

N° d'ordre : 335

50376
1983
169

50376
1983
169

THÈSE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNIQUES DE LILLE

pour obtenir le titre de

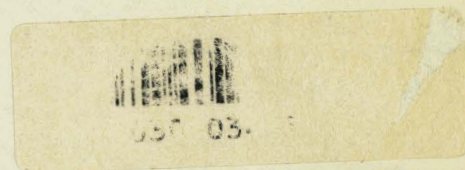
DOCTEUR INGENIEUR

par

Jean-François DHALLUIN

Ingénieur CNAM

**COMMANDE-CONTROLE DE PROCESSUS EN
SECURITE APPLICATION A LA COMMANDE D'UN
ENSEMBLE DE PORTES VEHICULE D'UNE RAME
DE METRO DE TYPE VAL**



Soutenu à Lille le 16 Décembre 1983 devant la Commission d'Examen

Membres du Jury :

R. GABILLARD
P. DEGAUQUE
M. STAROSWIECKI
Y. DAVID
D. FERBECK
M. FICHEUR
J.P. PERRIN

Président Rapporteur
Examineur
Examineur
Invité
Invité
Invité
Invité

Ce travail de recherche a été effectué au Laboratoire de Radiopropagation Electronique de l'Université des Sciences et Techniques de Lille sous la direction de Mr le Professeur Gabillard.

Je tiens à lui exprimer ici mes plus vifs remerciements pour les conseils judicieux qu'il m'a prodigués et pour l'opportunité qu'il m'a offerte en me proposant de travailler dans son Laboratoire sur un sujet aussi passionnant que celui de la sécurité des systèmes.

Messieurs les Professeurs Pierre Degauque et Marcel Staroswiecki ont bien voulu juger mon travail et participer à mon jury qu'ils en soient remerciés.

Je remercie également Monsieur Michel Ficheur Chef du Département Transports Urbanisme et Logement du Ministère de la Recherche et de l'Industrie du grand honneur qu'il me fait en participant au jugement de ce travail.

Cette recherche n'aurait pu être menée à bien sans l'aide financière apportée par le Service Métro de l'EPALE, qu'il me soit permis de remercier Monsieur Boudier son Directeur.

J'exprime ma profonde reconnaissance à Monsieur Jean-Paul Perrin Chef des Etudes Techniques de la RATP et à Monsieur Daniel Ferbeck Directeur du Service Systèmes de Transports de la société MATRA d'avoir accepté de venir apporter leur précieux jugement à ce travail voué à un transfert technologique vers l'Industrie des Transports.

Je tiens à remercier également Monsieur Yves David Directeur du Centre de Recherche et d'Etude sur les Transports Automatisés de l'honneur qu'il me fait en participant à mon jury.

Je désire aussi remercier de leur aide précieuse les services techniques et administratifs du Laboratoire, notamment Mlle Cuvelier et Monsieur Broquet, ainsi que les nombreux étudiants E.E.A. et élèves ingénieurs de l'EUDIL et de l'IDN qui ont participé avec beaucoup de dynamisme à l'élaboration de ce projet.

SOMMAIRE

Introduction

Première partie

Commande-contrôle de processus en sécurité

- I Considérations générales sur les problèmes de sécurité
- II Commande de processus en sécurité. Mise en oeuvre de systèmes microprocesseurs
- III Détection des défauts de fonctionnement sur les systèmes microprocesseurs
- IV Conclusion de la première partie.

Deuxième partie

Commande-contrôle en sécurité d'un ensemble

de portes véhicule d'une rame de métro

- I Etude du système de porte d'un véhicule de type VAL. Définition d'un dispositif de commande à microprocesseur
- II Définition de l'architecture micro-informatique globale de commande de porte au niveau d'un véhicule d'une rame de métro
- III Détection et analyse des pannes du processus par analyse séquentielle du vecteur d'état
- IV Etude de la mise en sécurité des cartes de commande de porte
- V Conclusion générale

Annexes

Table des matières

Bibliographie

I N T R O D U C T I O N

-O-O-O-O-O-O-O-O-O-

Notre décennie sera sans doute marquée par une mutation profonde de l'économie mondiale et par conséquent par une modification nécessaire de l'appareil économique.

Les tendances qui s'en dégagent sont de deux ordres ; développement de nouvelles techniques de production d'énergie et orientation de la production vers une automatisation accrue, la robotisation. Les principales fonctions attendues des automatismes concernent l'accomplissement à grande cadence et à haut niveau de qualité de tâches répétitives, et la mise en oeuvre de procédés de fabrication ou de transformation de la matière dans un environnement hostile à l'être humain.

Globalement le niveau de technicité s'est considérablement élevé notamment grâce à la pénétration de la micro-informatique.

Toutefois la mise en oeuvre d'automatismes ne peut plus, dans la plupart des cas, se concevoir sans la prise en compte de fonctions de sécurité. Sécurité pour les utilisateurs mais aussi pour l'environnement (pollution).

Le travail qui nous a été confié vient s'inscrire dans cette ligne de pensée. Il s'agit de la commande-contrôle de processus en sécurité. L'application proposée trouve son origine dans le domaine des transports publics puisque le processus à gérer consiste en un ensemble de portes véhicules d'une rame de métro.

Nous pensons toutefois que les concepts développés sont applicables à bien d'autres domaines d'activité.

L'automatisation du métro lillois, récemment mis en service public, a nécessité des efforts considérables de réflexion et la mise en oeuvre de nombreux organes de sécurité. L'absence de conducteurs dans les rames fait

reposer le problème de la sécurité des voyageurs sur des solutions purement techniques. Toute cette entreprise se justifie en partie par la qualité du service rendu par ce nouveau type de pilotage. La souplesse est telle que l'ensemble du système est capable de s'adapter aux variations rapides du flux des voyageurs, une simple intervention du poste central de commande suffit.

Les deux lignes directrices du travail que nous exposons dans ce mémoire sont orientées pour la première vers la recherche de solutions nouvelles à la conception des équipements de sécurité, à l'aide des performances des microprocesseurs disponibles sur le marché, et pour la seconde vers la mise au point de méthodes de conduites de processus dont la finalité est d'aider à la maintenabilité.

La commande-contrôle d'un ensemble de portes d'une rame de métro du type VAL pose un problème entier dans la mesure où, pour des raisons technologiques, il nous faut élaborer un véritable réseau local de commande-contrôle avec traitement et transfert d'informations de sécurité.

Avant d'aborder la conception proprement dite des dispositifs de commande il nous est paru important d'entamer une étude bibliographique portant sur la conception de systèmes microprocesseurs à haute sûreté de fonctionnement ainsi que sur les problèmes de détection d'erreurs de fonctionnement des microprocesseurs (Réf. 15).

La synthèse des publications dont nous avons pris connaissance et l'expérience que nous avons acquise sur les systèmes de sécurité du métro de Lille nous ont permis de proposer des solutions à notre problème.

L'organisation de ce mémoire reprend cette démarche. Une première partie présente sous une forme générale les problèmes de sécurité, la définition et l'évolution des processus et enfin la détection et l'analyse des pannes notamment sur les systèmes microprocesseurs. La seconde partie traite du problème de la commande de porte en particulier. Après un bref rappel du système en service sur VAL et de la définition des états de sécurité, nous développons nos solutions portant sur la réalisation d'un réseau local de commande de porte, sur la méthode de détection et de diagnostic des pannes et enfin sur la conception en sécurité d'une carte de commande de porte.

Nous attirons l'attention du lecteur sur la terminologie "commande-contrôle de processus" couramment employée dans ce mémoire. Il s'agit dans nos propos de deux fonctions distinctes commande et contrôle de processus qui, pour des raisons de sécurité dans la commande sont intimement liées.

o

o

o

PREMIERE PARTIE

COMMANDE-CONTROLE DE PROCESSUS
EN SECURITE

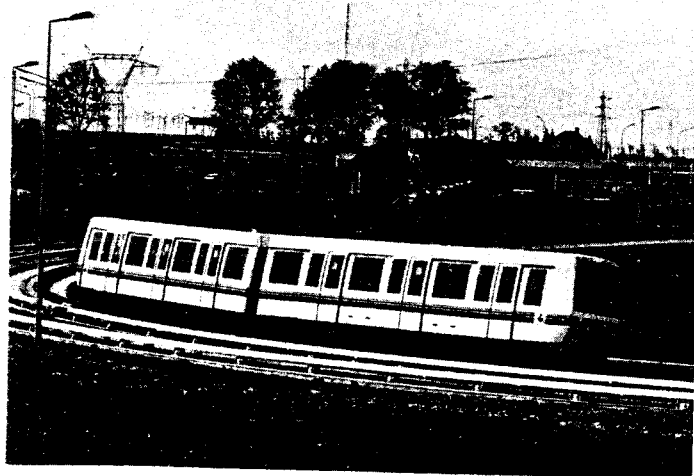


photo n° 1

BUS
LILLE

I - CONSIDERATIONS GENERALES SUR L'ETUDE DES PROBLEMES DE SECURITE

I₁ - Définition des objectifs à atteindre. Exemple du métro lillois

Le cahier des prescriptions techniques applicable au métro de Lille a basé la sécurité de ce système de transport automatisé sur l'emploi du principe de la sécurité positive.

Le concept de la sécurité positive implique une étude technologique très approfondie des éléments de sécurité, qu'ils soient mécaniques, pneumatiques, électromécaniques ou électroniques. Le principe retenu étant de démontrer qu'après une analyse très fine, aucune panne simple ou combinaison de pannes simples possédant un mode commun n'est susceptible de conduire à un accident (Réf. 53).

L'architecture des dispositifs de pilotage, ainsi que les périodicités de contrôle du bon fonctionnement des divers organes de sécurité ont été établis à partir des objectifs de sécurité, de disponibilité et en tenant compte de la fiabilité des ensembles. Les objectifs de sécurité ayant été référencés par rapport à l'expérience acquise sur d'autres réseaux de transport notamment la RATP. Afin de satisfaire à toutes ces directives, l'ensemblier du métro lillois a été amené à développer un ensemble de fonctions logiques élémentaires de sécurité répondant à la caractérisation définie ci-dessus. Chaque opérateur logique de sécurité se présente technologiquement sous forme d'un circuit hybride reconnu en sécurité intrinsèque. L'association de plusieurs opérateurs permet, moyennant le respect des règles d'assemblage, le traitement d'équations booléennes ou de fonctions séquentielles réalisant ainsi des chaînes d'action sécuritaires.

Examinons de plus près les dispositifs de pilotage automatique embarqués (PA embarqué) sur les rames de métro du VAL. Leur organisation est la suivante :

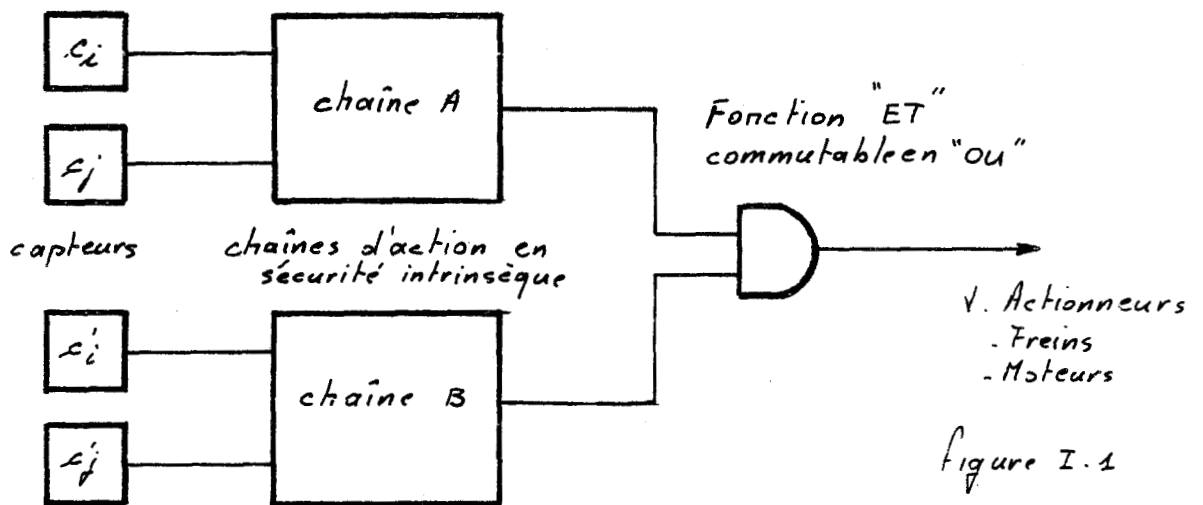
- un organe de pilotage est chargé de la gestion de l'automatisme de la rame en fonctionnement normal. La réalisation de ce dispositif fait appel à des circuits de technologie actuelle en logique micro-programmée (microprocesseurs INTEL 8085). Les fonctions de sécurité ne sont pas traitées par ce dispositif, par contre, il prend en charge l'acheminement de toutes les informations d'alarme, de télémessure et de télécommande vers le poste central de commande (PCC)

- une chaîne d'action sécuritaire, en sécurité intrinsèque, peut à tout moment et prioritairement agir sur les actionneurs et imposer au véhicule un état de sécurité (freinage d'urgence) si celui-ci sort des limites de fonctionnement imposées par la sécurité ;

De cette manière le dispositif de sécurité s'oppose de lui-même à tout disfonctionnement susceptible d'entraîner une situation dangereuse et ceci jusqu'à une erreur humaine de l'opérateur du PCC.

L'ensemble du système de pilotage que nous venons de décrire est entièrement doublé de façon à pouvoir, par commutation de redondance télécommandée depuis le PCC, maintenir le système en exploitation même en cas d'avarie sur un pilote automatique ou sur une chaîne de sécurité.

Une étude de sécurité (Réf. 5) menée par Mr le Professeur GABILLARD a montré que l'on pouvait encore améliorer la sécurité du système de transport en utilisant à tout moment les informations délivrées par les deux chaînes de sécurité selon une configuration en ET décrite par la figure ci-dessous



De cette façon, si il se produit, malgré tous les efforts de conception en sécurité intrinsèque, une panne simple contraire à la sécurité(*) sur la chaîne A ou sur la chaîne B, le circuit ET final ne délivrera pas vers les actionneurs la commande dangereuse qu'aurait fourni la chaîne en panne si on l'avait utilisée seule.

(*) panne qui évidemment aurait échappé à l'étude

A l'issue d'une discordance entre les deux chaînes, l'agent du PCC peut, après analyse, isoler le PA défectueux (mise en configuration logique ou) et continuer l'exploitation. La sécurité est alors assurée par la chaîne restant opérationnelle.

I₂ - Sécurité et sûreté de fonctionnement

Selon le domaine d'application envisagé les concepts utilisés pour garantir la sécurité d'un équipement diffèrent. Le tableau I.1 présente de façon synthétique les propos qui vont suivre.

Les transports terrestres guidés possèdent, vis-à-vis des voyageurs, un état de sécurité physiquement défini ; c'est l'état basse énergie à savoir tous les véhicules arrêtés alimentations coupées et dégagement possible des voyageurs.

En avionique ou en spatial ce cas de figure n'existe pas. La notion de sécurité est confondue avec la sûreté de fonctionnement des matériels. La sécurité est directement rattachée au bon fonctionnement des systèmes de pilotage et de tous les organes vitaux de l'appareil pendant toute la durée du vol.

I₂₋₁ - Sûreté de fonctionnement

La fiabilité d'un équipement quelconque se quantifie à un moment donné par la valeur numérique de probabilité de survie.

Les équipements électroniques ont une loi de fiabilité exponentielle bien connue (Réf. 2), l'expression de la fiabilité s'écrit

$$R(t) = e^{-\lambda_0 t}$$

avec λ_0 le taux de défaillance horaire de l'équipement

$R(t)$ la probabilité de survie à l'instant t .

Pour un dispositif électronique quelconque la sûreté de son fonctionnement se formule selon l'expression de sa fiabilité ou de probabilité de survie au terme de la mission.

DE PROCESSUS QUELCONQUE

Il n'existe pas d'état de sécurité physiquement défini pour l'utilisateur (Anionique - Spatial)

Il existe un état de sécurité (transports terrestres guidés)

Sécurité probabiliste

Sécurité déterministe

Principe de base	La sécurité repose sur la <u>sûreté de fonctionnement</u> du dispositif utilisé	Application d'un état de sécurité en cas de défaillance
Etude	<u>Analyse de fiabilité</u> (probabiliste)	<u>Sécurité Intrinsèque</u>
Quantifications	Valeur numérique de l'objectif de sécurité (probabilité) comparé avec la fiabilité du dispositif ($R(t)$)	<u>Analyse technologique</u> (Résultat déterministe) La sécurité serait absolue si on était sûr de l'étude de sécurité (test exhaustifs etc.)
Cas généralement rencontré	Objectif de sécurité incompatible avec les valeurs de fiabilité	Impossibilité de parvenir à la sécurité Intrinsèque (pannes non détectables etc...)
Moyen utilisé pour mettre en sécurité	Mise en sécurité de l'équipement par redondancement du matériel Redondance parallèle des matériels haute sûreté de fonctionnement * pas d'état de sécurité	Redondancement des organes déterminants pour établir l'état de sécurité * utilisation de l'état de sécurité
Contraintes d'exploitation	Maintenances périodiques préventives Renouvellement des matériels	Maintenances périodiques préventives Vérification du bon fonctionnement (pendant la durée de vie utile au-delà) renouvellement
	Sécurité probabiliste	
Utilisation des systèmes micro-programmés	Réalisation de dispositifs microprocesseurs redondants en auto commutation de redondance - haute sûreté de fonctionnement * pas d'état de sécurité	Dispositifs microprocesseurs de commande contrôle de processus en sécurité * utilisation de l'état de sécurité
Contraintes d'exploitation	Maintenances périodiques préventives de certains organes Renouvellement (comparateurs voteurs)	Messages d'appel à une maintenance curative en cas de panne



Les solutions employées pour tenir ces engagements font appel à des matériels de haut niveau de qualité (minimisation de λ_0) et dont on connaît le cycle de vie (figure I.2), l'expression de $R(t)$ n'étant applicable que pour la période de durée de vie utile de l'équipement.

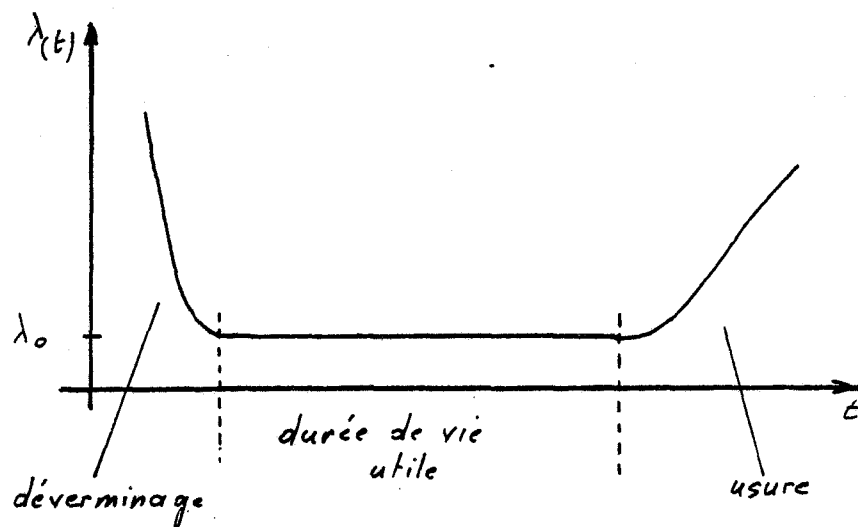


Figure I.2

La sécurité se quantifie sous la forme d'une valeur probabiliste (sécurité probabiliste).

Généralement les équipements ont une telle sophistication qu'il est indispensable de les redondancer. L'architecture choisie est telle que l'on réduit la probabilité de défaillance de l'ensemble par association de chaînes d'action en parallèle ou redondance parallèle (Réf. 2 - annexe 1).

La sécurité probabiliste implique de la part de l'utilisateur une contrainte majeure consistant en la nécessité de réviser (renouveler) périodiquement les matériels dans l'optique de maintenir un niveau de fiabilité compatible avec les objectifs de sécurité.

I₂₋₂ Existence d'un état de sécurité

Lorsqu'un état de sécurité existe, la démarche est différente. On peut, en cas de défaut, faire usage de cet état. Le problème consiste alors à bâtir un dispositif de commande capable de prendre de lui même, à l'issue

d'une panne, un état de sécurité défini au préalable. Physiquement l'état de sécurité se réfère à un état de basse énergie, répondant ainsi à un concept plus général de sécurité positive (Réf.54).

L'application de ce principe contraint le concepteur à entreprendre une étude technologique approfondie visant à prendre les précautions matérielles propres à mettre son dispositif en sécurité.

Lors de la conception d'un montage, pour un type de panne considéré sur un élément, deux critères sont à observer au choix.

-1- Il faut éviter que cette panne ne se produise (mode de panne démontré technologiquement comme impossible à l'aide d'investigations physico-chimiques)

-2- Si on ne peut éviter la panne, il faut étudier ses conséquences sur le fonctionnement du montage et s'arranger pour que la perturbation engendre un mode de fonctionnement tel que la sortie prenne l'état de sécurité (basse énergie). Cette contrainte est lourde de conséquence. Elle doit être appliquée à tous les types de pannes possibles sur tous les éléments du montage. La présence d'une panne non détectée (*) n'est tolérable que dans la mesure où, combinée avec toutes les autres pannes cataloguées, elle conduit à un mode de fonctionnement sécuritaire.

Une étude de ce genre est pour nous très pénalisante pour le concepteur, elle ne peut s'appliquer qu'à des structures à nombre limité de composants et pour lesquels la technologie est parfaitement maîtrisée.

Si la prise en compte de l'un des deux critères définis ci-dessus est applicable sur tous les éléments du montage le concepteur est alors parvenu à réaliser une structure en sécurité intrinsèque. Une chaîne d'action réalisée uniquement à l'aide de fonctions en sécurité intrinsèque, présente une sécurité absolue mais uniquement dans la mesure où l'on est certain d'avoir mené l'étude de sécurité de façon rigoureuse et exhaustive.

La sécurité intrinsèque ne nécessite aucune opération de maintenance préventive (si on ne s'occupe que de la sécurité) attendu que l'on connaît le comportement du dispositif en cas de panne (sécurité déterministe).

(*) ou panne dormante

Compte tenu de la complexité du problème ainsi posé, il n'existe pas forcément, pour une fonction à concevoir, de solution en sécurité intrinsèque. La difficulté étant d'éliminer les pannes dormantes, ou encore d'obtenir des modes de fonctionnement, en présence de panne, suffisamment différents du mode nominal, pour être détectés sans ambiguïté. Le concepteur se voit alors obligé pour mettre son dispositif en sécurité de revenir vers un concept probabiliste où l'on redondance les éléments déterminants pour la sécurité, et où l'utilisateur a pour contrainte de vérifier périodiquement leur bon fonctionnement.

Il est à noter l'effort important entrepris par le maître d'ouvrage du métro de Lille pour réaliser en sécurité intrinsèque les chaînes d'action disposées dans les équipements de pilotage fixes et embarqués.

I₃ - Evolution de la technique, mise en oeuvre de structures microprogrammées

Les progrès constants de la micro-informatique, tant en ce qui concerne la performance des produits que leur fiabilité, amènent les concepteurs d'équipements de sécurité à aborder le problème de façon différente.

Les motivations de cette remise en question résident en quatre points :

- simplification des systèmes (volume de circuiterie)
- simplification, voire disparition, de certaines maintenances préventives sur lesquelles s'appuie la sécurité
- amélioration des résultats de disponibilité par tolérance aux fautes
- accroissement de la souplesse et des performances.

Plusieurs réalisations ont déjà vu le jour en matière de signalisation et de pilotage automatique de systèmes de transport et dont la sécurité est gérée par microprocesseurs (Réf. 6-7-8-10).

Les concepts appliqués font appels aux possibilités de dialogue et d'autotest des unités de traitement.

Sur le plan matériel les structures s'apparentent selon le cas :

- à un système microprocesseur unique en autotest en comparaison avec une logique câblée extérieure
- à une redondance simple du système avec comparateur
- à une redondance multiple avec vote majoritaire.

Les logiciels sont évidemment conçus en relation avec la structure matérielle qui les exécute. Ils sont au même titre que le matériel, déterminants pour la sécurité. Les procédés suivants sont utilisés :

- dédoublement de la fonction ou redondance logicielle
 - * un processeur unique compare des résultats calculés de deux façons différentes
 - * plusieurs programmes indépendants traitent la même tâche, ils peuvent être exécutés par des microprocesseurs différents avec décorrélation dans le temps
- traitement de la synchronisation et des échanges de données
- utilisation du temps disponible pour assumer un autotest fonctionnel.

Le problème le plus important posé par le logiciel est celui de sa certification. Celle-ci impose l'emploi de méthodes rigoureuses d'analyse, (programmation structurée) et d'outils d'aide au développement et de la mise au point des programmes de la façon la plus exhaustive possible.

L'utilisation des microprocesseurs pour la réalisation de chaînes d'action en sécurité ou de systèmes de commande de processus en sécurité se justifie par la possibilité d'emploi d'une intelligence artificielle très spécifique appliquée à l'auto surveillance des matériels.

La notion de sécurité intrinsèque vue précédemment n'est pas immédiatement transposable. Comme nous le verrons plus loin (1ère partie, paragraphe III) on ne peut aujourd'hui concevoir la fabrication d'un microprocesseur en sécurité intrinsèque compte tenu du nombre excessivement grand de composants actifs intégrés.

Par contre le concepteur peut, moyennant une démarche intellectuelle traduite en logiciel, établir le diagnostic du fonctionnement de son système, et s'arranger pour que en cas de défaut on modifie de façon significative le comportement du système microprocesseur.

Le problème de sécurité se ramène dans ce cas à mettre au point des procédures de détection et d'analyse des pannes couvrant l'ensemble des matériels (système microprocesseur, circuiterie extérieure, processus) et à quantifier le taux global de couverture des pannes.

Comme postulat nous considérons que le taux de couverture des pannes d'un ensemble en sécurité doit tendre asymptotiquement vers 1 ou vers la certitude d'avoir testé l'ensemble des matériels.

A l'issue de la détection d'une panne, deux actions peuvent s'envisager selon le domaine d'application envisagé.

-1- L'ensemble du dispositif se reconfigure de telle façon que la fonction souhaitée soit traitée par une autre unité de fonctionnement, ceci suppose une redondance totale des équipements. Le dispositif est alors à haute sûreté de fonctionnement (voir annexe 1, Réf. 15-20).

-2- Le dispositif peut prendre de lui-même un état de sécurité, (à basse énergie) vue des sorties vers les effecteurs. C'est cet aspect du problème que nous développons dans les paragraphes suivants et notamment en seconde partie. Notons que cette seconde disposition n'exclue pas la première.

En fait les contraintes d'exploitation du processus, (existence ou non d'un état de sécurité), les objectifs de disponibilité et la fiabilité des matériels déterminent le type d'architecture du système à mettre en oeuvre et donc le volume des équipements.

L'apport notable présenté par les structures microprogrammées réside dans le fait que l'on peut à partir de procédures de test bien adaptées vérifier de façon exhaustive le bon fonctionnement d'un ensemble d'organes. Ceci peut se réaliser avec au départ des choix technologiques moins critiques puisqu'il suffit de mettre en relation le catalogue des pannes possibles avec la procédure de test.

*I₄ - Adaptation de l'architecture globale en fonction du processus à commander.
Réseau local de commande-contrôle en sécurité*

La détection puis l'utilisation des informations de pannes pour une reconfiguration du matériel constituent nous l'avons dit une particularité offerte par les systèmes microprogrammés. Si le processus à commander est localisé en un endroit connu et invariable de l'espace, le traitement de ces informations se fera par un dispositif lui-même localisé en relation directe avec un opérateur humain à qui revient la responsabilité de l'exploitation.

La gestion des portes véhicule d'un système de transport automatisé du type VAL pose le problème de façon différente.

La répartition dans l'espace d'un véhicule des portes d'accès des voyageurs, de même la répartition sur la ligne de transport de l'ensemble des rames en service, pose le problème du traitement en sécurité de toutes les informations "portes véhicules".

Il y a donc lieu de créer un dispositif de traitement décentralisé et de lui adjoindre, comme pour le reste, des contraintes de sécurité.

Dans ce cas, avec le souci de minimiser la dimension des organes de commande, et le câblage, il faut élaborer toutes les composantes d'un réseau local de commande-contrôle en s'attachant pour des raisons fonctionnelles à établir une répartition optimale des tâches ainsi qu'une hiérarchisation du traitement des informations. Autrement dit le réseau local vient mettre en place une intelligence répartie. L'objectif étant de ne transmettre aux opérateurs PCC que des informations synthétiques judicieusement utiles. La sécurité est bien gérée par les dispositifs de commande eux-mêmes, l'exploitant n'ayant pour charge que de remettre en état le système, à l'issue de la réception d'un message de panne.

Le travail que nous présentons en seconde partie (paragraphe II) prend en compte l'établissement d'un réseau local de commande de porte au sein d'un véhicule (6 mécanismes de porte). La continuation de l'étude, dans un programme de travail plus vaste, va dans le sens de la conception d'un réseau étendu à un train formé d'un nombre variable de véhicules, puis enfin des liaisons machines-voies destinées à relier l'ensemble des rames circulant sur la ligne au poste central de commande (PCC).

II - COMMANDE DE PROCESSUS EN SECURITE

II₁ - Caractérisation d'un processus. Définition des variables d'état, de sortie, et des sollicitations extérieures

Un processus quelconque peut être caractérisé par des grandeurs qu'il est classique de regrouper selon leur fonction (réf. 1). Nous apportons toutefois à cette présentation une notation particulière relative aux problèmes de sécurité.

Variables d'état. L'ensemble de ces grandeurs constitue le vecteur d'état du processus sous contrôle. Ces grandeurs, en nombre variable selon la complexité du système, sont entrées dans le dispositif de commande. Lors de l'établissement du cahier des charges il importe de dégager et de traiter avec une attention toute particulière les variables propres à caractériser le ou les états de sécurité.

Variables de sortie, ou vecteur de commande du processus. Elles sont générées par le dispositif de commande à partir du traitement des variables d'état et des sollicitations extérieures. Il convient, dans l'optique d'une commande en sécurité, d'interdire les combinaisons dangereuses des variables de sortie (réf. 23).

De par la nature des grandeurs d'état et de commande on peut distinguer deux classes de processus

- processus continus, les variables sont représentées par des grandeurs analogiques

- processus discontinus où les variables ont un format logique en tout ou rien. Les combinaisons des informations se présentent dans ce cas sous forme d'équations logiques booléennes (réf. 23-24).

Variables de commande ou sollicitation. Ces variables sont générées par le système d'exploitation. Elles sont entrées dans le dispositif de commande. L'exploitant peut être lui même un processus d'une hiérarchie plus élevée ou un opérateur humain. Il apparaît comme évident qu'à tout moment la sollicitation infligée au processus doit être propre à garantir la sécurité vue d'un niveau plus élevé. Un processus sous contrôle doit à tout moment être capable de prendre l'état de sécurité jugé bon pour le système d'exploitation.

II₂ - Evolution du processus. Etablissement d'un domaine d'évolution en sécurité. Etude de fiabilité

Les variables d'état et de commande d'un processus sont liées par relation de cause à effet selon l'évolution normale du système décrite dans le cahier des charges. Celui-ci doit clairement préciser quels sont les états de sécurité à respecter ainsi que les conditions requises pour les obtenir.

Les données fournies par le cahier des charges doivent permettre de borner un domaine à l'intérieur duquel le point de fonctionnement du processus évoluera en sécurité.

L'étude de l'évolution du processus doit tenir compte non seulement de l'évolution normale en phase de bon fonctionnement, mais aussi et surtout des conséquences sur cette évolution de l'apparition de pannes inopinées dont certaines pourraient conduire à des situations dangereuses ; franchissement des limites du domaine de sécurité.

Cette considération a plusieurs implications

* Le processus à contrôler doit dans la mesure du possible être simple ou simplifié par une décomposition en sous ensembles élémentaires, de manière à réduire au maximum la dimension des vecteurs d'état et de commande.

On réduit ainsi le nombre de phases de fonctionnement du système, l'étude de sécurité est plus aisée.

* Le concepteur doit porter une attention toute particulière sur la technologie des chaînes d'entrée et de sortie. La performance est bien sûr à prendre en compte mais aussi et surtout l'étude de fiabilité des éléments.

Etude de fiabilité

L'étude de fiabilité peut se décomposer de la façon suivante

1 - Etude des conséquences de pannes ou étude de sécurité

La connaissance des implications des pannes "possibles" des composants utilisés permet d'établir la liste des pannes dangereuses ou pannes de sécurité et des pannes non dangereuses mais contraires à la disponibilité du système.

L'évolution rapide de la technologie aidant, le concepteur est amené à introduire de nouveaux composants ou de nouvelles fonctions. Faute de certification par un organisme agréé (CNET, etc..) tous les types de pannes doivent être pris en considération.

2 - Calcul prévisionnel de fiabilité

Ce calcul est mené en vue de quantifier une probabilité de défaillance horaire correspondant à une situation dangereuse (ou contraire à la disponibilité). Généralement le calcul est mené par sommation des taux de défaillance des éléments utilisés lors de cette configuration (réf. 2).

L'étude de sécurité du dispositif de commande-contrôle peut révéler les cas de figure suivants

* La prise en compte de toutes les pannes "possibles" ne conduit à aucune phase contraire à la sécurité. Le concepteur est dans ce cas parvenu à réaliser un dispositif de commande en sécurité intrinsèque.

* Si à l'issue de l'étude de sécurité il apparaît qu'au moins une panne possible s'avère dangereuse par le fait qu'elle n'est pas détectée et/ou qu'elle conduit à une phase de fonctionnement susceptible de faire sortir le processus de son domaine de sécurité, dans ce cas le dispositif de commande n'est pas en sécurité.

Il est alors impératif de redondancer l'élément porteur de cette panne de façon à se prémunir de la panne simple et en faisant en sorte que seule une double panne, des deux éléments en redondance, puisse conduire à une situation dangereuse.

Cette précaution ne dispense pas l'exploitant de maintenir dans le temps un niveau de sécurité suffisant par vérification périodique du bon fonctionnement des organes redondancés sur lesquels repose la sécurité. Cette nécessité, très contraignante pour l'exploitation, résulte directement du fait que la panne simple "possible" n'est pas détectée.

Déterminons par calcul quelles sont les durées comprises entre deux vérifications. Si l'on compte le temps à partir de l'instant $t = 0$ où le bon fonctionnement des deux organes a été constaté une situation dangereuse ne peut survenir que si :

- 1 - l'un des deux organes (indice 1) a une défaillance non détectée entre l'instant t et $t + dt$. Soit λ_1 la probabilité horaire de défaillance de cet organe, la probabilité de l'évènement est (avec des lois de fiabilité exponentielles)

$$P_1 = \lambda_1 e^{-\lambda_1 t} dt$$

- 2 - le second organe a à son tour une défaillance pendant le temps qui reste avant la prochaine vérification périodique prévue à l'instant T . La probabilité de ce second évènement est

$$P_2 = 1 - e^{-\lambda_2 (T - t)}$$

λ_2 étant la probabilité de défaillance horaire du second organe.

Les deux éléments étant indépendants la probabilité de leur double défaillance entre 0 et T (intervalle entre deux vérifications périodiques) est donné par l'intégrale

$$P_3 = \int_0^T \lambda_1 e^{-\lambda_1 t} (1 - e^{-\lambda_2 (T - t)}) dt$$

Avec l'hypothèse

$$\lambda_1 T \ll 1 \quad \text{et} \quad \lambda_2 T \ll 1$$

P_3 devient

$$P_3 \approx \frac{\lambda_1 \lambda_2}{2} T^2$$

P_3 est la probabilité pour que le cycle de vérification périodique (période T) soit incapable d'empêcher l'apparition d'une situation dangereuse.

On peut tendre la valeur de P_3 aussi petite que l'on veut en réduisant l'intervalle T . Pratiquement on fixe la valeur de P_3 que l'on ne désire pas dépasser (cette valeur s'appelle "objectif de sécurité") et on en déduit la valeur de T

$$T \leq \frac{2P_3}{\sqrt{\lambda_1 \cdot \lambda_2}}$$

Pour fixer les ordres de grandeurs considérons, en rapport avec problème de commande de porte développé en seconde partie, les contacts électriques définissant l'état porte fermée. Afin d'assurer la sécurité il faut se prémunir de la défaillance "collage du contact en position fermé". Le remède consiste à disposer en redondance deux contacts indépendants manoeuvrés l'un par un vantail de porte, l'autre par le verrou

$$\text{soit } \lambda_1 = \lambda_2 = 0,20 \cdot 10^{-6}/\text{h} \quad (*)$$

l'objectif de sécurité attribué à un mécanisme de porte est de

$$P = 2 \cdot 10^{-6} \quad \text{Réf. (46)}$$

l'intervalle de temps T entre deux vérifications vaut alors

$$T = 9800 \text{ heures} \quad (\text{valeur majorante})$$

II₃ - Commande-contrôle de processus en sécurité par microprocesseur

L'introduction de microprocesseurs dans les dispositifs de commande de processus oriente l'étude de sécurité de façon différente.

Le traitement de fonctions de sécurité par un système microprocesseur implique à l'évidence de mettre ce dispositif lui même en sécurité.

Par définition on entend par système microprocesseur en sécurité une structure matérielle et logicielle capable de détecter ses propres défauts de fonctionnement, et capable, en cas d'avarie, de se reconfigurer façon à ne pas engendrer par rapport à son environnement des commandes ou des messages contraires à la sécurité.

Ceci nous amène à décomposer l'étude de sécurité de l'ensemble du dispositif de commande de processus en deux parties distinctes et indépendantes

(*) Les lois de fiabilité sont considérées pour notre exemple comme étant exponentielles.

- 1 - L'étude de sécurité de la commande et du contrôle du processus à partir d'un système microprocesseur en bon état de fonctionnement.

- 2 - L'étude de sécurité du système microprocesseur lui-même en vue de répondre à la définition présentée ci-dessus.

II₃₋₁ - Etude de sécurité de la commande du processus

L'étude de la commande en sécurité du processus doit envisager les implications des pannes "possibles" sur les voies de commande de mesure et sur le processus. Le but étant de respecter les limites d'évolution en sécurité du point de fonctionnement.

II₃₋₁₋₁ - Gestion d'une tâche de détection et d'analyse de panne du processus, des voies de commande et de mesure

La présence d'un système microprocesseur dans l'unité de commande autorise l'introduction d'une fonction de contrôle permanent du processus par analyse de son vecteur d'état. La finalité recherchée consiste à assumer, moyennant certaines méthodologies d'observation du processus que nous développons plus loin, une détection permanente des pannes.

Si la méthode utilisée permet de détecter toutes les pannes possibles du processus, et en considérant toujours comme hypothèse que le système microprocesseur est lui même en sécurité, c'est-à-dire capable d'établir un état de sécurité, on pourrait affirmer que la commande est réalisée en sécurité au sens de la sécurité intrinsèque. En fait deux remarques restrictives sont à considérer

- 1 - La mise en sécurité d'une unité de commande à microprocesseur ne peut se réaliser par analyse technologique à partir des modes de panne comme en sécurité intrinsèque traditionnelle. Les procédés d'étude sont différents (paragraphe III). On ne peut aujourd'hui affirmer qu'un microprocesseur est en sécurité intrinsèque. Tout au plus on peut contrôler périodiquement son bon état de fonctionnement.

- 2 - La détection et l'analyse des pannes du processus ne peut se concevoir en temps réel. Le microprocesseur ne peut en effet appréhender un défaut qu'après avoir perçu son effet. Il existe dans la plupart des cas un décalage dans le temps entre le moment où le défaut prend naissance et où il est perçu et identifié. Ceci est important car la sécurité dépend alors momentanément de la probabilité avec laquelle une phase dangereuse peut se produire durant cet intervalle de temps.

Examinons quelle est la probabilité de survie d'un équipement dont on vérifie périodiquement le bon fonctionnement.

Soit θ l'intervalle de temps séparant les tests, en supposant toujours des lois de fiabilité exponentielles, déterminons quelle est la probabilité conditionnelle pour que l'équipement testé à l'instant t soit encore en bon fonctionnement à l'instant $t + \theta$

Cette probabilité s'écrit

$$R(t, \theta) = \frac{\text{probabilité de survie en fin de mission}}{\text{probabilité de survie en début de mission}} = \frac{R(t + \theta)}{R(t)}$$

Soit pour des lois de fiabilité exponentielles

$$R(t, \theta) = \frac{e^{-\lambda_0(t + \theta)}}{e^{-\lambda_0 t}}$$

$$R(t, \theta) = e^{-\lambda_0 \theta} = R(\theta)$$

ceci pour $\lambda = \lambda_0 = \text{cte}$

La fiabilité de mission entre deux test distants de θ ne dépend plus de l'instant initial mais de l'intervalle de temps séparant les contrôles. Il est donc nécessaire de minimiser les temps de détection des pannes et de respecter l'inégalité

$$\lambda_0 \theta \ll 1$$

En pratique cette condition est toujours remplie dans la mesure où la fiabilité des équipements est bien supérieure aux cycles de détection des pannes. La durée du cycle étant celle du fonctionnement propre du processus (en activité cyclique) ou doit être imposée par l'exploitant en générant des procédures spécifiques à la détection de pannes.

III₃₋₁₋₂ - Configuration nécessaire et suffisante des vecteurs d'état et de commande

Le concepteur a pour tâche de dimensionner les vecteurs d'état et de commande en fonction des critères suivants

Vecteur de commande : il faut déterminer un nombre suffisant de voies de commande indépendantes de façon à se prémunir d'une panne simple "possible" entraînant une commande intempestive contraire à la sécurité ; critère de sécurité positive.

Vecteur d'état : celui-ci doit être dimensionné de manière à ce qu'il fournisse au microprocesseur le nombre d'informations nécessaires à la détection de "toutes les pannes possibles".

Cette condition amènera nécessairement le redondancement de certaines voies de mesure portant ou non sur des états de sécurité. La détection et la classification de certaines pannes s'opérant par comparaison des informations reçues. La duplication de certains états permet en outre de maintenir momentanément l'exploitation du processus même en présence d'une panne. (Tolérance à un défaut).

III₃₋₁₋₃ - Traitement des informations de panne

A l'issue de la détection et de l'identification d'une panne, le microprocesseur doit, pour assurer la sécurité, procéder aux actions suivantes

- Emission, vers le système d'exploitation, d'un message codé servant à la signalisation du défaut détecté

- Génération d'une commande en mode dégradé qui selon la nature et la localisation du défaut :

. immobilisera le processus dans un état de sécurité (cas des pannes généralement localisées sur les voies de commande ou sur le processus)

. continuera son exploitation apparemment normalement, dans l'optique de maintenir un bon niveau de disponibilité, mais à la condition qu'il subsiste un nombre suffisant d'informations significatives de l'état du processus permettant d'assurer sa sécurité pendant le temps nécessaire à une intervention de l'exploitant alerté par le message défini plus haut.

