Evaluation de la sûreté de fonctionnement des systèmes de sécurité - Application à la commande des postes à très haute tension

Karama Kanoun

N° d'ordre : 88

Année 1980

THÈSE

présentée

A L'INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE

pour l'obtention

du Diplôme de DOCTEUR INGÉNIEUR

par

Karima MEDHAFFER-KANOUN

Ingénieur ENAC

EVALUATION DE LA SURETE DE FONCTIONNEMENT DES SYSTEMES DE SECURITE

—

APPLICATION A LA COMMANDE DES POSTES A TRES HAUTE TENSION

Soutenue le 4 Juillet 1980, devant la Commission d'Examen :

MM.	A. COSTES	Président
	J.P. AUCLAIR	Examinateurs
	J.P. BARRET	
	L. CARPENTIER	
	J.C. LAPRIE	
	B. POTIN	
Mme	G. SAUCIER	

A Jean-Claude LAPRIE

A Alain COSTES

A Francis CEREJA

A mes camarades de l'Equipe "Architectures Sûres de Fonctionnement"

REMERCIEMENTS

Je ne saurais commencer ce mémoire sans remercier :

- *Monsieur le Professeur G. GRATELOUP, Directeur du Laboratoire d'Automatique et d'Analyse des Systèmes du C.N.R.S., qui m'a accueillie dans son Laboratoire et m'a honorée de sa confiance,*
- *Monsieur J.C. LAPRIE, Responsable de l'Equipe "Architectures Sûres de Fonctionnement" du L.A.A.S. du C.N.R.S., de m'avoir accueillie au sein de son équipe. Que ce mémoire soit pour lui le témoignage de ma reconnaissance pour l'orientation qu'il a su donner à mes travaux.*

Je tiens également à exprimer ma profonde gratitude à :

- *Monsieur A. COSTES, Professeur à l'Institut National Polytechnique de Toulouse, Président du Jury,*
- *Monsieur J.P. AUCLAIR, Ingénieur Principal à la S.N.C.F., Division VZA,*
- *Monsieur J.P. BARRET, Chef du Département Fonctionnement des Réseaux - Conduite Automatismes à E.D.F.*
- *Monsieur L. CARPENTIER, Directeur Technique à ALSTHOM C.G.E.E.,*
- *Monsieur J.C. LAPRIE, Chargé de Recherche au C.N.R.S.,*
- *Monsieur B. POTIN, Chef du Laboratoire d'Informatique du GIER-SCHLUMBERGER,*
- *Madame G. SAUCIER, Professeur à l'E.N.S.I.M.A.G.*

Ces travaux n'auraient pas été possibles sans l'aide d'ELECTRICITE DE FRANCE. Que cet Organisme et plus particulièrement l'ensemble du personnel du Département Fonctionnement des Réseaux - Conduites Automatismes, trouve ici l'expression de tous mes remerciements pour sa collaboration.

Je réserve ici une place privilégiée à Jean-Claude LAPRIE et à Alain Costes ; qu'ils trouvent ici l'expression de ma reconnaissance pour tous les conseils et l'aide qu'ils m'ont apportés dans la réalisation de ce mémoire.

Je remercie chaleureusement tous ceux qui m'ont aidée dans la réalisation de mon travail :

- *Francis CEREJA, ancien membre de l'équipe "Architectures Sûres de Fonctionnement",*
- *C. BEOUNES, J.P. BLANQUART, Y. CROUZET, C. LANDRAULT, A.M. LEGWINSKI, J. MOREIRA de SOUZA, D. NOYES, D. POWELL, L. RIOU, C. ROUZIES, membres de l'Equipe "Architectures Sûres de Fonctionnement",*
- *J. PENAVAYRE, Secrétaire de la Division "Structures des Systèmes de Commande Automatique",*
- *C. MARROT,*
- *G. BOUYSSOU, J.C. IPPOLITO, J.E. DOUCET, B. MEUNIER du Service Informatique et Simulation,*
- *M.T. IPPOLITO, J. CATALA, E. LAPEYRE-MESTRE, R. ZITTEL, D. DAURAT, R. LORTAL du Service "Documentation-Publications".*

SOMMAIRE

INTRODUCTION

La croissance de notre société industrielle s'accompagne d'un accroissement des risques encourus sur les plans économique, de l'environnement et des vies humaines. En particulier, et c'est là un fait nouveau de ces trente dernières années, le développement technologique s'accompagne de risques potentiels dont la gravité des conséquences est difficilement prévisible, sur les plans de la propagation spatiale (ampleur des dégâts) et temporelle (conséquences à long terme).

Chacun de nous a en mémoire des exemples récents qui furent catastrophiques ou pour lesquels une catastrophe fut évitée de justesse (pannes générales d'électricité de New-York et de la France, dégagement de dioxine à Seveso, "syndrome chinois" à Three Mile Island,...).

Ces risques industriels majeurs résident dans des installations extrêmement complexes dont la surveillance du comportement en temps réel excède les capacités d'opérateurs humains, et doit être confiée à des systèmes, dits de sécurité, basés sur des calculateurs qui, en raison même de la nature des tâches qui leur sont assignées, sont généralement tolérants aux fautes. Bien que les systèmes de sécurité aient donné lieu, d'un point de vue général, à de nombreuses publications [par exemple : LIE 76 - TAY 80], peu de communications publiées traitent de l'application de la tolérance aux fautes aux systèmes de sécurité [FRE 75 - MEW 79]. Ce mémoire a précisément pour but l'étude de systèmes de sécurité réalisés à partir de calculateurs.

Ce mémoire se compose de cinq chapitres regroupés en deux grandes parties :

- étude générale des systèmes de sécurité dans les deux premiers chapitres,
- étude d'un système de sécurité particulier : la commande des postes très haute tension (T.H.T.) du réseau 400/225 kV d'E.D.F., dans les trois autres chapitres.

Le premier chapitre est consacré à l'énoncé des fonctions d'un système de sécurité et à la définition de leurs différents niveaux de sûreté de fonctionnement.

Le second chapitre concerne l'étude détaillée de deux grandes catégories de système de sécurité : systèmes simplex non tolérants aux fautes, et systèmes tolérants aux fautes (duplex et vote majoritaire).

Le troisième chapitre a pour but de :

- situer l'étude que nous avons menée pour "Electricité de France" sur les postes à très haute tension,
- décrire le fonctionnement d'un poste,
- caractériser le poste sur le plan de la sûreté de fonctionnement.

Dans le quatrième chapitre, nous établissons les modèles représentatifs de la structure basse tension du poste, basés sur le système actuellement existant (modèles relatifs aux niveaux de sûreté définis dans le chapitre 3) et nous effectuons une étude de sensibilité des différents paramètres intervenant dans le comportement du poste.

Le cinquième chapitre nous permet de compléter le modèle obtenu dans le quatrième chapitre en incorporant deux points supplémentaires : détection de fautes et échanges d'information.

PREMIERE PARTIE

ÉTUDE GÉNÉRALE DES SYSTÈMES DE SÉCURITÉ

-

Le but de cette partie est l'étude des systèmes de sécurité assurant la protection de certains processus vis-à-vis d'incidents. Ces incidents peuvent être de cause interne ou externe et leur non élimination peut entraîner,du fait de la propagation de leurs effets, des conséquences catastrophiques pour le processus et son environnement.

Dans un premier chapitre, nous définirons, après une étude préliminaire, les différents niveaux de sûreté de fonctionnement associés aux systèmes de sécurité et nous établirons les graphes de transition correspondants.

Le second chapitre est consacré à l'évaluation de la sûreté de fonctionnement des systèmes de sécurité.

1. NIVEAUX DE SURETE DE FONCTIONNEMENT

Le but de ce chapitre est de déterminer les différentes grandeurs de la sûreté de fonctionnement des systèmes de sécurité.

Dans une première étape, nous allons d'abord nous intéresser aux principales raisons qui nous amènent à associer à certains types de processus des dispositifs de protection, qui sont en général constitués d'un, ou de plusieurs opérateurs humains, et d'un système de sécurité (calculateur) ; ensuite, nous définirons le rôle de l'opérateur et la fonction que doit remplir le système de sécurité.

Dans une seconde étape, nous commencerons par définir qualitativement les grandeurs de sûreté de fonctionnement ; ensuite, nous établirons le graphe de transition d'un tel système, ce qui nous permettra de définir quantitativement les grandeurs définies antérieurement, et de donner le graphe de transition relatif à chacune d'elles.

1.1. Pourquoi une protection ?

La complexité toujours croissante des ensembles industriels rend leur contrôle par des opérateurs humains de plus en plus difficile, voire impossible. Dans certains cas, cette croissance s'est accompagnée de l'utilisation de substances potentiellement dangereuses ce qui a augmenté le risque encouru en cas de mauvais fonctionnement. Simultanément, la technologie a fait de grands progrès et des méthodes scientifiques ont été adoptées pour le contrôle du risque.

Les conséquences d'une catastrophe peuvent être de nature très variée :

- sur le plan humain : risque de vies humaines et à long terme ceci peut entraîner des problèmes génétiques ou des maladies latentes,
- sur le plan économique : détérioration des installations, baisse importante dans la production moyenne entraînée par l'arrêt de la production pour réparation des dégâts,
- sur le plan écologique : détérioration du site.

L'importance des dégâts entraînés par le mauvais fonctionnement d'un processus potentiellement dangereux nous amène à le munir d'une protection très puissante contre les anomalies pouvant s'y produire.

Cette protection doit par exemple :

- empêcher le rayonnement radioactif dans une centrale nucléaire suite à un accident dans le réacteur [PED 78],
- éviter une coupure de courant généralisée et prolongée par suite d'un court-circuit en un point du réseau électrique [EDF 74],
- éviter la formation et la dispersion d'un gaz nocif lors de la fabrication d'un produit chimique, ou même lors d'une réaction nucléaire (vaporisation de sodium dans un réacteur à neutrons rapides refroidi au sodium) [SYN 75].

Avant de définir le rôle de la protection, il est essentiel de citer les principales catactéristiques des processus étudiés ainsi que celles des incidents qui doivent être pris en compte.

La caractéristique principale de ce type de processus est la propagation des effets d'un incident, à l'intérieur et à l'extérieur du processus ; au fur et à mesure, qu'il se propage, il prend de l'ampleur et ses conséquences deviennent de plus en plus graves (un court-circuit sur une ligne du réseau électrique non isolée à temps, se transforme en un court-circuit au niveau du poste et peut même atteindre les postes voisins si on n'a pu déconnecter ce dernier à temps).

Si on veut éviter l'aggravation ou plutôt minimiser les effets et les conséquences d'un incident, il faut empêcher sa propagation en le confinant : c'est le rôle de la protection.

La gravité d'un incident est relative à chaque processus ; elle est fonction de l'étendue des dégradations infligées au processus, de l'ampleur des actions nécessaires au retour à l'état de fonctionnement normal, des dommages causés au personnel exploitant, de la perte de production due à l'arrêt...

Dans certains cas, la protection peut-être assurée uniquement par un ou plusieurs opérateurs ; dans la plupart des cas, il est essentiel, vu la complexité des phénomènes mis en jeu et la rapidité exigée, d'avoir auprès de l'opérateur un système de calcul ; ce système sera appelé système de sécurité.

En fait la protection surveille et le processus et son système de commande. La distinction entre le système de commande et le système de sécurité est essentiellement fonctionnelle et ne préjuge en rien de la réalisation qui sera retenue :

- les deux fonctions peuvent être effectivement réalisées par des calculateurs différents (c'est le cas pour une centrale nucléaire ou une raffinerie de pétrole),
- les deux fonctions peuvent être réalisées par le même calculateur (dans certaines industries chimiques par exemple),
- la fonction de commande peut être inexistante.

Dans toute la suite de ce mémoire :

- le processus et le système de commande seront appelés système surveillé,
- le terme incident sera exclusivement réservé aux anomalies affectant le système surveillé.

La figure 1.1. donne les liens entre la protection et le système surveillé.

1.2. *Rôle de l'opérateur*

L'opérateur dispose :

- de tout ou partie des informations en provenance des capteurs connectés au système de sécurité,
- des informations en provenance du système de sécurité et concernant l'état du système surveillé : absence d'incident, présence et nature d'un incident,...
- des informations concernant le système de sécurité : bon état de fonctionnement, en défaillance, nature de la défaillance,...

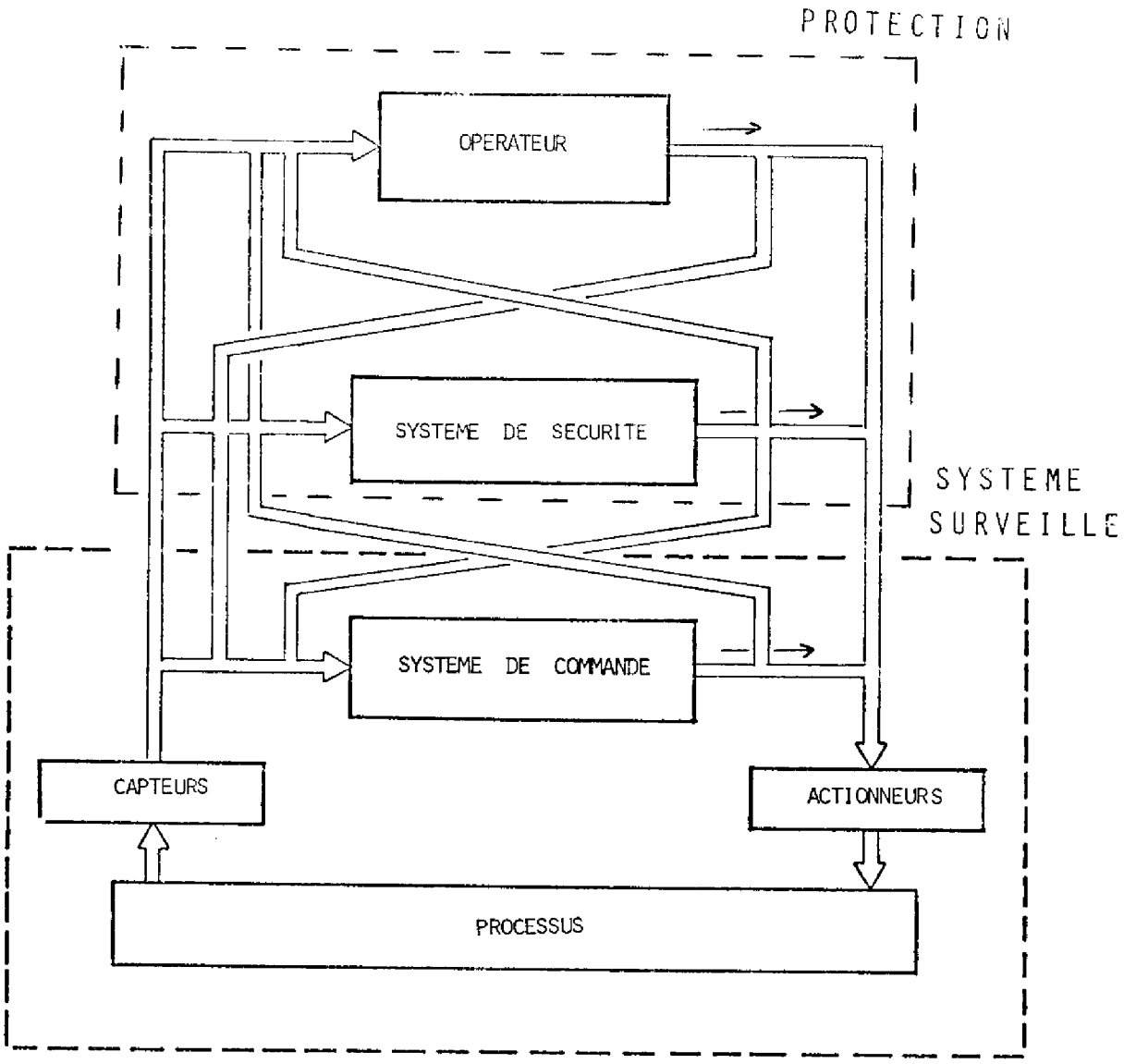


FIGURE 1.1. Liens entre la protection et le système surveillé

Il peut, à tout instant, contrôler le système de sécurité, le système de commande et intervenir au niveau du processus.

En cas de défaillance du système de sécurité, il a la possibilité d'arrêter partiellement ou totalement le processus ; si un incident survient avant qu'il n'ait eu le temps d'arrêter le processus, il peut essayer de l'éliminer manuellement.

Quelles que soient les conditions, la prise de décision finale est confiée à l'opérateur.

L'opérateur a également la possibilité d'arrêter le processus pour des raisons d'exploitation. Nous ne tiendrons pas compte de ces arrêts dans la suite de notre étude, dans la mesure où ils font partie de l'exploitation du processus alors que nous nous intéressons à la protection par rapport aux incidents.

1.3. Fonctions du système de sécurité

Le système de sécurité doit :

F1) En présence d'incident :

.détecter l'incident,

.signaler à l'opérateur la présence, et si possible la nature de l'incident,

.déclencher des actions de confinement de l'incident.

Selon le cas, ces actions peuvent être :

- des actions correctives permettant le retour du système surveillé dans l'état de fonctionnement normal,
- des actions d'arrêt partiel ou total du système surveillé.

F2) En l'absence d'incident :

.ne pas avoir d'action sur le système surveillé,

.ne pas entraîner l'arrêt de ce dernier.

1.3.1. Détection d'incidents

Le système de sécurité reçoit des informations du système de commande et dispose de capteurs placés à différents endroits du processus surveillé qui prélèvent de façon continue ou discontinue les paramètres caractéristiques du processus. Ces paramètres peuvent, soit représenter des grandeurs physiques dangereuses en elles-mêmes (toxicité), soit révéler par leur évolution, l'existence d'une anomalie.

Les valeurs de ces paramètres (valeurs numériques ou analogiques) constituent les données présentes à l'entrée du système de sécurité ; leur période d'arrivée, bien que liée à l'inertie du processus, est en général faible : de l'ordre de quelques millisecondes. La sortie du système de sécurité vers le processus est un signal tout ou rien, dont la période est beaucoup plus grande : période moyenne de l'ordre de quelques mois. La fréquence des sorties est en fait égale à la fréquence d'occurrence d'un incident dans le système surveillé. Ainsi, certaines parties du système de sécurité peuvent ne pas être activées pendant une longue période : nous dirons alors que le système de sécurité est un système dormant.

1.3.2. Actions du système de sécurité sur le système surveillé

Ces actions dépendent étroitement de la nature de l'incident c'est-à-dire de ses causes et de ses effets.

Les principales causes d'un incident peuvent être classées en quatre grands groupes :

- mauvais fonctionnement des capteurs ou des actionneurs,
- anomalie dans le processus lui-même,
- défaillance du système de commande,
- panne dans le support de communication.

Dans tous les cas, la cause peut être :

- fugitive (panne fugitive du calculateur de commande, court-circuit transitoire sur une ligne du réseau électrique,...),
- permanente (rupture d'une canalisation dans une colonne de distillation, rupture d'une ligne du réseau électrique,...).

Quelle que soit la cause de l'incident, les effets sont en général permanents en l'absence de protection ; le rôle de cette dernière est de rendre ces effets transitoires ou de les confiner et d'arrêter le système surveillé.

La première phase du traitement de l'incident permet de classer les incidents en deux catégories :

- incidents transitoires : le système de sécurité effectue sur le système surveillé des actions destinées à le ramener dans le domaine de fonctionnement normal ; suivant la nature même de l'incident, ces actions peuvent réussir ou échouer,
- incidents permanents : le système de sécurité confine les effets de l'incident et arrête partiellement ou totalement le processus.

a) Traitement d'un incident transitoire

Ayant classé un incident dans cette catégorie, le système de sécurité essaie de remettre le système surveillé à l'intérieur du domaine de fonctionnement normal :

- si l'essai a réussi (le système surveillé est retourné à l'état de fonctionnement normal), l'incident est déclaré transitoire,
- si l'essai a échoué l'incident est déclaré permanent et doit être traité en tant qu'incident permanent.

b) Traitement d'un incident permanent - notions de confinement et de barrières

Si on n'arrive pas à faire disparaître complètement un incident ou si l'incident est classé en tant qu'incident permanent dès son apparition, il faut absolument empêcher sa propagation en le confinant dans une zone aussi réduite que possible. Ce confinement se fait à l'intérieur de certaines "frontières" appelées barrières :

- dans un réacteur nucléaire, ces barrières correspondent aux gaines entourant l'élément combustible, contenues dans l'enveloppe du circuit primaire, elle-même contenue dans l'enceinte de confinement,
- dans un poste à très haute tension ces barrières sont respectivement la ligne, la barre et le poste.

A chaque incident, suivant l'endroit de son apparition, sa vitesse de propagation et le temps de réponse de la protection, on fait correspondre la barrière la plus proche à l'intérieur de laquelle on peut le confiner : c'est la barrière adéquate de confinement. La dernière barrière de confinement correspond à la limite au-delà de laquelle tout incident a des conséquences catastrophiques.

Un incident peut-être :

- bien éliminé si on a réussi à le confiner à la barrière adéquate,
- éliminé en dégradé s'il y a franchissement d'une ou de plusieurs barrières au-delà de la barrière adéquate, sans franchir toutefois la dernière barrière de confinement,
- non éliminé : c'est le cas où la dernière barrière de confinement est dépassée.

Le délai alloué aux opérations d'élimination est fonction de l'inertie du processus.

1.4. *Définition qualitative des niveaux de sûreté de fonctionnement*

Des études en cours sur la modélisation ont montré l'intérêt de considérer plusieurs niveaux de sûreté de fonctionnement suivant les conséquences des différentes sources de fautes, et selon les tâches que le système a à effectuer. Parmi ces études, nous pouvons citer les travaux de MEYER sur le concept de "performabilité" [MEY 78] ainsi que les travaux de GAY sur les modèles de charge de travail (workload models) [GAY 79].

Pour définir les niveaux de sûreté de fonctionnement, il est nécessaire de définir les niveaux d'accomplissement des tâches ; ceci pourrait être fait en considérant soit les tâches effectuées par le système soit les classes des conséquences des différentes sources des fautes (ces deux approches sont duales).

En ce qui nous concerne, nous définissons deux niveaux d'accomplissement des tâches se rapportant aux fonctions F1 et F2 (cf. 1.2.) :

- Niveau 1 se rapportant à F1 uniquement : le système de sécurité est capable d'éliminer un incident.
- Niveau 2 se rapportant à F1 et F2 : le système de sécurité est capable d'éliminer un incident et n'a pas d'action indésirable sur le système surveillé en l'absence d'incident.

Ces deux niveaux peuvent être considérés comme deux niveaux extrêmes : éviter la catastrophe quelles que soient les conditions (niveau 1) ou tout est en bon état de fonctionnement (niveau 2).

Dans la première partie de ce mémoire, nous ne considérons pas l'élimination dégradée d'un incident : nous supposerons qu'un incident est soit bien éliminé, soit non éliminé.

Dans le but de définir quantitativement ces niveaux, nous allons étudier le comportement du système de sécurité.

1.5. *Comportement du système de sécurité*

Le comportement d'un tel système résulte de deux processus alternants :

- défaillance du système de sécurité et maintenance du système de sécurité; dans la suite du mémoire ce processus sera appelé processus de capacité,
- occurrence d'incident dans le système surveillé, traitement de l'incident par le système de sécurité ; ce processus sera appelé processus de sollicitation.

Dans un premier temps, nous considérons que ces deux processus sont indépendants.

1.5.1. *Processus de capacité*

En l'absence d'incident, nous supposons que le système de sécurité a un comportement "binaire" :

- il est capable d'accomplir toutes ses tâches : aucune faute ne s'est développée dans le système, ou, s'il est tolérant aux fautes, une faute a déjà eu lieu et a été couverte : dans ce dernier cas, la partie défaillante du système est en réparation ou en attente d'être réparée,
- il est incapable d'accomplir ses tâches : une faute a lieu et le système est non tolérant aux fautes ou, s'il l'est, toutes les ressources ont été épuisées.

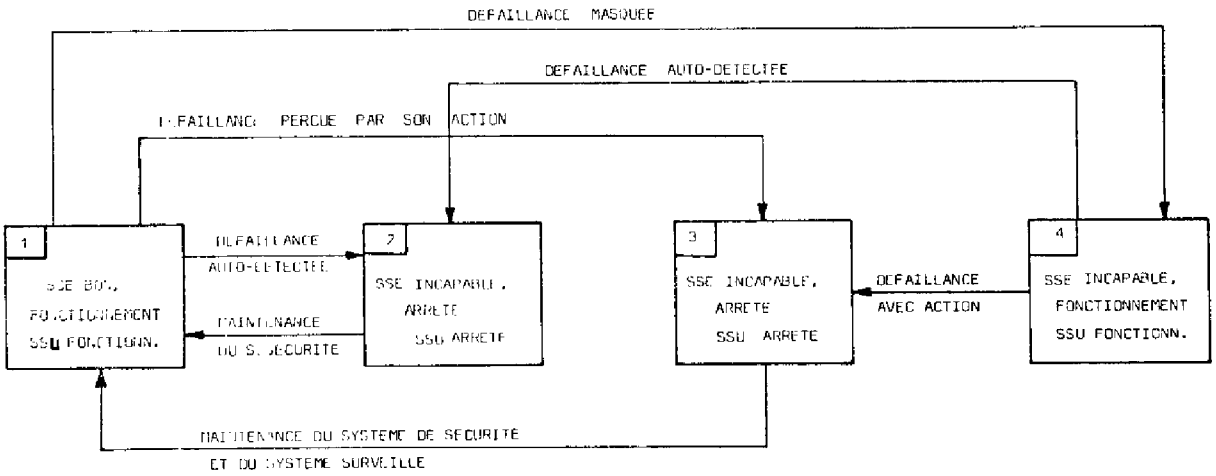
Quand le système de sécurité est incapable d'assurer ses tâches, trois situations sont possibles :

1) l'incapacité est auto-détectée : elle a été détectée par les mécanismes de détection implantés dans le système et aucune action incorrecte n'a eu lieu dans le système. Dans ce cas, le système surveillé est arrêté automatiquement par le système de sécurité, étant donné que ce dernier n'est plus en mesure d'assurer sa protection,
2) l'incapacité est perçue par son action sur le système surveillé. Dans ce cas, le système surveillé est arrêté par l'opérateur, pour les mêmes raisons que précédemment,

3) l'incapacité est masquée : ni auto-détectée ni perçue par son action ; dans ce cas, le système surveillé continue à fonctionner sans être protégé.

Le graphe de transition est donné par la figure 1.2. Les transitions à partir de l'état 4 vers les états 2 et 3 sont dues au fait que le système est dormant : quand le système a déjà une faute masquée, une ou plusieurs fautes peuvent se développer ce qui peut amener le système dans un état d'incapacité auto-détectée (état 2) ou perçue par son action (état 3) ou le laisser dans le même état 4.

Dans la suite du mémoire, les termes"défaillance", "faute" et "panne" seront exclusivement réservés aux anomalies survenant dans le système de sécurité.



SSE : système de sécurité ; SSU : système surveillé

FIGURE 1.2. Graphe de transition relatif au processus de capacité

1.5.2. *Processus de sollicitation*

On dit que le système de sécurité est sollicité lorsqu'un incident survient dans le système surveillé.

Quand le système de sécurité est en bon état de fonctionnement, il effectue, dès qu'un incident survient, un traitement pour déterminer si l'incident est à caractère transitoire ou permanent : soit R cet état. A la fin de cette phase de reconnaissance :

- le système est dans l'état T si l'incident est transitoire,
- le système est dans l'état P si l'incident est permanent.

Si les actions correctives dans l'état T réussissent, le système retourne dans l'état de bon fonctionnement en l'absence d'incident ; si elles échouent, le système va dans l'état P. A la fin de la phase de traitement d'un incident permanent (état P), le système surveillé est à l'arrêt pour maintenance. Le graphe de transition du traitement d'un incident est donné à la figure 1.3.

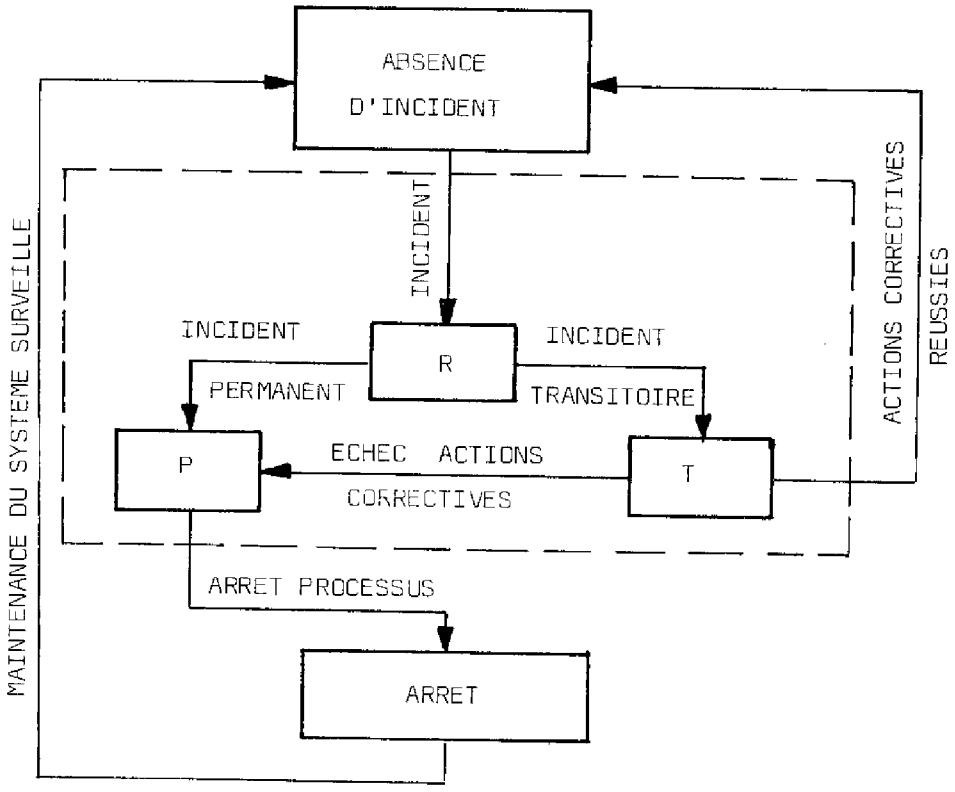


FIGURE 1.3. Graphe de transition du traitement d'un incident

Les états R, T et P peuvent être regroupés en un seul état : état de traitement d'un incident. Le graphe de transition résultant, relatif au processus de sollicitation est donné à la figure 1.4.

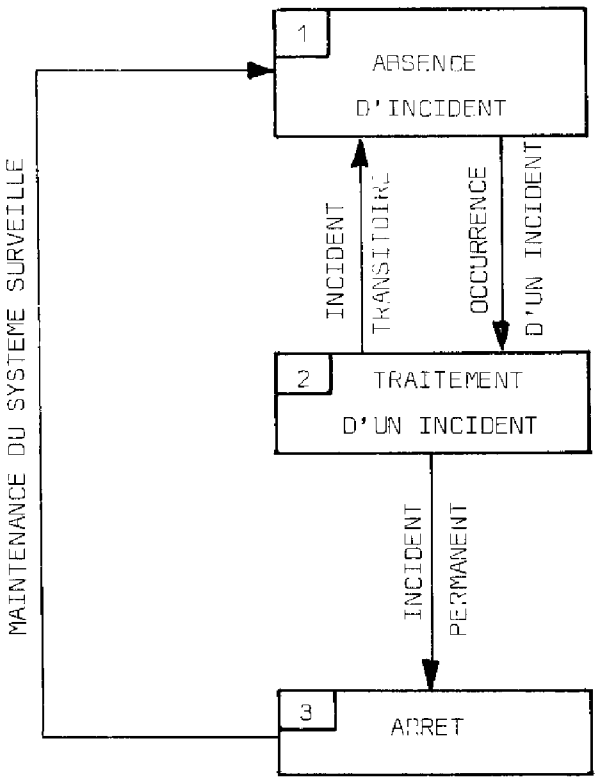
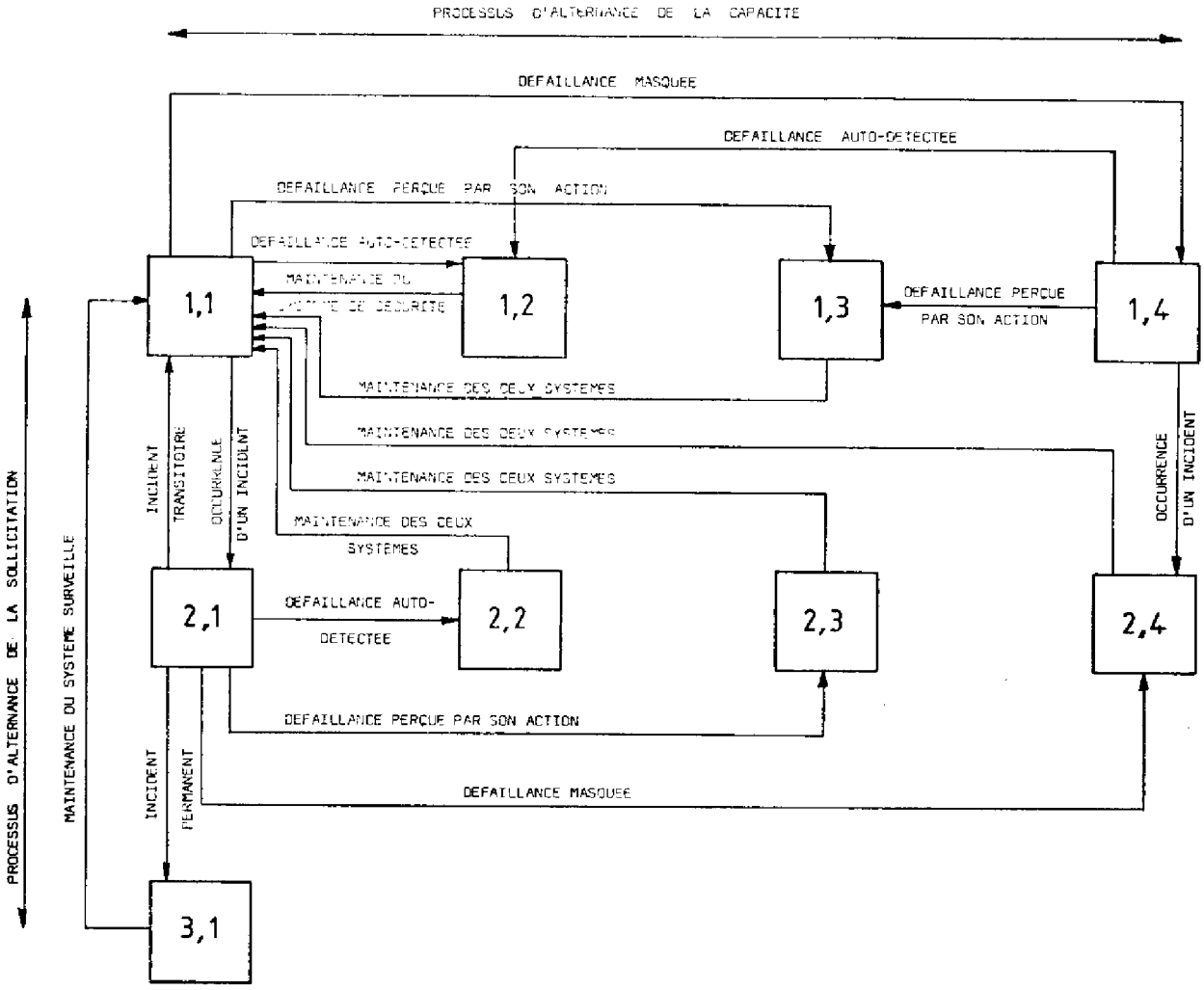


FIGURE 1.4. Graphe de transition relatif au processus de sollicitation

1.5.3. Graphe de transition du système de sécurité

Le graphe de transition complet du système de sécurité est obtenu par la combinaison des graphes des figures 1.2. et 1.4. en supposant que, durant l'arrêt du système surveillé, aucun incident et aucune défaillance ne peuvent avoir lieu (l'arrêt de l'un des deux systèmes entraîne l'arrêt de l'autre). Ce graphe est donné à la figure 1.5. Chaque état est représenté par un doublet (i,j) où i et j indiquent respectivement l'alternance de la sollicitation et de la capacité.



(1,1) Etat de bon fonctionnement

(1,2) Incapacité auto-détectée
(1,3) Incapacité perçue par son action
(1,4) Incapacité masquée
} en absence d'incident

(2,1) Traitement d'un incident

(3,1) Maintenance du système surveillé suite à un incident permanent

(2,2) Incident non éliminé
(2,3) Maintenance des deux systèmes
(2,4)

FIGURE 1.5. Graphe de transition du système de sécurité

L'état (2,2) est un état catastrophique, mais l'opérateur est prévenu de l'incapacité du système de sécurité et peut intervenir pour éliminer l'incident, alors que dans les états catastrophiques (2,3) et (2,4) l'opérateur n'est pas prévenu ; ces deux derniers états peuvent être regroupés en un seul : soit (2,3) cet état.

1.6. Définition quantitative et graphes des deux niveaux de sûreté de fonctionnement

Selon le niveau considéré, ces états sont classés comme états de succès ou de non succès.

NIVEAUX	ETATS DE SUCCES	ETATS DE NON SUCCES
Niveau 1	(1,1),(1,2),(1,3),(1,4),(2,1),(3,1)	(2,2),(2,3)
Niveau 2	(1,1),(2,1),(3,1)	(1,2),(1,3),(1,4),(2,2),(2,3)

La classification de l'état (1,4) nécessite quelques commentaires : cet état est non observable ce qui lui confère un caractère dangereux : si un incident survient, le système va dans un état catastrophique. Cependant, comme nous l'avons déjà mentionné, ces deux niveaux doivent être considérés comme des niveaux extrêmes ; c'est pour cela que nous l'avons classé comme état de succès pour le premier niveau et de non succès pour le second.

Les états (1,2) et (1,3) appartiennent à la même classe dans les deux niveaux. Si nous supposons que, dans ces états, le système de sécurité ne peut, en l'absence d'incident, avoir d'action entraînant des conséquences catastrophiques et que les temps de maintenance à partir de ces états sont du même ordre de grandeur, nous pourrons les regrouper en un seul : état de défaillance déclarée ou de maintenance en l'absence d'incident. L'hypothèse de temps de maintenance du même ordre de grandeur se justifie par le fait que la maintenance du système surveillé est indépendante de la maintenance du système de sécurité et inversement ; par conséquent, ces deux actions de maintenance peuvent être effectuées en parallèle par des équipes différentes.

Le problème qui se pose alors est le suivant : quelles mesures faut-il prendre pour chaque niveau ? C'est-à-dire quelles sont les transitions dont il faut tenir compte ? Pour répondre à cette question, il est possible de partitionner les états du système en trois sous-ensembles :

- E_I : états de succès pour les deux niveaux : $(1,1) \cup (2,1) \cup (3,1)$,
- E_{II} : états de succès pour le niveau 1 et de non succès pour le niveau 2 : $(1,2) \cup (1,3) \cup (1,4)$,
- E_{III} : états de non succès pour les deux niveaux ou états catastrophiques : $(2,2) \cup (2,3)$.

Cette partition permet de remplacer le graphe de la figure 1.5. par le graphe de la figure 1.6.

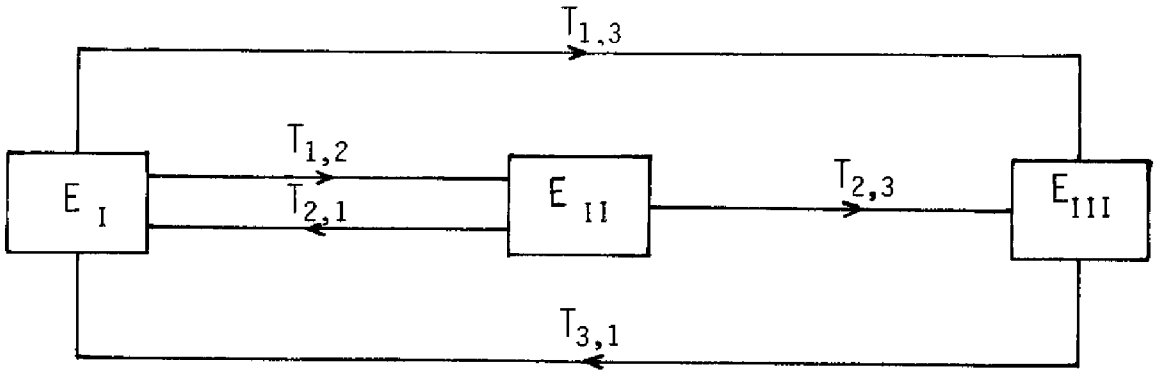


FIGURE 1.6.

Tenir compte de la maintenance à partir de E_{III} (transition $T_{3,1}$) revient à :

- considérer la disponibilité du système, c'est-à-dire la proportion de temps moyen passé dans les états non catastrophiques ; or, pour un système de sécurité nous sommes intéressé par la probabilité de ne pas aller dans les états catastrophiques E_{III},
- supposer que le système surveillé peut être restauré à partir de E_{III} ce qui n'est pas toujours possible.

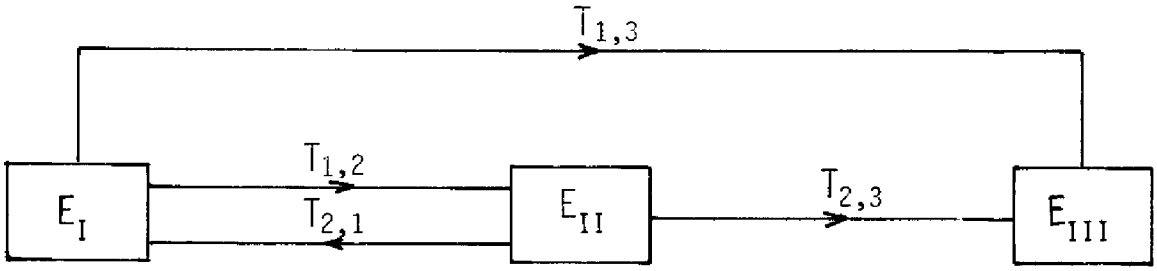
Nous ne pourrons donc pas tenir compte de $T_{3,1}$.

Pour le niveau 1, la mesure qui nous intéresse est donc du type fiabilité : les états de non succès sont absorbants : soit $D_1(t)$ cette mesure.

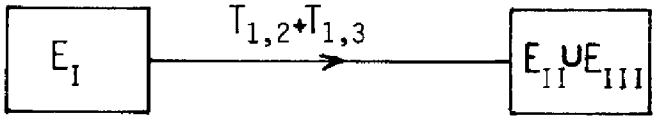
Pour le niveau 2, deux mesures sont possibles : l'une tient compte de la maintenance à partir de E_{II} (transition $T_{2,1}$) l'autre n'en tient pas compte.

Ces deux mesures seront respectivement notées $D_{21}(t)$ et $D_{22}(t)$.

Le graphe de transition de $D_{21}(t)$ est identique à celui de $D_1(t)$, il est représenté par la figure 1.7.a. ; le graphe de transition de $D_{22}(t)$ est représenté par la figure 1.7.b.



.a. Graphe de transition pour $D_1(t)$ et $D_{21}(t)$



.b. Graphe de transition pour $D_{22}(t)$

FIGURE 1.7. Graphes de transition relatifs aux deux niveaux pour les différentes mesures considérées.

Expressions analytiques :

Si $P_i(t)$ est la probabilité que le système soit dans l'un des états du sous-ensemble E_i à l'instant t, on a :

$D_1(t) = P_I(t) + P_{II}(t)$, évalués à partir du graphe de la figure 1.7.a.

