L'action des Pouvoirs publics ne se limite pas à fixer les directives générales qui doivent être suivies dans l'établissement de diverses normalisations. Il suffit pour s'en convaincre de lire la « Lettre 101 » du 11 décembre 1979 [lettre d'information du ministère de l'Industrie (1)]. On constate que les principales orientations fixées par les Pouvoirs publics sont (suivant le paragraphe « Pour une durée de vie optimale des produits ») :

- développer l'information des consommateurs avant et après l'achat;
- revaloriser la fonction maintenance;
- « développer les outils techniques (banques de données sur les causes de fin de vie ou de pannes, les coûts globaux d'usage, mise au point de méthodes et de moyens d'essais de fiabilité et durabilité) ».

Sur ce dernier point, nous citerons l'exemple de l'électroménager pour lequel le Laboratoire National d'Essais (L.N.E.) a été chargé de mettre au point, à titre d'expérience pilote, des critères d'usage et des méthodes d'essais normalisées pour deux types d'appareils domestiques de grande diffusion. La première étape de l'étude qui vient de démarrer est relative au casque sèche-cheveux dont la recherche de la fiabilité et de la durabilité a été confiée par le L.N.E. à notre organisme. La méthodologie retenue sera utilisée pour tout ou partie, dans l'étude du lave-linge.

2.2. – ACTIONS DES MÉDIAS ET DES ORGANISMES DE CONSOMMATEURS

Il n'est pas question de faire ici un inventaire complet de tout ce que l'on peut lire, entendre ou voir concernant la Fiabilité. Il est cependant significatif de noter que dans le texte de nombreuses publicités les termes « fiabilité » ou « fiable » sont utilisés et ceci dans des domaines très différents (automobile, transport, électronique...).

Il n'y a cependant pas que des actions publicitaires. C'est ainsi qu'en ce qui concerne l'automobile, deux enquêtes, au moins, ont été effectuées auprès d'utilisateurs dans le but de juger de la Fiabilité des véhicules.

Nous citerons :

- une enquête de l'Union Fédérale des Consommateurs, publiée dans la revue « Que Choisir » (N°s 145 et 146 de Novembre et Décembre 1979), effectuée sur « l'usage, le confort, l'entretien et la Fiabilité » de véhicules de constructions française et étrangère. Une nomenclature des pannes les plus courantes est donnée; pour chaque modèle et chaque année de fabrication, une appréciation sur le nombre de pannes est portée (par rapport à un nombre moyen), la taille de l'échantillon étant systématiquement précisée.
- une enquête de la revue « L'Action Automobile et Touristique », réalisée à partir d'un questionnaire intitulé : « A vous de juger la Fiabilité de votre voiture » et publiée dans les n°s 230 (Janvier 1980), 231 (Février 1980), 232 (Mars 1980), 233 (Avril 1980)... Une appréciation chiffrée (notes de 1 à 10) est donnée sur les principaux constituants des véhicules ainsi que sur le service après-vente. Le nombre de réponses n'est pas précisé de façon systématique.

Enfin les Associations de Consommateurs sont représentées dans le groupe de réflexion créé par le ministère de l'Industrie et par le ministère de l'Économie sur tous les aspects liés à la durée de vie (groupe « Fayard »).

2.3. – ACTIONS DE GROUPEMENTS PROFESSIONNELS ET D'ENTREPRISES

Nous donnerons ici quelques exemples de contribution à la promotion de la Fiabilité et des disciplines associées :

- actions systématiques de différentes associations :
  - Association Française pour le Contrôle Industriel de Qualité (A.F.C.I.Q.);
  - Association Française des Qualiticiens (A.F.Q.);
  - Société des Ingénieurs de l'Automobile (S.I.A.).

  ...
- actions de groupes de travail :

  En ce qui concerne la Fiabilité en Mécanique :
  - groupe de travail A.F.C.I.Q.;
  - groupe de travail du Comité de Coordination des Télécommunications (C.C.T.).

  Nous reviendrons sur l'activité de ces groupes au paragraphe 3.
- actions d'information et de sensibilisation :

  A titre d'exemple :
  - colloque A.F.N.O.R. « Durée de vie des biens d'équipements industriels : des professionnels font le point » (23-24 avril 1980);
  - deuxième congrès International de Fiabilité et Maintenabilité (8 au 12 septembre 1980 à Perros-Guirec).
  - actions de formation aux différentes techniques de la Fiabilité;
  - actions d'incitation contenues dans les contrats : Les clauses de Fiabilité, Maintenabilité, Disponibilité touchent non seulement l'Électronique mais également l'Électromécanique et la Mécanique (exemple : Métro de Caracas dont nous parlerons plus loin).

2.4. – CONCLUSION

Le rapide tour d'horizon que nous venons de faire conduit à constater qu'un aspect du développement récent en matière de Fiabilité et Durabilité est constitué par l'emploi de plus en plus fréquent de ces termes, dans des circonstances et en des lieux très variés.

3. – QUELQUES EXEMPLES DU DÉVELOPPEMENT DES TECHNIQUES DE FIABILITÉ ET DURABILITÉ

3.1. – ÉTUDES DE PRÉVISION AVEC RECHERCHE DE LA DISPONIBILITÉ ET ANALYSE DES FACTEURS INFLUANT SUR CELLE-CI

La fiabilité d'un matériel est relative au contexte d'utilisation. Il était donc tout naturel que les premières études de Fiabilité de matériels mécaniques ou électromécaniques aient été relatives au suivi en exploitation de ces produits (analyse des retours en garantie...). Cette approche, toujours nécessaire, est complétée de plus en plus par la prise en compte de la Fiabilité dès la conception.

En fait, du point de vue de l'utilisateur, il apparaît qu'une caractéristique essentielle du bien qu'il possède est sa *disponibilité;* celle-ci traduit le fait que l'appareil n'est pas en panne, n'est pas en réparation ou ne subit pas une opération de maintenance. Ce concept est traduit imparfaitement par la notion de disponibilité moyenne, généralement rencontrée cependant :

$$D_m = \frac{\text{M.T.B.F.}}{\text{M.T.B.F.} + \text{M.T.T.R.}}$$

avec : M.T.B.F. : Mean Time Between Failures
(moyenne des temps entre défaillances),
M.T.T.R. : Mean Time To Repair
(moyenne des temps des tâches de réparation).

La disponibilité est de toute manière fonction de la fiabilité du produit et de son aptitude à la maintenance.

La tendance des études actuelles est de rechercher un « juste équilibre » entre la fiabilité et la maintenabilité.

Le schéma de la figure 1 illustre une démarche type utilisée au stade de la *conception :* cet exemple est relatif au Métro de Caracas (2).

Nous reviendrons ultérieurement sur la répartition entre objectifs de fiabilité et de maintenabilité.

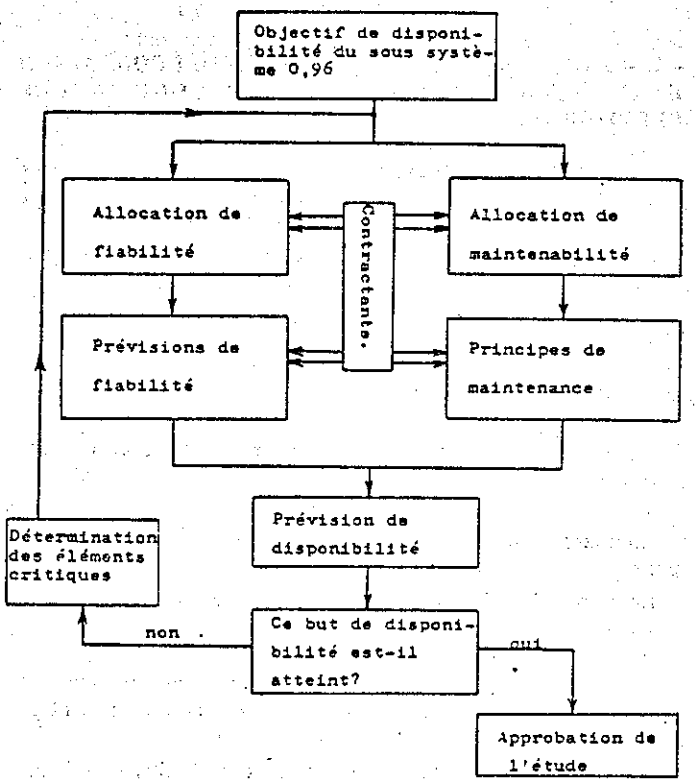


Fig. 1. – Organisation générale des tâches de disponibilité.

Pour l'instant, supposons que cette étape soit réalisée et intéressons-nous aux deux points suivants :

- prévisions de fiabilité;
- principes de maintenance.

Il est inutile de dire que ces deux points sont fondamentaux et seront abordés dans différentes conférences de ces deux journées.

La démarche actuelle consiste, lorsque cela est possible, non seulement à faire une étude prévisionnelle de manière à répondre à un objectif *chiffré* mais également à rechercher *l'influence* de différents paramètres sur le résultat escompté et, par là même, à tenter une optimisation.

Nous renvoyons le lecteur aux exposés suivants pour ce qui est de l'application de cette approche à la maintenabilité (conséquence des principes de maintenance).

En ce qui concerne les prévisions de fiabilité, différentes voies sont envisageables :

- utilisation de recueils de données;
- calculs de fiabiiité des systèmes à partir de la connaissance de la fiabilité des composants et de la configuration du système;
- calculs prévisionnels en mécanique, tirés de l'approche « stress-strength », particulièrement utiles dans les problèmes de fatigue et de mécanique de la rupture;
- essais de fiabilité de pièces ou de sous-ensembles (essais complets, suspendus, par mort soudaine, séquentiels, accélérés, ..., plans d'expériences).

Remarques :

– Les électroniciens connaissent le recueil de données de fiabilité du C.N.E.T.

– Il paraît important de signaler l'existence d'un groupe de travail « Recueil de Données de Fiabilité en Mécanique », placé sous l'égide du Comité de Coordination des télécommunications et animé par M. Ligeron. Ce groupe de travail publiera très prochainement un document qui représente une synthèse des sources et méthodes utilisables pour effectuer des études de Fiabilité en Mécanique. Ce document complétera le guide d'évaluation de la Fiabilité en Mécanique élaboré par le groupe de travail « Fiabilité en Mécanique » de l'A.F.C.I.Q., animé par M. Chaubaroux; ce document sera édité très prochainement par l'A.F.N.O.R.