Il est à remarquer que la perte d'une information d'état ou d'une voie de commande ne permet plus d'assumer le traitement de détection des pannes. Le microprocesseur n'effectue plus qu'une simple commande de son processus.

La sécurité repose alors sur la probabilité pour qu'il ne se produise pas un second défaut, indépendant du premier, entre le moment où le microprocesseur émet son message de panne et où l'exploitant décide l'arrêt du fonctionnement du processus pour sa remise en état.

La valeur maximum admissible de cet intervalle de temps peut être obtenue à partir du calcul développé au paragraphe II₂.

L'exploitant s'étant fixé au préalable un objectif de sécurité à respecter.

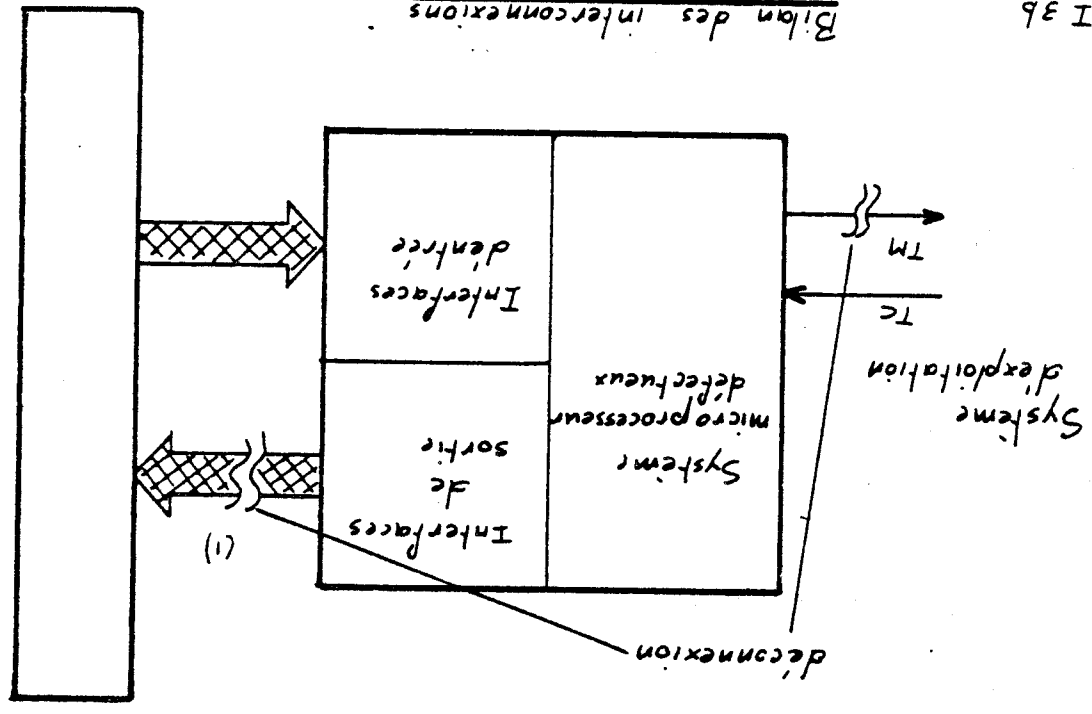
II₃₋₂ - Définition d'un état de sécurité du système de commande à microprocesseur

Notre propos dans ce paragraphe n'est pas d'aborder le problème de la mise en sécurité des systèmes microprocesseurs, (nous le développons plus loin), mais de définir et de faire appliquer au dispositif de commande un état de sécurité à la suite de la détection d'un mauvais fonctionnement de l'unité de traitement à microprocesseur.

* Etat de sécurité du microprocesseur de commande

Globalement on peut répertorier les échanges d'information entre le système microprocesseur et son environnement de la façon suivante :

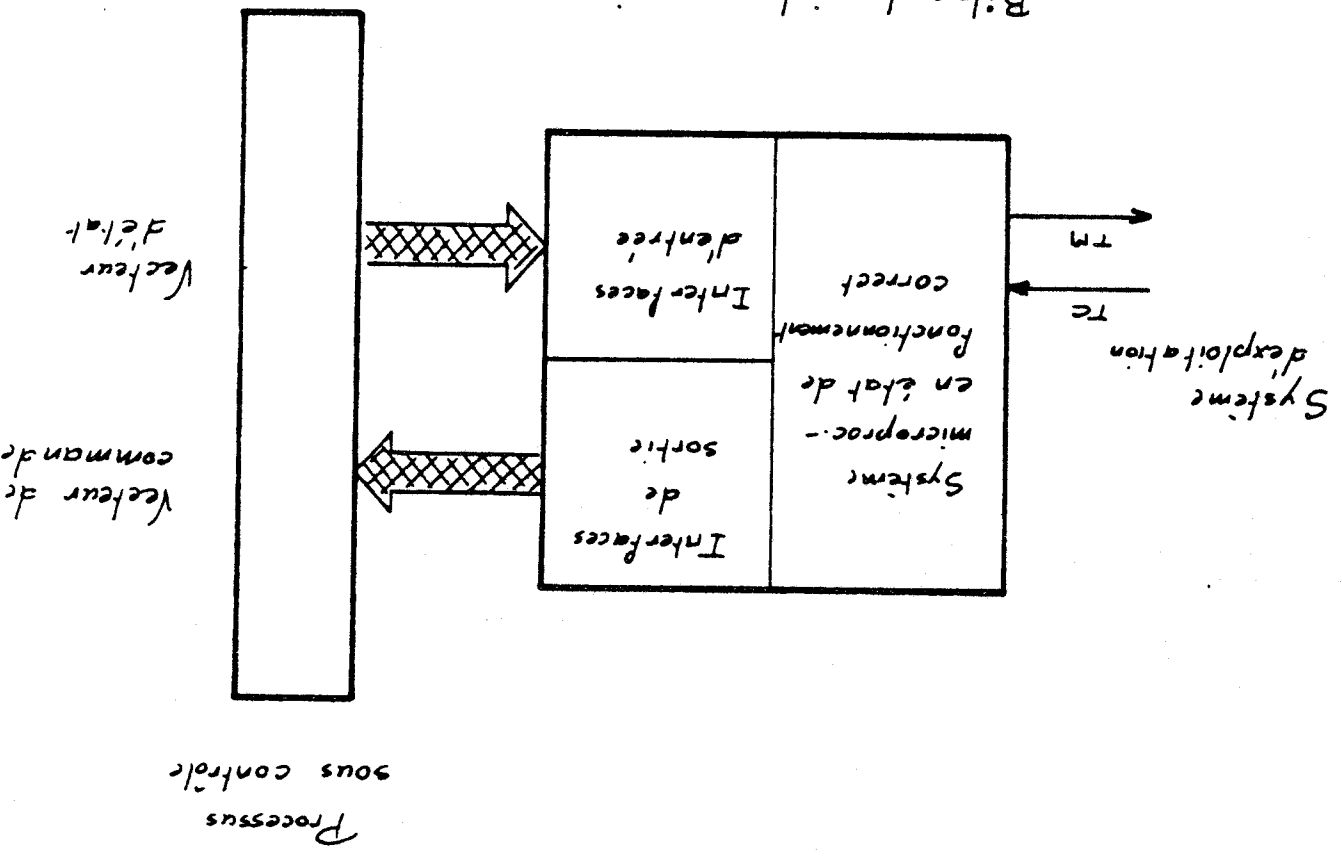
Bilan des interconnexions
en état de sécurité



(1) mot de commande statique imposant au processus un état de sécurité

Figure I.3

Bilan des interconnexions
en fonctionnement correct



Processus sous controle

Valeur d'état

Valeur de commande

- entrée de sollicitations extérieures sous forme de messages codés (série ou parallèle)

- sortie de messages codés vers le système d'exploitation, ces messages sont relatifs :

- . aux états de fonctionnement du processus en marche normale
- . aux messages d'alarme (détection de panne etc...) donc relatifs à la sécurité de la commande du processus

- entrée du vecteur d'état

- sortie d'un mot de commande pour l'activation du processus.

En cas de défaut de fonctionnement du microprocesseur il y a lieu de procéder à sa déconnexion du système. Il faut en effet se prémunir des dangers suivants : (figure I₂)

- vis-à-vis du processus : une commande intempestive contraire à la sécurité peut être engendrée à tout moment par un microprocesseur défectueux

- vis-à-vis du système d'exploitation : celui-ci peut recevoir des messages intelligibles mais non significatifs et contraires à la sécurité, capables d'induire en erreur sur la conduite à adopter.

La figure I₃ nous montre quel état de sécurité doit prendre le réseau d'interconnexion. La fonction de déconnexion du microprocesseur doit être réalisée en sécurité intrinsèque, on ne dispose plus à ce niveau de moyens de contrôle puisque le microprocesseur chargé de cette fonction est défectueux.

Sécurité par rapport à l'architecture globale d'un système de commande de processus distribué dans l'espace

L'arrêt total de l'exploitation du processus après établissement de l'état de sécurité prescrit, suffit à répondre aux objectifs de sécurité.

Toutefois par rapport à la globalité d'un système une action sécuritaire sur un sous ensemble peut s'avérer très pénalisante pour le reste. Il est dommage d'immobiliser une rame de métro pour un défaut "porte véhicule". L'absence détectable de communication avec le dispositif déficient laisse l'opérateur humain aveugle et rend caduque l'exploitation.

Il y a donc lieu d'assurer, par une liaison indépendante, l'acheminement d'un minimum d'informations caractérisant la prise en compte de l'état de sécurité infligé au processus.

II₄ - Méthodologie d'observation d'un processus en vue de détecter et de diagnostiquer les défauts de fonctionnement

Plusieurs méthodes d'observation ont été dégagées et présentées par l'équipe ADERSA - GERBIOS (réf. 1) dans le cadre d'une étude sur la surveillance et le diagnostic de processus. Quatre voies principales sont retenues.

- 1 - La procédure commune, c'est historiquement la première méthode d'observation. Un opérateur humain relève la valeur des variables et fait une estimation du fonctionnement du processus. L'objectif de détection est généralement atteint mais sans toutefois permettre la caractérisation ni la classification des pannes, voire même la distinction avec des perturbations passagères.

- 2 - Multiplexage et vote. Les voies de mesure sont redondancées. La détection de défaut est effectuée par vote majoritaire, elle est quasi immédiate ainsi que la classification des informations reçues. De plus une reconfiguration est possible.

- 3 - Modélisation - estimation d'état - test d'hypothèse :
Dans cette procédure la connaissance à priori de l'état normal du processus est résumée dans un ou plusieurs modèles statiques ou dynamiques autour d'un point de fonctionnement donné. Le modèle de l'état normal permet de prévoir l'observation à venir. La comparaison de la prédiction et de l'observation réelle est la base du principe de détection. Le diagnostic est réalisé par test d'hypothèse.

- 4 - Modélisation - identification temps réel - test d'hypothèse :
L'état de panne défini comme étant une modification des relations de cause à effet reliant les variables, on peut envisager une détection de panne par observation des relations physiques entre ces variables.

L'observation s'effectue par une identification en temps réel du processus, le diagnostic est réalisé par test d'hypothèse.

D'une manière générale il s'agit d'effectuer séquentiellement des tests d'hypothèses capables d'apprécier si oui ou non le processus est en fonctionnement conforme à sa définition et de là, de dégager une structure de décision. La décision est en général une variable aléatoire puisqu'elle repose sur des informations de pannes dont l'apparition est aléatoire. Il faut minimiser le risque d'erreur correspondant aux prises de décision. Diverses études ont permis de mettre au point des méthodologies de détection et de classification de pannes (Réf. 17 - 18 - 19).

II₅ - Conclusion

La mise en oeuvre de microprocesseurs dans les dispositifs de commande de processus en sécurité fait évoluer, nous l'avons vu, la fonction de commande vers l'association intime de deux fonctions : commande et contrôle. Les grandes possibilités de traitement d'information offertes par les composants micro-informatiques apportent de nouvelles solutions.

Si auparavant la conception d'équipements en sécurité nécessitait fréquemment de recourir à des résultats fiabilistes nécessitant des organes surdimensionnés, redondancés et dont il fallait assurer une maintenance préventive, le système de commande est à présent capable, moyennant une intelligence artificielle bien spécifique de prendre à sa charge le contrôle du bon fonctionnement de l'ensemble des éléments qui lui sont confiés.

Après avoir établi une configuration convenable des vecteurs d'état et de commande, capable de permettre au microprocesseur de détecter toutes les pannes "possibles" l'ensemble du processus est donc parfaitement contrôlé et mis en sécurité.

- La naissance d'un défaut ne diminue que très peu le niveau de sécurité et d'autant moins que la durée du cycle de détection des pannes est faible ; l'inégalité suivante est à respecter

$$\lambda_0 \cdot \theta \ll 1$$

λ_0 taux de défaillance horaire de l'équipement

θ intervalle de temps entre deux tests

- La présence d'un défaut n'a également pratiquement pas d'incidence sur la sécurité si les conditions suivantes sont respectées :

- . transmission du message de panne vers le système d'exploitation
- . remise en état de l'élément défectueux bien avant qu'une seconde panne contraire à la sécurité puisse apparaître.

- Les maintenances préventives ne sont plus nécessaires car les défauts sont identifiés et signalés peu de temps après leur apparition.

- Les choix technologiques sur les éléments de commande et de mesure sont moins critiques ; ceci pour deux raisons :

- 1 - la détection de panne est permanente, les intervalles de temps où l'on confie la sécurité à un organe sont courts

- 2 - si le vecteur d'état est bien dimensionné et les tests d'hypothèse bien effectués on peut tolérer des éléments pouvant présenter tous les modes de pannes comme possibles. En particulier il n'est plus nécessaire de disposer de contacts électriques ne pouvant jamais tomber en panne "contact fermé" comme c'était le cas des relais de sécurité traditionnels.

REMARQUE

En définitive la différence entre la méthode de mise en sécurité par redondance et vérification périodique et la méthode utilisant les microprocesseurs se réduit au seul fait que le microprocesseur effectue ces vérifications en permanence. Mais le principe reste le même.

III - DETECTION DES DEFAUTS DE FONCTIONNEMENT SUR LES SYSTEMES MICROPROCESSEURS

L'objet de ce paragraphe est de rendre compte d'une étude bibliographique concernant les procédés de détection de défauts sur les microprocesseurs (Réf. 27).

Ce problème, nous l'avons vu, est crucial à partir du moment où l'on envisage de commander en sécurité un processus à l'aide de systèmes **micro-informatiques**.

La présentation ci-dessous nous paraît importante pour deux raisons :

1 - on y pose le problème de la détection d'erreurs de fonctionnement des circuits à grande échelle d'intégration (LSI - VLSI)

2 - nous balaçons de façon non exhaustive un champs étendu d'idées et de méthodes de détection. C'est parmi ces procédés que nous avons puisé nos sources permettant de présenter un logiciel d'autotest exécuté par un microprocesseur affecté à la commande d'un processus en sécurité (2ème partie - 4ème paragraphe).

A l'issue d'une étude sur la modélisation des défauts des microprocesseurs, nous présentons une classification proprement dite des procédés de détection de panne puis quelques résultats fiables sur les systèmes microprocesseurs.

III₁ - Modes de pannes imputables aux microprocesseurs et composants associés

Il nous paraît utile de rappeler au préalable les différentes parties qui constituent une unité centrale microprocesseur. La décomposition peut se présenter de la façon suivante.

- l'unité arithmétique et logique (PLA) son format détermine généralement la classe du microprocesseur (8 - 16 bits). A cette unité est intimement associé un registre d'état
- le décodeur d'instruction
- l'unité de gestion du séquençement des opérations internes.

Cette unité gère le chaînage des actions correspondantes à une instruction donnée (opérations synchrones de l'horloge)

- l'unité de contrôle d'adressage des registres internes
- l'unité de calcul et de gestion du compteur ordinal (PC)
- une ou plusieurs unités de gestion de fonctions spéciales spécifiques au microprocesseur employé. Nous citons principalement l'unité de contrôle et d'exécution des séquences d'interruption
- enfin les interfaces électriques d'entrée-sortie du microprocesseur ou buffers. Ils réalisent la normalisation des signaux électriques envoyés et reçus par le circuit ainsi que la séparation entre les organes internes du microprocesseur et ses ressources extérieures.

Nous citons très rapidement les quelques principales fonctions environnant le microprocesseur, à savoir ;

- les mémoires vives (RAM) et morte (ROM.....)
- les périphériques pour lesquels nous retenons :
 - . les interfaces série synchrones ou asynchrones (USART)
 - . les interfaces parallèles banalisés (ports programmables)
 - . les interfaces spécifiques (GPIB - HLDC... etc)
- les boîtiers de fonction spéciales :
 - . contrôleur d'interruption
 - . compteur d'évènements ou séquenceur.

La particularité commune à toutes ces fonctions est qu'elles se présentent, vu du microprocesseur, comme des registres parmi lesquels nous retenons :

- les registres de commande, en général accessibles à l'écriture
- les registres d'état accessibles uniquement à la lecture
- les registres de données qui selon le cas seront accessibles à la lecture seule, à l'écriture, ou des 2 façons.

III₁₋₁ - Hypothèses sur l'apparition des fautes

Il est généralement admis, qu'à un instant donné, un microprocesseur peut être le siège d'un nombre quelconque de défauts. Il est tout-à-fait plausible de considérer qu'à une dégradation naissante puisse se joindre une cascade d'avaries.

Autrement dit on est en droit de s'attendre à un comportement parfaitement inattendu, non contrôlable et rigoureusement contraire à la sécurité du processus que l'on désire contrôler.

Certaines hypothèses limitatives (Réf. 14) considèrent, à l'issue d'une décomposition en blocs fonctionnels d'une unité microprocesseur, que les défauts naissants n'affectent qu'un seul bloc.

Cette hypothèse n'est justifiée que dans la mesure où la fréquence des tests est plus rapide que la propagation du défaut.

On peut également considérer que les défauts naissants peuvent n'affecter que des fonctions non utilisées du microprocesseur. Dans ce cas la panne est dormante

- momentanément si une propagation de défaut est en cours
- à demeure si le défaut reste localisé.

Dans cet état d'esprit on peut envisager de ne réaliser des tests que sur les blocs fonctionnels activés par le programme d'application.

III₁₋₂ - Classement des types d'instructions et modèles de fautes associées

La classification et la modélisation présentée ci-dessous a été établie et appliquée à la génération de séquences de tests des unités microprocesseurs du système SARGOS (Réf.14) (repérage de balises de détresse).

Trois classes d'instruction ont été retenues

- 1 - les instructions chargées du transfert des informations
- 2 - les instructions chargées de la manipulation des informations
- 3 - les instructions chargées du branchement des programmes.

* Fonction de transfert et de stockage d'informations

Pour ce type d'instruction on peut considérer que n'importe quel bit de n'importe quel registre peut être collé en position 0 ou 1. Chaque paire de bit adjacents peut être le siège d'un couplage. Dans le même esprit chaque ligne établissant le cheminement d'une information peut être figée dans un état quelconque et chaque paire de lignes peut être couplée.

* Fonction de manipulation des informations

Ce sont l'unité arithmétique et logique ainsi que son registre d'état qui traitent ce type d'opérations. L'apparition d'un défaut modifie le comportement de cette unité. La modélisation du défaut est fonction de l'effet provoqué (test comportementel).

* Fonction d'adressage des registres et fonctions de décalage des instructions

La modélisation est là aussi établie à partir des effets produits. On peut détecter les défauts suivantes

- les instructions ne sont pas exécutées
- les entrées sorties sont actionnées anormalement
- les éléments de stockage sont incorrectement modifiés
 - . placés en 0 ou en 1 anormalement
 - . substitués ou échangés par le contenu d'un autre élément
 - . remplacés par le résultat d'une opération.

On peut encore supposer

- l'exécution partielle d'une instruction
- l'exécution d'une instruction par une autre résultant d'un mauvais décodage
 - la sélection inopinée d'un ou plusieurs autres registres non utiles à la présente instruction.

Nous le voyons les hypothèses de pannes sont nombreuses, on pourrait aller jusqu'à donner libre cours à son imagination.

Une analyse technologique des conséquences des pannes du type de celle utilisée en sécurité traditionnelle, est impossible sur un circuit à grande échelle d'intégration. Seules des méthodes rigoureuses d'analyse fonctionnelle, de représentation ou de traitement par calcul peuvent apporter une réponse au problème de la détection d'erreurs.

Plusieurs méthodes de détection de pannes ont été développées en vue de détecter des défauts du type collage, couplage ou mauvais adressage d'espaces mémoires vive RAM (Réf. 14).

Le moyen le plus employé pour la détection d'erreurs en mémoire morte est le calcul de checksum. La discordance de la checksum recalculée

et de celle inscrite en mémoire informe, sans pouvoir dissocier, une modification sur une case mémoire, ou une séquence d'appel non conforme de toutes les valeurs stockées dans la mémoire.

En ce qui concerne les fonctions environnantes du microprocesseur (périphériques) étant entendu que l'on y accède par des registres situés en amont de la fonction désirée. Il n'existe, à notre avis, pas d'autres possibilités de test que la vérification du comportement de la fonction attendue au moyen d'une voie de mesure indépendante (gestion d'un écho en liaison série par exemple).

III₂ - Méthodes du type auto-test de détection d'erreurs de fonctionnement des microprocesseurs

Les méthodes de détection d'erreurs que nous développons ci-dessous se présentent sous forme de programmes d'autotests. Ces procédés viennent donc s'inscrire en complément à d'autres méthodes de détection s'appuyant sur des architectures redondantes où l'on détecte une erreur par comparaison des résultats obtenus.

Ce qui nous semble important, c'est de dégager pour chaque procédé les points suivants :

- les hypothèses de départ
- les types de défauts détectés et leur localisation, ces particularités en font des critères de choix d'utilisation
- la possibilité de quantifier la couverture de détection de panne obtenue par le procédé envisagé.

III₂₋₁ - Détection de défaut par test fonctionnel (Réf. 26-14)

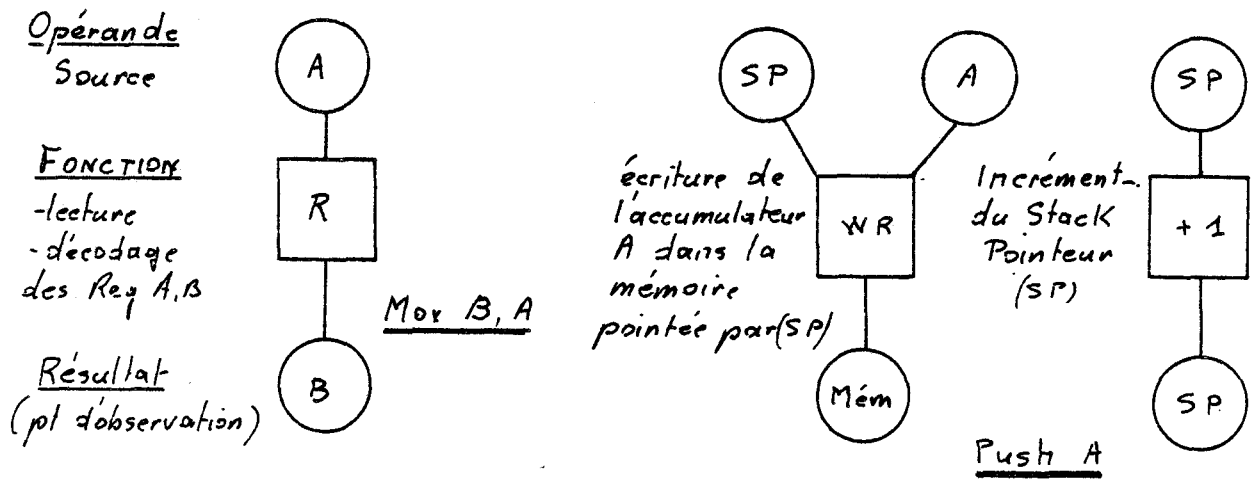
Cette méthode de détection déterministe est souvent opposée aux méthodes de test aléatoires Réf. 22 (non développée ici car elle suppose un élément microprocesseur de référence). Elle se présente sous forme de modules de programmes capables de valider la conformité du fonctionnement des divers sous-ensembles du microprocesseur.

L'écriture des logiciels s'appuie sur une décomposition fine des unités de fonctionnement représentés sous forme graphique.

La méthode s'attache à vérifier le comportement attendu de chaque bloc fonctionnel. Ce comportement est décrit dans la notice d'utilisation du microprocesseur délivrée par le constructeur. L'information d'erreur est fournie par le microprocesseur lui-même après avoir défini dans le programme des points d'observation significatifs.

Chaque instruction met en oeuvre un certain nombre de blocs fonctionnels. Pour un microprocesseur donné, il faut effectuer un classement des diverses instructions selon la complexité du graphe qui la représente. Il se peut que certaines instructions complexes fassent appel à des portions de graphes déjà définies pour d'autres instructions plus élémentaires.

A titre d'exemple nous présentons les graphes de deux instructions distinctes



On peut selon la finalité imposée au test distinguer plusieurs applications

- Test de fin de chaîne de fabrication du microprocesseur

On vérifie de façon exhaustive tous les blocs fonctionnels avec toutes les valeurs possibles des opérandes de test. Le temps de vérification est important (quelques dizaines de secondes pour un microprocesseur 8 bits).

- Test partiel du microprocesseur

On peut effectuer périodiquement un test de tous les blocs fonctionnels utilisés par le programme d'application et ceci avec des valeurs d'opérandes reconnues comme significatives.

On opère alors un test réduit en utilisant des instructions complexes mettant en oeuvre un maximum d'unités de fonctionnement activées par le programme d'application. Selon le résultat, et si nécessaire, on peut ensuite cerner le défaut à l'aide d'autres instructions plus élémentaires.

Par ce procédé la durée du test peut être considérablement réduite et ramenée à l'exécution de quelques dizaines d'instructions.

On parvient donc grâce à cette méthode à une détection nominative du défaut. La connaissance de toutes les unités fonctionnelles du microprocesseur, le balayage d'un nombre défini de test permet d'établir la quantification des unités testées et de là la couverture de panne du test proposé.

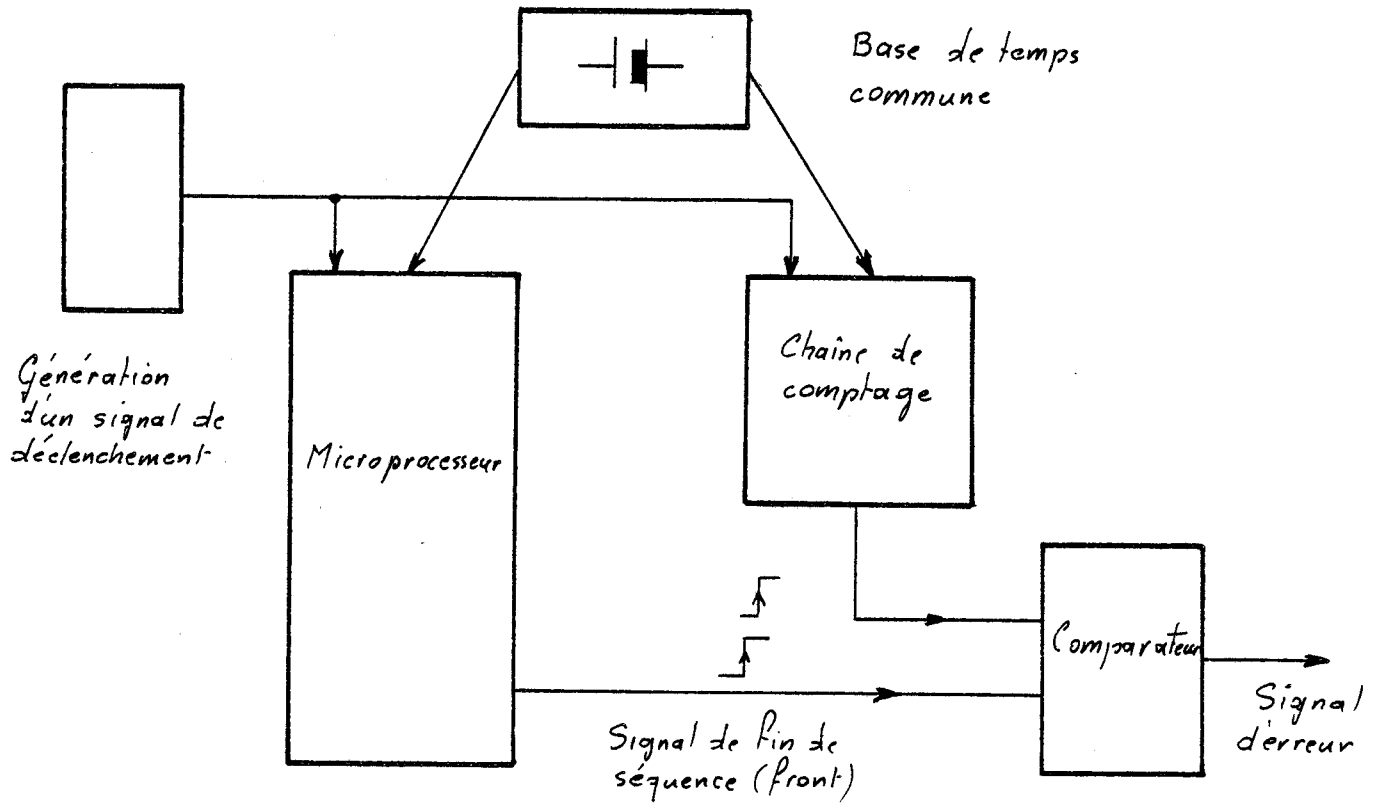
III₂₋₂ - Détection d'erreur par test temporel

Un autre procédé de détection d'erreur de fonctionnement consiste à vérifier le temps d'exécution d'un programme. Une méthode originale de représentation d'un programme par graphe orienté (réf. 16) a été établie en vue de permettre une comptabilisation aisée du temps nécessaire pour parcourir une portion de programme.

L'hypothèse de départ réside dans le fait que les instructions sont exécutées de façon synchrone avec l'horloge du système. La durée d'exécution est donc parfaitement connue.

Trois types d'instructions sont à distinguer

- les instructions à durée d'exécution fixe (quasi totalité des cas)
- les instructions à durée d'exécution variable mais limitée et bornée (branchements)
- les instructions à temps d'exécution non borné (attente, interruption...etc) non utilisables pour les tests temporels.



Détection des erreurs de fonctionnement
par test temporel - Description
du schéma fonctionnel

Figure N° 1.4



Le graphe orienté représente le cheminement du programme. Il est constitué d'arrêtes correspondant chacune à une instruction exécutée

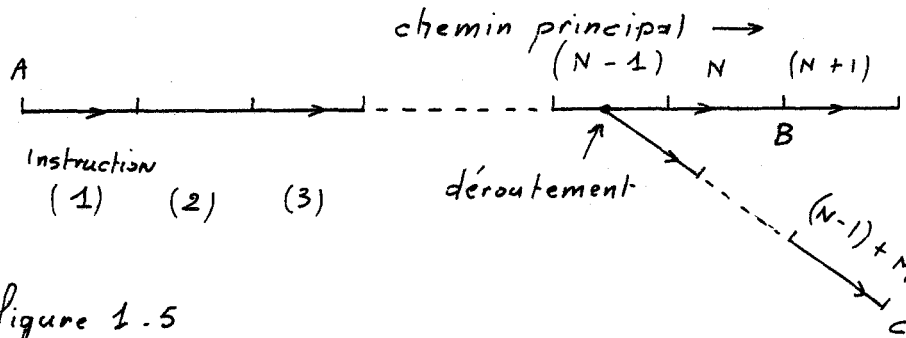


figure 1.5

Le chemin de A à B correspond à une séquence de N instructions. Le temps nécessaire pour parcourir ce chemin correspond à la somme de tous les microcycles d'horloge consommés par chaque instruction.

Certaines instructions peuvent avoir deux points de sortie, telles les instructions de branchement. A la condition de branchement peut être associée une information de panne, (non acquittement d'un test) la discrimination étant réalisée par un cheminement différent (exemple AC équivaut à $(N-1) + M$ instructions), figure 1.5

Pour un graphe G donné on considère un ensemble prescrit de chemins SG correspondant à toutes les séquences d'instruction possibles

Le test mis en oeuvre consiste donc pour certains chemins choisis à vérifier la durée d'exécution de ces portions de programme.

La mise en oeuvre de ce procédé de test nécessite, en plus du microprocesseur, une unité de comptage et un comparateur (celui-ci doit être en sécurité intrinsèque). La base de temps est évidemment commune aux deux systèmes. Le schéma fonctionnel est représenté ci-contre, figure 1.4

Le signal d'erreur délivré par le système ne donne pas d'indications quant à l'origine du défaut détecté.

Cette méthode présente des avantages parmi lesquels nous retenons :

- sa mise en oeuvre simple et adaptable au test d'un système en exploitation normale (test en ligne)
- la possibilité de détecter les erreurs tant sur le microprocesseur que sur son dispositif de contrôle.

Toutefois elle ne s'applique qu'aux processeurs synchrones d'une seule horloge et à un seul flux d'instructions, ce qui correspond tout de même à la majorité des microprocesseurs 8 bits sur le marché.

Tout en présentant une possibilité de détection sensible, car on comptabilise des quantités discrètes, il faudrait pouvoir quantifier l'efficacité du test d'abord par une analyse approfondie de toutes les possibilités de cheminement d'un programme (analyse et mise au point du programme d'application) puis par une analyse fonctionnelle des chemins requis pour les séquences de test.

III₂₋₃ - Détection de défaut par utilisation des codages (Réf. 44-52)

Le concept utilisé ici diffère des précédents dans la mesure où le test ne porte plus sur l'unité de fonctionnement mais sur les données en traitement.

Le procédé repose sur des propriétés de codage d'information. Il s'applique plus particulièrement au transfert et à la combinaison d'informations entre elles.

L'hypothèse de départ réside dans le fait qu'une donnée codée selon certaines propriétés peut être transmise et, selon le code utilisé, affectée d'opérations tout en gardant ses propriétés initiales. On dit que le code employé est stable.

La vérification systématique de la conservation des propriétés permettra de détecter l'apparition de défauts introduits lors de la transmission ou des calculs.

Les codes arithmétiques répondent à cette propriété.

Soit S l'ensemble des valeurs codées

$$A, B \in S$$

$$A \circ B \in S$$

L'opérateur "o" est un opérateur arithmétique du type addition ou soustraction, opérations élémentaires pour l'unité arithmétique et logique d'un microprocesseur.

Les codes arithmétiques se prêtent bien au problème de détection d'erreur. Deux types de présentation se distinguent pour les codes arithmétiques, les codes séparables ou non séparables selon que les bits de contrôle sont juxtaposés ou confondus dans la donnée codée.

Parmi les codes non séparables nous citons le code "AN + B". Il porte la particularité de présenter 2 propriétés :

- il est autocomplémentaire à savoir
le codage du complément est égal au complément du codage

$$C(\bar{N}) = \overline{C(N)}$$

- il conserve après opérations arithmétiques ses propriétés

$$N = \frac{C(N) - B}{A} \quad \text{avec un reste de division par A nul.}$$

Ceci permet d'envisager sur une donnée N codée C(N), une double vérification traitée par deux modules différents de programme comme le montrent les organigrammes ci contre. (figure I.6)

Le nombre d'erreurs détectées est lié à la notion de distance arithmétique comme pour la distance de Hamming (Réf.44).

Pour détecter T erreurs il faut et il suffit que la distance entre les nombres soit égale

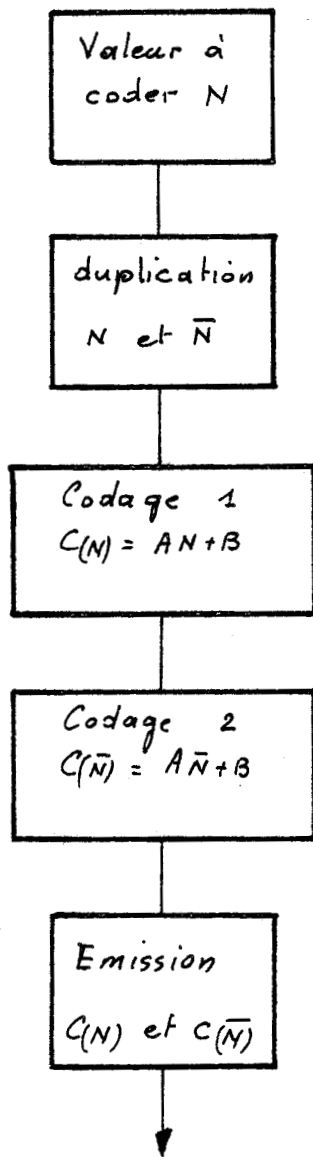
$$D = T + 1 \quad \text{distance arithmétique}$$

Ce type de codage autorise la correction d'erreurs, il faut dans ce cas pour E erreurs à corriger

$$D = 2E + 1$$

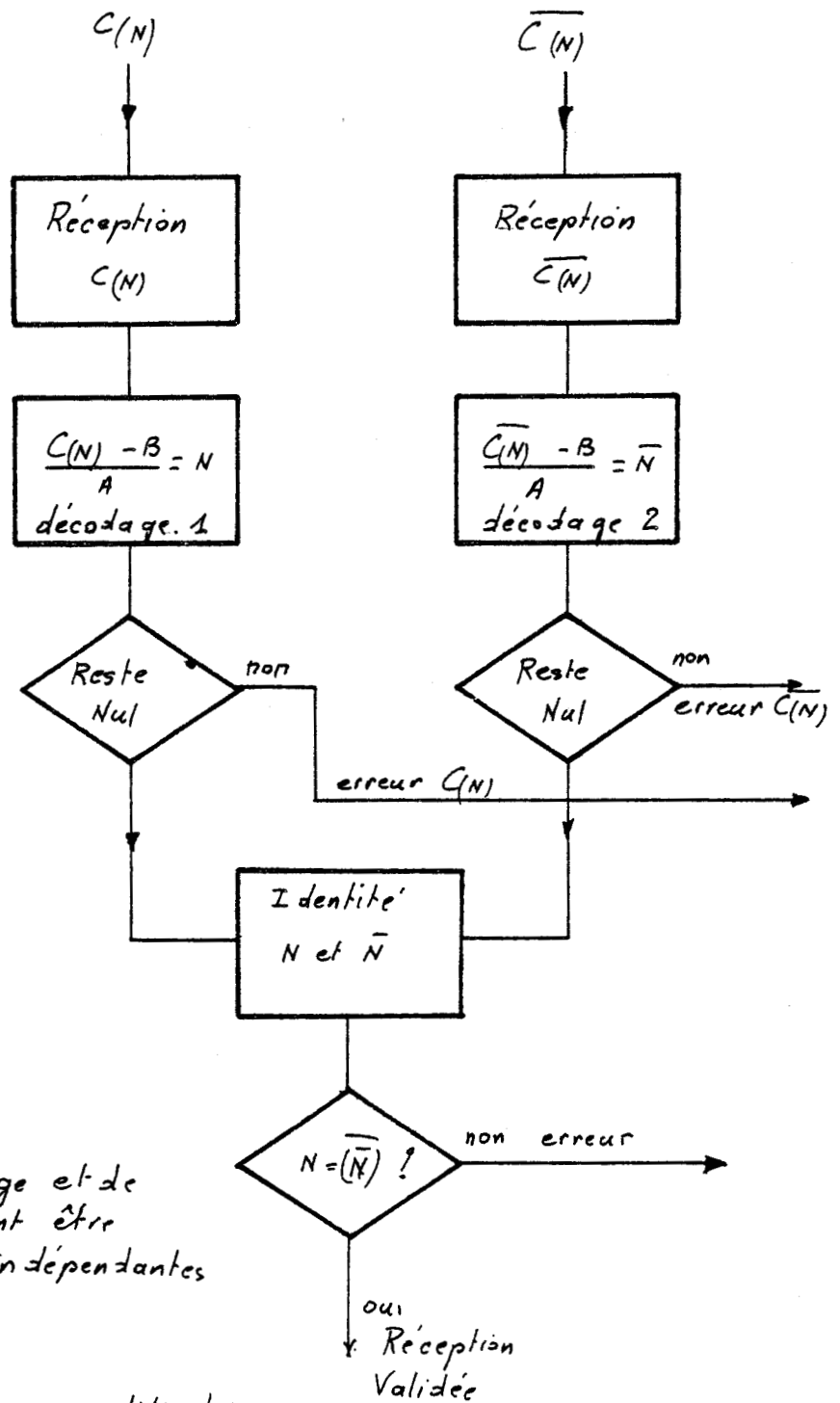
Connaissant la valeur maximale du nombre à coder (N), ainsi que le nombre d'erreur à détecter on peut déduire la valeur du coefficient A et de la constante B.

Emission



Remarque
 Les opérations de codage et de décodage (1 et 2) peuvent être réalisées par des unités indépendantes

Réception



Détection d'erreurs par utilisation des codages.

Figure I.6

L'intérêt de ce type de codage réside, nous l'avons dit, dans le fait qu'une information de sécurité peut être transmise et combinée avec d'autres informations de sécurité homogènes. L'unité de traitement pouvant être un simple microprocesseur. Celui-ci a la possibilité de valider les données après réception ainsi que les résultats de calcul avant réémission ou actionnement.

Ce procédé de détection d'erreur se prête mieux par nature au traitement numérique de données qu'au contrôle de processus.

L'information d'erreur signale, sans les distinguer, les défauts de fonctionnement de l'unité de calcul et ceux des dispositifs de transmission de données. Le nombre d'erreurs à détecter doit être déterminé en tenant compte non seulement du taux d'erreur introduit par la transmission des messages parasites sur la voie de transmission, mais aussi de modèles de fautes applicables à l'unité de calcul du microprocesseur.

III₃ - Fiabilité des microprocesseurs

Les valeurs des taux de défaillance des microprocesseurs sont en général rarement fournies par les constructeurs, surtout s'il s'agit d'un composant récemment mis sur le marché.

Seul un organisme officiel agréé peut fournir objectivement des résultats, mais on les trouve que pour des produits largement utilisés et éprouvés. Les résultats fournis sont pondérés en fonction de nombreux paramètres parmi lesquels nous citons (Réf.4).

- la complexité ou le nombre de composants actifs sur le circuit
- le type de technologie : MOS - bipolaire, avec par ordre décroissant de fiabilité : la technologie bipolaire, MOS N-P, et enfin la CMOS
- la température des jonctions
- la tension d'alimentation (CMOS)
- le type de boîtier
- l'environnement (fixe - mobile, etc...)
- le nombre de connexions d'accès au circuit
- l'ancienneté de fabrication chez le constructeur (rapport 10 à 1 de 6 mois à 2 ans d'ancienneté)
- la qualification des lots de composants
- la période d'utilisation.