$D_{21}(t) = P_I(t)$, évalué à partir du graphe de la figure 1.7.a.

$D_{22}(t) = P_I(t)$, évalué à partir du graphe de la figure 1.7.b.

Les graphes de transitions déduits du graphe de la figure 1.5. sont donnés figure 1.8. Sur cette figure, les états (1,2) et (1,3) ont été regroupés ainsi que tous les états absorbants.

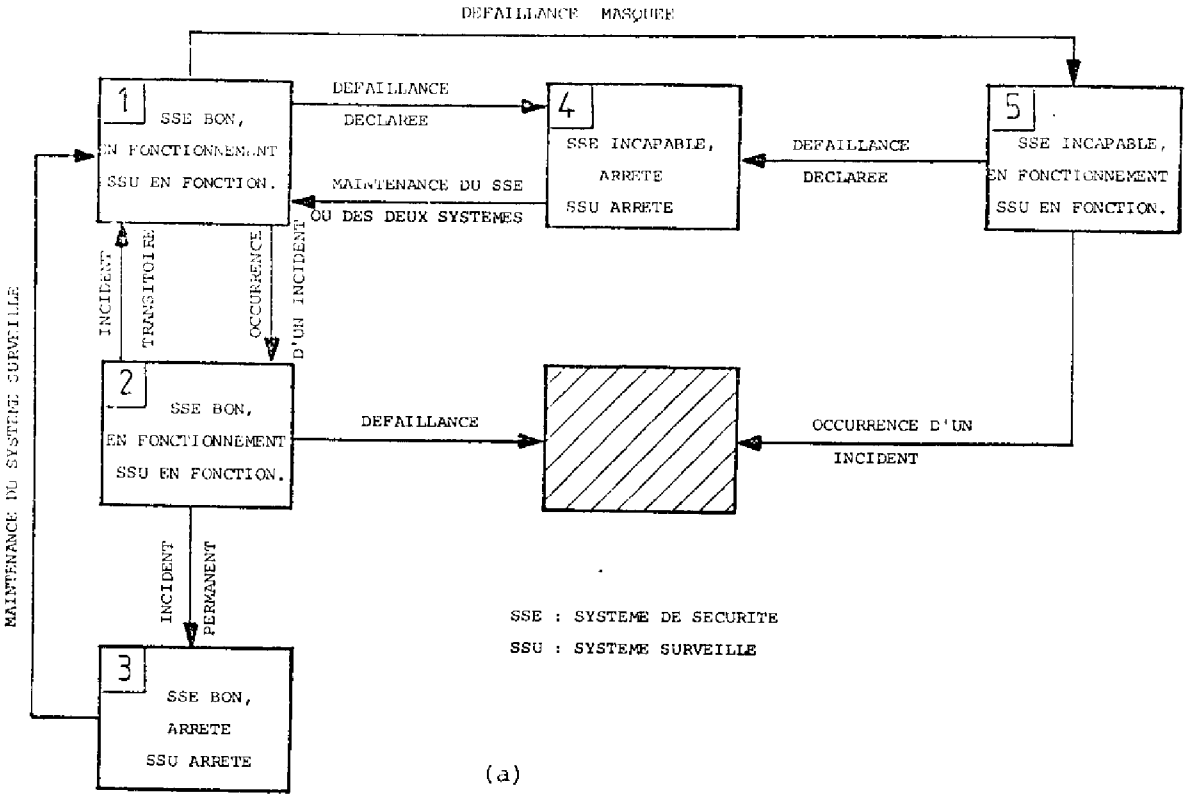
Les états sont renumérotés avec un seul indice dans un but de simplification.

Les expressions des différentes mesures de la sûreté de fonctionnement sont données par :

$D_1(t) = \sum_{i=1}^{5} P_i(t)$, les P_i étant évalués à partir du graphe de la figure 1.8.a.

$D_{21}(t) = \sum_{i=1}^{3} P_i(t)$, les P_i étant évalués à partir du graphe de la figure 1.8.a.

$D_{22}(t) = \sum_{i=1}^{3} P_i(t)$, les P_i étant évalués à partir du graphe de la figure 1.8.b.



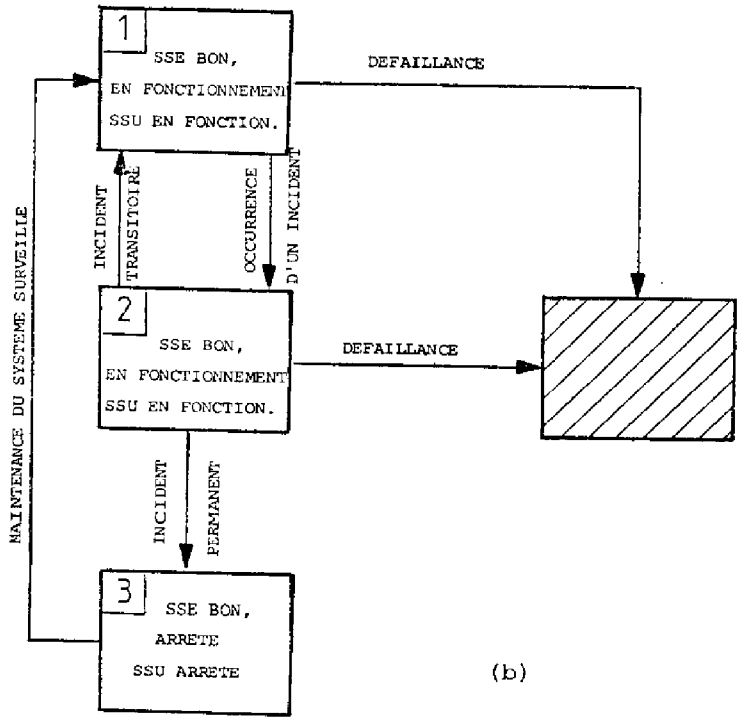


FIGURE 1.8. Graphes de transition des mesures de sûreté de fonctionnement

2. EVALUATION DE LA SURETE DES SYSTEMES DE SECURITE

Le but de ce chapitre est l'évaluation comparative de la sûreté de fonctionnement de deux catégories de systèmes de sécurité : systèmes simplex non tolérants aux fautes et systèmes tolérants aux fautes.

Nous procéderons en quatre étapes :

- exposé de la méthode d'évaluation suivie,
- étude du processus de manifestation de fautes,
- modélisation et évaluation de la sûreté de fonctionnement d'un système simplex non tolérant aux fautes,
- modélisation et évaluation de deux catégories de systèmes tolérants aux fautes : système duplex et système à vote majoritaire, comparaison des performances des divers systèmes étudiés.

2.1. *Méthode d'évaluation suivie*

Nous supposerons que toutes les variables aléatoires intervenant dans le comportement du système sont exponentiellement distribuées et possèdent donc des taux de hasard constants. Le degré de validité de cette hypothèse varie selon les processus considérés :

- processus de manifestation des fautes : pour les fautes dues à une panne physique cette hypothèse est parfaitement confirmée par l'expérience, pour les fautes dues à des erreurs de conception cette hypothèse est une bonne approximation dans certaines conditions qui seront précisées lors de l'étude du processus de manifestation de fautes (cf. 2.2.),
- processus d'apparition d'incident : l'occurrence d'un incident est accidentelle et on peut considérer en première approximation que la distribution est exponentielle,
- processus de maintenance : dans ce cas, l'hypothèse de la distribution exponentielle ne constitue en première approche qu'une approximation grossière ; cependant, des études antérieures [LAP 75 , COS 78] ont montré que cette hypothèse est valable lorsque la valeur moyenne des

temps de maintenance est petite devant celles des autres variables aléatoires mises en jeu, ce qui est le cas pour le processus de maintenance.

L'hypothèse de taux de hasard constants permet l'évaluation des mesures de sûreté de fonctionnement précédemment définies par les processus markoviens ; ces mesures s'expriment par la relation :

$$D(t) = \mathbb{P}(o).\exp(\mathbb{A}t).\mathbb{1} \qquad (1)$$

où :

- $\mathbb{A}$ est la matrice de transition pour la mesure considérée (matrice formée par les taux de transition entre les m états non absorbants du graphe associé à cette mesure),
- $\mathbb{P}(o)$: vecteur des probabilités initiales,
- $\mathbb{1}$: vecteur colonne de sommation, dont toutes les composantes sont égales à 1.

Le temps moyen avant absorption, MTA, qui est le temps moyen passé dans les états non absorbants et qui joue le même rôle pour D(t) que le MTFF pour la fiabilité, est donné par la relation :

$$MTA = -\mathbb{P}(o).\mathbb{A}^{-1}.\mathbb{1} \qquad (2)$$

Le MTA peut être considéré comme étant la source des temps conditionnels $\theta_i, i=1,2,\ldots,m$ qui représentent les temps moyens passés dans les états non absorbants. Les θ_i sont solution du système :

$$\Theta.\mathbb{A} = -\mathbb{P}(o) \quad \text{avec} \quad \Theta = [\theta_1, \theta_2, \ldots, \theta_m] \qquad (3)$$

Il n'est pas toujours possible de calculer l'expression analytique de D(t) et nous ferons une large utilisation du programme d'évaluation numérique de la sûreté conçu et développé dans l'équipe A.S.F. : le programme SURF [COS 79]. La structure de ce programme est décrite à la figure 2.1., les figures 2.2. et 2.3. détaillent l'organisation des différents niveaux du programme.

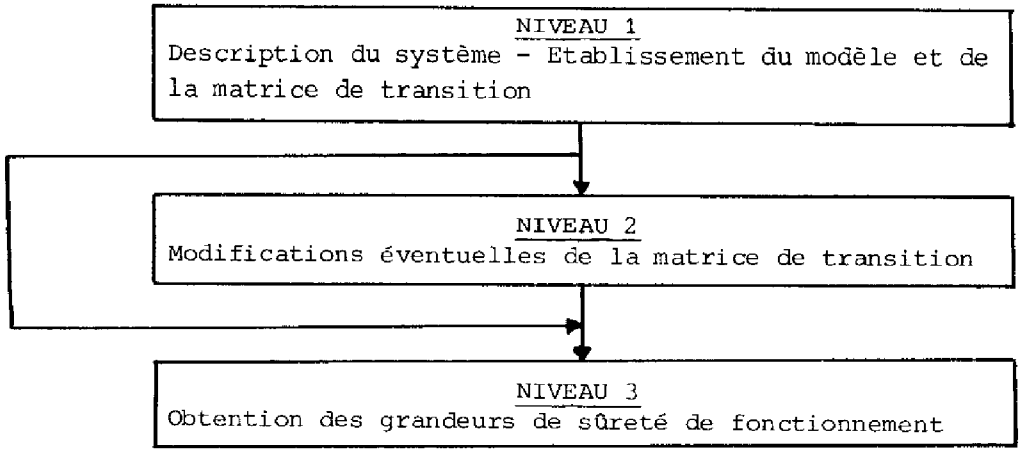


FIGURE 2.1. Structure du programme SURF

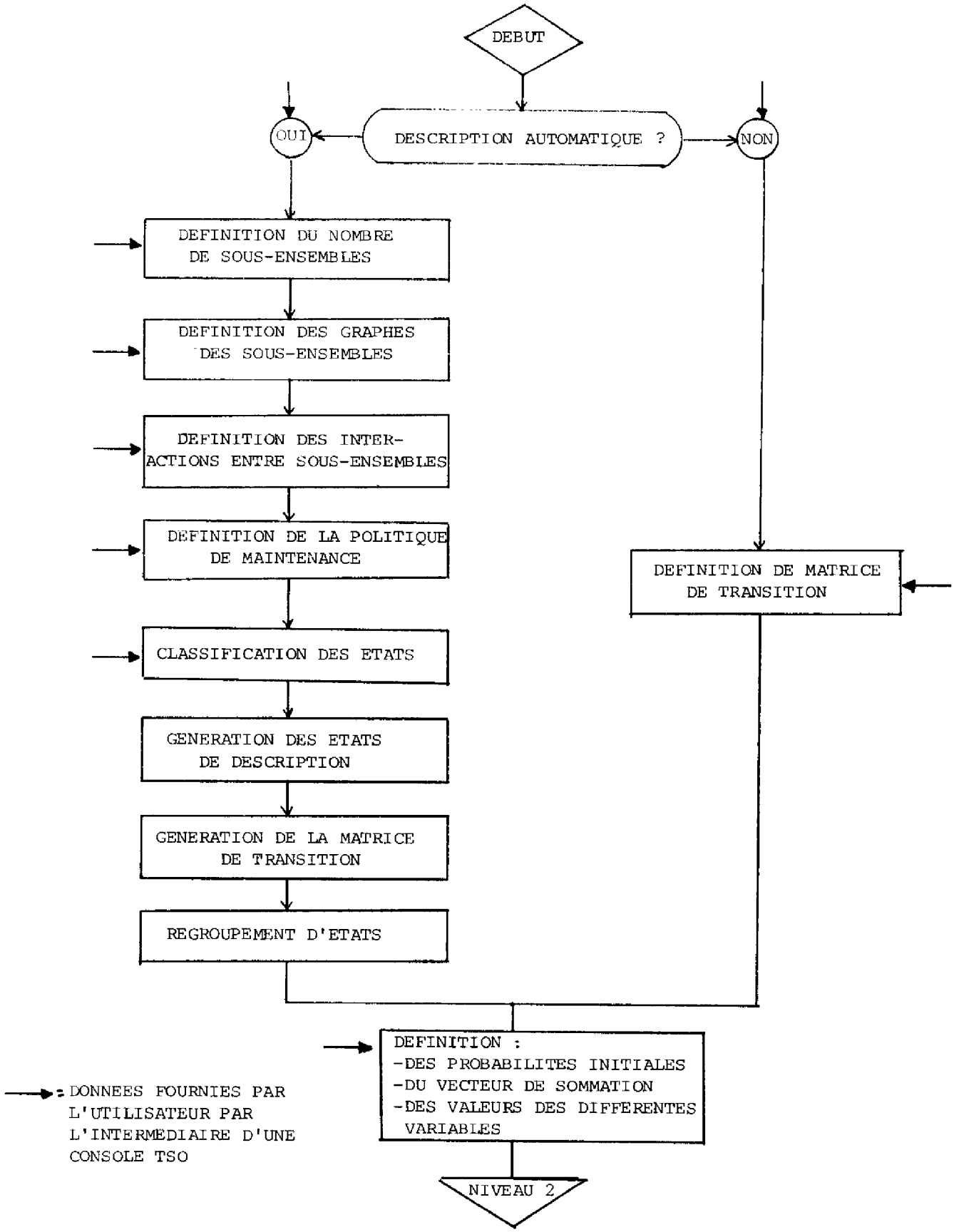


FIGURE 2.2. Description détaillée du niveau 1 du programme SURF

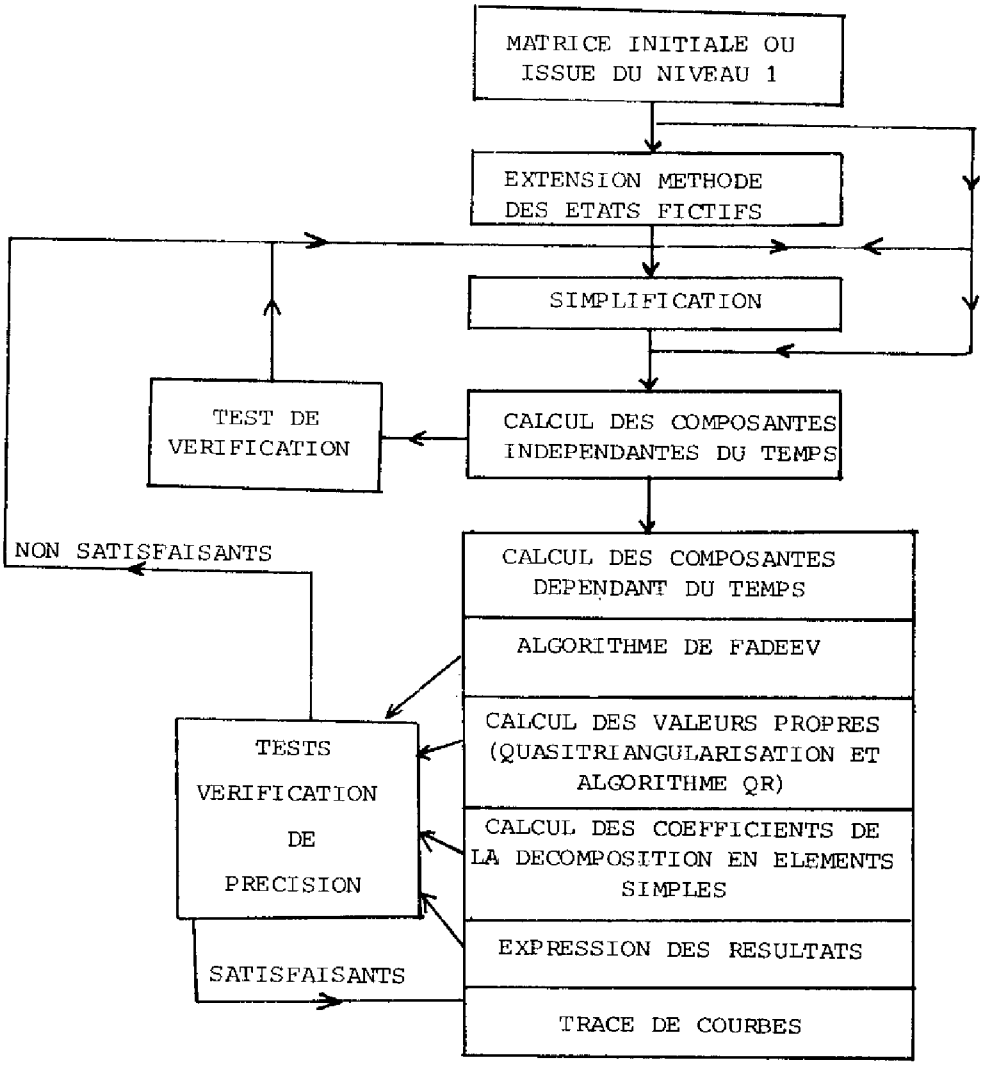


FIGURE 2.3. Description détaillée des niveaux 2 et 3 du programme SURF

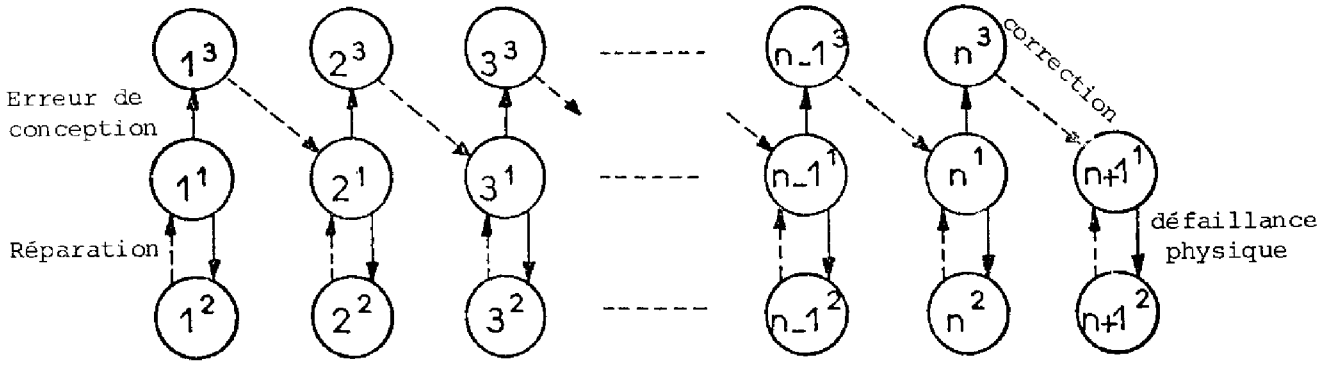
2.2. *Processus de manifestation de fautes*

Ce paragraphe est consacré à l'étude du processus de manifestation de fautes dans un système soumis au processus de fautes physiques, dans lequel il y a encore des erreurs de conception et qui peut être placé dans un environnement très perturbé.

Nous allons d'abord étudier l'influence de la prise en compte des erreurs de conception puis l'influence d'un environnement très perturbé.

2.2.1. Prise en compte des erreurs de conception

Considérons un système soumis au processus de fautes physiques et dans lequel il y a des erreurs de conception ; nous supposerons que ce système est opérationnel, c'est-à-dire qu'il a déjà subi tous les tests nécessaires avant son utilisation sur le site. Le graphe représentatif du comportement d'un tel système est donné à la figure 2.4.



état (i) : il y a eu (i-1) corrections du logiciel suite à des défaillances dues à une erreur de conception.

- taux d'apparition d'une défaillance physique : λ
- taux de réparation du système après une défaillance physique : μ
- taux d'apparition de la ième défaillance due à une erreur de conception : λ_i
- taux de correction du logiciel suite à la ième défaillance due à une erreur de conception : μ_i.

FIGURE 2.4. Graphe représentatif d'un système assujetti à des défaillances physiques et à des erreurs de conception

Des études antérieures [LAN 77] ont montré que la courbe d'indisponibilité de ce système présente un dépassement important par rapport à sa valeur asymptotique (courbe (2A) de la figure 2.5.b.).

Ces études ont montré que le maximum d'indisponibilité est fonction du taux d'occurrence de la première défaillance due à une erreur de conception (λ_1), l'influence des autres λ_i se ramenant à maintenir la

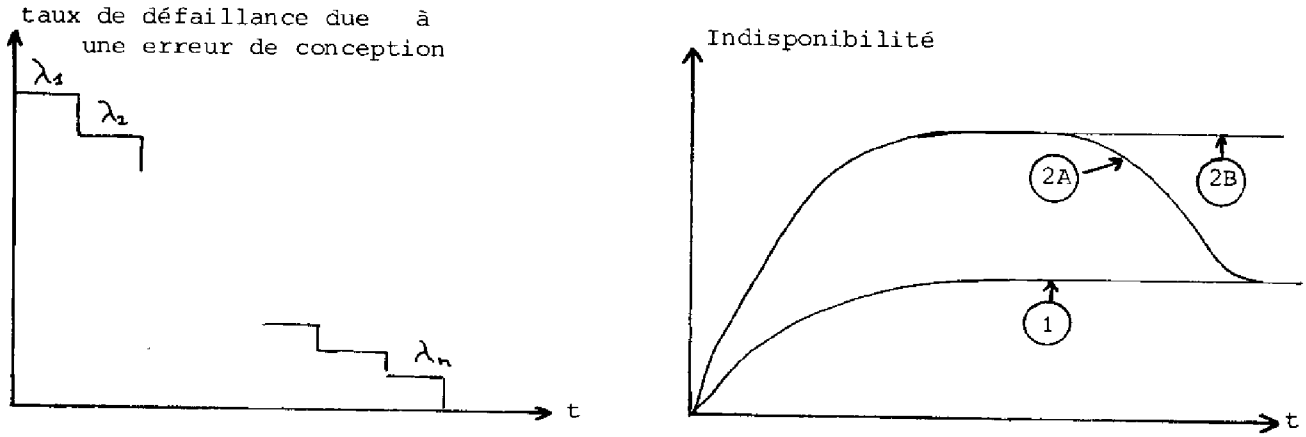
courbe d'indisponibilité plus ou moins longtemps au niveau de ce maximum, sous réserve que les hypothèses suivantes soient vérifiées :

- l'intervalle entre fautes physiques est grand devant les temps moyens de réparation,
- les temps moyens de correction du logiciel et de réparation du matériel sont à peu près identiques quelle que soit l'origine de la faute ($\mu_i \sim \mu$),
- la correction d'une erreur de logiciel n'introduit pas de sources de défaillance plus importantesque celles corrigées : taux de fautes dues à des erreurs de conception décroissant (figure 2.5.a.).

Si nous faisons tendre n vers l'infini et tous les λ_i vers λ_1 le graphe obtenu est représenté à la figure 2.6.

Si nous supposons $\mu_1 = \mu$ le graphe se transforme en un graphe à deux états dont le taux de défaillance est ($\lambda_1 + \lambda$) et le taux de réparation est μ. La courbe d'indisponibilité est maintenue au niveau de son maximum : courbe (2B) de la figure 2.5.b.

Par conséquent, nous adopterons les mêmes hypothèses pour le taux de fautes dues à des erreurs de conception que pour le taux de fautes physiques : taux constant.



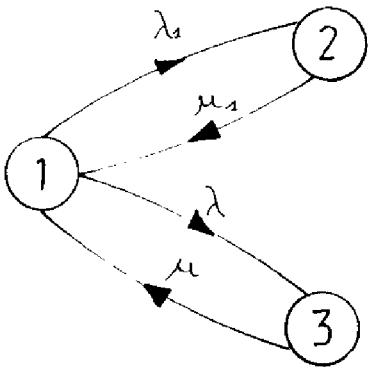
(1) structure soumise à des fautes physiques uniquement

(2) structure soumise à des fautes physiques et à des erreurs de conception :

A : taux de défaillance due à des erreurs de conception décroissant,

B : taux de défaillance due à des erreurs de conception constant.

FIGURE 2.5. Taux de défaillance et indisponibilité d'une structure soumise à des fautes matérielles et à des erreurs de conception



(1) : état de fonctionnement

(2) : état de correction d'une faute due à une erreur de conception

(3) : état de réparation après une faute due à une panne physique

FIGURE 2.6. Graphe de disponibilité approché

2.2.2. *Facteur d'environnement*

Durant une sollicitation, les conditions d'environnement peuvent devenir très sévères pour certains systèmes (parasites à haute énergie, potentiel de terre très élevé, vibrations,...); le taux de fautes physiques d'un calculateur peut donc augmenter de façon significative.

Certaines parties du programme du système de sécurité ne sont exécutées que lors d'une sollicitation (celles qui sont relatives au traitement de l'incident) ainsi le taux de manifestation de fautes dues à des erreurs de conception peut augmenter lors d'une sollicitation.

Nous supposerons que globalement le taux de fautes (dues à une défaillance physique ou à des erreurs de conception) est multiplié par un facteur K qui traduit le facteur d'environnement.

2.3. *Système non tolérant aux fautes (simplex)*

La modélisation d'un système non tolérant aux fautes permet d'étudier l'influence des différents paramètres agissant sur le système et d'évaluer l'amélioration des mesures de sûreté de fonctionnement amenée par l'introduction des techniques de tolérance aux fautes.

La modélisation ne peut être effectuée que si l'on connaît les techniques de détection de fautes utilisées et les paramètres associés aux processus agissant sur le système.

2.3.1. *Détection de fautes*

Les mécanismes de détection de fautes sont imposés par les deux principales propriétés du système de sécurité : pas d'action amenant le système surveillé dans un état catastrophique (sûreté en présence de fautes) et "dormance".

Pour que la première propriété soit réalisée, il est nécessaire que le système soit muni d'une détection continue. Cette technique repose sur l'incorporation dans les modules, strictement destinés à l'accomplissement des fonctions du système, de mécanismes de détection.

La seconde propriété entraîne que certaines parties du système ne sont activées qu'en présence d'un incident. Dans ce cas, la latence de la faute peut être très grande [SHE 75], et la faute n'est détectée qu'au moment crucial entraînant ainsi le système surveillé dans un état catastrophique ; il est donc nécessaire d'implanter des techniques de détection périodique. Leur principe réside dans l'exécution de programmes de test à intervalles réguliers afin de détecter si une faute est survenue depuis la dernière exécution. L'exécution des programmes de test ne doit pas empêcher le système de sécurité de "servir" les sollicitations.

Le système de sécurité doit donc posséder les deux types de détection : continue et périodique.

2.3.2. *Définitions et ordre de grandeur des variables et paramètres associés aux processus*

Nous allons associer à chaque processus agissant sur le système de sécurité une ou plusieurs variables aléatoires ainsi que certains paramètres.

Nous allons dans les sous-paragraphes suivants, nous intéresser successivement au processus de capacité et au processus de sollicitation pour conclure sur les ordres de grandeur des différents paramètres.

2.3.2.1. *Processus de capacité*

Nous considérons ici toutes les défaillances consécutives à une faute physique ou à une erreur de conception.

Nous noterons λ le taux de faute d'un calculateur en l'absence de sollicitation, taux de faute qui correspond à un calculateur de référence sans détection. L'augmentation de ce taux entraînée par les techniques de détection sera notée b ; le taux de faute d'un calculateur muni de sa propre détection de faute est donc $\lambda' = b\,\lambda$.

Nous avons vu qu'une faute peut se manifester de trois manières :

- faute détectée par les dispositifs de détection associés au système de sécurité ; soit P_D l'efficacité de ce type de détection définie par : $P_D = \mathcal{P}\{\text{une faute soit détectée/une faute a lieu}\}$,
- faute perçue par son action intempestive sur le système surveillé ; nous noterons $(1-q_o)$ la probabilité qu'une faute ait une action intempestive,
- faute masquée, c'est-à-dire non perçue par les dispositifs de détection et sans action intempestive ; la probabilité qu'une faute soit masquée sera notée $q = q_o\ (1-P_D)$.

Le système étant en défaillance déclarée (détectée ou perçue par son action), sa maintenance ne fait intervenir que le processus de réparation. Le temps de réparation correspond à l'intervalle de temps entre la mise hors service des deux systèmes (système de sécurité et système surveillé) et leur remise en marche, ce temps moyen sera noté $1/\mu$.

L'expérience montre que la réparation n'est pas toujours parfaite et que l'opérateur peut introduire de nouvelles fautes dans le système lors de la réparation. Des études antérieures [LAP 75 - APO 77] ont montré l'influence d'une réparation imparfaite. Nous introduisons un facteur d'efficacité de réparation P_m défini par :

$$P_m = \mathcal{P}\{\text{une faute soit bien réparée/une faute a été déclarée}\}$$

2.3.2.2. Processus de sollicitation

Comme nous l'avons précédemment indiqué, la fréquence de sollicitation n'est pas en général très élevée. Soient γ ce taux de sollicitation, $1/\xi$ le temps moyen de traitement d'une sollicitation et ρ la probabilité qu'un incident soit transitoire (ne nécessitant pas l'arrêt du processus). Le temps d'arrêt moyen engendré par un incident permanent sera noté $1/\eta$.

2.3.2.3. Ordres de grandeur des différents paramètres

Pour étudier le comportement des différents systèmes de sécurité, nous ferons varier les paramètres introduits au paragraphe précédent dans une plage assez large permettant de couvrir la majorité des systèmes. Toutes les courbes seront tracées de façon adimensionnelle en fontion de λt et certaines variables seront données en fonction de λ qui correspond au taux d'occurrence de la première faute dans le système.

- Taux de faute : le taux d'occurrence de la première faute sera pris constant et égal à 10^{-4}/h soit une faute/an. Nous considérons que ce taux est fonction du nombre de fautes ayant lieu dans le système. La valeur relative de ces taux sera discutée dans la partie suivante.

- Le facteur b dépend des techniques de détection utilisées, il est au moins égal à 1 et peut dépasser légèrement 2.

- D'après les normes MIL-HDBK-217-B, le facteur d'environnement le plus sévère est de l'ordre de 36 ; il correspond à un missile en lancement. La borne supérieure de ce facteur a été prise égale à 50.

- Taux de sollicitation : nous considérons qu'un système peut être sollicité en moyenne une à cent fois avant la défaillance du système, ce qui donne un intervalle moyen entre deux sollicitations compris entre quatre jours et un an soit $1 \leq \gamma/\lambda \leq 100$ ou $10^{-4}/h \leq \gamma \leq 10^{-2}/h$.

- Taux de réparation : le taux de réparation est 100 à 1000 fois plus grand que le taux de faute du système, ce qui implique une durée de réparation comprise entre une dizaine d'heures et quelques jours ; soit $100 \leq \mu/\lambda \leq 1000$ ou $10^{-2}/h \leq \mu \leq 10^{-1}/h$.

- Taux de maintenance du processus : nous supposerons que l'arrêt du système surveillé peut durer de quelques heures à quelques mois soit $10 \leq \nu/\delta \leq 10^{5}$ ou $10^{-3}/h \leq \nu \leq 1/h$.

- Durée moyenne du traitement d'une sollicitation : elle peut varier de quelques secondes à une dizaine d'heures, soit $10^{-1}/h \leq \xi \leq 10^{+4}/h$ avec $\xi/\gamma \geq 10$.

- La probabilité qu'une faute soit sans action sur le système surveillé q_o, la probabilité qu'un incident soit transitoire e, l'efficacité de détection P_D et l'efficacité de réparation P_m sont des paramètres compris entre 0 et 1 et dépendent étroitement du processus, de l'architecture et de la nature du système étudié ; nous étudierons donc l'influence de leurs variations.

Le tableau de la figure 2.7. résume les différents paramètres utilisés, leurs définitions et les valeurs retenues.

PROCESSUS	VARIABLE	SIGLE		VALEUR
CAPACITE	taux de fautes d'un calculateur	λ	une faute/an	10^{-4}/h
	facteur d'environnement	K		$1 \leq K \leq 50$
	taux de maintenance	μ	$10^2 \leq \frac{\mu}{\lambda} \leq 10^4$	$10^{-2}/H \leq \mu \leq 1/h$
SOLLICITATION	taux de sollicitation	γ	$1 \leq \frac{\gamma}{\lambda} \leq 100$	$10^{-4}/h \leq \gamma \leq 10^{-2}/h$
	taux de traitement	ξ	$\xi/\gamma \geq 10$	$10^{-1}/h \leq \xi \leq 10^{+4}/h$
	taux de maintenance	ν	$10 \leq \frac{\nu}{\gamma} \leq 10^5$	$10^{-3}/h \leq \nu \leq 1/h$

FIGURE 2.7. Définitions et valeurs des variables utilisées

Ces variables et paramètres vont nous permettre d'établir les graphes de transition markoviens et d'étudier l'influence des différents processus sur les mesures de sûreté de fonctionnement définies en 1.5.

2.3.3. *Modélisation du niveau 1*

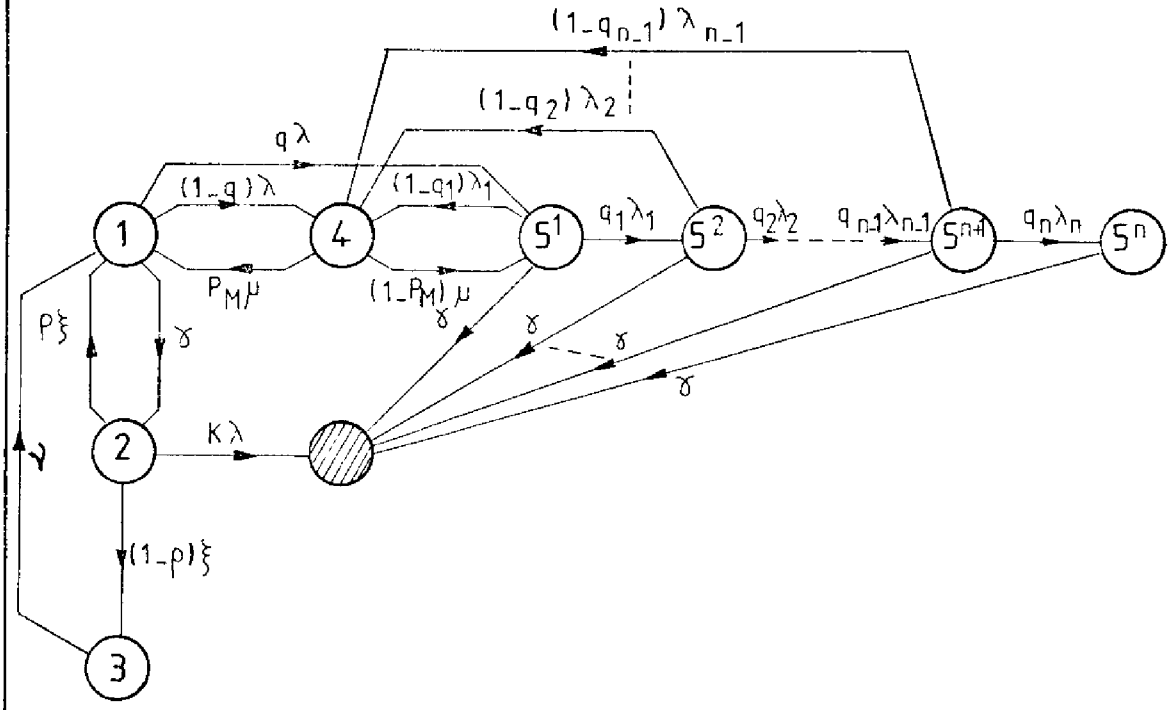
Le graphe de transition markovien est donné par la figure 2.8. ; il se déduit du graphe de la figure 1.8.a. en :

- décomposant l'état (5) en n états distincts, où n indique le nombre de fautes masquées successives dans le système,
- considérant que la réparation du système de sécurité n'est pas toujours parfaite et qu'une mauvaise réparation amène le système dans un état où il y a une seule faute masquée, état où le système peut avoir d'autres fautes,
- affectant aux transitions les taux correspondants.

Pour étudier l'influence des différents paramètres, il serait intéressant de calculer l'expression analytique de $D_1(t)$, mais ce calcul est très compliqué étant donné la complexité du graphe.

Il est cependant possible d'effectuer le calcul analytique du temps moyen avant absorption MTA1 ; le MTA1 s'obtient en calculant les différents θ_i solution du système (S1) :

GRAPHE



ETATS

(1) Etat de bon fonctionnement en absence de sollicitation

(2) Traitement d'une sollicitation

(3) Maintenance suite à un incident permanent

(4) Maintenance des deux systèmes suite à une défaillance déclarée

(S^i) Le système a eu i fautes masquées, $1 \leq i \leq n$

FIGURE 2.8. Graphe de transitions du premier niveau tenant compte de n fautes successives

$$\text{(état 1)} : -(\lambda+\gamma)\theta_1 + \rho\xi\theta_2 + \nu\theta_3 + P_m\mu\theta_4 = -1 \qquad \text{(S1)}$$

$$\text{(état 2)} : \gamma\theta_1 - (\xi + K\lambda)\theta_2 = 0$$

$$\text{(état 3)} : (1-\rho)\xi\theta_2 - \nu\theta_3 = 0$$

$$\text{(état 4)} : (1-q)\lambda\theta_1 + \sum_{i=1}^{n-1}(1-q_i)\lambda_i\theta_{5i} - \mu\theta_4 = 0$$

$$\text{(état } 5^1\text{)} : q\lambda\theta_1 + (1-P_m)\mu\theta_4 - (\lambda_1+\gamma)\theta_{51} = 0$$

$$\text{(état } 5^i\text{)} : q_{i-1}\lambda_{i-1}\theta_{5i-1} - (\lambda_i+\gamma)\theta_{5i} = 0 \quad ; \quad i = 2, \ldots, n-1$$

$$\text{(état } 5^n\text{)} : q_{n-1}\lambda_{n-1}\theta_{5n-1} - \gamma\theta_{5n} = 0$$

Après résolution de ces équations et développement limité au premier ordre en fonction de : λ/ξ , λ/μ , λ/ν , γ/ξ , γ/ν , γ/μ , q et $(1-P_m)$, on obtient :

.pour n=1, $$MTA1 = \frac{1}{\lambda\left[q\,P_m+(1-P_m)+K\,\gamma/\xi\right]} \qquad (4)$$

.pour $n \geqslant 2$, $$MTA1 = \frac{1}{\lambda\left\{(q\,P_m+1-P_m)\left[1-P_m(1-q_1)\frac{\lambda_1}{\gamma+\lambda_1}\right]+K\,\gamma/\xi\right\}} \qquad (5)$$

Ces expressions ainsi que le calcul numérique de $D_1(t)$ et le tracé des courbes grâce à l'utilisation du programme SURF nous ont permis d'avoir une évaluation précise de l'influence de tous les paramètres.

Nous allons successivement analyser l'influence :

- du nombre de fautes dans le système,
- des durées de maintenance et de l'efficacité de réparation,
- de la probabilité q qu'une faute soit masquée,
- de la prise en compte de la défaillance pendant une sollicitation.

2.3.3.1. Influence du nombre n de fautes dans le système

Nous avons considéré successivement plusieurs modèles : le premier ne tient compte que d'une seule faute masquée dans le système, le second de deux fautes et le nième de n fautes successives ; pour le tracé des différents $D_1(t)$ relatifs à ces modèles, un problème se pose : quelles sont les valeurs relatives de (q_i, λ_i) et de (q, λ) ?

- suivant l'hypothèse adoptée λ_1 peut être considéré plus petit ou plus grand que λ :
  .si nous supposons que les sources de fautes restent indépendantes, λ_1 peut être considéré comme inférieur à λ puisqu'il reste moins de matériel,
  .si nous supposons qu'une faute peut en entraîner d'autres dans le système, λ_1 peut être considéré plus grand que λ ;
- l'efficacité de détection P_D ne peut que conserver la même valeur ou diminuer à cause des phénomènes de masquage [STI 79], par contre, il est raisonnable de supposer que q_o reste constant ($q_i=q_o(1-P_{Di})$), q_1 est donc supérieur à q.

Ainsi, le produit $q_1 \lambda_1$ peut être inférieur, égal ou supérieur à $q\lambda$. Le raisonnement reste valable pour (q_i, λ_i) et (q_{i+1}, λ_{i+1}) mais du fait :

- du manque de données expérimentales concernant les variations effectives éventuelles de ces valeurs,
- de la faible influence de q_i, λ_i (voir relation (5)) : (q_i, λ_i) intervient au second ordre pour $i \geq 2$ et (q_1, λ_1) au premier ordre,

nous prendrons $\lambda_i = \lambda$ et $q_i=q$ $\forall$ $i \geq 1$.

A partir de ces hypothèses et des données indiquées dans le tableau de la figure 1.5., nous avons tracé $D_1(t)$ pour les différents modèles avec un taux de faute constant. Les courbes sont données à la figure 2.9.

On voit que les courbes sont confondues pour les modèles tenant compte de plus d'une faute masquée dans le système : il faut noter que ces résultats sont en parfait accord avec le calcul du MTA1.

Pour la modélisation d'un système de sécurité, nous prendrons donc comme hypothèse la possibilité d'occurrence de deux fautes successives avant sollicitation. Le graphe résultant, tenant compte de deux fautes successives, est donné à la figure 2.10.