– De son côté, la Commission Électrotechnique internationale a publié récemment des textes sur les « Essais de Fiabilité des Équipements » (3).

3.2. – PRISE EN COMPTE DES COUTS

De la lecture du paragraphe précédent découlent au moins deux interrogations :

– On imagine qu'*a priori,* il est rentable de payer un produit un peu plus cher pour avoir moins de pannes donc une meilleure fiabilité : mais jusqu'où faut-il aller?

– Quand le matériel devient vieux, les pannes nombreuses nécessitent une maintenance importante qui a de lourdes conséquences sur le coût d'utilisation et sur la disponibilité. Quand faut-il envisager le renouvellement d'un matériel?

Il n'est pas possible d'apporter dans cet exposé à caractère général de réponses détaillées à ces questions qui correspondent à un développement récent du sujet de ces journées : la prise en compte du coût de cycle de vie d'un produit. Ce point sera traité par M. Chaigneau et apportera des éléments de réponse aux conséquences du choix des allocations de fiabilité et maintenabilité.

Revenons cependant sur la deuxième question et comparons son contenu avec celui de la définition de la durabilité donnée au paragraphe 2.1.

Nous constatons qu'il s'agit de la même idée exprimée différemment.

La recherche de la *durabilité* d'un produit suppose donc d'avoir défini :

- les critères d'usage du produit;
- le critère économique qui conduira à remplacer ce produit par un produit neuf.

Ce dernier critère peut s'exprimer par un coût de maintenance « intolérable » rapporté au prix d'achat ou bien encore à la valeur vénale (elle-même liée au prix d'achat). C'est l'hypothèse du schéma de la figure 2 (4).

L'unité d'usage, en abscisse de la figure 2, correspond au cycle le plus court significatif de l'usage d'un bien (un kilomètre, une lessive, une vaisselle, ...).

L'approche « coût de cycle de vie » qui sera étudiée ultérieurement et qui intègre coût d'achat, de fonctionnement et d'entretien, permet de chiffrer le coût de l'unité d'usage, d'en étudier la variation et par suite de définir rationnellement la période à laquelle il faut changer le produit, c'est-à-dire la durabilité.

Il apparaît donc que la notion de durabilité est complexe : elle est liée à la maintenance donc à la fiabilité et à l'aptitude du bien à être réparé (conception modulaire, interchangeabilité...) mais peut être limitée par différents facteurs : absence de pièces de rechange, obsolescence...

Optimisation de la sécurité d'un système au stade de la conception

par MM. A. Viney, J. Debray, M. Blot, F. Bonneval* et M. Lecrivain**

1. – INTRODUCTION

Cet exposé donne une méthodologie d'attaque des problèmes Fiabilité-Sécurité dès le stade de l'avant-projet.

Extrait des Travaux Novatome, il montre comment la sécurité et la fiabilité (vue dans le sens du succès de la mission) peuvent être prises en compte dès le départ de la conception d'un système, au même titre que les paramètres habituels d'avant-projet (masse, encombrement, coût, performances...) et de quelle manière on peut les introduire dans l'optimisation des différents choix (schémas, technologies, dimensionnement, redondances...).

L'application au départ d'un critère de redondance déterministe impliquant dans l'exemple traité :

- 3 redondances pour les défaillances de gravité 3 (sécurité des passagers);
- 2 redondances pour les défaillances de gravité 2 (sécurité mission);

permet :

- de démarrer un projet en aidant le concepteur à sélectionner sur des bases analytiques simples un nombre restreint de schémas sains (1) sur le plan de la sécurité et conformes aux conditions opérationnelles de fonctionnement;
- de mieux évaluer les difficultés que le projet risque de rencontrer au cours de son développement;

et évite d'opter pour des choix sur lesquels il est parfois difficile de revenir.

Puis un affinage probabiliste conduit :

- à se prononcer sur le meilleur choix entre des solutions concurrentes, toutes conformes aux critères sécurité;
- à une première sécurisation, en s'assurant que le schéma retenu satisfait bien les conditions contractuelles d'allocations de fiabilité.

Afin d'être présenté sous un aspect concret, l'exposé est étayé d'un exemple d'application au « Conditionnement Habitacle de la Navette spatiale européenne ».

Nous montrons ensuite, comment moyennant quelques aménagements, sa transposition à l'automobile est envisageable et les avantages que l'on peut en attendre.

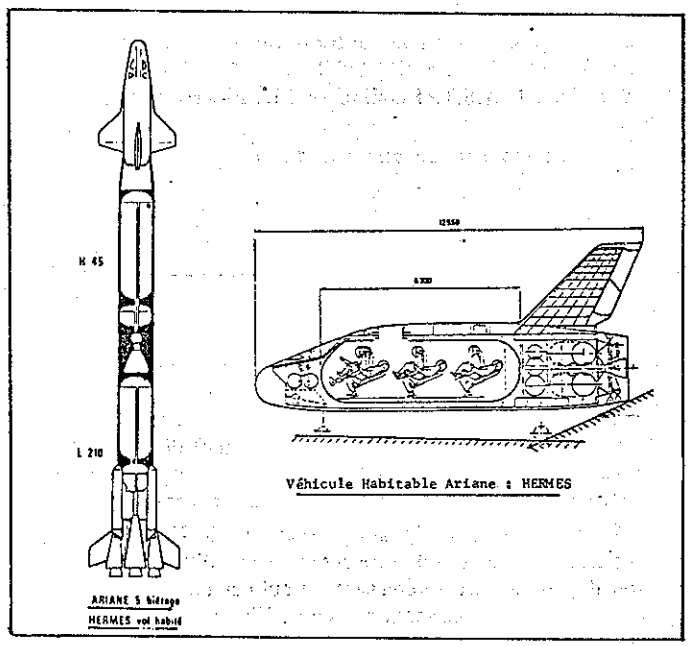
(1) Conformes dans le cas présent aux critères Sécurité-Fiabilité imposés par le C.N.E.S. (Centre National d'Études Spatiales).

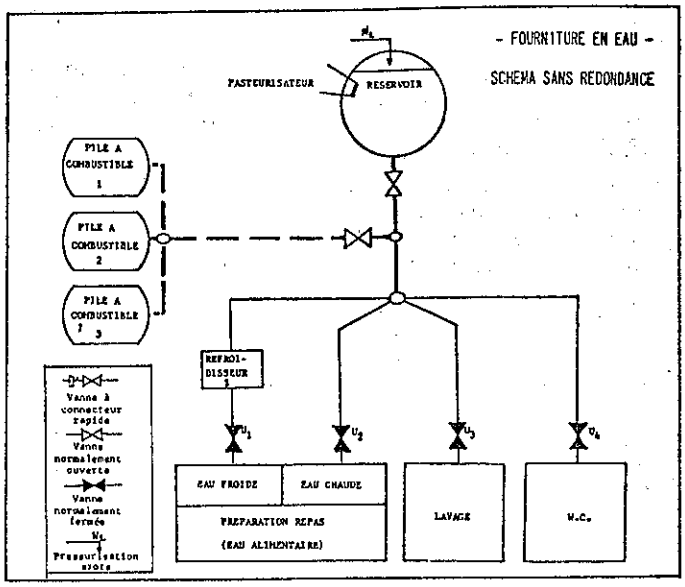
* Société Novatome.

** C.N.E.S.

2. – PRÉSENTATION DU SYSTÈME

Dans un but didactique, nous avons choisi comme support, un dispositif peu complexe : le système de fourniture en eau du véhi-





cule Hermes (planeur hypersonique envisagé comme étape future du programme Ariane).

Ce système comporte 3 fonctions principales :

- alimentation : récupération de l'eau produite par les piles à combustible;
- stockage : conservation de l'eau et maintien de ses caractéristiques de potabilité;
- distribution et conditionnement pour les différentes utilisations : alimentation et hygiène.

3. – PHASES DE L'ANALYSE ET LOGIGRAMME

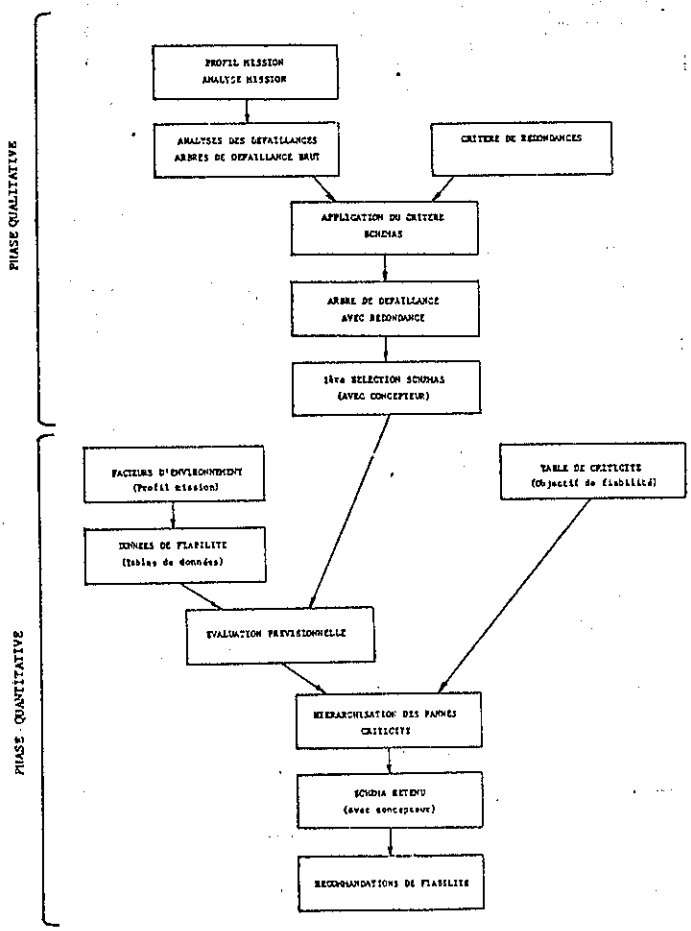
Ce type d'analyse comporte deux phases principales :

– *Une phase qualitative*

Cette phase consiste dans un premier temps à analyser les missions et modes de fonctionnement, à rechercher les modes de défaillance du système et d'en déduire l'arbre de défaillance. Puis, l'application du critère de sécurité permet de définir les redondances nécessaires compte tenu de la gravité des conséquences, et d'établir les schémas correspondants.

