatique", Journée des Transports, "Pilotage automatique", IRT, Arcueil, Nov. 1978

(BLA73)

M. BLANCHARD et al, "Automatismes à séquences", Rapport DGRST n°71.7.2912 Juillet 1973

(BLA79)

M. BLANCHARD, "Grafcet ou Réseau de Pétri ?", le Nouvel Automatisme, mai 1979.

(CAM78)

P.CAMARDA, F.CORSI, A.TRENTADUE, "An efficient simple Algorithm for Fault Tree Automatic Synthesis from the reliability graph", IEEE trans on Reliability, vol 27 n° 3, Aug. 78

(GAR73)

A. CARNINO, "Mémento pour la préparation d'analyses de sûreté par arbres de défaillances", Rapport SETS, n° 14, CEA, Mai 1973.

(CHA74)

P. CHATTERJEE, "Fault-tree Analysis : Reliability theory and Systems Safety Analysis", Ph. D.Thesis, Calif. Univ., Nov. 1974.

(FUS74)

J.B. FUSSEL et al, "Fault Trees, "a state of the art Discussions," IEEE Trans on Reliability, vol 23, n° 1, April 1974, pp 51-55.

(GAB73)

R. GABILLARD, "Automatisme du VAL, Revue "Rail International", Mars 73.

(GAB74)

R.GABILLARD, "Réflexions sur l'applicabilité aux modes de Transports nouveaux de l'étude de la sécurité dans les modes actuels du B.C.E.O.M., Rapport n° 73000 35 USTL-Ministère Transp.

(GAR77)

S. GARRIBA et al, "An Efficient Construction of Minimal Cut Sets from fault-trees, "IEEE Trans on Reliability, vol 26, n° 2, June 77, pp 88-93.

(GOL75)

J. GOLDBERG, "New problems in Fault Tolerant Computing", FTC5, June 75, Paris, pp 29-34.

(GRA77)

Groupe de travail "Systèmes Logiques de l'AFCET, "Pour une représentation normalisée du Cahier des Charges d'un automatisme logique", Automatismes industriels, n° 61, Nov. 77.

(HEN76)

E.J. HENLEY, "Systems Analysis by Sequential Fault Trees," Microelectronic and Reliability", vol 15, 1976, pp 247-248.

(LAPR75)

J.C. LAPRIE, "Prévision de la sûreté de fonctionnement des systèmes numériques réparables", thèse d'Etat, INP Toulouse 1975.

(LAP75)

S.A. LAPP et al, "Computer aided Synthesis of Fault Trees", IEEE trans. on Reliability, April 1977, pp. 2-12.

(MOA76)

M. MOALLA, "L'approche fonctionnelle dans la vérification des Systèmes Informatiques. Proposition d'un ensemble de méthodologies. Thèse Dr-Ing, Grenoble, Déc. 76.

(MOA78)

M. MOALLA, J. PULOU, J. SIFAKIS, "Réseaux de Pétri Synchronisés, RR, n° 80, ENSIMAG, Sep 77.

(PET77)

J.L. PETERSON, "Petri Nets", Computing Surveys, vol. 9, n° 3, Sep. 77, pp. 223-252.

(RAL73)

J.C. RALITE, "LE V.A.L. : Transport en commun automatique"
Revue "Rail International, Mars 1973.

.../...

(RAM73)

C. RAMCHANDANI, "Analysis of asynchronous Concurrent Systems by timed Petri Nets", Ph. D. Thesis, MIT, July 73.

(SIF77)

J. SIFAKIS, "Réseaux de Pétri temporisés", RR n° 68 , ENSIMAG, 1977.

(VAL78)

R. VALETTE, Etude comparative de deux outils de représentation Grafcet et Réseau de Pétri". Le Nouvel Automatisme", Mai 1979.

(1YEL75)

T.W. YELIMAN, Comments on fault-trees, IEEE Trans on Rel. vol 24, n° 5, Déc. 75

(2YEL75)

T.W. YELIMAN, "Event-Sequence Analysis, Proc 1975 Annual Reliability and Maintainability Symp. pp. 286-291.

dernière page de la thèse

AUTORISATION DE SOUTENANCE

VU les dispositions de l'article 3 de l'arrêté du 16 Avril 1974,

VU les rapports de présentation de :

- Madame G. SAUCIER, Professeur à l'Institut National Polytechnique de GRENOBLE

- M. LEMAITRE, Directeur au CERT/DERA - TOULOUSE -

Monsieur Mahrez A Z O U N I

est autorisé à présenter une thèse en soutenance pour l'obtention du diplôme de DOCTEUR-INGENIEUR, spécialité "Génie Informatique".

Grenoble, le 11 Décembre 1979

Le Président de l'I.N.P.G.

Ph. TRAYNARD
Président
de l'Institut National Polytechnique