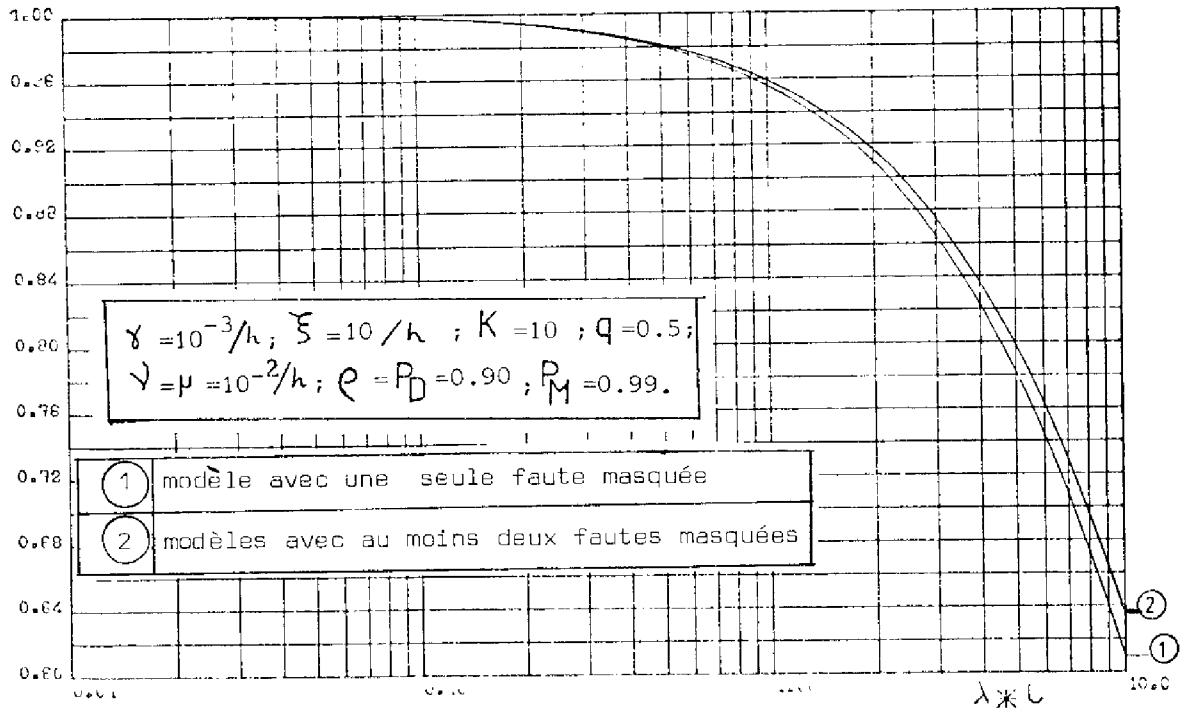


FIGURE 2.9. Influence du nombre de fautes masquées

2.3.3.2. Influence des durées de maintenance et de l'efficacité de réparation

Nous avons tracé $D_1(t)$ en faisant varier successivement (μ, P_m) et ν ; ces courbes sont données par les figures 2.11. et 2.12., elles montrent que seul P_m a une grande influence sur $D_1(t)$ et que les temps de maintenance peuvent être négligés (μ et ν infiniment grands). Les probabilités d'être dans les états (3) et (4) sont donc négligeables et ces états peuvent être supprimés. La méthode de réduction du graphe [LAP 76] est donnée en Annexe, le graphe de transition résultant est donné à la figure 2.13.

2.3.3.3. Influence de q

Etudier l'influence de q revient à étudier l'influence des deux paramètres q_o et P_D ($q=q_o(1-P_D)$). Nous les avons fait varier simultanément dans leurs plages respectives.

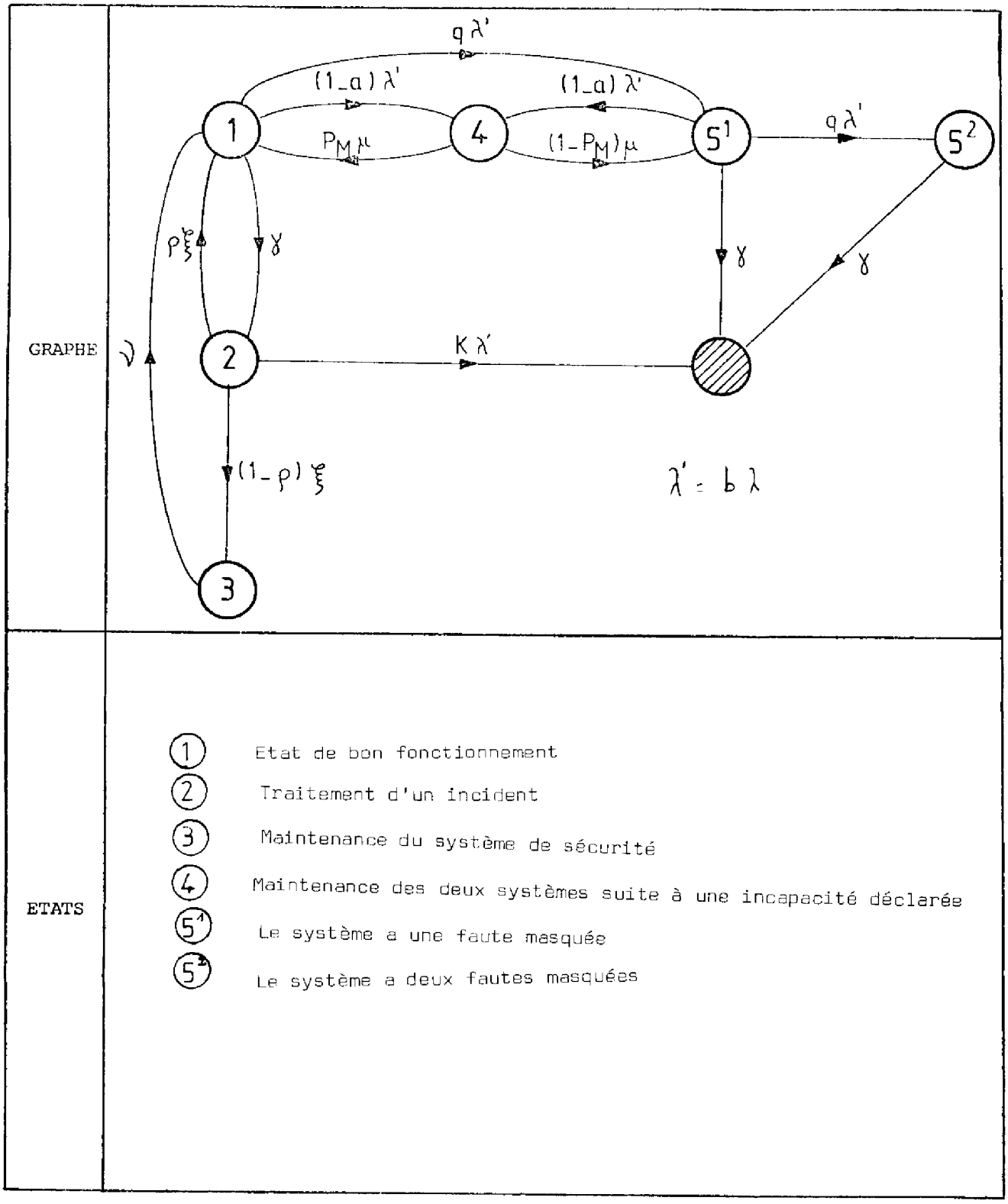


FIGURE 2.10. Graphe de transition du niveau 1 tenant compte de deux fautes masquées

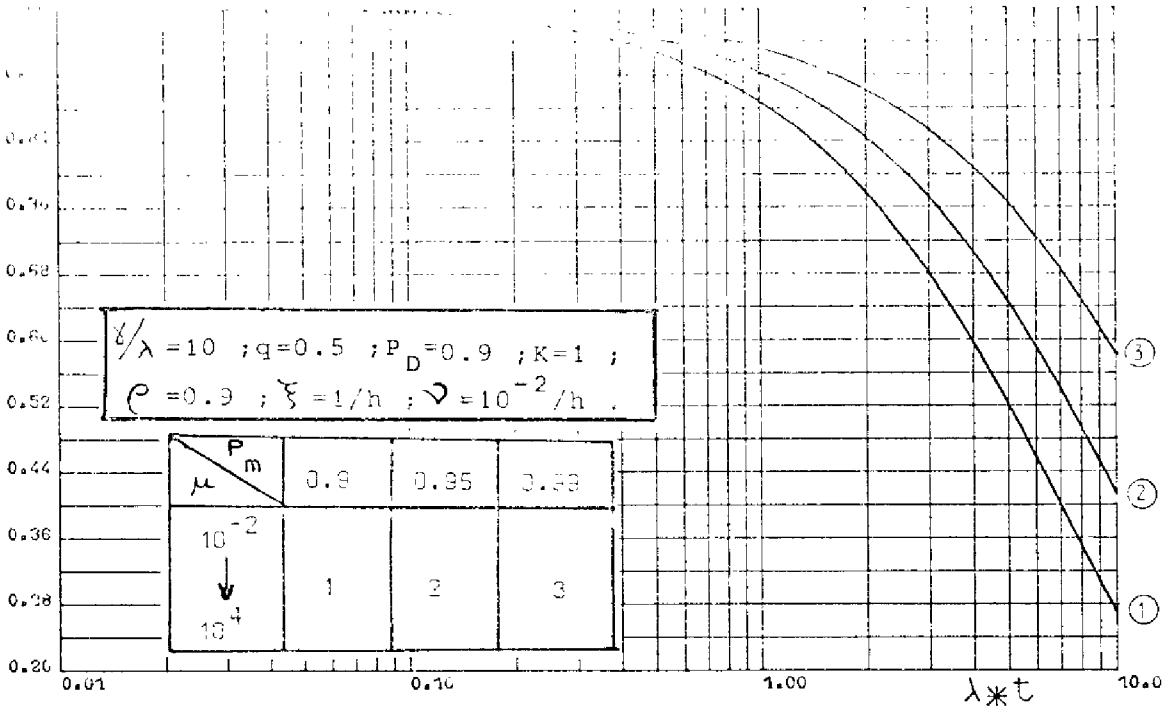


FIGURE 2.11. Influence de μ, P_m

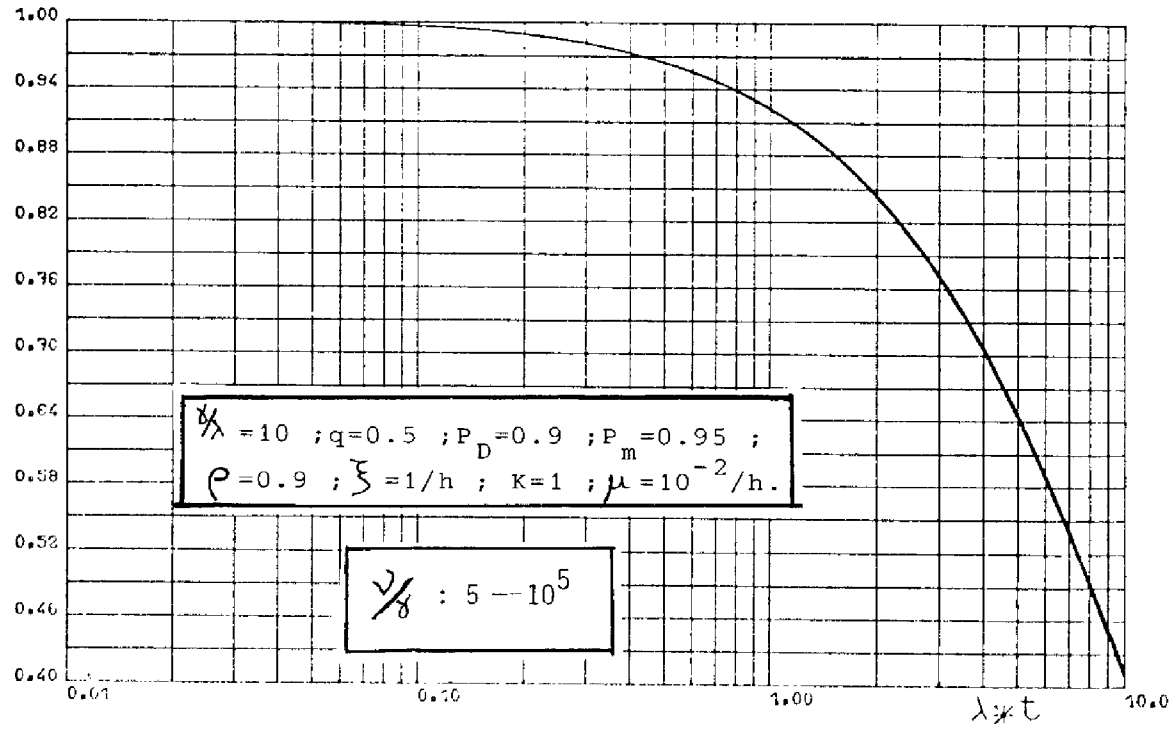


FIGURE 2.12. Influence de ν

Le tracé des courbes qui en résultent montre (figure 2.14.) que ces deux paramètres ont une grande influence sur $D_1(t)$ mais que pour une bonne efficacité de détection (P_D=0.99) q_o a peu d'influence ; ceci confirme le fait qu'il faut munir le système d'une détection de faute très efficace.

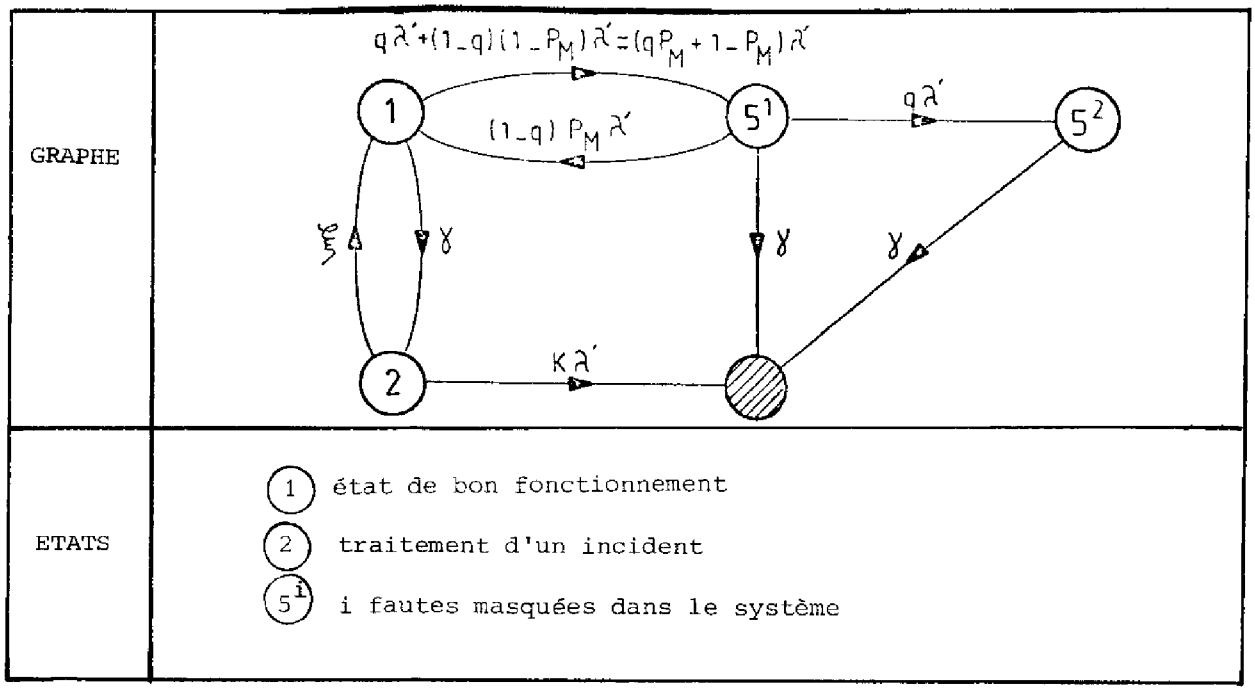
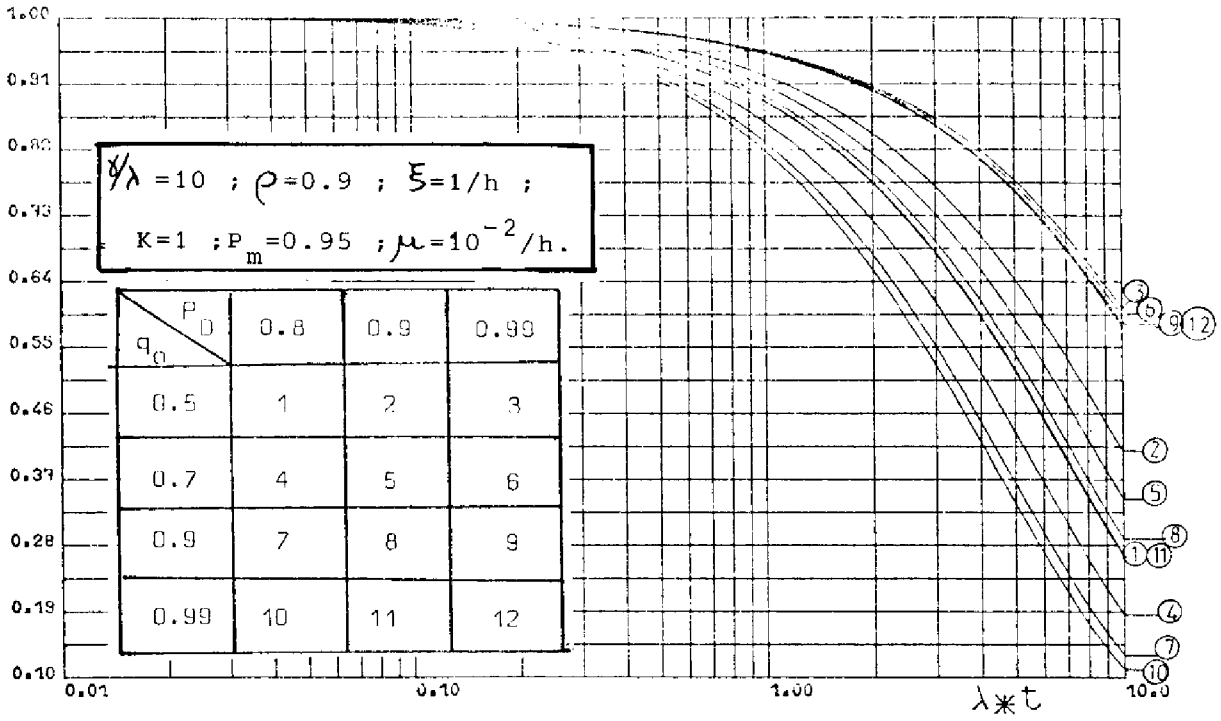


FIGURE 2.13. Graphe réduit du niveau 1



q_o \ P_D	0.8	0.9	0.99
0.5	1	2	3
0.7	4	5	6
0.9	7	8	9
0.99	10	11	12

FIGURE 2.14. Influence de $q=q_o(1-P_D)$

2.3.3.4. Prise en compte de la défaillance pendant une sollicitation

La défaillance pendant une sollicitation se traduit par la transition K λ entre l'état (2) et l'état absorbant du graphe de la figure 2.10., et par le terme $K\lambda\frac{\gamma}{5}$ dans l'expression de MTA1 (voir relation (5)).

D'après l'expression de MTA1, la probabilité qu'une faute ait lieu dans le système lors du traitement d'un incident n'est pas négligeable pour les systèmes tels que $K\frac{\gamma}{5}$ est de l'ordre de q et de $(1-P_m)$. Le tracé des courbes (figure 2.15.) confirme ces résultats :

- pour un système tel que $K\gamma/5 \sim q$ et $(1-P_m)$, il faut tenir compte de la transition de l'état (2) vers l'état absorbant. Le graphe représentatif d'un tel système est donné sur la figure 2.13.,
- pour un système tel que $K\gamma/5 \ll q$ et $(1-P_m)$, la probabilité de passage de l'état (2) vers l'état absorbant est négligeable. Le calcul par le programme SURF de la probabilité que le système soit dans l'état (2) montre que cette probabilité est tout à fait négligeable ; nous concluons que cet état peut être supprimé. Le graphe de transition obtenu après suppression de l'état (2) est donné sur la figure 2.16.

2.3.4. Modélisation du niveau 2

Nous avons vu qu'il y a deux mesures ($D_{21}(t)$ et $D_{22}(t)$) pour le niveau 2 ; nous allons les examiner successivement.

Le graphe de transition de $D_{21}(t)$ étant le même que celui du niveau 1, le MTA_{21} s'obtient en calculant θ_i pour $i \in \{1,2,3\}$ solution de (S1) (cf. 2.3.3.). Nous avons alors :

$$MTA_1 - MTA_{21} \# \theta_4 + \theta_{51} + \theta_{52}$$

La résolution de (S1) avec $\lambda_i = \lambda$ et $q_i = q$ donne au premier ordre par rapport à q et $(1-P_m)$:

$$\theta_4 \# \frac{\lambda}{\mu}(1-q)\left[1+q\frac{\lambda}{\lambda+\gamma}\right]\theta_1 \leq \frac{\lambda}{\mu}\theta_1$$

$$\theta_{5^1} \# \left[q+(1-P_m)(1-q)\right]\frac{\lambda}{\lambda+\gamma}\theta_1$$

$$\theta_{5^2} = q\frac{\lambda}{\lambda+\gamma}\theta_{5^1}$$

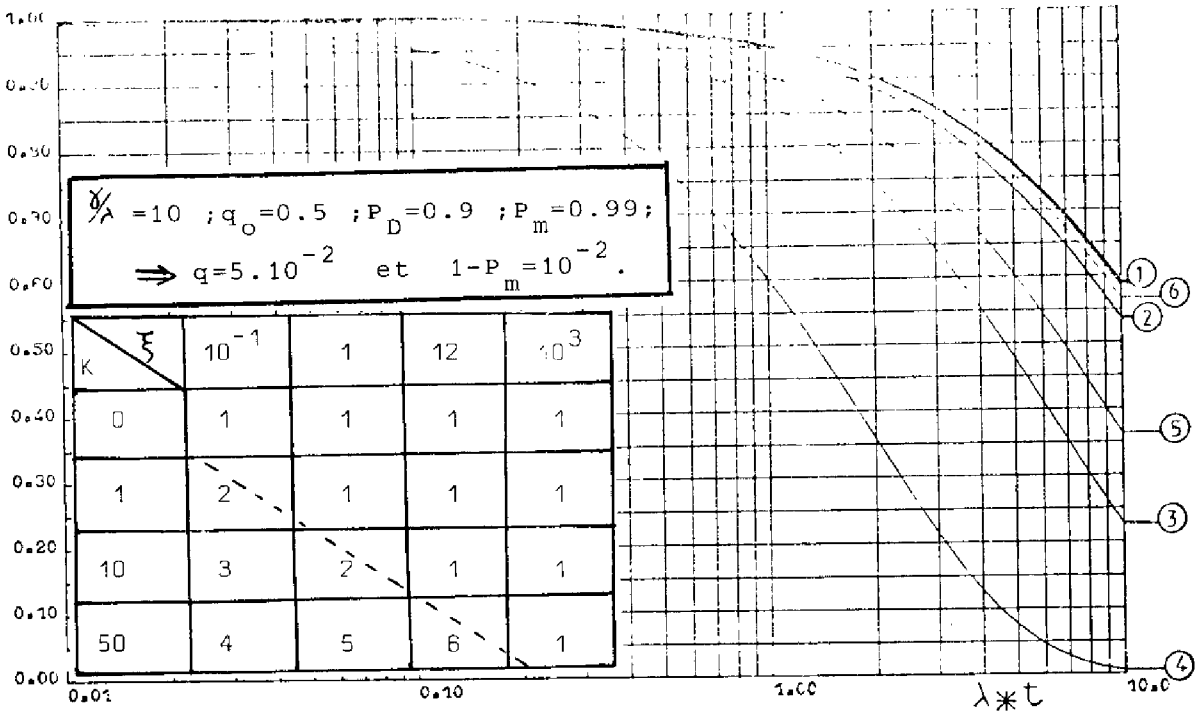


FIGURE 2.15. Défaillance pendant une sollicitation

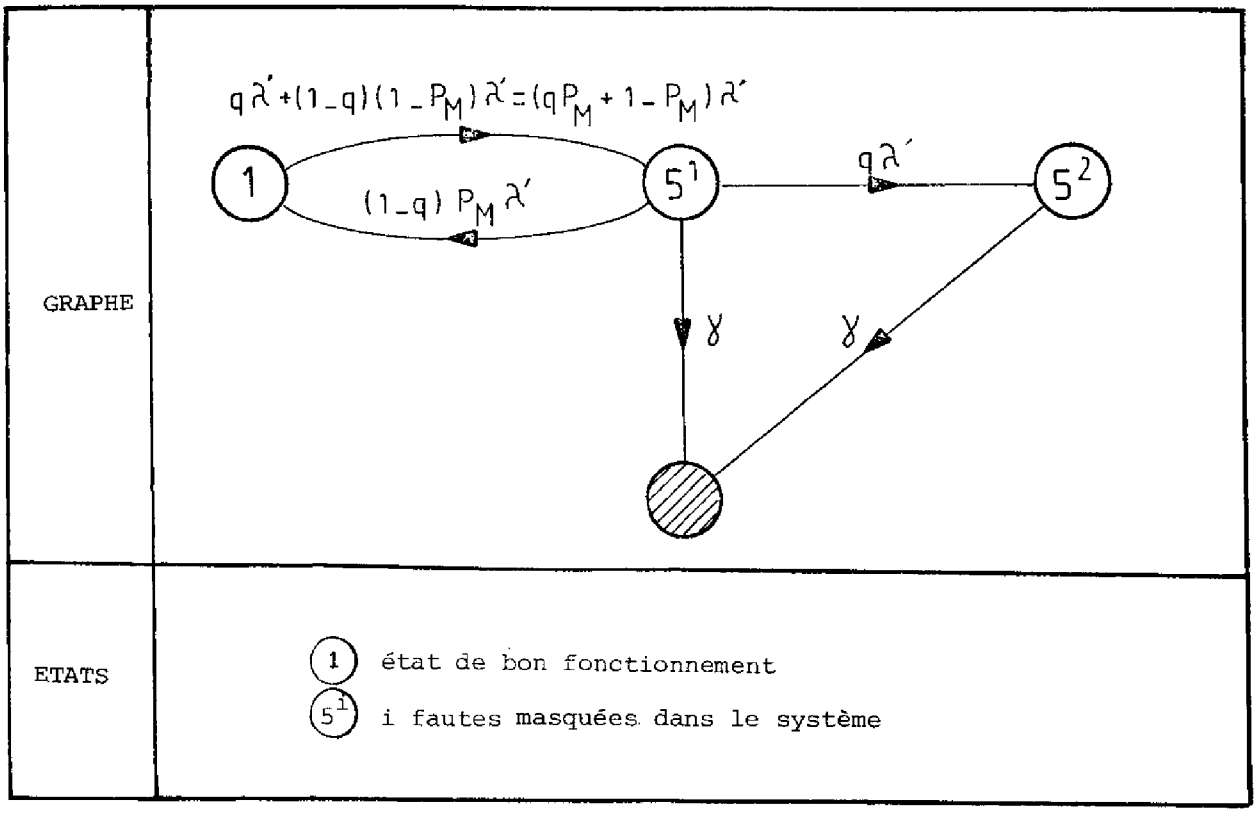


FIGURE 2.16. Graphe obtenu après suppression de l'état de traitement d'un incident pour un système tel que $K\gamma/\lambda \ll q$ et $(1-P_m)$

Nous avons donc au premier ordre $MTA_1 = MTA_{21}$; $D_1(t)$ et $D_{21}(t)$ sont donc très peu différents, et les résultats que nous pourrons tirer de $D_{21}(t)$ seront équivalents à ceux de $D_1(t)$. La figure 2.17. est en accord avec ces calculs. Dans la suite, seul $D_{22}(t)$ sera considéré, et sera noté $D_2(t)$.

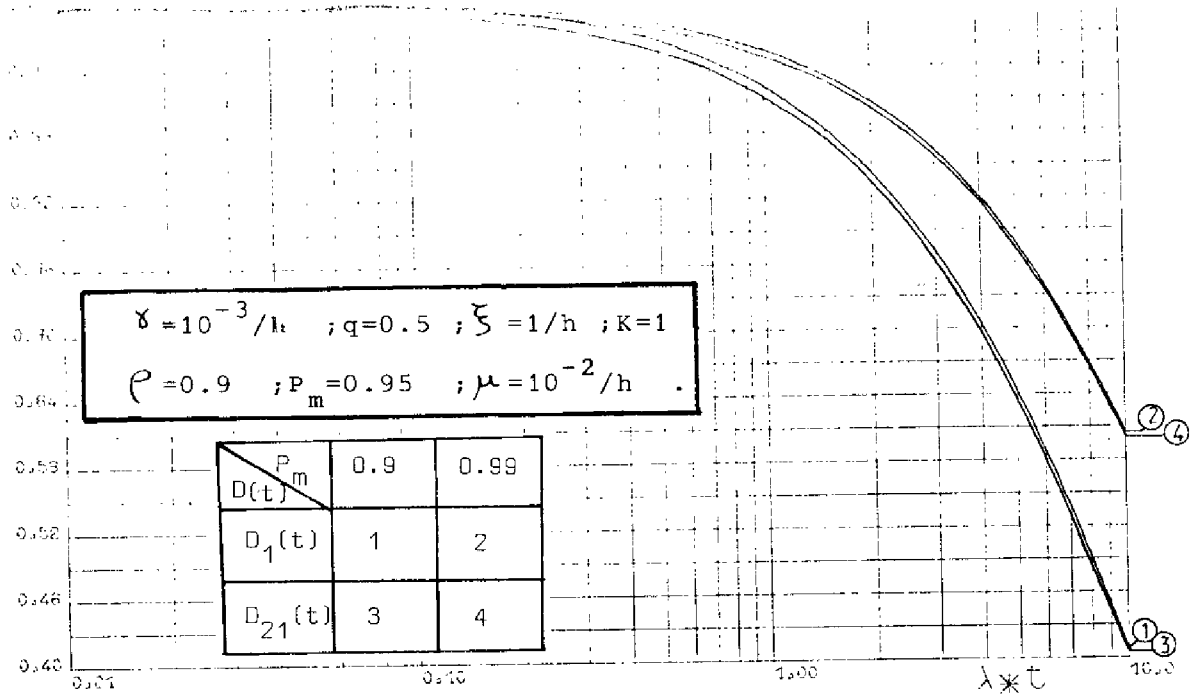


FIGURE 2.17. $D_1(t)$ et $D_{21}(t)$

Le graphe de transition de $D_2(t)$ qui est donné par la figure 2.18. se déduit de celui de la figure 1.8.b. en affectant aux transitions les taux correspondants.

Le MTA_2 s'obtient en calculant les θ_i solutions du système (S2) :

(état 1) : $-(\lambda+\gamma)\,\theta_1 + \rho\xi\,\theta_2 + \mu\,\theta_3 = -1$ (S2)

(état 2) : $\gamma\theta_1 - (K\lambda+\xi)\,\theta_2 = 0$

(état 3) : $(1-\rho)\,\xi\,\theta_2 - \mu\,\theta_3 = 0$

ce qui donne au premier ordre par rapport à λ/ξ, γ/ξ et γ/ν :

$$MTA_2 \# \frac{1}{\lambda}\left[1-(K-1)\frac{\gamma}{\xi} + (1-\rho)\frac{\gamma}{\nu}\right] \qquad (6)$$

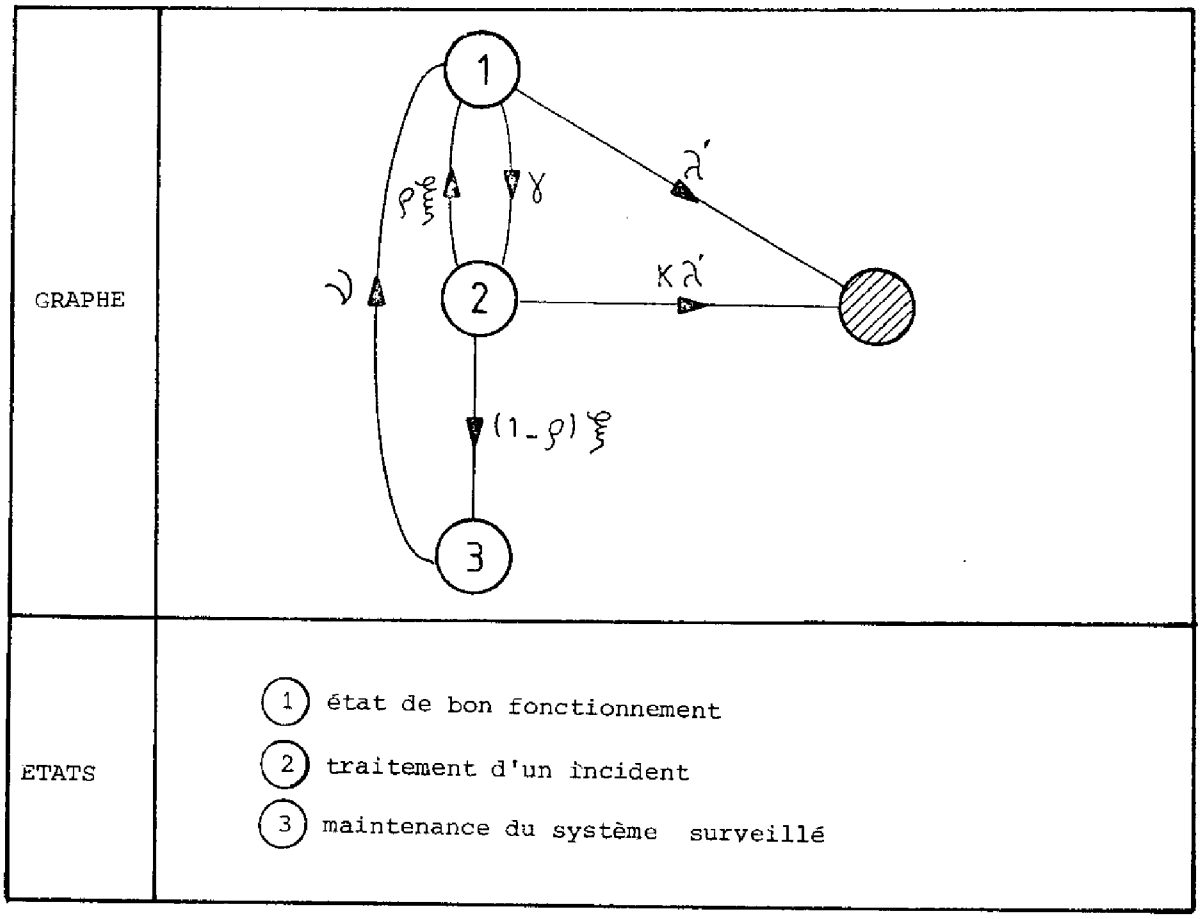


FIGURE 2.18. Graphe de transition de $D_2(t)$

Bien que tous les paramètres interviennent dans l'expression de MTA_2, leur influence est très faible. Cette influence est donnée par les courbes de la figure 2.19., courbes qui sont très rapprochées ; les courbes relatives aux systèmes qui sont tels que $(K-1)\,\nu \sim (1-\rho)\,\xi$ sont confondues avec $e^{-\lambda t}$. Ceci est dû au fait que $D_2(t)$ est très proche de la notion de fiabilité au sens classique. On en déduit que : $D_2(t) \neq e^{-\lambda t}$.

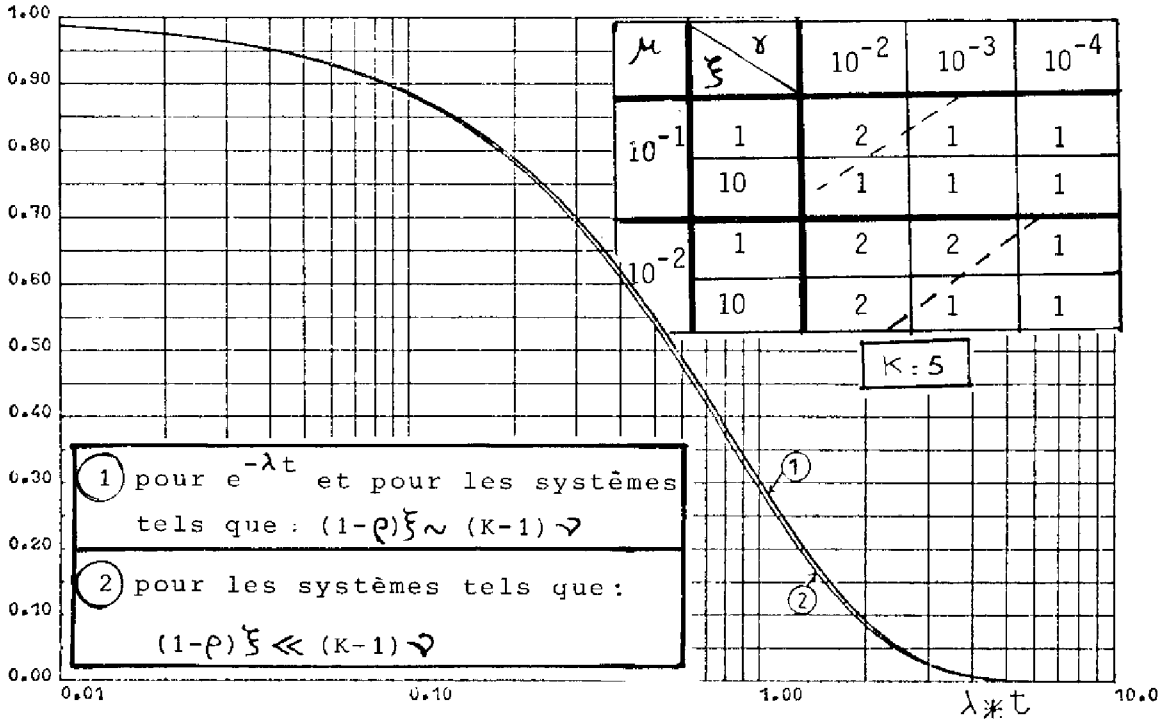


FIGURE 2.19. $D_2(t)$ et $e^{-\lambda t}$

L'étude du système non tolérant aux fautes nous a permis de dégager les résultats suivants :

- il est inutile de tenir compte de plus de deux fautes masquées pour la modélisation d'un tel système,
- les temps de maintenance peuvent être négligés,
- les efficacités de détection et de réparation (P_D et P_m) sont des paramètres très importants,
- pour le niveau 2 une seule mesure est intéressante : $D_{22}(t)$.

2.4. *Systèmes tolérants aux fautes*

Ce paragraphe est consacré à l'étude de deux systèmes de sécurité tolérants aux fautes : système duplex et système avec vote majoritaire.

Ces deux systèmes sont modélisés dans le but de mener une étude de sensibilité qui permettra de déterminer les paramètres les plus influents afin de rendre possible leur comparaison entre eux et avec le système non tolérant aux fautes étudié dans le paragraphe précédent.

2.4.1. Détection de fautes

Lorsqu'une des unités est défaillante suite à la manifestation d'une faute, il est nécessaire que l'(es) unité(s) restante(s) soit (soient) capable(s) d'assurer à elles seules la sécurité du système surveillé :

- dans le cas du système duplex : chaque unité doit donc posséder ses propres techniques de détection,
- dans le cas du système à vote majoritaire, un dispositif de détection de désaccord est nécessaire.

2.4.2. Paramètres associés aux systèmes tolérants aux fautes

L'introduction d'un paramètre supplémentaire, a, qui représente le nombre d'unités dans le système (a=2 pour le système duplex et a=3 pour le système à vote majoritaire), permet de représenter ces deux systèmes par le même graphe.

Pour l'établissement du graphe, il est nécessaire de définir les paramètres relatifs à la détection - couverture et à la maintenance de ces systèmes :

a) détection - couverture

- avant manifestation d'une faute : le taux de couverture c, défini comme suit [BOU 69 - ARN 72] :
  $c = \mathcal{P}\{\text{le système continue à fonctionner/une faute est apparue}\}$

  Une faute est couverte si elle a été détectée, localisée, si l'unité défaillante a été déconnectée et si la reprise des opérations de fonctionnement normal s'est effectuée correctement ; de ce fait, c peut être décomposé de la façon suivante : $c = P_D.P_R$
  - P_D est l'efficacité de détection du système telle que définie au paragraphe 2.3.2.1.,
  - $P_R = \mathcal{P}\{$faute soit localisée, que l'unité défaillante soit déconnectée et que la reprise des opérations de fonctionnement normal soit effectuée correctement/une faute a été détectée$\}$.

  Le problème qui se pose alors est le suivant : ce taux de couverture est-il le même en présence et en l'absence d'incident ? Soient respectivement $c_p = P_{Dp}.P_{Rp}$ et $c_a = P_{Da}.P_{Ra}$ ces taux ; logiquement, nous avons : $P_D \geqslant P_{Da}$ puisque certaines parties du système ne sont activées qu'en présence d'incident, ce qui permet une meilleure détection,

.$P_{Rp} \leq P_{Ra}$ puisque lors d'un incident, le système est assujetti à plus de contraintes, quelles soient temporelles ou dues à l'environnement.

Ainsi c_p peut être supérieur, inférieur ou égal à c_a.

- après manifestation de la première défaillance, la détection est effectuée de manière différente et on ne peut plus écrire que l'efficacité de détection est égale à P_D ; soit P_c cette efficacité. Si une faute masquée a lieu dans l'(es) unité(s) restante(s), cette faute peut être détectée et réparée par l'opérateur lors de la remise en marche du système ; soit P_o cette probabilité :
$P_o = \mathcal{P}\{$l'opérateur détecte et répare correctement l'unité en défaillance masquée lors de la remise en marche du système/une ou deux fautes masquées ont eu lieu dans le système après manifestation de la première défaillance et durant la réparation de l'unité en défaillance couverte$\}$.

b) maintenance

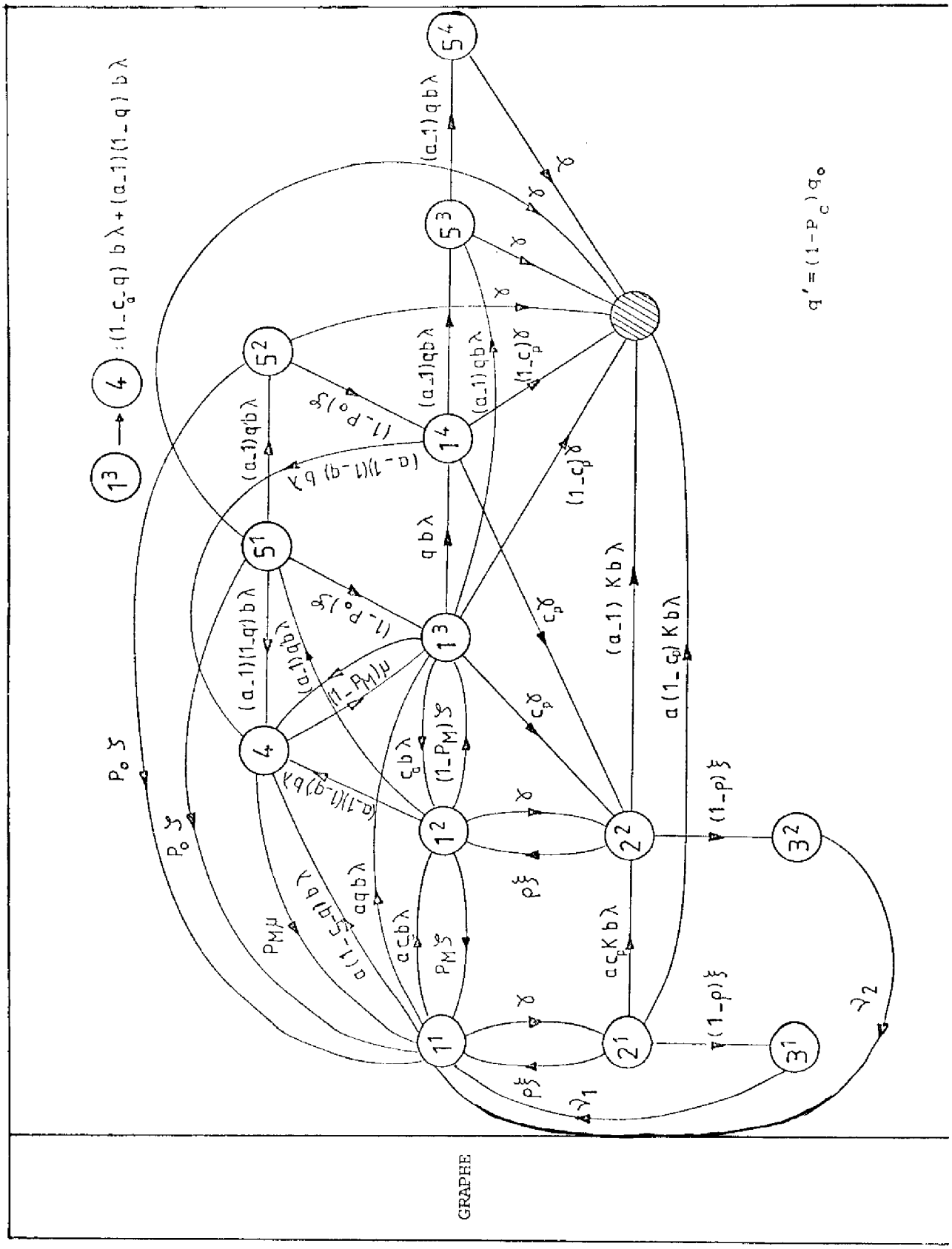
- après manifestation de la première défaillance le taux de réparation de l'unité défaillante sera noté ζ ,
- le taux de maintenance du système surveillé après un incident permanent sera noté γ_1,
- le taux de maintenance du système surveillé et de l'unité en défaillance couverte suite à un incident permanent éliminé par l'(es) unité(s) restante(s) sera noté γ_2.