Des considérations de performances éliminent éventuellement un certain nombre de schémas envisagés. Pour les schémas restant la construction des arbres de défaillance permet de vérifier l'application du critère, de proposer des actions qualitatives de fiabilité et de fournir les modèles mathématiques nécessaires à l'étude quantitative.

LOGIGRAMME DE L'ETUDE FIABILITE



– *Une phase quantitative*

permettant de choisir la ou les meilleures solutions envisageables parmi celles retenues lors de la première phase, d'ordonner les causes de panne par rang d'importance, de vérifier qu'il n'y a pas distorsion notable entre l'évaluation prévisionnelle de fiabilité et les objectifs chiffrés, de déterminer les éléments critiques pour la fiabilité du système sur lesquels seront focalisées les actions qualité fiabilité.

Les différentes opérations de ces deux phases s'articulent suivant le logigramme ci-contre.

4. – CRITÈRE DE REDONDANCE

A ce stade du projet, le choix du type de matériel et des technologies n'est pas encore fait. Il est, par conséquent difficile de justifier des valeurs de probabilité de défaillance des composants et, à plus forte raison d'effectuer des calculs de fiabilité sur plans. Se référer au départ à un critère qualitatif est donc préférable.

Ce critère permet, avant toute considération probabiliste complexe, de sélectionner un nombre restreint de schémas sains sur le plan de la sécurité (redondances suffisantes mais non superflues), en pondérant les redondances, la classe de qualité ou les critères de dimensionnement en fonction des gravités de conséquences.

Le critère retenu pour cette étude est le critère « Fail Operational - Fail Safe », il impose :

1° Pour les éléments actifs (équipements) :

- redondance d'ordre 3 pour les conséquences affectant la Sauvegarde;
- redondance d'ordre 2 pour les conséquences affectant la Mission;
- pas de redondance pour les conséquences dites Mineures.

2° Pour les éléments passifs (structures), en général plus fiables :

- redondance d'ordre 2 pour les conséquences affectant la Sauvegarde;
- pas de redondance pour les conséquences affectant la Mission.

La redondance peut exister soit au niveau du composant élémentaire, soit au niveau de la fonction ou du mode de pannes. Par exemple, pour le système analysé ici, la redondance vis-à-vis du manque d'eau peut être réalisée au niveau des circuits d'alimentation (deux circuits distincts) ou au niveau du stockage.

5. – PHASE QUALITATIVE

5.1. – ANALYSE MISSION

5.1.1. – Nature et perspective

Cette analyse est réalisée dans une double perspective : la détermination des modes de défaillance d'une part, et le choix de données permettant l'évaluation de la fiabilité (phase quantitative) d'autre part.

Elle comporte l'examen :

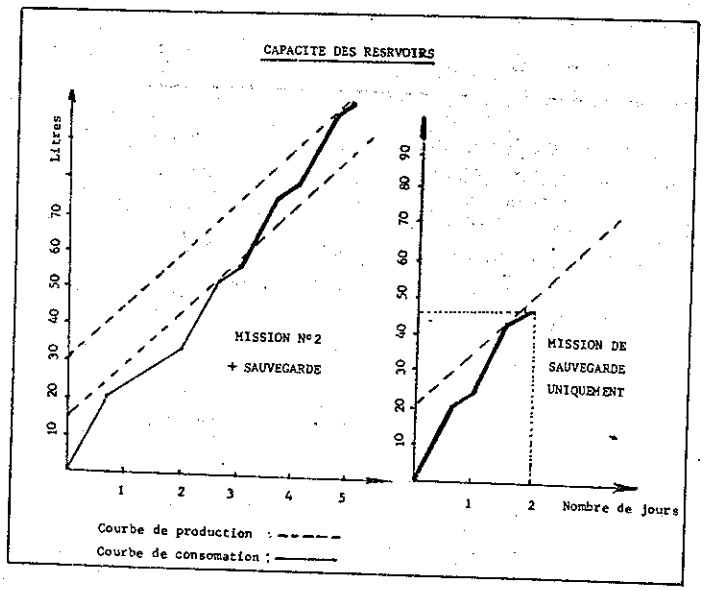
- des modes et durées de fonctionnement (profil mission);
- des spécifications fonctionnelles et d'interface, des configurations dimensionnantes, et des performances nécessaires, en modes nominal et dégradés;

– des conditions d'ambiance et d'environnement (thermique, chimique, vibratoire, etc.).

Cette phase très importante, qui doit être menée avec le concepteur, permet au fiabiliste de connaître parfaitement le fonctionnement du système.

5.1.2. – Spécification sur les besoins en stockage

L'analyse tenant compte de la production et de la consommation d'eau, conduit à optimiser les quantités d'eau à stocker pour assurer les besoins correspondant aux différentes phases de la mission.



5.2. – ANALYSE DES DÉFAILLANCES (sur le schéma sans redondance)

5.2.1. – Méthode utilisée

Il s'agit de la méthode classique d'analyse par arbre de défaillances qui, dans certains cas, nécessite une approche par arbre d'événements. Elle a fait l'objet d'une précédente conférence à la S.I.A. et d'une publication dans la revue des Ingénieurs de l'Automobile (n°4-5 avril-mai 1978) : « Impact d'une analyse de fiabilité sur la conception d'une installation ».

Cette méthode consiste, à partir de la détermination des modes principaux de pannes, à remonter aux causes de ces pannes (au niveau des composants élémentaires). Elle permet d'éliminer d'emblée toutes les défaillances qui n'affectent pas les conséquences analysées, ici la mission ou la sauvegarde.

Le risque de manque d'exhaustivité ne peut provenir que d'une mauvaise analyse des modes principaux de défaillance. C'est pourquoi un soin particulier doit être apporté à cette tâche, ne pouvant être correctement menée à bien qu'en collaboration étroite avec le concepteur qui est le seul à pouvoir déterminer les conséquences exactes de certaines défaillances.

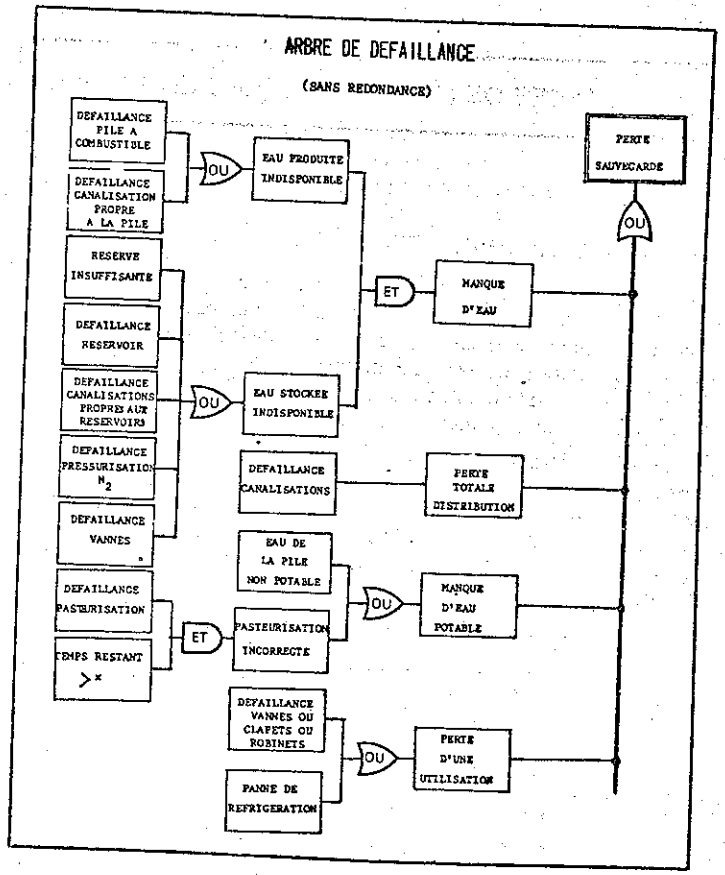
5.2.2. – Description de l'arbre

Seules ont été envisagées, dans cette étude, les défaillances fonctionnelles. L'unique conséquence représentée sur la figure est la perte sauvegarde.

En effet, compte tenu de la définition de la sauvegarde (deux jours dans les conditions nominales de fonctionnement), toute panne significative conduit à la perte sauvegarde. La notion de perte mission ne peut être définie que par un risque de perte sauvegarde (une panne en moins).

On constate d'autre part qu'apparaissent au niveau des feuilles élémentaires de l'arbre de défaillance, trois types d'événements ou causes de défaillances :

– des défaillances d'organes du système considéré;
– des défaillances d'autres systèmes ou sous-systèmes (interfaces);
– des circonstances associées à ces défaillances (instant, état du système au moment où se produit la panne, etc.



5.2.3. – Application du critère

L'application du critère peut faire appel à l'analyse plus ou moins détaillée de certains cas de panne et à l'appréciation des risques admissibles.

5.2.4. – Redondances nécessaires

Compte tenu de l'analyse des défaillances, les redondances minimales nécessaires sont :

– deux réservoirs de stockage;
– une redondance de la pasteurisation (de type « équipement »);
– deux circuits de distribution indépendants;
– deux refroidisseurs;
– redondance sur les vannes d'utilisation;
– séparation entre eau pasteurisée et eau stérilisée chimiquement (redondante).

5.2.5. – Choix possible

Les choix concernant la distribution, le stockage, l'alimentation sont résumés ci-après.

Pour la distribution deux configurations simples peuvent être envisagées :

- la solution dite « normale ». Cette configuration conduit à munir chaque circuit de distribution de 12 robinets d'utilisation (4 groupes de 3 robinets) soit au total : 24 robinets (2 circuits indépendants);
- une autre solution consiste à remplacer les robinets par des connecteurs rapides du type « Staubli ». Ceci conduit à utiliser un seul connecteur rapide par utilisation et un connecteur de rechange pour l'ensemble des utilisations, soit au total $(2 \times 4) + 1 = 9$ connecteurs.