Afin de fixer les idées nous avons effectué le calcul du taux de défaillance de quelques boîtiers bien connus dont l'association correspond sensiblement aux caractéristiques du microprocesseur monochip que nous utilisons pour la commande des portes développée en seconde partie (INTEL 8751).

Les fonctions sont les suivantes

- un microprocesseur INTEL 8085 (NMOS)
- une unité de transmission série INTEL 8251 (NMOS)
- un séquenceur, compteur d'évènements INTEL 8253 (NMOS)
- une mémoire EPROM 32Kbits du type 2732 (NMOS).

Avec des conditions d'environnement défavorables en température, en type de matériel (mobile), en type de boîtier nous parvenons à un taux de défaillance de (détail annexe 3).

$$\lambda = 28,5 \cdot 10^{-6} / \text{h}$$

Nous pensons devoir majorer ce résultat dans un rapport 2 compte tenu de l'implantation de toutes les fonctions sur la même puce; soit pour la technologie NMOS (extrapolation à partir des abaques - CNET)

$$\lambda_6 \approx 0,7 \cdot 10^{-4} / \text{h}$$

Ce résultat vient corroborer une analyse de fiabilité de la SFENA concernant l'application des microprocesseurs au pilotage automatique dans le domaine ferroviaire (réf.7) où l'on fait mention de systèmes microprocesseurs plus complexes (carte complète 8085) que notre exemple ci-dessus.

La valeur citée du taux de défaillance est de

$$\lambda \approx 3 \cdot 10^{-4} / \text{h}$$

Cette évaluation grossière, mais sur des bases de données officielles sera utilisée lors des calculs prévisionnels de fiabilité développés sur le système de commande de porte. Il est à remarquer que ces résultats déterminés avec des paramètres choisis de manière volontairement pessimiste pour la fiabilité, ne sauraient évoluer que favorablement en fonction des progrès constants de la technologie.

Cette tendance favorable est importante pour notre étude. On ne peut envisager d'étendre l'emploi des microprocesseurs si ceux-ci s'avèrent peu fiables. Si cela était, les avantages développés plus haut concernant la simplification des opérations de maintenance seraient compensés négativement par la nécessité de remettre plus fréquemment les systèmes en état suite aux défaillances des microprocesseurs.

Nous avons vu plus haut que parmi les facteurs importants jouant sur la valeur du taux de défaillance horaire, figurait l'ancienneté de fabrication. On imagine aisément que compte tenu de la grande complexité des fonctions à intégrer il faut de la part du constructeur posséder une certaine maîtrise des procédés de fabrication, ceci en vue de parvenir non seulement à une production rentable mais aussi afin d'obtenir des produits de qualité (fiables).

L'évolution aujourd'hui très rapide de la micro-informatique oblige les fabricants à modifier sans cesse leur production. On peut donc penser que les résultats de fiabilité actuellement disponibles ne sont peut être pas stabilisés dans la période de vie utile du composant (déverminage non achevé - figure I.2) ou encore qu'une amélioration possible des procédés de fabrication, dans le cadre d'une fabrication à long terme, permettrait de minimiser la valeur du taux de défaillance (λ_0).



SUD
LILLE

photo n° 2

CONCLUSION DE LA PREMIERE PARTIE

La classification des problèmes posés par la mise en sécurité d'un dispositif quelconque, que nous avons établi sur le tableau I₁, nous a permis de replacer les concepts généraux utilisables à ce genre d'étude, et de prendre position pour le travail qui nous était demandé.

A partir d'un bref appel sur les principes de base présidant à la conception de circuits en sécurité intrinsèque, nous avons essayé dans le même esprit de dégager d'une manière très générale quelques principes fondamentaux applicables à la conception d'un dispositif de commande-contrôle de processus en sécurité géré par microprocesseur.

Nous avons établi paragraphe II₃₋₁₋₂, qu'il fallait à l'issue d'une étude sur les modes de panne possibles du processus et de ses organes de commande et de contrôle, déterminer une configuration nécessaire et suffisante des vecteurs d'état et de commande propres à assurer la sécurité. Cette configuration système, doit être entérinée par le choix judicieux d'une procédure de détection et d'analyse des pannes capable de présenter une couverture totale des défaillances relatives à ces organes. Le choix de cette procédure doit aller dans le sens d'une minimisation des temps de latence de panne, contrairement à la sécurité, notamment pour les processus discontinus à fonctionnement non cyclique ou à cycle irrégulier.

Après avoir détecté et identifié une panne le dispositif de commande a pour tâche d'engendrer deux actions indépendantes dans leur effet, mais indissociables pour la sécurité.

-1- La première action consiste à imposer au cycle de commande une modification consistant à forcer le processus dans un état de sécurité pour l'utilisateur, ou si possible à générer un mode de fonctionnement dégradé allant vers un maintien de l'exploitation, d'où un gain de disponibilité (tolérance à un défaut).

-2- La seconde action nécessite la transmission d'un message d'alarme relatif à la panne détectée en vue d'une remise en état (maintenance curative) dans un intervalle de temps compatible avec les objectifs de sécurité. Les maintenances préventives périodiques ne sont alors plus nécessaires, ce qui constitue un avantage certain.

Jusqu'alors l'hypothèse de travail était de considérer le microprocesseur en bon fonctionnement.

Un calcul approximatif du taux de défaillance horaire d'un système microprocesseur nous a permis de dégager que celui-ci était relativement peu fiable même dans une configuration totalement intégrée du type monochip.

Cette constatation nous amène à penser qu'il faut limiter en nombre l'emploi des microprocesseurs d'où l'intérêt porté sur les méthodes d'analyse de fonctionnement en autotest développées au paragraphe III. La configuration monoprocesseur en sécurité n'excluant pas à priori une redondance totale des matériels dans le cas où un objectif de disponibilité très contraignant serait souhaité.

La difficulté rencontrée dans cette partie de l'étude réside dans l'établissement du taux de couverture de panne compte tenu de la complexité présentée par les systèmes microprocesseurs et du nombre important d'hypothèses de pannes envisageables.

Dans le problème qui nous était posé et que nous développons dans la seconde partie de ce mémoire, il s'agit à terme, de remplacer un dispositif décentralisé de commande de portes véhicule d'une rame de métro réalisée à partir de composants électromécaniques traditionnels, par une structure microprogrammée dont on attend deux améliorations importantes :

- la suppression des maintenances périodiques préventives nécessaire au respect des objectifs de sécurité

- l'amélioration de la disponibilité d'une rame de métro en relation avec les avaries "portes véhicule".

DEUXIEME PARTIE

COMMANDE D'UN ENSEMBLE DE
PORTES VEHICULE D'UNE RAME
DE METRO DU TYPE VAL

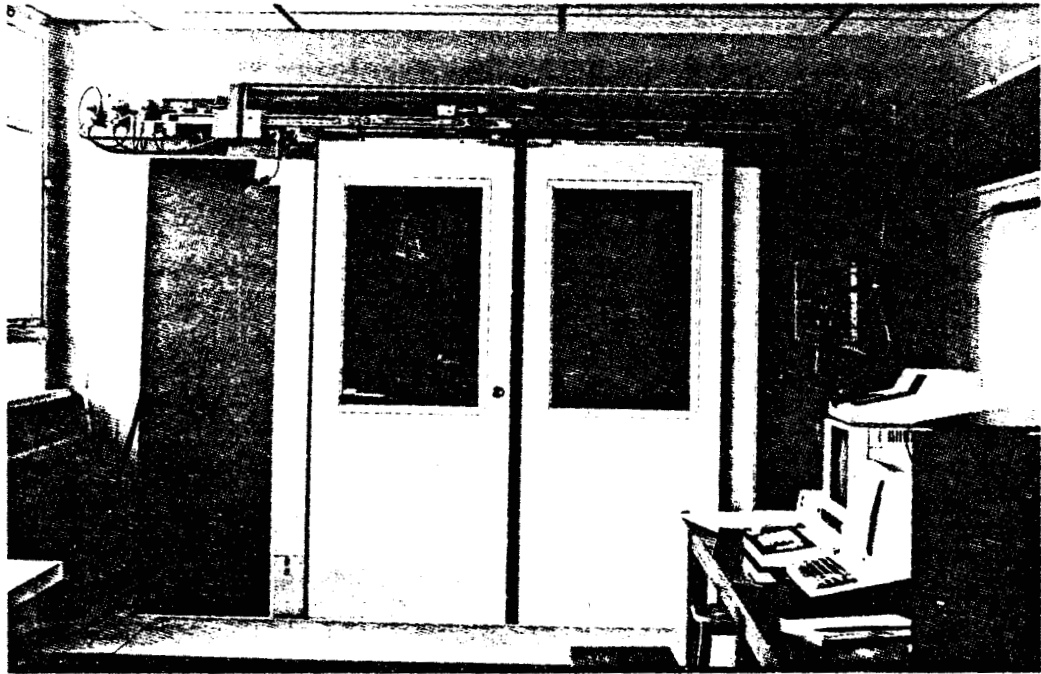


photo n° 3

SIS
LILLE

I - ETUDE DU SYSTEME DE PORTE D'UN VEHICULE DE TYPE VAL - DEFINITION
D'UN DISPOSITIF DE COMMANDE A MICROPROCESSEUR

Dans la seconde partie de ce mémoire nous abordons une réalisation concrète de commande-contrôle de processus en sécurité. Le travail qui nous était demandé consistait à réaliser un dispositif de commande d'un ensemble de portes véhicule d'une rame de métro de type VAL.

Nous avons pu disposer pour notre étude d'un mécanisme de porte VAL représenté sur la photo n° 3. L'ensemble se compose des éléments suivants :

- deux vantaux de porte
- le rail de guidage des vantaux et le mécanisme de conjugaison de mouvement
- un moteur de porte pneumatique
- des composants électromécaniques et pneumatiques de commande et de contrôle du mécanisme à savoir :
 - . les électrovalves d'alimentation du moteur de porte
 - . les contacts fin de course délivrant les informations d'état relatives à la porte.

Notons enfin la présence d'un groupe d'alimentation en air comprimé permettant de faire fonctionner le système dans des conditions nominales telles qu'elles existent sur le VAL (10 bars).

La figure 2.1 représente la formation d'un élément ou d'une rame de métro par association de 2 véhicules, on notera les différents repérages de sens de marche et de numérotation des mécanismes de porte.

I₁ - Description du système de commande de porte installé sur VAL

Comme nous le voyons sur la figure 2.1, chaque véhicule comporte 6 mécanismes de porte disposés latéralement. Lors d'une arrivée en station, après positionnement, les portes véhicule se trouvent en regard des portes palières de station. A ce moment un ordre d'ouverture est délivré

- par le DCA (*) pour la commande des portes véhicule
- par le système électronique d'arrêt en station pour les portes palières de station.

(*) DCA : dispositif de conduite automatique

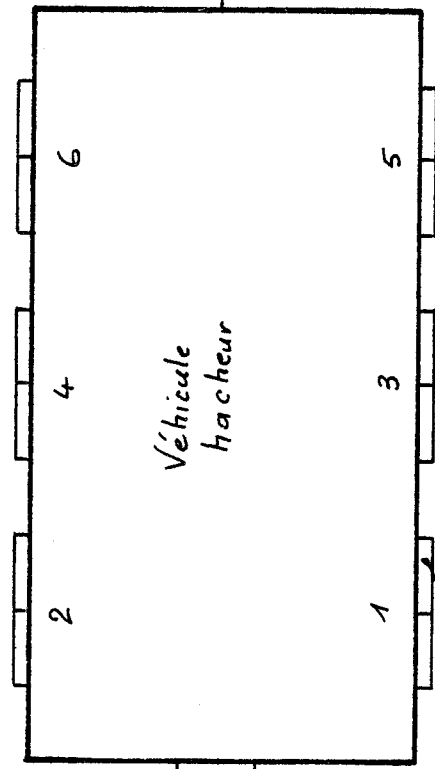


CHR

Sens 1

Cité Scientifique

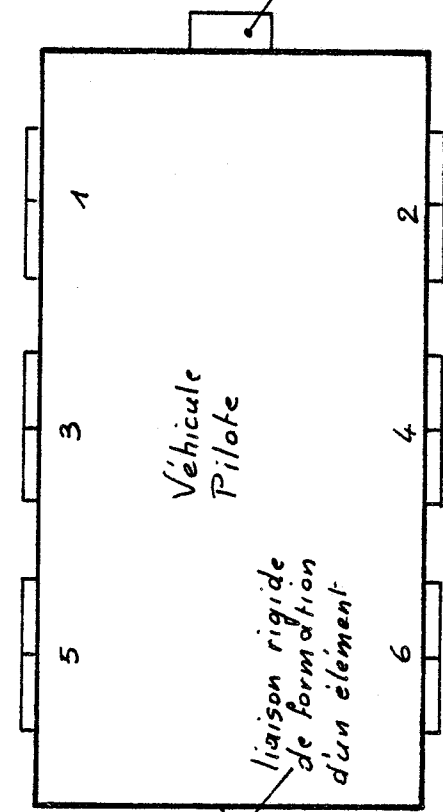
Côté droit de l'élément



connecteur d'attelage (accostage)

Véhicule hacheur

mécanisme de porte (2 vantaux)



Véhicule Pilote

liaison rigide de formation d'un élément

connecteur d'attelage

Côté gauche de l'élément

2,6 m

Sens 2

figure 2-1

Formation d'une rame (1 élément)
dans la configuration VAL ligne N°1 début d'exploitation

Au terme de l'ouverture l'échange des voyageurs entre la station et le véhicule est alors possible.

Cette fonction "échange des voyageurs" est réalisée par un processus que nous définissons comme étant l'ensemble des systèmes de porte.

Notre travail ne prend en compte que les portes véhicule.

Plusieurs remarques sont à formuler.

1 - Le processus est "discontinu" à savoir ; les variables d'entrée et de sortie se présentent sous forme de grandeurs logiques

2 - Le processus est distribué dans l'espace, ceci est pénalisant pour son système de commande au niveau de la répartition et de l'implantation des matériels et du câblage

3 - Le processus est de par sa nature en structure redondante. Cette particularité va dans le sens d'une simplification. On peut en effet supposer qu'une porte défectueuse puisse être immobilisée en station en position fermée sans que la fonction échange des voyageurs soit interrompue totalement.

I₁₋₁ - Fonctions propres à garantir la sécurité des voyageurs

Le processus que nous avons défini doit présenter par rapport aux voyageurs des fonctions de sécurité que l'on peut présenter comme suit :

- en service normal : il faut pouvoir garantir l'état porte fermée avant démarrage de station et de même la non ouverture intempestive des portes en ligne.

- lors d'un évènement dont l'origine se situe à l'intérieur des véhicules (incendie, agression...) il faut pouvoir garantir l'évacuation des passagers par le système de porte. Notons que dans ce cas l'état de sécurité de la porte est alors rigoureusement opposé au cas précédent.

Précisons enfin que pour la qualité et le confort du service rendu aux voyageurs il faut pouvoir gérer les fonctions suivantes :

- ouverture d'au moins un système de porte après arrêt en station
- réouverture momentanée des portes lorsqu'un obstacle s'oppose à la fermeture normale. Cet aspect est très pénalisant pour l'exploitation d'un métro entièrement automatisé ; un simple obstacle permanent dans l'entrebaillement d'une porte peut immobiliser tout un tronçon de ligne.



BUZ
LILLE

photo n° 4

I₁₋₂ - Génération de la commande d'ouverture

Après arrêt en station le pilote automatique de la rame (DCA) vérifie à l'aide d'équations logiques booléennes la présence de variables d'entrée après quoi il délivre une commande latéralisée d'ouverture de portes en fonction de la position relative du quai et du véhicule. Cet ordre non sécuritaire (voir 1ère partie paragraphe I) est validé en sécurité par 2 informations, vitesse nulle et présence station, traitées par la chaîne sécurité (Figure 2.2).

La sortie validée attaque respectivement les lignes de train commande des portes droites ou gauches.

L'ensemble de cette fonction est redondancée.

Une ligne de train est constituée d'une paire de fil parcourant toute la longueur de la rame voire de plusieurs rames dans le cas d'un accostage par exemple. Cette liaison bifilaire transporte l'énergie nécessaire à l'élaboration de la fonction à exécuter.

Dans le cas de la commande d'ouverture, les lignes de train considérées iront alimenter les bobines des relais de commande d'ouverture.

L'absence d'énergie ou une coupure dans les liaisons ira dans le sens d'une interdiction d'ouverture des portes, la commande du système sera rendue impossible.

La commande individuelle de chaque mécanisme de porte est gérée par une platine de relayage spécifique installée à proximité du mécanisme commandé. Les fonctions traitées sont simples :

- commande d'ouverture ; (alimentation en air comprimé du moteur de porte)
- commande de fermeture avec réouverture sur obstacle.

I₁₋₃ - Elaboration des informations de sécurité - Analyse de sécurité

Sur chaque mécanisme de porte sont installés des contacts fin de course permettant de suivre l'évolution des séquences d'ouverture et de fermeture. Les informations fournies sont les suivantes :

- état du verrou (BKPV)
- état porte fermée (BKPF)
- information de demande d'évacuation d'urgence (EVAC)

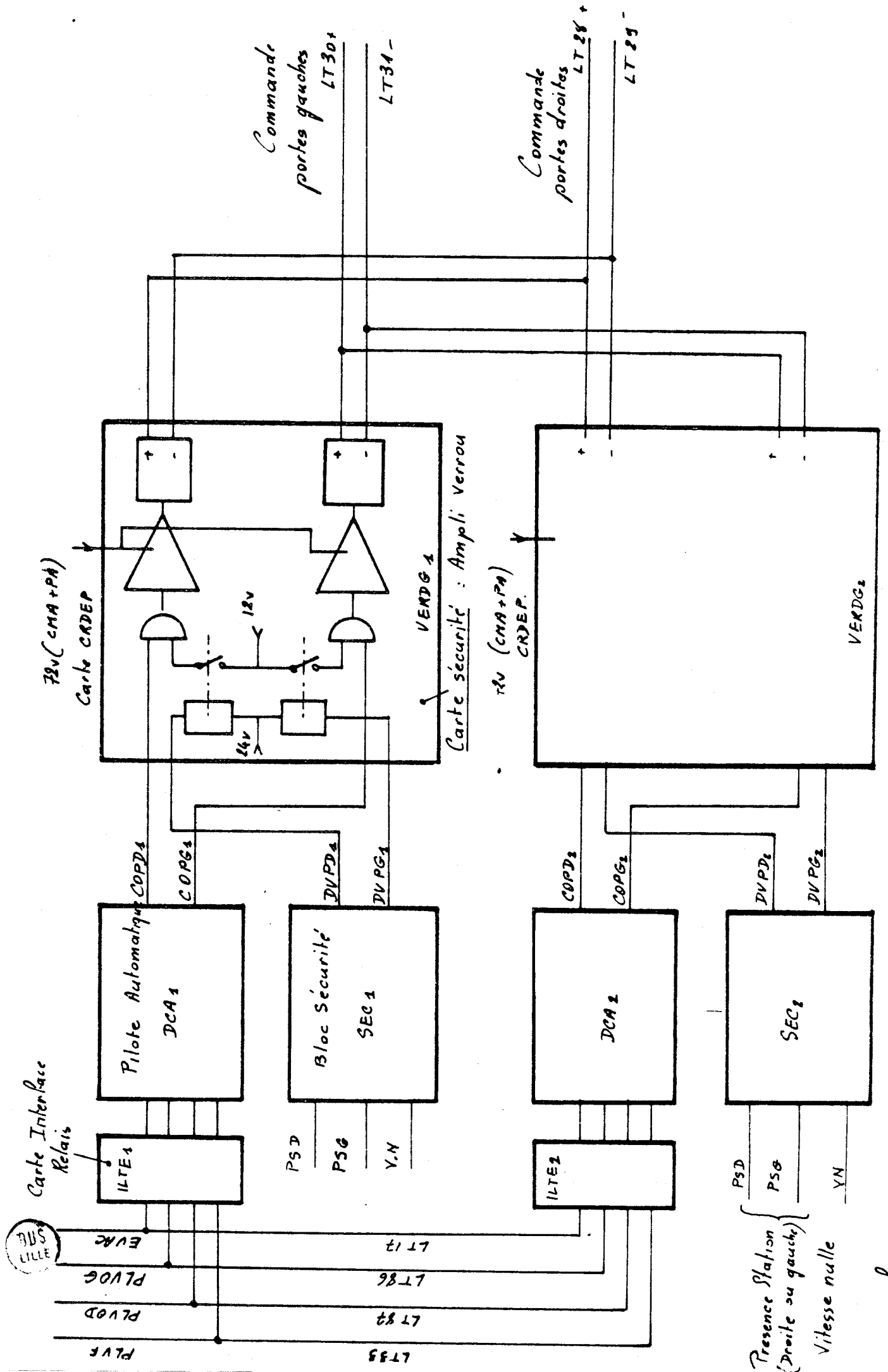


Figure II.2

Ces 3 premiers contacts délivrent les informations de sécurité du mécanisme de porte.

- contact porte ouverte (BKPO)
- contact intermédiaire (BKDOP) dont la fonction est de donner la position à partir de laquelle il n'y aura plus de réouverture sur obstacle
- manostat de détection d'obstacle (MDOP)
- contact de commande manuelle d'ouverture depuis l'extérieur (BKPE).

Les informations de sécurité relatives à l'ensemble des 6 portes d'un véhicule sont les suivantes :

- demande d'évacuation d'urgence par action sur une poignée accessible depuis chaque porte. Une ligne de train spécifique traite cette fonction par association série de tous les contacts EVAC

- état porte fermée verrouillée

* pour garantir la sécurité des voyageurs lors du redémarrage d'une rame en station

* pour garantir l'état porte fermée verrouillée en ligne

Une seconde ligne de train, portes latérales véhicule fermées permet par l'association en série des contacts BKPV et BKPF de délivrer cette information de sécurité.

Le schéma de la figure 2.3 nous décrit en détail le câblage et le cheminement de ces lignes de train.

Le schéma fonctionnel ci-dessous (fig. 2.4) montre une représentation simplifiée. Lors de la formation d'une rame étendue à 52 m par accouplement de 2 rames, par l'avant ou par l'arrière, la ligne de train se reconfigure de manière à mettre en série les contacts des 24 portes de l'élément ainsi formé (commutation RAR et ouverture du contact d'attelage).

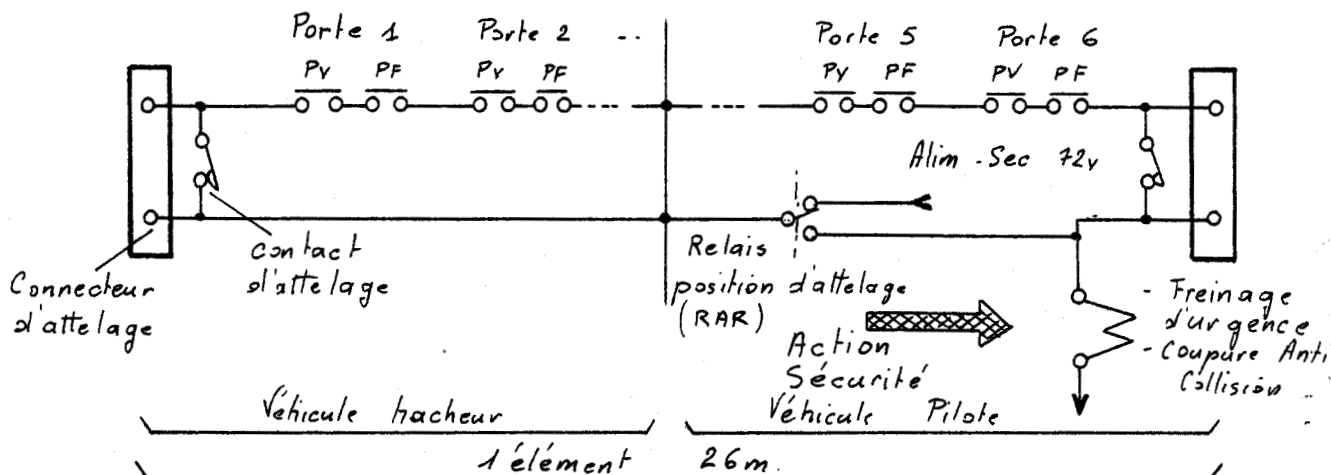
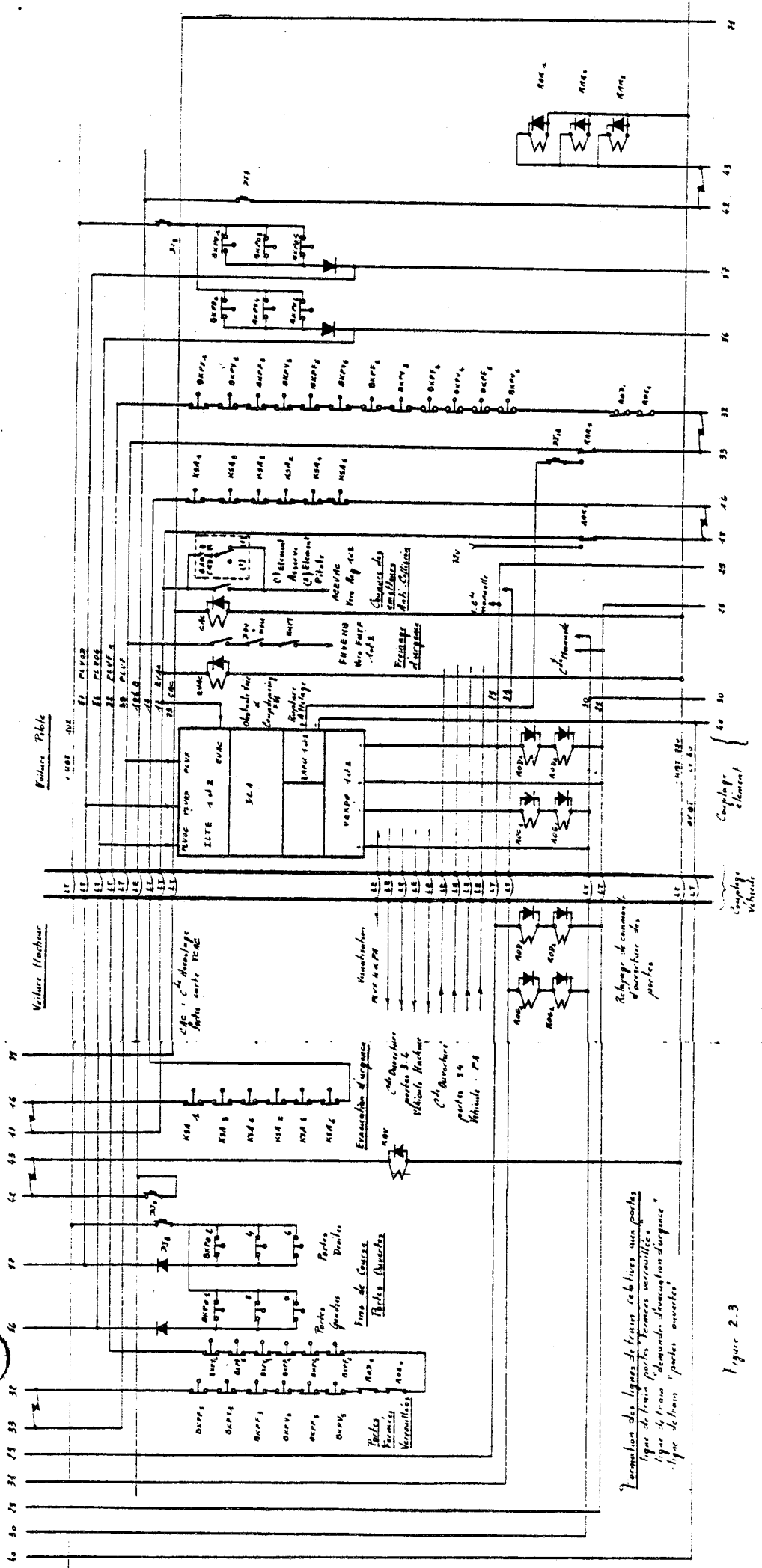


Figure 2.4



Formation des lignes de train relatives aux parties
 Ligne de train pour les parties accessoires
 Ligne de train pour les parties principales
 Ligne de train pour les parties accessoires

Figure 2.3

Analyse sécurité

Lorsque la rame est en ligne, toutes portes fermées, les contacts des 12 portes sont en position fermée, l'alimentation (72 v) active le relais de sécurité commandant le défreinage, le véhicule peut circuler normalement.

Si une porte s'ouvre, pour une raison quelconque, les contacts relatifs à cette porte ouvrent la ligne de train ; le relais de sécurité n'est alors plus alimenté et le véhicule se met en freinage d'urgence.

Pour que cette action sécuritaire se produise et puisse répondre au concept de la sécurité préalablement défini, il a fallu recourir à l'installation pour chaque porte, de deux contacts disposés en série de façon à se prémunir de la panne simple du type collage de contact.

Toutefois la sécurité reste probabiliste. La panne "collage de contact" étant considérée comme possible il existe une probabilité résiduelle pour que la panne double puisse se produire.

La sécurité se calcule alors selon un objectif défini par l'exploitant fixant la valeur de probabilité d'insécurité à ne pas dépasser. Cet objectif nécessite une intervention périodique et préventive consistant à vérifier le bon fonctionnement de chaque contact.

Le calcul développé en 1ère partie, paragraphe II₂, permet, connaissant la valeur des objectifs alloués et les taux de défaillance des contacts, de déterminer le temps séparant deux vérifications soit :

$$T_0 = 9800 \text{ heures}$$

L'intervalle de temps T séparant deux révisions doit être inférieur à la valeur calculée $T < T_0$.

I₂ - Définition des fonctions de sécurité d'un nouveau système de commande de porte à microprocesseur

De l'analyse de sécurité des lignes de train, nous avons dégagé le fait que la sécurité reposait sur le bon fonctionnement des contacts électriques et donc sur la nécessité d'établir des contrôles périodiques.

Ce point constitue sans doute l'une des principales motivations de notre étude. En effet la multiplicité des contrôles constitue pour l'exploitant une lourde charge de travail ainsi qu'une immobilisation des matériels.

De plus il faut pouvoir, lors des vérifications périodiques, faire appliquer des procédures strictes de manière à se prémunir des défaillances humaines et ne pas rendre les contrôles contraires à la sécurité à la suite d'erreurs ou de distractions des contrôleurs.

Nous pensons qu'aujourd'hui le problème de la commande de porte peut être traité de façon radicalement différente par l'emploi d'une architecture micro-informatique s'apparentant à un réseau local de commande-contrôle de processus. La proposition que nous avançons n'est pas spécifique au problème de commande de porte. Les solutions exposées dans les paragraphes qui vont suivre peuvent s'appliquer à bon nombre de problèmes de commande de processus discontinus dont on veut assurer la sécurité par rapport à l'environnement (application à la robotique par exemple).

La grande intégration des composants microinformatiques (VLSI) ainsi que les performances présentées aujourd'hui par ces produits très largement diffusés sur le marché incitent le concepteur à banaliser l'implantation de systèmes à intelligence répartie.

On peut, pour notre problème, envisager l'incorporation d'un microprocesseur par porte et d'utiliser toutes ses potentialités aux finalités suivantes

1 - La gestion des séquences de commande (fonction jusque là assurée par les platines de relais électro-mécaniques)

2 - Le traitement d'une tâche permanente de détection et d'analyse de toutes les pannes possibles sur le processus et sur les voies de commande et de mesure. (1ère partie - paragraphe II₃₋₁₁). Cette disposition permet de connaître à tout moment l'état de fonctionnement du système sous contrôle et donc de s'affranchir des maintenances préventives.

3 - La génération, après reconnaissance d'une panne, d'un mode de fonctionnement dégradé allant vers une meilleure disponibilité du processus.

4 - L'établissement de la sécurité du microprocesseur assigné à la commande du processus.

Considérons un mécanisme de porte, la génération des séquences de commande est simple, d'autant que les grandeurs de commandes sont statiques (commutation d'électrovalves), de plus la faible vitesse d'évolution du mécanisme en regard de la rapidité d'un microprocesseur laissent à penser que celui-ci est dans le temps très disponible.

Nous approximons, pour notre application, la disponibilité du microprocesseur à sa mise en sécurité (point -4- développé plus haut) à mieux de 95 % du temps. Cet état de fait a également conditionné le choix d'une méthode de mise en sécurité par autotest plutôt que par structure redondante (avec comparateur) ou en redondance majoritaire beaucoup plus lourde en matériel. Le microprocesseur utilisé est un circuit monochip (Intel. 8051) capable d'exécuter environ 0,6 million d'instructions à la seconde avec une horloge à 8 MHz.

Remarques préliminaires sur l'étude d'un dispositif de commande de porte en sécurité

La sécurité des voyageurs ayant pris place dans une rame de métro circulant en interstation dépend bien en partie de la sécurité de la commande de l'ensemble des portes. Nous pensons devoir dégager plusieurs aspects du problème de sécurité

* Le système de commande à développer doit être à même d'appréhender en permanence les phases de fonctionnement où la sécurité des voyageurs peut être menacée notamment les cas suivants :

- traitement d'une demande d'évacuation d'urgence
- garantir l'état porte fermée verrouillée en ligne et au redémarrage d'une station

* Le système de commande doit comme nous l'avons dit procéder en permanence à la détection et à l'analyse des pannes du processus. Dans l'optique d'une commande en sécurité cette fonction doit être entérinée par les actions suivantes :

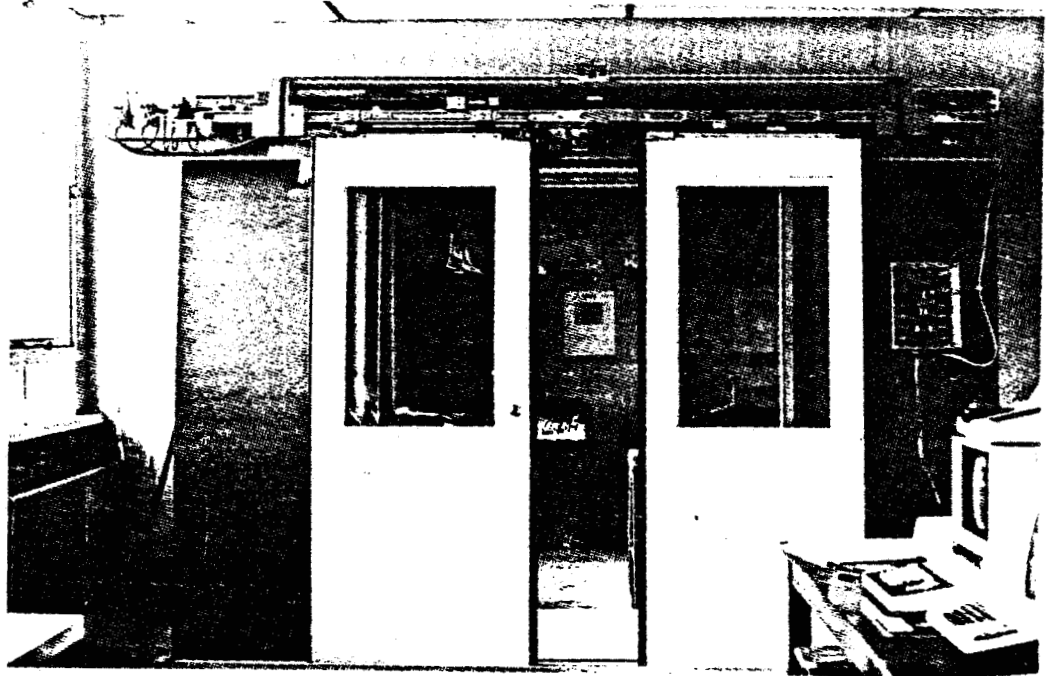


photo n° 5



- définition et application d'un état de sécurité si la panne se révèle dangereuse
- transmission de messages de panne vers l'exploitation en vue d'une remise en état

* Enfin le système de commande doit en permanence détecter ses propres défauts de fonctionnement (internes au microprocesseur) en vue de garantir la sécurité du processus commandé (définition donnée en 1ère partie - paragraphe II₃₋₂).

I₃ - Organisation et développement du projet "commande de porte"

Le problème posé consiste à commander l'ensemble des mécanismes de porte d'un véhicule (figure 2.1) tout en assurant la sécurité des voyageurs et avec le souci d'apporter des améliorations à l'exploitation d'un système de transport automatisé.

Ces améliorations peuvent se formuler de la façon suivante

1 - Aide à la maintenabilité de l'ensemble des mécanismes de porte

Ceci est rendu possible par l'utilisation de microprocesseurs dont une des fonctions consiste à détecter et diagnostiquer les pannes du processus. Il en résulte :

- la suppression des révisions périodiques
- la mise en oeuvre d'interventions de maintenance simplifiées puisque les défauts sont déjà identifiés ; les temps de remise en état peuvent donc être diminués.

2 - Amélioration de la disponibilité d'une rame de métro par tolérance aux fautes

Il est envisageable en effet, à l'issue du dépistage d'une panne, d'analyser son incidence sur la disponibilité (et sur la sécurité). La génération de modes de fonctionnement dégradés permet d'améliorer sensiblement la disponibilité (condamnation de la porte, ou maintien de l'exploitation normale en présence du défaut).

Il est à remarquer que les deux améliorations citées ne s'établissent pas au détriment de la sécurité du système.

Il appartient en effet au dispositif de définir et de faire appliquer en présence de défaut une commande allant vers la sécurité, puis de réceptionner et de retransmettre vers l'exploitant les messages de panne en vue d'une remise en état. Le délai d'intervention peut être déterminé par calcul à partir d'un objectif de sécurité fixé au préalable (1ère partie - paragraphe II₂).

Schématiquement l'étude du problème ainsi défini a été menée en s'attachant à résoudre les points cités ci-dessous et développés dans les paragraphes suivants (2-3-4).

* Décomposition de l'ensemble du processus à commander (6 mécanismes de porte) en une somme de sous ensembles élémentaires (1 mécanisme) pour lesquels les fonctions de sécurité définies plus haut ont été prises en compte et traitées par un microprocesseur spécialisé (monochip Intel. 8051).

* Définition d'un réseau local à voies point à point en étoile réalisant la fonction d'interconnexion et de coordination des divers sous ensembles et dont notamment l'acheminement des informations de panne.

* Etablissement d'une configuration vecteur d'état, vecteur de commande d'un mécanisme de porte suffisante pour permettre au microprocesseur d'opérer la fonction détection et analyse des pannes.

* Application d'une méthodologie de détection et d'analyse des pannes du processus durant les cycles de commande. Le procédé consiste à vérifier l'évolution chronologique du vecteur d'état pendant les phases d'ouverture et de fermeture des vantaux de porte. A chaque changement de valeur du vecteur d'état on effectue un test d'hypothèse en vue de valider ou non le bon fonctionnement, puis si le test n'est pas validé (détection d'une panne) à procéder à d'autres tests d'hypothèse de façon à localiser l'origine et le type de panne.

* Formalisation du problème par représentation des séquences de fonctionnement d'une porte, y compris les procédures de détection et d'analyse de panne, par graphe de Pétri.

* Elaboration d'un logiciel de traitement de la fonction globale décrite par graphe de Pétri selon une méthode basée sur l'évolution synchrone du marquage du graphe.

* Etude de la mise en sécurité du système microprocesseur affecté à la commande d'une porte. L'étude s'oriente vers une méthode de détection d'erreur du microprocesseur par auto-test (traitement d'une fonction équitemps) et vers un dispositif en sécurité intrinsèque de déconnexion et de verrouillage du microprocesseur défectueux.

I₄ - Etablissement de la configuration vecteur d'état, vecteur de commande propre à tenir les objectifs de sécurité

La figure 2-5 présente la nouvelle définition des vecteurs d'état et de commande d'un mécanisme de porte. Cette configuration permet de répondre aux critères définis au paragraphe III₃₋₁₋₂ de la première partie de ce mémoire.

Le nombre de voies du vecteur d'état est tel que le microprocesseur de commande de porte peut détecter et localiser tous les types de panne définis préalablement comme possibles.

Le vecteur de commande est configuré de telle façon qu'une panne simple sur un organe de commande quelconque ne puisse pas présenter vis-à-vis des voyageurs un état contraire à leur sécurité.