2.4.3. Graphes de transition

L'hypothèse de faute adoptée découle de l'étude faite en 2.3.3.1., nous tenons compte de deux fautes successives par ensemble, un ensemble est constitué par :

- une unité pour le système duplex,
- une unité pour le système à vote majoritaire avant manifestation d'une faute et l'ensemble formé par les deux unités restantes après manifestation de la première défaillance, ce qui est logique puisque ces deux unités forment un système muni de sa détection de faute.

Les graphes de transition markoviens obtenus à partir des graphes de la figure 1.8. en décomposant les différents états et en affectant aux transitions les taux correspondants sont donnés par les figures 2.20. et 2.21.


GRAPHE
$q' = (1-p_c)\,q_o$
$P_o\,\gamma$
$P_o\,\gamma$
$P_M\mu$
$\rho\,\xi$
γ_1
γ_2
$(1-\rho)\,\xi$
$a\,(1-c_\beta)\,K\,b\,\lambda$
$(a-1)\,K\,b\,\lambda$
$c_\beta\,\gamma$
$(1-c_\beta)\,\gamma$
$q\,b\,\lambda$
$(a-1)\,q\,b\,\lambda$
$(1-P_M)\,\mu$
$(1-P_M)\,\gamma$
$(1-P_o)\,\gamma$
$(a-1)(1-q)\,b\,\lambda$
$(a-1)(1-q')\,b\,\lambda$
$a\,c_\beta\,K\,b\,\lambda$
$a\,c_\alpha\,b\,\lambda$
$a\,(1-c_\alpha-c_\beta)\,q\,b\,\lambda$
$(1-c_\alpha-q)\,b\,\lambda + (a-1)(1-q)\,b\,\lambda$

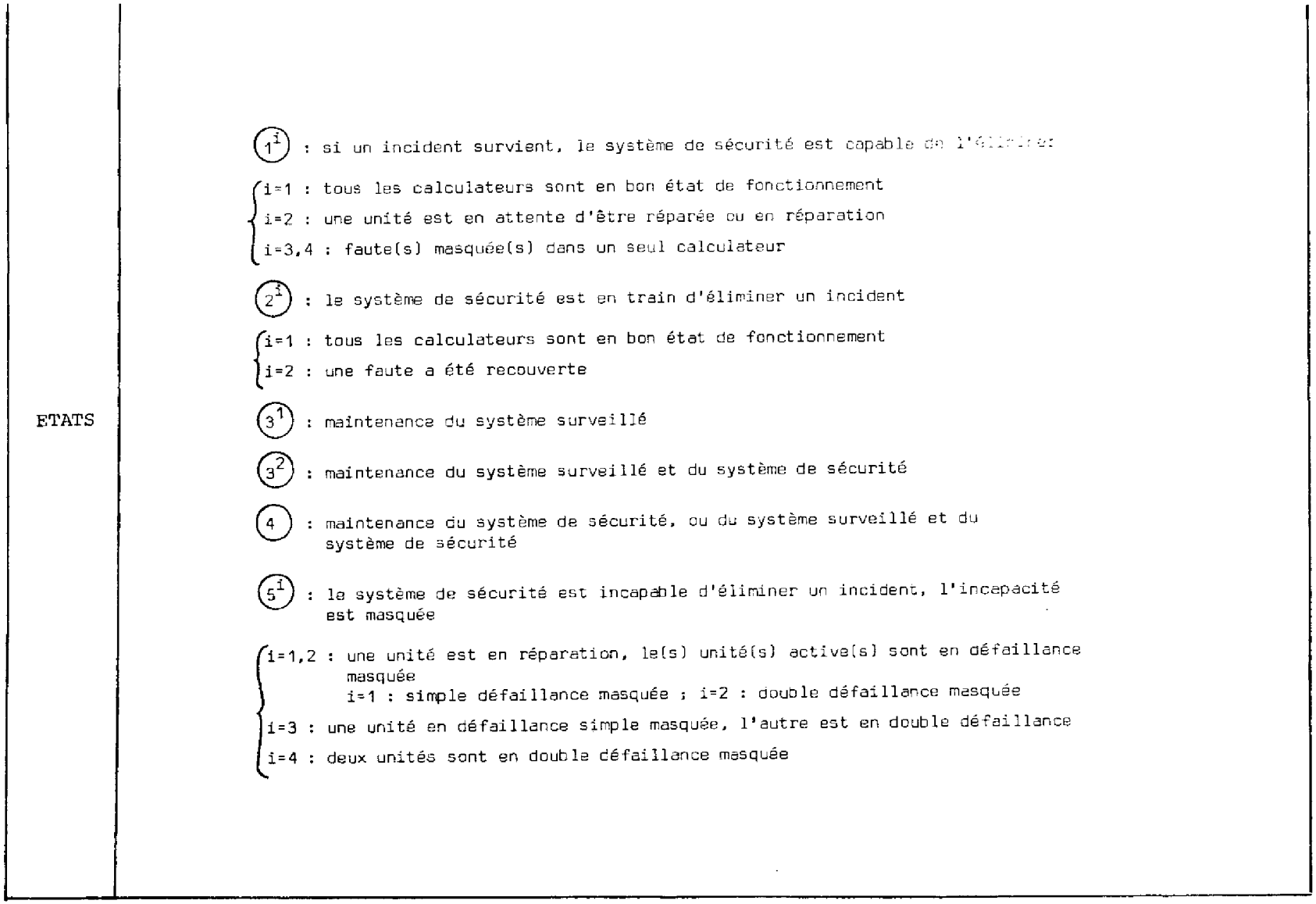
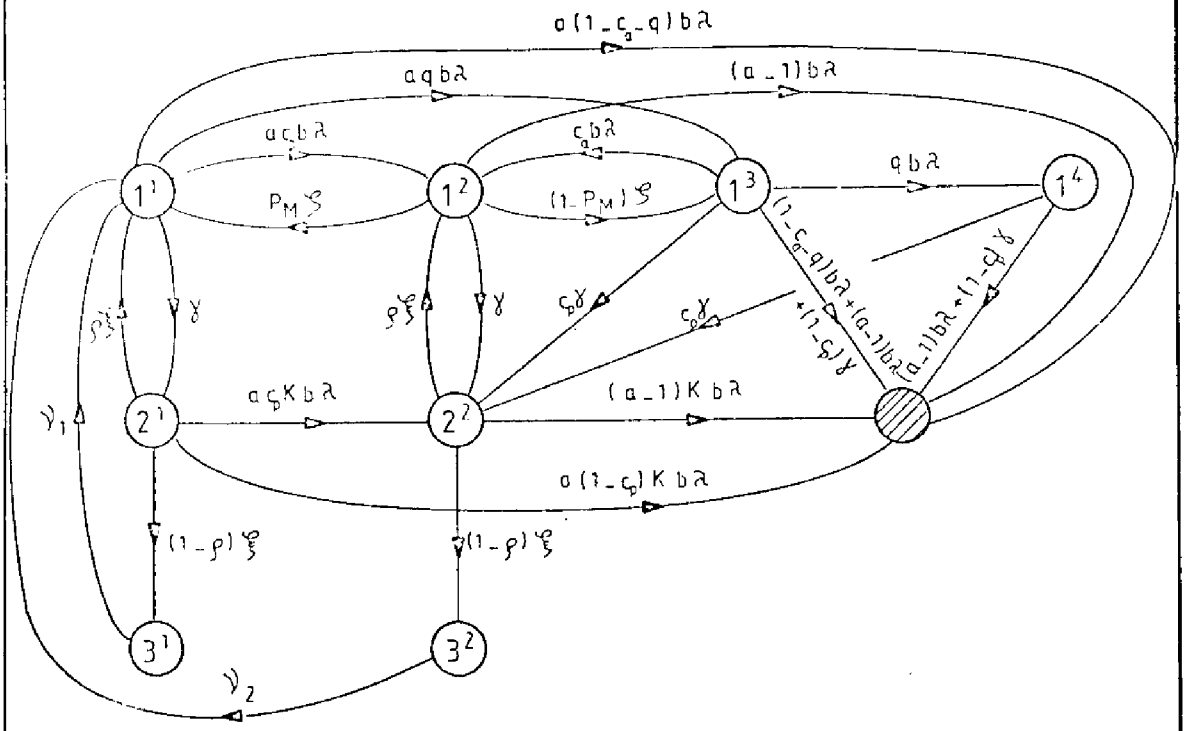


FIGURE 2.20. Graphe de transition du niveau 1, pour un système tolérant aux fautes

GRAPHE



ETATS

(1^i) : si un incident survient, le système de sécurité est capable de l'éliminer

- i=1 : tous les calculateurs sont en bon état de fonctionnement
- i=2 : une unité est en attente d'être réparée ou en réparation
- i=3,4 : faute(s) masquée(s) dans un seul calculateur

(2^i) : le système de sécurité est en train d'éliminer un incident

- i=1 : tous les calculateurs sont en bon état de fonctionnement
- i=2 : une faute a été recouverte

(3^1) : maintenance du système surveillé

(3^2) : maintenance du système surveillé et du système de sécurité

FIGURE 2.21. Graphes de transition du niveau 2, pour un système tolérant aux fautes

2.4.4. *Etude de sensibilité aux différents paramètres*

Nous donnons ci-après les principaux résultats obtenus lors de l'étude de sensibilité aux différents paramètres. Ces résultats sont valables pour les deux systèmes (a=2 et a=3) et peuvent être résumés comme suit :

- pour les deux niveaux, ζ et ν_i n'ont pas d'influence et peuvent donc être pris infinis,
- pour le niveau 1 : μ, P_o et P_c n'ont aucune influence,
- pour les deux niveaux les paramètres les plus importants sont : P_D, P_R et P_m. La figure 2.22. montre l'influence de P_m alors que la figure 2.23. donne l'influence simultanée de P_D et de P_R; sur cette figure on voit que P_D a plus d'influence que P_R ; ceci est dû au fait que P_D intervient dans q et c alors que P_R n'intervient que dans c,
- le rapport c_p/c_a a beaucoup d'influence sur $D_1(t)$ et aucune influence sur $D_2(t)$.

2.4.5. *Comparaison*

Les figures 2.24. et 2.25. permettent de comparer ces deux systèmes entre eux et avec le système non tolérant aux fautes. L'amélioration introduite sur les deux niveaux par les techniques de tolérance aux fautes est indiscutable, cependant le niveau 2 est plus sensible à cette augmentation.

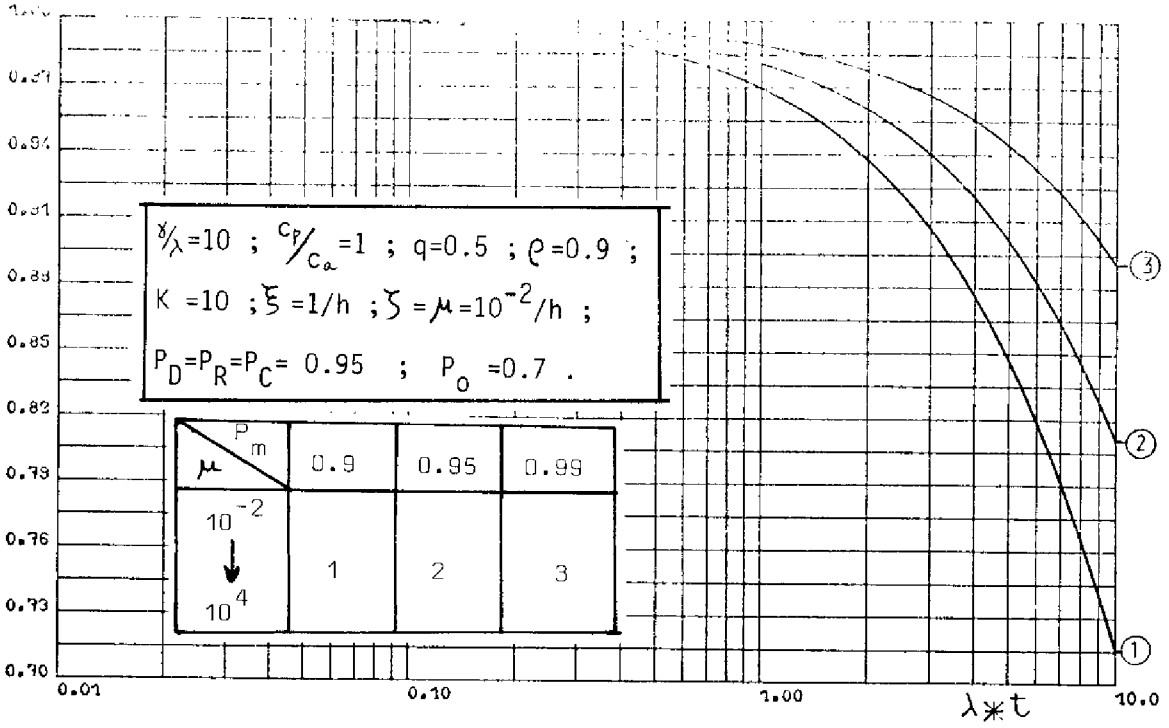


FIGURE 2.22. Influence de μ, P_m, niveau 1, a = 3

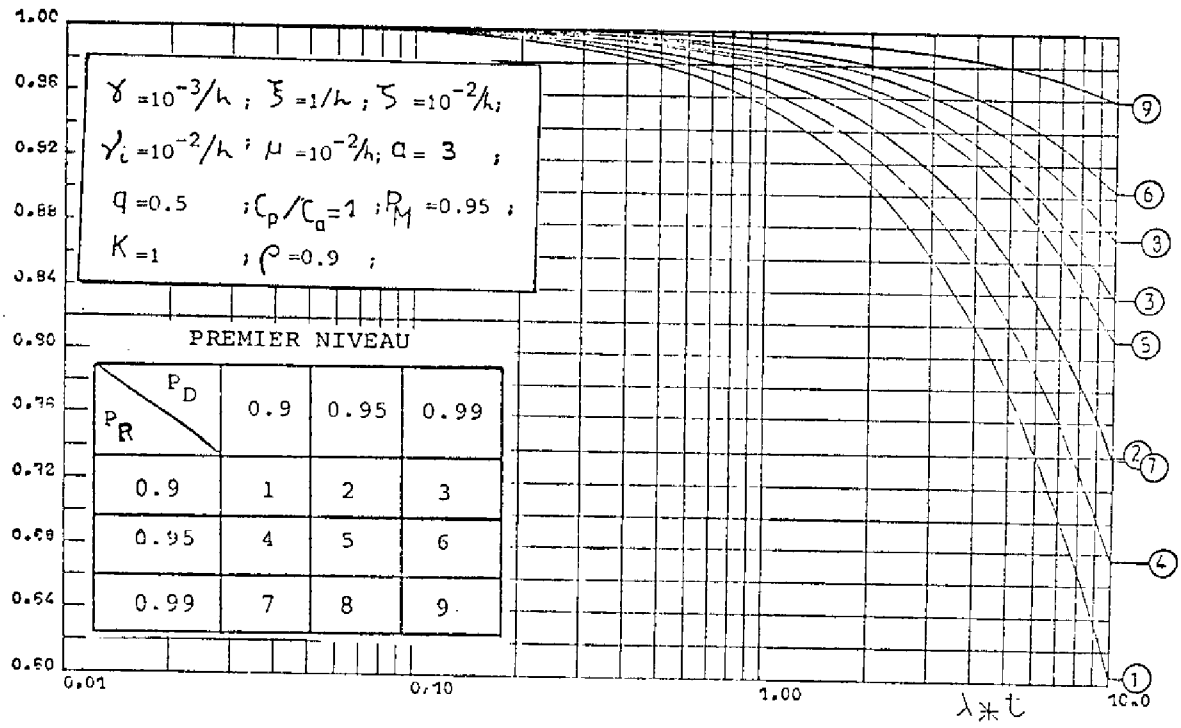
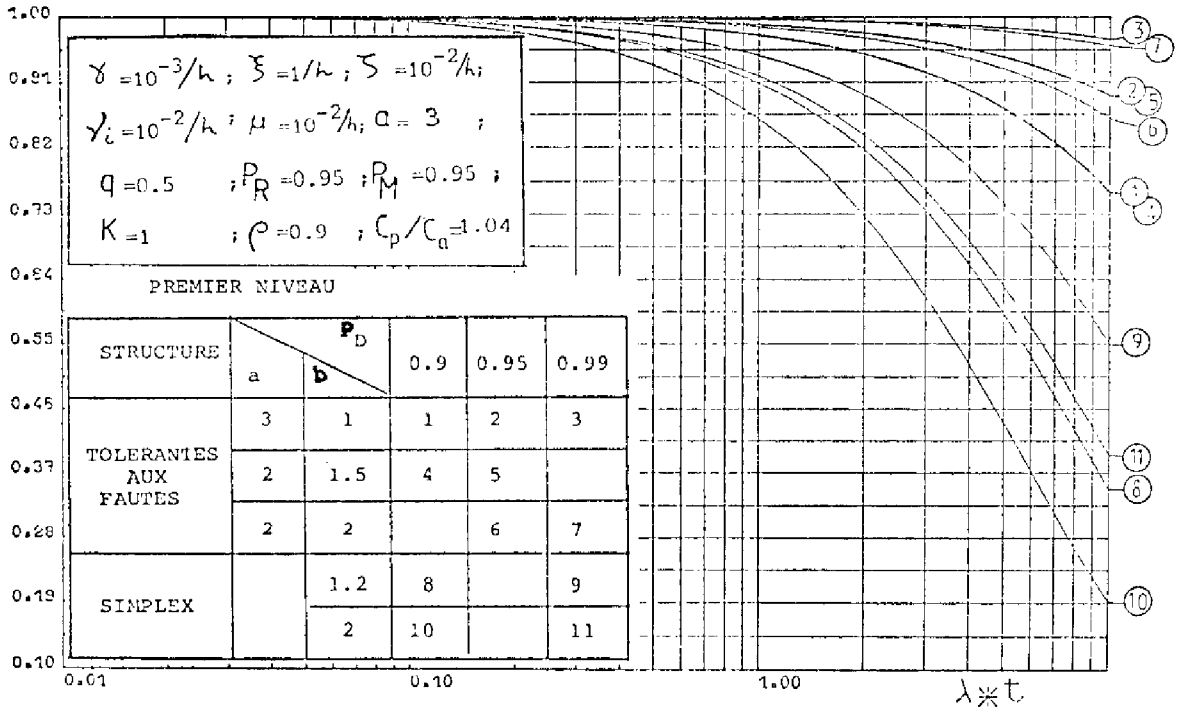
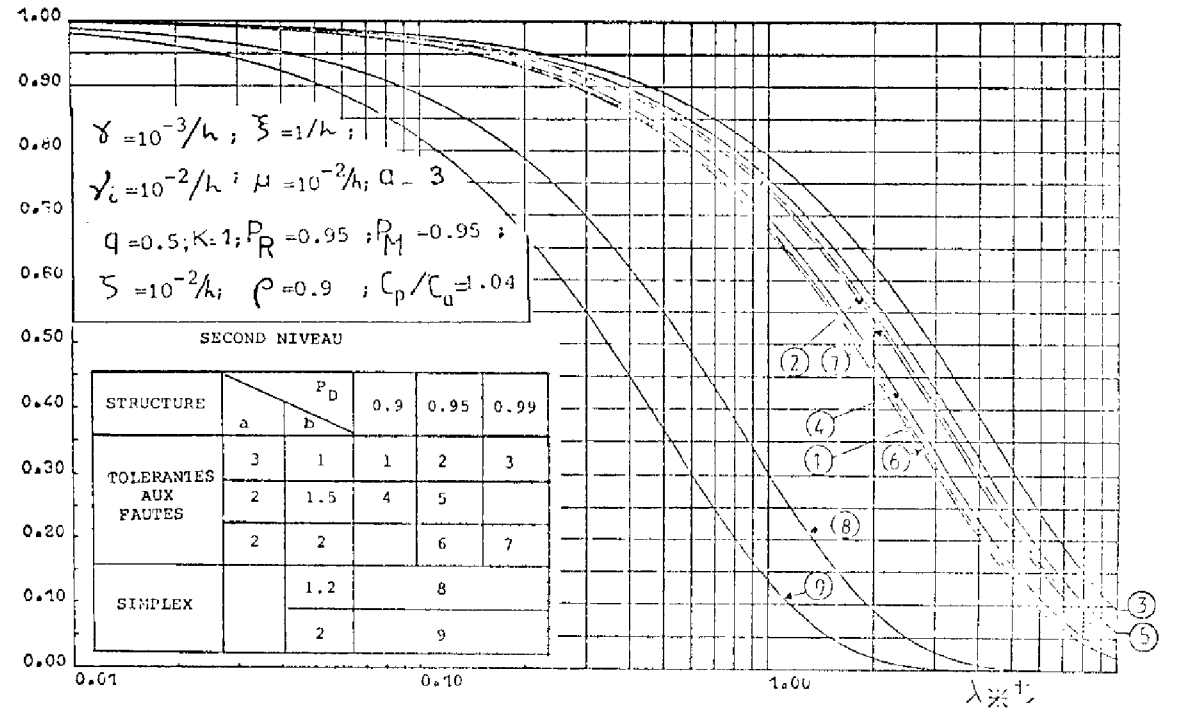


FIGURE 2.23. Influence de P_D, P_R, niveau 1, a = 3



STRUCTURE	a \ PD / b	0.9	0.95	0.99
TOLERANCES AUX FAUTES	3	1	1	2	3
	2	1.5	4	5	
	2	2		6	7
SIMPLEX		1.2	8		9
		2	10		11

FIGURE 2.24. Comparaison niveau 1



STRUCTURE	a \ PD / b	0.9	0.95	0.99
TOLERANCES AUX FAUTES	3	1	1	2	3
	2	1.5	4	5	
	2	2		6	7
SIMPLEX		1.2	8		
		2	9		

FIGURE 2.25. Comparaison niveau 2

DEUXIEME PARTIE

ÉTUDE D'UN SYSTÈME PARTICULIER :

POSTE À TRÈS HAUTE TENSION

-

Cette partie est consacrée à la recherche de la sûreté de fonctionnement du système destiné à la protection contre les courts-circuits dans les postes à très haute tension [LAP 79]. Elle se divise en trois chapitres :

- dans le premier, nous donnerons la position du problème et nous décrirons le fonctionnement d'un poste,
- dans le deuxième, nous établirons le modèle d'un système de commande d'un poste T.H.T., en nous basant sur le système actuel,
- le dernier chapitre sera consacré à l'inclusion dans le modèle de deux points importants pour le futur système de commande : détection des fautes et échanges d'informations entre les sous-ensembles.

3. POSITION DU PROBLEME : BUT ET CONTEXTE DE L'ETUDE, DESCRIPTION ET CARACTERISATION D'UN POSTE A TRES HAUTE TENSION

Ce chapitre introductif a pour but de donner le contexte de l'étude que nous avons menée sur les postes à très haute tension, de décrire le fonctionnement de ces derniers [EDF 74] et de les caractériser sur le plan de la sûreté de fonctionnement.

A cette fin, nous allons donner successivement :

- le contexte de l'étude,
- la description d'un poste à très haute tension,
- les grandeurs caractéristiques de la sûreté de fonctionnement d'un poste.

3.1. But et contexte de l'étude

Le rapport entre la puissance des centrales et celle véhiculée par le réseau de transport (réseau 400 KV) ne cessant de croître, la stabilité du réseau de transport devient de plus en plus difficile à assurer. C'est pourquoi la vitesse d'élimination des défauts (par exemple amorçage d'un arc entre une phase et la terre) revêt une importance capitale. Les performances des dispositifs de détection et d'élimination des défauts doivent donc être accrues par rapport aux solutions actuelles. Ceci a amené "Electricité de France" à élaborer un nouveau palier du plan de protection du réseau.

Le but de notre étude est donc la conception et la réalisation d'une maquette de la commande du poste, en mettant l'accent sur la sûreté de fonctionnement. L'intégration des résultats obtenus lors de cette étude aux résultats obtenus sur un plan plus général par E.D.F. permettra à cet organisme d'établir un cahier des charges détaillé pour la réalisation des postes T.H.T.

En ce qui concerne l'étude qui a été confiée à l'équipe "Architectures Sûres de Fonctionnement" du L.A.A.S., la méthode de conception qui sera suivie est celle qui est développée depuis plusieurs années dans cette équipe. Son principe est donné par la figure 3.1. :

- l'exploitation première des spécifications conduit à distinguer deux catégories de contraintes (ou objectifs) selon qu'elles laissent ou non des degrés de liberté au concepteur dans le choix des solutions,
- les contraintes sans degré de liberté entraînent des choix de principe qui, s'ils ne sont pas validés par l'évaluation des performances ou s'ils sont en conflit, entraînent une remise en cause des spécifications,
- les contraintes avec degrés de liberté permettent de définir une famille de structures acceptables parmi lesquelles une sélection sera faite. Cette sélection, basée sur l'évaluation prévisionnelle des performances se fera à chaque étape de la conception pour aboutir aux spécifications de réalisation (cahier des charges ou prototype),
- le nombre et la sélection des niveaux d'abstraction est limité, et spécifique de l'application envisagée.

Cette méthode a déjà été appliquée avec succès à la conception d'un calculateur de régulation de turboréacteur [BEO 77] et est actuellement mise en oeuvre dans la conception du système informationnel d'ateliers flexibles, en collaboration avec la Régie RENAULT.

Cette méthode est basée sur l'évaluation des solutions possibles ; or, nous avons vu dans la première partie, que les systèmes de sécurité présentent de nombreuses spécificités, par conséquent l'utilisation de cette méthode dans les systèmes de commande des postes T.H.T. nécessite une étape préliminaire : l'établissement du modèle détaillé du comportement d'un tel système, auquel cette seconde partie sera essentiellement consacrée.

3.2. *Description d'un poste à très haute tension*

Les réseaux électriques français à 400 KV et 225 KV ont une structure maillée. Les postes à très haute tension (T.H.T.) constituent les noeuds de ces réseaux. Ce paragraphe, qui a pour objet la description d'un poste T.H.T., reprend la note [TOU 76].

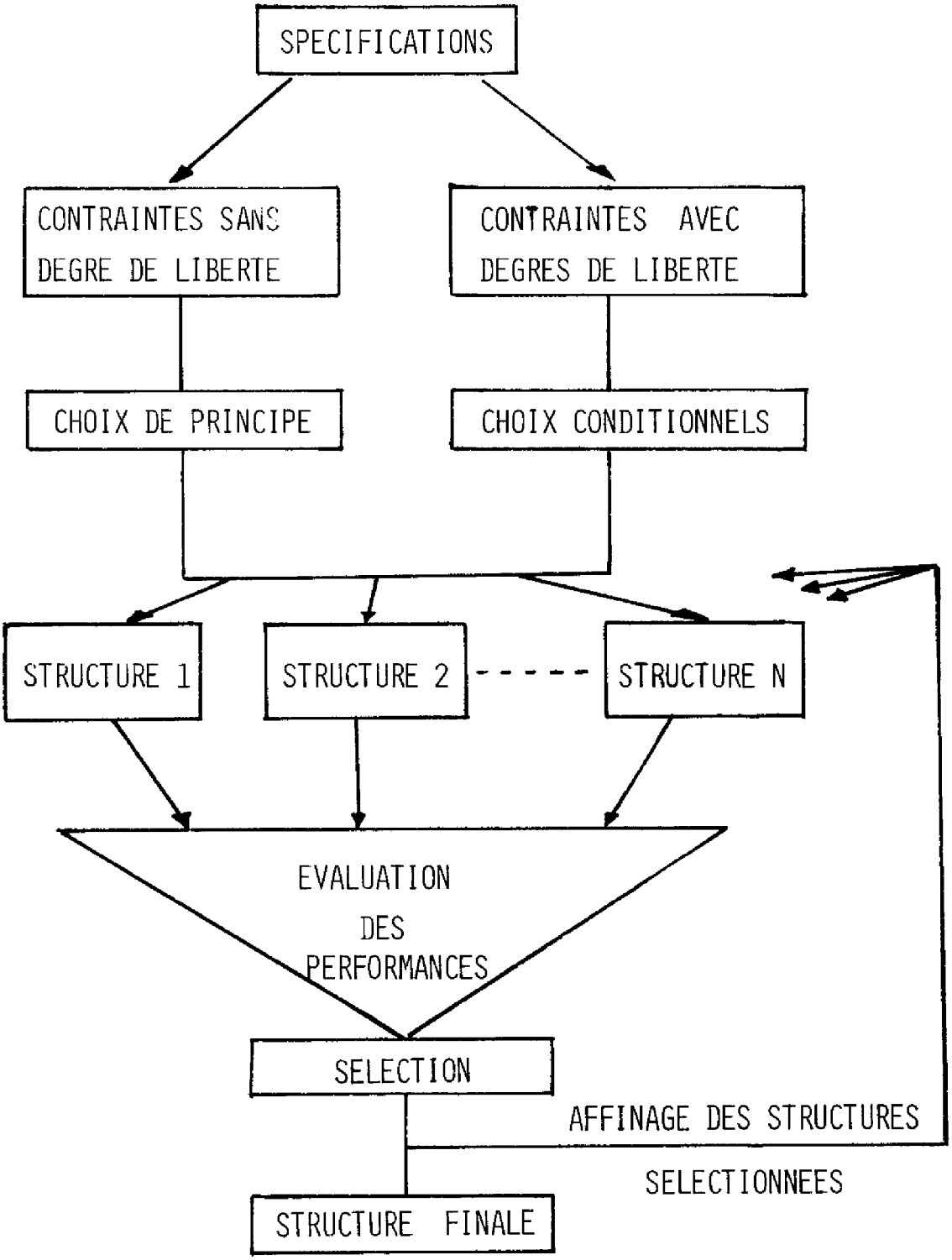


FIGURE 3.1. Méthode de conception utilisée

Le réseau de transport est un réseau triphasé à 50 HZ dont l'exploitation courante s'effectue en régime équilibré. Les ouvrages du réseau sont donc, en première approximation, organisés de façon identique pour chaque phase et on les représente fréquemment, dans un but de compréhension, par leur schéma monophasé équivalent dit "schéma unifilaire". Le schéma unifilaire d'un poste T.H.T. typique est donné par la figure 3.2. Ce schéma montre qu'un poste est constitué de matériels haute tension et de matériels basse tension ; nous allons étudier successivement la structure haute tension et la structure basse tension du poste.

3.2.1. Structure haute tension du poste T.H.T.

Les appareils de coupure marqués (1) sont des disjoncteurs. Ils sont dimensionnés pour pouvoir interrompre de forts courants en particulier les courants consécutifs à des défauts, qui peuvent atteindre 40 kA sur le réseau 400 KV alors que les courants normaux sont de l'ordre de 500 à 1000 A. Le rôle des disjoncteurs est d'assurer la sécurité des matériels.

Pour assurer la sécurité des personnes, par exemple lorsque l'on effectue des opérations d'entretien, on ne peut envisager de mettre tout ou partie d'un ouvrage hors tension uniquement à l'aide de disjoncteurs car leur pouvoir d'isolement à l'état ouvert ne les met pas à l'abri d'un réamorçage ; on utilise donc des sectionneurs, numérotés (2) sur la figure 3.2., qui, n'ayant aucun pouvoir de coupure, ne peuvent être manoeuvrés qu'à vide mais assurent un isolement parfait.

Les différentes branches du réseau qui convergent sur un poste et auxquelles on donne par convention le nom de "départs"* sont reliées par l'intermédiaire des disjoncteurs (1) et des sectionneurs (2) à un jeu de barres omnibus (3). Pour faciliter l'exploitation, un poste possède généralement deux jeux de barres, parfois trois. Un départ peut être raccordé à l'un ou l'autre de ces jeux de barres par l'intermédiaire des sectionneurs (2).

*on aurait pu dire tout aussi bien "arrivées", puisque, le réseau étant maillé, la seule chose que l'on sache a priori est que la somme algébrique des courants aux noeuds est nulle.

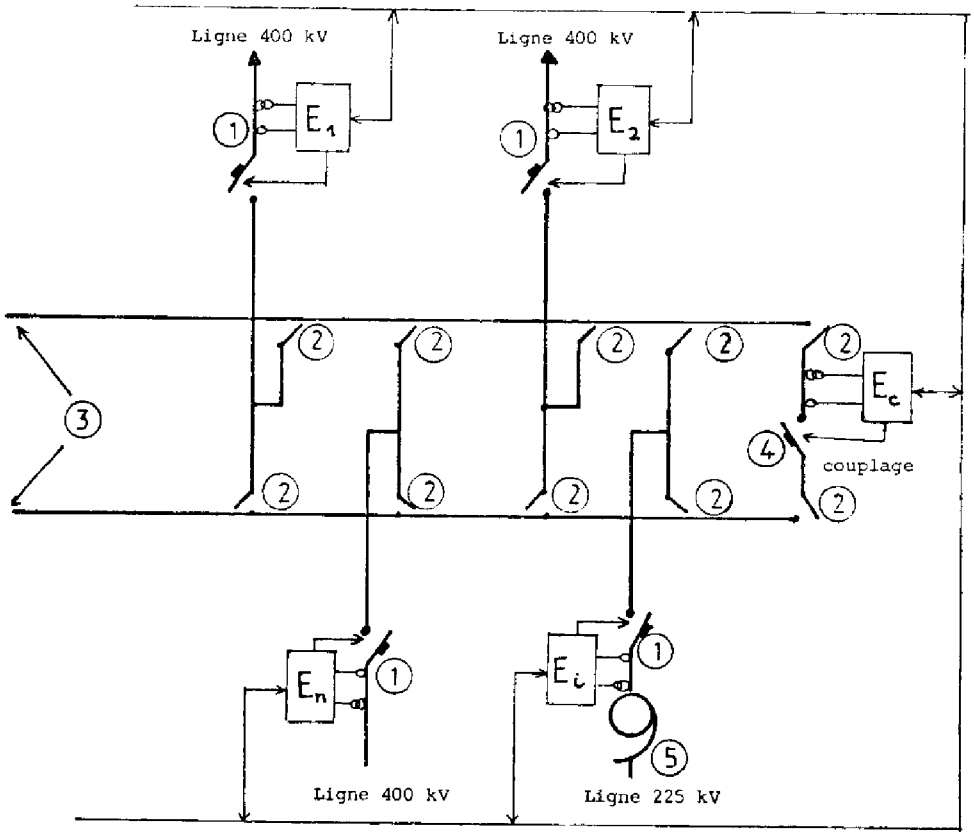


FIGURE 3.2. Schéma unifilaire d'un poste T.H.T.

Les jeux de barres peuvent être reliés entre eux par un disjoncteur de "couplage" (4) mis en série avec deux sectionneurs (2) pour les raisons mentionnées ci-dessus.

Pour assurer la continuité entre les différents niveaux de tension, on juxtapose dans une même enceinte des postes dont la structure générale est sensiblement analogue mais dont les tensions nominales sont différentes, et on les relie par l'intermédiaire d'un transformateur (5).

3.1.2. *Structure basse tension du poste : système de sécurité*

Les différents ouvrages du réseau doivent être protégés contre les courts-circuits et défauts d'isolement dont ils peuvent être le siège. De tels incidents sont en effet préjudiciables à la bonne tenue du réseau interconnecté, par les contraintes accrues qu'ils imposent au niveau des matériels, et par les risques qu'ils font courir à la stabilité d'ensemble du réseau. En effet, étant donné la structure maillée du réseau T.H.T., un défaut mal éliminé ou même éliminé trop tardivement peut conduire à une réaction en chaîne aux conséquences catastrophiques.

Le réseau étant maillé , l'élimination complète d'un défaut suppose toujours l'ouverture d'au moins deux disjoncteurs pour isoler l'ouvrage défaillant de la partie saine du réseau. L'ouverture d'un disjoncteur est commandée par l'action d'un dispositif de protection chargé de détecter les défauts. En effet, chaque départ dispose d'informations en provenance des réducteurs de courant et de tension placés au niveau de la ligne qu'ils surveillent. Ces informations permettent, grâce à des algorithmes de calcul appropriés, de savoir si la ligne est saine ou s'il y a un défaut. On peut donc connaître pour chaque départ la présence ou non d'un défaut, sa direction et sa distance par rapport au point de mesure. On a choisi, en France comme dans d'autres pays, d'assurer la protection des lignes en se fondant sur des critères ne nécessitant pas de liaison entre les deux extrémités (protection dite "de distance") de l'ouvrage protégé. On peut ainsi dire, en première approximation, que pour éliminer un défaut sur une ligne, chaque extrémité "fait son travail" à partir des mesures qu'elle effectue, indépendamment de l'autre. Chaque départ est ainsi équipé d'un dispositif de protection, souvent doublé. Il convient de remarquer qu'une protection de distance qui est en fait un calculateur d'impédance, ne donne d'ordre de déclenchement (d'ouverture) au disjoncteur associé que lorsqu'elle "voit" le défaut "à l'aval" c'est-à-dire situé du côté de la ligne qu'elle est chargée de surveiller (défaut ligne).

Les défauts affectant le jeu de barres sont extrêmement contraignants pour la stabilité du réseau, étant donné le grand nombre de lignes qui y sont impliquées : il importe donc de les éliminer rapidement. Le principe retenu en France est le traitement des informations de direction issues des

protections des départs : si toutes les protections des départs reliés à un même jeu de barres détectent un défaut "à l'amont", c'est que le défaut affecte le jeu de barres lui-même et il convient alors d'ouvrir les disjoncteurs de tous les départs reliés au jeu de barres. Pour des raisons de sûreté de fonctionnement, cette protection n'est pas assurée par un automatisme centralisé mais par un automatisme auxiliaire associé à chaque protection de départ : si la protection d'un départ voit un défaut "à l'amont", l'automatisme auxiliaire associé fera ouvrir le disjoncteur situé sous sa dépendance à moins qu'il ne reçoive une information de verrouillage émise par la protection d'un départ qui aurait vu le défaut "à l'aval" (figure 3.3.).

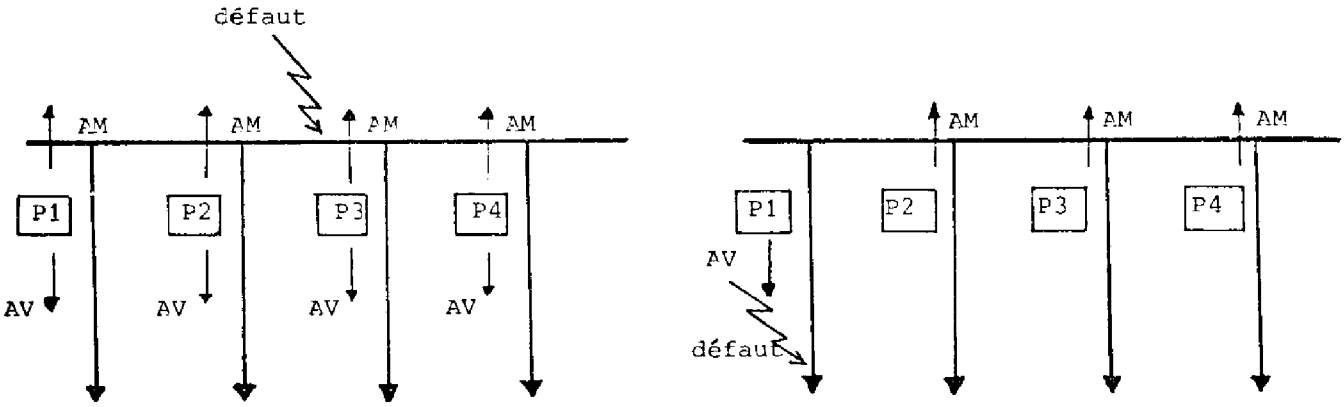
La décentralisation de la fonction des automatismes auxiliaires nécessite des échanges d'information entre les automatismes et les protections des différents départs.

Tout défaut ligne est traité en tant que défaut transitoire a priori : après ouverture du disjoncteur, il y a essai de fermeture automatique, par l'automatisme de manoeuvre du disjoncteur :

- si le défaut est transitoire, lors de la fermeture, les conditions de tension sont bonnes et le disjoncteur reste fermé ; le défaut a été éliminé après un cycle d'ouverture-fermeture,
- si le défaut est permanent, le disjoncteur ne peut rester fermé et il y a ré-ouverture : vu du système de sécurité le défaut est considéré comme étant éliminé.

Tout défaut barre est traité en tant que défaut permanent : les disjoncteurs restent ouverts pour ne pas alimenter le défaut et il n'y a pas de tentative de fermeture automatique.

L'ensemble des fonctions : protection de distance, automatisme auxiliaire et automatisme de manoeuvre du disjoncteur relatives à une ligne est appelé équipement d'un départ et l'ensemble de ces équipements forme le système de sécurité du poste ; ce système sera appelé système de commande, conformément à la terminologie d'E.D.F.



a) si toutes les protections voient le défaut à l'amont, c'est que ce défaut est sur le jeu de barres

b) P_1, P_3 et P_4 voient le défaut à l'amont mais P_1 le voit à l'aval : le défaut est sur la ligne 1

FIGURE 3.3. Défaut ligne et défaut barre

Ce système présente une redondance fonctionnelle inhérente : en effet, si, dans le cas représenté à la figure 3.2.b., le disjoncteur associé à E1 ne s'ouvre pas (soit à cause de la défaillance de E1, soit à cause de la défaillance du disjoncteur lui-même), le défaut se propage et affecte toutes les lignes aboutissant au même jeu de barres (on parle alors d'un "faux défaut jeu de barres") et le seul moyen de l'éliminer est, comme dans le cas du "vrai défaut jeu de barres" d'ouvrir tous les autres disjoncteurs reliés à ce jeu de barres : nous parlerons alors d'une élimination dégradée.

3.3. *Grandeurs caractéristiques de la sûreté de fonctionnement d'un poste T.H.T.*

Comme nous venons de le voir au paragraphe 3.2., la fonction dévolue à l'ensemble des équipements d'un poste T.H.T. est de commander l'ouverture de l'un ou des disjoncteurs associés aux départs lorsqu'un défaut est détecté par le système de protection.

Dans toute la suite, le terme "défaut" sera exclusivement utilisé pour les incidents se produisant sur les lignes ou sur les barres.

Dans les paragraphes suivants, nous déterminerons tout d'abord les états du poste puis nous définirons les grandeurs caractéristiques de la sûreté de fonctionnement.

3.3.1. Etats d'un poste T.H.T.

Les états d'un poste, d'un poste T.H.T., peuvent être caractérisés en examinant l'état des disjoncteurs. Nous avons considéré pour un disjoncteur les trois états suivants :

- état de bon fonctionnement (B),
- état de "panne", le disjoncteur étant ouvert (O),
- état de "panne", le disjoncteur étant fermé (F).

L'influence de l'état du disjoncteur sur l'état du départ n'est pas identique selon que le départ est sollicité ou non par l'occurrence d'un défaut. Le tableau de la figure 3.4. donne les différents états observables du départ par rapport à ceux du disjoncteur.