Pour l'alimentation deux solutions peuvent également être envisagées :

- l'alimentation n'est pas, par elle-même, redondante et l'eau en cas de perte d'alimentation, est fournie par le stockage (A 1);
- l'alimentation est redondante, ce qui assure en toutes circonstances, la fourniture en eau produite par les piles (A 2).

Pour la stérilisation, lors du stockage, deux solutions sont envisageables :

- une pasteurisation (maintient en température);
- une stérilisation chimique.

Pour le stockage, afin de satisfaire au critère, trois solutions sont envisageables :

- un réservoir « normal » et un réservoir « de sauvegarde » tous deux pasteurisés (S 2);
- un réservoir « normal » pasteurisé et un réservoir « de sauvegarde » stérilisé chimiquement (S 1);
- deux réservoirs pasteurisés (un « normal » et un de « secours ») et un réservoir « de sauvegarde » stérilisé chimiquement (S 3).

Cette dernière configuration qui n'impose pas, par ailleurs, de vanne supplémentaire offre des possibilités d'aménagement plus variées et ne condamne pas l'utilisation de l'eau produite par les piles en cas de panne du réservoir « normal ».

Enfin, compte tenu du fonctionnement en état d'apesanteur, deux modes d'expulsion de l'eau des réservoirs sont utilisables :

- expulsion par membrane;
- rétention capillaire.

Toutefois, le choix entre ces deux solutions n'a pas été effectué ici, car il n'influe pas sur la conception du circuit et peut être réalisé au niveau du programme de développement de l'organe. Il n'influe pas non plus notablement sur le bilan masse.

5.3. – PREMIÈRE SÉLECTION DE SCHÉMAS

5.3.1. – Critères de choix

Les critères de choix entre ces différentes solutions seront avant tout, des critères de projet :

- masse, encombrement (éventuellement performance) du système;
- coût de développement et d'exploitation.

En outre, interviendront des critères qualitatifs de fiabilité et sécurité, issus de l'analyse des défaillances, pondérés par l'expérience des responsables de projet.

5.3.2. – Comparaison des schémas

5.3.2.1. – *Distribution*

La comparaison des deux solutions possible.

- D 1 à 24 orbinets;
- D 2 à 9 connecteurs rapides

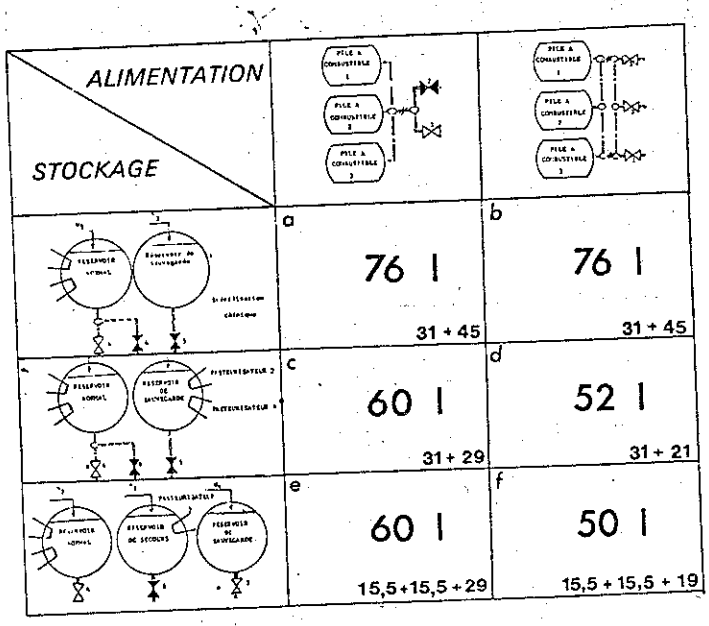
donne un très net avantage à la solution D 2 qui bien qu'un peu moins fiable que D 1 reste acceptable, tous les autres critères étant en faveur de la solution D 2.

5.3.2.2. – *Alimentation-stockage*

Les systèmes alimentation et stockage n'étant pas indépendants, car l'eau stockée peut servir de redondance à l'eau produite (alimentation), on ne peut optimiser ces deux systèmes de façon séparée. On compare donc leurs différentes combinaisons. Les six solutions en compétition sont définies dans le tableau ci-après :

Alimentation \ Stockage	S_1	S_2	S_3
A_1	a	c	e
A_2	b	d	f

où S_1, S_2, S_3, A_1 et A_2 sont les solutions définies § 5-2-5. La comparaison des solutions selon des différents critères permet d'éliminer les schémas a, b et c. La figure ci-après indique, à titre d'exemple, les volumes de stockages pour les 6 solutions envisagées.



5.4. – ARBRE DE DÉFAILLANCE AVEC REDONDANCE

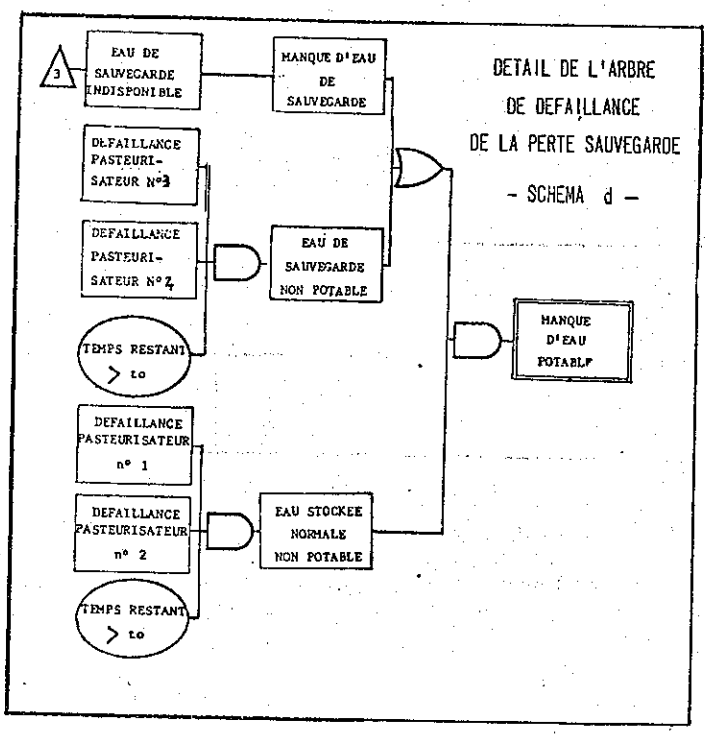
Pour chacun des trois schémas retenus, on établit les arbres de défaillances correspondants (à titre d'exemple, nous donnons un extrait de l'arbre de défaillance du schéma « d » conduisant à la « perte sauvegarde »).

Ces arbres de défaillance servent, à vérifier que le critère est bien appliqué, à rechercher d'éventuels modes communs et à fournir les modèles mathématiques nécessaires à l'évaluation prévisionnelle.

5.5. – MODES COMMUNS

L'analyse qui précède doit être complétée par l'examen des modes communs de défaillances, c'est-à-dire des causes ou événements risquant de provoquer ou de favoriser la défaillance simultanée ou en cascade de plusieurs éléments.

Ce type d'événement ou de cause de défaillance doit être pris en compte car il peut rendre inopérantes certaines redondances concernées par ces modes communs.



Une recherche systématique de ceux-ci doit donc être entreprise et des parades doivent être trouvées chaque fois que cela est possible et que le risque correspondant est significatif (différenciation des types, fournisseurs, spécifications d'environnement d'organes redondants par exemple).

6. – PHASE QUANTITATIVE

6.1. – DONNÉES DE FIABILITÉ

Les taux de défaillances des différents composants peuvent être issus de différentes sources :

- banques de données;
- données de fabricants ou d'utilisateurs de matériels semblables (analyse statistique de résultats d'essais ou d'exploitation).

Comme cette étude se situe au stade de la conception, nous avons utilisé les banques de données, seules exploitables.

L'ajustement des données de fiabilité nécessite de prendre en compte les facteurs suivants :

- profil mission (environnements, contraintes, facteurs de charge, durées de fonctionnement, périodes d'attente, etc.);
- classe de qualité des matériels;
- types de matériel (classique ou nouveau).

6.2. – ÉVALUATION PRÉVISIONNELLE

Dans bien des cas, ces calculs peuvent être effectués manuellement mais, pour cet exemple, nous avons utilisé, à titre didactique, un programme de traitement par ordinateur, qui permet :

- de calculer la fiabilité de systèmes complexes décrits sous forme d'arbres de défaillance avec ou sans dépendances (différents types de loi de probabilité peuvent être introduits dans les feuilles élémentaires);
- de repérer les points faibles de ces systèmes et d'évaluer leur poids dans la probabilité globale de défaillance.

Les résultats du calcul sont fournis sous forme de tableau, où les causes d'indisponibilité (simples, doubles ou triples) sont repérées par des numéros et classés par ordre de probabilité décroissante.

Cette quantification permet, pour une fonction donnée : disponibilité, sécurité..., de vérifier si l'estimation effectuée est homogène avec l'objectif que l'on s'est fixé **(allocation)**, de classer les différents schémas et d'identifier les principaux éléments risquant d'avoir une influence notable sur cette fonction.

6.3. – HIÉRARCHISATION DES PANNES, CRITICITÉ

6.3.1. – Intérêt de la méthode

Dès que plusieurs types de gravité de conséquences de pannes sont à prendre en considération, la hiérarchisation des causes de défaillances ne peut plus s'effectuer de manière aussi simple, de même que le choix définitif du meilleur schéma.

Il est alors intéressant de construire une table de criticité permettant d'effectuer un classement unique hiérarchisant les défaillances selon le double critère de la probabilité d'occurrence et de la gravité des conséquences. Elle permet de déterminer le meilleur compromis entre des exigences souvent contradictoires de fiabilité, de disponibilité et sécurité, et doit être construite, à partir des objectifs qui ont été spécifiés *a priori*.

6.3.2. – Gravité des pannes

On a défini dans cet exemple, quatre degrés de gravité :

Panne mineure

Le risque correspondant est l'indisponibilité (report mission et opérations de maintenance entraînant un surcoût).

Perte mission (ou panne majeure)

Le risque correspondant est l'interruption de mission (perte partielle ou totale des objectifs mission).

Perte sauvegarde (ou panne critique)

Le risque est de ne pouvoir assurer, après la panne, les conditions nominales d'environnement pendant deux jours (sauvegarde du personnel et du système).