I₄₋₁ - Optique sécurité

1 - La commande d'ouverture de porte s'effectue moyennant deux voies de commande indépendantes :

- une commande déverrouillage (DVER) acquittée par l'information verrou (BKPV)

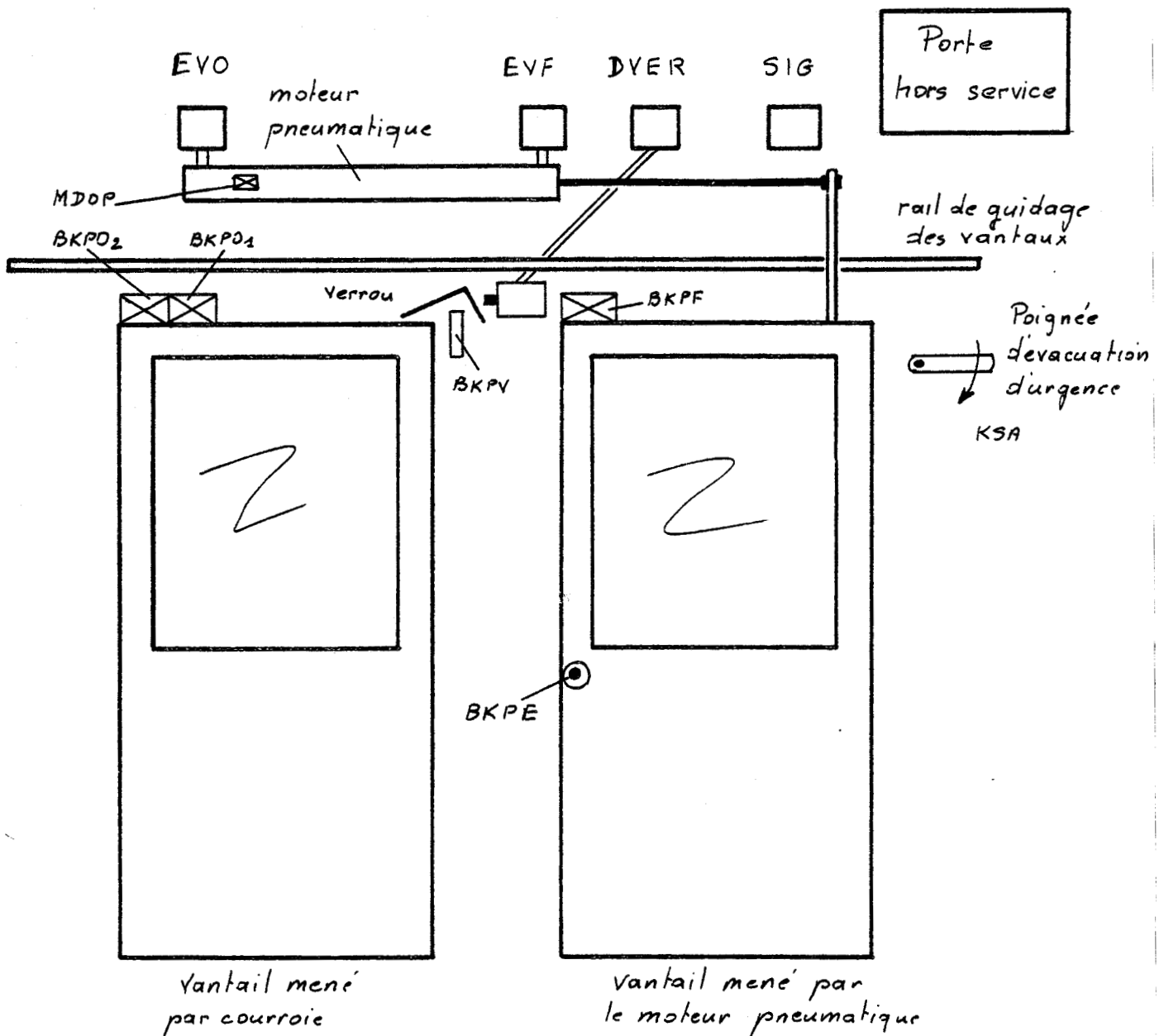
- une commande d'ouverture (EVO) acquittée par les informations . porte en position fermée (BKPF)
. manostat de détection d'obstacle (MDOP)

2 - Deux capteurs indépendants informent de l'état de sécurité porte fermée verrouillée ce sont :

- le contact porte en position fermée (BKPF)
- le contact verrou (BKPV)

Configuration d'un mécanisme de Porte

Figure 2.5



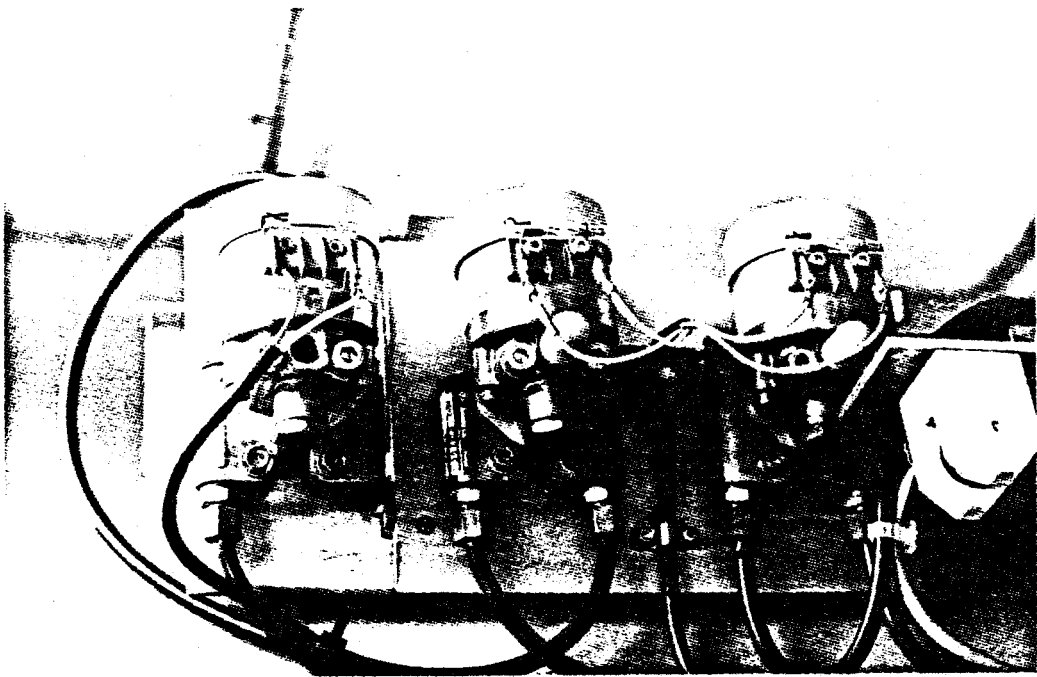
Vecteur de commande

- EVO électrovalve d'ouverture
- EVF - de fermeture
- DYER - de déverrouillage
- SIG signalétique

Vecteur d'état

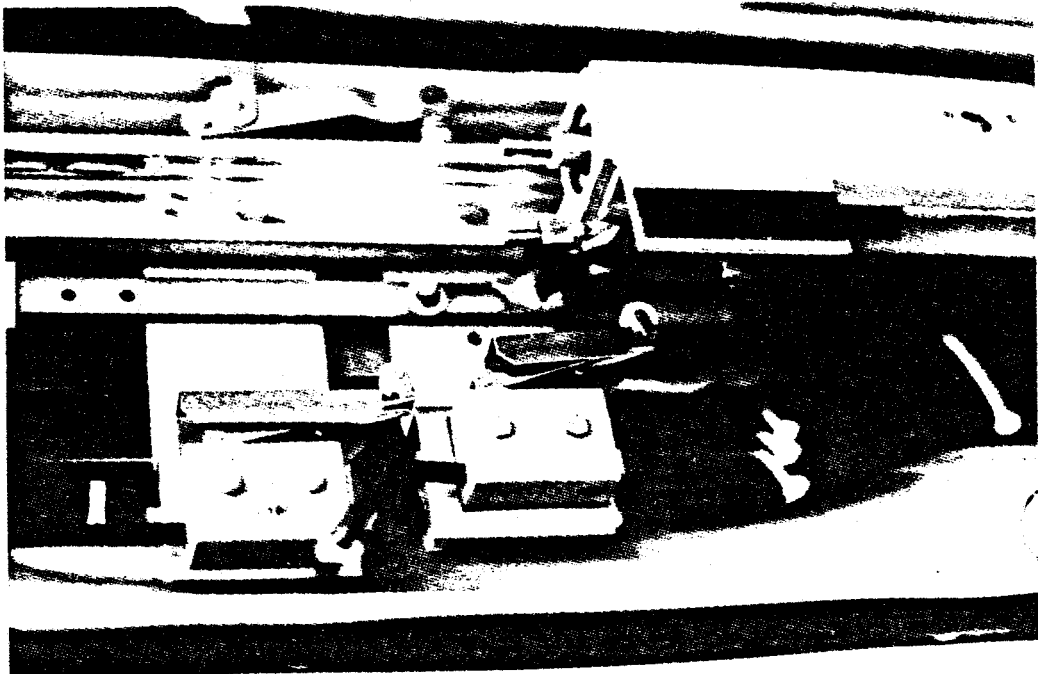
- BKPV contact porte verrouillée
- BKPF - - fermée
- BKPO₁ } contacts porte
- BKPO₂ } ouverte
- KSA contact d'évacuation d'urgence
- MDOP manostat obstacle à la fermeture
- BKPE déverrouillage extérieur





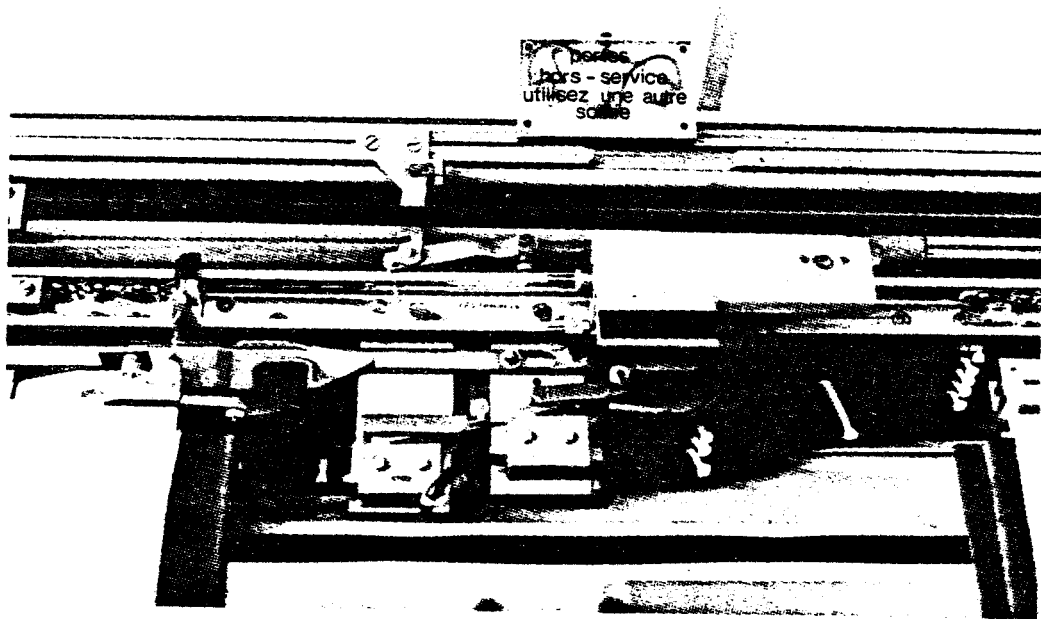
Electrovalves de commande
du moteur pneumatique

photo n° 6



Contacts électriques de position
des vantaux

photo n° 7



Panneau signalétique

photo n° 8



3 - Deux capteurs indépendants assurent la prise en compte d'une demande d'évacuation d'urgence par un passager, à savoir :

- le contact demande d'évacuation d'urgence (KSA)
- le contact verrou (BKPV)

I₄₋₂ - Optique disponibilité

1 - Une plaque signalétique installée sur chaque mécanisme de porte à l'intérieur du véhicule, (voie de commande SIG) informe les passagers que la porte peut être condamnée à l'issue de la détection de certains types de pannes (du microprocesseur par exemple).

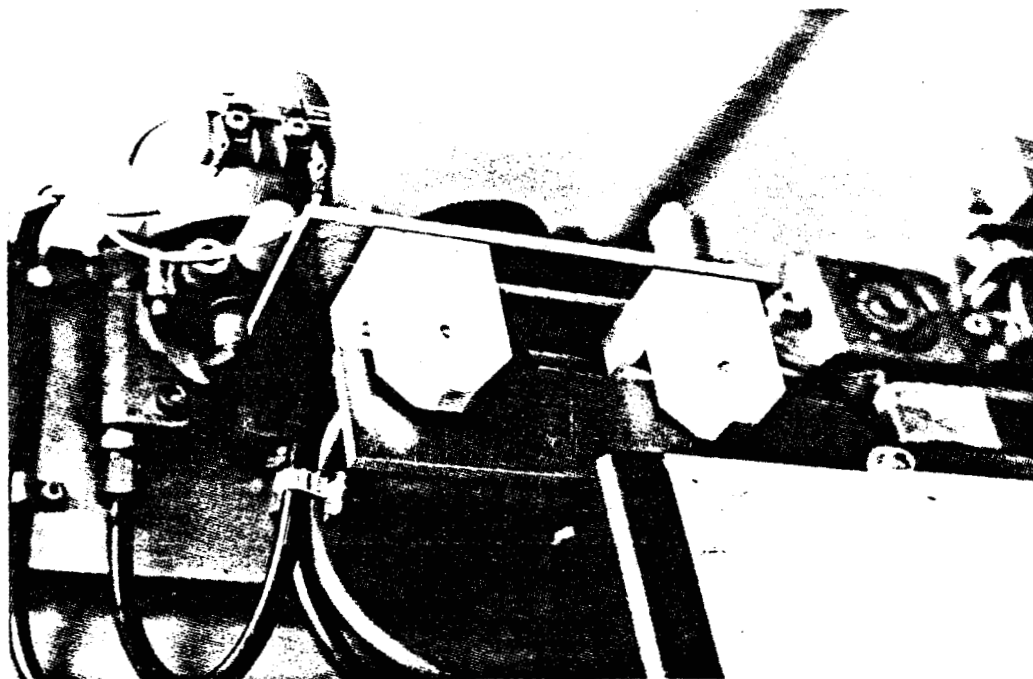
2 - Deux capteurs indépendants porte ouverte (BKPO 1 et BKPO 2) sont disposés sur l'axe horizontal. Le redoncancement de cette information permet d'une part de discriminer bon nombre de défauts et d'autre part autorise le maintien de l'exploitation même en présence d'une de ces voies défectueuse.

La réalisation de ce détecteur porte ouverte redondancée utilise un système magnétique du type détecteur de proximité (Réf. 41). Ce dispositif monté en détecteur à fente peut localiser la présence d'une tôle d'aluminium (épaisseur 3 mm) se déplaçant latéralement dans une fente de 10 mm de largeur. La gamme de température de fonctionnement est comprise entre -20°C et +70°C.

Les avantages que nous dégagons de cette réalisation sont les suivants :

- grande simplicité de mise en oeuvre sur le mécanisme de porte
- absence d'usure mécanique et jeu fonctionnel important à l'intérieur de la fente
- absence de rebondissement lors des changements d'état par un hystérésis réglable sur le détecteur.

Globalement par rapport à la configuration d'origine le nombre de voies de mesure n'a pas changé, l'ancien contact (BKDOP) est remplacé par un second capteur : état porte ouverte. Le nombre de voies de commande est accru ; deux commandes pour actionner le déverrouillage puis l'ouverture et une commande de signalétique.



Détecteurs de proximité donnant
l'indication porte ouverte

photo n° 9



La redondance totale des informations porte ouverte, porte fermée permet au microprocesseur de détecter, par comparaison, la présence d'une panne, puis de continuer l'exploitation à l'aide de l'autre voie après avoir généré un message d'alarme relatif au défaut détecté.

II - DEFINITION DE L'ARCHITECTURE MICROINFORMATIQUE GLOBALE DE COMMANDE DE PORTE AU NIVEAU D'UN VEHICULE D'UNE RAME DE METRO

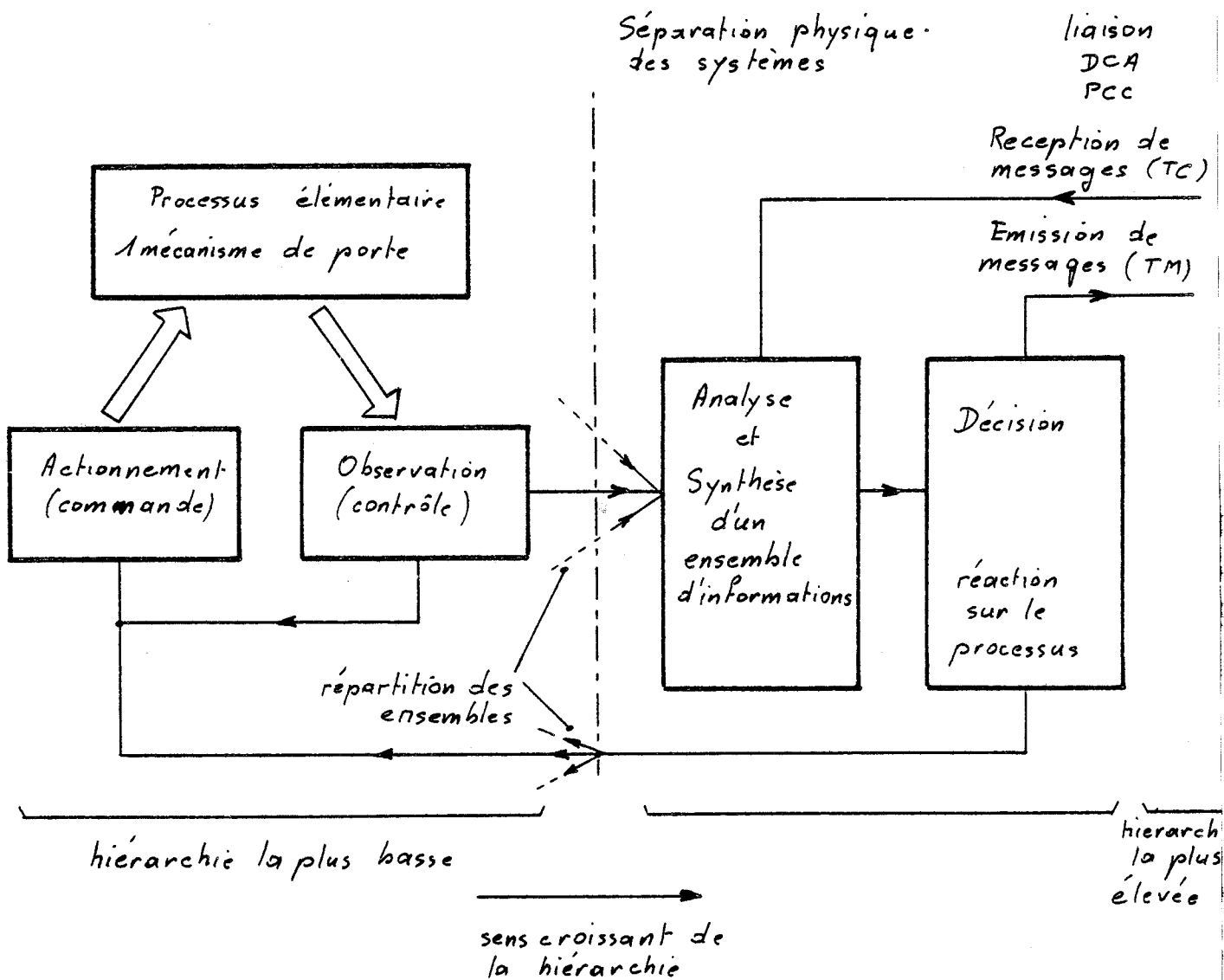
II₁ - Position du problème. Introduction du concept de réseau local étendu à l'ensemble d'une rame de métro formée d'un nombre variable de véhicules

La commande de processus en sécurité développée plus en avant dans ce mémoire met en évidence l'intérêt de l'emploi de structures à intelligence artificielle, ou plus simplement de structures microprogrammées.

Sans revenir sur l'intérêt des choix effectués, il nous semble toutefois important de préciser que la contre partie de cette intelligence réside pour l'utilisateur dans la présence d'une somme d'informations disponibles qu'il faut pouvoir acheminer puis analyser en vue d'en extraire la partie utile.

Les grandes orientations de l'informatique d'aujourd'hui tendent vers la décentralisation ou l'intelligence répartie. Les constructeurs d'appareils d'instrumentation mettent à disposition de véritables réseaux de chaînes d'acquisition et de traitement de données connectables sur bus de liaison (GPIB) où chaque élément est capable d'opérer localement un prétraitement.

Les réseaux de mini informatique appliqués à la gestion ou à la commande d'outils industriels (ateliers flexibles) mettent à profit l'intelligence répartie en vue d'améliorer les rendements par une meilleure scuplesse des capacités de production. Les moyens utilisés sont d'une part le partage des tâches mais aussi la possibilité donnée à un processeur quelconque d'accéder à des ressources communes (banques de données). Il y a véritablement mouvance des informations.



Répartition des tâches sur l'ensemble du dispositif de commande et de contrôle

Figure 2-6



Reprenons l'exemple de la commande d'un ensemble de portes. On peut considérer que chaque unité de commande reçoit des messages de télécommande (TC) spécialisés propres à assurer la fonction attendue d'un mécanisme de porte, en retour elle renvoie des télémessures (TM) pour rendre compte du travail fourni mais aussi pour informer l'exploitant sur l'état de fonctionnement du système, afin de lui permettre de maintenir le niveau de sécurité souhaité.

Il va donc de pair que la conception d'une structure décentralisée s'accompagnant d'un réseau d'interconnexions capable de diffuser les télécommandes et de drainer tous les messages d'état du système.

Dans un ensemble relativement complexe tel une rame de métro automatisée dont l'exploitation s'effectue en temps réel, il est impensable de garder dans l'état toutes les informations de télémessure et de les faire converger puis traiter par le processeur central chargé du pilotage de la rame (DCA) et encore moins par le poste central de commande (PCC). Les informations tant par leur quantité que par leur spécificité ne pourraient que nuire à la bonne marche du système de transport.

Le problème consiste donc à mettre en place un réseau d'interconnexions desservant une architecture hiérarchisée capable de traiter par analyse et synthèse un sous ensemble de messages et capable de prendre localement une décision. Globalement les fonctions traitées peuvent se schématiser par la figure 2.6.

II₂ - Réseau local de commande de processus en sécurité

La fonction du réseau consiste nous l'avons dit à acheminer les informations de télémessure et de télécommande. Les contraintes de sécurité propres à notre étude nous imposent à nouveau de revenir vers les concepts de sécurité.

La caractéristique essentielle de la structure du réseau pourrait être basée sur la notion de sûreté de fonctionnement. Un travail entrepris dans ce domaine traite du problème des réseaux locaux de commande-contrôle sûrs de fonctionnement (Réf. 11). La sécurité est alors de nature probabiliste. L'objectif recherché consiste à améliorer la fiabilité de l'ensemble

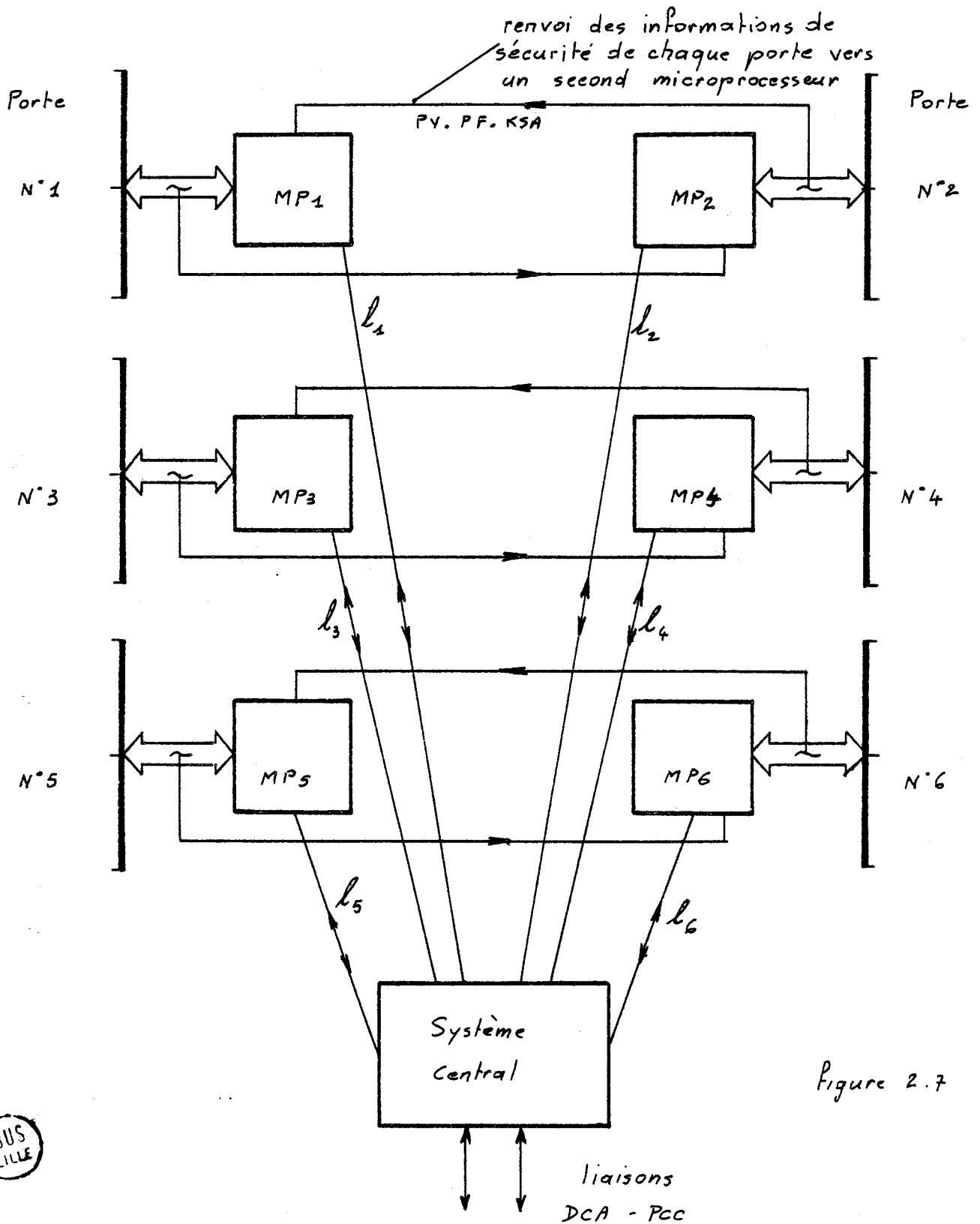


Figure 2.7



Schéma de principe du réseau local de commande-contrôle de porte en sécurité
Bilan des liaisons

en s'attachant à établir, à l'aide du réseau, une répartition des tâches capable de maintenir, même en cas de panne partielle, la fonction demandée.

Ceci nécessite d'établir entre les diverses unités de traitement une coopérabilité telle que la répartition des fonctions puisse se réorganiser selon l'état de fonctionnement des organes constituant le réseau.

Ce point de vue quoique très satisfaisant pour l'esprit, ne nous paraît pas applicable à notre problème, ceci pour plusieurs raisons :

1 - Problème de connectique

L'allocation d'une tâche de commande-contrôle d'un processus nécessite une connexion directe au processeur chargé de cette fonction (vecteurs d'état et de commande). Cette contrainte conduit, dans le cas d'une généralisation du partage des fonctions, à un alourdissement considérable du câblage.

2 - Problème de logiciel

Pour que notre étude puisse à terme trouver un aboutissant industriel, il nous paraît important de minimiser la circuiterie électronique par l'emploi de composants microinformatiques très largement intégrés (monochip). Le faible espace mémoire disponible sur les circuits microcontrôleurs limite d'emblée la sophistication des logiciels (gestion des protocoles d'échanges etc...).

3 - Il existe un état de sécurité

Notre problème, concernant le domaine des transports terrestres, nous autorise l'emploi d'un état de sécurité dont il serait maladroit de ne pas faire usage.

Ces réflexions nous amènent donc à revenir vers les concepts traditionnels de sécurité. Il s'agit alors de réaliser un réseau dont la structure est telle qu'aucune panne simple ne puisse conduire à un accident.

La conséquence de cette proposition impose qu'il faille détecter toutes les pannes dangereuses possibles imputables au réseau et qu'à l'issue de leur détection on puisse imposer à la rame de métro de se placer dans un état de sécurité prescrit (freinage d'urgence par exemple).

Deux procédures distinctes de contrôle sont à réaliser

- A - Vérification fonctionnelle de toutes les liaisons ou de tous les cheminements possibles qu'autorise le réseau.
- B - Vérification à l'aide de codes détecteurs d'erreur que les messages véhiculés par le réseau ne soient pas entâchés d'erreurs, celles-ci pouvant être contraires à la sécurité.

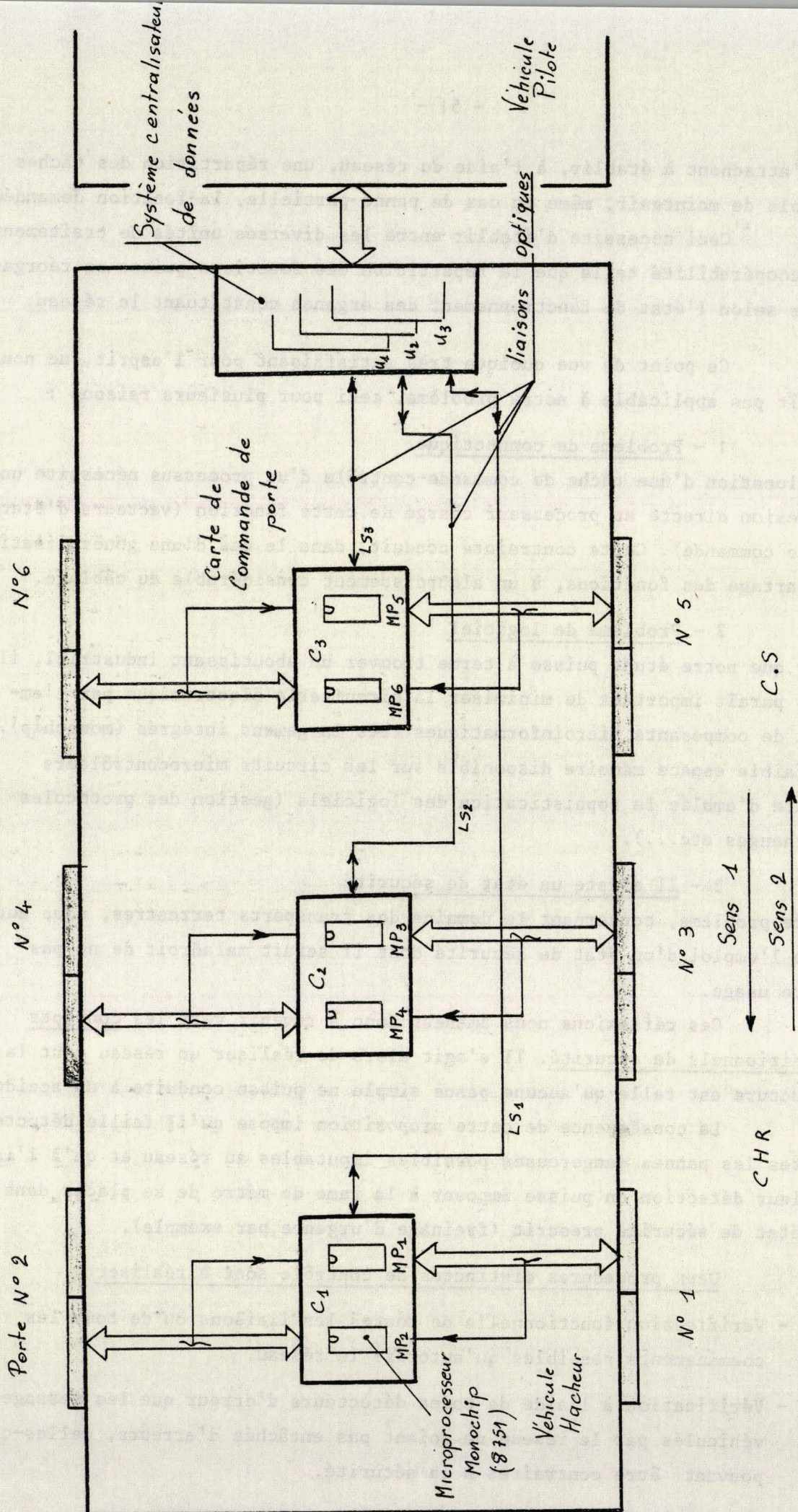


Figure 2.8

Architecture globale du dispositif de commande de porte d'un véhicule d'une rame de métro

La mise en oeuvre de la fonction A a des implications sur le choix du type de réseau. On aura en effet intérêt à employer un maillage simple où le nombre de connexions et de chemins possibles sera réduit au minimum.

Définition du réseau local de commande de porte

Notre travail se limite dans ce mémoire à la définition d'un réseau desservant un véhicule d'une rame de métro. A terme se pose le problème de la connexion entre véhicules et donc de l'extension possible du réseau.

Afin de satisfaire les conditions évoquées ci-dessus le réseau choisi s'apparente à une structure en étoile à voies point à point figure 2.7. De par sa nature toutes les données transitent par le coeur de l'étoile. Ceci est pénalisant pour le débit d'information traité par le réseau, mais par contre la présence d'un système central de traitement permet de gérer complètement la tâche "détection des pannes de liaison" et d'autre part d'assumer la fonction analyse et synthèse des télémessures relatives à l'ensemble des 6 mécanismes de porte.

Physiquement les microprocesseurs sont regroupés deux à deux sur une seule carte, ou carte de commande de porte. Chacun d'eux est connecté au système central par une liaison série bidirectionnelle (L1 à L6) réalisée à l'aide de fibres optiques. Le réseau constitué au sein d'un véhicule est représenté figure 2.8.

II₃ - Rappel de quelques concepts sur les réseaux locaux

A partir d'une normalisation internationale (OSI) (Réf. 49) sur les concepts d'interconnexion des calculateurs hétérogènes dans les réseaux de type à commutation de paquets a été élaborée une hiérarchie des tâches à réaliser dans l'optique de la commande-contrôle de processus répartis sur un réseau local (Réf. 11) - Tableau 2-1.

Cette hiérarchie, plus restreinte, distingue 4 niveaux :

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

Application	Utilisateur
Présentation	
Session	Exploitation
Transport	Transfert
Réseau	
Liaison	
Physique	Transmission

Modèle ISO

Modèle restreint

Correspondance du modèle ISO et de la hiérarchie restreinte
appliquée aux réseaux locaux de commande-contrôle

Tableau 2.1



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

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

- Le niveau de transmission ; à ce dernier stade on réalise l'interconnexion physique des différents systèmes en incluant les problèmes de modulation.

II₃₋₁ - Application au réseau local de commande de portes d'un véhicule

Appliquons ces notions à notre réseau et considérons la répartition des tâches entre les différents systèmes :

- Chaque microprocesseur installé sur les cartes de commande gère le niveau utilisateur, l'utilisation est ici matérialisée par l'ensemble des portes véhicule.

- Le niveau exploitation est traité à la fois sur le système central chargé de l'exploitation de l'ensemble des portes d'un véhicule et sur chaque microcontrôleur (8751) affecté plus particulièrement à la commande d'un mécanisme de porte.

- Le niveau de transfert sera, sous contrôle du logiciel, géré par des unités de transmission série (UART) notamment celles intégrées dans les boîtiers microprocesseur monochip situés sur les cartes de commande

- Le niveau de transmission prend en compte l'interfaçage opto-électronique via le réseau de connexions réalisé par fibres optiques.

II₃₋₂ - Gestion des accès entre les différents systèmes

Sur les réseaux locaux la gestion des accès peut s'envisager de deux façons distinctes

a) la gestion par consultation

la consultation s'opérant par chaînage ou par scrutation

b) la gestion par compétition

après détection et résolution de conflits un dispositif peut émettre un paquet d'informations vers une destination qu'il aura préalablement choisi.

En vertu des contraintes de sécurité qui nous sont posées et du choix que nous avons effectué (recours possible à un état de sécurité), nous pensons que la gestion des accès au réseau par consultation, en mode scrutation, représente le moyen le plus simple à mettre en oeuvre (volume de logiciel) avec l'avantage de pouvoir vérifier sans ambiguïté le bon fonctionnement de toutes les liaisons du réseau.

II₄ - Choix de la technologie optique en tant que support du réseau

Le choix de la technologie optique comme support matériel du réseau s'appuie sur plusieurs raisons que nous exposons ci-dessous

II₄₋₁ - Isolement galvanique

Les différentes cartes constituant l'architecture globale (fig. 2.8) ne sont électriquement reliées que par les lignes d'alimentation (alimentation de sécurité 10 - 15 v avec batterie de secours). L'isolement galvanique apporté par les connexions optiques interdit tout rebouchage électrique d'une carte vers une autre. Le plan de masse de chaque circuit est donc localement défini.

II₄₋₂ - Immunité totale aux perturbations électromagnétiques

Cet aspect est fondamental lorsque l'on considère l'ambiance fortement parasitée d'une rame de métro. Les principales sources de parasites EM sont rappelons le les moteurs de traction, les hacheurs, les dispositifs de captation d'énergie (frotteurs) ainsi que les divers éléments électromécaniques (relais, éclairage etc...).

II₄₋₃ - Marge de sécurité importante sur les performances

Les longueurs de connexions relativement faibles (20 mètres max. pour un véhicule de 13 m de largeur) et le faible débit de transmission

envisagé (inférieur à 10 Kbaud) sont bien en deça des performances des systèmes optiques actuels. On peut donc, à priori, envisager que les voies de transmission introduisent peu d'erreurs. Une étude bibliographique (Réf. 42) a montré que pour un bilan des pertes d'insertion de l'ordre de 20 dB le taux d'erreur se situe à une valeur inférieure à 10^{-8} .

II₄₋₄ - Technologie optique. Etat de l'art et perspective dans son application aux transports terrestres

Quoique particulièrement intéressante par les caractéristiques citées plus haut, l'introduction de la technologie à fibres optiques dans les systèmes de transport terrestres pose quelques problèmes de mise en oeuvre.

1 - Problème de câblage

Le câblage des équipements dans la plupart des systèmes et notamment en transport terrestre nécessite l'emploi d'un nombre important de connecteurs amovibles. Les problèmes rencontrés sont alors les suivants

- les connecteurs optiques sont coûteux
- à chaque connexion amovible vient se joindre une perte d'inversion non négligeable (2dB pour un diamètre de fibre de 100-140 μ m)
- la fiabilité des connecteurs optiques reste à démontrer (tenue aux vibrations etc...) bien que les quelques résultats disponibles soient encourageants : variation d'atténuation de 0,1 dB pour 10^6 cycles 50 Hz - 8 g - 6 mm (Réf. 50).

2 - Coût de mise en oeuvre

L'expérience révèle, qu'au delà des connecteurs, la technologie optique est financièrement coûteuse. Le développement considérable de cette technologie annoncé pour les prochaines années devrait cependant réduire les coûts de mise en oeuvre.

Il nous semble toutefois intéressant de dégager une proposition caractérisant un type de fabrication adapté au domaine des transports terrestres (matériel embarqué).

Les éléments sont les suivants :

- les distances de transmission sont faibles (quelques dizaines de mètres au plus)

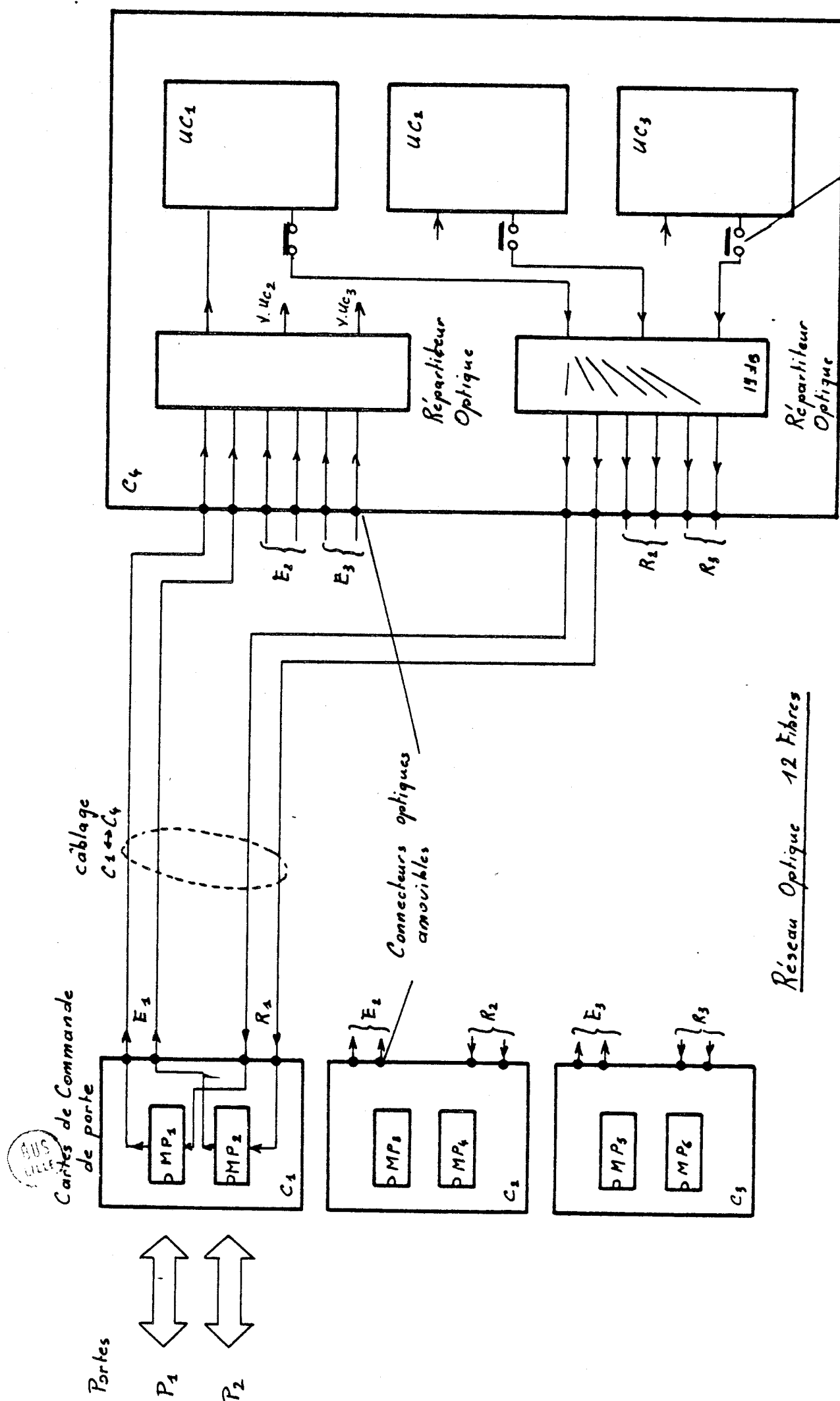


Figure 2.9

Réseau Optique 12 Fibres

Système Central

excitation du réseau par commutation

Pertes d'insertion max 24dB

- les débits sont faibles également (100 K baud constitue un majorant)

- les connexions amovibles sont nombreuses
- des contraintes mécaniques existent (vibrations etc...)

La particularité des produits à développer serait d'utiliser des fibres d'un diamètre plus important que ceux généralement utilisés permettant ainsi de réduire les problèmes mécaniques au niveau des connecteurs amovibles d'où une meilleure fiabilité et à moindre coût (étude Réf. 42).

II₅ - Réalisation d'un réseau local à transmissions optiques de commande de porte véhicule d'une rame de métro

L'examen de documentations sur des familles de composants pour liaisons optiques nous permet de proposer le schéma de la figure 2-9. Le bilan des liaisons est schématisé sur la figure 2-10. L'emploi de coupleurs-répartiteurs optiques permet sur le système central, de minimiser le nombre d'émetteurs et de récepteurs électro-optiques. De plus ces composants, purement passifs, permettent de présenter un isolement galvanique parfait entre les diverses unités de traitement (UC₁).

Il est à noter que les cartes de commande de porte sont placées à proximité des mécanismes (figure 2-8). Cette disposition minimise le câblage entre les divers ensembles. Les lignes de train sont supprimées. Les connexions entre une carte de commande et le système central se ramènent à un câble optique quatre fibres, une alimentation basse tension (10-12 v) et une alimentation moyenne tension (72 v) pour la partie puissance de la commande, rien de plus.