ETATS DU DISJONCTEUR / SOLLICITATION	B	O	F
non sollicité	bon fonctionnement	ligne perdue	bon fonctionnement
sollicité	bon fonctionnement	sollicitation sans action	défaut propagé

FIGURE 3.4. Etats observables d'un départ

En considérant à présent l'ensemble des départs du poste, on peut caractériser ce dernier par rapport à la sollicitation :

- en l'absence de sollicitation le poste peut être dans l'un des deux états suivants :
  - .tous les disjoncteurs sont fermés : état E1,
  - .une ou plusieurs lignes sont perdues, suite à l'ouverture intempestive d'un ou de plusieurs disjoncteurs : état E2,
- lors d'une sollicitation, nous avons trois états possibles :
  - .le défaut est éliminé correctement (ouverture des disjoncteurs concernés uniquement) : état E3,

.le défaut est éliminé en dégradé (perte de plus de sous-ensembles que le défaut ne l'exige) : état E4,

.le défaut est propagé : état E5.

Le tableau de la figure 3.5. résume tous les états E_i que peut prendre le poste.

3.2.3. *Grandeurs caractéristiques de la sûreté de fonctionnement*

Dans le paragraphe 1.4., nous avons défini deux niveaux de sûreté de fonctionnement :

niveau 1 : le système de commande du poste est capable d'éliminer un défaut,

niveau 2 : le système de commande du poste est capable d'éliminer un défaut et n'a pas d'action intempestive sur les disjoncteurs en l'absence de défaut.

Or, en l'absence de défaut, l'ouverture d'un disjoncteur entraîne la perte de la ligne correspondante ce qui n'est pas catastrophique pour la stabilité du réseau étant donné que ce dernier est maillé. Le niveau 2 n'est donc pas une grandeur très importante pour le poste. La seule grandeur que nous retiendrons est le niveau 1. Cependant, vu la redondance fonctionnelle du système (possibilité d'élimination dégradée d'un défaut) deux mesures sont à considérer pour tenir compte de cette possibilité de dégradation. Ces deux mesures sont définies comme suit :

- sûreté de fonctionnement nominale : probabilité d'éliminer les défauts en n'ouvrant que les disjoncteurs concernés :
  .états de succès : E1, E2 et E3
  .états de non succès : E4 et E5
- sûreté de fonctionnement dégradée : probabilité de non propagation des défauts à travers le réseau :
  .états de succès : E1, E2, E3 et E4
  .états de non succès : E5.

Pour ces deux mesures, les états de non succès sont des états absorbants.

ETAT / SOLLICITATION	E1	E2	E3	E4	E5
non sollicité	pas de ligne perdue	une ligne au moins perdue			
Défaut ligne			ligne en défaut isolée : ouverture du disjoncteur associé à cette ligne, tous les autres restant fermés	le disjoncteur de la ligne en défaut n'est pas ouvert ; ouverture de tous les disjoncteurs des lignes reliées à la même barre, et du disjoncteur de couplage	le disjoncteur de la ligne en défaut ne s'est pas ouvert, ainsi que un ou plusieurs disjoncteurs des lignes reliées à la même barre : le défaut est propagé sur le réseau
Défaut barre			barre en défaut isolée : ouverture des disjoncteurs de toutes les lignes reliées à cette barre et du disjoncteur de couplage	le disjoncteur de couplage ne s'est pas ouvert ; ouverture de tous les disjoncteurs des lignes reliées aux deux barres	au moins un disjoncteur de ligne ne s'est pas ouvert et le défaut et propagé sur le réseau

FIGURE 3.5. Etats du poste

4. EVALUATION DE LA SURETE DE FONCTIONNEMENT DU SYSTEME ACTUEL

Afin de pouvoir proposer de nouvelles architectures pour la structure basse tension du poste, il est nécessaire d'étudier le comportement du système actuel et de dégager les paramètres les plus significatifs pour un tel système.

Pour la modélisation du système actuel, nous ne tiendrons pas compte des communications entre les différents départs du poste, car nous avons affaire à des liaisons fil à fil, et les informations échangées entre ces départs possèdent une certaine redondance ; la perte globale de cette communication a une probabilité négligeable.

On fera l'hypothèse que tous les départs du poste ont le même modèle.

Etant donné la complexité des phénomènes mis en jeu, nous suivrons une approche ascendante pour la modélisation du poste. Nous examinerons donc successivement :

- l'équipement d'un départ,
- l'ensemble des équipements d'une barre,
- le poste entier.

4.1. *Modélisation d'un départ*

Si nous considérons l'équipement d'un départ pris tout seul, la notion d'élimination dégradée n'a plus de sens : nous avons donc une seule mesure de sûreté de fonctionnement pour un départ, cette mesure correspond à $D_1(t)$, défini dans 1.6. :

$D_1(t) = \mathcal{P}\{$ le système élimine correctement un défaut $\}$

La modélisation d'un départ se base sur les résultats obtenus dans la première partie : nous ne tiendrons compte que de deux fautes masquées successives pour un départ. Toutefois, la politique de maintenance préventive adoptée à E.D.F. est différente de celle énoncée dans le paragraphe 2.3.1. ;

elle sera donc détaillée dans le paragraphe suivant. Nous donnerons ensuite l'ordre de grandeur des différents paramètres associés au poste.

4.1.1. Maintenance préventive

Dans le système actuel, les équipements ne sont pas tolérants aux fautes. Pour chaque équipement, la détection de faute est basée sur la cohérence des informations en provenance des équipements reliés à la même barre. Dans le but de minimiser l'influence des fautes masquées, les équipements sont inspectés à intervalles réguliers ; soit $1/\delta$ la valeur moyenne de cet intervalle de temps. Pendant l'inspection, le départ est consigné.

4.1.2. Valeur des paramètres associés au poste

Pour l'évaluation de la sûreté de fonctionnement, nous prendrons pour les paramètres associés aux processus agissant sur le poste, les valeurs communément utilisées à E.D.F. [ACT 76] :

- taux de faute d'un départ : $\lambda = 10^{-4}$/h soit une faute par an en moyenne,
- taux d'occurrence d'un défaut ligne :
  - .sur les lignes sans câble de garde (le câble de garde sert à protéger la ligne de la foudre) $\gamma_\ell = 10^{-3}$ défaut/h, soit dix défauts par an en moyenne,
  - .sur les lignes avec câble de garde $\gamma_\ell = 2.10^{-4}$ défaut/h, soit en moyenne deux défauts par an,
- taux d'occurrence d'un défaut barre : $\gamma_b = 10^{-5}$ défaut/h, soit un défaut tous les dix ans en moyenne,
- temps moyen d'élimination d'un défaut $1/\xi$, $\xi = 10^{+3}$/h, soit trois secondes environ (ce temps correspond au temps de manoeuvre des disjoncteurs et ne tient pas compte du temps nécessaire à la suppression de la cause du défaut dans le cas des défauts permanents),
- taux d'inspection : $\delta = 10^{-4}$ à 4.10^{-4}/h, soit une à quatre inspections en moyenne par an,
- taux de réparation $\mu = 10^{-2}$ à 4.10^{-2}/h, soit une durée de réparation de l'ordre de quelques jours.

Le tableau de la figure 4.1. récapitule les différents taux utilisés, leur définition et leur valeur.

PROCESSUS	TAUX	SIGLE	VALEUR
SOLLICITATION	Taux d'occurrence d'un défaut ligne	γ_ℓ	10^{-4}/h à 10^{-3}/h
	Taux d'occurrence d'un défaut barre	γ_b	10^{-5}/h
	Temps moyen d'élimination d'un défaut	$1/\xi$	$\xi = 10^{+3}$/h
MANIFESTATION DE FAUTES	Taux de fautes d'un départ	λ	10^{-4}/h
MAINTENANCE	Taux d'inspection à intervalles réguliers	δ	10^{-4}/h à 4.10^{-4}/h
	Taux de réparation	μ	10^{-2}/h à 4.10^{-2}/h

FIGURE 4.1. Définition et valeur des taux relatifs au poste

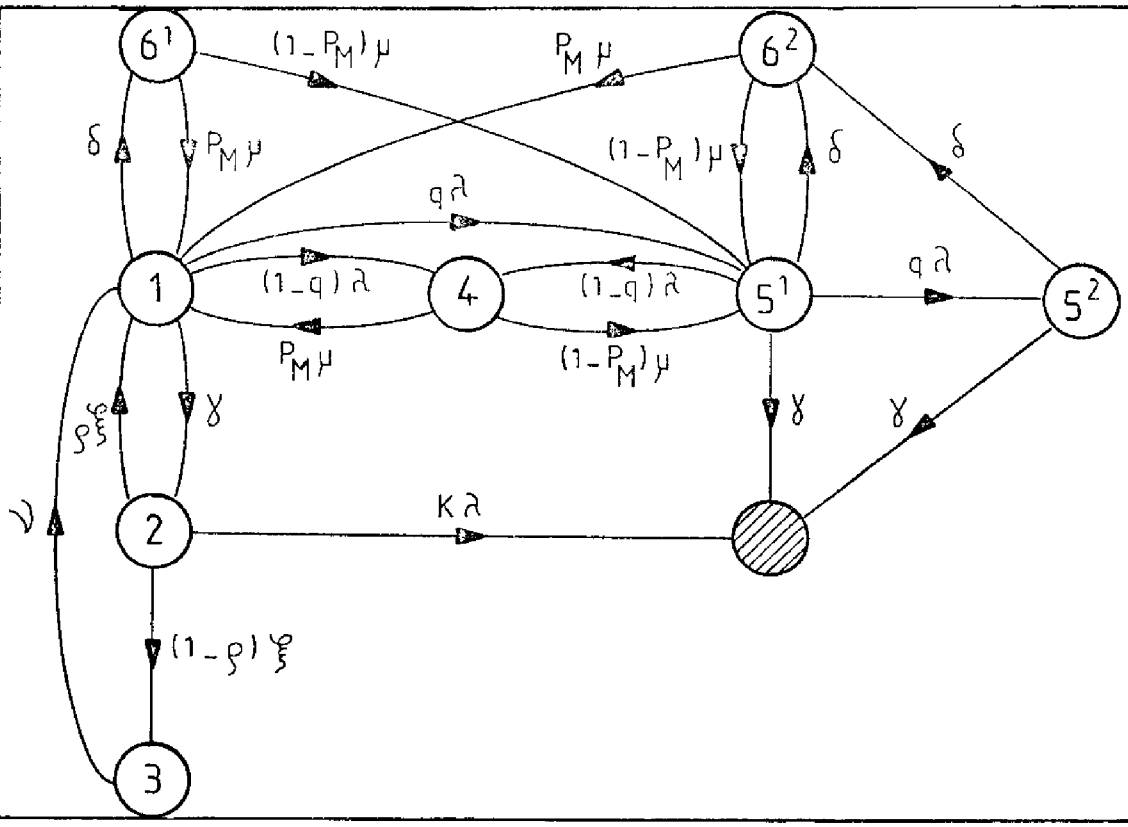
Aucune statistique ne permet de connaître l'exacte valeur de q_o, P_D et P_m. Nous étudierons l'influence de leur variation.

La probabilité p qu'une faute soit transitoire ainsi que le temps de maintenance $1/\nu$ n'interviennent pas, étant donné que $K\ \gamma/\xi \leq 5.10^{-5}$ alors que q et $(1-P_m)$ sont au moins supérieurs à 10^{-3} (cf. 2.3.3.2.).

4.1.3. Graphe complet de l'équipement d'un départ

Le graphe d'un départ se déduit du graphe de la figure 2.10. en ajoutant les états d'inspection à intervalles réguliers : états (6i) . Ce graphe est donné à la figure 4.2. L'inspection du système ne peut avoir lieu que dans l'état de bon fonctionnement ou dans les états de fautes masquées (5¹) et (5²) . Nous supposons que l'opérateur peut, soit introduire une faute dans le système lors de l'inspection : transition de (6¹) vers (5¹) , soit mal réparer le système : transition de (6²) vers (5¹) . Nous supposons aussi qu'une mauvaise réparation amène le système dans un état à une seule faute masquée : état (5¹) .

GRAPHE



ETATS

(1) bon état de fonctionnement en l'absence de défaut

(2) traitement d'un défaut

(3) ligne isolée suite à un défaut ligne permanent ou à un défaut barre

(4) ligne perdue suite à une ouverture intempestive du disjoncteur

(5^i) équipement d'une ligne incapable d'éliminer un défaut:

- i=1 une seule faute masquée
- i=2 deux fautes masquées successives

(6^i) inspection du départ ,ligne isolée

FIGURE 4-2 Graphe complet d'un départ

Ce graphe a au total neuf états ; si l'on suppose que l'on a n départs reliés à une barre, on aura pour cette dernière a priori 9^n états et pour un poste à deux barres et un disjoncteur de couplage un graphe à 9^{2n+1} états. En fait, parmi ces 9^{2n+1} états, certains sont identiques et pourront être, de ce fait, regroupés. On peut, par exemple, regrouper tous les états où i départs sur une même barre sont en défaillance déclarée et (n-i) en bon état de fonctionnement, ce qui nous fait au total $(\sum_{i=1}^{n} C_n^i)$-n états en moins ; ce nombre est à multiplier par deux si on considère le poste. Nous pourrons donc réduire, de proche en proche, le graphe en regroupant les états identiques ; néanmoins, le nombre d'états résultant reste assez élevé. Ceci nous amène à réduire le nombre d'états du modèle, tout en gardant un modèle représentatif.

4.1.4. Réduction du graphe d'un départ

Partant du graphe de la figure 4.2., nous avons suivi la même approche que celle utilisée dans 2.3.3. ; il en résulte que :

- les états (2) et (3) du graphe de la figure 4.2. peuvent être supprimés,
- le temps de réparation $1/\mu$ peut être considéré comme étant nul.

Le graphe réduit résultant ne comporte que quatre états ; il est donné à la figure 4.3. Nous avons renuméroté les états :

- l'état (2) remplace l'état (5^1) de la figure 4.2.,
- l'état (3) remplace l'état (5^2) de la figure 4.2.,
- l'état (D) représente l'état défaillant : état de non élimination d'un défaut.

Ce dernier graphe rend néanmoins compte de tous les processus qui ont une influence sur le système. Les transitions entre ces états sont relatives aux processus suivants :

- transition état (1) vers état (2) : le terme $q\lambda$ correspond à l'occurrence d'une faute masquée, le terme $(1-q)(1-P_m)\lambda$ correspond à une panne déclarée et mal réparée, et le terme $\delta(1-P_m)$ correspond à une inspection qui a dégradé le système,

- transition état (2) vers état (1) : cette transition se fait par l'occurrence d'une panne déclarée et bien réparée : terme $P_m(1-q)\lambda$, ou par une bonne réparation après inspection : $P_m\delta$,
- transition état (2) vers état (3) : une deuxième panne masquée a eu lieu,
- transition état (3) vers état (2) : le système a été inspecté et mal réparé,
- transition état (3) vers état (1) : le système a été inspecté et bien réparé,
- transitions état (2) et état (3) vers état (D) : le système est sollicité par un défaut.

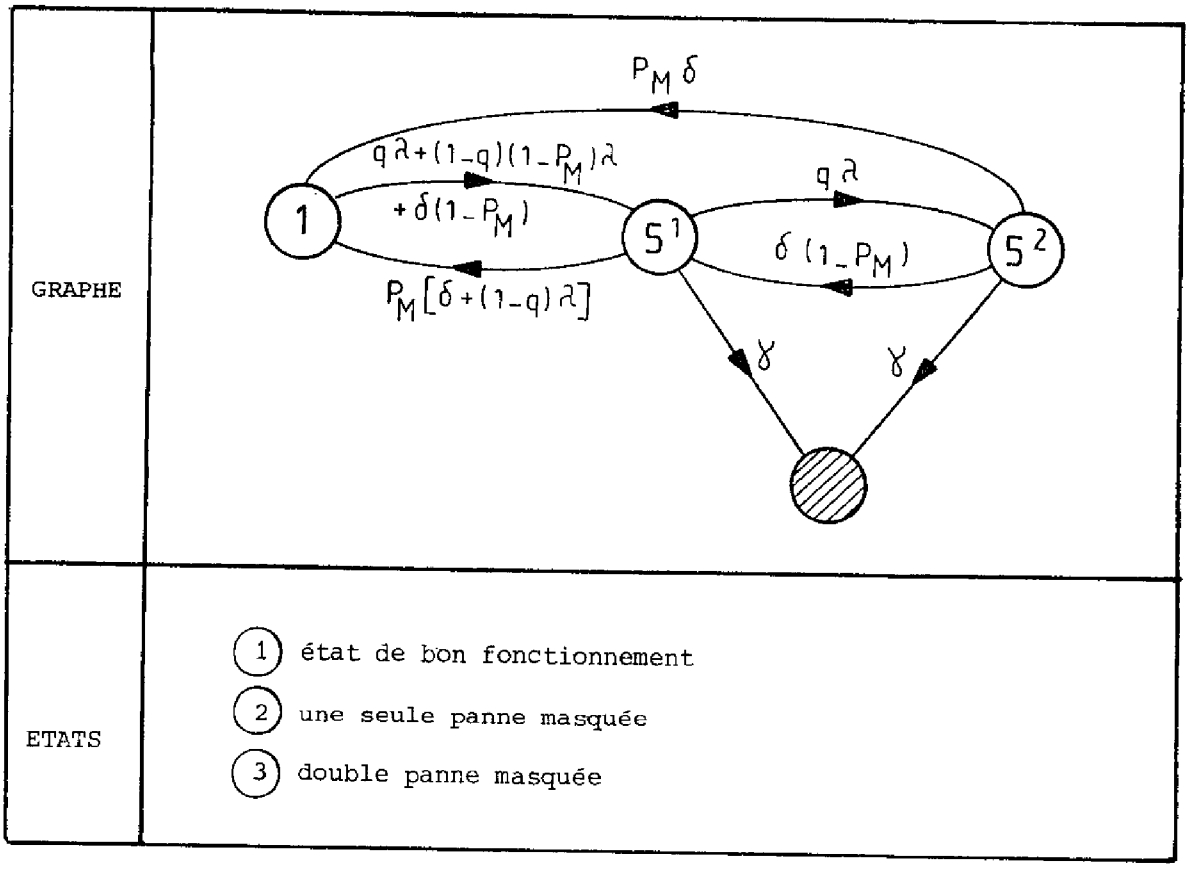


FIGURE 4.3. Graphe réduit d'un départ

Nous avons tracé $D_1(t)$ pour le modèle complet de la figure 4.2. et pour le modèle réduit de la figure 4.3. La figure 4.4. montre que les résultats obtenus sont très voisins, et que le modèle réduit suffit à rendre compte des caractéristiques de sûreté de fonctionnement pour un départ.

C'est ce dernier modèle qui servira de base à l'établissement du modèle relatif aux départs reliés à une même barre.

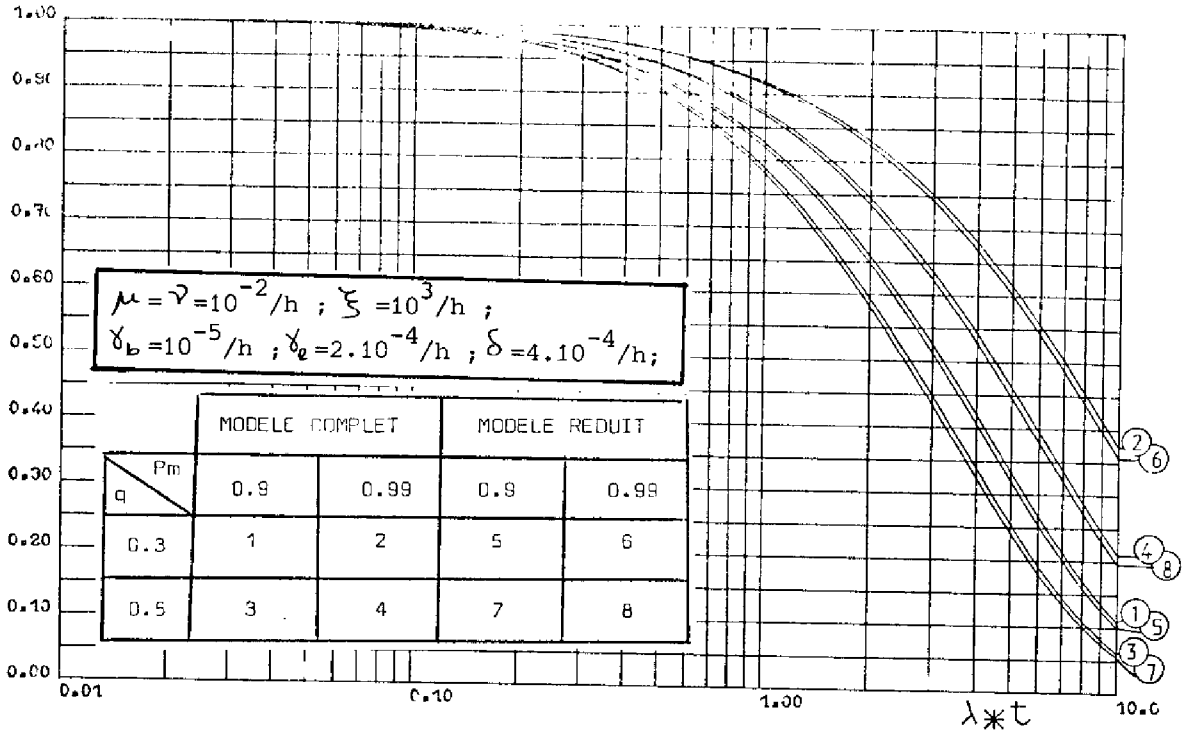


FIGURE 4.4. $D_1(t)$ pour le modèle complet et le modèle réduit

4.2. *Modélisation de l'ensemble des départs reliés à une barre*

Ayant établi, dans la partie précédente, un graphe représentatif simplifié du modèle d'un départ, nous établirons de la même façon, dans cette partie, un graphe représentatif de l'ensemble des départs reliés à une même barre, et nous évaluerons la sûreté nominale et la sûreté dégradée.

4.2.1. Modèle complet d'une barre

Le modèle d'une barre s'obtient à partir du modèle d'un départ qui est présenté à la figure 4.3., en considérant n sous-ensembles identiques, où n représente le nombre de départs reliés à la barre.

Le modèle d'un départ comportant quatre états, le modèle de la barre en aura 4^n a priori. En réalité, après regroupement de tous les états identiques, ce nombre est nettement inférieur à 4^n. Cependant, l'opération de regroupement est une source d'erreurs supplémentaires et elle est fastidieuse ; c'est pour cela que nous avons adopté une méthode progressive de construction du modèle, fondée sur l'analyse des phénomènes rencontrés.

4.2.1.1. Politique d'inspection

a) L'inspection de la barre à intervalles réguliers se fait de façon globale pour tous les départs et peut entraîner une dégradation de l'état du système :

- une inspection ramenant le système dans un état de bon fonctionnement se traduit par une transition $P_m^n \delta$, où n indique le nombre de départs,
- une inspection mettant ou laissant j départs en panne se traduit par une transition : $C_n^j \; P_m^{(n-j)} \; (1-P_m)^j \; \delta$.

b) A partir du moment où une panne est déclarée, on inspecte tous les départs. Cette inspection/réparation peut aussi entraîner des dégradations.

Pour alléger l'expression des transitions dans les graphes d'état, nous introduisons un état d'inspection/réparation ; c'est l'état (2) dans tous les graphes suivants :

- une inspection/réparation ramenant le système dans un état de bon fonctionnement se traduit par $P_m^n \delta$,
- si au contraire, elle met j départs en panne, la transition de (2) vers l'état où il y a j départs en panne se fait par $C_n^j \; P_m^{n-j} \; (1-P_m)^j \; \delta$.

Pour le tracé des courbes de sûreté, μ sera pris égal à l'infini, conformément aux résultats du paragraphe précédent (cf. 4.1.4.).

Notation utilisée :

Dans la suite du mémoire, nous adopterons la notation suivante :

$R_i = \mathcal{P}\{$ l'inspection/réparation est effectuée correctement sur (n-i) départs$\}$

$= \mathcal{P}\{$ l'inspection/réparation laisse i départs en panne $\}$.

L'expression "laisse i départs en panne" signifie que i départs sont dans un état de panne simple masquée à la fin de la réparation et peuvent tomber une seconde fois en panne, la seconde panne pouvant être déclarée ou masquée ; soit :

$$R_o = P_m^n$$

$$R_1 = C_n^1 \, P_m^{n-1} \, (1-P_m)$$

$$R_2 = C_n^2 \, P_m^{n-2} \, (1-P_m)^2$$

$$R_i = C_n^i \, P_m^{n-i} \, (1-P_m)^i$$

$$R_n = (1-P_m)^n$$

4.2.1.2. Etablissement du modèle

Afin de faciliter la compréhension du modèle, nous avons procédé en deux étapes :

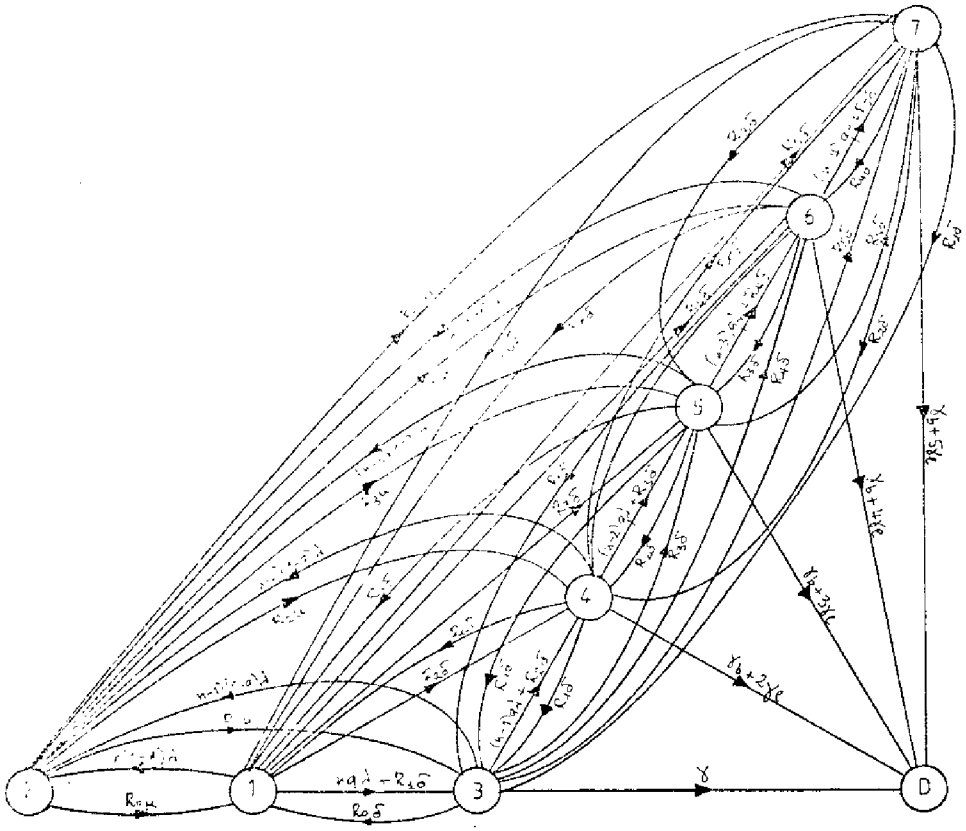
- modèle prenant en compte les pannes de tous les départs mais une seule panne par départ,
- modèle prenant en compte les pannes de tous les départs, et deux pannes par départ.

Pour l'établissement de ces modèles, nous prendrons n=5, ce qui correspond à un poste type, ayant deux barres et dix départs.

Le premier modèle, donné à la figure 4.5., dérive du modèle d'un départ (cf. figure 4.3.) et tient compte de la politique d'inspection/réparation définie au paragraphe 4.2.1.1.

Le graphe de la figure 4.5. est en fait valable à la fois pour la sûreté nominale et la sûreté dégradée. En effet, la différence entre ces modèles réside dans la définition de l'état défaillant (D).

GRAPHE



ETATS

(1) : état de bon fonctionnement
(2) : inspection/réparation après une panne déclarée
(3) : un départ en panne simple masquée
(4) : deux départs en panne simple masquée
(5) : trois départs en panne simple masquée
(6) : quatre départs en panne simple masquée
(7) : cinq départs en panne simple masquée
(D) : état défaillant

$\gamma = \gamma_b + \gamma_e$ pour la sûreté nominale

$\gamma = \gamma_b$ pour la sûreté dégradée

FIGURE 4.5. Graphe représentatif d'une barre avec prise en compte des pannes simples de tous les départs.

- lorsque l'on s'intéresse à la sûreté nominale (cf. 3.2.2.), l'état d'élimination du défaut par ouverture de plus de disjoncteurs que le défaut ne l'exige est défaillant, et par conséquent, cet état est regroupé avec l'état de non-élimination du défaut en un seul état (D),
- lorsque l'on s'intéresse à la sûreté dégradée (cf. 3.2.2.), seule la non-élimination du défaut est considérée comme défaillante, et l'état (D) ne représente que l'état de propagation du défaut.

Comportement à partir de l'état (1) : une panne déclarée sur l'un quelconque des départs amène le système dans l'état (2), le taux de transition correspondant étant $n\,(1-q)\lambda$.

Une panne masquée (terme $nq\lambda$), ou une dégradation suite à une inspection (terme $R_1\,\delta$), amènent le système dans l'état (3).

Des dégradations suite à une inspection amènent le système dans les états (4), (5), (6) et (7) suivant le nombre de départs laissés en panne.

Comportement à partir de l'état (2) : de cet état d'inspection/réparation, on va vers tous les autres états (sauf l'état (D)) avec un taux de transition $R_i\,\delta$, i dépendant du nombre de départs laissés en panne.

Comportement à partir de l'état (3) : cet état correspond au système avec un départ en panne masquée. Une panne déclarée de l'un quelconque des (n-1) autres départs amène le système dans l'état (2) ; le taux de transition est $(n-1)(1-q)\lambda$.

Une panne masquée de l'un quelconque des (n-1) autres départs amène le système dans l'état (4), le taux de transition étant $(n-1)\,q\,\lambda$. Une bonne réparation après inspection amène le système dans l'état (1).

Les mauvaises réparations après inspection amènent le système dans les états (4), (5), (6) et (7) suivant le nombre de départs laissés en panne.

Lorsque le système est sollicité par un défaut, on va dans l'état défaillant (D). Le taux de transition γ est en fait différent selon qu'on s'intéresse à la sûreté nominale ou dégradée :

- pour la sûreté nominale, nous avons $\gamma = \gamma_b + \gamma_\ell$, ce qui correspond à la sollicitation par un défaut barre, ou par un défaut ligne sur le départ en panne,
- pour la sûreté dégradée, nous avons $\gamma = \gamma_b$ car nous admettons l'élimination de façon dégradée, c'est-à-dire l'élimination par ouverture de plus de disjoncteurs que le défaut ne l'exige.

Comportement à partir des états (4), (5) et (6) : une panne déclarée amène le système dans l'état (2) ; le taux de transition est $(n-i)(1-q)\lambda$, où i est le nombre de départs en panne.

Une panne masquée provoque le passage du système de l'état correspondant à i départs en panne à l'état correspondant à (i+1) départs en panne, le taux de transition étant $(n-i)q\lambda$.

Une bonne réparation après inspection amène le système dans l'état (1) .

Les mauvaises réparations après inspection amènent le système dans les états (3), (4), (5), (6) et (7) suivant le nombre de départs laissés en panne.

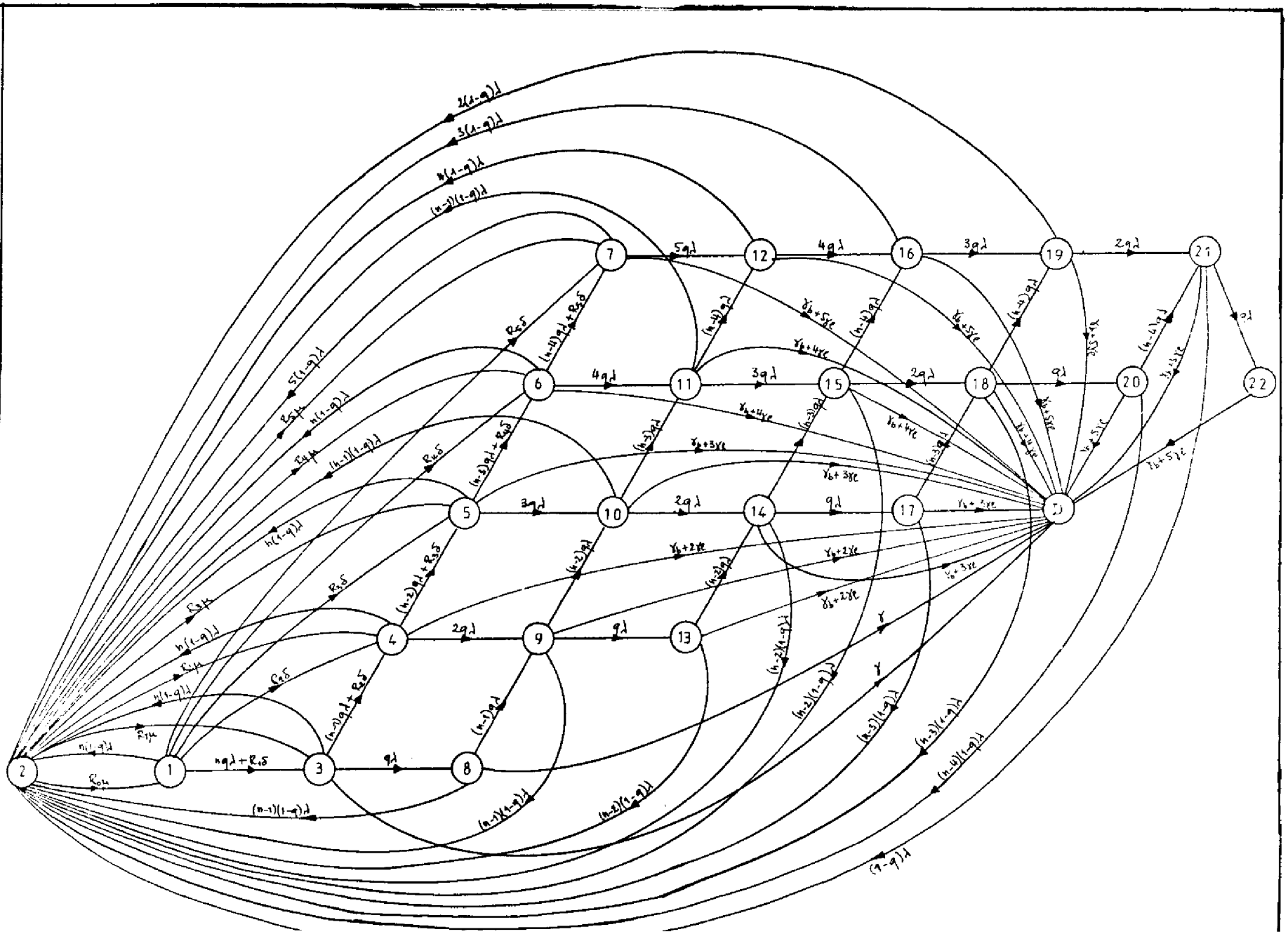
La sollicitation sur défaut amène le système dans l'état (D) ; le taux de transition est $\gamma_b + i\,\gamma_\ell$, où i représente le nombre de départs en panne.

Comportement à partir de l'état (7) : tous les départs étant en panne masquée, seuls les processus d'inspection et de sollicitation interviennent dans cet état.

Une bonne réparation ramène le système dans l'état (1) ; les mauvaises réparations amènent le système dans les états (3), (4), (5), (6) et (7) suivant le nombre de départs laissés en panne.

Pour obtenir le modèle complet d'une barre, il faut considérer la seconde panne de chaque départ ; le graphe de la figure 4.5. est modifié en conséquence et nous obtenons alors celui de la figure 4.6.

GRAPHE


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
nq\lambda + R_{1,5}
q\lambda
2q\lambda
3q\lambda
4q\lambda
5q\lambda
\gamma_6 + 2\gamma_\epsilon
\gamma_6 + 3\gamma_\epsilon
\gamma_6 + 4\gamma_\epsilon
\gamma_6 + 5\gamma_\epsilon
\gamma
2\gamma
3\gamma
4\gamma
5\gamma
(n-1)(1-q)\lambda
(n-2)(1-q)\lambda
(n-3)(1-q)\lambda
(n-4)(1-q)\lambda
(q-q)\lambda

ETATS

(1) : état de bon fonctionnement
(2) : état d'inspection/réparation après une panne déclarée
(3) : un seul départ en panne simple
(4) : deux departs en panne simple
(5) : trois départs en panne simple
(6) : quatre départs en panne simple
(7) : cinq départs en panne simple
(8) : un départ en panne double
(9) : un départ en panne double et un en panne simple
(10) : un départ en panne double et deux en panne simple
(11) : un départ en panne double et trois en panne simple
(12) : un départ en panne double et quatre en panne simple
(13) : deux départs en panne double
(14) : deux départs en panne double et un en panne simple
(15) : deux départs en panne double et deux en panne simple
(16) : deux départs en panne double et trois en panne simple
(17) : trois départs en panne double
(18) : trois départs en panne double et un en panne simple
(19) : trois départs en panne double et deux en panne simple
(20) : quatre départs en panne double
(21) : quatre départs en panne double et un en panne simple
(D) : état défaillant

N.B. tous les états de panne correspondent à des pannes masquées.

$\gamma = \gamma_b + \gamma_\ell$ pour la sûreté nominale , $\gamma = \gamma_b$ pour la sûreté dégradée

L'inspection/réparation à intervalles réguliers dans les états (3) à (22) n'est pas représentée sur le graphe. De tous ces états il y a une transition vers les états : (1) par $R_0\delta$, (3) par $R_1\delta$, (4) par $R_2\delta$, (5) par $R_3\delta$, (6) par $R_4\delta$, (7) par $R_5\delta$.

FIGURE 4.6. Graphe représentatif d'une barre avec prise en compte des pannes de tous les départs.

L'inspection du système dans les états de panne double (états (8) à (22)) le ramène dans les états de panne simple (états (3) et (7)) en cas de mauvaise réparation. Ceci est dû au fait que nous avons fait l'hypothèse qu'un départ pouvait avoir deux pannes masquées avant d'être sollicité.

Ce modèle complet est bien sûr valable pour la sûreté nominale et la sûreté dégradée ; seuls les taux de transition à partir des états (3) et (8) vers l'état défaillant sont différents ; ils valent $\gamma_e + \gamma_b$ pour la sûreté nominale, et γ_b pour la sûreté dégradée.

4.2.2. *Simplification des modèles*

La probabilité que le système soit dans un état correspondant à la panne simple ou double de plusieurs départs décroît avec le nombre de départs en panne. Nous avons donc effectué, dans le but de simplifier le modèle de la figure 4.6., une étude de sensibilité, en examinant successivement l'influence sur la sûreté nominale et la sûreté dégradée :

- du nombre de départs dont la panne est prise en compte,
- des modes de panne (simple ou double) de chaque départ.

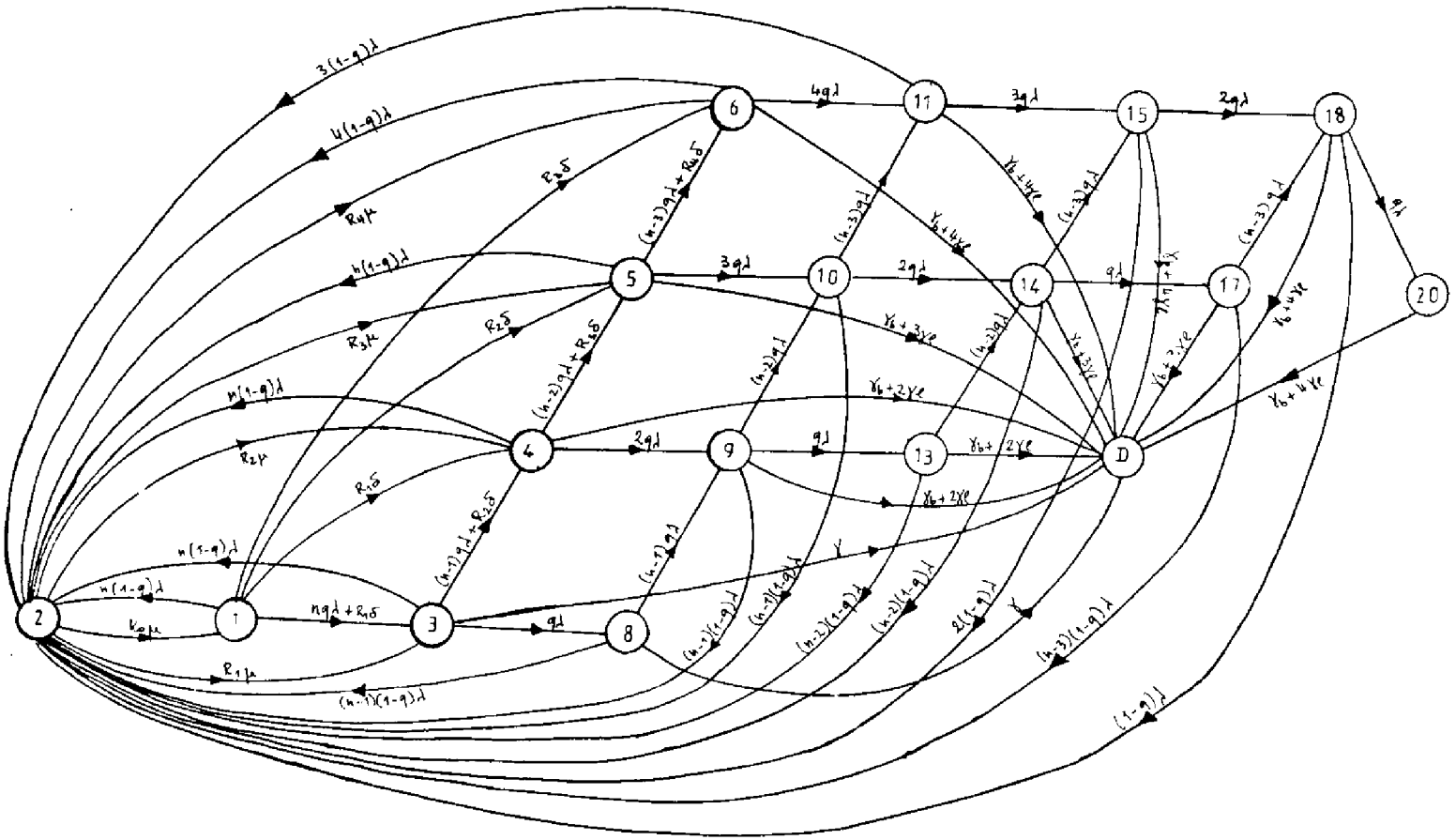
4.2.2.1. *Influence du nombre de départs dont la panne est prise en compte*

A partir du graphe de la figure 4.6. par suppression de certains des états, nous avons déterminé les modèles prenant en compte un nombre décroissant de départs en panne :

- le graphe d'état de la figure 4.7. correspond au modèle avec quatre départs en panne,
- le graphe de la figure 4.8. à un modèle avec trois départs en panne,
- le graphe de la figure 4.9. à un modèle avec deux départs en panne,
- le graphe de la figure 4.10. à un modèle avec un seul départ en panne.

Pour tous ces graphes, la différence entre les modèles de la sûreté nominale et la sûreté dégradée réside dans les taux de transitions entre les états (3) et (8) et l'état défaillant (D).