Perte survie (ou panne catastrophique)

Le risque correspondant est de ne plus pouvoir assurer le maintien des conditions de survie de l'équipage.

6.3.3. – Allocation fiabilité

Le Maître-d'Œuvre fixe pour chacun (ou certains) de ces degrés de gravité un objectif de fiabilité chiffré selon des critères philosophiques, politiques, économiques ou financiers qui définit la performance visée.

Cet objectif, souvent choisi par comparaison avec un matériel existant, est en général défini au niveau de la mission ou de l'ensemble du système, et une répartition des risques doit être effectuée au niveau sous-systèmes. C'est l'opération d'allocation de fiabilité. Dans le cas qui nous intéresse, cette répartition a pu être effectuée par comparaison avec des objectifs de la Navette spatiale américaine.

6.3.4. – Classes de probabilité

Compte tenu de ces objectifs et pour construire une table de criticité, quatre classes de probabilité ont été définies :

- probable : $P > 10^{-5}$;
- peu probable : $10^{-7} \leqslant P \leqslant 10^{-5}$;
- très peu probable : $10^{-9} < P \leqslant 10^{-7}$;
- hautement improbable : $P \leqslant 10^{-9}$.

6.3.5. – Criticité

Le niveau et l'étendue de ces classes de probabilité sont choisis de manière à pouvoir ranger les pannes formant la diagonale principale de la table de criticité dans la catégorie des pannes de criticité moyenne, c'est-à-dire acceptables (conforme à l'objectif), mais significatives; les pannes situées au-dessus étant de criticité faible ou négligeable et les pannes situées en dessous étant de criticité prohibitive. Voir table de criticité.

- TABLE DE CRITICITE -

- Objectif de fiabilité : Perte sauvegarde : $\pi 10^{-7}$

probabilité / mission — gravité	$> 10^{-5}$ probable	10^{-7} à 10^{-5} peu probable	10^{-9} à 10^{-7} très peu probable	$< 10^{-9}$ hautement improbable
panne mineure	2	1	1	1
perte mission	3	2	1	1
perte sauvegarde	3	3	2	1
perte survie	3	3	3	2

- Pannes de criticité faible : classe 1
- Pannes de criticité moyenne : classe 2
- Pannes de criticité prohibitive : classe 3

Compte tenu de cette classification :

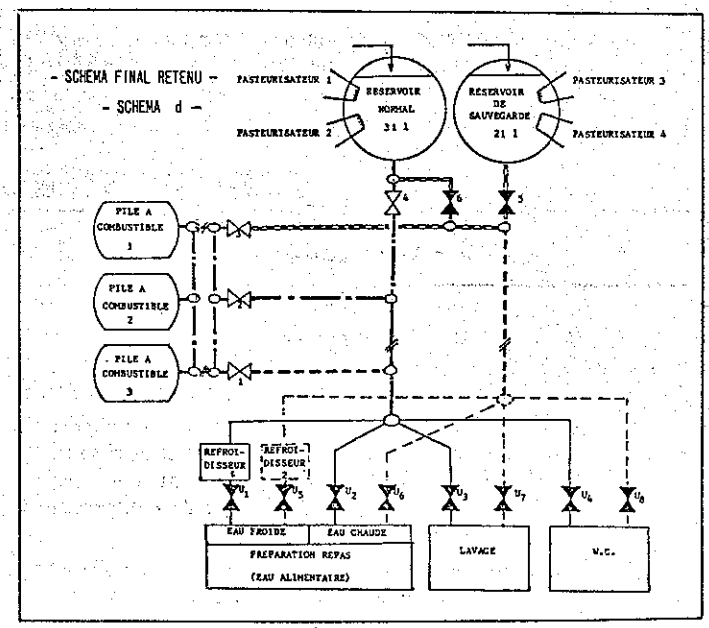
- sont considérées comme prohibitives les pannes de classe 3. La présence de telles pannes signifie en général qu'il faut modifier la conception du schéma ou choisir d'utiliser un matériel de qualité très supérieure à celle prévue antérieurement;
- sont considérées comme critiques les pannes de classe 2 les organes élémentaires en cause devront être considérés comme des points sensibles pour la fiabilité du système lors de la mise au point du système des organes élémentaires et devront faire l'objet de spécifications (objectifs fiabilité) et d'essais permettant de vérifier que les valeurs que l'on s'est fixé pour les taux de défaillance lors du calcul sont correctes ou « pessimistes »;
- sont considérées comme de criticité faible les pannes de classe 1. Elles n'influent que de manière négligeable sur la fiabilité de l'ensemble et à condition que les composants correspondants n'interviennent pas dans les pannes critiques relatifs à un autre risque et soient réalisées de manière convenable, ils n'ont pas à faire l'objet d'un suivi fiabilité particulier.

7. – DÉBOUCHÉS PRATIQUES DE L'ÉTUDE

Cette analyse a permis :

7.1. – De classer les schémas fonctionnels possibles par ordre d'intérêt décroissant et de sélectionner le meilleur (ici choix du schéma d) :

7.2. – De définir les redondances et chaînes de sécurité éventuelles nécessaires, exemple : détection de vidange du réservoir normal;



7.3. – De proposer ou préparer un certain nombre de **spécifications d'organes :**

- classe de qualité des matériels ou allocation fiabilité au niveau sous-systèmes et composants;
- recommandations de conception : capacité, volume des réservoirs, étanchéité, environnement, démontabilité, réparabilité (vannes d'utilisation à déconnexion rapide plus une vanne de rechange), redondances internes, dispositifs en sécurité intrinsèque : la panne la plus probable (en général la mise en position « repos » de l'organe) conduit à une situation sûre (ne pouvant entraîner d'accident grave) ou si ce n'est possible à la mise en route d'un système de sécurité dont la panne conduit à une situation sûre.

Exemple :

La détection de manque d'eau de panne ou de pasteurisation (température de l'eau) conduit à la connexion automatique sur le réservoir de sauvegarde (avec signalisation). La panne de ce système de connexion doit aussi conduire au basculement sur réservoir de sauvegarde.

7.4. – De préparer des spécifications d'essais (essais d'endurance et essais fiabilité).

– *Essais de fiabilité*

Matériels pour lesquels des essais fiabilité doivent être effectués :

- nombre d'exemplaires à essayer;
- nombre et durée des essais;
- conditions d'essais;
- types d'essais.

Ce qui évite des essais trop longs et trop coûteux, ou trop courts et pas assez significatifs.

– *Autres essais*

D'autres essais de mise au point ou de mesure de performances peuvent être suggérés par l'analyse des défaillances.

Exemple :

Mesures de la durée pendant laquelle l'eau des réservoirs reste potable après une défaillance de pasteurisation.

7.5. – De proposer éventuellement des redondances de survie : c'est-à-dire ultimes redondances permettant encore d'assurer la survie de l'équipage malgré des conditions dégradées dans le cas de pannes conduisant à la perte sauvegarde.

8. – CONCLUSION

Toute étude de faisabilité ou d'avant-projet devrait comporter ce type de démarche, chaque fois qu'un ou plusieurs paramètres de fiabilité revêtent un caractère important pour le système concerné.

Il permet d'évaluer les répercussions des exigences fiabilité sur la conception du système et par conséquent sur les autres paramètres caractéristiques principaux : masse, encombrement, coût, performance... Il donne en outre des indications sur le développement du système (définition du plan d'essais entre autres).

La méthode proposée s'adapte particulièrement à l'établissement du meilleur compromis entre deux caractéristiques de fiabilité-sécurité et disponibilité par exemple.

Ce type d'analyse doit être considéré comme la première étape d'un ensemble d'actions de fiabilité qui devront se poursuivre tout au long du développement; il doit être réalisé par le fiabiliste en étroite collaboration avec le concepteur et constitue un important volet de l'*« Analyse de la valeur »* qui, sans prise en compte de l'élément sécurité-fiabilité, risque de conduire à des solutions dangereuses.

9. – ADAPTATION A L'AUTOMOBILE

Conservant l'esprit général de la démarche, nous retiendrons les points suivants :

– *Critère Sécurité*

Dans la définition du critère une variante Automobile impliquerait, par exemple, par degré d'importance décroissante :

Par degré d'importance :

- pannes conduisant à la perte de contrôle du véhicule;
- pannes nécessitant un remorquage jusqu'au parc de réparation;
- pannes permettant la rentrée du véhicule, au parc, par ses propres moyens.

– *Redondance*

La redondance ne sera pas vue strictement comme le doublement ou la multiplication d'une fonction ou d'une pièce, mais éventuellement comme une ou plusieurs actions visant à réduire ou annuler une probabilité de panne ou, comme la mise en place de dispositifs de tests, périodiques ou continus, permettant de détecter ou de prévenir une panne avant que celle-ci n'entraîne la conséquence redoutée. ■

– *De façon générale*

Nous noterons que pour l'automobile :

- les calculs de fiabilité peuvent être faits à la main en raison du nombre réduit de modes communs;
- le déroulement du projet est plus rapide. Le niveau prototype est vite atteint et l'analyse se fera très tôt à l'aide des plans;
- l'évaluation prévisionnelle disposera d'une richesse particulière en matière de statistique opérationnelle;
- les redondances sont facilement applicables au niveau des tests de sécurité et de disponibilité (voyant de détection de pannes pour les systèmes multiples et de détection d'usures pour les systèmes uniques.

Exemples d'applications des arbres de défaillance à l'évaluation des risques

par M. Jean-François Guyonnet (1)

L'évaluation des risques, n'a de sens que par rapport à l'intention de discerner *ce qui est acceptable* de ce qui ne l'est pas et, dans ce cas, de choisir les mesures qui se justifient le mieux pour tous.

Installer sur une automobile un système de répartition de freinage a l'avantage d'améliorer l'adhérence, et donc de réduire le risque d'accident. La vérification trop rare des avantages du système, seulement possibles en effet dans des cas exceptionnels, le freinage à grande vitesse sur une courbe par exemple, réduit son intérêt auprès de l'utilisateur, déjà contraint à payer un surcoût faible mais inévitable. Les impératifs de la compétitivité commerciale motivent la suppression du système, et par conséquent ses avantages. Un dilemme semblable apparaît aujourd'hui avec la transposition d'un système issu de l'expérience en aéronautique, l'antirayeur (1).