II₅₋₁ - Description fonctionnelle du réseau

Deux types de circuits composent le réseau

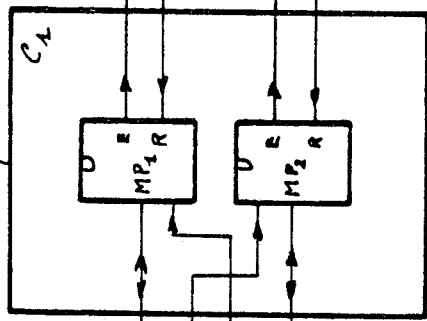
- les cartes de commande de porte (C1 - C2 - C3)
- le système centralisateur de données

II₅₋₁₋₁ - Cartes de commande de porte (Ci)

Elles sont au nombre de trois. Chacune est affectée à la commande de deux mécanismes de porte (figure 2-3). Chaque mécanisme est géré par

BUS LILLE

Carte de commande de Porte

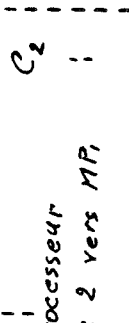


Porte 1

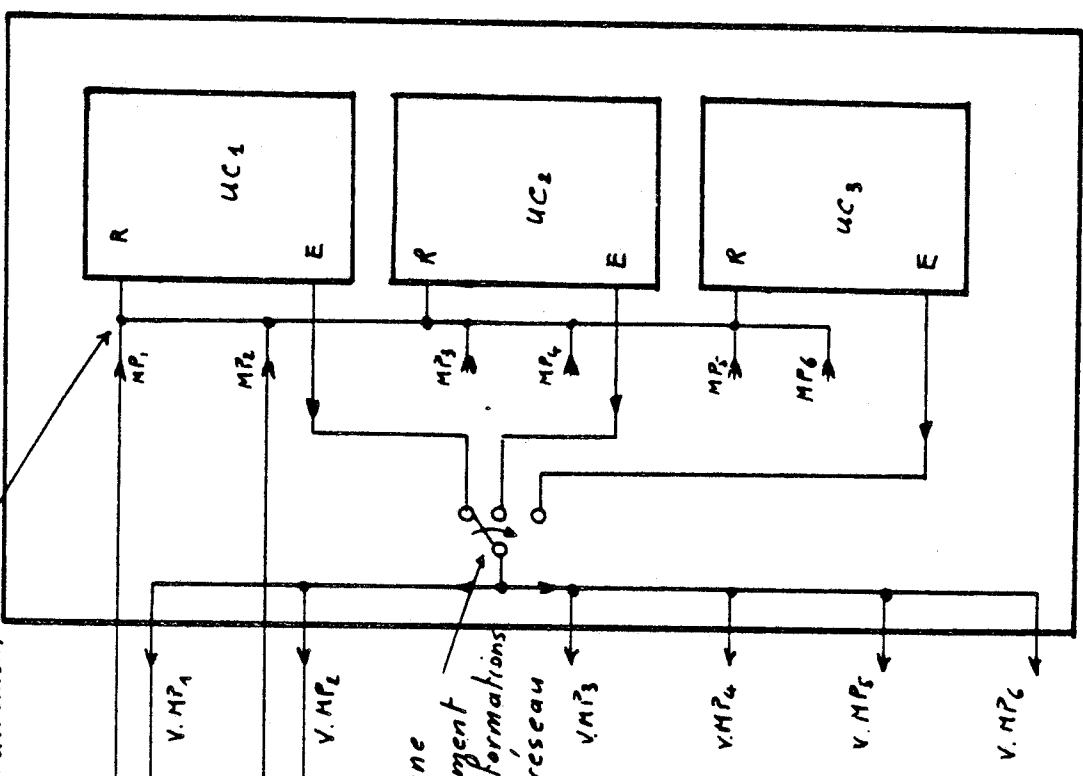
Porte 2

renvoi des informations de sécurité sur le microprocesseur opposé : Porte 2 vers MP1

- PV
- PF
- KSA



Réception des messages sur toutes les unités de traitement



Sélection d'une unité de traitement, diffusion des informations à l'ensemble du réseau

Figure 2.10

Schema fonctionnel des connexions

du réseau local.

Système Central

3 unités de traitement en redondance majoritaire

un microprocesseur monochip (microcontrôleur INTEL 8751), par contre les informations de sécurité relatives à chaque porte sont traitées simultanément par les deux microprocesseurs (états porte fermée - verrouillée - demande d'évacuation d'urgence).

L'étude détaillée de ces circuits est donnée dans le paragraphe IV de cette seconde partie.

II₅₋₁₋₂ - Système centralisateur de données

Ce dispositif a pour fonction la coordination du fonctionnement de l'ensemble des portes d'un véhicule. Trois tâches sont à distinguer :

- élaboration des télécommandes spécifiques à chaque porte
- synthèse de l'ensemble des messages de télémessure
- dialogue avec un autre dispositif microinformatique plus élevé dans la hiérarchie fonctionnelle du système de transport à savoir : dispositif de pilotage automatique (DCA) et poste central de commande (PCC).

La constitution de ce dispositif s'apparente à un système microprocesseur à redondance majoritaire. Chaque unité de traitement (UC₁) reçoit en permanence toutes les informations émises depuis le réseau. Par contre une seule unité, considérée à l'issue de tests comme en fonctionnement correct, peut par commutation accéder au réseau.

L'emploi de ce type d'architecture permet par comparaison puis vote majoritaire de détecter la défaillance d'une unité de traitement. La reconfiguration possible du système par commutation permet de tolérer une défaillance, la fiabilité est donc meilleure. (Annexe 1).

Toutefois dans l'esprit avec lequel nous pensons assurer la sécurité, il faut se mettre à l'abri d'une mauvaise commutation suite à une défaillance du commutateur. Celui-ci ne doit pas pouvoir connecter au réseau une unité de traitement défectueuse.

II₅₋₁₋₃ - Gestion des accès

De la gestion des accès au réseau dépendent les protocoles d'échange de données entre les diverses unités de traitement (C1, C2, C3 et UC₁). C'est, rappelons le, une gestion des accès par scrutation que nous avons retenu.

Reprenons le schéma de la figure 2-7. Les échanges peuvent s'effectuer de la façon suivante :

* au niveau des cartes de commande de porte ; chaque microprocesseur gère son mécanisme, les messages de télémessure résultant de l'exploitation et de l'analyse de l'état du processus sont empilés en mémoire vive en attente d'émission

* le système centralisateur de données lance cycliquement un appel vers chaque microprocesseur (MP_1 à MP_6) pour lui demander d'émettre son paquet de télémessures. Cet appel adressé est décodé puis validé par le microprocesseur concerné. On réalise ainsi la scrutation récurrente de toutes les cartes de commande de porte et de chaque microprocesseur.

Entre deux cycles d'appel le système central établit la synthèse des informations reçues. Celle-ci porte sur l'exploitation normale mais aussi sur l'état de fonctionnement de l'ensemble des mécanismes de porte.

II₅₋₁₋₄ - Mode de fonctionnement dégradé du réseau

La figure 2-7 montre que les informations relatives à la sécurité de chaque porte sont envoyées vers les deux microprocesseurs disposés sur la carte de commande correspondante. Ces connexions supplémentaires sont réalisées en vue d'améliorer la disponibilité offerte par le réseau en présentant deux modes de fonctionnement.

Cette caractéristique permet de minimiser le nombre de fois où l'on a recours à l'état de sécurité de la rame (freinage d'urgence) ceci par tolérance à un défaut de liaison.

1 - Mode de fonctionnement nominal

L'ensemble du système est en état de bon fonctionnement. Chaque microprocesseur de commande de porte dialogue directement avec le système central. Tous les mécanismes de porte sont activés.

2 - Mode de fonctionnement dégradé

Suite à la défektivité d'une liaison entre un microprocesseur (MP_1 à MP_6) et le coeur de l'étoile, ou à la défaillance de l'un des microprocesseurs, le système central peut interroger le microprocesseur conjoint

présent sur la même carte, sur l'état de sécurité de la porte. La connaissance de cet état autorise le maintien de l'exploitation de la rame.

Toutefois l'exploitation du mécanisme de la porte est rendu impossible, celle-ci doit être fermée puis condamnée.

II₅₋₂ - Répartition des fonctions de sécurité sur les diverses composantes du réseau

II₅₋₂₋₁ - Fonctions de sécurité allouées aux cartes de commande de porte

Les cartes de commande de porte doivent assurer chacune la sécurité de la commande du couple du mécanisme de porte mais aussi des connexions au réseau.

* Sécurité de la commande des mécanismes de porte

Les fonctions à assurer sont les suivantes :

- Traitement des fonctions de "sécurité voyageurs" ; évacuation d'urgence, départ portes fermées verrouillées, pas d'ouverture intempestive en ligne.

- Détection, analyse et télésignalisation des pannes pouvant apparaître sur les systèmes de porte. Ces deux aspects sont traités dans le paragraphe suivant (2ème partie paragraphe III).

* Sécurité par rapport à l'ensemble du réseau.

Chaque carte de commande de porte doit présenter par rapport au réseau les caractéristiques suivantes :

- discrimination des faux messages de télécommande reçus par l'emploi de codes détecteurs d'erreur

- codage des messages de télémessure en vue de s'affranchir des erreurs de transmission

- interdiction d'envoi de messages vers le réseau de façon intempestive et non significative (pollution du réseau).

L'ensemble de ces fonctions de sécurité sous entendent que chaque microprocesseur soit lui-même sous test et capable de prendre un état de sécurité (2ème partie, paragraphe IV).

II₅₋₂₋₂ - Fonctions de sécurité du système central

La coordination du fonctionnement de l'ensemble des portes d'un véhicule sous entend l'émission de messages de télécommande cohérents puis la réception et l'interprétation non équivoque des télémessures.

Il faut se prémunir des cas dangereux suivants :

- génération intempestive de faux messages contraires à la sécurité : ouverture des portes en ligne
- mauvaise interprétation des messages reçus du pilote automatique de la rame (DCA) ; ouverture des portes du mauvais côté du véhicule après arrêt en station
- mauvaise interprétation de l'ensemble des messages reçus depuis les cartes de commande de porte : envoi d'un message "ordre de départ de station autorisé" alors qu'une porte ne serait pas en position fermée verrouillée - non prise en compte d'une demande d'évacuation d'urgence.

* La sécurité fonctionnelle de ce dispositif s'articule sur deux points :

1 - utilisation de procédures de codage et de décodage d'informations en vue de s'affranchir des erreurs de transmission ; application des codes arithmétiques par exemple. La probabilité résiduelle de non détection d'erreur doit être inférieure à une valeur que l'on peut considérer comme hautement improbable

$$\text{soit } P < 10^{-10}$$

2 - Traitement de la fonction détection des pannes de liaison à l'intérieur du réseau. Cette procédure peut être mise en oeuvre lors de la scrutation de tous les microprocesseurs de commande de porte (MP₁ à MP₆).

* La sécurité structurelle est comme nous l'avons dit liée à la détection du mauvais fonctionnement d'une unité de traitement (UC_i) par vote majoritaire ainsi qu'à la sécurité propre du commutateur de sélection d'une unité vers le réseau.

II₆ - Conclusion

En conclusion à ce paragraphe il nous semble important de dégager le double objectif recherché dans cette réalisation.

Le premier, primordial, est celui de la sécurité, il pose ses contraintes et oblige de par le concept de sécurité choisi à maintenir l'ensemble du réseau en auto-diagnostic permanent en vue d'appliquer s'il y a lieu un état de sécurité vis-à-vis des voyageurs.

Le second objectif vise la disponibilité. Le compromis à résoudre consiste à concevoir un réseau au maillage simple mais pour lequel il existe quand même un mode de fonctionnement dégradé à partir duquel on puisse maintenir l'exploitation même en présence d'un défaut.

L'emploi d'éléments microprogrammés sur les diverses composantes du réseau autorise la mise en oeuvre de ces fonctions et réalise le compromis sécurité disponibilité sans intervention humaine.

L'objectif recherché par ce compromis étant de réduire au minimum le nombre de messages d'alarme transmis au PCC et accompagnés d'une perturbation du trafic sur le réseau de transport. Le système s'auto-maintient en exploitation (en mode dégradé ou non) le temps nécessaire d'une remise en état de l'équipement défectueux tout en maintenant le niveau de sécurité à sa valeur nominale (1ère partie - paragraphe II₅).

III - DETECTION ET ANALYSE DES PANNES DU PROCESSUS PAR ANALYSE SEQUENTIELLE
DU VECTEUR D'ETAT

III₁ - Description des séquences de commande de porte

Avant d'entrer plus en détail sur le procédé de détection de panne nous nous proposons de décrire les différentes phases de fonctionnement des mécanismes de porte. Celles-ci sont toutes représentées à l'aide de graphe de Pétri dont nous présentons le détail en annexe 2.

III₁₋₁ - Séquences de commande du mécanisme de porte en mode normal

La commande d'ouverture ne présente pas de dispositions particulières. La commande de fermeture présente trois phases consécutives.

1 - Début de fermeture sans possibilité de réouverture sur obstacle. Cette phase dure le temps nécessaire (0,6 sec.) pour présenter un aspect dissuasif vis-à-vis d'un voyageur qui s'interposerait intentionnellement à la fermeture. La temporisation échue, les vantaux de porte ont parcouru le tiers de la trajectoire de fermeture pour une pression d'air comprimé nominale (10 bars).

2 - Fin de fermeture, à ce moment la réouverture sur obstacle est possible, elle s'opère de façon identique aux portes véhicule VAL ligne N° 1. En cas d'obstacle permanent une télésignalisation graduée, fonction du nombre de réouvertures, est générée en vue d'alerter le poste central de commande (PCC) via le système central de commande de porte. Il est en effet concevable par une communication phonique depuis le PCC, ou par synthèse vocale à bord des véhicules, de faire participer les voyageurs en dégagement de l'obstacle.

3 - Séquence de non-entraînement après fermeture et verrouillage de la porte (ce cycle est décrit dans les fonctions de sécurité ci-dessous).

Sécurité fonctionnelle présentée par les systèmes de porte vis-à-vis des voyageurs

- Demande d'évacuation d'urgence. Cette fonction est traitée prioritairement et de façon redondante par les deux microprocesseurs disposés sur une carte de commande de porte. Cet appel, par poignée accessible sur chaque porte,

après interprétation est transmis sous forme de message codé vers le système central en vue de l'exécution de la procédure sécuritaire de coupure de la fréquence sécurité et de la haute tension (FS-HT) et du déclenchement du freinage d'urgence.

- Vérification de l'état porte fermée verrouillée lorsque le véhicule est en ligne et au démarrage de station, par scrutation permanente du mot d'état correspondant à cette position.

- Traitement de la fonction porte non entraînée. Cette fonction proposée par Mr le Pr Gabillard a pour but d'apporter aux voyageurs un état de sécurité supplémentaire.

La souplesse de programmation du microprocesseur aidant il est concevable (et démontré pratiquement au Laboratoire) de relâcher la commande de fermeture, donc la poussée du moteur pneumatique le temps que le véhicule quitte la station. Cette liberté supplémentaire autorise la réouverture sans effort des vantaux de porte d'une distance limitée par le pêne de verrouillage (Réf. 41).

Cette fonction de sécurité "dynamique" devrait permettre un dégagement in extremis d'objets de faible épaisseur lors du redémarrage d'une rame en station.

III₁₋₂ - Séquences de commande en mode dégradé

La finalité des séquences de fonctionnement en mode dégradé est de conférer une meilleure disponibilité au système de transport par minimisation des temps d'arrêt dûs aux défauts de porte. Le choix du mode de fonctionnement dégradé est lié au type de défaut reconnu.

Outre les cas où la présence d'un défaut est toléré donc sans modification apparente des cycles de commande, trois modes de fonctionnement dégradés sont proposés.

1 - Condamnation de la porte

Le mécanisme de porte est immobilisé en position fermée jusqu'au moment où interviendra le dépannage. Les passagers peuvent utiliser les autres portes mises à leur disposition, un panneau signalétique visible depuis l'intérieur du véhicule informe de cet état de fait.

2 - Fermeture en mode dégradé

Ce mode de fonctionnement intervient à l'issue d'une panne sur le manostat de détection d'obstacle. La fermeture des vantaux de porte s'établit alors en supposant des obstacles fictifs. Cette séquence permet en outre d'améliorer le confort des passagers, mais aussi d'éviter le coincement d'un obstacle et donc une immobilisation permanente du mécanisme de porte.

3 - Inhibition de la séquence "porte non entraînée"

La sécurité du non entraînement repose sur le fait que la porte reste mécaniquement verrouillée. Si une commande intempestive du verrou ou une coupure impossible de son alimentation se produit ou ne peut plus valider la sécurité de cette séquence de fonctionnement du système de porte.

III₂ - Présentation de la méthode de détection des pannes du processus sous contrôle

III₂₋₁ - Hypothèses de travail

L'utilisation des graphes de Pétri pour décrire les séquences de fonctionnement confère beaucoup de rigueur quant à la définition des états successifs que prendra le processus.

Les déroulements des séquences ont été déduits du cahier des charges mais aussi d'une étude détaillée du fonctionnement du mécanisme de porte tant en état correct qu'en considérant la présence de pannes possibles.

Trois hypothèses sont à prendre en compte dans ce qui va suivre

* Le vecteur d'état d'un système de porte comprend 6 bits d'information, chaque bit est lié à un capteur indépendant des 5 autres. Les valeurs successives que prendra le vecteur en fonction du temps seront liées à la chronologie établie par la position respective des capteurs (contacts de fin de course) disposés sur le mécanisme de commande de porte. Cette chronologie est parfaitement identifiée et invariable pour chaque phase de déplacement des vantaux de porte.

* Pour que la détection des pannes soit sans équivoque, nous avons supposé que celles-ci ne pouvaient se manifester qu'une seule à la fois. La conception de l'électronique de la carte de commande a été faite dans cet état d'esprit. Nous nous sommes attachés à ce que toutes les voies (mesure et commande) soient indépendantes, l'apparition d'une panne n'entraîne donc pas de cascade d'avarie telle que plusieurs défauts soient générés par un mode commun.

* Enfin la procédure de détection de panne s'entend avec des types de défauts reconnus comme possibles par une étude technologique des composants utilisés.

III₂₋₂ - Modélisation des pannes

Toute la procédure de détection et d'analyse des pannes que nous allons décrire couvre l'ensemble des matériels interconnectés au microprocesseur à savoir :

- le processus commandé ; mécanisme de porte, motorisation guidage des vantaux et conjugaison de mouvement

- les voies de commande depuis le port de sortie du microprocesseur, l'électronique de conditionnement du signal, le transistor MOS de puissance et l'actuateur (électrovalve) figure 2-11

- les voies de mesure comprenant le port d'entrée du microprocesseur, la chaîne de traitement avec pour chaque voie le photocoupleur assurant l'isolement galvanique, ainsi que le capteur (contact électrique ou détecteur de proximité) figure 2-12.

Types de pannes considérés comme possibles

Pannes relatives au mécanisme et à la motorisation de la porte

L'ensemble du système mécanique a pour fonction le guidage et la transmission de mouvement aux vantaux de porte. Le mode de défaillance principal d'un tel dispositif se ramène à l'immobilisation ou à un actionnement difficile des vantaux à un endroit quelconque entraînant un temps d'ouverture ou de fermeture prohibitif. Ceci est possible par grippage mécanique dû lui-même à l'usure ou à un graissage insuffisant.

Schéma détaillé d'une voie
de commande

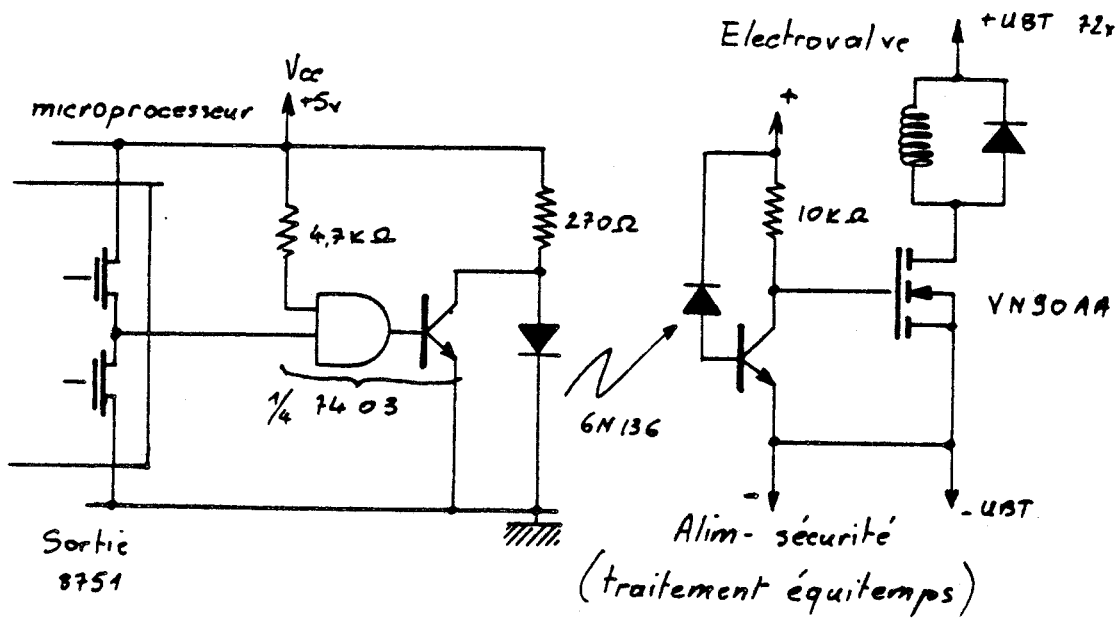


Figure 2-11

Schéma détaillé d'une voie
de mesure

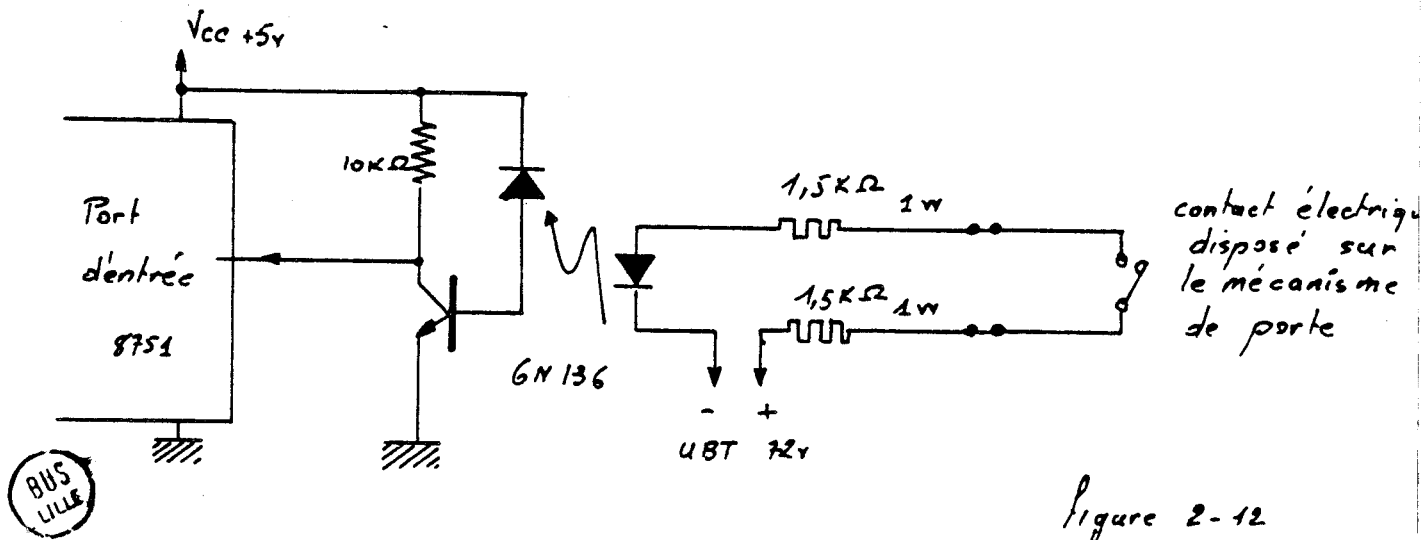


Figure 2-12

Pannes sur les voies de commande (déverrouillage - ouverture - fermeture)

Par rapport aux fonctions à exécuter, les pannes considérées comme possibles sont les suivantes :

- collage d'un état en cours
 - . soit collage en position alimentation permanente d'air comprimé
 - . soit collage en position alimentation interrompue d'air comprimé
- possibilité à tout moment d'un changement d'état intempestif conduisant à annuler ou à rendre contraire le sens de la commande.

Pannes sur les voies de mesure (états Po_1 - Po_2 - PV - PF - EVAC - MDOP)

En se plaçant à l'entrée du microprocesseur les pannes considérées comme possibles sont :

- collage dans un état 0 ou 1
- changement d'état intempestif

Compte tenu des structures de schéma utilisées (figure 2-11 et 2-12) où l'on constate qu'il n'existe pas de rétrobouclage, nous n'avons pas retenu les pannes du type relaxation, par contre nous avons tenu compte des rebondissements des contacts électriques.

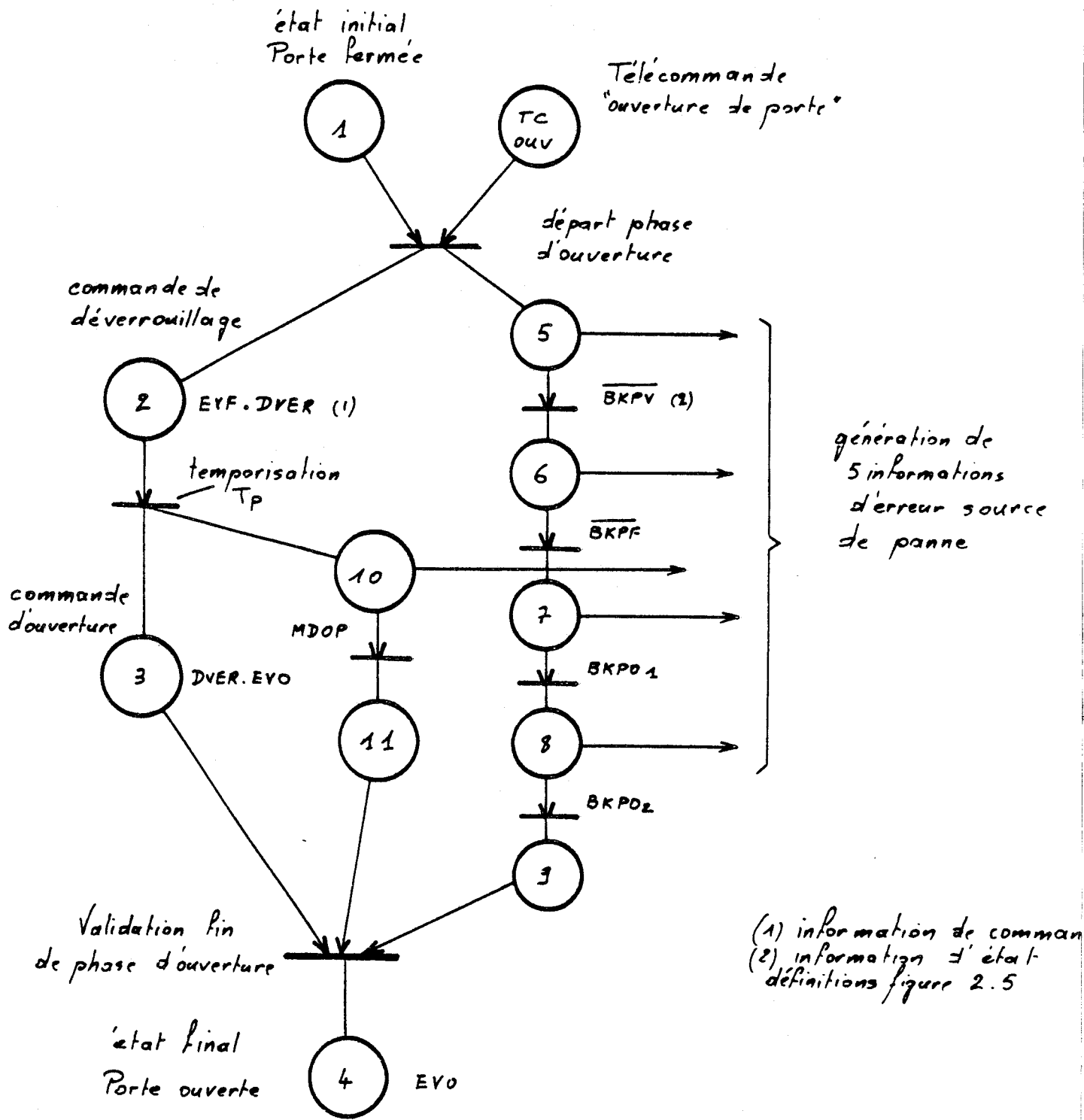
Une fonction anti-rebondissements traitée par programme lors du franchissement d'une transition du graphe de Pétri permet de nous affranchir de ce problème.

III₂₋₃ - Mode d'observation du fonctionnement du processus

Deux types d'observation du processus sont réalisés

1 - Vérification de la bonne chronologie des changements de valeur du mot d'état, ceci durant les phases d'ouverture et de fermeture du mécanisme de porte. Cette procédure suffit à détecter toutes les pannes du système de porte modélisées sous forme de collage.

2 - Détection des changements de valeurs intempestives du mot d'état lorsque la porte est fermée verrouillée et que le véhicule est en ligne. Le traitement de la fonction de sécurité "ouverture des portes en ligne" nous a obligé à développer cette fonction. Pour ce faire il nous a



Représentation de la partie opérative

détection des pannes.

Figure 2-13

Séquence d'ouverture de porte

fallu établir une procédure étendue de détection des changements d'état intempestifs dûs non seulement à une ouverture effective du système de porte mais aussi à l'apparition de défauts sur toutes les voies de mesure.

Considérons les figures 2-13 et 2-14 où l'on représente les graphes de Pétri correspondants aux phases d'ouverture et de fermeture du mécanisme de porte.

A chaque place du graphe correspond un état stable et défini du mot de commande délivré au mécanisme de porte.

Chaque transition représente une évolution du fonctionnement du processus. Celle-ci prend naissance de plusieurs façons :

- soit sur le mot d'état par changement de valeur d'un bit d'information
- soit à partir des sollicitations extérieures ; télécommandes d'ouverture, de fermeture ou par génération de séquences de temporisation, ou par validation du tir d'une transition suite au passage d'un test préalable.

III₂₋₄ - Procédure de détection et d'analyse de panne

Détection de panne

En temps réel le microprocesseur affecté à la commande de porte suit l'évolution du mot d'état, celle-ci fera évoluer conformément à la description, le marquage du graphe de Pétri.

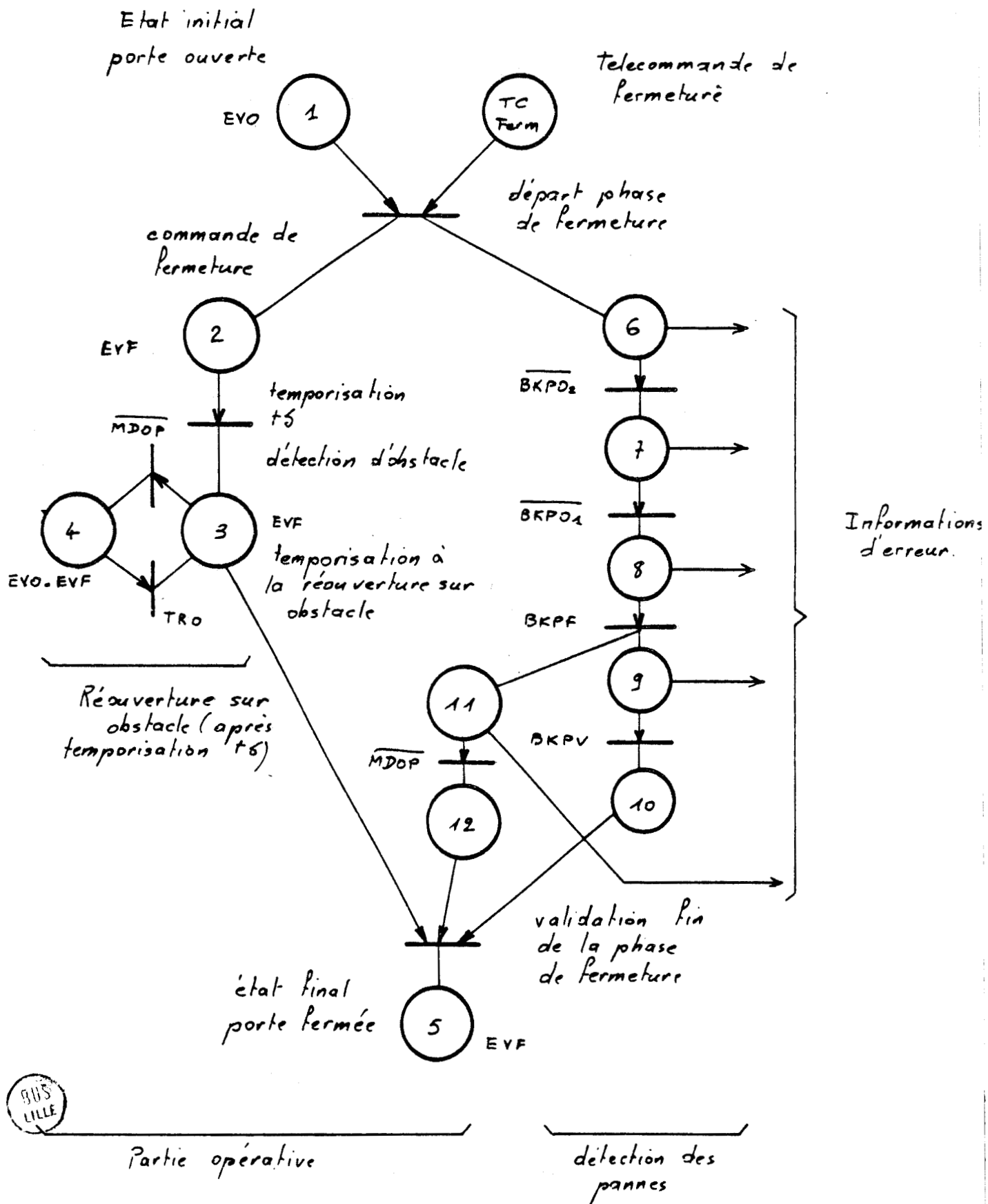
Considérons les exemples illustrés par les figures 2-13 et 2-14 si l'évolution est normale, les transitions se succédant, on parcourt sans se dérouter les cycles de vérification de la bonne chronologie du mot d'état

- places 5 à 11 pour la phase d'ouverture fig. 2-13
- places 6 à 12 pour la phase de fermeture fig. 2-14

Si un défaut intervient, la chronologie des transitions n'est plus respectée. On peut alors par tests d'hypothèse :

- vérifier une autre chronologie vraisemblable
- discriminer par temporisation, le non actionnement d'un organe de commande ou une défectuosité d'une voie de mesure.

Pour chaque phase de fonctionnement (ouverture ou fermeture) on génère 5 informations d'erreur correspondant à la fonction de détection de panne.

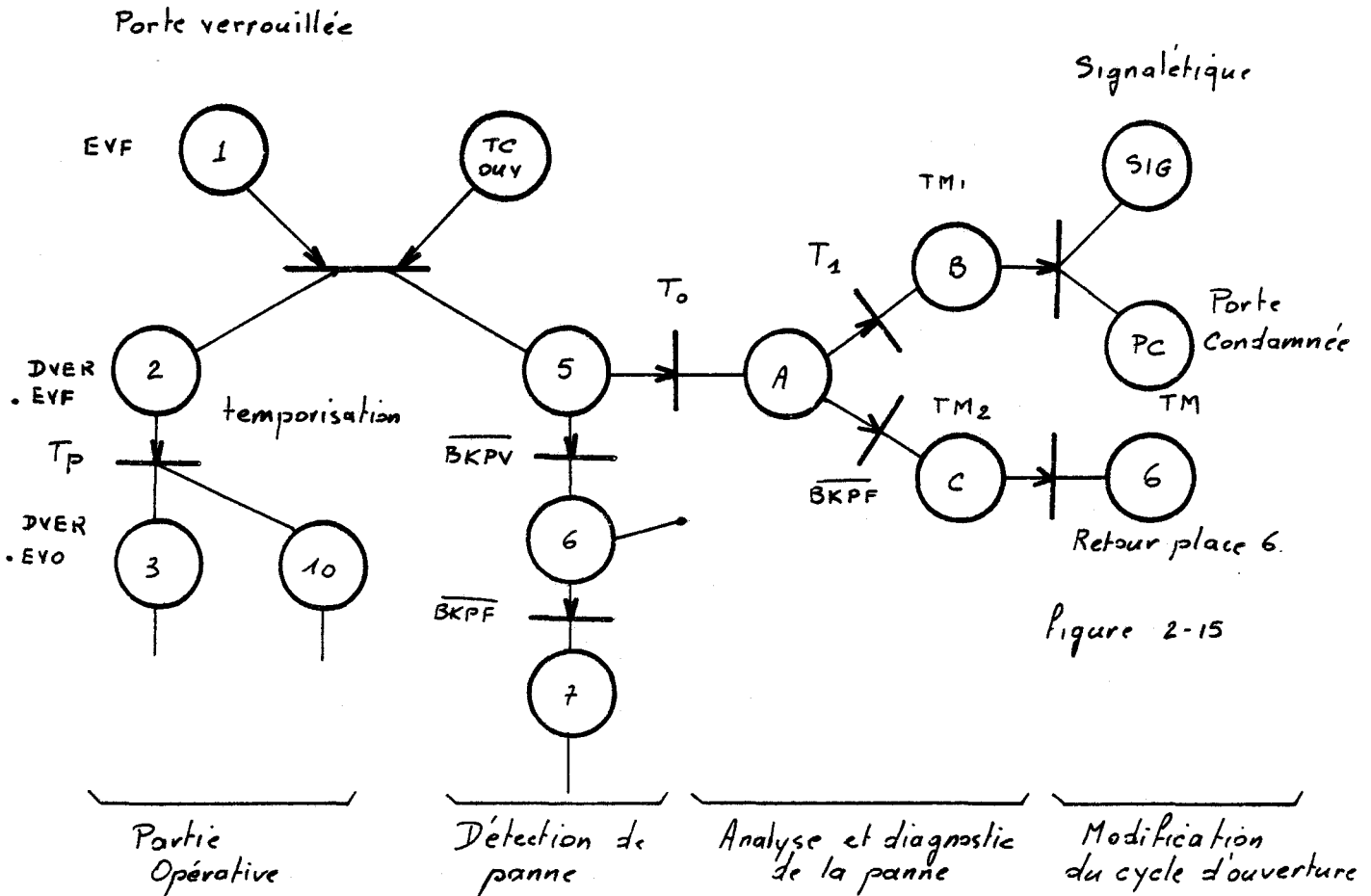


Séquence de fermeture

Figure 2-14.

Localisation de la panne

Illustrons nos propos par l'exemple de la figure 2-15. A l'issue de la télécommande d'ouverture, on vient actionner le déverrouillage puis, après une temporisation de 0,1 seconde, l'ouverture des vantaux de porte



Le mot d'état évolue de la façon suivante :

- changement de valeur de l'information verrou (BKPV) après activation du déverrouillage (DVER)
- changement de valeur de l'information porte fermée après commande d'ouverture (EVO)

Supposons que la transition BKPV ne puisse être franchie suite à une défectuosité, le microprocesseur peut démarquer la place 5 au terme d'une temporisation T_0 . La valeur de T_0 étant par hypothèse prise comme une valeur majorante du temps de réponse de la commande de déverrouillage. La place A est alors marquée, une panne est détectée.

On peut alors lancer deux nouveaux tests (transitions T_1 et \overline{BKPF}) vérifiant les hypothèses suivantes :

1 - si après un temps T_1 échu, temps nécessaire pour ouvrir normalement la porte, rien ne se passe ; la commande de déverrouillage est défectueuse, la porte ne peut s'ouvrir.

2 - si après le marquage de la place A la transition \overline{BKPF} est franchie cela signifie que la voie de mesure de l'information verrou est défectueuse. Autrement dit la porte s'est ouverte mais le changement d'état du verrou n'a pas été perçu.

Génération d'une commande en mode dégradé

L'origine de la panne étant à présent identifiée, on peut effectuer un choix sur le mode de fonctionnement du système de porte et de là engendrer plusieurs actions. Globalement par rapport à la disponibilité, deux types de panne sont à détecter :

- Les pannes sans incidence pour l'exploitation. Elles sont généralement situées sur les capteurs ou les voies de mesure, la configuration redondante du vecteur d'état autorise la présence d'un défaut sans incidence apparente pour l'exploitation.

- Les pannes contraires à la disponibilité (voies de commande, mécanismes). Les séquences de fonctionnement en mode dégradé ont alors pour but de minimiser les phases de fonctionnement durant lesquelles la rame de métro reste immobilisée porte ouverte en station. La description de ces séquences a été donnée ci-dessus.

III₂₋₅ - Remarque sécurité sur la détection des pannes

La remarque sécurité que nous formulons vient en conséquence de la seconde hypothèse de travail présentée plus haut ; en effet la présence d'un défaut rend caduque la procédure de détection et d'analyse des pannes. Il faut donc pour la sécurité, après avoir détecté et signalé le défaut à l'exploitant, qu'une remise en état du système soit envisagée dans un délai inférieur à celui calculé à partir des objectifs de sécurité (1ère partie paragraphe II₃₋₁₃).

Autrement dit la présence du défaut n'est tolérée que momentanément, et en s'arrangeant pour que durant cette période la probabilité d'apparition d'un second défaut, qui pourrait être contraire à la sécurité, soit négligeable.

Cette proposition est vraie quelle que soit la panne détectée. Les tests d'hypothèse effectués peuvent en effet s'appuyer sur l'une quelconque des informations restant disponibles sur le vecteur d'état.

Pour tolérer la présence de plusieurs défauts il faudrait accroître la quantité d'informations délivrées au microprocesseur. Ceci ne nous paraît pas utile dans la mesure où les temps de tolérance de défaut sont conciliables avec les temps d'intervention des agents de maintenance (voir paragraphe III₄).

III₃ - Logiciel de traitement du graphe de Pétri

Le microprocesseur affecté à la commande du mécanisme de porte exécute un programme dont la fonction consiste à suivre l'évolution du marquage du graphe de Pétri selon les règles qui leur sont applicables (Réf. 51). Une méthode d'implémentation de programme mise au point pour le microprocesseur utilisé (8051) a été développée au Laboratoire (Réf. 37-38). Elle permet à partir d'un graphe, dont on a vérifié au préalable qu'il était sain et vivant, de faire exécuter toutes les séquences décrites.

La méthode employée suppose une évolution synchrone du marquage ; après validation du tir d'une transition, on fige momentanément l'état du vecteur d'entrée tant que toutes les places descendantes ne sont pas affectées du marqueur qui leur revient.