GRAPHE


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
20
D
nqλ + R₁δ
qλ
2qλ
3qλ
4qλ
(n-1)qλ + R₂δ
(n-2)qλ + R₃δ
(n-3)qλ + R₄δ
n(1-q)λ
2(1-q)λ
3(1-q)λ
4(1-q)λ
(n-1)(1-q)λ
(n-2)(1-q)λ
(n-3)(1-q)λ
R₁μ
R₂μ
R₃μ
R₄μ
R₁δ
R₂δ
R₃δ
R₄δ
γ
γ₆ + 2γ₈
γ₆ + 3γ₈
γ₆ + 4γ₈

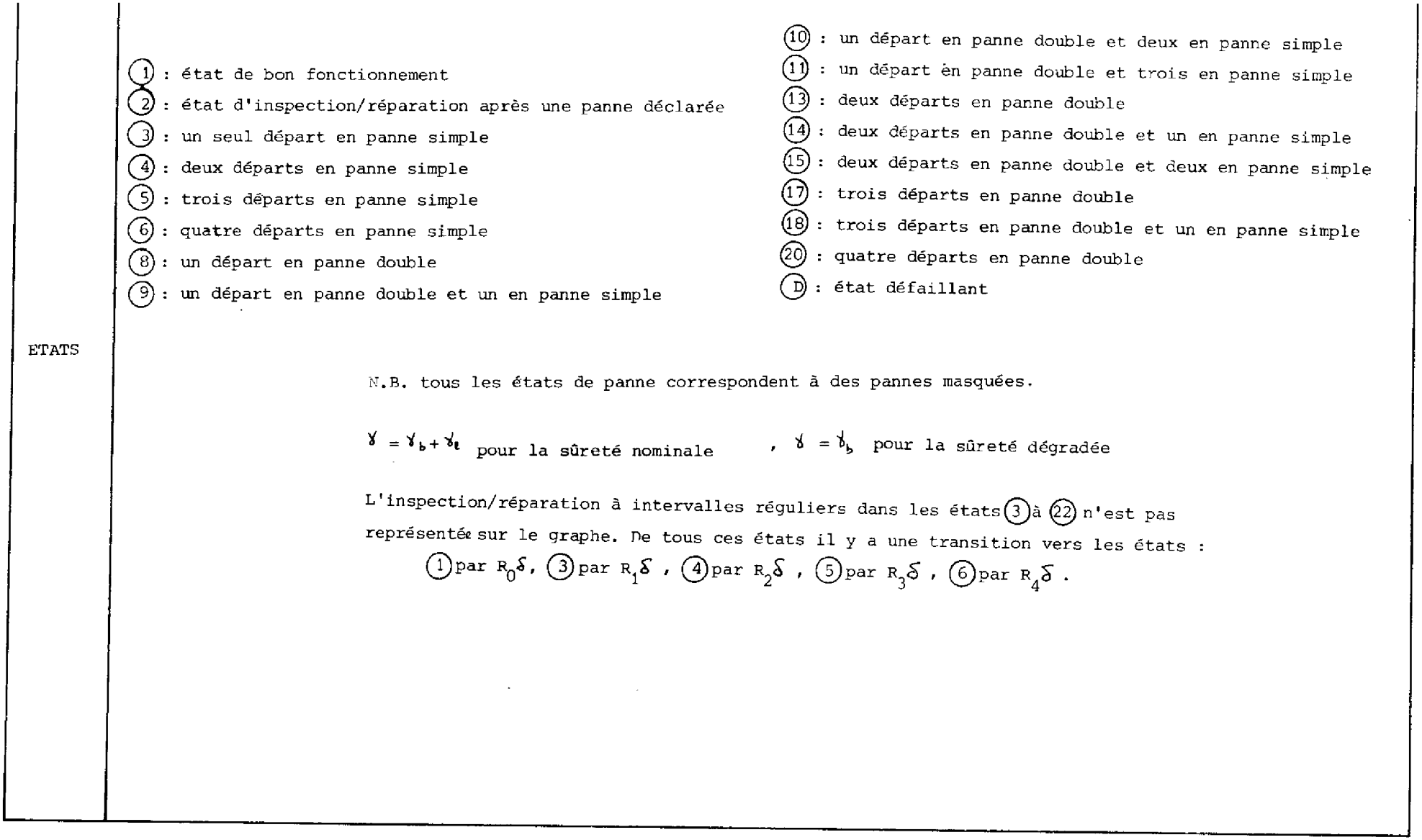
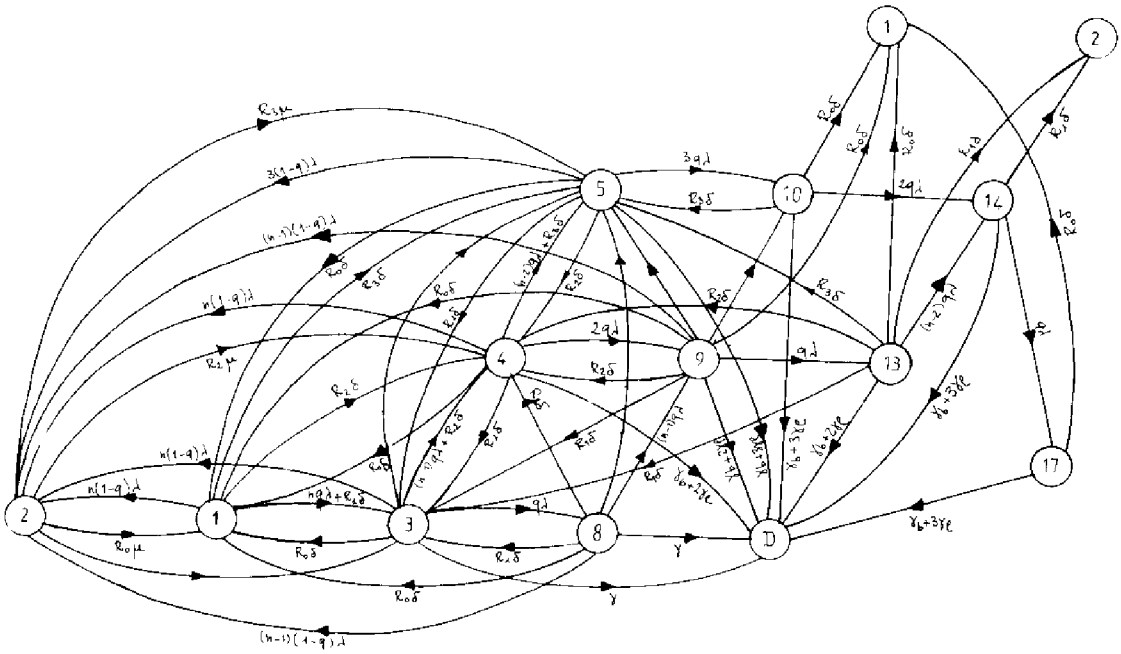


FIGURE 4.7. Graphe représentatif d'une barre avec prise en compte des pannes de quatre départs.

GRAPHE



ETATS

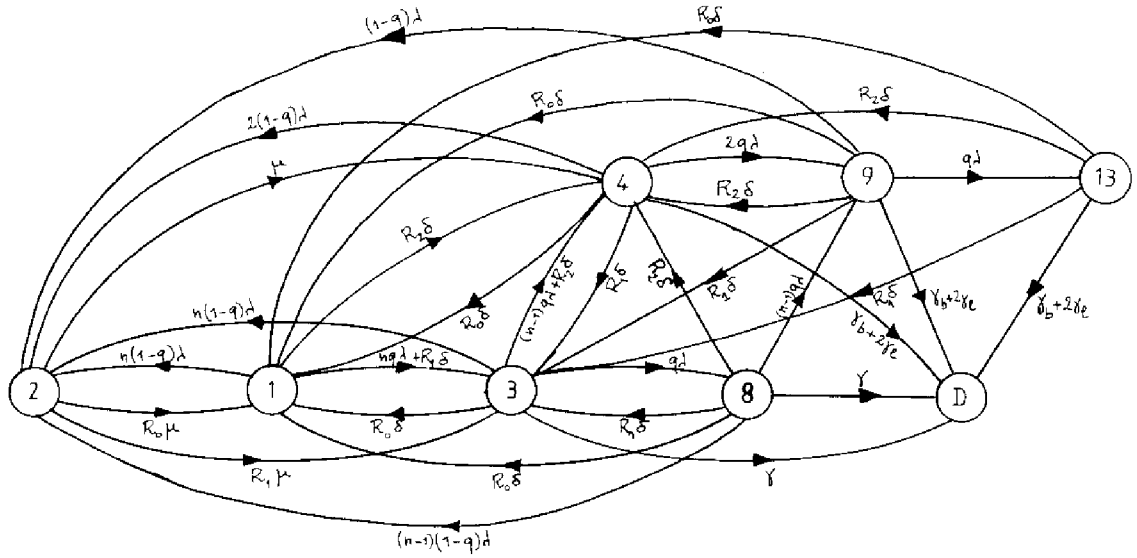
(1) : état de bon fonctionnement
(2) : inspection/réparation après une panne déclarée
(3) : un départ en panne simple
(4) : deux départs en panne simple
(5) : trois départs en panne simple
(8) : un départ en panne double
(9) : un départ en panne double et un en panne simple
(10) : un départ en panne double et deux en panne simple
(13) : deux départs en panne double
(14) : deux départs en panne double et un en panne simple
(17) : trois départs en panne double
(D) : état défaillant

N.B. Tous les états de panne correspondent à des pannes masquées.

$\gamma = \gamma_b + \gamma_e$ pour la sûreté nominale
$\gamma = \gamma_b$ pour la sûreté dégradée

FIGURE 4.8. Graphe représentatif d'une barre avec prise en compte des pannes de trois départs.

GRAPHE



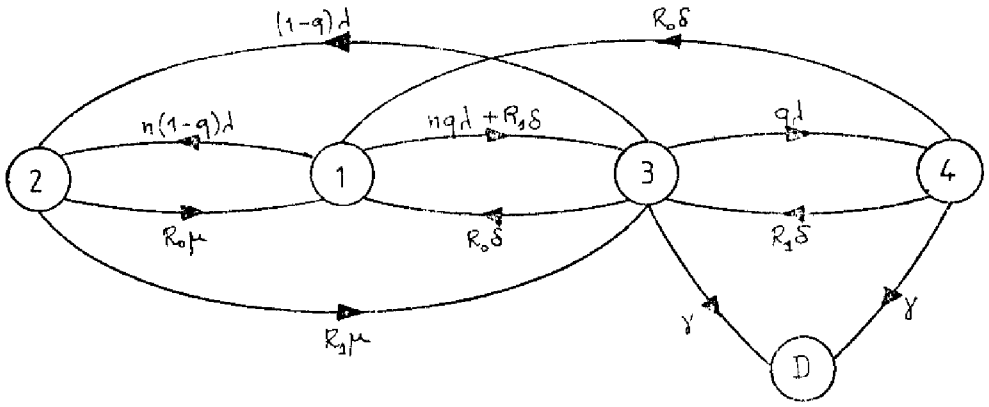
ETATS

(1) : état de bon fonctionnement
(2) : inspection/réparation après une panne déclarée
(3) : un départ en panne simple masquée
(4) : deux départs en panne simple masquée
(8) : un départ en panne double masquée
(9) : un départ en panne simple masquée et un en panne double masquée
(13) : deux départs en panne double masquée
(D) : état défaillant

$\gamma = \gamma_b + \gamma_\ell$ pour la sûreté nominale
$\gamma = \gamma_b$ pour la sûreté dégradée

FIGURE 4.9. Graphe représentatif d'une barre avec prise en compte des pannes doubles de deux départs.

GRAPHE



ETATS

(1) : état de bon fonctionnement
(2) : inspection/réparation après panne déclarée
(3) : un départ en panne simple masquée
(4) : un départ en panne double masquée
(D) : état défaillant

$\gamma = \gamma_b + \gamma_\ell$ pour la sûreté nominale
$\gamma = \gamma_b$ pour la sûreté dégradée

FIGURE 4.10. Graphe représentatif d'une barre avec prise en compte des pannes d'un seul départ.

Les résultats relatifs à la sûreté nominale des cinq modèles considérés sont donnés par les figures 4.11.a.,b. et c. où nous avons également considéré l'influence de l'efficacité de réparation P_m et du nombre n de départs que comporte la barre. L'ensemble de ces courbes montre qu'il est nécessaire de ne prendre en compte que la panne de deux départs.

En ce qui concerne la sûreté de fonctionnement, nous n'avons pas considéré l'influence de P_m. Les résultats correspondants, donnés par les courbes de la figure 4.12., conduisent à la conclusion que, dans ce cas, il est nécessaire de considérer que trois départs peuvent tomber en panne.

4.2.2.2. Influence des modes de panne de chaque départ

Nous avons étudié l'influence de la prise en compte des pannes doubles sur la sûreté nominale. Dans ce but, nous l'avons évaluée pour les modèles prenant en compte :

- la panne double d'un seul départ (graphe de la figure 4.9.),
- la panne double d'un seul départ (graphe de la figure 4.9. moins l'état (13)),
- les pannes simples uniquement (graphe de la figure 4.9. moins les états (8), (9) et (13)).

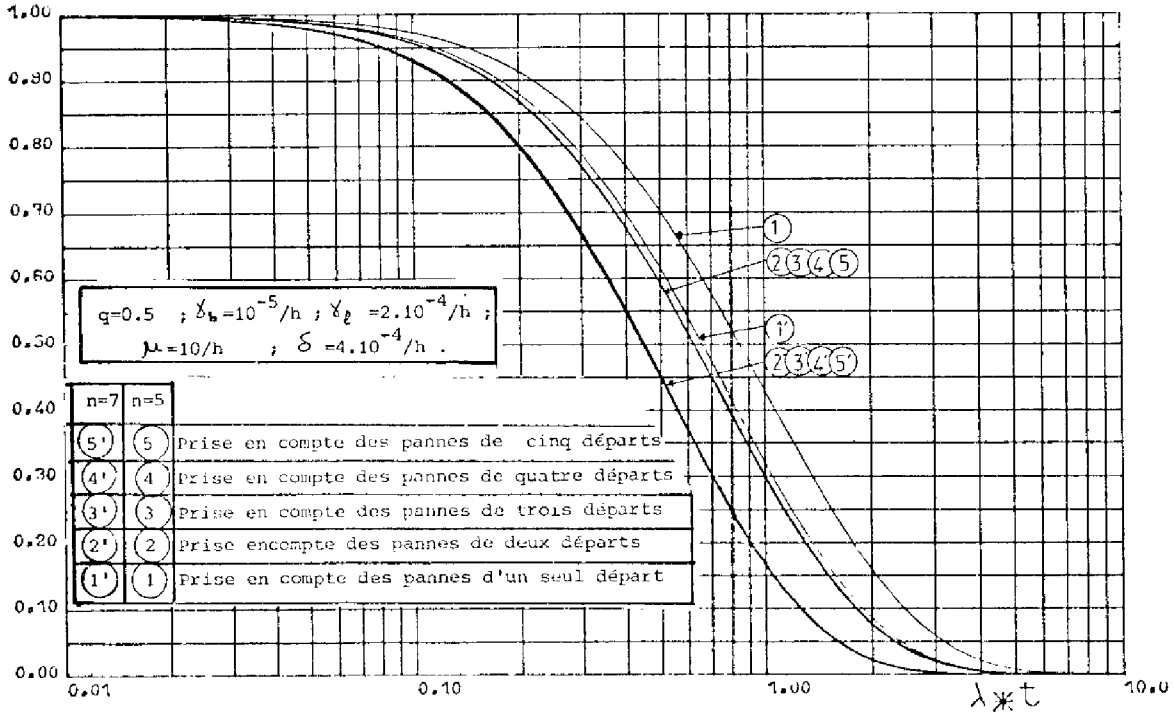


FIGURE 4.11.a. Sûreté nominale pour n=5,7 et P_m=0.9

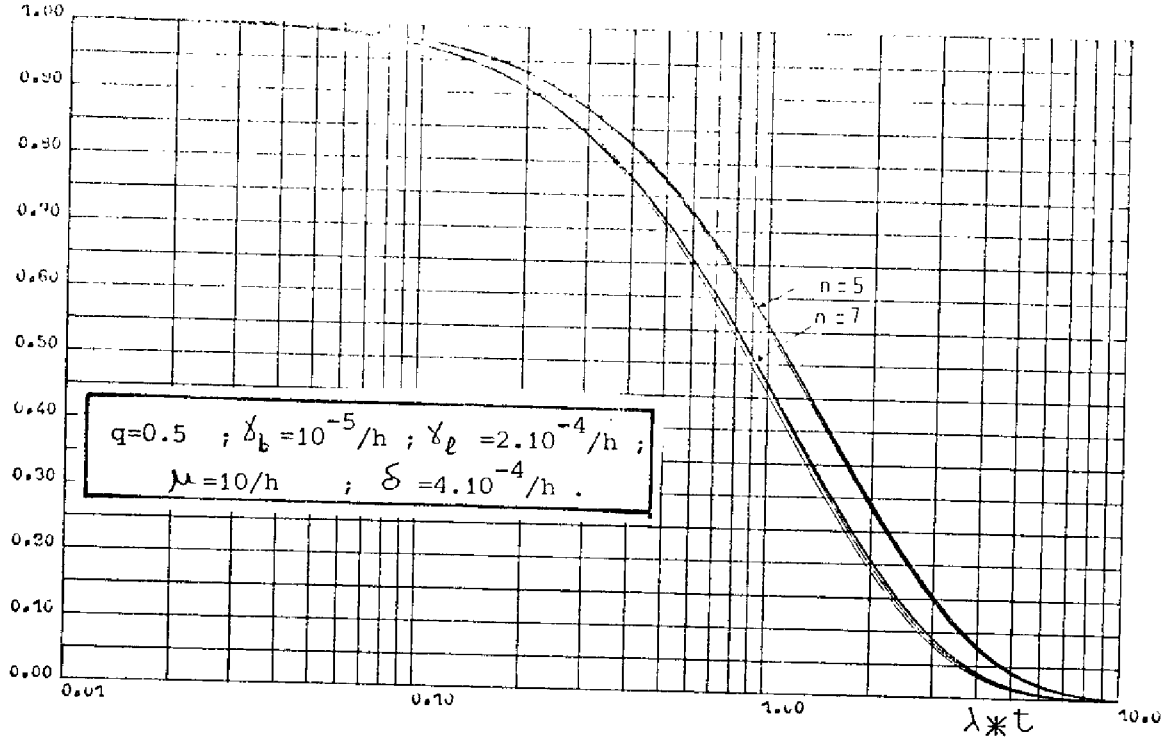


FIGURE 4.11.b. Sûreté nominale pour n=5,7 et P_m=0.99

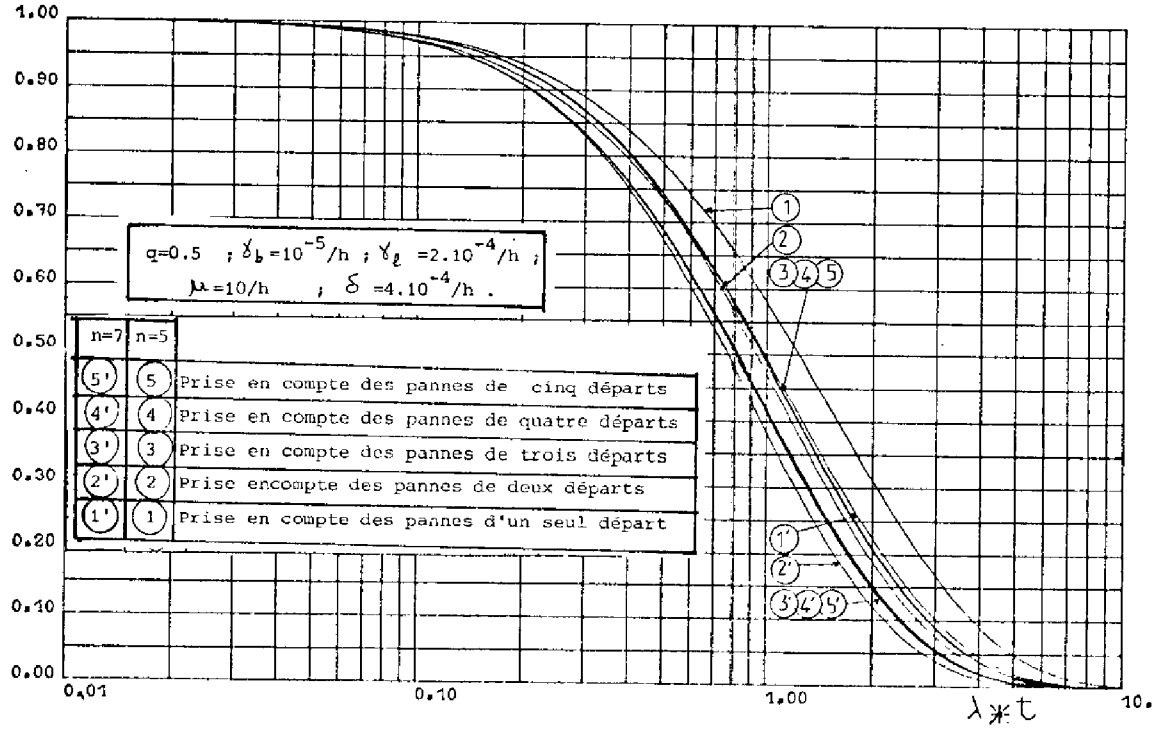


FIGURE 4.11.c. Sûreté nominale pour n=5,7 et P_m=1

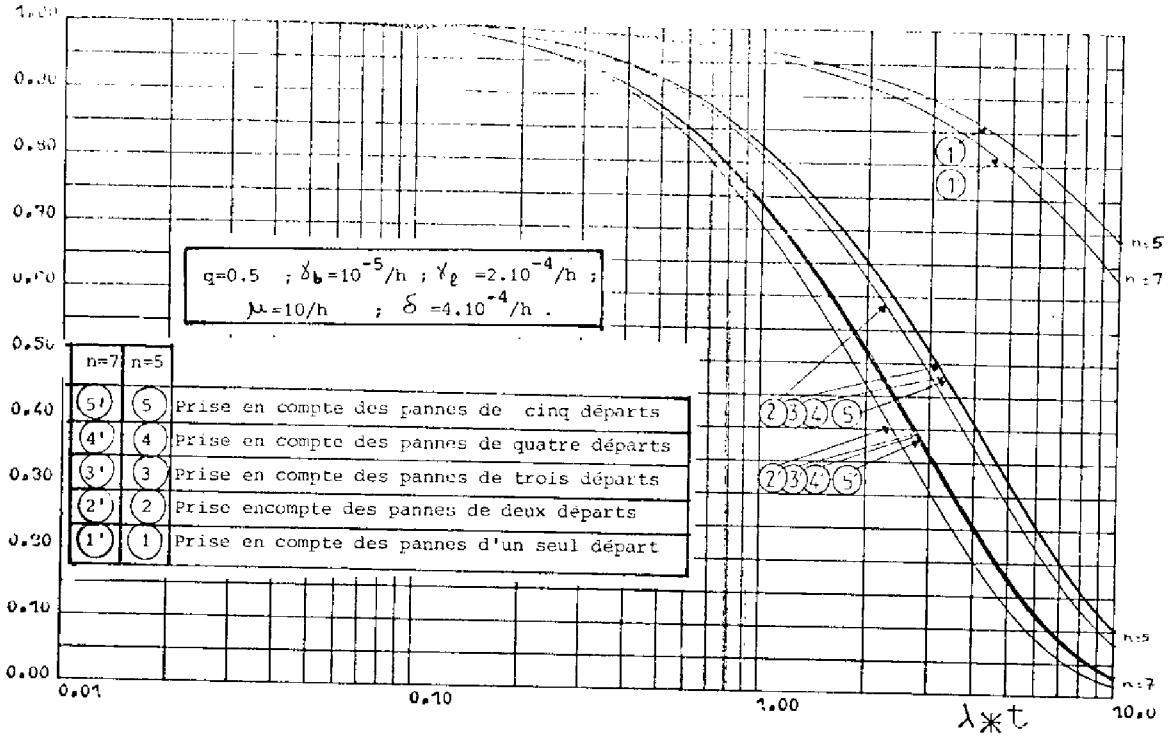


FIGURE 4.12. Sûreté dégradée pour n=5,7 et P_m=0.99

La figure 4.13. donne les courbes obtenues pour ces trois modèles. Nous remarquons que les courbes (2) et (3), correspondant respectivement à la panne double d'un seul départ et à la panne double de deux départs, sont confondues.

Comme pour la sûreté nominale, nous avons étudié l'influence de la prise en compte des pannes doubles sur la sûreté dégradée. Les courbes de la figure 4.14. donnent la sûreté dégradée pour les modèles suivants :

- modèle prenant en compte la panne double de trois départs (graphe de la figure 4.8.),
- modèle prenant en compte la panne double de deux départs (graphe de la figure 4.8. moins l'état (17)),
- modèle prenant en compte la panne double d'un seul départ (graphe de la figure 4.8. moins les états (13), (14) et (17)),
- modèle prenant en compte les pannes simples uniquement (graphe de la figure 4.8. moins les états (8), (9), (10), (13), (14) et (17)).

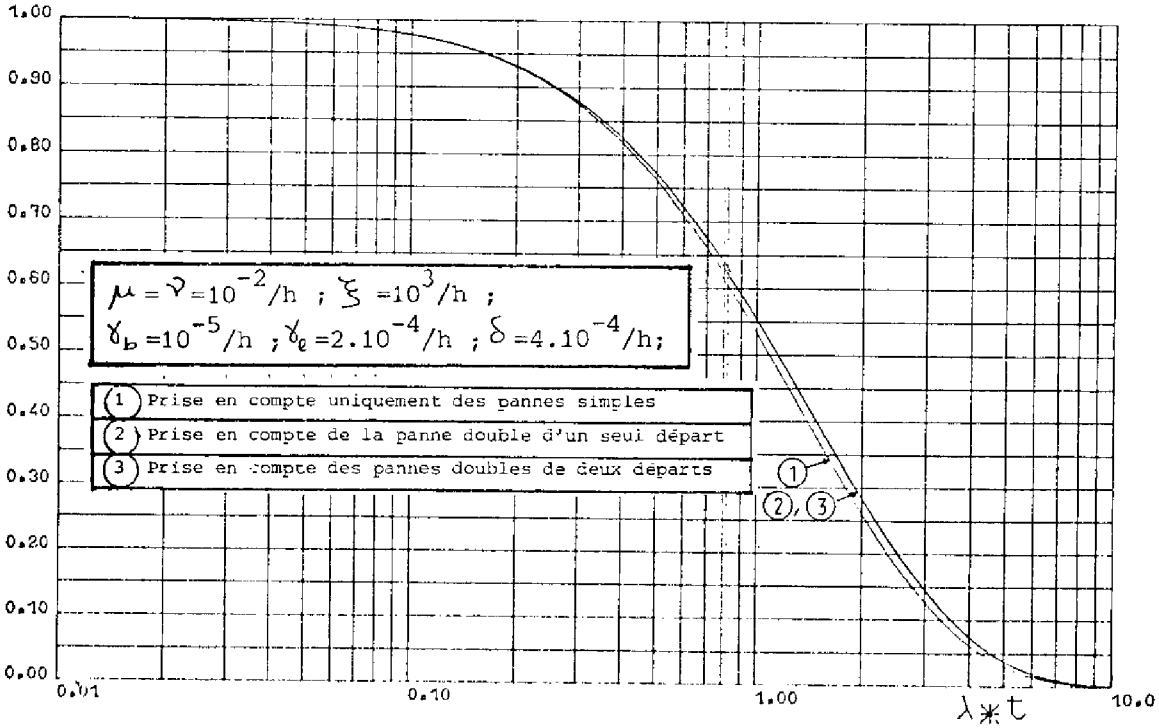


FIGURE 4.13. Influence du mode de panne sur la sûreté nominale

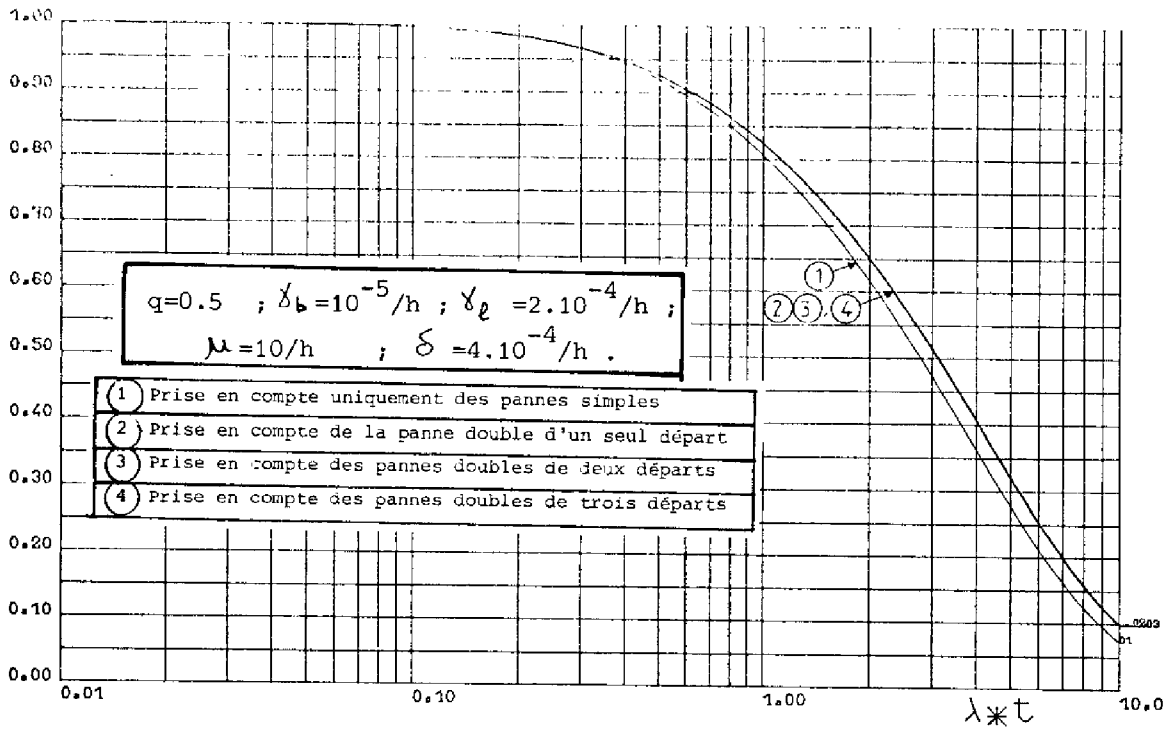


FIGURE 4.14. Influence du mode de panne sur la sûreté dégradée

4.2.2.3. Modèles retenus

En conclusion de cette étude de sensibilité, nous retenons comme modèles :

- de sûreté nominale : le modèle de la figure 4.15. qui prend en compte la panne de deux départs, la panne de l'un des deux étant double et celle de l'autre étant simple,
- du sûreté dégradée : le modèle de la figure 4.16. qui prend en compte la panne de trois départs, la panne de l'un des trois départs étant double, la panne des deux autres étant simple.

4.3. *Modélisation de l'ensemble des départs d'un poste*

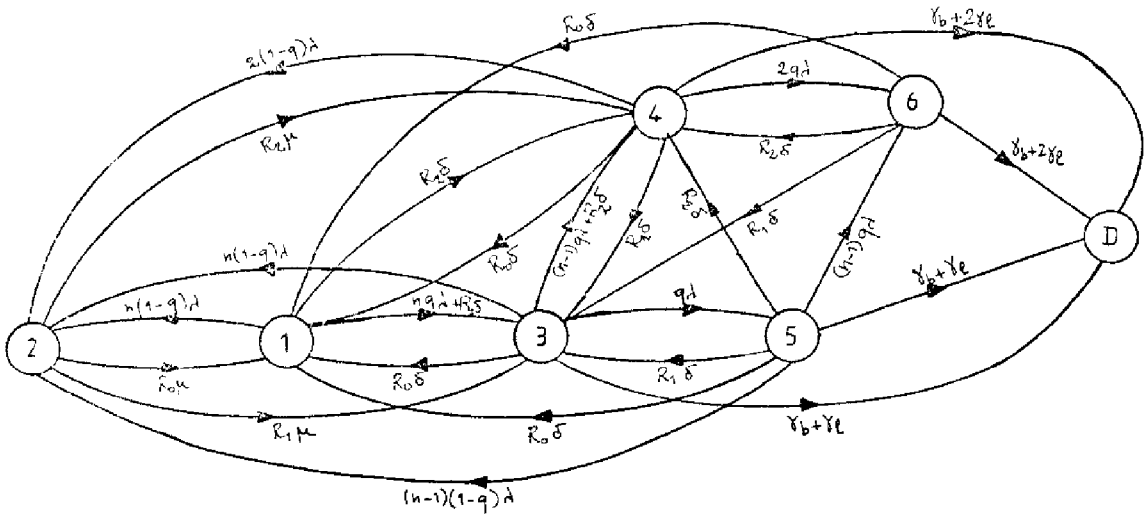
Le poste que nous nous proposons de modéliser dans le paragraphe est un poste type, comportant deux barres ayant respectivement N_1 et N_2 départs. Ces deux barres sont reliées par un couplage dont le taux de panne est λ_c.

Pour les évaluations des sûretés nominale et dégradée, nous supposerons que :

- le taux de panne du couplage est égal au taux de panne d'un départ quelconque ($\lambda_c = \lambda$),
- le nombre de départs pour chaque barre est identique et égal à cinq ($N_1 = N_2 = 5$).

Les modèles finals retenus pour les sûretés nominale et dégradée d'une barre prennent tous les deux en compte la panne double d'un seul départ. On remarque que le graphe représentatif du modèle de la sûreté nominale est un sous-ensemble de celui représentant le modèle de la sûreté dégradée, exception faite des taux de transition à partir des états représentant la panne masquée simple ou double d'un départ vers l'état défaillant (D) . En conséquence, nous pouvons nous contenter, au niveau du poste, d'un seul graphe représentant à la fois la sûreté nominale et la sûreté dégradée. Ce graphe est donné à la figure 4.17. et tient donc compte de la panne simple de trois départs et de la deuxième panne d'un seul départ. La panne du couplage est assimilée à la panne d'un départ quelconque.

GRAPHE



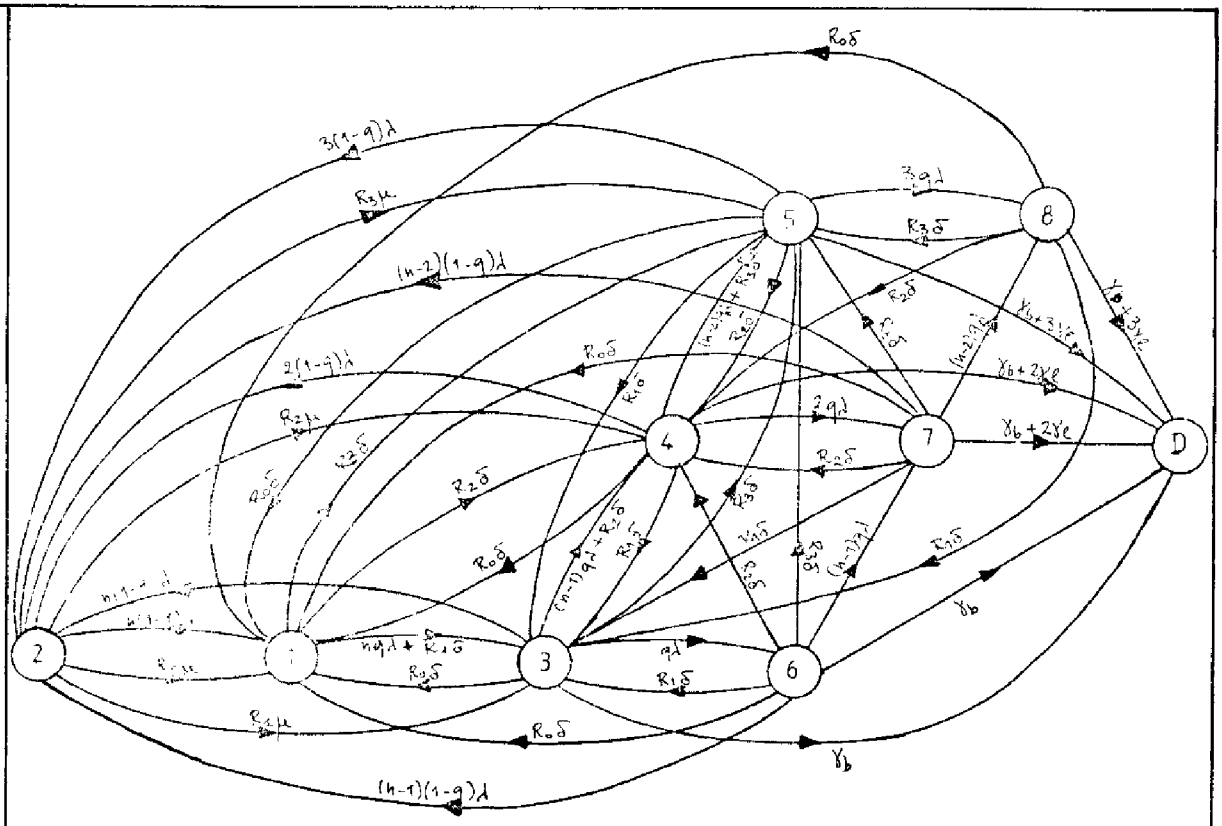
ETATS

(1): état de bon fonctionnement
(2): inspection/réparation après une panne déclarée
(3): un départ en panne simple
(4): deux départs en panne simple
(5): un départ en panne double
(6): un départ en panne double et un en panne simple
(D): état défaillant

N.B. Tous les états de panne correspondent à des pannes masquées.

FIGURE 4.15. Graphe de la sûreté nominale d'une barre

GRAPHE



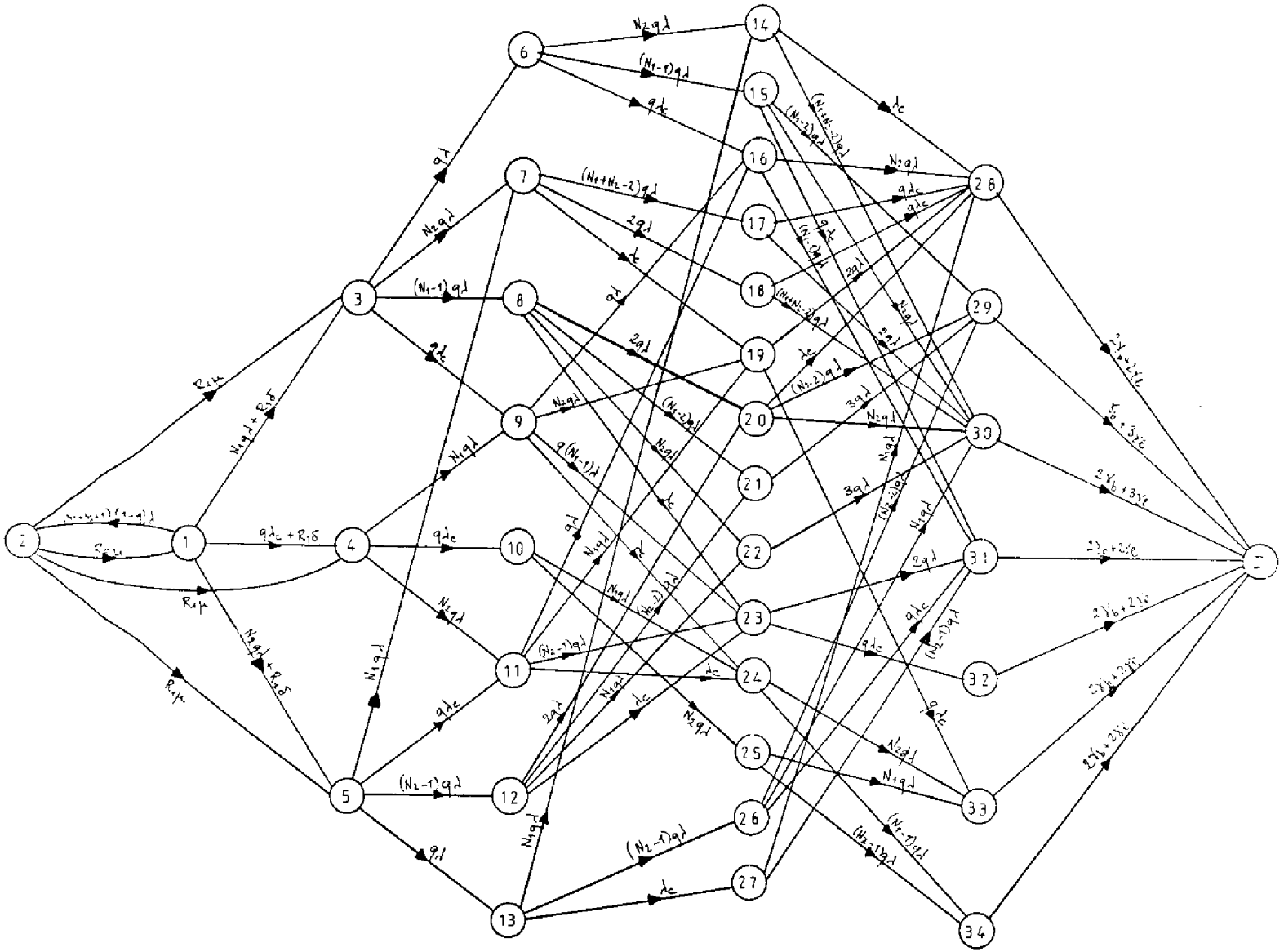
ETATS

(1) : état de bon fonctionnement
(2) : inspection/réparation après une panne déclarée
(3) : un départ en panne simple
(4) : deux départs en panne simple
(5) : trois départs en panne simple
(6) : un départ en panne double
(7) : un départ en panne double et un en panne simple
(8) : un départ en panne double et deux en panne simple
(D) : état défaillant

N.B. Tous les états de panne correspondent à des pannes masquées.

FIGURE 4.16. Graphe de la sûreté dégradée d'une barre

GRAPHE


2
1
4
5
3
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
T

ETATS

(1) : état de bon fonctionnement

(2) : état d'inspection/réparation après une panne déclarée

(3), (4), (5) : un départ en panne simple

(6), (10), (13) : un départ en panne double

(7) : un départ en panne simple sur chaque barre

(8), (12) : deux départs en panne simple sur la même barre

(9), (11) : un départ en panne et le couplage en panne

(14) à (27) : états où il y a soit un départ en panne simple et un en panne double, soit trois départs en panne simple

(28) à (34) : un départ en panne double et deux en panne simple

(D) : état défaillant

Note 2 :

L'occurrence d'un défaut barre ou d'un défaut ligne dans les états (3) à (27) n'est pas représentée. Les transitions de ces états vers l'état défaillant (D) se font par :

- $\gamma_b + a.\gamma_\ell$ pour les états (3), (5), (6) et (13),
- $\gamma_b + 2.\gamma_\ell$ pour les états (8), (12), (15), (20) et (26),
- $\gamma_b + 3.\gamma_\ell$ pour l'état (21),
- $2.\gamma_b$ pour les états (4) et (10),
- $2.\gamma_b + a.\gamma_\ell$ pour les états (9), (11), (16), (24), (25) et (27),
- $2.\gamma_b + 2.\gamma_\ell$ pour les états (7), (14), (18), (19) et (23),
- $2.\gamma_b + 3.\gamma_\ell$ pour les états (17) et (22).

a = 1 pour la sûreté nominale

a = 0 pour la sûreté dégradée

Note 1 :

L'inspection dans les états (3) à (34) n'est pas représentée sur le graphe, de chacun de ces états il y a une transition vers les états :

- (1) par $R_0\delta$,
- (3), (4), (5) par $R_1\delta$,
- (7), (8), (9), (11), (12) par $R_2\delta$,
- (17), (19), (21), (22), (23) par $R_3\delta$.

Note 3 :

L'occurrence d'une panne déclarée (transition vers l'état (2)) n'est pas non plus représentée sur le graphe pour les états (3) à (27).