De même, la détermination de la hauteur de digue en fonction de la crue millénaire, de la résistance d'une plate-forme en fonction de la vague centenaire sont des problèmes types d'évaluation du risque à la fois déterministes et probabilistes.

Cinq questions fondamentales se posent à l'homme de décision aujourd'hui comme au premier hominien hier : 1° Quels sont les risques liés au développement d'une activité? 2° Quelles sont leurs importances? 3° Ces risques sont-ils acceptables? 4° Comment s'en prémunir? 5° Au prix de quels efforts?

LES DIMENSIONS ET LES CARACTÉRISTIQUES DES RISQUES

Un risque peut se mesurer avec une, deux, trois dimensions ou plus. Fondamentalement d'abord, par la probabilité d'apparition d'un événement redouté, ensuite, par la gravité des conséquences, dommages ou pertes entraînés par l'événement indésirable; enfin par la dimension de l'exposition à ce risque estimée souvent en durée passée, en longueur parcourue en surface concernée.

On peut noter l'importance de bien d'autres caractères du risque, données brutes ou affinées, spécifiques tel le millirad par heure ou génériques telle l'espérance de vie perdue. Quelques-unes de ces caractéristiques sont rappelées dans les figures 1 à 8 (2, 3, 5).

La circulation automobile est un risque, et la gravité des accidents de la route avec 250 000 victimes par an le situe, sur le plan national, au même rang que les catastrophes naturelles (fig. 1), bien au-dessus d'autres activités humaines en valeur absolue (fig. 2) mais du même ordre relativement que celui encouru par le boxeur ou le mineur (fig. 3). Cette gravité semble suivre d'assez près une loi exponentielle en fonction du nombre de véhicules impliqués dans un accident (fig. 2). Si la probabilité d'accident, rapportée à l'heure d'exposition, a régulièrement diminué depuis 70 ans de presque un facteur 1 000, par contre actuellement toute la population (> 99 %) est maintenant impliquée.

Le risque dépend de l'activité, et du bénéfice attendu, qui augmentent ensemble selon une loi exponentielle, en fonction du salaire horaire par exemple (fig. 4). On vérifie aussi que l'homme accepte plus de risques si l'activité est libre que si elle est imposée. Par contre dans le passé, pendant ces 30 dernières années, le risque semble être un invariant, quelque soit l'activité, lorsqu'il est mesuré par l'espérance de vie perdue, dimension qui tient compte de l'âge et du niveau de vie des personnes touchées et qui évite une évaluation monétaire de la vie perdue (fig. 7).

Si l'on constate que le risque décroît en valeur absolue lorsqu'il est évalué en fonction du nombre des victimes annuelles, il peut en réalité rester constant s'il est rapporté à d'autres dimensions (fig. 6). Globalement, quelque soit l'activité, l'homme a tendance à vivre à risque constant, comme le montrent les figures 5 et 7.

On peut aussi constater qu'il y a un grand décalage, une décade au moins, entre les risques « naturels » et les risques « humains » (2) et qu'il existe de fait une similitude persistante entre accidents et désastres, ces derniers étant déterminants à cause des décisions législatives qu'ils provoquent (8) de même l'introduction d'une nouvelle technologie dans l'activité (aviation) ou une maintenance relachée avec le temps (rail) augmentent les risques (fig. 7).

EXEMPLES D'ÉVALUATION DE RISQUES

Pour évaluer les risques il existe de nombreuses méthodes. Elles ne sont que des instruments qu'il faut choisir selon les cas et les questions posées et qu'il faut utiliser convenablement. Parmi ces méthodes une des plus intéressantes pour un ingénieur est celle de l'arbre de défaillance (AdD). Quelques exemples variés d'évaluation des risques montreront les résultats que l'on peut obtenir avec cette méthode.

(1) Ingénieur diplômé E.P.F.Z., Enseignant-chercheur U.T.C., Département Génie Chimique.

N°	Genres de grandes catastrophes d'origines naturelles	Classées par ordre croissant de fréquence	
		Fréquence d'apparition	Indice de gravité en morts (m.)*
1	Avalanches et éboulements	12 en 178 ans ≅ 6,74 en 100 ans	de 400 à 4 000 (Pérou 1962)
2	Inondations par mer ou fleuves	38 en 102 ans ≅ 37,3 en 100 ans	de 200 à 900 000 (Chine 1887)
3	Typhons, cyclones et ouragans	42 en 112 ans ≅ 37,5 en 100 ans	de 137 à 250 000 (Bengale 1970)
4	Tremblements de terre	330 depuis 100 ans	de 5 à 700 000 (Chine)
5	Eruptions volcaniques	2 500 depuis 100 ans	de 1 à 28 000 (Mont Pelé 1902)

* Identification de la plus grave entre parenthèses.

N°	Genres de grandes catastrophes dont l'homme est à l'origine	Classées par ordre décroissant de gravité maxi enregistrée	
		Fréquence d'apparition	Indice de gravité en m.*
6	Agressions toxicologiques (et grandes pollutions)	+ de 10 en 20 ans	0 à 6 000 (Pakistan, oxyde de mercure, 1972)
7	Ruptures de barrages (inondations par)	+ de 14 en 82 ans	de 60 à 2 118 (Italie, Vaiont, 1963)
8	Grands incendies	+ de 40 en 90 ans	de 20 à 1 700 (Chine, Tchongking, 1949)
9	Grandes explosions	+ de 19 en 156 ans	de 17 à 1 600 (Halifax, 1917)
10	Accidents dans les mines	+ de 27 en 70 ans	de 11 à 1 549 (Honkeiko, 1942)
11.1	Accidents de transport en mer	+ de 25 en 30 ans	de 17 à 1 913 (Titanic, 1912)
11.2	Accidents de transport sur rail	+ de 39 en 63 ans	de 12 à 800 (Modane, 1917)
11.3	Accidents de transport par aéronefs	+ de 7 en 22 ans	de 128 à 570 (Espagne, 1976)
12	Des grandes paniques (sur les stades)	+ de 4 en 14 ans	de 40 à 400 (Lima, 1964)
11.4	Des accidents de la route (en 1971)	font ≅ 250 000 m. et 7 500 000 blessés par an: France ≅ 15 000 m. pour 170 000 accidents par an.	

* Il y a dans beaucoup de cas, beaucoup plus de personnes atteintes par l'événement que de morts.

Fig. 1.

Premier Cas. Recherche et discussion de l'importance des causes de non-démarrage d'un moteur à essence (6)

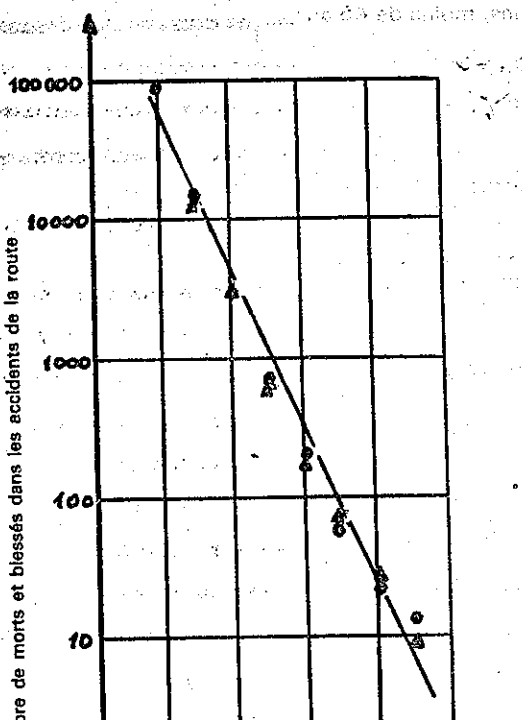
Cet exemple didactique montre les étapes de cette méthode, les résultats possibles et les développements mathématiques nécessaires.

a) On considère le moteur à 2 cylindres et ses principaux composants (fig. 9).

L'événement redouté le non-démarrage (ND) est le sommet de l'arbre de défaillance. L'AdD est une représentation graphique des liens logiques existant entre une défaillance globale particulière du moteur et des défaillances de ses éléments. L'événement terminal, dont on écrit les causes développées progressivement selon la logique de fonctionnement du système, est la panne globale, c'est-à-dire le ND.

Ce processus logique aboutit aux dernières causes, événements dits de base; c'est-à-dire ceux qu'on ne souhaite plus développer parce qu'ils sont indépendants (par exemple des pannes élémentaires appelées pannes primaires). En outre, on peut connaître leurs probabilités.

Facteur potentiel d'accident bien connu auquel on se trouve confronté dans la vie quotidienne (USA, 1975)	Total des victimes annuelles classé par ordre décroissant (en m.)
Parcours en auto	56 000
Activité professionnelle	14 200 pour 2 500 000 accidents
Natation	7 300
Dans un incendie domestique	6 800
En mangeant un steack, par étouffement	3 000
Vol en avion	1 500
En jouant au golf et par la foudre	150
Par une installation nucléaire	0



Accidents de la route en Californie en 1968 ▲ et 1969 ●

Fig. 2.

L'AdD comporte, outre des événements, des « portes » qui sont des symboles indiquant un type de relation logique existant entre causes, événements en entrée de porte et conséquence, événement sortie de porte. Les plus utilisées sont le ET et le OU ordinaires. L'arbre ainsi construit permet de recenser 34 causes à la base qui seules ou combinées provoquent le ND redouté (fig. 10).

b) L'analyse logique de l'arbre dite évaluation qualitative du risque passe d'abord par l'écriture de la logique de l'arbre de porte à porte du bas jusqu'en haut, il y a ici 29 équations dont la dernière au sommet de l'arbre s'écrit (64) = (56) × (63) et la première (35) = (1) + (2), × veut dire ET, + veut dire OU (fig. 11). (56), (63) représentent 2 des 64 − 35 = 29, événements intermédiaires entre le ND redouté et ses 34 causes possibles les plus élémentaires dont la panne de batterie (1) et la rupture de la clé de contact (2).