Cette hypothèse s'applique aisément à notre problème dans la mesure où le traitement relatif au marquage d'une place s'effectue bien plus rapidement (environ 100 μ sec) que l'évolution la plus rapide du processus (1000 fois plus lente).

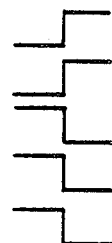
A chaque place correspond un module de programme indépendant. Une place est physiquement représentée par l'adresse en mémoire de ce module. Le chaînage du traitement de N places marquées à un moment donné est géré par un programme moniteur.

RECAPITULATIF DES PANNES DETECTEES* Phase d'ouverture des vantaux de porte

- Vérification des transitions sur les bits d'information du mot d'état
 - BKPV
 - BKPF
 - MDOP
- 1 état actif du contact électrique BKPO 1
- 0 état passif du contact électrique BKPO 2
- Vérification des commandes :
 - activation DVER
 - activation EVO
 - coupure EVF

* Phase de fermeture des vantaux de porte

- Vérification des transitions sur les bits d'information du mot d'état
 - BKPV
 - BKPF
 - MDOP
 - BKPO 1
 - BKPO 2
- Vérification des commandes :
 - coupure EVO
 - coupure DVER
 - activation EVF

* Phase porte fermée, véhicule en ligne

détection des changements d'état intempestifs	<u>voies de mesure</u>	<u>voies de commande</u>
	mot d'état	
	BKPV	commande intempestive DVER
	BKPF	
	BKPO 1	
	BKPO 2	
(1) ambiguïté	MDOP	commande intempestive EVO
(2) non détectée		coupure intempestive EVF

(1) l'ambiguïté sera levée au cycle d'ouverture suivant (la porte reste verrouillée)

(2) le défaut sera détecté au cycle de fermeture suivant.

Le programme moniteur permet, à l'aide de protections logicielles, de faire évoluer le marquage de façon non équivoque. On peut démarquer une place puis, par voie de conséquence, en marquer une ou plusieurs autres sans que ces opérations puissent détruire les marqueurs des autres places en attente de traitement, et non concernées par la transition qui vient d'être franchie.

La méthode présentée a été appliquée à la gestion du graphe représenté en annexe 2. A titre indicatif le logiciel développé pour le traitement des 60 places occupe un espace mémoire de 3 kilo octets environ. Le langage d'écriture du programme est l'assembleur. Le détail du travail est donné dans la référence bibliographique N° 39.

Nous attirons l'attention sur les choix qui ont été opérés dans cette partie de l'élaboration du projet. Les objectifs à atteindre étaient les suivants :

- utiliser une méthode simple et rigoureuse de description du fonctionnement du système de porte par graphe de Pétri

- mettre au point un outil proche de la méthode de description permettant d'écrire un logiciel très modulaire donc fiable et évolutif.

Cette démarche vient s'inscrire dans le sens de la réalisation de progiciels (produits logiciels) peu répandus en ce qui concerne les graphes de Pétri mais à l'étude chez certains constructeurs d'équipements informatiques appliqués à la commande de processus industriels Réf. 25. L'outil de description utilisé est en général le Grafset.

III₄ - Bilan de la fonction détection et analyse de panne. Périodicité du cycle de détection. Temps de tolérance aux fautes.

Le tableau ci contre nous montre que les trois phases de fonctionnement du mécanisme de porte durant lesquelles on effectue la détection des pannes suffisent à fournir toutes les informations utiles.

* Toutes les pannes du type collage de contact sur le vecteur d'état sont détectées. On vérifie en effet pour chaque bit les transitions montantes et descendantes activées durant les phases d'ouverture et de fermeture des portes.

* Tous les collages sur les voies de commande sont détectés (homis la signalétique pour laquelle il n'existe pas d'informations de retour).

* Durant l'état porte fermée verrouillée, véhicule en interstation tous les changements d'état intempestifs sont détectés. Il subsiste toutefois une ambiguïté entre une défectuosité soudaine du manostat de détection d'obstacle (MDOP) et une alimentation intempestive de l'électrovalve d'ouverture (EVO), de même une coupure intempestive de l'électrovalve de fermeture ne sera pas détectée instantanément.

Il est à noter que l'apparition de ces défauts en ligne n'expose pas les voyageurs à une insécurité, de plus ils seront détectés lors de l'ouverture des portes à la station suivante.

Indisponibilité d'une rame de métro engendrée par un de ses mécanismes de porte

Malgré la procédure de détection et d'analyse des pannes, ainsi que la génération possible de commande en mode dégradé, il subsiste quelques cas résiduels de pannes qui conduisent à immobiliser la rame de métro porte ouverte en station.

Les cas de pannes contraires à la disponibilité sont les suivants

1 - Présence d'un dur mécanique dans le système de porte :

* à l'ouverture ; à ce moment on tente une refermeture, si celle-ci s'avère impossible il faut appeler un agent itinérant

* à la fermeture ; si un appel sonore à la coopération des passagers ne suffit pas à refermer la porte il y a lieu de faire déplacer un agent.

2 - Lors de l'établissement de la commande de fermeture deux types de pannes peuvent immobiliser la porte en position ouverte :

* coupure impossible de l'électrovalve d'ouverture (EVO)

* alimentation impossible de l'électrovalve de fermeture (EVF).

Nous remarquons que ces deux types de défauts, pour être pénalisants du point de vue de la disponibilité, doivent se produire après que

la porte ait pu s'ouvrir normalement. En effet durant le cycle précédent de fermeture et durant l'état porte fermée on a vérifié que ces pannes n'existaient pas sinon on aurait condamné la porte à l'état fermé.

La durée d'occurrence de ces deux défauts contraires à la disponibilité est donc réduite dans un rapport que nous évaluons comme suit :

Soit le coefficient

$$R = \frac{\text{temps d'ouverture de porte en station}}{\text{temps total d'exploitation}} \neq 0,2 \text{ valeur majorante}$$

Le taux de défaillance horaire de ces deux défauts (calcul en annexe 3) peut être pondéré par la valeur du coefficient R

$$\text{soit } \lambda'_1 = 5,4 \cdot 10^{-6} / \text{h} \quad \text{coupure EVO impossible}$$

$$\lambda''_1 = 6,5 \cdot 10^{-6} / \text{h} \quad \text{alimentation EVF impossible}$$

d'où une probabilité horaire d'indisponibilité de la rame à cause d'un défaut de porte

$$R \cdot (\lambda'_1 + \lambda''_1) = 2,3 \cdot 10^{-6} / \text{h}$$

Remarque

Dans ce qui précède nous n'avons pas pris en compte les défaillances du microprocesseur, elles sont pourtant numériquement plus importantes.

La raison en est que toute la procédure de détection des pannes est, conformément aux hypothèses, sous entendue avec un microprocesseur en bon état de fonctionnement.

En cas de défaillance du microprocesseur, nous imposons (conformément au paragraphe II₃₋₂ de la première partie) un état de sécurité au mécanisme de porte. Celui-ci est établi ; d'une part par la déconnexion du microprocesseur au vecteur de commande, et d'autre part par le forçage du vecteur à une valeur statique correspondant à la commande de fermeture.

Autrement dit ; dès qu'une défaillance du microprocesseur est détectée (voir traitement équitemps) le mécanisme de porte se voit infligé

d'une commande permanente de fermeture. La porte une fois refermée est donc indisponible, mais cet état vis-à-vis des voyageurs est sécuritaire (information par une signalétique) et la rame de métro peut continuer normalement son exploitation, les échanges voyageurs peuvent en effet être réalisés par les autres portes latérales du véhicule.

Périodicité du cycle de détection

Comme nous l'avons vu, un cycle complet d'ouverture et de fermeture des portes suffit à détecter un maximum de pannes.

Naturellement le cycle de détection sera donc celui imposé par l'exploitation de la rame de métro, soit d'après les prévisions de la ligne N° 1 du VAL une périodicité minimum d'arrivée des rames en station de 1 mn environ. En fait en service normal (en dehors des heures de pointe) cette périodicité, pour le calcul qui suit, peut prendre une valeur majorante de 10 mn.

Calculons quelle est la probabilité de défaillance du dispositif commande et contrôle de porte entre deux phases de vérification

soit $R(t, \theta) = e^{-\lambda_0 \theta}$ la probabilité de survie (1ère partie, II₃₋₁₁)

$D = 1 - R(t, \theta)$ la probabilité de défaillance

avec $\lambda_0 = 48,2 \cdot 10^{-6}/h$ le taux de défaillance de l'ensemble du dispositif (hors microprocesseur)

$\theta = 10 \text{ mn}$

le calcul donne une valeur de probabilité de

$$D = 8 \cdot 10^{-6}$$

Cette valeur nous renseigne sur la faible probabilité de laisser des pannes dormantes dans le système.

Il est à remarquer qu'après une immobilisation prolongée de la rame, il y a lieu avant réinjection sur la ligne, de réinitialiser le cycle de détection des pannes en actionnant à vide l'ensemble des mécanismes de porte.

Temps de tolérance aux fautes

A l'issue de la détection d'un défaut, déterminons approximativement quel est l'intervalle de temps dont dispose l'exploitant avant de remettre le dispositif en état.

Hypothèse de calcul

Considérons une défaillance quelconque mais admissible sur une voie de mesure ($\lambda_1 \approx 4.24.10^{-6}/h$), quel est l'intervalle de temps pendant lequel on peut laisser l'équipement dans l'état sans que l'on excède une probabilité évaluée a priori à $P = 10^{-10}$ pour que se produise un second défaut, celui-ci non détectable à tout coup par la procédure de détection de panne, pouvant conduire à une situation dangereuse.

Soit le taux de défaillance horaire du dispositif de commande contrôle (calcul en annexe 3)

$$\lambda_0 = 48,20 \cdot 10^{-6}/h$$

Le taux de défaillance du reste de l'équipement λ_2 est de

$$\lambda_2 = \lambda_0 - \lambda_1 = 43,9 \cdot 10^{-6}/h$$

L'intervalle de temps disponible pour l'exploitant est de

$$T < \frac{2P}{\lambda_1 \lambda_2} \quad (\text{1ère partie, paragraphe II}_2)$$

$$\text{soit } T < 1^h 3 \text{ mn}$$

Il est à remarquer que cette valeur est compatible avec les contraintes d'exploitation de la ligne de transport. Il correspond sensiblement à un aller-retour d'une rame sur la ligne N° 1 du VAL.

Les autres pannes envisageables (voie de mesure, processus) ayant des valeurs de taux de défaillance du même ordre de grandeur laissent envisager des résultats analogues.

III₅ - Conclusion

Les valeurs numériques établies ci-dessus sont approximatives, elles dépendent des conditions de calcul des valeurs des taux de défaillance horaire. Le détail des calculs est donné en annexe 3. Ces résultats nous permettent toutefois de dégager plusieurs remarques.

Remarques sécurité

La présence d'un microprocesseur affecté à la commande et au contrôle de processus apporte de notables avantages

- une très faible probabilité de panne dormante dans l'ensemble du système

- moyennant un objectif de sécurité fixé à l'avance et de loin bien supérieur à celui adopté sur les mécanismes de portes VAL ligne N° 1 (Réf. 46) il s'avère que l'exploitant dispose d'un temps de remise en état compatible avec les contraintes d'exploitation.

Remarque disponibilité

Il est à noter que le taux de défaillance horaire pondéré des pannes conduisant à une immobilisation de la rame porte ouverte en station est faible. Il est inférieur à celui établi pour le système de porte actuellement en service (Réf. 47).

Ce résultat en lui même est intéressant mais il est à remarquer qu'il est obtenu à partir de matériels dont la fiabilité est globalement inférieure aux systèmes de commande traditionnels par relayage électromécanique actuellement en service.

IV - ETUDE DE LA MISE EN SECURITE DES CARTES DE COMMANDE DE PORTE

L'ensemble du réseau local que nous avons défini pour toutes les portes d'un véhicule comprend trois cartes de commande, (figure 2-8), installées à proximité d'un jeu de deux mécanismes disposés sur la caisse du véhicule en vis-à-vis, (figure 2-16).

Un microprocesseur monochip (microcontrôleur INTEL 8751) est spécialement affecté à la commande et au contrôle de chaque mécanisme ainsi qu'au traitement des informations de sécurité de la porte opposée (*)

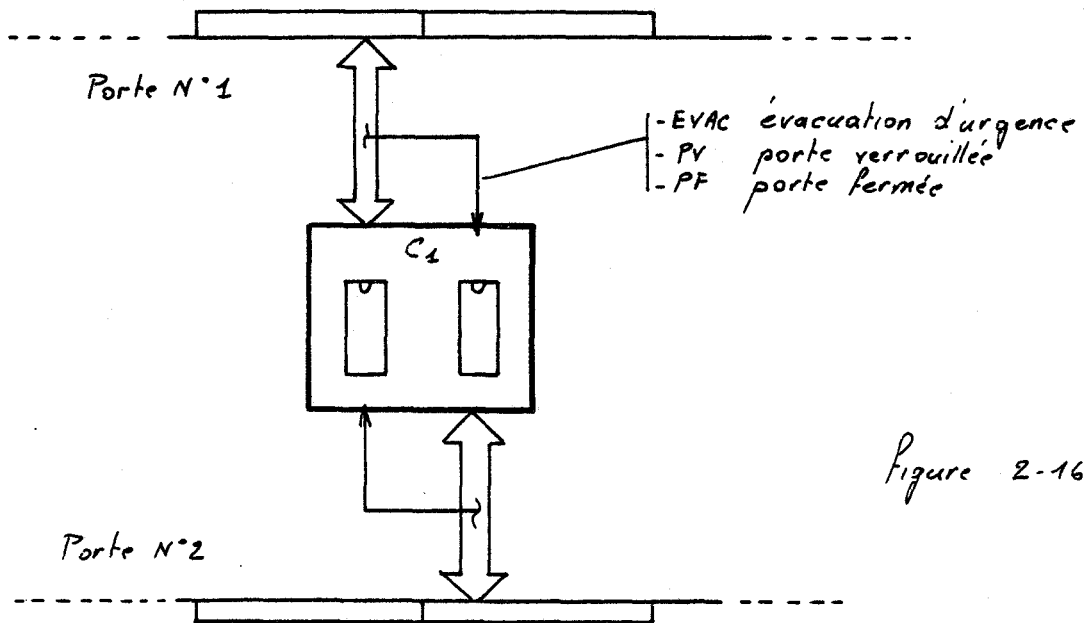
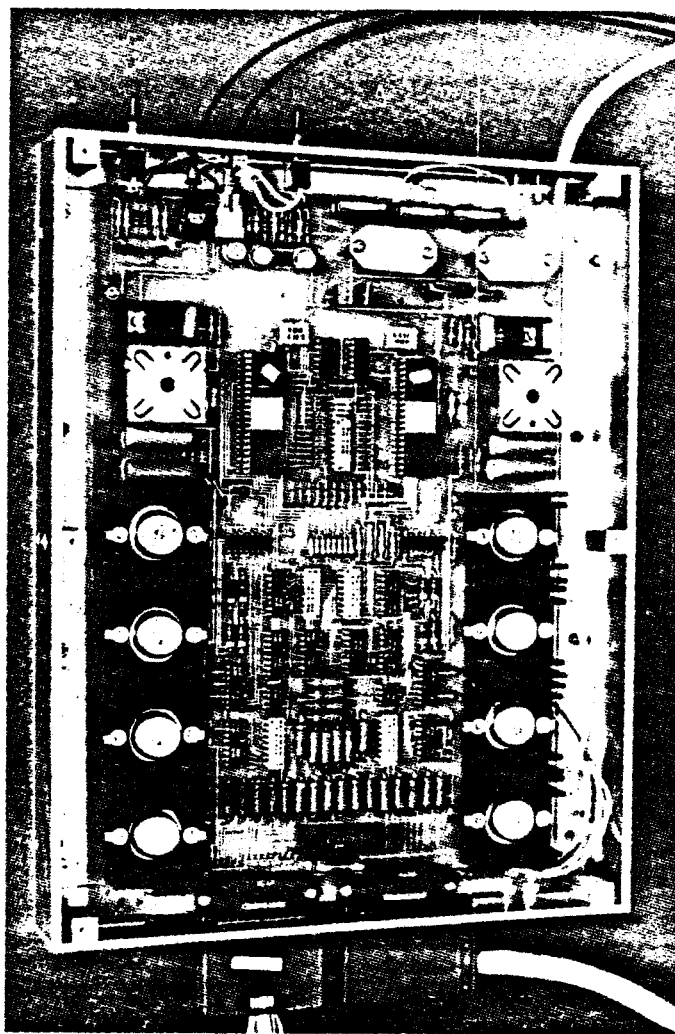


Figure 2-16

Nous avons montré que l'analyse séquentielle du vecteur d'état, représentée par Graphe de Pétri, permettait au microprocesseur d'assumer toutes les fonctions de commande en sécurité, y compris en présence de certains défauts momentanément tolérés. Une des hypothèses de travail posée pour cette partie de l'étude était que le microprocesseur devait être lui-même en état de fonctionnement correct.

Pour que l'étude de sécurité soit complète, il reste donc à établir la mise en sécurité du système microprocesseur conformément à la définition donnée en première partie paragraphe II - 3.

(*) famille INTEL 8051 version mémoire programme en EPROM (8751)



BUS
LILLE

Carte de commande de porte

photo n° 10

Avant d'entrer plus en avant dans cette partie de l'étude, il nous semble bon de revenir vers une remarque développée en première partie de ce mémoire.

Compte tenu du nombre important de mécanismes de porte disposés sur un véhicule et à fortiori sur l'ensemble des rames d'un réseau de transport, notre souci a été de minimiser le nombre de microprocesseurs ceci en vue de maintenir un bon niveau de fiabilité. Notre choix s'est donc fixé sur la mise en sécurité des systèmes à l'aide d'une architecture monoprocesseur en autotest le microprocesseur étant lui-même constitué d'un système totalement intégré sur une seule puce (microcontrôleur). Cette solution conduit évidemment à minimiser le nombre de composants et permet d'obtenir une circuiterie relativement simple (photo n° 10).

IV-1 Mise en sécurité d'un microprocesseur par traitement d'une fonction équitemps (EQT)

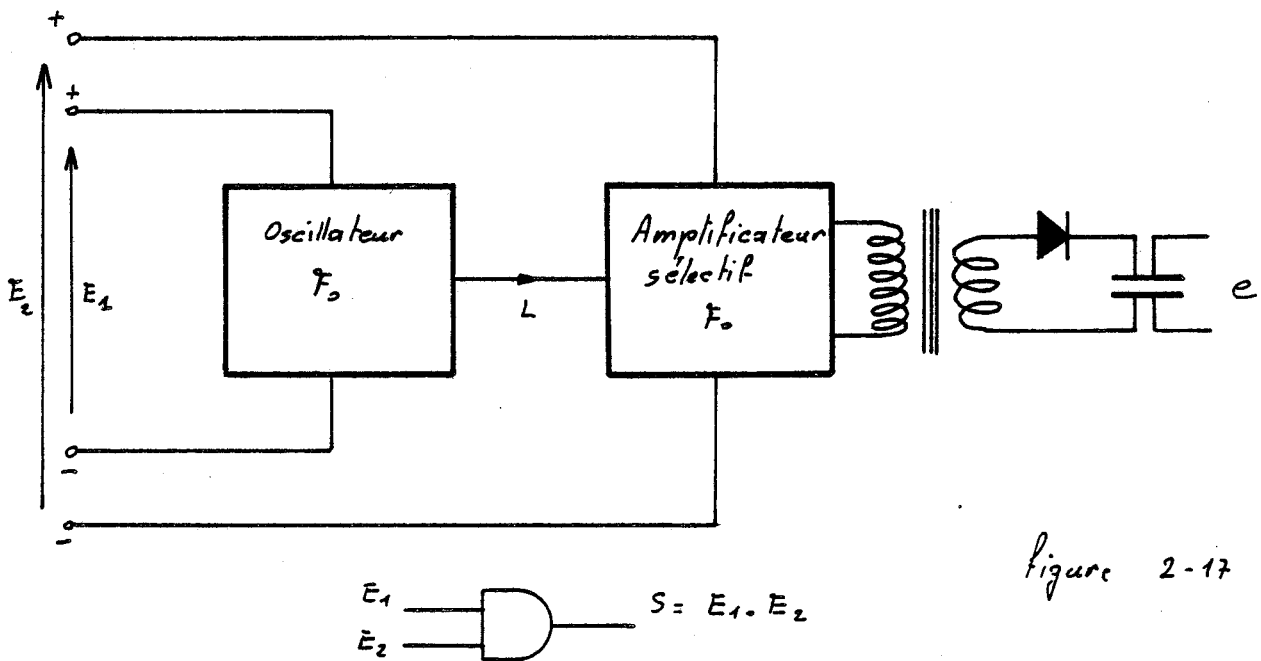
La mise en sécurité d'un microprocesseur nécessite de réaliser deux fonctions. Il s'agit non seulement de détecter les défauts de fonctionnement internes mais aussi de concevoir un actionneur capable de déconnecter en sécurité le microprocesseur de son environnement en cas d'avarie (paragraphe II₃₋₂).

La réalisation d'un tel dispositif mérite une attention toute particulière. En vertu du principe de la sécurité positive il ne faut pas en effet qu'une simple panne puisse engendrer une commande contraire à la sécurité.

Afin d'éviter l'introduction vers le microprocesseur d'une fonction de contrôle sur cet élément, il paraît judicieux de le réaliser en sécurité intrinsèque.

L'idée nous est venue de bâtir cette fonction à l'aide d'une circuiterie s'apparentant au ET de sécurité utilisé dans les chaînes de sécurité du VAL.

La figure ci-dessous nous décrit le schéma fonctionnel de cet opérateur logique.



L'énergie sur le secondaire du transformateur n'est présente que si et seulement si les entrées E_1 et E_2 sont alimentées.

La liaison entre les blocs oscillateur et amplificateur sélectif s'effectue par une information dynamisée L dont la caractéristique essentielle ; la fréquence, n'est satisfaite que si l'oscillateur est en bon fonctionnement.

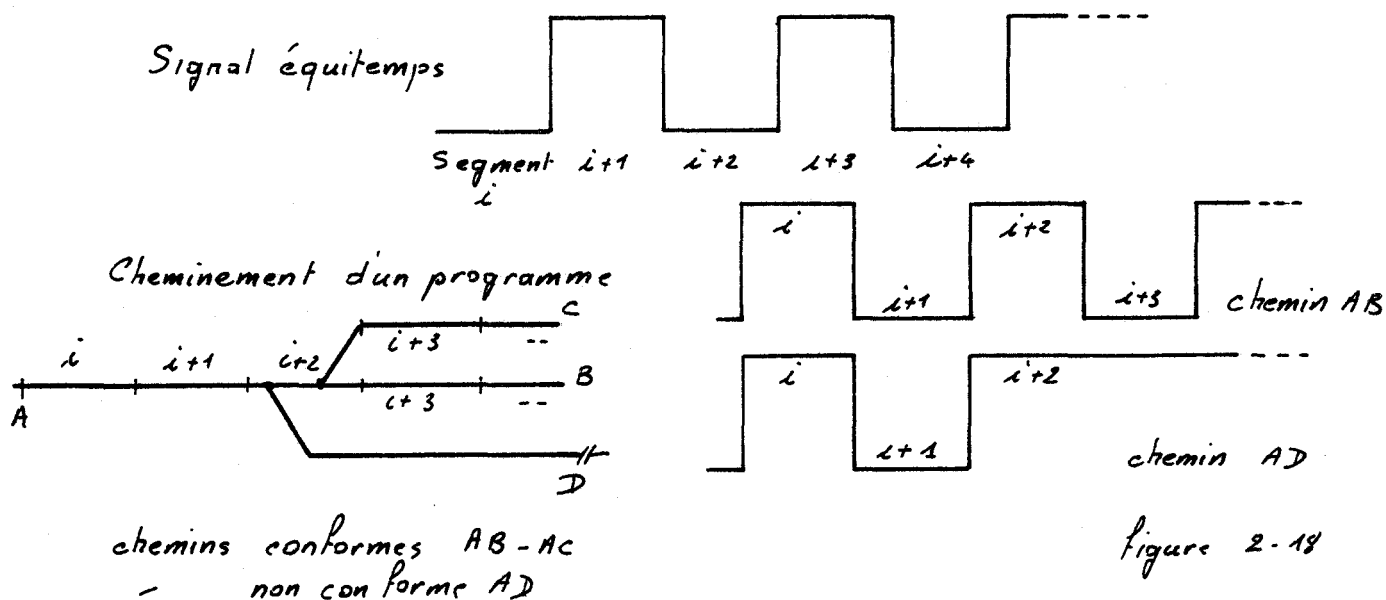
L'association de ce principe et d'un procédé de détection d'erreurs de fonctionnement des microprocesseurs par tests temporels (1ère partie - paragraphe III₂₋₃) nous a amené à formuler la proposition suivante.

Le microprocesseur peut durant l'exécution de son programme d'application (commande de porte par graphe de Pétri) effectuer des tests internes ou un mini traitement dont la validation du résultat permet de vérifier son bon fonctionnement.

L'idée consiste à introduire les résultats des tests comme conditions supplémentaires au déroulement normal du programme.

Le programme d'application peut, lors de sa conception, être tronçonné de telle façon que chaque segment ait une durée d'exécution connue et invariable.

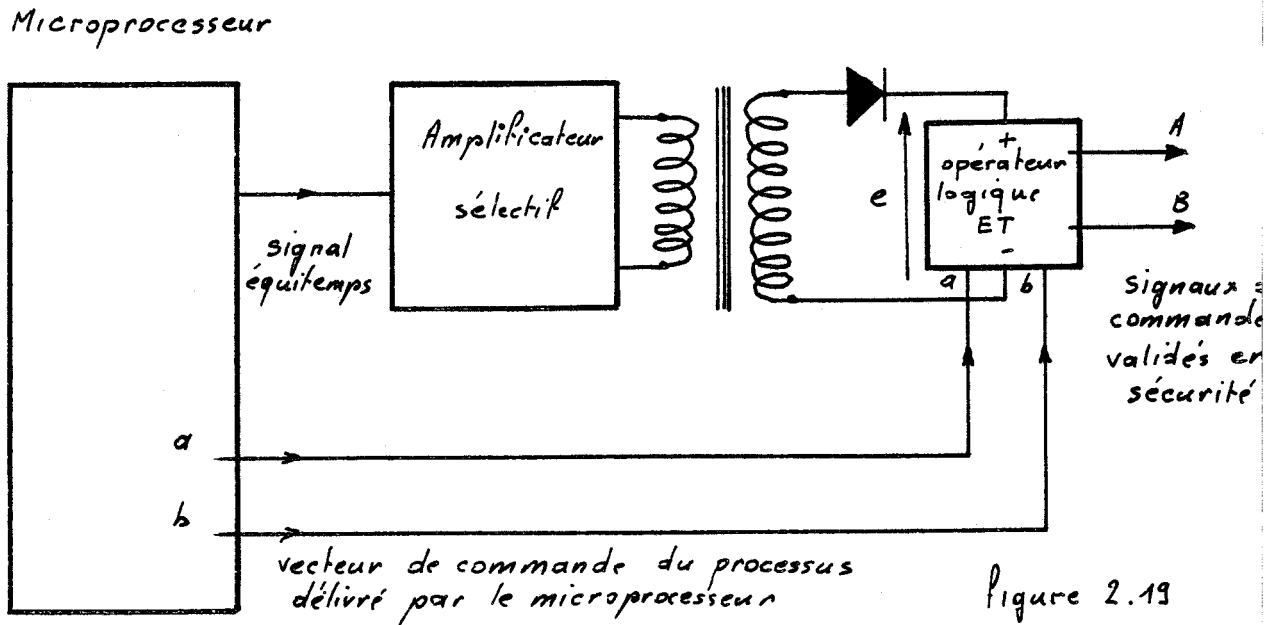
Un signal indicateur, ou chien de garde, activé lors de l'exécution de chaque segment fournit à l'extérieur une information dynamisée dont la valeur nominale de la fréquence est synonyme du bon fonctionnement du microprocesseur. Ceci est vrai dans la mesure où les tests gérés par le microprocesseur lui même peuvent conditionner les chemins parcourus pour exécuter le programme et de là l'existence ou la non existence du signal équitemps (figure 2-18).



La source de signal dynamisé que constitue le microprocesseur peut venir se substituer à la fonction "oscillateur" du ET de sécurité.

Il ne reste plus, à l'aide d'un amplificateur sélectif accordé sur la fréquence du créneau équitemps, qu'à fournir une énergie utile validée en sécurité par les tests du microprocesseur, et par la structure en sécurité intrinsèque. L'énergie disponible (e) est ensuite consacrée à l'alimentation des actuateurs de puissance commandant les électrovalves des moteurs de porte.

Le schéma de principe est le suivant



Le collage du signal équitemps a pour conséquence de faire disparaître l'énergie (e) disponible en sortie de l'amplificateur.

Les signaux de commande (A et B) envoyés au processeur sont inhibés (voir schéma de détail figure 2.21).

IV-2 Traitement de la fonction équitemps (EQT)

La seule vérification sécuritaire que puisse réaliser un amplificateur sélectif c'est la valeur de la fréquence du créneau équitemps F_{EQT} .

$$F_{EQT} = \frac{1}{\text{durée 2 segments}}$$

Cette valeur est comparée à la fréquence d'accord de l'amplificateur déterminée par les valeurs de self et capacité

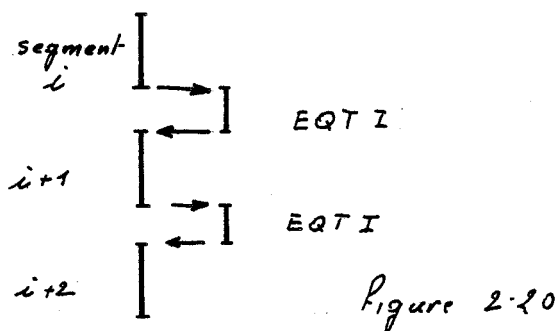
$$F_{Asel} = \frac{1}{2\pi \sqrt{LC}}$$

Remarque

Les fluctuations instantanées de la durée des segments équitemps et même la disparition momentanée de quelques périodes ne seront pas prises en compte. L'amplificateur sélectif ne fonctionne nominalement qu'en régime établi du signal d'entrée.

IV₂₋₁ Traitement équitemps par tests chronologiques

La nécessité d'engendrer un signal dynamisé dont seule la fréquence est porteuse de l'information d'état du fonctionnement du microprocesseur nous a amené à traiter une fonction de chaînage des segments de programme.



Le programme d'application est tronçonné en segments i numérotés I par une étiquette. La durée de chaque segment est rendue constante par comptabilisation et ajustage du nombre de cycles d'horloge utilisés dans le segment.

Au terme de l'exécution de chaque segment le microprocesseur se dérouté vers un module de programme (EQTI) chargé de vérifier le chaînage ou la succession correcte des segments. La fonction qui y est traitée est la suivante

$$i = \frac{I_{(n-2)} + I_{(n-1)} + 3}{2}$$

La valeur de I est recalculée à partir des valeurs calculées antérieurement lors des 2 segments précédents, le résultat i du calcul est comparé avec la valeur de l'étiquette $I_{(n)}$ inscrite dans le segment de programme. La coïncidence des résultats ($i = I_{(n)}$) permet d'acquiescer le segment en délivrant le signal équitemps (génération d'un front) et en allant exécuter le segment suivant (voir détail en annexe IV).

La décomposition temporelle du déroulement d'un programme implique l'emploi de règles d'analyse ; tronçonnage, réduction du nombre de points d'entrée, de sortie d'un segment, (programmation structurée).

IV₂₋₂ Traitement équitemps par test logiques

Le traitement de la fonction de chaînage est indépendant de certaines fonctions logiques du microprocesseur ; état des espaces mémoires vives, mortes, portes d'entrée sortie etc... Nous avons dû, en conséquence, introduire des tests fonctionnels à l'intérieur des segments de programme sur toutes les parties utiles à notre application.

Les résultats des tests sont, comme pour le traitement du chaînage, introduits comme conditions sur le cheminement emprunté par le microprocesseur pour parcourir son programme.

A l'issue d'un test fonctionnel non validé le programme se dérouté en empruntant un cheminement non conforme à la génération des créneaux équitemps.

IV-3 Analyse critique des test effectués

La combinaison des test chronologiques et logiques permet de rendre le traitement équitemps sensible à tous les modèles de fautes envisageables sur les microprocesseurs.

Nous pensons que le mode d'observation (temporel) du fonctionnement du microprocesseur constitue un moyen particulièrement sensible et significatif car il prend en compte un nombre important de blocs fonctionnels du microprocesseur (horloges, décodage, séquençement de l'exécution des instructions etc...) Le travail consiste à rendre le traitement du chaînage des segments équitemps, sensible à l'apparition des fautes par déroutement du programme compteur (PC) d'au moins un segment équitemps. Le but étant d'éviter qu'un défaut ne puisse se manifester par une fluctuation rapide d'un créneau, fluctuation non détectable par l'amplificateur sélectif.

Un exemple de programme de traitement d'un graphe de Pétri, mettant en oeuvre le traitement équitemps décrit ci-dessus a été réalisé dans le but de mettre au point une méthodologie d'analyse du problème (annexe IV).

Une difficulté rencontrée réside dans le fait que les applications envisagées (traitement de graphe de Pétri) présentent des modes d'exécution multiples selon les séquences d'apparition des évènements faisant évoluer le marquage des graphes. Autrement dit, les chemins empruntés pour répondre à l'application sont variables. Il est donc inconcevable d'affecter chaque segment d'une étiquette I de valeur constante.

La solution à ce problème serait d'établir une procédure d'étiquetage paramétrable permettant de vérifier la conformité du chaînage des tronçons équitemps.

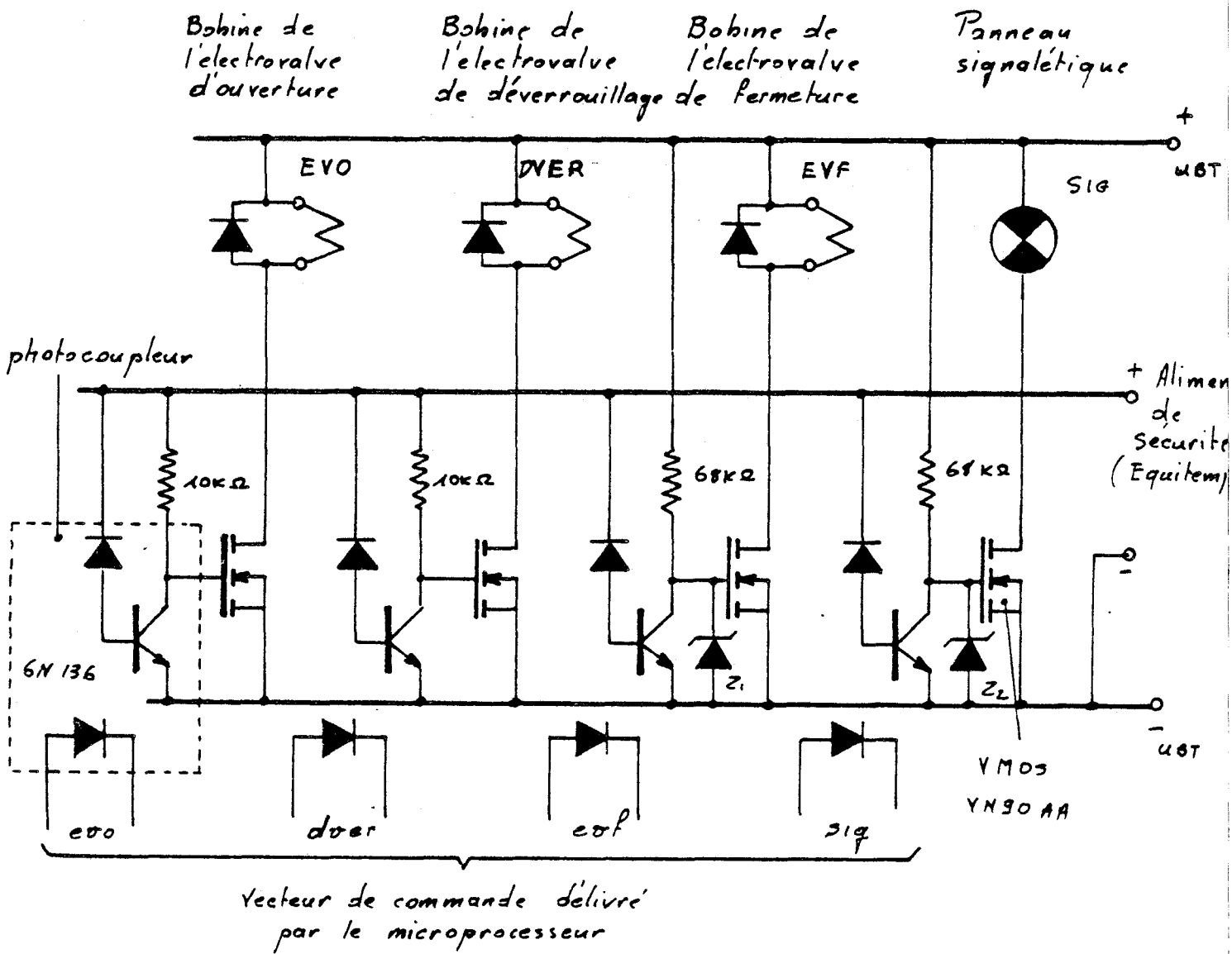
IV-4 Certification du logiciel

Le découpage du programme d'application en segments courts avec limitation des points d'entrée et de sortie va dans le sens d'une analyse fine et rigoureuse du programme. Cet aspect est important car il débouche sur la réalisation de logiciels fiables.

D'autre part une analyse fonctionnelle complète du microprocesseur utilisé (Réf. 45) reprenant une méthode d'analyse et de représentation graphique des instructions (Réf. 26) devrait permettre d'établir une bibliothèque exhaustive de tests logiques du microprocesseur.

L'acceptation du procédé de mise en sécurité du microprocesseur en autotest que nous venons de décrire passe par l'établissement d'une méthode de quantification des tests proposés puis par l'utilisation de cette méthode au calcul du taux de couverture de détection des pannes.

La valeur du taux de couverture devra tendre asymptotiquement vers 1 soit la quasi certitude d'avoir détecté tous les défauts capables de perturber le déroulement du programme de commande-contrôle du processus envisagé.



-1- l'alimentation de sécurité existe (sortie de l'amplificateur sélectif) les effecteurs sont commandés par le microprocesseur : evo, evf, sig, dver

-2- l'alimentation de sécurité n'existe pas (plus de signal équitemps) : EVF et SIG sont activés en permanence

Figure 2.21

Remarque

L'obtention de la valeur 1 pour le taux de couverture de panne apporterait une certitude de sécurité assez analogue à celle obtenue en sécurité intrinsèque.

En effet celle-ci ne peut être mise en échec que par l'apparition d'un défaut (ou d'une combinaison de défauts) auquel personne n'avait encore pensé, et qui par suite était, (par définition même) non encore connu. L'obtention de la valeur 1 peut donc bien être établie alors qu'il peut subsister des défauts que personne n'a imaginé.

En définitive si il se produit encore des accidents malgré toutes les précautions prises cela provient de la différence subtile entre les expressions "impensable" et "non encore pensé".

IV - 5 Application d'un état de sécurité au mécanisme de porte en cas de défaillance du microprocesseur. Etude de la carte de commande de porte

Les figures 2-5, 2-11 et 2-21 aideront le lecteur à suivre l'examen technique de cette partie de la réalisation.

Le vecteur de commande de chaque mécanisme de porte est conforme à ce qui a été défini au paragraphe I-4 de la seconde partie.

L'état de sécurité présenté aux voyageurs par le mécanisme de porte est, nous l'avons vu, l'état porte fermée. Pour des raisons de commodité d'utilisation du système de transport, lorsque le dispositif de commande de porte condamne l'utilisation d'un mécanisme, les voyageurs en sont informés par une signalétique. Rappelons que même en présence d'une porte condamnée, un voyageur peut par cet accès, à l'aide de la poignée d'évacuation d'urgence, sortir du véhicule pour assurer sa sécurité.

Le forçage d'un état de sécurité impose l'application d'une valeur statique particulière au vecteur de commande (figure 2-21). Le détail est donné ci-dessous :

- commandes d'ouverture (EVO) et de déverrouillage (DVER) non activées
- illumination du panneau signalétique (SIG)
- activation de la commande de fermeture.

Cette dernière disposition permet non seulement de maintenir statiquement l'effort de fermeture mais également de créer artificiellement une commande de fermeture dans le cas où le microprocesseur subit une défaillance alors que le véhicule est en station porte ouverte (amélioration de la disponibilité de la rame paragraphe III-4 - 2ème partie).

La chaîne d'action permettant au microprocesseur d'activer une électrovalve est représentée figure 2-11. L'emploi d'un photocoupleur permet de réaliser l'isolement galvanique entre le système de commande à microprocesseur installé sur une carte de circuit imprimé (photo n°) et les électrovalves (photo n°) alimentées sous 72 v et disposées à proximité du moteur pneumatique.

La commutation des électrovalves est assurée par des transistors MOS de puissance dont la particularité est de réaliser leur changement d'état à partir d'une très faible énergie sur la grille de commande.

L'alimentation de sécurité n'est autre qu'une sortie redressée de l'amplificateur sélectif vu précédemment.

En cas de disparition du créneau équitemps la tension de l'alimentation de sécurité tombe à 0v. L'absence de cette tension combinée à l'isolement galvanique apporté par les photocoupleurs rend impossible la commutation du transistor MOS.

L'état pris par la commande est alors fonction de la tension statique appliquée aux grilles des transistors, celle-ci peut être nulle (cas des transistors DVER et EVO) ou portée à un potentiel fixé par les diodes zenes (Z_1 et Z_2) alimentées elles-mêmes par le 72 v (UBT).

Etude de la carte de commande de porte

Le principe de base qui a servi à l'élaboration de la carte de commande de porte a été de concevoir une circuiterie modulaire en essayant de conférer à chaque module une certaine indépendance. L'effet recherché étant d'éviter que l'apparition d'une panne ne puisse engendrer une cascade de défauts. Cette caractéristique est importante, lors de la détection et de l'analyse des pannes du processus et de ses organes d'entrée sortie (paragraphe III₂₋₁, 2ème partie) nous avons supposé par hypothèse que les défauts apparaissent individuellement.

En résumé, et d'une manière générale, la conception d'une carte de commande de processus en sécurité par microprocesseur, utilisant la méthode d'analyse de fonctionnement que nous avons choisi suppose de prendre en compte les points suivants :

-1- Développer une étude de sécurité consistant en l'établissement d'un catalogue des pannes "possibles" et "impossibles" sur les divers composants utilisés. De cette étude découle

- l'établissement d'une configuration convenable des vecteurs d'état et de commande
- la mise au point et la description par paragraphe de Pétri de la procédure de détection et d'analyse des pannes.