Ces transitions se font par :

- $(N_1+N_2+1)(1-q)\lambda$ pour les états (3), (4), (5), (7), (8), (9), (11) et (12)
- $(N_1+N_2)(1-q)\lambda$ pour les états (6), (10), (13), (15), (20) et (26)
- $(N_1+N_2-1)(1-q)\lambda$ pour les états (14), (16), (17), (18), (19), (23), (24), (25) et (27)
- $3(1-q)\lambda$ pour les états (21) et (22)

FIGURE 4.17. Modèle représentatif du poste.

La figure 4.18. donne les courbes de sûreté nominale et dégradée du poste.

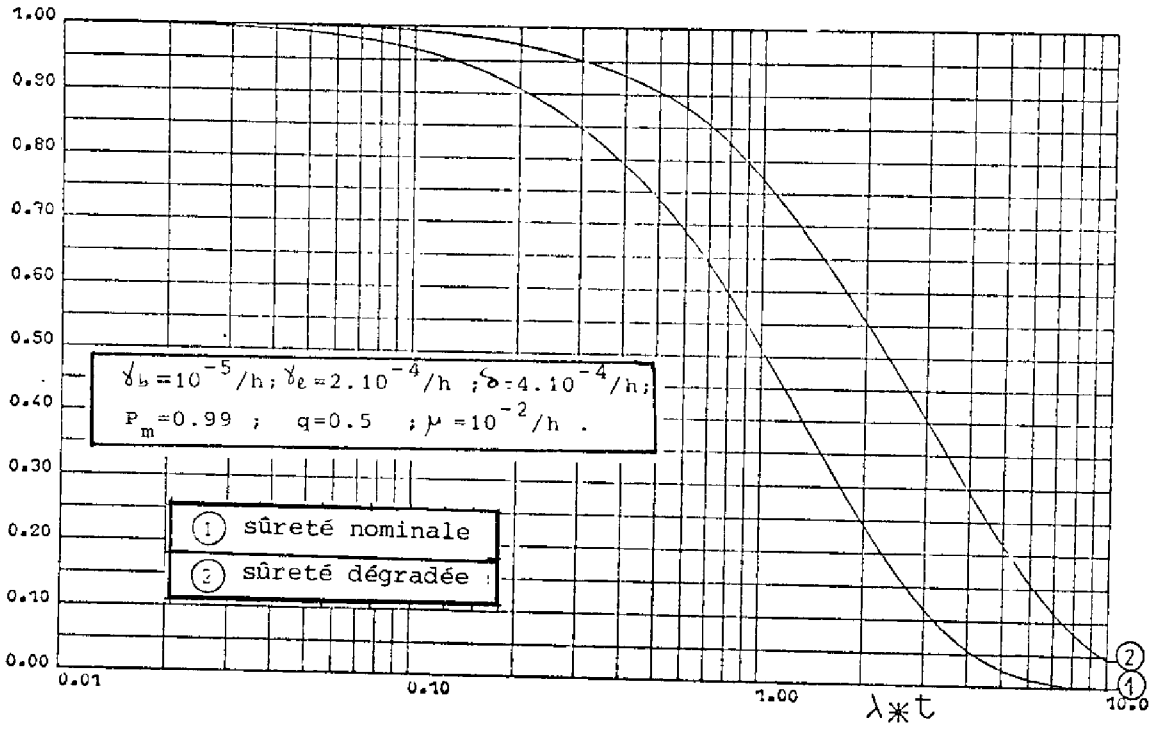


FIGURE 4.18. Sûreté nominale et dégradée du poste

Ces courbes laissent apparaître des performances médiocres (sûreté nominale de 50 %, sûreté dégradée de 70 % pour t ∼ un an) pour le poste actuel. Il faut cependant remarquer que ces courbes ont été tracées pour une valeur moyenne du paramètre q et ne peuvent guère fournir d'indications valables sur les valeurs absolues des grandeurs caractéristiques. Une étude plus fine du poste actuel serait donc nécessaire pour connaître avec précision la valeur du paramètre q.

4.4. *Conclusions*

L'étude du poste actuel a permis de mettre en évidence les points suivants :

- il est inutile de tenir compte, au niveau des modèles, de l'état du système correspondant à l'état de traitement d'un défaut,
- l'efficacité de réparation a une grande influence sur les sûretés nominale et dégradée,
- la réparation peut être considérée comme étant instantanée,
- les modèles de sûreté nominale et dégradée ne prennent en compte la panne double que d'un seul départ.

Les modèles que nous avons définis serviront de base à la modélisation des nouvelles architectures qui seront proposées dans le chapitre suivant.

5. PROPOSITIONS D'ARCHITECTURES

Les différents modèles et les évaluations des composantes de la sûreté de fonctionnement basés sur le système actuel ont permis de mettre en évidence les processus dont les influences étaient les plus importantes.

En particulier, nous avons montré que la détection des fautes nécessitait une attention particulière. D'autre part, l'implantation des échanges d'informations par des techniques compatibles avec l'état de l'art (multiplexage sur une voie banalisée en particulier) nécessite l'examen de l'influence de ce sous-système sur les performances du système global.

Ce chapitre est consacré à l'incorporation dans le modèle établi précédemment de ces deux points dans une optique de première définition de solutions envisageables.

Nous resterons donc à un niveau d'abstraction élevé et indépendant de la manière effective dont seront implantées les solutions étudiées ; en particulier, l'incorporation de tolérances locales dans chaque équipement ne sera pas examinée ici.

5.1. *Premières définitions d'architectures pour le système de commande*

Dans ce paragraphe, nous examinerons brièvement les spécifications fonctionnelles du système de commande, la communication, entre les différents départs et avec le bâtiment de commande, et les techniques de détection de fautes pour de tels systèmes. En conclusion, nous proposerons deux architectures pour le système de commande du poste qui se différencient par la méthode de détection de fautes.

5.1.1. *Spécifications fonctionnelles*

Le système de commande du poste doit remplir deux fonctions complémentaires :

- la fonction de surveillance et de calcul de l'impédance de la ligne surveillée,
- la fonction de décision,

que nous allons analyser successivement.

5.1.1.1. Fonction de surveillance

Nous avons vu au paragraphe 3.1.2. que chaque départ dispose d'informations, en provenance des réducteurs de mesures placés au niveau de la ligne qu'il surveille, qui lui permettent de savoir s'il y a un défaut ou non sur la ligne. Cette fonction de surveillance est indépendante pour chaque départ et peut être réalisée de façon décentralisée.

5.1.1.2. Fonction de décision

La fonction de décision d'effectuer ou non des actions sur les disjoncteurs du poste prend en compte, de façon générale, toutes les informations de présence et de direction de défaut délivrées par tous les départs. Ceci peut se formaliser en utilisant la méthode suivante :

considérons une barre avec n départs ; on dispose d'un vecteur d'entrée E de la forme $E=(e_1\ e_2 \ldots e_i\ e_{i+1} \ldots e_n)$, chaque élément e_i de E pouvant prendre trois valeurs a, b ou c qui correspondent respectivement à l'absence de défaut, à un défaut aval (défaut ligne) ou à un défaut amont (défaut barre). La fonction de décision fait correspondre à ce vecteur d'entrée E un vecteur de sortie S de la forme $S=(S_1\ S_2 \ldots S_i\ S_{i+1} \ldots S_n)$ (on suppose qu'on a un seul disjoncteur par départ), chaque élément s_i de S pouvant prendre deux valeurs 0 et $\overline{0}$ correspondant respectivement à une ou pas d'action sur le disjoncteur.

On peut avoir a priori 3^n vecteurs d'entrée, mais dans la mesure où tout défaut sur un départ est vu également par tous les autres départs, un certain nombre de vecteurs n'ont pas de réalité physique ; par exemple, le vecteur $E_D=(a\ a \ldots a\ b\ a \ldots a)$ indiquant la présence d'un défaut ligne sur un départ alors que les autres départs ne détectent pas ce défaut côté barre, ne correspond à aucun phénomène physique dans la partie haute tension du poste.

L'ensemble des vecteurs d'entrée forme donc un code redondant et le processus apparaît comme étant "autocodant". Si l'on fait l'hypothèse d'un seul défaut ligne, nous obtenons les vecteurs d'entrée et les vecteurs de sortie correspondants suivants :

(b,c,c...c)	$(o,\overline{o},\overline{o}\ldots\overline{o})$
(c,b,c...c)	$(\overline{o},o,\overline{o}\ldots\overline{o})$
(c,c,c...b)	$(\overline{o},\overline{o},\ldots\overline{o},o)$

Ces vecteurs sont au nombre de n. Deux autres vecteurs sont à considérer : les vecteurs d'entrée (a a...a) et (c,c...c) indiquant respectivement l'absence de défaut et un défaut barre. Les vecteurs de sortie correspondants sont respectivement $(\bar{o},\bar{o}...\bar{o})$ et (o,o...o).
On a donc (n+2) vecteurs d'entrée physiquement réalisables sur 3^n vecteurs théoriquement possibles, ce qui constitue un code relativement puissant pour la détection et la correction éventuelle des erreurs sur les vecteurs d'entrée.
En ce qui concerne les vecteurs de sortie, on voit que chaque élément s_i du vecteur S est fonction de tous les éléments du vecteur d'entrée E.

Si l'on veut étendre ce formalisme à tout le poste, il faut alors prendre en compte les informations relatives à la configuration du poste et celles relatives à la position du disjoncteur de couplage.

Cette brève analyse fait apparaître que d'un point de vue purement fonctionnel, la solution consistant à centraliser la fonction de décision d'action sur les disjoncteurs du poste est la plus facile à implanter dans la mesure où l'action sur un disjoncteur quelconque dépend des informations recueillies au niveau de tous les départs.

Le principe d'une telle solution doit cependant être rejeté immédiatement pour les performances de sûreté de fonctionnement ; on ne peut, en effet, accepter qu'une panne du système central de commande entraîne la défaillance totale du poste.

En conséquence, nous choisirons pour le système de commande du poste une solution décentralisée avec un ou plusieurs calculateurs par départ ; cette solution nécessite un échange d'informations entre les différents départs, ce qui entraîne l'existence d'une liaison entre ces départs que nous appellerons, par la suite, communication intertranche.

5.1.2. Systèmes de communication

Chaque calculateur de départ reçoit, outre les informations en provenance de tous les autres départs du poste, des consignes en provenance du bâtiment de commande. Nous allons examiner successivement la communication intertranche et la communication avec le bâtiment de commande.

5.1.2.1. Communication intertranche

En l'absence de sollicitation, le flux d'informations échangées entre les différents départs est très faible et ces informations n'ont pas une importance primordiale pour le bon fonctionnement du poste.

Par contre lors d'un défaut, cette communication joue un rôle fondamental pour l'élimination du défaut en n'ouvrant que les disjoncteurs concernés. L'importance que revêt cette communication nous a amené à étudier en détail son influence sur la sûreté de fonctionnement du poste (cf.5.2.3.).

5.1.2.2. Communication avec le bâtiment de commande

Les informations échangées entre le bâtiment de commande et les calculateurs de départs [TRA 75] sont :

- des consignes en provenance du bâtiment de commande à destination des départs,
- des signalisations en provenance des départs et à destination du bâtiment de commande.

En général, le temps de transmission de ces informations n'est pas critique et un support de communication commun à tous les départs paraît suffisant d'un point de vue fonctionnel.

En ce qui concerne la sûreté de fonctionnement, un support de communication non redondant nous paraît également suffisant compte tenu de la non criticité de la tâche d'échange de ces informations.

5.1.3. Détection de fautes

Ayant déterminé l'architecture du système de commande d'un point de vue fonctionnel (système distribué), le problème qui se pose alors est de savoir comment assurer la détection de fautes. Pour ce faire, deux grands ensembles de méthodes utilisant respectivement les données traitées ou des données spécifiques au test sont envisageables. Nous allons examiner successivement ces deux ensembles de méthodes.

5.1.3.1. Méthodes utilisant les données traitées

Les données dont on dispose au niveau du poste sont de deux types : données globales concernant tous les départs et données locales relatives à chaque départ :

.nous avons vu au paragraphe 5.1.1. que les données représentant l'état de sortie de tous les départs présentent une redondance inhérente au poste. Cette redondance constitue un bon moyen de détection et de localisation des fautes dans les différents départs. Des techniques de détection se basant sur cette redondance de l'information peuvent être implantées localement (au niveau de chaque départ) ou de manière centralisée : avec un calculateur qui reçoit les sorties des différents départs et qui effectue des tests se basant sur la cohérence de ces sorties ;

.localement, on peut munir chaque calculateur de départ de techniques de redondance matérielles (cf. 2.3.1.).

5.1.3.2. Méthodes utilisant des données spécifiques au test

Chaque départ peut être muni de ses propres programmes de test périodique indépendamment de tous les autres départs (cf. 2.3.1.). De plus, l'existence de liens fonctionnels entre les différents départs permet d'implanter des méthodes de diagnostic se basant sur le test mutuel des différentes unités [PRE 67] . Le vecteur de test peut être traité soit au niveau de chaque départ, soit de façon centralisée.

Une autre méthode peut reposer sur l'existence d'un calculateur central qui interroge périodiquement tous les départs pour faire un diagnostic global.

5.1.4. Conclusions : propositions d'architectures

Nous avons vu que pour des raisons de sûreté de fonctionnement, le poste doit avoir une architecture décentralisée nécessitant des liens entre les différents départs. Les choix conditionnels ne peuvent donc se faire que pour les structures de communication et les techniques de détection de fautes. Nous avons choisi de situer la différence entre les deux architectures que nous proposerons au niveau de la détection c'est-à-dire au niveau de la réalisation des calculateurs de départs.

La première architecture se caractérise par la décentralisation complète de la détection de faute : chaque calculateur possède ses propres techniques de détection de fautes.

Pour la seconde architecture, la détection de fautes se fait à l'aide d'un calculateur central, possédant lui-même ses propres techniques de détection de fautes, et il peut exister sur chaque calculateur un programme de test local permettant de détecter certaines pannes. En aucun cas, l'organe centralisé ne peut agir sur les calculateurs de départs dans la mesure où sa défaillance ne doit pas entraîner celle du système complet.

Pour ces architectures, nous ne nous intéresserons qu'à l'élimination nominale des défauts, c'est-à-dire à l'élimination par l'ouverture du nombre minimal de disjoncteurs : seule la sûreté nominale sera évaluée.

5.2. *Modélisation et évaluation de l'architecture à détection décentralisée*

Les modèles utilisés pour l'évaluation des caractéristiques de la sûreté de fonctionnement des architectures proposées sont fondés sur les résultats du chapitre 4.

Nous introduisons tout d'abord les hypothèses conduisant aux modèles puis nous nous intéressons successivement à :

- la politique de maintenance,
- l'influence de la prise en compte de la panne du support de communication intertranche,
- l'étude de sensibilité des paramètres relatifs à cette architecture.

5.2.1. *Introduction*

Il est bien sûr inutile pour cette architecture de commencer la modélisation au niveau départ. En effet, les résultats obtenus restent valables, seules les valeurs de certains paramètres sont modifiées ; la détection des pannes étant une caractéristique importante dans le choix de l'architecture, nous ne regrouperons plus les états de pannes qui auront été détectées par les mécanismes de détection et celles qui auront été perçues par leur action sur le disjoncteur.

Nous nous placerons pour les différents modèles au niveau de la barre du fait que nous considérons que le calculateur de couplage joue un rôle identique à celui joué par un calculateur de départ.

5.2.2. *Politique de maintenance*

Le système étant doté d'une détection de panne efficace, la maintenance préventive par inspection à intervalles réguliers n'est pas nécessaire, d'autant plus que ce type de maintenance peut être destructif (efficacité de réparation inférieure à 100 %).

En ce qui concerne les actions de réparation, nous avons retenu les deux principes suivants :

- en cas de panne détectée, que la panne ait une action sur le disjoncteur ou non, seul le calculateur en panne est réparé,
- le seul cas de panne qui conduit à une inspection globale de tout le poste est celui d'une panne non détectée qui provoque une action intempestive sur le disjoncteur.

5.2.3. *Influence de la prise en compte de la panne du support de communication intertranche*

Si nous considérons une structure à interconnexion totale entre les différents calculateurs ou une structure en boucle réalisée par tronçons avec régénération du signal, la panne d'une liaison quelconque n'entraîne pas de conséquence catastrophique au niveau du poste. La probabilité de perte de la communication complète est très faible et nous pourrons en première approximation considérer que le support de communication est parfait.

Par contre, si nous considérons une structure en bus ou en boucle, la perte de la liaison en un point quelconque entraîne la perte totale de la communication et il est nécessaire de tenir compte de la panne du support de communication.

Pour ces raisons, nous allons modéliser cette architecture dans les trois cas suivants :

- sans tenir compte de la panne du support de communication,

- en supposant que le support de communication peut tomber en panne et qu'il n'est pas redondant,
- en supposant que le support de communication est redondant.

Ces trois modèles seront ensuite évalués comparativement.

5.2.3.1. Modèle ne tenant pas compte de la communication intertranche

Pour l'évaluation de la sûreté nominale, nous avons montré qu'un modèle prenant en compte la panne unique d'un départ et la panne double d'un autre départ était suffisant (cf. 4.2.2.3.).

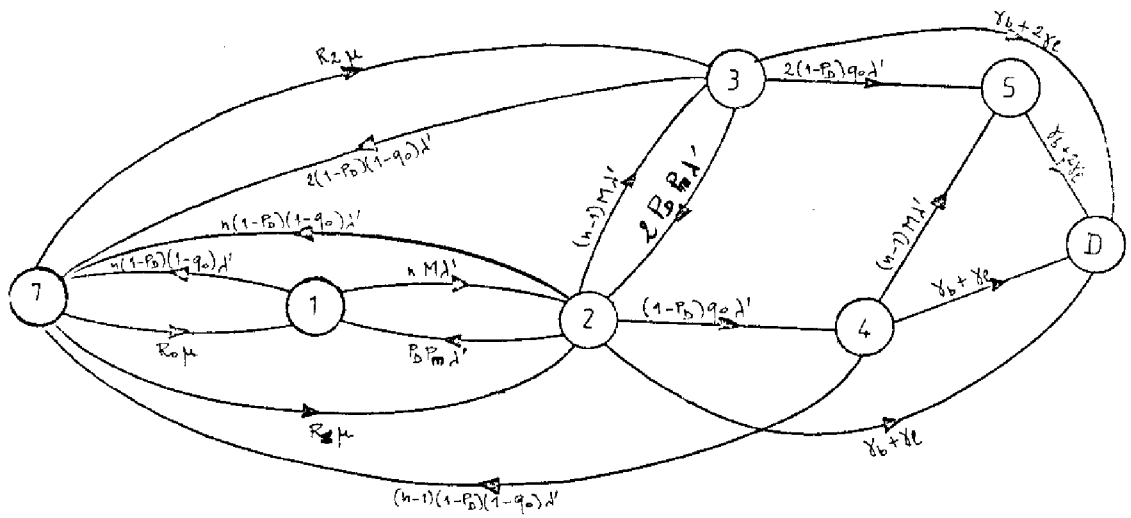
Le modèle obtenu pour une barre est celui donné à la figure 5.1. Il se déduit directement du graphe de la figure 4.15. :

- on a posé $U = (1-P_D)(1-q_o)$; les termes $R_o\ U\ \lambda'$, $R_1\ U\ \lambda'$ et $R_2\ U\ \lambda'$ rendent compte d'une réparation globale après une panne non détectée à action intempestive, réparation effectuée correctement ($R_o = P_m^n$) ou ayant laissé un départ en panne ($R_1 = C_n^1\ P_m^{n-1}\ (1-P_m)$) ou ayant laissé deux départs en panne ($R_2 = C_n^2\ P_m^{n-2}\ (1-P_m)^2$),
- le facteur $M = P_D(1-P_m)+(1-P_D)\ q_o$ rend compte d'une mauvaise réparation après une panne détectée : terme $P_D(1-P_m)$, et d'une panne non détectée sans action intempestive : terme $(1-P_D)q_o$,
- le terme $P_D\ P_m$ correspond à la réparation correcte d'un départ après une panne détectée.

Nous avons montré au paragraphe 4.1.4. que l'on pouvait supposer que les réparations sont effectuées instantanément (μ infini), ce qui permet de supprimer l'état (7) du graphe de la figure 5.1. ; nous obtenons alors le graphe donné à la figure 5.2.

Dans ce graphe, la signification des états reste la même ; seuls les taux de transition sont modifiés.

GRAPHE



ETATS

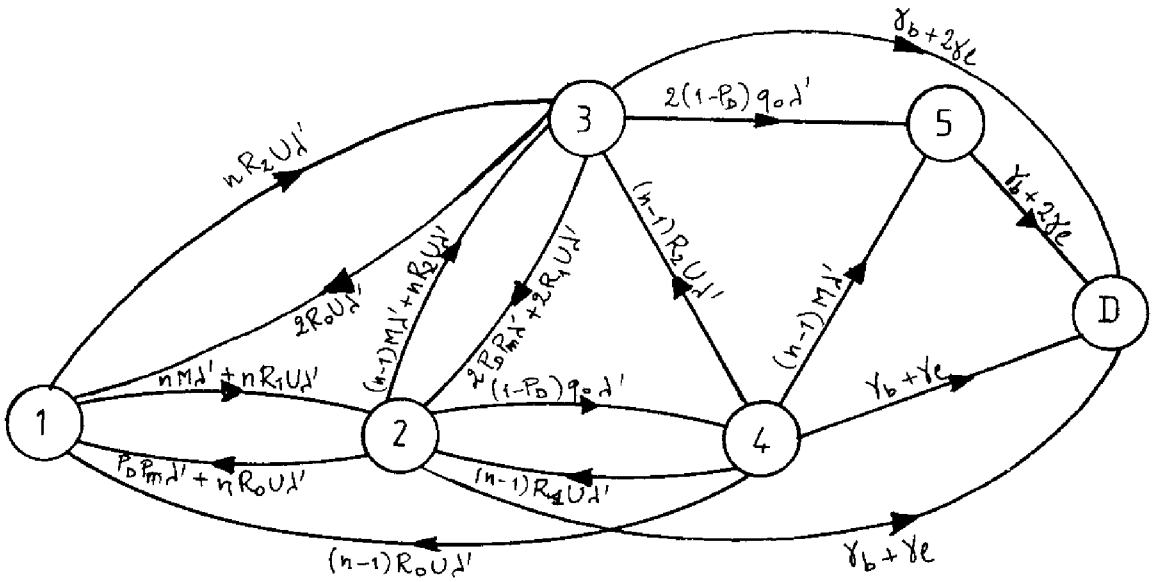
$$M = P_D(1-P_m)+(1-P_D)q_0 \qquad U = (1-P_D)(1-q_0)$$

$\lambda' = b\lambda$ = taux de panne d'un calculateur avec détection de panne

(1) : état de bon fonctionnement
(2) : un départ en panne simple
(3) : deux départs en panne simple
(4) : un départ en panne double
(5) : un départ en panne double et un en panne simple
(7) : état d'inspection globale de tous les départs après une panne non détectée et avec action sur le disjoncteur.
(D) : état défaillant

FIGURE 5.1. Modèle de l'architecture à détection décentralisée ne tenant pas compte du support de communication intertranche

GRAPHE



ETATS

$$M = P_D(1-P_m) + (1-P_D)q_o \qquad U = (1-P_D)(1-q_o)$$

(1) : état de bon fonctionnement
(2) : un départ en panne simple
(3) : deux départs en panne simple
(4) : un départ en panne double
(5) : un départ en panne double et un en panne simple
(D) : état défaillant

FIGURE 5.2. Modèle obtenu en supposant le temps de réparation des calculateurs infiniment petit

5.2.3.2. Modèle avec le support de communication non redondant

Pour ce second modèle, nous prenons en compte les défaillances du support de communication intertranche en faisant l'hypothèse qu'elles n'ont aucune influence sur les calculateurs de départs, et réciproquement. Le modèle est donné à la figure 5.3.

Ce graphe a été obtenu à partir du graphe de la figure 5.2. par duplication des états (1) à (5), le passage d'un sous-ensemble à l'autre s'effectuant par la panne du support, représentée par le taux de panne λ_s et par la réparation du support de communication, représentée par le taux de réparation μ_s.

Lorsque le support de communication est en panne, l'occurrence d'un défaut ligne va provoquer l'ouverture généralisée de n départs. Ceci conduit à ajouter une transition entre l'état (6) et l'état défaillant (D), le taux correspondant étant $n\ \gamma_\ell$. Le passage des états (7) , (8) , (9) et (10) vers l'état (D) se fait par $\gamma_b + n\ \gamma_\ell$ ce qui correspond :

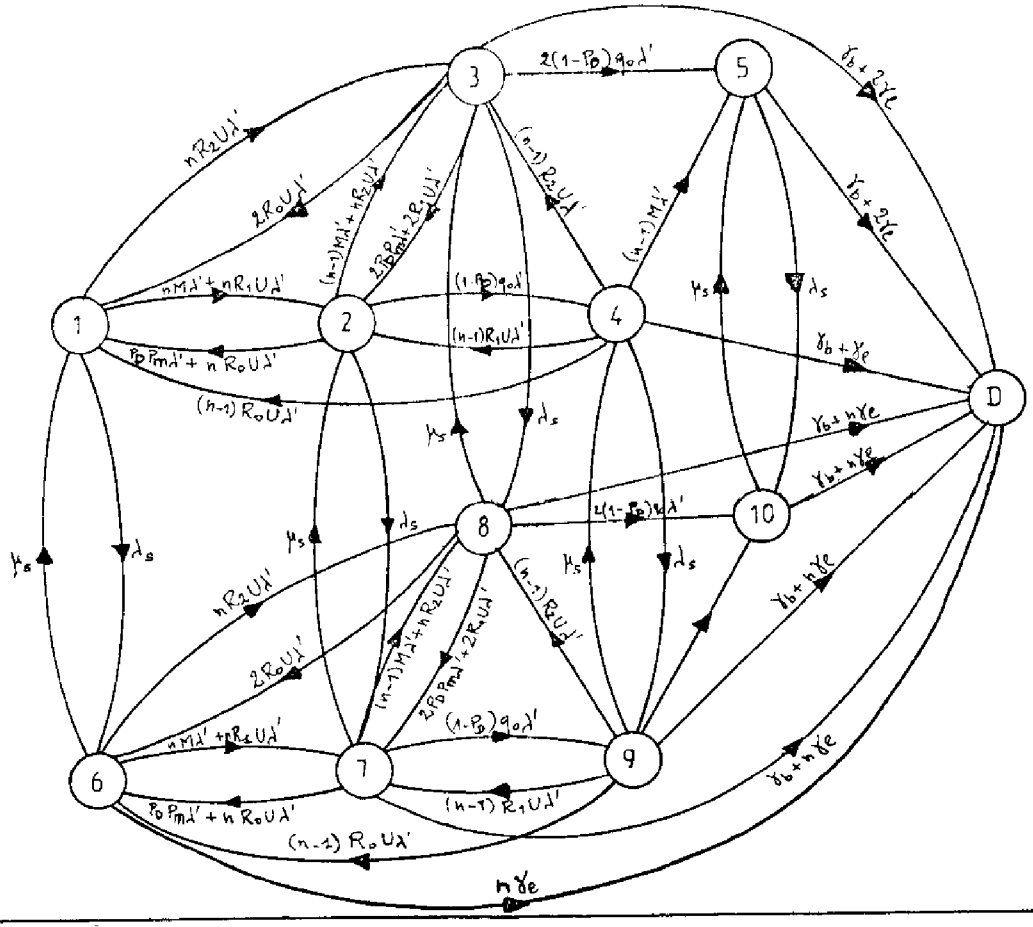
- à la non élimination du défaut en cas de défaut barre (γ_b), ou de défaut ligne sur un départ en panne (γ_ℓ pour les états (7) et (9), $2\ \gamma_\ell$ pour les états (8) et (10)),
- à l'ouverture intempestive en cas de défaut ligne sur un départ sain ($(n-1)\ \gamma_\ell$ pour les états (7) et (9), $(n-2)\ \gamma_\ell$ pour les états (8) et (10)).

Nous ne pouvons pas considérer que le temps de réparation du support est infiniment petit (μ_s infini) car dans les états de réparation de ce support (états (6) et (10)) le système peut être sollicité : tout défaut ligne amène le système dans l'état défaillant (D) .

5.2.3.3. Modèle avec un support de communication redondant

Ce dernier modèle est déduit de celui donné par la figure 5.3., en considérant un support redondant, c'est-à-dire que la première panne couverte de ce support ne modifie pas l'aptitude d'action du système car la redondance a pris le relais ; la panne du second support conduit alors à la perte totale de la communication entre les calculateurs, et l'on a alors des ouvertures généralisées des n départs en cas de défaut ligne.

GRAPHE



ETATS

$$M = P_D(1-P_m) + (1-P_D)q_o \qquad U = (1-P_D)(1-q_o)$$

(1) : état de bon fonctionnement
(2) : un départ en panne simple
(3) : deux départs en panne simple
(4) : un départ en panne double
(5) : un départ en panne double et un en panne simple
(D) : état défaillant

Dans les états (6) à (10) le support de communication est en panne. Ces états ont respectivement la même signification que les états (1) à (5).

FIGURE 5.3. Architecture à détection décentralisée. Modèle avec le support de communication intertranche non redondant

La panne détectée et non couverte du support de communication amène le système dans un état de réparation du support.

La panne non détectée du support entraîne la perte totale de la communication.

Nous introduisons donc un paramètre supplémentaire, C_s, qui est le taux de couverture du support de communication. Comme nous l'avons déjà vu, ce taux peut être décomposé comme suit :

$$C_S = P_{Ds}.P_{Rs}$$

avec : $C_s = \wp\{$la panne du support de communication soit couverte/ le support est en panne$\}$,

$P_{Ds} = \wp\{$la panne du support de communication soit détectée/ le support est en panne$\}$,

$P_{Rs} = \wp\{$la panne du support soit couverte/une panne a été détectée$\}$.

Le graphe du modèle est donné à la figure 5.4.

5.2.3.4. Comparaison des résultats obtenus pour les trois types de communication

Les courbes de la figure 5.5. donnent la sûreté nominale pour les trois modèles.

L'examen de ces courbes montre nettement l'importance du support de communication sur la sûreté de fonctionnement nominale, et il apparaît indispensable de disposer d'un support de communication redondant pour les systèmes tels qu'une défaillance du support en un point entraîne la défaillance totale du support. Nous remarquons également que la courbe (8) obtenue pour un taux de couverture égal à 1 est confondue avec la courbe (1) correspondant à un support de communication parfait, et que les courbes (6) et (7) sont très rapprochées de la courbe (1) . Ceci nous permet d'utiliser pour la suite le modèle avec support de communication parfait au lieu du modèle plus compliqué correspondant au support de communication redondant.

GRAPHE

ETATS

$$M = P_D(1-P_m) + (1-P_D)q_o \qquad U = (1-P_D)(1-q_o)$$

(1) Etat de bon fonctionnement

(2) Un départ en panne simple

(3) Deux départs en panne simple

(4) Un départ en panne double

(5) Un départ en panne double et un en panne simple

Dans tous les états (6) à (10) le support est en panne couverte ; la redondance a pris le secours ; ces états ont respectivement la même définition que les états (1) à (5) .

Dans tous les états (11) à (15) les deux supports sont en panne ; ces états ont respectivement la même définition que les états (1) à (5).

(16), (17) Le support de communication est en panne détectée non couverte, tous les calculateurs sont en bon état de fonctionnement

(18), (19) Le support de communication est en panne non détectée, au moins un calculateur est en panne

Les transitions des états (2) à (5) vers l'état (19) se font par : $P_{Ds}(1-P_{Rs})$

Les transitions des états (2) à (5) vers l'état (18) se font par : $(1-P_{Ds})\ \lambda_s$

(D) Etat défaillant

FIGURE 5.4. Architecture à détection décentralisée avec le support de communication intertranche redondant

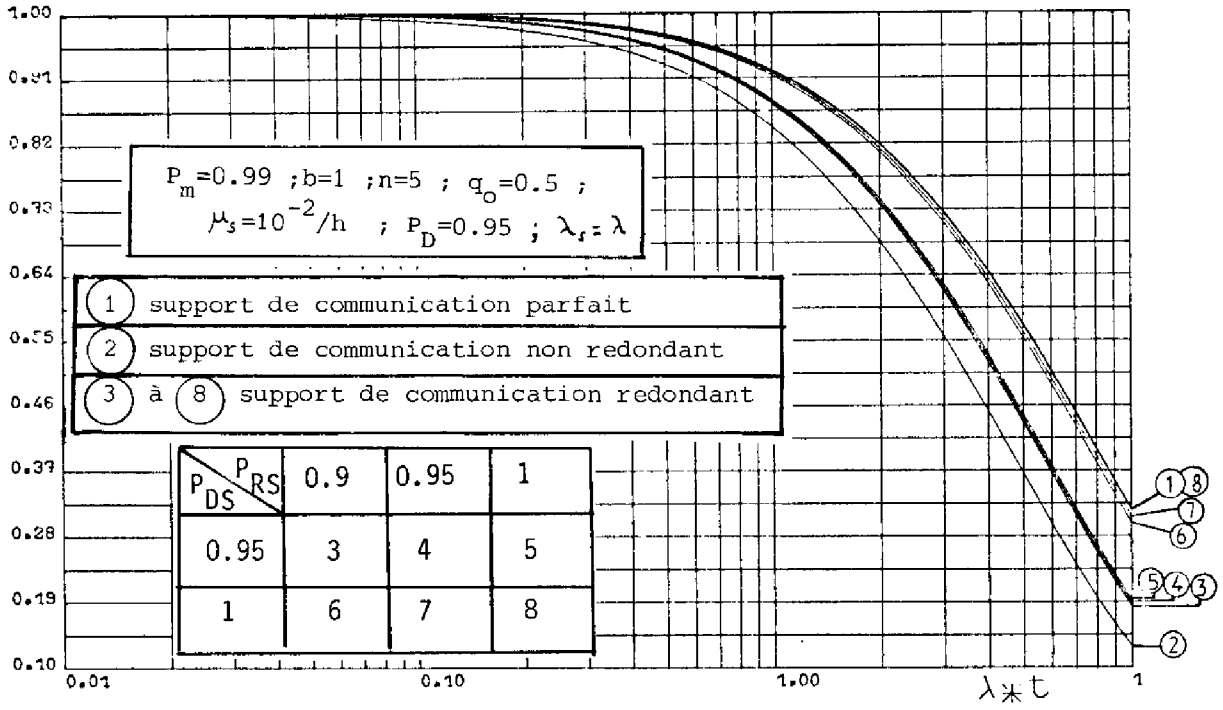


FIGURE 5.5. Détection décentralisée - Influence de la prise en compte de la panne du support de communication

5.2.4. *Détermination des paramètres significatifs*

Les calculateurs de départs étant munis d'une détection matérielle de faute, leur taux λ' peut se mettre sous la forme $\lambda' = b\,\lambda$ où b représente l'accroissement du matériel dû à la détection. Le second paramètre significatif est P_D, facteur d'efficacité de détection. Le lien entre ces deux paramètres est évident d'un point de vue qualitatif mais il ne nous est pas possible d'avoir une information quantitative à ce niveau de description, ce qui nous a conduit à faire varier b et P_D indépendamment l'un de l'autre.

Les courbes de la figure 5.6. montrent, par comparaison avec les courbes de référence (3) et (6), que cette architecture est beaucoup plus sensible à l'efficacité de détection qu'à l'augmentation du matériel pour la détection de panne.

Les courbes de la figure 5.7. montrent que la sûreté de fonctionnement d'une barre diminue quand on augmente le nombre n de départs reliés à cette barre et que la position relative des courbes reste inchangée quand on fait varier n.

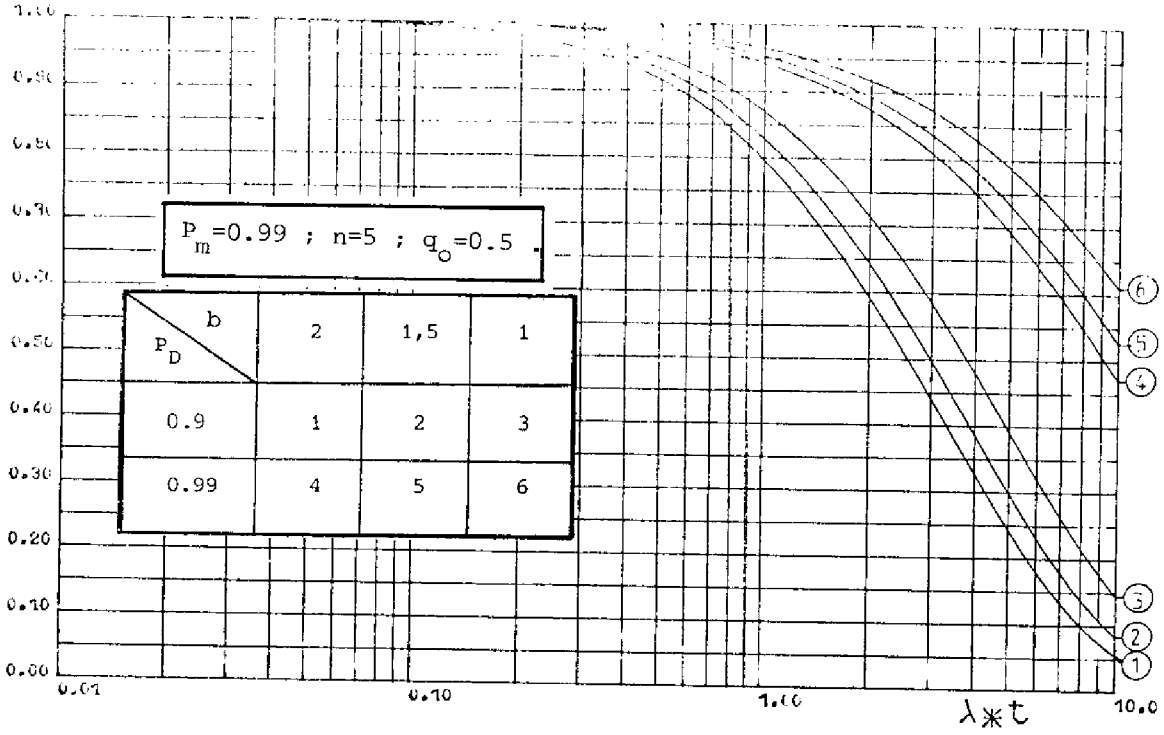


FIGURE 5.6. Détection décentralisée : variation de b et P_D

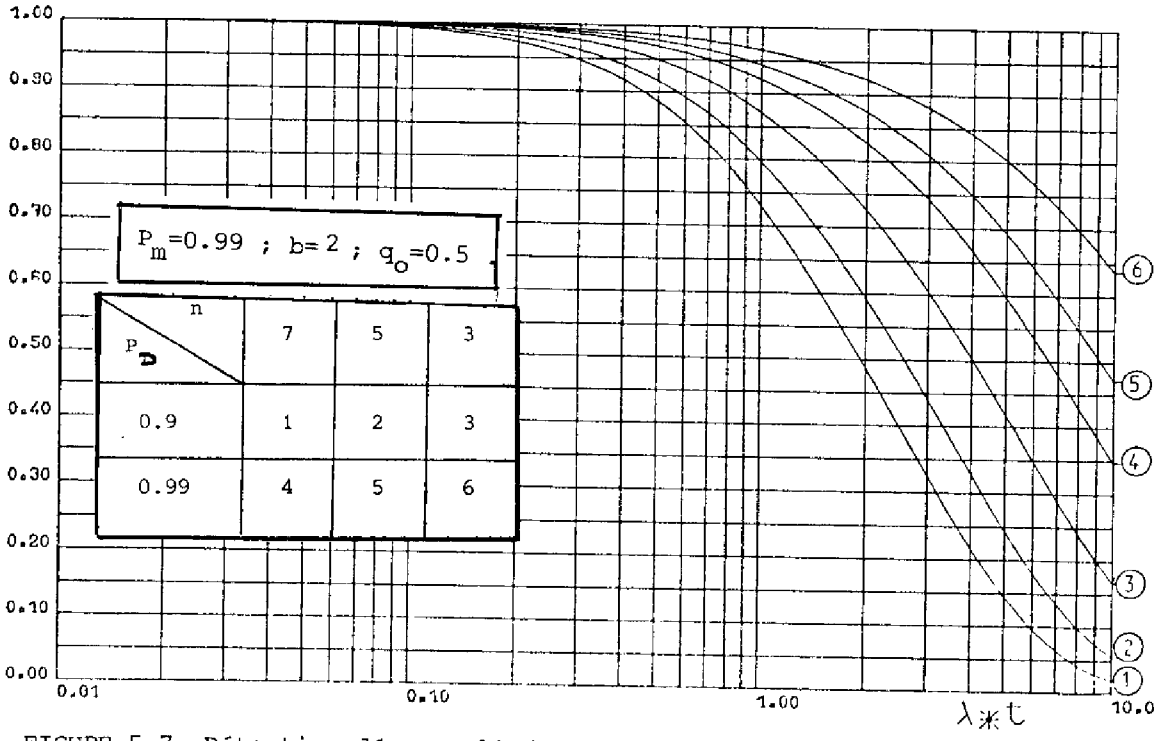


FIGURE 5.7. Détection décentralisée : influence du nombre de départs, n, et de l'efficacité de détection

5.3. *Modélisation et évaluation de l'architecture à détection centralisée*

Pour cette deuxième architecture, nous donnerons d'abord la politique de maintenance puis le modèle du système et nous déterminerons enfin les paramètres les plus significatifs pour cette architecture.

5.3.1. *Politique de maintenance*

Lorsque la détection centralisée fonctionne correctement, seuls les calculateurs de départ sur lesquels une panne a été détectée sont réparés, la panne ayant povoquée ou non une action intempestive sur le disjoncteur.

Une panne non détectée et avec action sur le disjoncteur conduit à l'inspection globale du système. Lorsque la détection centralisée tombe en panne, on ne dispose pour la détection des pannes des calculateurs que des programmes locaux de test. Ces programmes ayant une efficacité nettement moindre que la détection centralisée (cf. 5.1.4.), plus de pannes risquent d'être non détectées, aussi faut-il lors de la remise en service de l'organe centralisé inspecter le système globalement, l'organe centralisé participant activement à cette inspection.