La résolution de l'équation logique fournit le nombre et l'identité des combinaisons de pannes, appelées coupes, provoquant le ND

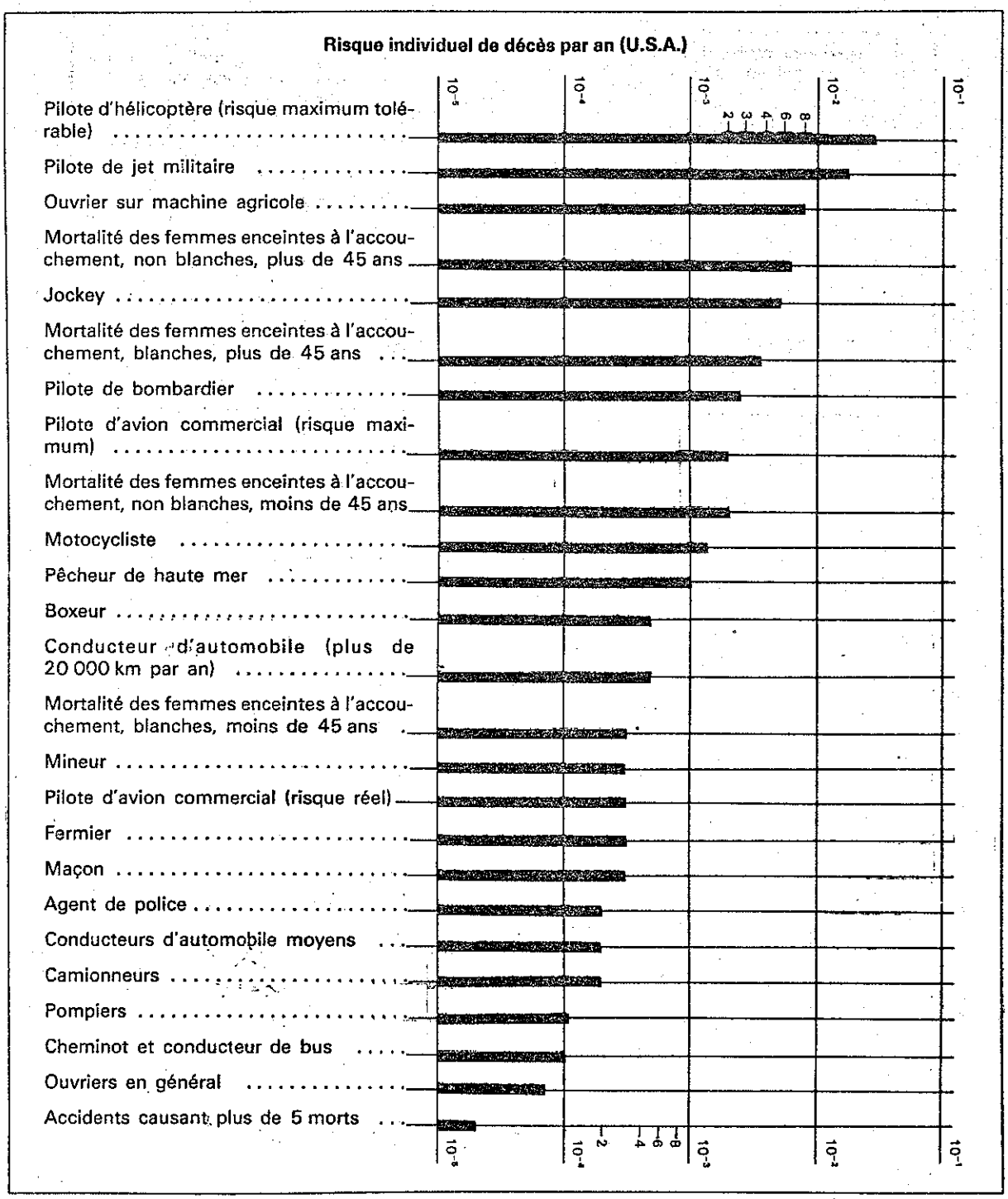


Fig. 3.

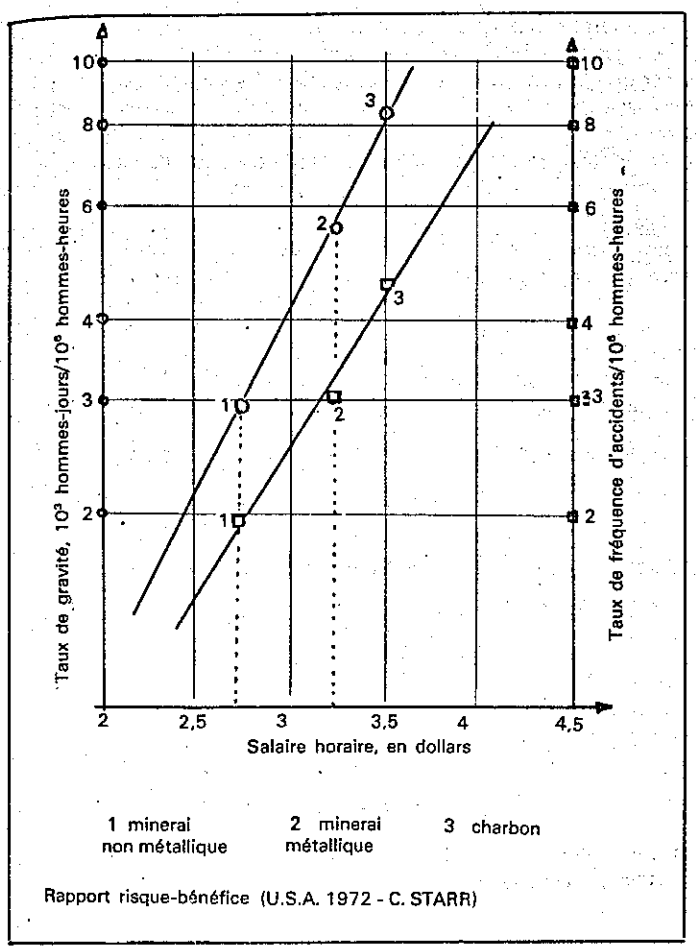
soit 1849 avant simplifications et seulement 58 après, appelées alors coupes minimales (C.M.), dont 22 sont des pannes simples, dite CM de longueur 1 et 36 sont des pannes doubles dites CM de longueur 2 (fig. 11).

Les simplifications dites réductions logiques basées sur les principes $A \times A = A$, $A + A = A$, $A + 1 = 1$, $A \times 1 = A$, ce qui donne par exemple $(A + B) \times (A + C) = A + BC$, viennent de la répétition dans l'arbre des mêmes causes qui sont ici au nombre de 5 : (1), (35), (39), (46), (53).

L'inspection des 58 C.M. trouvées permet de répertorier le nombre de fois qu'apparaît chaque anomalie et ce dans quel type de combinaison, ce qui est une première indication de l'importance de chaque élément relativement au tout ou aux autres.

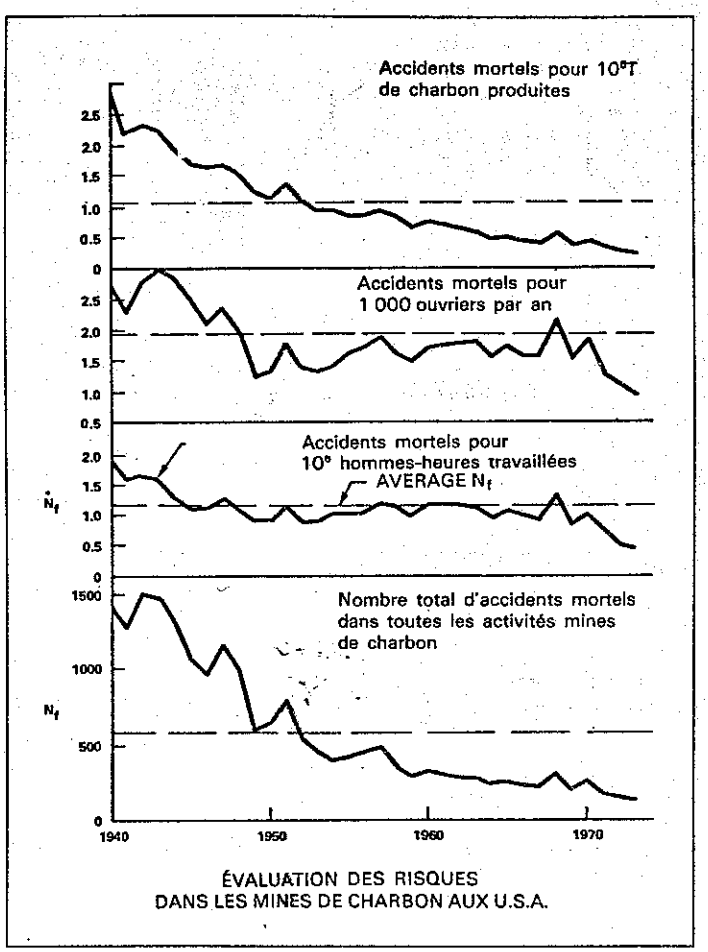
Ainsi 22 causes sont de première importance : par exemple, l'événement (4), qui est un défaut de ligne entre la borne + et la pompe à essence, etc. Les 12 autres restantes apparaissent 6 fois plus que les premières mais sont toujours combinées 2 à 2 (fig. 11), par exemple l'événement (10) qui indique que la soupape d'admission du cylindre n° 1 du piston est bloquée fermée et l'événement (29) qui est la non-admission à la soupape du cylindre 2.

c) Le calcul des probabilités dit évaluation quantitative du risque fournit la probabilité de ND en fonction des probabilités des 34 causes et donc indique aussi — c'est une des façons de procéder — les probabilités de chaque CM. On obtient ainsi un deuxième classement des événements.