-2- Réaliser une circuiterie sous forme modulaire comme vu ci-dessus.

Il va de soi que si à une panne naissante était engendré 2 ou N défauts (de mode commun) il y aurait lieu :

- soit de tolérer les 2 ou N défauts (ce qui aurait des conséquences sur le dimensionnement du vecteur d'état)
- soit d'arrêter l'exploitation du processus (ici condamnation de la porte).

-3- Entreprendre une étude prévisionnelle de fiabilité dont le but est d'établir à partir des objectifs de sécurité, les temps de tolérance aux fautes et de là les procédures exceptionnelles d'exploitation propres à assurer la remise en état des systèmes.

Dans cet état d'esprit la carte de commande de porte possède les particularités suivantes (Réf. 40) :

- le plan de masse de la carte est localement défini sur le circuit imprimé (pas de rebouchage de masse par les interconnexions de cartes du réseau local)

- les alimentations de chaque microprocesseur sont indépendantes en régulation et en protection

- les voies de commande et de mesure sont toutes indépendantes les unes des autres avec des précautions particulières pour le transfert des informations de sécurité (PV-PF-KSA) vers les deux microprocesseurs (hypothèses de panne sur les ports d'entrée des microcontrôleurs).

Remarque sur les pannes considérées comme possibles

Ces remarques concernent les composants de technologie relativement récente non couramment employés dans les systèmes de sécurité :

* Nous avons considéré, par hypothèse, que les photocoupleurs ne pouvaient pas présenter de liaison galvanique directe entre la diode d'entrée et le transistor de sortie, notre choix s'est porté sur des produits agréés par le CNET.

* Sur les transistors MOS de puissance (VMOS) nous avons supposé que toutes les pannes du type coupure, ou fuite jusqu'au court-circuit étaient possibles.



photo n° 11

CONCLUSION GENERALE

La commande en sécurité d'un ensemble de portes véhicule d'une rame de métro traité dans la seconde partie de ce mémoire présente à plus d'un titre un intérêt certain.

D'abord par l'enjeu que représente la sécurité des voyageurs prenant place dans les rames de métro. Cet enjeu oblige à la rigueur de l'analyse des problèmes et à un exposé parfaitement transparent des solutions proposées, seul moyen valable à notre avis de recevoir une critique objective mais aussi de parvenir à terme à une acceptation sans réserve de la part des décideurs.

L'autre intérêt présenté par ce travail est qu'il révèle d'emblée un nombre important de facettes du problème très général de commande-contrôle de processus. Un progrès sensible présenté par les systèmes automatisés se situe justement dans la juxtaposition et la coordination d'un ensemble de processus élémentaires contribuant à la même tâche ici représentée par la fonction échange des voyageurs.

La configuration auto-redondante des portes véhicule des rames de métro, telle qu'elle nous était proposée, a conforté notre choix sur la mise en sécurité des microprocesseurs de commande de porte par autotest en structure monoprocesseur (sans redondancement de la fonction commande de porte).

Il faut bien reconnaître toutefois que beaucoup reste à faire en la matière. Nous pensons néanmoins que l'analyse temporelle du fonctionnement d'un microprocesseur constitue une voie de recherche intéressante méritant d'être développée parce que bien adaptée au test "en ligne". Toujours dans le même état d'esprit, c'est avec rigueur qu'il nous faudra établir parallèlement les procédures de test et la quantification du taux de couverture de pannes, l'objectif étant de tendre vers une vérification exhaustive et cyclique de toutes les fonctions activées par le programme d'application et ce dans un intervalle de temps suffisamment court pour ne pas engendrer une situation dangereuse.

Le réseau local de commande-contrôle de l'ensemble des portes disposées sur un véhicule, tel que nous l'avons défini et avec les contraintes de sécurité que nous y avons apporté, devrait permettre de solutionner le problème de l'acheminement et du traitement des informations de panne en vue de

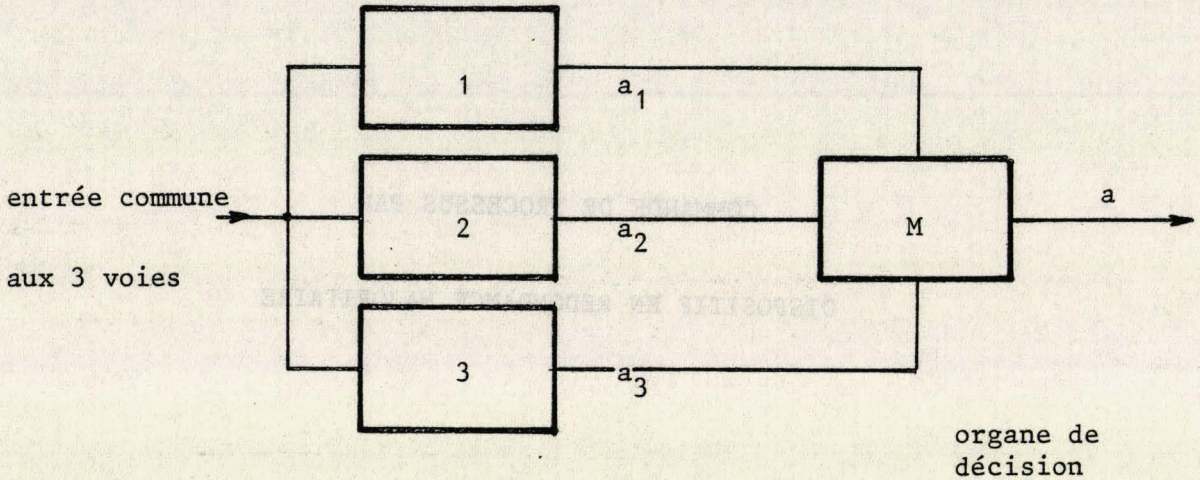
leur analyse et de la génération d'un message synthétique transmis à l'opérateur humain chargé de l'exploitation du réseau de transport.

Nous croyons enfin que l'architecture d'une carte de commande de porte telle que nous l'avons développée, la procédure de détection exhaustive des pannes du processus et de ses organes de commande et de contrôle, et enfin le nombre important de modes de fonctionnement dégradés prévus, constitue une solution optimisée au problème de commande des mécanismes de porte. Les contraintes étant, outre la sécurité, la disponibilité de la rame de métro (en relation avec les défauts porte), l'aide à la maintenance, mais aussi la minimisation de la circuiterie électronique en vue d'un transfert possible de cette étude vers l'industrie des transports.

A N N E X E 1
-o-o-o-o-

COMMANDE DE PROCESSUS PAR
DISPOSITIF EN REDONDANCE MAJORITAIRE

Examinons le système en redondance majoritaire représenté par la figure ci-dessous et déterminons la fiabilité de l'ensemble.



Les réponses fournies par les unités de traitement 1-2-3 sont comparées 2 à 2. On peut, par vote majoritaire, détecter le mauvais fonctionnement d'une voie puis l'isoler et utiliser le résultat commun aux deux autres.

Si chaque équipement a une loi de fiabilité exponentielle la probabilité de survie de chaque élément s'écrit ;

$$R_a = e^{-\lambda_a t} \quad \text{probabilité de survie de chaque voie}$$

$$R_M = e^{-\lambda_M t} \quad \text{probabilité de survie de l'organe de décision}$$

La fiabilité de l'ensemble s'écrit

$$R = R_M (3R_a^2 - 2R_a^3)$$

En remplaçant R_M et R_a par leur valeur et pour t faible vis-à-vis de la durée de vie utile, l'expression de la fiabilité de l'ensemble s'écrit

$$R = 1 - \lambda_M t$$

Selon l'objectif recherché pour que la fiabilité de l'ensemble soit supérieure à celle d'une voie unique il faut que la fiabilité de

l'organe de décision respecte l'inégalité (Réf. 2)

$$R_M > 0,9$$

A cette condition, la sûreté de fonctionnement de l'ensemble est directement liée à la fiabilité propre de l'organe de décision et non plus à celle d'unités de traitement.

Si la réalisation de systèmes informatiques en redondance majoritaire est envisageable (il faut toutefois se garantir de l'indépendance des unités de traitement*) le problème de sécurité est donc déporté au niveau de l'organe de décision.

Il existe un état de sécurité physiquement défini. Le problème consiste alors à se prémunir d'une simple défaillance telle que l'aiguillage des signaux de sortie ne soit pas effectué correctement et puisse délivrer vers l'actionneur un état contraire à la sécurité issu de l'unité de traitement défectueuse.

La sortie de l'organe de décision peut prendre un état de sécurité. La conception de cet élément peut donc s'envisager selon les règles traditionnelles de sécurité intrinsèque.

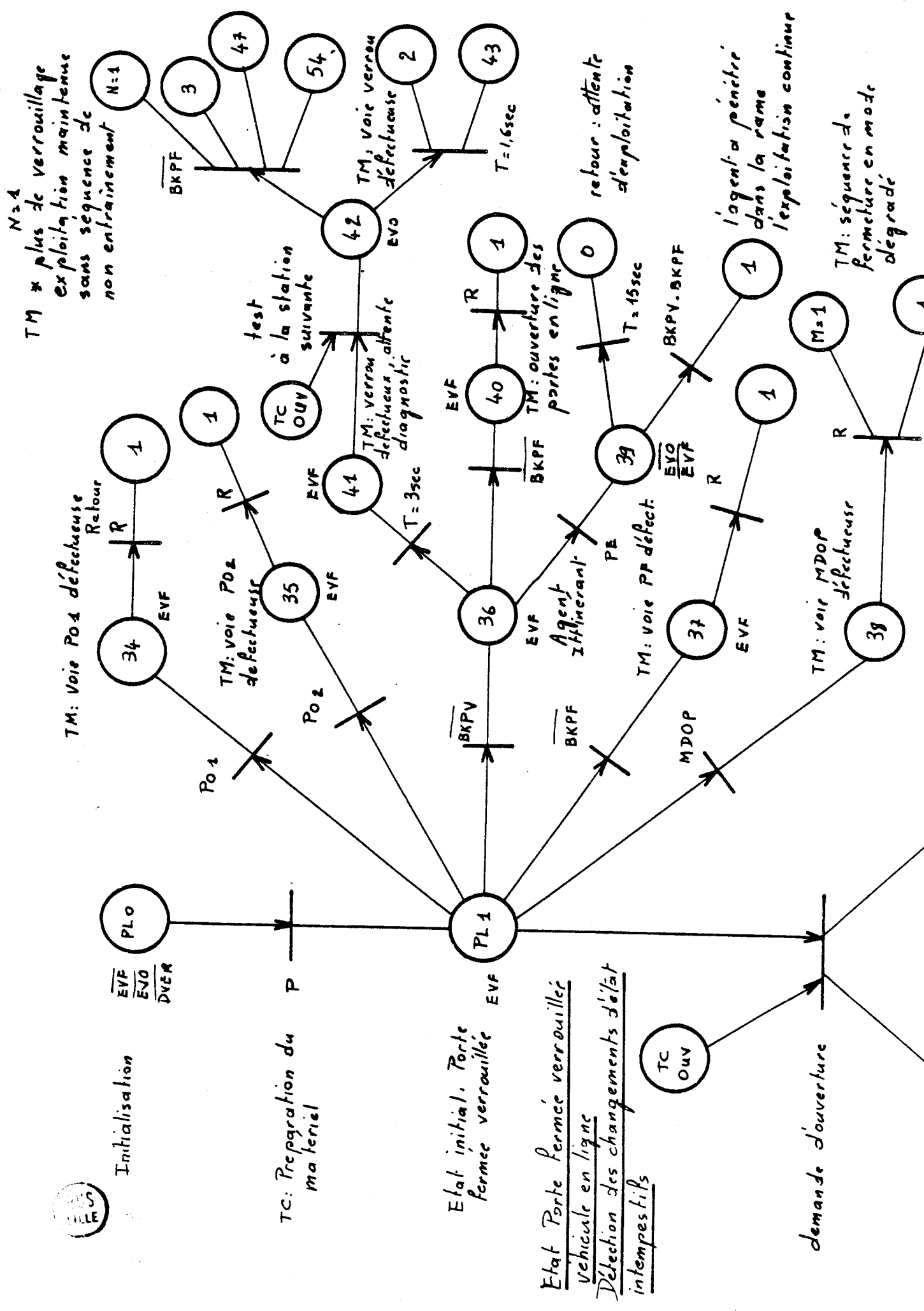
Il n'existe pas d'état de sécurité. Dans ce cas la sécurité repose sur le bon fonctionnement de l'organe de décision durant toute la période de son utilisation.

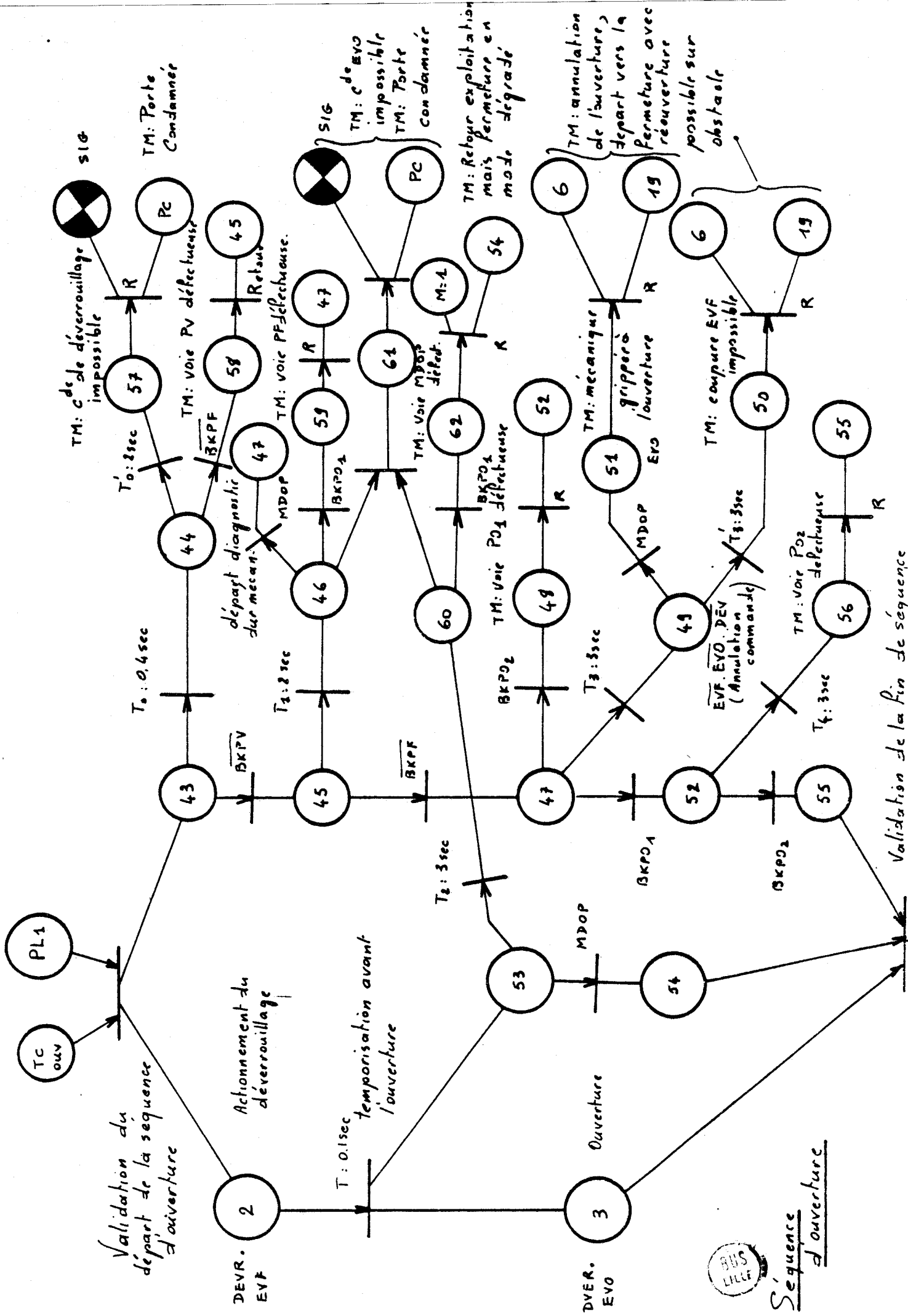
* évitement des pannes de mode commun.

A N N E X E 2

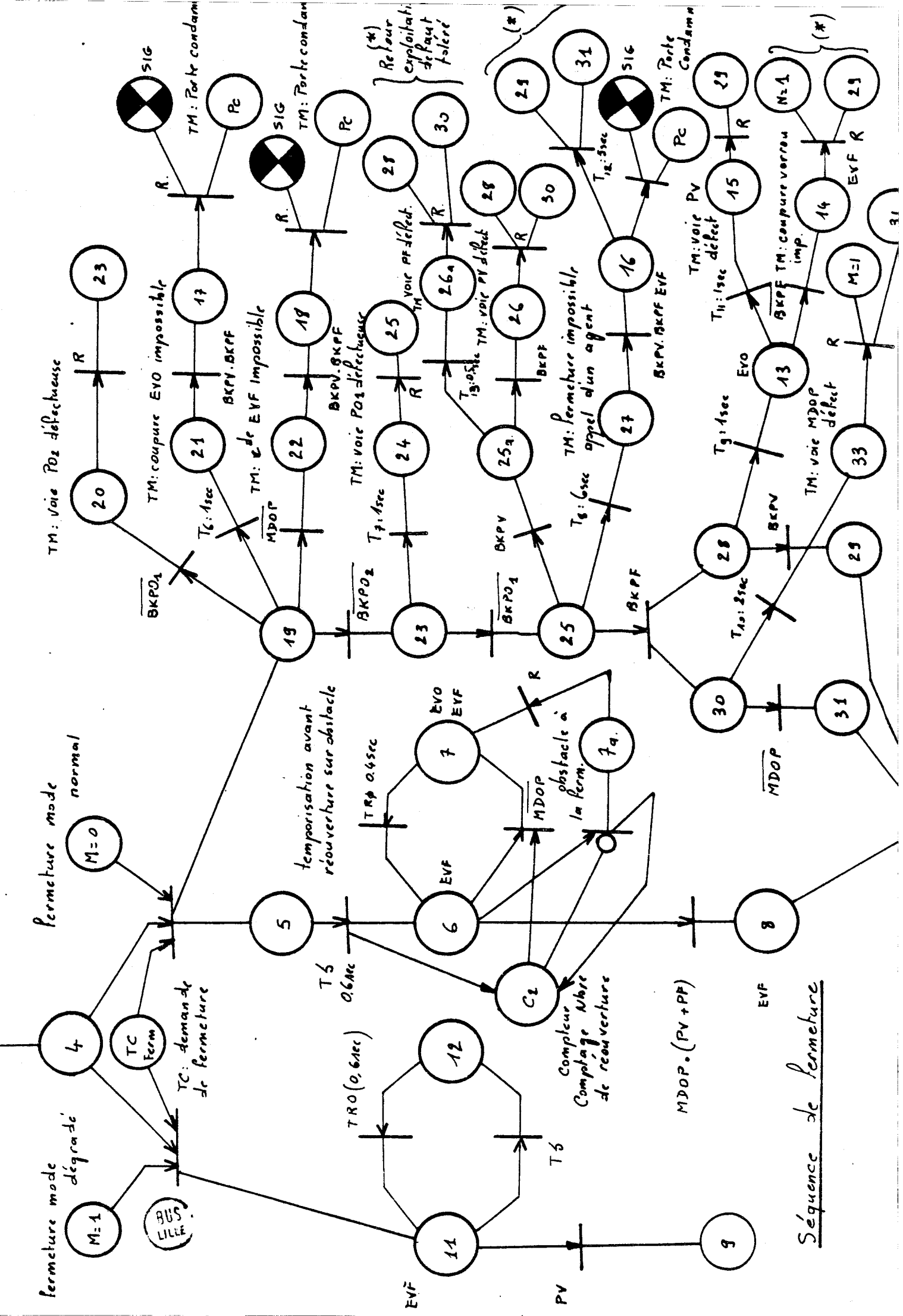
-O-O-O-O-O-

REPRESENTATION PAR GRAPHE DE PETRI DES PHASES DE
FONCTIONNEMENT D'UN MECANISME DE PORTE ET DES
TESTS D'HYPOTHESE EFFECTUES EN VUE DE LA DETECTION
DES PANNES.

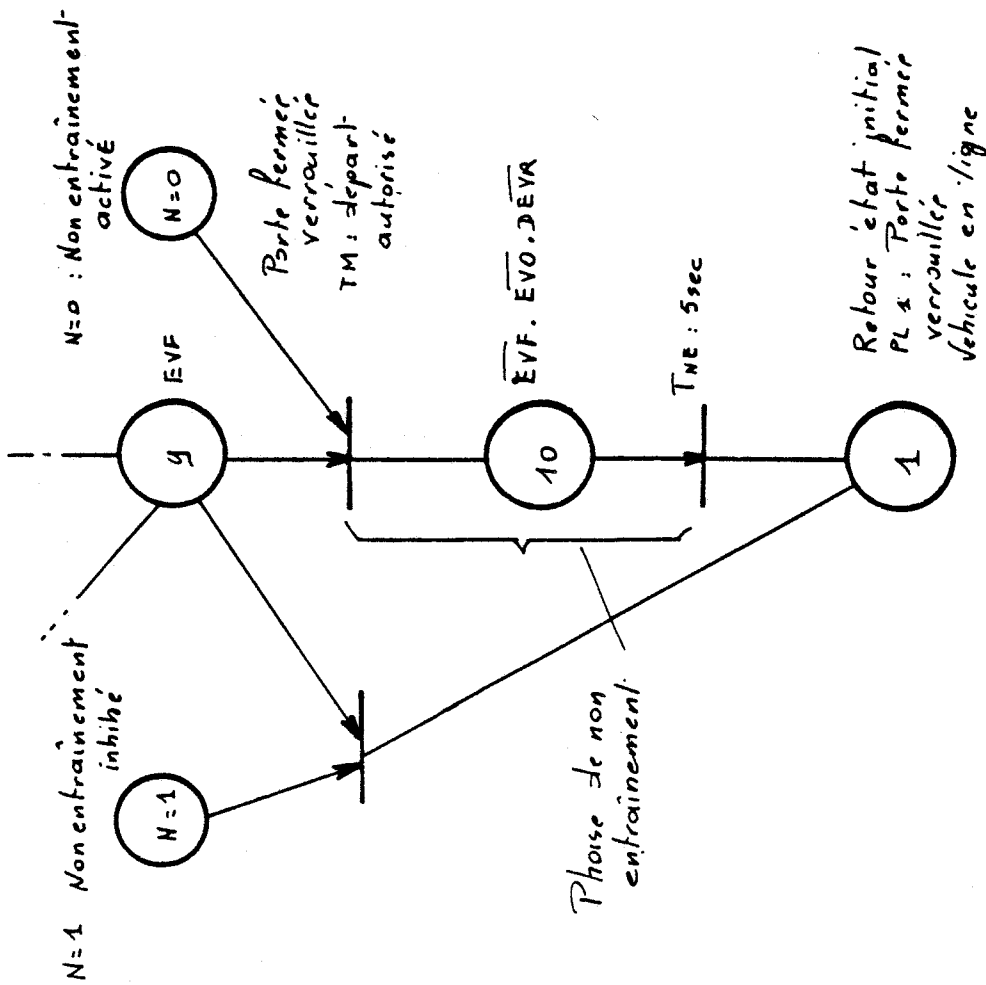




Permeture mode dégradé (M=1) / normal (M=0)

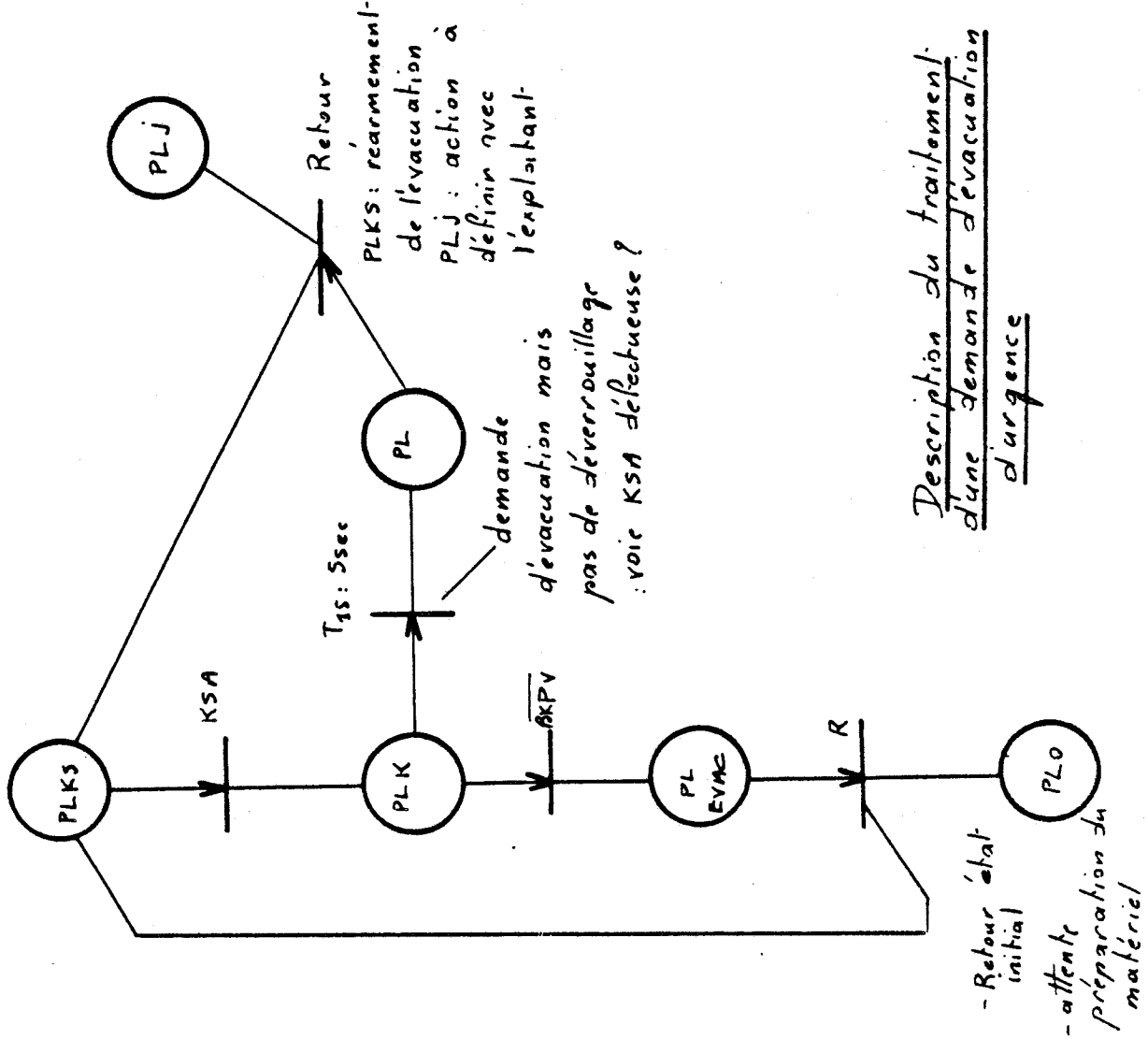


Séquence de fermeture



Fin de la séquence de perméture

Description de la séquence de non entraînement



Description du traitement d'une demande d'évacuation d'urgence



A N N E X E 3

-0-0-0-0-0-

CALCULS DE FIABILITE

- * Calcul du taux de défaillance d'une voie de commande du moteur pneumatique de porte
- * Calcul du taux de défaillance d'une voie de mesure
- * Evaluation du taux de défaillance du microprocesseur 8751 utilisé pour la commande de porte
- * Calcul décomposé du taux de défaillance d'un dispositif de commande-contrôle d'un mécanisme de porte
 - 1- partie couverte par la procédure de détection de panne décrite par Graphe de Pétri (test d'hypothèses)
 - 2- partie couverte par le traitement de la fonction équitemps
 - 3- liaison à fibre optique, détection des pannes par le système centralisateur de données.

Remarques préliminaires sur les conditions de calcul

La principale source d'information sur les valeurs numériques des taux de défaillance horaire des composants utilisés provient du recueil de données de fiabilité du CNET édition 1976 remise à jour janvier 1979 elle même remise à jour en janvier 1982.

Les valeurs particulières des composants non répertoriées proviennent de données délivrées par les constructeurs (Réf. 3-4-28).

Les conditions choisies pour mener les calculs sont les suivantes :

- feuilles de données simplifiées
- niveau de qualification des composants : agréés PTT sans contrôle de qualité
- température ambiante : 40°C
- environnement : au sol mais mobile

Dans nos calculs n'ont pas été prises en compte les défaillances dues au montage des composants sur circuit imprimé (soudure etc...).

Calcul du taux de défaillance d'une voie de commande

du moteur pneumatique de porte

schéma de principe figure

<u>Composant</u>	<u>Nb</u>	<u>λ en $10^{-9}/h$</u>	<u>Remarque</u>	<u>Sources</u>
TTL 7403	1	175		Réf. 3
photocoupleur 6N 136	1	3 000		"
MOS POWER	1	2 000	(1) toutes pannes	" 28
diode roue libre sur bobinage de l'électrovalve	1	80	confondues	" 3
résistance agglomé-	2	56		" 3
électrovalve	1	1 760	(2) λ_o	" 48

$$\text{Total } \lambda_1 = 7026,2 \cdot 10^{-9}$$

$$\lambda_1 \neq 7 \cdot 10^{-6}$$

(1) La valeur utilisée tient compte d'un test "Operating life" sur des MOS POWER HPRW 6501 Hewlett Packard (Réf. 28)

(2) Valeur effective de λ_o source Faiveley toutes pannes confondues

- panne conduisant à une commande de fermeture impossible

la valeur de λ_o devient $\lambda_o = 1,214 \cdot 10^{-6}$ et λ_1 devient $6,5 \cdot 10^{-6} = \lambda_1'$

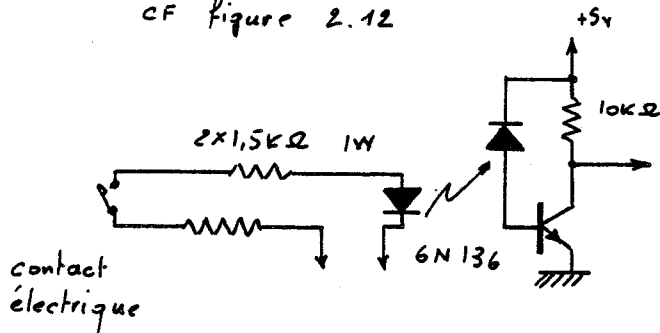
- panne conduisant à la coupure impossible de l'électrovalve d'ouverture

λ_o devient $\lambda_o = 1,21 \cdot 10^{-6}$ et λ_1 devient $5,4 \cdot 10^{-6} = \lambda_1''$

Calcul du taux de défaillance d'une voie de mesure

schéma de principe

cf figure 2.12



<u>Composant</u>	<u>Nb</u>	<u>λ en $10^{-9}/h$</u>	<u>Remarque</u>	<u>Source</u>
Contact électrique	1	870		Réf. 48
Résistance de puissance	2	180	toutes pannes confondues	" 3
Photocoupleur 6N136	1	3 000		" 3
Résistance agglomérée	1	5,6		" 3

Total $\lambda_2 = 4235,6 \cdot 10^{-9}$
 $\lambda_2 \# 4,24 \cdot 10^{-6}$

Taux de défaillance d'un moteur pneumatique de porte

$\lambda_3 = 1,73 \cdot 10^{-6}/h$ (Réf. 48)

Taux de défaillance des transducteurs électro-optique d'une liaison par fibre optique

diode DEL $\lambda_4 = 10 \cdot 10^{-6}/h$

photodiode PIN $\lambda_5 = 20 \cdot 10^{-6}/h$ (Réf. 3)

Evaluation du taux de défaillance du microprocesseur 8751
utilisé pour la commande de porte

Base de calcul : modélisation fonctionnelle du 8751 à partir de blocs dont la fiabilité est donnée dans le recueil du CNET (Réf. 4)

soit - une unité microprocesseur	8085	équivalent à	2067	portes
- une unité de transmission asynchrone	8251	"	875	"
- une unité de temporisation	8253	"	875	"
- une mémoire EPROM LK	2732	"	32 K	éléments binaires

La technologie employée pour ces fonctions est la NMOS alors que le 8751 emploie la technologie HMOS.

Le 8751 se ramène donc à une somme de 3817 portes logiques (4 transistors par porte) et 32768 éléments binaires.

Le calcul est le suivant

$$\lambda = \left[C_1 \cdot \Pi_T \cdot \Pi_L \cdot \Pi_V + C_2 \cdot \Pi_B \cdot \Pi_E \cdot \Pi_S \right] \Pi_L \cdot \Pi_Q$$

en $10^{-9}/h$

nombre d'éléments (transistors ou éléments binaires) technologie NMOS

température de jonction $100^{\circ}C$

tension appliquée 5V


nombre d'éléments

boîtier enrobé

matériel mobile

boîtier 40 pattes

(1) (2)



- (1) Π_L fabrication antérieure à 24 mois
 (2) Π_Q lot de composant agréé PTT sans CCQ

Le calcul donne

1 pour la partie opérative 3817 x 4 = 15268 transistors

$$\lambda_a = 16 \cdot 10^{-6}/h$$

2 pour la partie mémoire 32768 éléments binaires

$$\lambda_b = 12,5 \cdot 10^{-6}/h$$

soit un total $\lambda_a + \lambda_b = 28,5 \cdot 10^{-6}/h$

Soit pour un boîtier, une technologie HMOS (et non NMOS) et l'implantation de toutes les fonctions dans un même boîtier ($7 \cdot 10^4$ transistors) nous pensons devoir majorer ce résultat dans un rapport de 2 environ soit pour le 8751

$$\lambda_6 = 70 \cdot 10^{-6}/h$$

Calcul du taux de défaillance d'un dispositif de commande
contrôle d'un mécanisme de porte

Le calcul est décomposé en trois parties selon la procédure de détection de panne employée

1 - Détection des pannes par tests d'hypothèse décrits par graphe de Pétri soient :

6 voies de mesure
y compris le déverrouillage manuel extérieur $\lambda_2 = 4,24 \cdot 10^{-6}/h$

3 voies de commande
signalétique non comprise $\lambda_1 = 7 \cdot 10^{-6}/h$

1 mécanisme de porte $\lambda_3 = 1,73 \cdot 10^{-6}/h$

$$\text{Total : } 6\lambda_2 + 3\lambda_1 + \lambda_3 = 48,17 \cdot 10^{-6}/h$$

2 - Détection des pannes par traitement équitemps (dispositif de déconnexion en sécurité intrinsèque) soient :

1 système microprocesseur et alimentation associée $\lambda = \lambda_6 = 71,5 \cdot 10^{-6}/h$

1 dispositif de déconnexion (amplificateur sélectif) $\lambda_7 = 0,75 \cdot 10^{-6}/h$

soit un total $\lambda + \lambda_7 = \lambda_8 = 72,25 \cdot 10^{-6}/h$

3 - Détection des pannes de communication dans le réseau local effectué par le système central soit

une liaison à fibre optique (non compris la fibre et les connecteurs optiques) $\lambda_9 = \lambda_4 + \lambda_5 = 30 \cdot 10^{-6}/h$

soit un total 1 + 2 + 3 $\lambda_{10} = 150,5 \cdot 10^{-6}/h$

Cet ensemble représente depuis le dispositif central du réseau local de commande de porte la globalité du matériel pour effectuer la fonction commande-contrôle d'un mécanisme de porte.

Une carte de commande de porte comprend deux dispositifs sensiblement identiques (2ème partie - paragraphe 4).

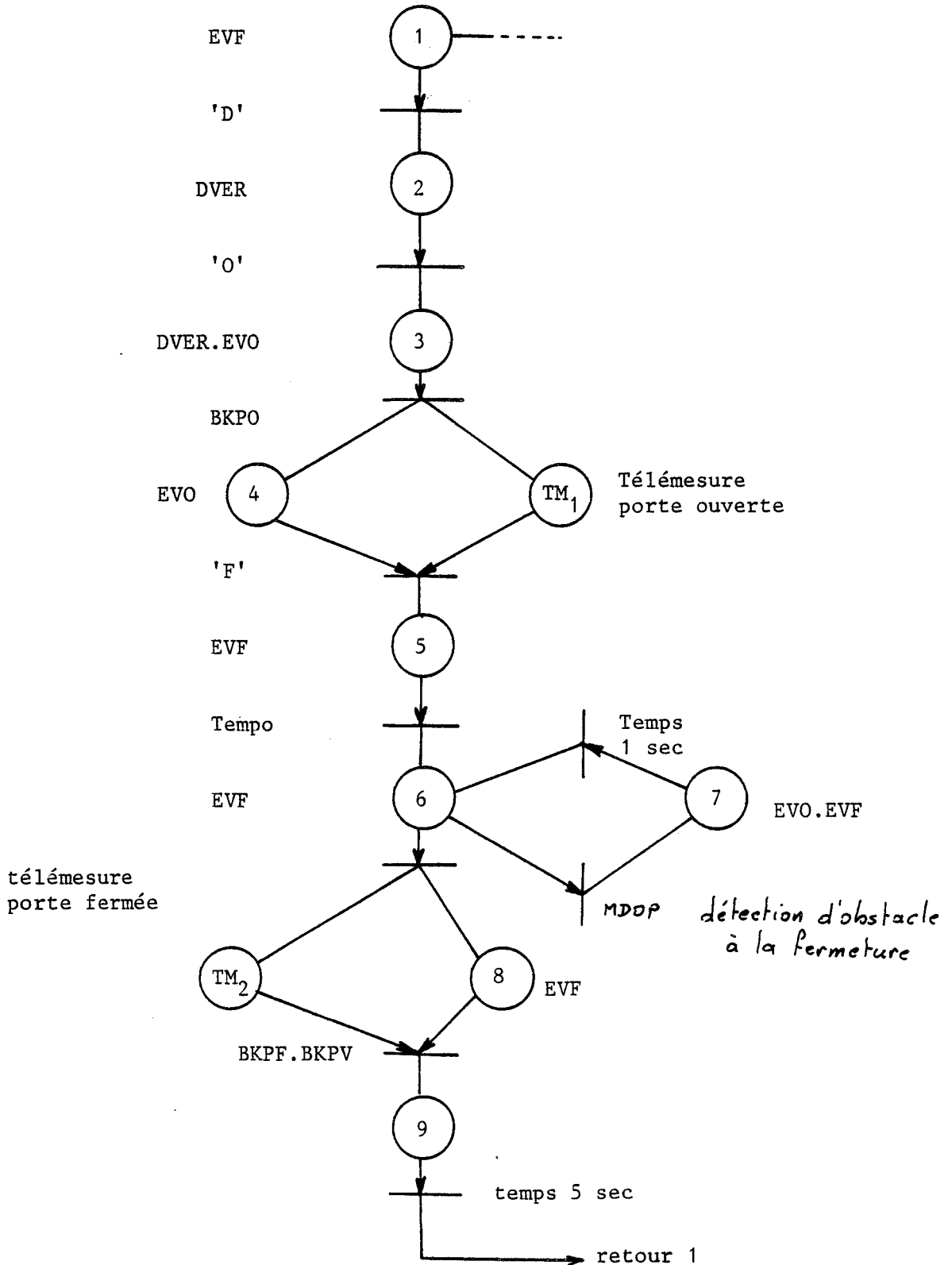
Il est à noter que la valeur du taux de défaillance horaire du microprocesseur entre pour 50 % dans la valeur de l'ensemble (λ_{10}).

A N N E X E 4

-O-O-O-O-O-

APPLICATION DU TRAITEMENT EQUITEMPS A UN LOGICIEL DE
COMMANDE DE PORTE REPRESENTE PAR GRAPHE DE PETRI

Le programme d'application choisi pour mettre en oeuvre le traitement équitemps est décrit pour sa partie fonctionnelle par le Graphe de Pétri représenté ci-dessous. La fonction mise en oeuvre correspond à la partie opérative de la commande de porte (actionnement du mécanisme) décrite plus en détail en annexe II.



Chaque place numérotée de 1 à 9 représente un état stable des grandeurs de commande (repérées EVO-EVF-DVER).

Successivement la porte passe de l'état porte fermée verrouillée (place 1) à l'état porte ouverte (place 4) pour revenir à l'état porte fermée phase de non entraînement (place 9) puis retour à l'état initial (place 1). Un cycle de détection et de réouverture sur obstacle a été prévu durant la phase de fermeture (places 6 et 7).

Les transitions correspondent à des changements d'état provenant

- soit du processus BKPO contact porte ouverte

BKPF " " fermée

BKPV " " verrouillée

- soit d'une sollicitation extérieure

'D' commande de déverrouillage

'O' " d'ouverture

'F' " de fermeture

- soit des cycles de fonctionnement imposés au système (temporisation)

Le programme mis au point réside dans un kit de développement spécifique au microprocesseur 8051 (kit INTEL SDK 51).

L'horloge du microprocesseur (8031) installée sur le kit est constituée d'un quartz 12 MHz ce qui permet au microprocesseur d'exécuter ses instructions en 1 - 2 ou 4 microsecondes selon le cas.

La durée d'un segment équitemps a été portée à 100 microsecondes (statistiquement 66 instructions). La fréquence du créneau équitemps est alors de 5 KHz.

L'évolution du marquage du graphe respecte le principe du synchronisme décrit au paragraphe 3 de la seconde partie (Réf. 37-38).

Traitement équitemps

Le problème du chaînage des tronçons équitemps a été traité pour 3 cas spécifiques de déroulement du programme

- déroulement (ou cheminement) linéaire du programme, cas le plus simple où plusieurs tronçons sont à exécuter consécutivement sans bouclage ni déroutement. La routine de traitement s'appelle EQTI.

- déroutement du programme par appel d'une routine (elle-même sans bouclage). Traitement par EQTJ.

- déroulement d'un morceau de programme en boucle d'attente (chaque place marquée en attente du tir d'une transition constitue une boucle d'attente), traitement par EQTK.

Traitement de la fonction équitemps dans le cas d'un déroulement linéaire du programme

Chaque tronçon porte une étiquette I_n pointée dans le programme. Au terme de l'exécution d'un tronçon le traitement consiste à vérifier la relation

$$i_n = \frac{I_{n-2} + I_{n-1} + 3}{2}$$

et $i_n = I_n$

Si l'identité est vérifiée on retourne à l'exécution du tronçon suivant I_{n+1} . Il est à remarquer qu'à chaque traitement EQTI tous les registres ont leur valeur modifiée.