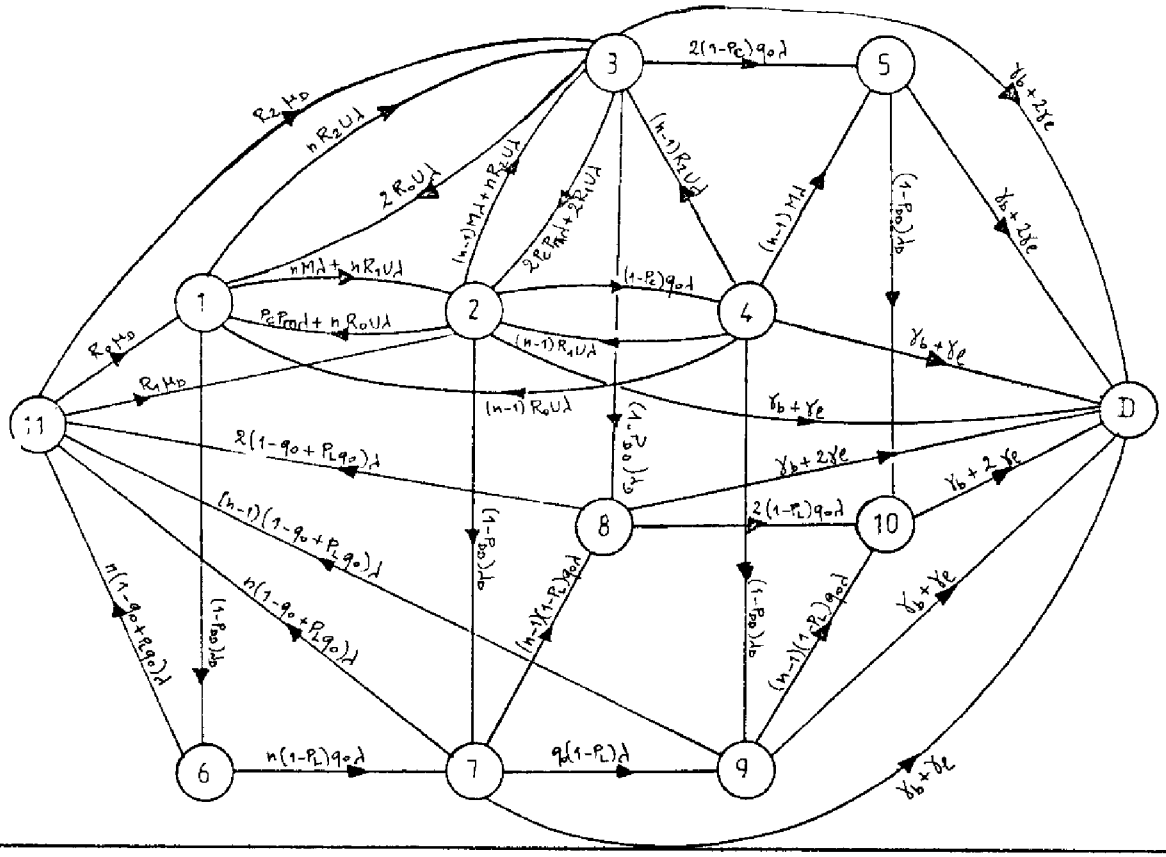
Les informations de panne obtenues localement par les programmes de test des calculateurs sont confrontées avec les informations de panne fournies par l'organe centralisé. Ceci permet de détecter les pannes non auto-détectées de l'organe de détection centralisée.

5.3.2. *Modèle*

Le modèle utilisé est basé sur les résultats obtenus pour l'architecture à détection décentralisée qui indiquent que le support de communication intertranche peut être considéré comme parfait s'il est redondant et que le taux de couverture est élevé.

Le graphe obtenu est celui de la figure 5.8. Le taux de panne de l'organe de détection est λ_D, l'efficacité de sa propre détection est P_{DD}. Le facteur P_C désigne l'efficacité de détection du système lorsque la détection centralisée fonctionne, et P_L désigne l'efficacité locale obtenue par les programmes de test des calculateurs.

GRAPHE



ETATS

$$M = P_c(1-P_m)+(1-P_c)q_0 \qquad U = (1-P_c)(1-q_0)$$

(1) : état de bon fonctionnement
(2) : un départ en panne simple
(3) : deux départs en panne simple
(4) : un départ en panne double
(5) : un départ en panne double et un en panne simple

Dans les états (6) à (10) l'organe central de détection est en panne non auto-détectée. Ces états ont respectivement la même signification que les états (1) à (5).

(11) : état de réparation de l'organe centralisé de détection
(D) : état défaillant

N.B. Les transitions à partir des états (1), (2), (3), (4) et (5) vers l'état (11) ne figurent pas sur le graphe. De chacun de ces états la transition se fait par $P_{DD}\lambda_3$.

FIGURE 5.8. Modèle de l'architecture à détection centralisée

La panne non détectée de l'organe centralisée fait passer du sous-graphe formé par les états (1) à (5) au sous-graphe formé par les états (6) à (10) , chaque sous-graphe représentant l'évolution du système par rapport aux pannes des calculateurs de départ.

En supposant que la réparation de l'organe centralisé est instantanée (μ infini) on obtient le graphe de la figure 5.9. par suppression de l'état (11) de la figure 5.8.

5.3.3. Détermination des paramètres significatifs

Nous avons évalué l'influence de la détection locale au niveau de chaque départ, c'est-à-dire du programme de test associé à chaque calculateur.

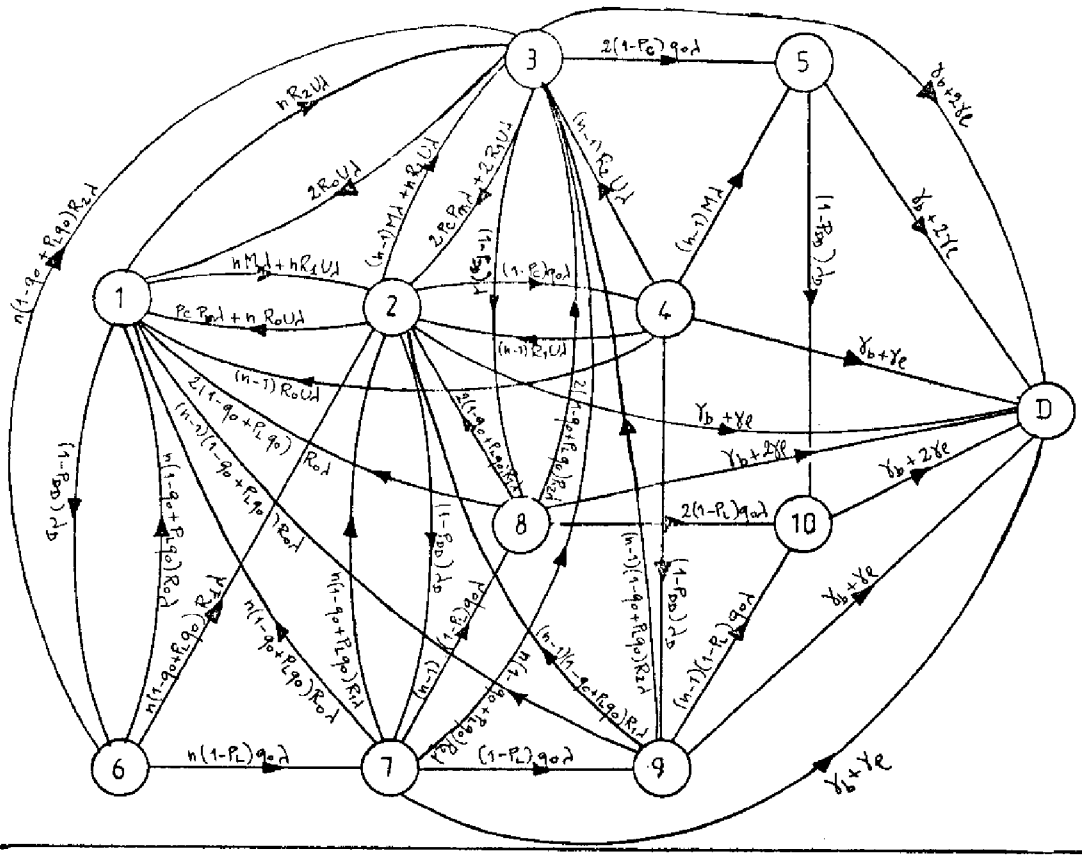
Dans ce but, nous avons fait varier le facteur P_L d'efficacité de la détection locale, ainsi que le facteur P_C d'efficacité de détection de l'organe central. La figure 5.10. donne les courbes obtenues pour la sûreté de fonctionnement de cette architecture.

L'examen de ces courbes montre que cette architecture est beaucoup plus sensible à l'efficacité de la détection centrale qu'à celle de la détection locale. Ceci s'explique par le fait que la détection centrale concerne tous les départs alors que la détection locale ne concerne qu'un seul départ.

L'influence de l'efficacité de détection propre de l'organe central P_{DD} est donnée par les courbes (1) à (6) de la figure 5.11.

La courbe (4) de cette figure : $P_{DD} = 0.99$ et $P_C = 0.9$ et la courbe (5) : $P_{DD} = 0.9$ et $P_C = 0.99$ sont très rapprochées ce qui montre que ces deux facteurs jouent un rôle à peu près équivalent dans l'évaluation de la sûreté de fonctionnement du système à détection centralisée.

GRAPHE



$$M = P_c(1-P_m) + (1-P_c)q_0 \qquad U = (1-P_c)(1-q_0)$$

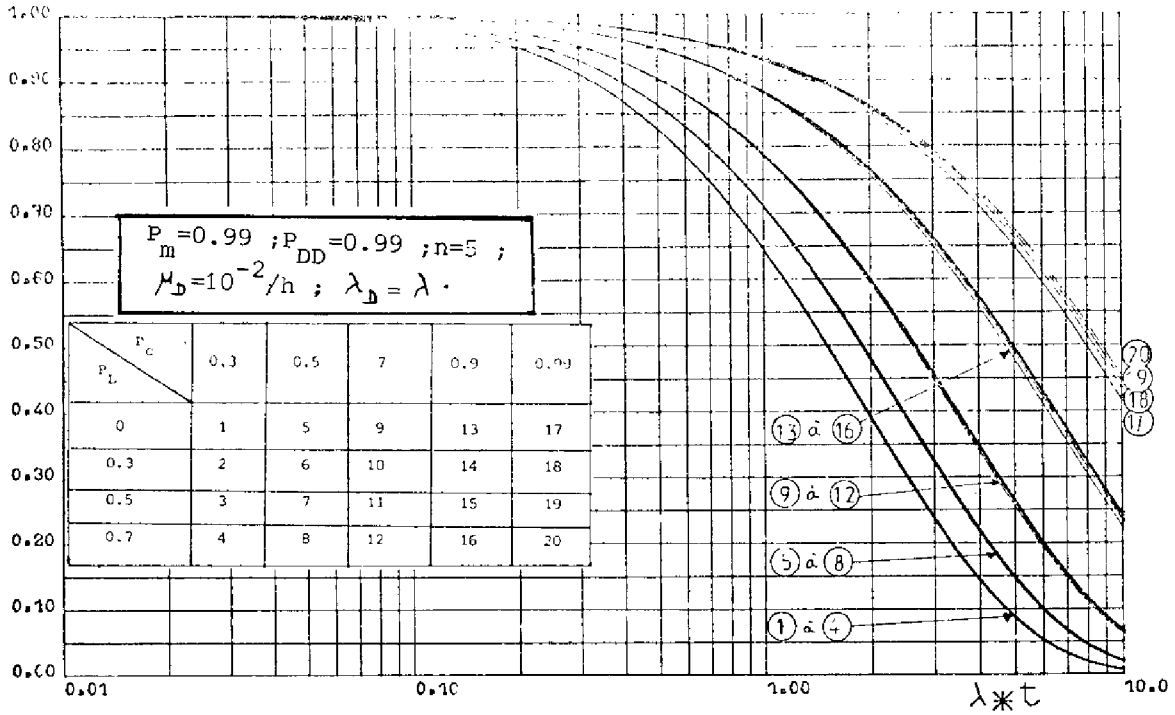
ETATS

(1) : état de bon fonctionnement
(2) : un départ en panne simple
(3) : deux départs en panne simple
(4) : un départ en panne double
(5) : un départ en panne double et un en panne simple

Dans les états (6) à (10) l'organe centralisé de détection est en panne non auto-détectée. Ces états ont respectivement la même signification que les états (1) à (5).

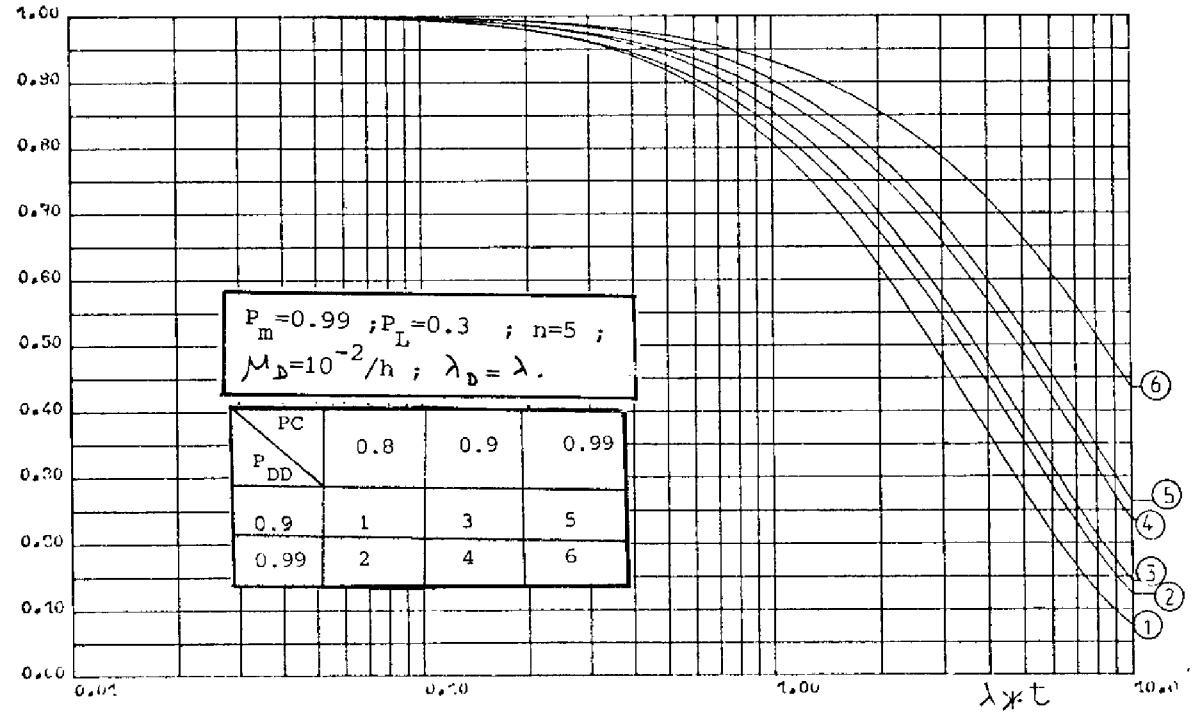
(D) : état défaillant

FIGURE 5.9. Détection centralisée avec temps de réparation du calculateur central infiniment petit



P_L \ P_c	0.3	0.5	7	0.9	0.99
0	1	5	9	13	17
0.3	2	6	10	14	18
0.5	3	7	11	15	19
0.7	4	8	12	16	20

FIGURE 5.10. Détection centralisée. Influence de l'efficacité de la détection locale et de l'efficacité de la détection centrale



P_{DD} \ PC	0.8	0.9	0.99
0.9	1	3	5
0.99	2	4	6

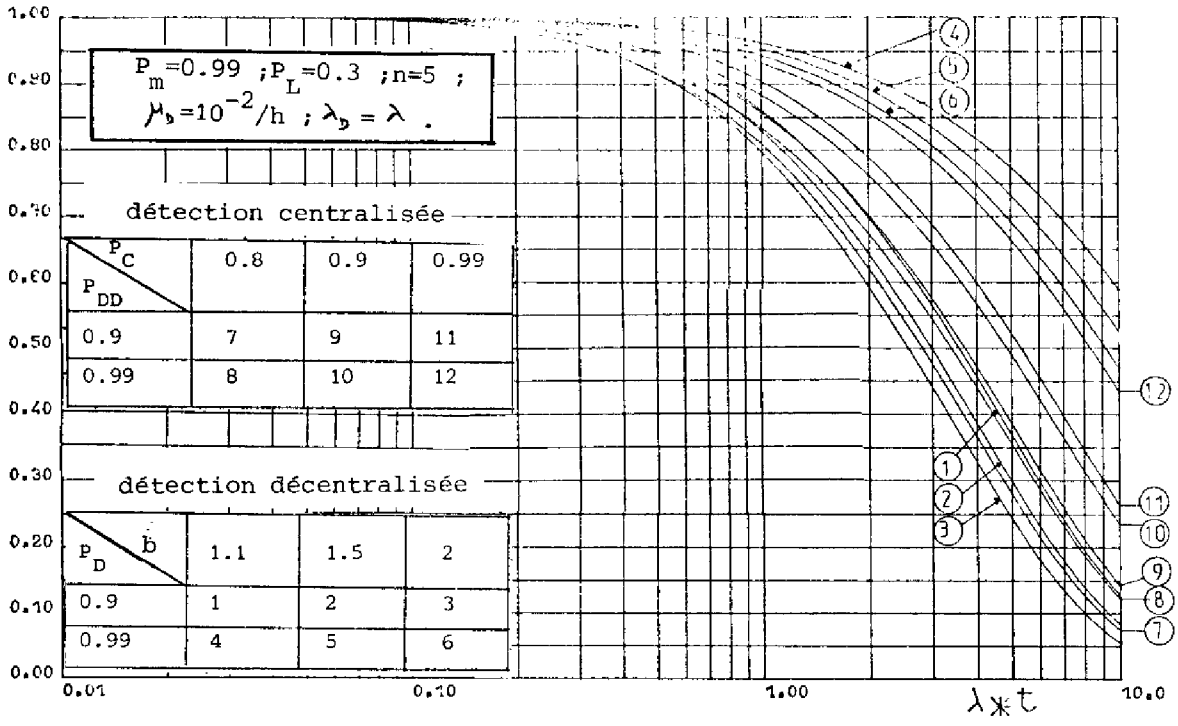
FIGURE 5.11. Détection centralisée : variation de P_c et P_{DD}

5.4. *Comparaison des deux politiques de détection*

Nous avons étudié dans les paragraphes précédents, les caractéristiques propres à chaque architecture ; il est maintenant intéressant de comparer les architectures entre elles afin de disposer d'un critère de sélection.

Pour ce faire, nous avons tracé sur la même figure (Figure 3.12.), la sûreté nominale des deux systèmes en donnant différentes valeurs aux paramètres reconnus comme les plus significatifs à la suite des résultats obtenus dans les paragraphes précédents.

Au vu de ces résultats, il n'est pas possible de dire quelle est l'architecture la meilleure. Selon les valeurs des paramètres, l'une emporte sur l'autre, et réciproquement. Le choix n'est donc pas encore possible lorsque l'on se place à ce niveau d'abstraction. Seules, une description fonctionnelle et une évaluation de la sûreté de fonctionnement plus fines permettront d'effectuer un choix final.



P_{DD} \ P_C	0.8	0.9	0.99
0.9	7	9	11
0.99	8	10	12

P_D \ b	1.1	1.5	2
0.9	1	2	3
0.99	4	5	6

FIGURE 5.12. Comparaison des deux architectures

CONCLUSION

Les résultats exposés dans ce mémoire peuvent être classés en trois catégories selon la généralité de leur applicabilité. En allant du général au spéficique :

- modélisation de la sûreté d'un système complexe,
- évaluation des systèmes de sécurité,
- étude des postes T.H.T.

En ce qui concerne la modélisation de la sûreté, l'approche que nous avons suivie nous semble susceptible de généralisation à tout type de système complexe. Cette approche peut se résumer par les points suivants :

- définition de niveaux de sûreté significatifs pour l'utilisateur, directement à partir de l'énoncé des fonctions du système,
- définition des mesures probabilistes des niveaux de sûreté aisément interprétables physiquement, et vérification par des études de sensibilité de leur bien fondé,
- construction du modèle par agrégation des modèles des sous-ensembles, en effectuant à chaque étape des études de sensibilité afin de ne conserver que les paramètres ayant effectivement une influence.

Dans une telle démarche, la question qui se pose alors est : quelle est la validité du modèle ? Devant l'impossibilité de confronter le modèle obtenu à un hypothétique "modèle complet", la réponse que nous donnons est : signification physique de tous les résultats, à chaque étape.

En ce qui concerne l'évaluation des systèmes de sécurité, les résultats obtenus peuvent être classés en deux catégories :

- modèles des systèmes de sécurité : le principal résultat est à notre avis l'influence des fautes masquées : il est nécessaire de prendre en compte deux fautes masquées successives,
- retombées de l'évaluation sur l'architecture : deux points sont à souligner ici :
  - .l'extrême importance des mécanismes de détection des fautes,
  - .l'accent qui doit être mis dans les procédures de maintenance sur l'efficacité de la réparation plus que sur sa durée.

En ce qui concerne l'étude des postes T.H.T., l'ensemble des résultats obtenus constitue une base de données (modèles, processus, paramètres de structures,...) qui servira de référence tant dans la méthode que dans les résultats quantitatifs pour la recherche de nouvelles architectures utilisant la méthode générale mise au point au sein de l'équipe "Architectures Sûres de Fonctionnement".

Cette étude nous paraît riche d'enseignements sur deux plans au moins :

- d'un strict point de vue scientifique, la rigueur de la démarche,
- d'un point de vue de l'utilisation des résultats par le secteur socio-économique, les résultats obtenus constitueront pour notre partenaire, E.D.F., une aide à la définition du cahier des charges des futurs équipements des postes T.H.T.

L'ensemble des résultats exposés dans ce mémoire est bien entendu susceptible de nombreux développements. Nous n'insisterons pas dans cette optique sur les postes T.H.T., dont l'étude en collaboration avec E.D.F. est actuellement activement poursuivie. En ce qui concerne les systèmes de sécurité en général et compte tenu de leur importance croissante dans la capacité à maîtriser les risques industriels majeurs engendrés par notre société industrielle, nous pensons qu'il est nécessaire d'effectuer des études sur :

- la prise en compte dans la définition des niveaux de sûreté des concepts de barrière de confinement et d'élimination dégradée,
- l'établissement des modèles incluant toutes les sources de fautes susceptibles de se manifester.

ANNEXE

MÉTHODE SUIVIE POUR LA RÉDUCTION DES GRAPHES

-

Dans le cas où il existe un taux de transition qui est plus grand (beaucoup plus grand) que les autres, il est possible d'émettre des hypothèses simplificatrices :

H1) la probabilité que le système reste dans un état où agit la variable dont le taux de transition est grand est négligeable,

H2) la probabilité qu'il y ait une autre action que l'action due à la variable concernée est négligeable.

Si l'on note μ_i le taux concerné qui va agir dans l'état i, et λ_{ij} les autres taux, ces deux hypothèses s'écrivent alors :

H1) $1 + (-\mu_i - \sum_{\forall j, i \neq j} \lambda_{ij})\, dt = \sigma(dt)$

ou $1 + (\lambda_{ii} - \mu_i)\, dt = \sigma(dt)$ avec $\lambda_{ii} = -\sum_{\forall j, i \neq j} \lambda_{ij}$

H2) $\lambda_{ij}\, dt = \sigma(dt) \quad \forall j \neq i$

Suivant que l'on prend en compte les deux hypothèses simultanément ou bien seulement l'hypothèse H1 on aboutit aux résultats présentés dans les prochains paragraphes.

A.1. - Prise en compte des hypothèses H1 et H2

Si l'on ordonne les états que peut prendre le système de telle manière que les n_1 premiers états ne sont pas soumis à la variable concernée (taux de transition de μ_i) on peut alors écrire en appliquant le théorème des probabilités totales :

$$\begin{cases} P_j(t+dt) = \sum_{i=1}^{n_1} (\delta_{ij} + \lambda_{ij}\, dt)\, P_i(t) + \sum_{i=n_1+1}^{n} (\alpha_{ij}\mu_i + \lambda_{ij})\, dt\, P_i(t) & \forall j \in \{1, \ldots, n_1\} \\ P_j(t+dt) = \sum_{i=1}^{n_1} \lambda_{ij}\, dt\, P_i(t) + \sum_{i=n_1+1}^{n} [\delta_{ij} + (\alpha_{ij}\mu_i + \lambda_{ij})\, dt]\, P_i(t) & \forall j \in \{n_1+1, \ldots, n\} \end{cases}$$

où δ_{ij} est le symbole de Kronecker ($\delta_{ij} = 0$ si $i \neq j$, $\delta_{ij} = 1$ si $i = j$)

$$\sum_{j=1}^{n} \alpha_{ij} = 0 \quad , \quad \alpha_{ii} = -1 \left(\sum_{\substack{j=1 \\ j \neq i}}^{n} \alpha_{ij} = 1 \right)$$

Les hypothèses H1 et H2 qui s'écrivent

- $1 + (\lambda_{ii} - \mu_i)\, dt = \sigma(dt)$
- $\lambda_{ij}\, dt = \sigma(dt)$ (dans un état où la variable concernée agit)

peuvent aussi s'écrire :

- $1 - \mu_i\, dt = \sigma(dt) \quad \left(\lambda_{ii}\, dt = -\sum_{\substack{\forall j \\ i \neq j}} \lambda_{ij}\, dt = 0 \right)$
- $\lambda_{ij}\, dt = \sigma(dt)$ (dans un état où agit la variable concernée)

En utilisant ces deux dernières relations on arrive alors à :

$$\begin{cases} P_j(t+dt) = \sum_{i=1}^{n_1} (\delta_{ij} + \lambda_{ij}\,dt)\, P_i(t) + \sum_{i=n_1+1}^{n} \alpha_{ij}\, P_i(t) & \forall j \in \{1, \dots, n_1\} \\ P_j(t+dt) = \sum_{\substack{i=1 \\ i \neq j}}^{n_1} \lambda_{ij}\, P_i(t)\, dt + \sum_{i=n_1+1}^{n} \alpha_{ij}\, P_i(t) & \forall j \in \{n_1+1, \dots, n\} \end{cases}$$

Si l'on utilise les notations matricielles suivantes

$$(\lambda_{ij}) = \begin{pmatrix} \Pi_1^\lambda & \Pi_2^\lambda \\ \textcircled{0} & \textcircled{0} \end{pmatrix} \begin{matrix} \} n_1 \\ \} n-n_1 \end{matrix}$$

$$\underbrace{}_{n_1} \quad \underbrace{}_{n-n_1}$$

$$(\alpha_{ij}) = \mathbb{A} = \begin{pmatrix} \textcircled{0} & \textcircled{0} \\ \mathbb{A}_1 & \mathbb{A}_2 \end{pmatrix} \begin{matrix} \} n_1 \\ \} n-n_1 \end{matrix}$$

$$\underbrace{\phantom{\mathbb{A}_1}}_{n_1} \quad \underbrace{\phantom{\mathbb{A}_2}}_{n-n_1}$$

$$\mathbb{P}(t) = [\underbrace{\mathbb{P}_1(t)}_{n_1}, \underbrace{\mathbb{P}_2(t)}_{n-n_1}]$$

On peut écrire ces deux relations sous la forme suivante :

$$\begin{cases} \mathbb{P}_1(t+dt) = \mathbb{P}_1(t)[\mathbb{I} + \Pi_1^\lambda\, dt] + \mathbb{P}_2(t)\, \mathbb{A}_1 \\ \mathbb{P}_2(t+dt) = \mathbb{P}_1(t)\, \Pi_2^\lambda\, dt + \mathbb{P}_2(t)\, [\mathbb{A}_2 + \mathbb{I}] \end{cases}$$

(le terme $\mathbb{A}_2 + \mathbb{I}$ s'explique par le fait que $\alpha_{ii} = -1$)

Si maintenant on développe $\mathbb{P}_2\,(t + dt)$ en série de Taylor au premier ordre, on obtient :

$$\mathbb{P}_2(t+dt) = \mathbb{P}_2(t) + \dot{\mathbb{P}}_2(t)\, dt + o(dt)$$

Si on porte cette valeur de $\mathbb{P}_2\,(t + dt)$ dans la deuxième relation on a

$$\mathbb{P}_2(t) + \dot{\mathbb{P}}_2(t)\, dt = \mathbb{P}_1(t)\, \Pi_2^\lambda\, dt + \mathbb{P}_2(t)\, \mathbb{A}_2 + \mathbb{P}_2(t)$$

$$\mathbb{P}_2(t)\,\mathbb{A}_2 = \dot{\mathbb{P}}_2(t)\,dt - \mathbb{P}_1(t)\,\Gamma_2^{\lambda}\,dt$$

$$\mathbb{P}_2(t) = \left(\dot{\mathbb{P}}_2(t) - \mathbb{P}_1(t)\,\Gamma_2^{\lambda}\right)\mathbb{A}_2^{-1}\,dt$$

En portant cette valeur de $\mathbb{P}_2$ (t) dans la première relation on obtient :

$$\mathbb{P}_1(t+dt) = \mathbb{P}_1(t)\left[\mathbb{I} + \left(\Gamma_1^{\lambda} - \Gamma_2^{\lambda}\,\mathbb{A}_2^{-1}\,\mathbb{A}_1\right)dt\right] + \dot{\mathbb{P}}_2(t)\,\mathbb{A}_2^{-1}\,\mathbb{A}_1\,dt$$

Si l'on fait tendre dt vers zéro $\mathbb{P}_2(t)$ tend vers zéro ainsi que $\dot{\mathbb{P}}_2(t)$ (pas de discontinuité) et l'on peut alors écrire :

$$\dot{\mathbb{P}}_1(t) = \lim_{dt \to 0} \frac{\mathbb{P}_1(t+dt) - \mathbb{P}_1(t)}{dt} = \mathbb{P}_1(t)\left[\Gamma_1^{\lambda} - \Gamma_2^{\lambda}\,\mathbb{A}_2^{-1}\,\mathbb{A}_1\right]$$

A partir de cette relation on calcule donc les probabilités $P_i(t)$ de se trouver dans le n_1 premiers états de la structure les autres probabilités $P_k(t)$ $(k \in \{n_1 + 1, \ldots n\})$ étant nulles.

Cette relation serait la relation de Chapman Kolmogorov d'un système dont la matrice de transition serait égale à :

$$\Gamma_1^{\lambda} - \Gamma_2^{\lambda}\,\mathbb{A}_2^{-1}\,\mathbb{A}_1$$

C'est à dire que l'on a réduit le graphe de départ à un graphe à n_1 états ayant pour matrice de transition la matrice

$$\Gamma_1^{\lambda} - \Gamma_2^{\lambda}\,\mathbb{A}_2^{-1}\,\mathbb{A}_1$$

D'un point de vue pratique, la marche à suivre pour obtenir le nouveau graphe à partir de l'ancien peut se résumer par la procédure suivante :

1) supprimer les transitions (agissant sur l'(les) état (s)) autre (s) que celle (s) de la variable que l'on cherche à supprimer (c'est l'hypothèse H2),
2) remplacer la variable que l'on cherche à supprimer par 1,
3) supprimer les états où agissaient la variable,
4) supprimer les bouclages sur état,

Cette procédure est schématisée dans le cas précédent par la figure A.1.

A .2- Prise en compte de l'hypothèse H1 seule

Dans ce cas, on néglige la probabilité d'être dans les états où la variable agit, par contre on tient compte des possibles actions d'autres variables.

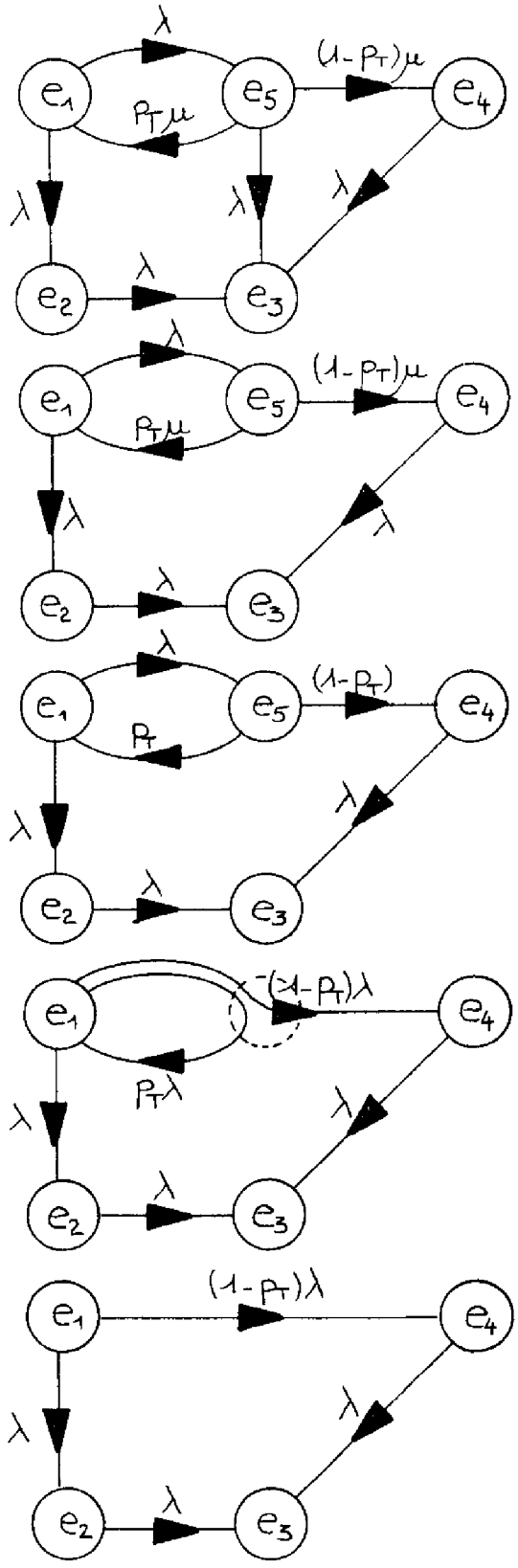

λ
(1-pT)μ
e1
e5
e4
pTμ
λ
λ
λ
e2
λ
e3
graphe au départ
λ
(1-pT)μ
e1
e5
e4
pTμ
λ
λ
e2
λ
e3
1ère étape
λ
(1-pT)
e1
e5
e4
pT
λ
λ
e2
λ
e3
2ème étape
-(1-pT)λ
e1
e4
pTλ
λ
λ
e2
λ
e3
3ème étape
4ème étape
(1-pT)λ
e1
e4
λ
λ
e2
λ
e3

FIGURE A.1.

Dans ce cas on a donc seulement la relation :

$$1 + (\lambda_{ii} - \mu_i)\,dt = o(dt)$$

$$dt = \frac{1}{\mu_i - \lambda_{ii}} + o(dt)$$

ce qui permet d'écrire :

$$\mu_i\,dt = \frac{\mu_i}{\mu_i - \lambda_{ii}} + o(dt)$$

$$(\lambda_{ij} + \alpha_{ij}\mu_i)\,dt = \frac{\lambda_{ij} + \alpha_{ij}\mu_i}{\mu_i - \lambda_{ii}} + o(dt)$$

En raisonnant de manière identique au cas précédent on arrive à :

$$\begin{cases} P_j(t+dt) = \sum_{i=1}^{n_1} (\delta_{ij} + \lambda_{ij}\,dt)\,P_i(t) + \sum_{i=n_1+1}^{n} \frac{\alpha_{ij}\mu_i + \lambda_{ij}}{\mu_i - \lambda_{ii}} P_i(t) & \forall j \in \{1, \dots, n_1\} \\ P_j(t+dt) = \sum_{i=1}^{n_1} \lambda_{ij} P_i(t) + \sum_{\substack{i=n_1+1 \\ i \neq j}}^{n} \frac{\alpha_{ij}\mu_i + \lambda_{ij}}{\mu_i - \lambda_{ii}} P_i(t) & \forall j \in \{n_1+1, \dots, n\} \end{cases}$$

Et finalement en utilisant les notations matricielles supplémentaires suivantes :

$$^*\mathbb{A}_2 = \left(\frac{\alpha_{ij}\mu_i + \lambda_{ij}}{\mu_i - \lambda_{ii}}\right) \qquad i, j \in \{n_1+1, \dots, n\}$$

$$^*\mathbb{A}_1 = \left(\frac{\alpha_{ij}\mu_i + \lambda_{ij}}{\mu_i - \lambda_{ii}}\right) \qquad i \in \{n_1+1, \dots, n\},\ j \in \{1, \dots, n_1\}$$

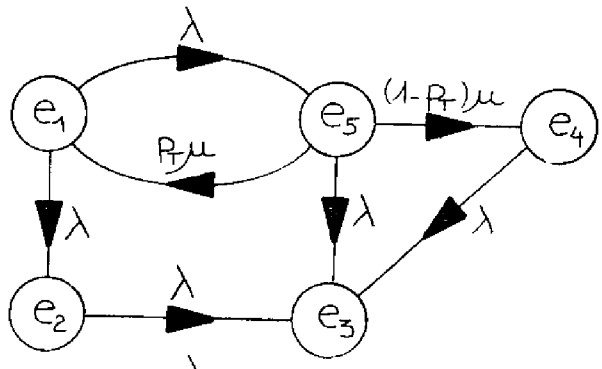
on obtient la relation :

$$\dot{\mathbb{P}}_1(t) = \mathbb{P}_1(t)\left[\,\mathbb{\Gamma}_1^{\lambda} - \mathbb{\Gamma}_2^{\lambda}\,{}^*\mathbb{A}_2^{-1}\,\mathbb{A}_1\,\right]$$

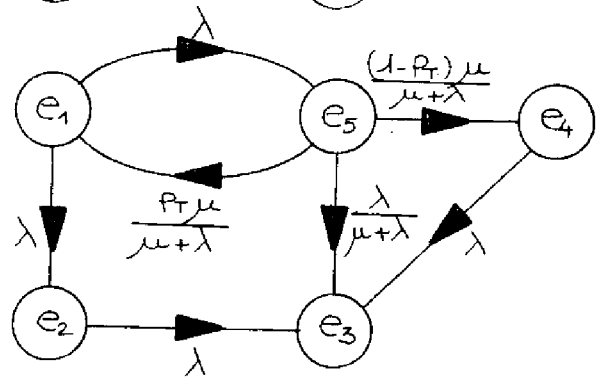
D'un point de vue pratique, la marche à suivre pour obtenir le nouveau graphe à partir de l'ancien peut se résumer par la procédure suivante :

1) faire la somme des taux sortant d'un état où agit la variable considérée,
2) diviser tous les taux sortant de l'état par cette somme (recommencer les étapes 1 et 2 pour tous les états concernés),
3) supprimer l'(es)état (s),
4) supprimer les bouclages sur état (s).

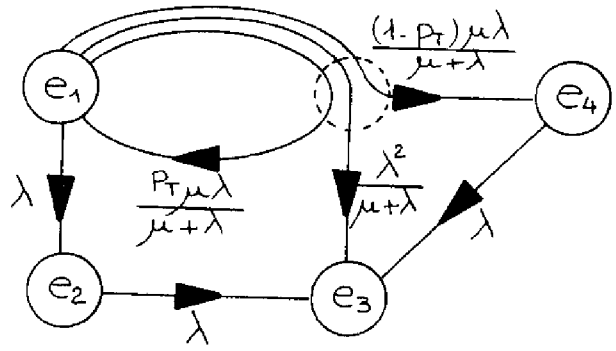
Cette procédure est schématisée dans le cas précédent par la figure A.2.



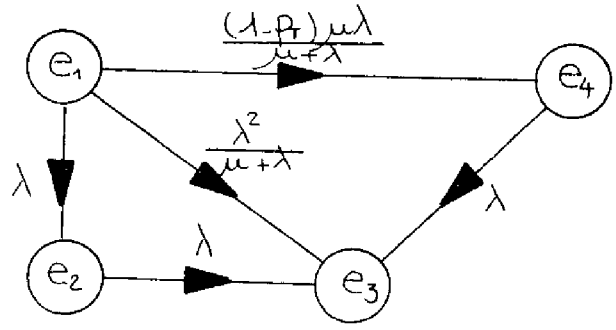
graphe de départ



1ère et 2ème étapes



3ème étape



4ème étape

FIGURE A.2.

BIBLIOGRAPHIE

ACT 76 Rapport d'activité E.D.F. 76.

APO 77 G.E. APOSTOLAKIS, P.P. BANSAL, "Effect of human errors on the availability of periodically inspected redundant systems", IEEE Trans. on Reliability, vol.R-26, n°3, Août 77, pp.220-225.

ARN 72 T.F. ARNOLD, "The concept of coverage and its effect on the reliability model of a repairable system", Proc. of the 2nd International Conference on Fault-Tolerant Computing, Newton, Massachussetts, 19-21 Juin 1972, pp.200-204.

BEO 77 C. BEOUNES, "Automate sûr et modulaire adapté aux régulations avioniques : A.S.M.A.R.A.", Thèse de Docteur-Ingénieur, Université Paul Sabatier, Toulouse, Novembre 1977.

BOU 69 W.G. BOURRICIUS, W.C. CARTER, P.R. SCHNEIDER, "Reliability modeling techniques for self-repairing computer systems", Proc. of the 12th ACM National Conference, Août 1969, pp.295-309.

COS 78 A. COSTES, C. LANDRAULT, J.C. LAPRIE, "Reliability and availability models for maintained systems featuring hardware failures and design faults", IEEE Transactions on Computers, vol.C-27, n°6, Juin 1978, pp.548-560.

COS 79 A. COSTES, J.E. DOUCET, C. LANDRAULT, J.C. LAPRIE, "SURF : Système d'évaluation de la sûreté de fonctionnement ; 1ère Partie : Méthode", Note Technique 79.T.37 ; J.E. DOUCET "2ème Partie : Notice d'utilisation", Note Technique 79.T.38, L.A.A.S., Toulouse, Septembre 1979.

EDF 74 Le plan de protection "palier technique 1975" ses principes, Novembre 1975.

D. MANIGLIER, Automatismes des postes T.H.T./H.T.

Spécifications fonctionnelles et technologiques de l'ALPL D.651/74-12

Spécifications fonctionnelles et technologiques de l'ALPI D.651/74-19a

Spécifications fonctionnelles et technologiques de l'ALPC D.651/74-18

Spécifications fonctionnelles et technologiques de l'AMD D.651/74-44

Spécifications fonctionnelles et technologiques de l'ALPT D.651/74-14

FRE 74 H.F. FREY, "Safety evaluation of mass transit systems by reliability analysis", IEEE Transactions on Reliability, vol.R-23, n°3, Août 1974, pp.161-169.

GAY 79 F.A. GAY, "Performance modeling for gracefully degrading systems", Ph.D. Dissertation, Northwestern University, Evanston, Illinois, Juin 1979.

LAN 77 C. LANDRAULT, "Prévision de la sûreté de fonctionnement des systèmes numériques réparables", Thèse de Doctorat ès-Sciences, Institut National Polytechnique de Toulouse, 11 Mars 1977.

LAP 75 J.C. LAPRIE, "Reliability and availability of repairable structures", Digest of the Fifth International Symposium on Fault Tolerant Computing, Paris, Juin 1975, pp.87-92

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

LAP 79 J.C. LAPRIE, F. CEREJA, K. MEDHAFFER, "Etude de nouvelles architectures sûres de fonctionnement pour les automatismes de protection et de reprise de service des postes à très haute tension", E.D.F. Contrat n° 47559, Rapport final, L.A.A.S. Publication n°1894, Toulouse, Février 1979.

LIE 76 C. LIEVENS, "Sécurité des systèmes", Cepadues Edition, Toulouse, 1976.

MEW 79 R.N. MEWIES, "Triplicated microprocessor controlled automatic shutdown system", Microprocessors and Microsystems, vol.3, n°8, Octobre 1979, pp.347-351.

MEY 78 J.F. MEYER, "On evaluating the performability of degradable computing systems", Proc. of the 8th International Symposium on Fault-Tolerant Computing (FTCS-8), Toulouse, Juin 1978, pp.44-49.

PED 78 E.S. PEDERSEN, "Nuclear power", 2 volumes, Ann-Arbor Science, 1978.

PRE 67 F.P. PREPARATA, G. METZE, R.T. CHIEN, "On the connection assignment problem of diagnosable systems", IEEE Transactions on Electronic Computers, vol.EC-16, Décembre 1967, pp.848-854.

SHE 75 J.J. SHEDLETSKY, E.J. McCLUSKEY, "The error latency of a fault in a combinational digital circuit", Proc. of the 5th International Symposium on Fault-Tolerant Computing (FTCS-5), Paris, Juin 1975, pp.210-214.

STI 78 J.J. STIFFLER, "Fault-coverage and the point of diministring returns", Journal of Design Automation and Fault-Tolerant Computing, vol.3, n°2, Octobre 1978, pp.289-301.

SYN 75 Syndicat C.F.D.T. de l'Energie Atomique, "L'Electronucléaire en France", Editions du Seuil, Collection Points, 1975.

TRA 75 Traitement des signalisations nécessaires à la conduite et à la surveillance des installations, Septembre 1975.

TABLE DES MATIERES