Traitement de portions de programmes se présentant sous forme de routines

Le type de traitement est le même, il suffit avant d'appeler une routine de charger la pile de registres J de façon à préconditionner le calcul de l'expression

$$j_m = \frac{J_{(m-2)} + J_{(m-1)} + 3}{2}$$

Ceci suppose que chaque routine porte une étiquette dont la valeur initiale (1er segment) lui soit spécifique.

Traitement des boucles d'attentes

Les boucles d'attentes posent un problème particulier par le fait que le programme parcourt de façon récurrente le ou les mêmes segments. L'idée consiste alors à attribuer au (x) segment (s) une étiquette dont la valeur est fixée quelquesoit le nombre de segments, et à comptabiliser le nombre de fois où l'on parcourt la boucle d'attente.

A chaque segment parcouru on recalcule la valeur de l'étiquette. Le programme est tel que tous les registres utilisés sont modifiés à l'issue d'un calcul ceci de façon à éliminer les défauts latents.

Le traitement est le suivant EQTK

$$K_o = \frac{K_{(n-2)} + K_{n-1} + 3}{2}$$

K_o
 $K_{(-1)}$ Registres
 $K_{(-2)}$ chargés au départ
 $X = o$
 $Y = FF$

soient X et Y les compteurs de boucle

avec $X = \bar{Y}$

on effectue le calcul suivant de façon récurrente à chaque segment

$$\frac{K_{(n-2)} + K_{(n-1)} + 3}{2} = L$$

de par les opérations les valeurs de $K_{(n-2)}$ $K_{(n-1)}$ et L sont incrémentées à chaque calcul.

Pour obtenir la relation

$$K = cte$$

il suffit d'appliquer les conditions

$$\text{si } L \geq K_o$$

$$K_o = L - X$$

$$\text{si } L < K$$

$$K_o = L + Y$$

Dans les deux cas la valeur de K_o recalculée est comparée avec la valeur de l'étiquette inscrite dans le segment.

Les valeurs des registres (8 bits) de K_o , $K_{(n-1)}$, $K_{(n-2)}$, L, X, Y sont modifiées lors de chaque calcul. (Ref. 55)

ISIS-II MCS-51 MACRO ASSEMBLER V1.0
 OBJECT MODULE PLACED IN :FI:EQT12.HEX
 ASSEMBLER INVOKED BY: ASMS1 :FI:EQT12 SYMBOLS XREF DATE(15.11.83)



LOC	OBJ	LINE	SOURCE
		1	*****
		2	*****
		3	*****
		4	*****
		5	*****
		6	*****
		7	*****
		8	*****
		9	*****
		10	*****
		11	*****
		12	*****
		13	*****
		14	*****
		15	*****
		16	*****
		17	*****
		18	*****
		19	*****
		20	*****
		21	*****
		22	*****
		23	*****
		24	*****
		25	*****
		26	*****
		27	*****
		28	*****
		29	*****
		30	*****
		31	*****
		32	*****
		33	*****
		34	*****
		35	*****
		36	*****
		37	*****
		38	*****
		39	*****
		40	*****
		41	*****
		42	*****
		43	*****
		44	*****
		45	*****
		46	*****
		47	*****
		48	*****
		49	*****
		50	*****

LABORATOIRE DE RADIOPROPAGATION ELECTRONIQUE
Nom du programme: PROGRAMME DE GESTION DE LA PORTE VAL EN SECURITE
Fonction: commande des portes VAL par graphe de PETRI avec une
securite logique par traitement d'une fonction equitemps
Le systeme microprocesseur est constitue d'un kit SDK 51
muni d'une extension 'Commande des portes VAL'
Entree: sans / programme a joindre : GRPH.PET
Sortie: traitement des places dans GRPH.PET
Sortie anticipee: OUI , PIVOT(N) en cas d'erreur boucle d'attente
sans traitement equitemps
Subroutines utilisees:/
Date: FEVRIER 1983
Redacteur: JF DHALLUIN

0000		CSEG		
0000	802E	ORG	0000H	
		JMP	0030H	
0030		ORG	0030H	
0030	758920	MOV	TMDD, #020H	
0033	758DF9	MOV	TH1, #0F9H	
0036	D28E	SETB	TRI	
003B	759840	MOV	SCON, #40H	
				; INIT PORT SERIE
003B	758160	MOV	SP, #60H	
003E	7840	MOV	RO, #40H	
0040	7950	MOV	R1, #50H	
0042	900167	MOV	DPTR, #SYN	
0045	A682	MOV	ERO, DPL	
0047	08	INC	RO	
0048	A683	MOV	ERO, DPH	
004A	A782	MOV	ERI, DPL	
004C	09	INC	R1	
004D	A783	MOV	ERI, DPH	
004F	09	INC	R1	


```

LOC  OBJ          LINE      SOURCE
0050 750901       51          MOV      09H,#01H          ;INIT BANK 1 GESTION PROG PRINC (I)
0053 750A00       52          MOV      0AH,#00H
0056 751100       53          MOV      11H,#00H          ;INIT BANK 2 GESTION ROUTINES (J)
0059 751200       54          MOV      12H,#00H
005C C2D3         55          CLR      R50              ;SEL BANK 0
005E C2D4         56          CLR      RS1
0060 00           57          NOP
0061 0201EF       58          JMP      PL1              ;DEPART VERS LE TRAIT. DE LA PLACE PL1
59          ;
60          ;*****
61          ;
62          ;      ROUTINES DE TEST DES BLOCS FONCTIONNELS
63          ;      *****
64          ;
65          ;      TSTDPT: TEST DE CHARGEMENT DU POINTEUR DPTR
66          ;
0064 E6           67          TSTDPT: MOV      A,@R0          ;1;
0065 B5B322       68          CJNE     A,DPH,PIVOT1        ;2;
0068 18           69          DEC      R0                ;1;
0069 E6           70          MOV      A,@R0          ;1;
006A B5B21D       71          CJNE     A,DPL,PIVOT1        ;2;
006D 08           72          INC      R0                ;1;
006E 22           73          RET                          ;2; 10U
74          ;
75          ;      TSTSRT: TEST DU MOT DE COMMANDE
76          ;
006F E590         77          TSTSRT: MOV      A,P1          ;2;
0071 23           78          RL      A                  ;1;
0072 23           79          RL      A                  ;1;
0073 23           80          RL      A                  ;1;
0074 5407         81          ANL     A,#07H            ;1;
0076 B5F0         82          XRL     A,B                ;1;
0078 F4           83          CPL     A                  ;1;
0079 700F         84          JNZ     PIVOT1             ;2;
007B 22           85          RET                          ;2;12 U
86          ;
87          ;      TSTPLS: TEST DE MARQUAGE DE LA PLACE DE SYNCHRONISME
88          ;
007C E52E         89          TSTPLS: MOV      A,02EH        ;1;
007E 5401         90          ANL     A,#01H            ;1;
0080 600B         91          JZ      PIVOT1             ;2;
0082 22           92          RET                          ;2;
93          ;
94          ;      TSTRPS: TEST R.A.Z PLACE DE SYNCHRONISME
95          ;
0083 E52E         96          TSTRPS: MOV      A,02EH        ;1;
0085 5401         97          ANL     A,#01H            ;1;
0087 7001         98          JNZ     PIVOT1             ;2;
0089 22           99          RET                          ;2;
100         ;
101         ;      DEPART VERS UNE BOUCLE D'ATTENTE
102         ;
008A 020700      103         PIVOT1: LJMP     0700H
104         ;
105         ;*****

```





LOC	OBJ	LINE	SOURCE
009D	D2D3	111	EQT1: SEGMENT EQUITEMPS DU PROGRAMME PRINCIPAL
00BF	F8	112	SETB R50
0090	E9	113	MOV RO,A
0091	2A	114	MOV A,R1
0092	2A03	115	ADD A,R2
0094	13	116	ADD A,#03H
0095	B5086B	117	RRC A
0098	B90A	118	CJNE A,09H,NEGT
009A	B809	119	MOV 06H,R1
009C	69	120	MOV 09H,RO
009D	7064	121	XRL A,R1
009F	C2D3	122	JNZ NEGT
00A1	B294	123	CLR R50
00A3	C2B7	124	CPL P1.4
00A5	22	125	CLR P3.7
		126	RET
		127	
		128	EQTJ: SEGMENT EQUITEMPS D'UNE ROUTINE INDICEE
		129	M=MO
		130	
00A6	D2D4	131	EQTJ:
00A8	F8	132	SETB R51
00A9	E9	133	MOV RO,A
00AA	2A	134	MOV A,R1
00AB	2A03	135	ADD A,R2
00AD	13	136	ADD A,#03H
00AE	B51052	137	RRC A
00B1	8912	138	CJNE A,010H,NEGT
00B3	8811	139	MOV 12H,R1
00B5	69	140	MOV 11H,RO
00B6	704B	141	XRL A,R1
00B8	C2D4	142	JNZ NEGT
00BA	B294	143	CLR R51
00BC	22	144	CPL P1.4
		145	RET
		146	
		147	EQTK: SEGMENT EQUITEMPS D'UNE BOUCLE D'ATTENTE
		148	INDICEE K=KO
		149	
00BD	D2D3	150	EQTK:
00BF	D2D4	151	SETB R50
00C1	E9	152	MOV A,R1
00C2	2A	153	ADD A,R2
00C3	9277	154	ADD 077H,C
00C5	2A03	155	ADD A,#03H
00C7	FD	156	MOV R5,A
00CA	7400	157	MOV A,#00H
00CC	92E0	158	ACC.0,C
00CE	A277	159	C.077H
00D0	A2E0	160	MOV A,#00H
			C,ACC.0

:1: DYNAMISATION DU SIGNAL D'ACTIVATION X (équil'emps)

LOC	OBJ	LINE	SOURCE
00D2	ED	161	MOV A, R5 ;1;
00D3	13	162	RRC A ;1;
00D4	FD	163	MOV R5, A ;1;
00D5	6013	164	JZ NUL ;2;
00D7	C3	165	CLR C ;1;
00D8	98	166	SUBB A, R0 ;1;
00D9	4008	167	JC NEG ;2;
00DB	ED	168	POS: MOV A, R5 ;1;
00DC	C3	169	CLR C ;1;
00DD	9B	170	SUBB A, R3 ;1;
00DE	B51822	171	CJNE A, 18H, NEQT ;2;
00E1	8011	172	SJMP ACQ ;2;
00E3	ED	173	NEG: MOV A, R5 ;1;
00E4	2C	174	ADD A, R4 ;1;
00E5	B5181B	175	CJNE A, 18H, NEQT ;2;
00E8	800A	176	SJMP ACQ ;2;
00EA	2C	177	NUL: ADD A, R4 ;1;
00EB	B51815	178	CJNE A, 18H, NEQT ;2;
00EE	7D01	179	MOV R5, #01H ;1;
00F0	0B	180	INC R3 ;1;
00F1	1C	181	DEC R4 ;1;
00F2	00	182	NOP ;3;
00F3	00	183	NOP ;1;
00F4	F8	184	ACQ: MOV R0, A ;1;
00F5	A91D	185	MOV R1, 1DH ;2;
00F7	AA1D	186	MOV R2, 1DH ;2;
00F9	1A	187	DEC R2 ;1;
00FA	0B	188	INC R3 ;1;
00FB	1C	189	DEC R4 ;1;
00FC	C2D3	190	CLR RS0 ;1;
00FE	C2D4	191	CLR RS1 ;1;
0100	B294	192	CPL P1.4 ;1; x dynamisation du signal equitemps
0102	22	193	RET ;2;
		194	
		195	
0103	020700	196	NEQT: LJMP 0700H
		197	
		198	*****
		199	
		200	; UTILITAIRES DU GRAPHE DE PETRI
		201	; *****
		202	
		203	; ETAT: LECTURE DU MOT D'ETAT
		204	
0106	E5B0	205	ETAT: MOV A, P3 ;2;
0108	5470	206	ANL A, #070H ;2;
010A	00	207	NOP
010B	00	208	NOP ;2;
010C	22	209	RET ;2; B U
		210	
		211	; COMD: ROUTINE DE SORTIE D'UN MOT DE COMMANDE
		212	
010D	03	213	COMD: RR A ;1;
010E	03	214	RR A ;1;
010F	03	215	RR A ;1;



LOC	OBJ	LINE	SOURCE
0110	441F	216	ORL A, #1FH ;1;
0112	F590	217	MOV P1, A ;2;
0114	22	218	RET ;2; 8 U
0115	751909	219	;
0118	751A08	220	CHRUCI: APPEL DE UCI
011B	751B00	221	MOV 19H, #09D ;2;
011E	751C00	222	MOV 1AH, #08D ;2;
0121	22	223	MOV 1BH, #00H ;2;
		224	MOV 1CH, #00H ;2;
		225	RET ;2;
		226	;
		227	;
		228	UCI: BOUCLE D'ATTENTE D'ENTREE D'UN CARACTERE
		229	DEPUIS LE CLAVIER DU SDK 51 K=10
		230	;
0122	C0B2	231	DPL ;2;
0124	C0B3	232	DPH ;2;
0126	E590	233	A, P1 ;2;
012B	540E	234	ANL A, #0EH XXXX 101X
012A	44F1	235	ORL A, #0F1H 1111 1011
012C	64FF	236	XRL 64FF ;1; 1111 1111
012E	00	237	NOP ;1;
012F	700F	238	JNZ CAR ;2; 0000 0100
0131	7A1A	239	MOV R2, #26D ;1;
0133	DAFE	240	DJNZ R2, \$;50;
0135	751B0A	241	MOV 18H, #10D ;2;
0138	11ED	242	ACALL E0TK ;2+32+2
013A	00	243	NOP
013B	00	244	NOP
013C	00	245	NOP
013D	00	246	NOP
013E	80E6	247	JMP BOUCL ;4;
0140	00	248	NOP ;2;
0141	00	249	NOP ;5;
0142	00	250	NOP
0143	00	251	NOP
0144	00	252	NOP
0145	B504E9	253	CJNE A, 04H, PCAR ;2;
0148	00	254	NOP
0149	7A1A	255	MOV R2, #26D ;1;
014B	DAFE	256	DJNZ R2, \$;50;
014D	751B0A	257	MOV 18H, #10D ;2;
0150	11ED	258	ACALL E0TK ;2+32+2
0152	D0B3	259	POP DPH ;2;
0154	D0B2	260	POP DPL ;2;
0156	22	261	RET ;2;
		262	;
		263	;
		264	CHRSHN: CHARGEMENT DE LA ROUTINE DE SYNCHRONISME
0157	751E14	265	MOV 1EH, #20D ;2;
015A	751913	266	MOV 19H, #19D ;2;
015D	751A12	267	MOV 1AH, #18D ;2;
0160	751B00	268	MOV 1BH, #00H ;2;
0163	751C00	269	MOV 1CH, #00H ;2;
0166	22	270	RET ;2;

```

LOC  OBJ          LINE    SOURCE
                                271
                                272      ;      SYN:  ROUTINE DE SYNCHRONISME DU GRAPHE DE PETRI.
                                273      ;      TRAITEMENT ANTI REBONDISSEMENT, ARBD, SUR LE VECTEUR D'ENTREE
                                274      ;      R3 (BANK 0) UTILISE - INDICE :20 PAR CHRSYN
                                275      ;      SINON PARAMETRER LA VALEUR DE L'INDICE DANS LE REG 01EH
                                276
                                277
0167  E8          278      SYN:  MOV    A, R0          ;1;
0168  C9          279              XCH    A, R1          ;1;
0169  F8          280              MOV    R0, A         ;1;
016A  900167      281              MOV    DPTR, #SYN    ;2;
016D  A682        282              MOV    @R0, DPL     ;2;
016F  08          283              INC    R0           ;1;
0170  A683        284              MOV    @R0, DPH     ;2;
0172  3106        285              ACALL  ETAT         ;8;
0174  B52F0C      286              CJNE   A, 02FH, ARBD ;2;
0177  7A11        287              MOV    R2, #17D    ;1;
0179  DAFE        288              DJNZ   R2, $        ;32;
017B  851E18      289              MOV    18H, 1EH    ;2;
017E  11BD        290              ACALL  EQTK         ;40+2;
0180  02019F      291              JMP    RETR         ;2;
0183  F5F0        292      ARBD:  MOV    B, A          ;1;
0185  7B32        293              MOV    R3, #50D    ;1;50*100MSEC DE TRAITEMENT ARBD
0187  851E18      294      BCLE:  MOV    18H, 1EH    ;2;
018A  00          295              NOP                    ;1;
018B  11BD        296              ACALL  EQTK         ;40+2;
018D  7A1B        297              MOV    R2, #27D    ;1;
018F  DAFE        298              DJNZ   R2, $        ;52;
0191  DBF4        299              DJNZ   R3, BCLE    ;2;
0193  851E18      300              MOV    18H, 1EH    ;2;
0196  11BD        301              ACALL  EQTK         ;40+2;
0198  3106        302              ACALL  ETAT         ;8;
019A  B5F0E6      303              CJNE   A, B, ARBD  ;2;
019D  F52F        304              MOV    02FH, A     ;1;
019F  8783        305      RETR:  MOV    DPH, @R1    ;2;
01A1  19          306              DEC    R1           ;1;
01A2  8782        307              MOV    DPL, @R1    ;2;
01A4  7A14        308              MOV    R2, #20D    ;1;
01A6  DAFE        309              DJNZ   R2, $        ;38;
01A8  851E18      310              MOV    18H, 1EH    ;2;
01AB  11BD        311              ACALL  EQTK         ;40+2;
01AD  7400        312              MOV    A, #00H     ;1;
01AF  73          313              JMP    @A+DPTR     ;2;
                                314
                                315      ;      BOUCLE D'ATTENTE DE TEMPORISATION TMP
                                316      ;      CHARGER DANS R3 (BANK 0) LA DUREE EN 1/10 DE SECONDE
                                317      ;      R4 ET R5 (BANK 0) SONT UTILISES . INDICE K=40D
                                318      ;      *****
                                319
                                320      ;      CHRTMP: CHARGEMENT DE LA BOUCLE D'ATTENTE TMP
                                321
01B0  751927      322      CHRTMP: MOV    19H, #39D    ;2;
01B3  751A26      323              MOV    1AH, #38D    ;2;
01B6  751B00      324              MOV    1BH, #00H    ;2;
01B9  751C00      325              MOV    1CH, #00H    ;2;

```



209
1100

```

LOC OBJ          LINE      SOURCE
01BC 22          326          RET                ;2;
                   327
                   328          ;          TMP:      BOUCLE D'ATTENTE DE TEMPORISATION
                   329
01BD 7D0B        330          TMP:      MOV        R5, #11D          ;1;
01BF 7C65        331          WTM:      MOV        R4, #101D         ;1;
01C1 7A1B        332          WTMP:     MOV        R2, #27D         ;1;
01C3 DAFE        333                   DJNZ       R2, $              ;52;
01C5 75182B      334                   MOV        18H, #40D          ;2;
01C8 11BD        335                   ACALL      EQTK               ;40+2;
01CA 00          336                   NOP                          ;1;
01CB DCF4        337                   DJNZ       R4, WTMP           ;2;
01CD DDF0        338                   DJNZ       R5, WTM            ;2;
01CF DBEC        339                   DJNZ       R3, TMP            ;2;  TEMPO: R3(100microsec*100*10)=R3*0, 1SECONDE
01D1 7A1B        340                   MOV        R2, #24D           ;1;
01D3 DAFE        341                   DJNZ       R2, $              ;48;
01D5 75182B      342                   MOV        18H, #40D          ;2;
01D8 11BD        343                   ACALL      EQTK               ;40+2;
01DA 22          344                   RET                            ;2;
                   345
                   346          ;          CHRRO:   CHARGEMENT DE LA PILE R0
                   347
01DB 08          348          CHRRO:   INC        R0            ;1;
01DC A682        349                   MOV        @R0, DPL           ;2;
01DE 08          350                   INC        R0                ;1;
01DF A683        351                   MOV        @R0, DPH           ;2;
01E1 22          352                   RET                            ;2;
                   353
                   354          ;          DCHR1:   DECHARGEMENT DE LA PILE R1
                   355
01E2 19          356          DCHR1:   DEC        R1            ;1;
01E3 8783        357                   MOV        DPH, @R1           ;2;
01E5 19          358                   DEC        R1                ;1;
01E6 8782        359                   MOV        DPL, @R1           ;2;
01E8 22          360                   RET                            ;2;
                   361
                   362          ;          DEMRQ:   DEMARQUAGE DE LA PILE D'ECRITURE
                   363
01E9 18          364          DEMRQ:   DEC        R0            ;1;
01EA 18          365                   DEC        R0                ;1;
01EB 22          366                   RET                            ;2;
                   367
01EC 020700      368          PIVOT2:  LJMP       0700H         ;PIVOT DE SORTIE
                   369
                   370          ;*****
                   371
                   372          ;          TRAITEMENT DU GRAPHE DE PETRI
                   373          ;          *****
                   374
                   375          ;          PL1:      PHASE PORTE FERMEE VERROUILLEE ATTENTE
                   376          ;          DE LA COMMANDE DE DEVERROUILLAGE 'D'
                   377
01EF 9001EF      378          PL1:      MOV        DPTR, #PL1         ;2;
01F2 31DB        379                   ACALL      CHRRO              ;10;
01F4 7404        380                   MOV        A, #04H            ;1;

```

← début du programme d'application

LOC	OBJ	LINE	SOURCE
01F6	310D	381	ACALL
01F8	75F0FB	382	MOV B, #0FBH
01FB	116F	383	TSTSRT
01FD	7C02	384	MOV R4, #02H
01FF	3115	385	CHRUCI
0201	7A11	386	MOV R2, #17D
0203	DAFE	387	R2, \$
0205	7402	388	DJNZ A, #02H
0207	118D	389	ACALL EDITI
0209	3122	390	ACALL UCI
020B	E518	391	MOV A, 18H
020D	B40ADC	392	A, #10D, PIVOT2
0210	31E9	393	DEMRO
0212	90022D	394	DPTR, #PL2
0215	31DB	395	MOV CHRRO
0217	1164	396	TSTDPT
0219	75F0FB	397	MOV B, #0FBH
021C	116F	398	TSTSRT
021E	7A04	399	MOV R2, #04D
0220	DAFE	400	R2, \$
0222	31E2	401	DJNZ DCHR1
0224	3157	402	CHR SYN
0226	7403	403	MOV A, #03H
0228	118D	404	EDITI
022A	7400	405	MOV A, #00H
022C	73	406	DPTR, #PL2
407			PHASE DE DEVERROUILLAGE ATTENTE DE LA
408			COMMANDE D'OUVERTURE '0'
409			PL2:
410			PL2:
022D	90022D	411	MOV DPTR, #PL2
0230	31DB	412	CHRRO
0232	7405	413	MOV A, #05H
0234	310D	414	COMD
0236	75F0FA	415	MOV B, #0FAH
0239	116F	416	TSTSRT
023B	7C04	417	MOV R4, #04H
023D	3115	418	CHRUCI
023F	7A12	419	MOV R2, #18D
0241	DAFE	420	R2, \$
0243	7404	421	MOV A, #04H
0245	118D	422	EDITI
0247	3122	423	ACALL UCI
0249	E518	424	MOV A, 18H
024B	B4009E	425	A, #10D, PIVOT2
024E	31E9	426	DEMRO
0250	90027B	427	DPTR, #PL3
0253	31DB	428	CHRRO
0255	1164	429	TSTDPT
0257	75F0FA	430	MOV B, #0FAH
025A	116F	431	TSTSRT
025C	7A02	432	MOV R2, #02D
025E	DAFE	433	R2, \$
0260	516E	434	DJNZ CHRPL3
0262	751E0F	435	MOV O1EH, #15D

→ Fin du premier segment équitemps
 → Appel de la boucle d'attente
 traitant la transition 'D'

→ Fin du second segment équitemps
 Fin de traitement de la place 1

→

PREPARATION DE LA BOUCLE D'ATTENTE PL3
 PARAMETRE K POUR LA BOUCLE SYN



TABLE DES MATIERES

INTRODUCTION

PREMIERE PARTIE

<i>I - <u>CONSIDERATIONS GENERALES SUR LES PROBLEMES DE SECURITE</u></i>	p. 1
<i>I₁ - Définition des objectifs à atteindre, exemple du métro Lillois</i>	p. 1
<i>I₂ - Sécurité et sûreté de fonctionnement</i>	p. 3
<i>I₂₋₁ - Sûreté de fonctionnement</i>	p. 3
<i>I₂₋₂ - Existence d'un état de sécurité</i>	p. 4
<i>I₃ - Evolution de la technique, mise en oeuvre de structures micro-programmées</i>	p. 6
<i>I₄ - Adaptation de l'architecture en fonction du processus à commander</i>	p. 8
<i>II - <u>COMMANDE DE PROCESSUS EN SECURITE. MISE EN OEUVRE DE SYSTEMES MICROPROCESSEURS</u></i>	p. 10
<i>II₁ - Caractérisation d'un processus. Définition des variables d'état, de sortie, et des sollicitations extérieures</i>	p. 10
<i>II₂ - Evolution du processus. Etablissement d'un domaine d'évolution en sécurité. Etude de fiabilité</i>	p. 11
<i>II₃ - Commande-contrôle de processus en sécurité par microprocesseur</i>	p. 14
<i>II₃₋₁ - Etude de sécurité de la commande d'un processus</i>	p. 15
<i>II₃₋₁₋₁ - Gestion d'une tâche de détection et d'analyse des pannes du processus, des voies de mesure et de commande</i>	p. 15
<i>II₃₋₁₋₂ - Configuration nécessaire et suffisante des vecteurs d'état et de commande</i>	p. 17
<i>II₃₋₁₋₃ - Traitement des informations de panne</i>	p. 17
<i>II₃₋₂ - Définition d'un état de sécurité du système de commande à microprocesseur</i>	p. 18
<i>II₄ - Méthodologie d'observation d'un processus en vue de détecter et de diagnostiquer un défaut de fonctionnement</i>	p. 20
<i>II₅ - Conclusion.</i>	p. 21

<u>III - DETECTION DES DEFAUTS DE FONCTIONNEMENT SUR LES SYSTEMES</u>	p. 23
<u>MICROPROCESSEURS</u>	
III ₁ - Modes de pannes imputables aux microprocesseurs et composants associés	p. 23
III ₁₋₁ - Hypothèses sur l'apparition des défauts	p. 24
III ₁₋₂ - Classement des types d'instruction et modèles de fautes associés	p. 25
III ₂ - Méthodes de type auto-test de détection d'erreurs de fonctionnement des microprocesseurs	p. 27
III ₂₋₁ - Détection d'erreur par test fonctionnel	p. 27
III ₂₋₂ - Détection d'erreur par test temporel	p. 29
III ₂₋₃ - Détection d'erreur par utilisation des codages	p. 31
III ₃ - Fiabilité des systèmes microprocesseurs	p. 33
Conclusion de la première partie.	p. 36

DEUXIEME PARTIE

<u>I - ETUDE DU SYSTEME DE PORTE D'UN VEHICULE DE TYPE VAL.</u>	p. 38
<u>DEFINITION D'UN DISPOSITIF DE COMMANDE A MICROPROCESSEUR</u>	
I ₁ - Description du système de commande de porte installé sur VAL	p. 38
I ₁₋₁ - Fonctions propres à garantir la sécurité des voyageurs	p. 39
I ₁₋₂ - Génération de la commande d'ouverture	p. 40
I ₁₋₃ - Elaboration des informations de sécurité.	p. 40
Analyse de sécurité	
I ₂ - Définition des fonctions de sécurité d'un nouveau système de commande de porte à microprocesseur. Remarques préliminaires	p. 43
I ₃ - Organisation et développement du projet "commande de porte"	p. 45
I ₄ - Etablissement de la configuration vecteur d'état, vecteur de commande propre à tenir les objectifs de sécurité	p. 47
I ₄₋₁ - Optique sécurité	p. 47
I ₄₋₂ - Optique disponibilité	p. 48

<u>II - DEFINITION DE L'ARCHITECTURE MICROINFORMATIQUE GLOBALE DE</u>	p. 49
<u>COMMANDE DE PORTE AU NIVEAU D'UN VEHICULE D'UNE RAME DE METRO</u>	
II ₁ - Position du problème. Introduction du concept de réseau local étendu à l'ensemble d'une rame de métro formée d'un nombre variable de véhicules	p. 49
II ₂ - Réseau local de commande de processus en sécurité. Réseau local de commande de porte	p. 50
II ₃ - Rappel de quelques concepts sur les réseaux locaux	p. 52
II ₃₋₁ - Application au réseau local de commande de porte d'un véhicule	p. 53
II ₃₋₂ - Gestion des accès entre les différents systèmes	p. 53
II ₄ - Choix de la technologie optique en tant que support matériel du réseau	p. 54
II ₄₋₁ - Isolement galvanique	p. 54
II ₄₋₂ - Immunité totale aux parasites électromagnétiques	p. 54
II ₄₋₃ - Marge de sécurité importante sur les performances	p. 54
II ₄₋₄ - Technologie optique. Etat de l'art et perspectives dans son application aux transports terrestres	p. 55
II ₅ - Réalisation d'un réseau local à transmissions optiques de commande-contrôle de portes véhicules d'une rame de métro	p. 56
II ₅₋₁ - Description fonctionnelle du réseau	p. 56
II ₅₋₁₋₁ - Cartes de commande de porte (Ci)	p. 56
II ₅₋₁₋₂ - Système centralisateur de données	p. 57
II ₅₋₁₋₃ - Gestion des accès	p. 57
II ₅₋₁₋₄ - Mode de fonctionnement dégradé du réseau	p. 58
II ₅₋₂ - Répartition des fonctions de sécurité sur les diverses composantes du réseau	p. 59
II ₅₋₂₋₁ - Fonctions de sécurité allouées aux cartes de commande de porte	p. 59
II ₅₋₂₋₂ - Fonctions de sécurité du système central	p. 60
II ₆ - Conclusion.	p. 60

<i>III - <u>DETECTION ET ANALYSE DES PANNES DU PROCESSUS PAR ANALYSE SEQUENTIELLE DU VECTEUR D'ETAT</u></i>	p. 62
<i>III₁ - Description des séquences de commande de porte</i>	p. 62
<i>III₁₋₁ - Séquences de commande du mécanisme de porte en mode normal</i>	p. 62
<i>III₁₋₂ - Séquences de commande en mode dégradé</i>	p. 63
<i>III₂ - Présentation de la méthode de détection des pannes du processus sous contrôle</i>	p. 64
<i>III₂₋₁ - Hypothèses de travail</i>	p. 64
<i>III₂₋₂ - Modélisation des pannes possibles</i>	p. 65
<i>III₂₋₃ - Mode l'observation et de représentation du fonctionnement du processus</i>	p. 66
<i>III₂₋₄ - Procédure de détection et d'analyse des pannes</i>	p. 67
<i>III₂₋₅ - Remarque de sécurité sur la détection des pannes</i>	p. 69
<i>III₃ - Logiciel de traitement du graphe de Pétri</i>	p. 70
<i>III₄ - Bilan de la fonction détection et analyse de panne. Périodicité du cycle de détection. Temps de tolérance aux fautes</i>	p. 71
<i>III₅ - Conclusion.</i>	p. 76
<i>IV - <u>ETUDE DE LA MISE EN SECURITE DES CARTES DE COMMANDE DE PORTE</u></i>	p. 77
<i>IV₁ - Mise en sécurité d'un microprocesseur par traitement d'une fonction équitemps (EQT)</i>	p. 78
<i>IV₂ - Traitement de la fonction équitemps</i>	p. 81
<i>IV₂₋₁ - Traitement équitemps par tests chronologiques</i>	p. 82
<i>IV₂₋₂ - Traitement équitemps par tests logiques</i>	p. 83
<i>IV₃ - Analyse critique des tests effectués</i>	p. 83
<i>IV₄ - Certification du logiciel</i>	p. 84
<i>IV₅ - Application d'un état de sécurité au mécanisme de porte en cas de défaillance du microprocesseur.</i>	p. 85
<i>CONCLUSION GENERALE</i>	p. 89

ANNEXES

- Annexe 1 - Commande de processus par dispositif en redondance majoritaire* p. 91
- Annexe 2 - Représentation par graphe de Pétri des phases de fonctionnement d'un mécanisme de porte, et des tests d'hypothèse effectués en vue de la détection des pannes* p. 94
- Annexe 3 - Calculs de fiabilité* p. 95
- Annexe 4 - Application du traitement équitemps à un logiciel de commande de porte représenté par graphe de Pétri.* p. 102

B I B L I O G R A P H I E

- 1 - A. RAULT, C. BASKIOTIS
"Surveillance, détection et diagnostic de processus".
Communication journées SURF - Janvier 1982.
- 2 - M. SCHWOB, G. PEYRACHE
"Traité de fiabilité".
Ed. Masson - 1969.
- 3 - Documentation CNET
"Recueil de données de fiabilité".
Edition 1976 - remise à jour janvier 1979.
- 4 - Documentation CNET
"Recueil de données de fiabilité : circuits intégrés".
Remise à jour janvier 1982.
- 5 - R. GABILLARD
"Tentative de vérification de vraisemblance de l'affirmation de sécurité reposant sur le recours au concept de la sécurité positive".
Note U.S.T.L. - diffusion MATRA - EPALE - Mars 1978.
- 6 - H. HUBEL
"Commande automatique de véhicules sur rail".
Revue des Télécommunications - N° 52/4 - 1977.
- 7 - *"Commentaire sur l'étude SFENA concernant l'application en sécurité des microprocesseurs dans le pilotage automatique".*
Document IRT - Rapport MA 78 190 - 1ère édition Décembre 1978.
- 8 - *"Comtrac. Fault tolerant computer system with three symmetric computers".*
Proc IEEE - 10p 1160 - Octobre 1978.
- 9 - A. COSTES, J.C. LAPRIE
"Ordinateurs non stop".
Revue La Recherche N° 140 - Janvier 1983.

- 10 - *"Utilisation des microprocesseurs dans les applications ferroviaires de sécurité"*.
Document IRT - Recherche bibliographique - Rapport MA 82 - 103 - Août 1982.
- 11 - D. POWELL
"Réseaux locaux de commande-contrôle de processus sûrs de fonctionnement".
Thèse d'état - Institut National Polytechnique de Toulouse - Octobre 1981.
- 12 - J.P. JAGUIN
"Propriétés mécaniques et vieillissement des fibres optiques".
Thèse Docteur Ingénieur - Université de Rennes - 1980.
- 13 - *"Réalisation d'un réseau d'interconnexions optiques"*.
Rapport d'étude Compagnie Lyonnaise de Transmissions Optiques - Janvier 1982
- 14 - J. ABADIR, Y. DESWARTE
"Auto-dest des processeurs du système informatique SARGOS".
Communication journées SURF - Janvier 1982.
- 15- *"Projet Pilote - Sûreté de fonctionnement"*.
Bilan et perspectives - 20-21-22 janvier 1982.
Agence de l'Informatique.
- 16 - R.N. MARCZYNSKI, P. KERNTOPF, F. ANCEAU, B. COURTOIS
"A method for detection of microcomputer malfunctions".
Digital Structures Department - Polish Academy of Sciences -
Architecture des calculateurs - Ensimag Université de Grenoble.
- 17 - A. WILLSKY
"A survey of design methods for failure detection in dynamic systems".
Automatica, vol. 12, p 601-611 - 1976.
- 18 - TZE THONG CHIEN, M. ADAMS
"A sequential failure detection technique and its application".
Revue IEEE Transactions on Automatic Control - Octobre 1976.
- 19 - A. WALD
"Sequential analysis".
John Wiley - 1947.
- 20 - *"Sûreté de fonctionnement des systèmes informatiques"*
Monographies d'informatique de l'AFCEC - 1980.
Sous la direction de E. Gelembe - Editions Hommes et techniques.

- 21 - J. ARLAT
"Conception d'un microcalculateur tolérant aux fautes par diversification fonctionnelle".
Thèse Docteur Ingénieur - Institut National Polytechnique de Toulouse -
Avril 1979.

- 22 - D. JOURDAN
"Un dispositif de test aléatoire pour microprocesseur".
Thèse Docteur Ingénieur - Institut National Polytechnique de Grenoble -
Novembre 1981.

- 23 - D. SUALDI, J.P. VAUTRIN
"Les précautions à prendre lors de la simplification des expressions logiques".
Revue Electronique Industrielle N° 35 p 45 à 51 - Juin 1982.

- 24 - P. ITICSOHN
"Sécurité et automates programmables".
Revue Electronique Industrielle N° 35 p 57 à 62 - Juin 1982.

- 25 - C. GROSS
"Trogiciels et langages de commande-contrôle".
Revue Electronique Industrielle N° 39 p 51 à 53 - Octobre 1982.

- 26 - C. ROBACH, G. SAUCIER
*"Le test des microprocesseurs et des systèmes à microprocesseurs -
état de l'art et perspectives".*
Revue l'Onde électrique - vol 61, n° 3 - 1981.

- 27 - J.F. DHALLUIN
*"Rapport bibliographique sur la mise en sécurité des systèmes micro-
processeurs".*
Note USTL - Septembre 1983.

- 28 - *"Power Mosfet : reliability tests and results".*
Hewlett Tackard - Application bulletin N° 34.

- 29 - D. PELAND, G. SAUCIER
*"Conception de systèmes temps réel à très haute sécurité sur micro-
processeur".*
Rapport de recherche IMAG - 1978.

- 30 - *"H MOS Reliability".*
Intel. Reliability report RR 18.

- 31 - "Intec. ISBC 86/12 Single board computer".
Reliability Report RR 23.
- 32 - J.F. DHALLUIN
"Etude de sécurité et de fiabilité disponibilité des portes véhicule du métro de Lille".
Note USTL - Avril 1980.
- 33 - R. GABILLARD
"Analyse théorique de la stabilité des amplificateurs des fonctions "ET" de sécurité".
Note USTL - Janvier 1982.
- 34 - F. GEZE, M. DHOOGHE
"Réalisation d'un ensemble sécuritaire de commande des portes du métro de Lille".
Rapport de projet de fin d'études EUDIL - Juin 1982.
- 35 - M. CUVELIER
"Participation aux essais de sécurité d'un système microprocesseur destiné à la commande des portes VAL".
Rapport de stage IUT Lille Génie électrique - Juin 1982.
- 36 - A. FICHAUX
"Participation aux essais de sécurité d'un système microprocesseur destiné à la commande des portes VAL".
Rapport de stage IUT Calais Génie électrique - Juin 1982.
- 37 - E. EL KOURSI
"Implantation de réseaux de Petri sur microprocesseur".
Intel. 8085.
Rapport DEA USTL - Octobre 1982.
- 38 - E. KOURSI
"Manuel d'utilisation d'une méthode d'implantation des réseaux de Petri sur microprocesseur - Application au microprocesseur 8051".
Note USTL - Mars 1983.
- 39 - E. KOURSI
"Commande des portes VAL - Logiciel de commande et de contrôle".
Note USTL - Avril 1983.
- 40 - M. CUVELIER
"Commande des portes VAL - Carte de commande à microprocesseur".
Notice technique USTL - Avril 1983.

- 41 - G. BROQUET
"Commande des portes VAL - Réalisations technologiques sur le mécanisme de porte "VAL".
Notice technique USTL - Mars 1983.
- 42 - CH. MAGNIEZ
"Commande d'un ensemble de processus en sécurité - Application à la commande d'un ensemble de portes véhicules de métro".
Rapport DEA USTL - Juillet 1983.
- 43 - P. BARBIER, J. HULOUX
"Mise en sécurité d'un système à microprocesseurs".
Rapport de projet de fin d'études EUDIL - Juin 1983.
- 44 - A. OUADGHIRI
"Application de la théorie des codages en traitement d'informations de sécurité analysées par microprocesseur".
Rapport DEA USTL - Juillet 1983.
- 45 - PH. DELANGHE
"Contribution à la mise en sécurité d'un système de commande à micro-processeurs".
Rapport DEA USTL - Juin 1983.
- 46 - M. CARTIER
"Sécurité des portes d'accès véhicule".
Note sécurité Matra-CIMT - Octobre 1980.
- 47 - R. CARTIER
"Portes d'accès".
Note fiabilité Matra-CIMT - Décembre 1978.
- 48 - R. CARTIER
"Table des taux de défaillance - Composants électromécaniques et électroniques".
Note fiabilité Matra-CIMT - Février 1979.
- 49 - C. GROSS
"Les réseaux de mini vont-ils s'ouvrir sur l'extérieur".
Revue Electronique Industrielle N° 12 p 45 à 48 - Mars 1981.
- 50 - *"Etude de faisabilité d'un réseau d'interconnexions à fibres optiques selon les spécifications données par l'U.S.T.L.*
Document de la Compagnie Lyonnaise de Transmissions Optiques (CLTO) - Janvier 1983.

- 51 - Sylvain THELLIEZ
"Pratique séquentielle et réseaux de Pétri".
Edition Eprolles - Paris - 1978.
- 52 - John F. WAKERLY
"Error detecting codes - Self checking circuits".
Palo Alto - California - 1977.
- 53 - *"Proposition pour une nouvelle réglementation de systèmes de transport collectif terrestre de voyageurs".*
Rapport du groupe de travail pour l'étude d'une réglementation de nouveaux moyens de transport collectif urbain, présidé par J. Chauchoy - Conseil Général des Ponts et Chaussées - Mars 1976.
- 54 - R. GABILLARD
"Propositions en vue de la définition d'un cahier des charges de sécurité des modes nouveaux de transports".
Rapport final de contrat conclu entre l'USTL et le Ministère des Transports 1977.
- 55 - J.F. DHALLUIN
"Mise en sécurité d'un microprocesseur par traitement d'une fonction équitemps. Application à la commande d'une porte de métro dont la séquence est décrite par graphe de Pétri".
Rapport USTL - Novembre 1983.



R E S U M E

Le travail présenté est le résultat d'une recherche portant sur la commande de processus en sécurité à l'aide de microprocesseurs. L'application envisagée est celle de la commande d'un ensemble de portes véhicule d'une rame de métro du type VAL.

La première partie de ce mémoire présente les concepts traditionnels de la commande de processus en sécurité. Les aspects nouveaux du problème naissant de la présence des microprocesseurs y sont développés, à l'issue de quoi quelques principes généraux d'étude sont exposés ainsi qu'une recherche bibliographique sur la mise en sécurité des microprocesseurs en autotest.

La seconde partie traite de l'application sur la commande des portes de métro où après une étude du système existant on y développe l'établissement d'un réseau local de commande-contrôle au sein d'un véhicule. Les méthodologies d'analyse de fonctionnement du processus et du microprocesseur y sont présentées.

MOTS CLES

- Sécurité des transports - Microprocesseur -
- (Graphe) Réseaux de Pétri - Analyse séquentielle - Détection de pannes
- Test temporel - Test fonctionnel - Tolérance aux fautes
- Réseau local - Commande-contrôle