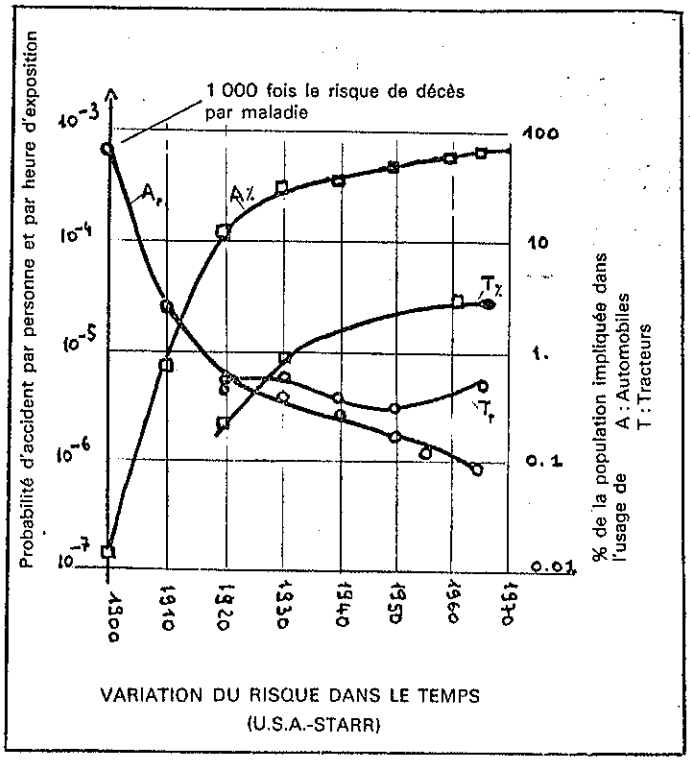
Rapport risque-bénéfice (U.S.A. 1972 - C. STARR)

Fig. 4.



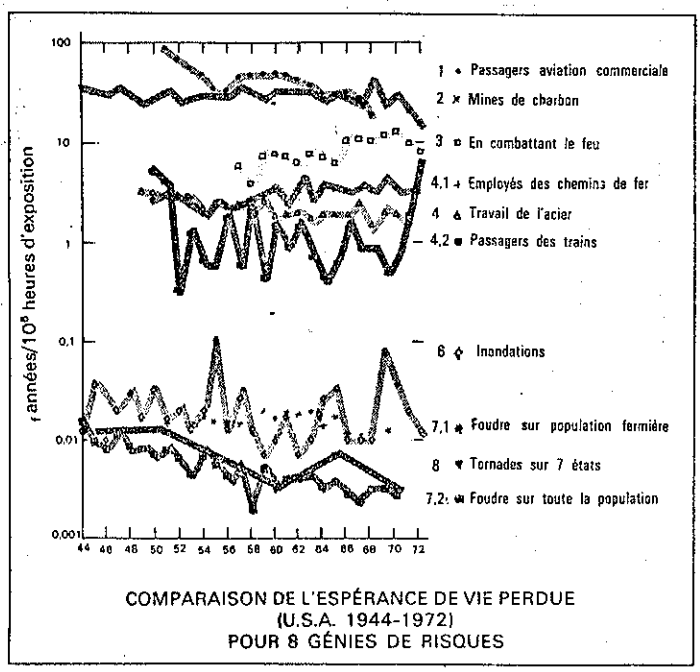
ÉVALUATION DES RISQUES
DANS LES MINES DE CHARBON AUX U.S.A.

Fig. 6.



VARIATION DU RISQUE DANS LE TEMPS
(U.S.A.-STARR)

Fig. 5.



COMPARAISON DE L'ESPÉRANCE DE VIE PERDUE
(U.S.A. 1944-1972)
POUR 8 GÉNIES DE RISQUES

Fig. 7.

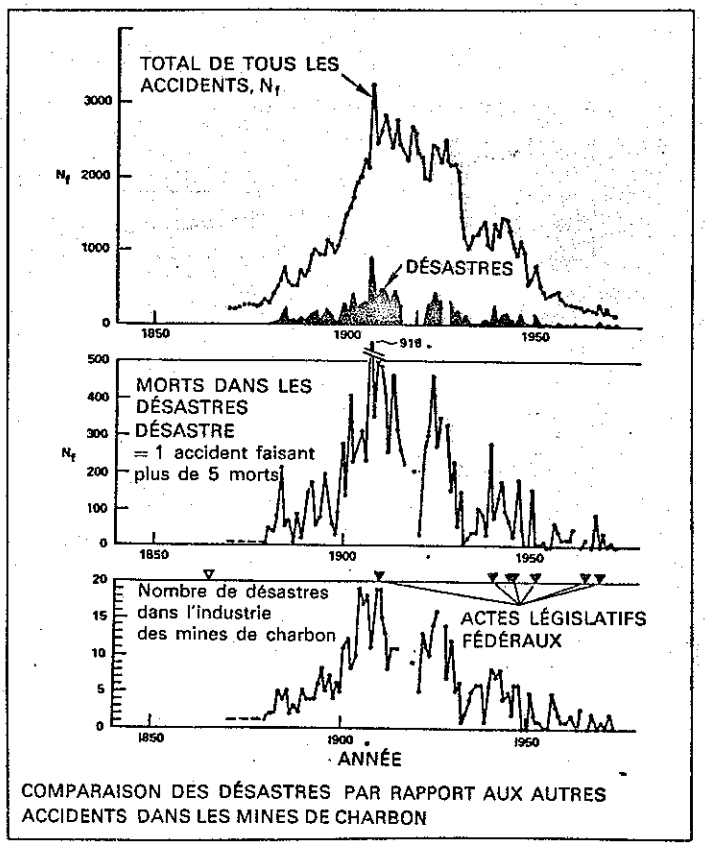


Fig. 8.

Plusieurs précautions s'imposent dans de tels calculs en plus de l'indépendance des événements élémentaires déjà notée, il faut s'assurer que le système est cohérent ce qui est vérifiable par le fait de n'avoir que des ET et des OU ordinaires et des événements élémentaires ce qui a l'avantage de rendre monotone la fonction indicatrice de l'événement terminal duale de la fonction de structure du système.

Les 34 probabilités q_l des 34 causes élémentaires y_l sont estimées l'une après l'autre. Soit, par exemple, $q_1 = p_1[(y_1) = 1]$, avec (1) absence sortie + batterie $= 5 \cdot 10^{-3}$ où par définition $p(y = 1) = q$. On calcule $p(E_s) = \prod_{i \in K_s} q_i$ avec E_s occurrence de tous les événements élémentaires de la coupe K_s. Comme il suffit qu'une des coupes au moins arrive pour que l'événement terminal se produise sa probabilité est donnée par $p(64) = p\left(\overset{58}{\underset{s=1'}{\text{UE}}}\right)$ et en posant : $S_1 = \sum_{s=1}^{58} \prod_{i \in K_s} q_i$, et S_2 somme des double-produits etc., jusqu'à $S_{58} = \prod_{s=1}^{58} \prod_{i \in K_s} q_i$, on trouve :

$$p(64) = S_1 - S_2 \ldots (-1)^{k-1} S_K$$

en s'appuyant sur les théorèmes de Morgan et Poincaré, pour calculer $p(\text{AvB})$ en général.

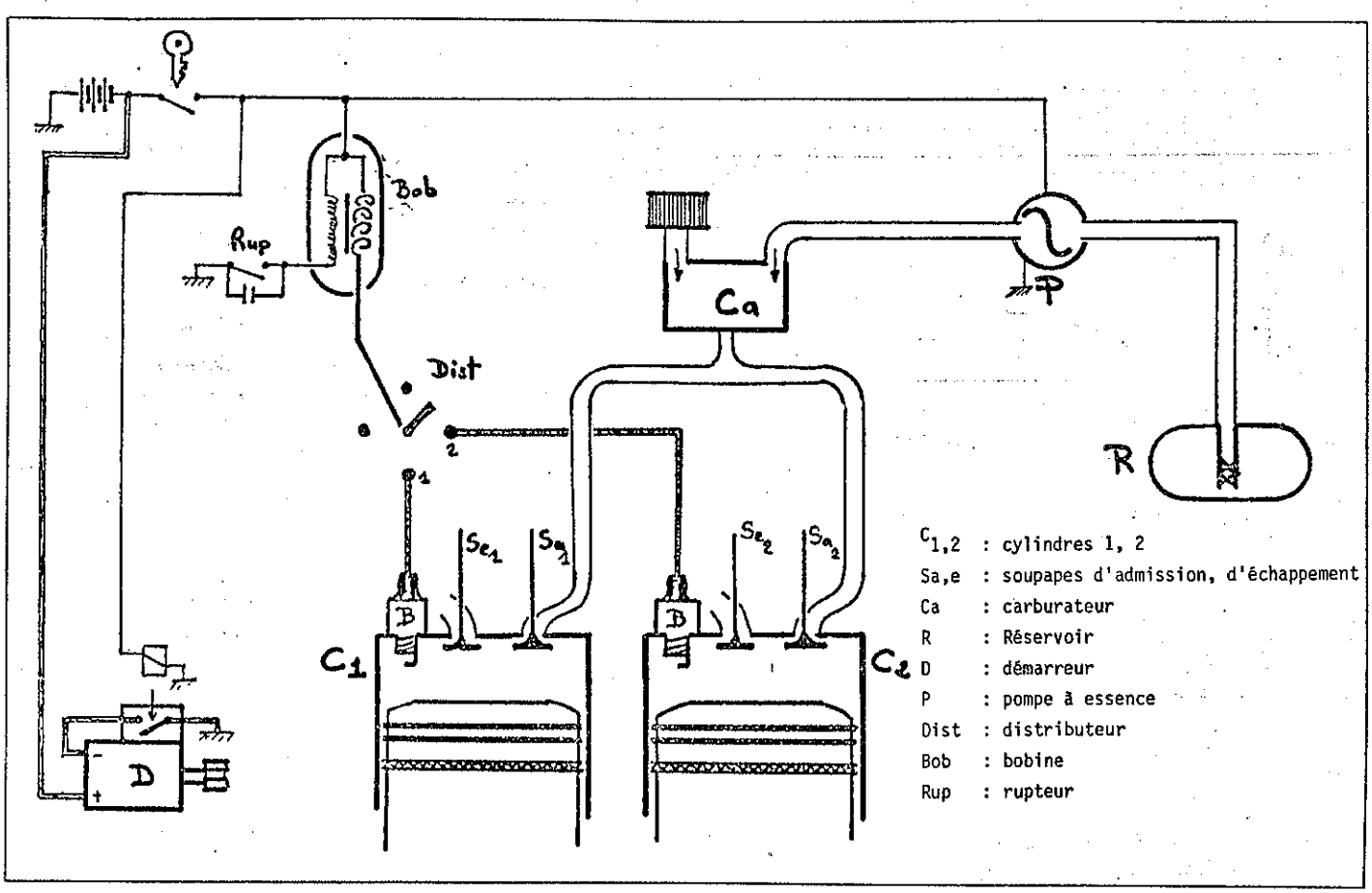


Fig. 9.

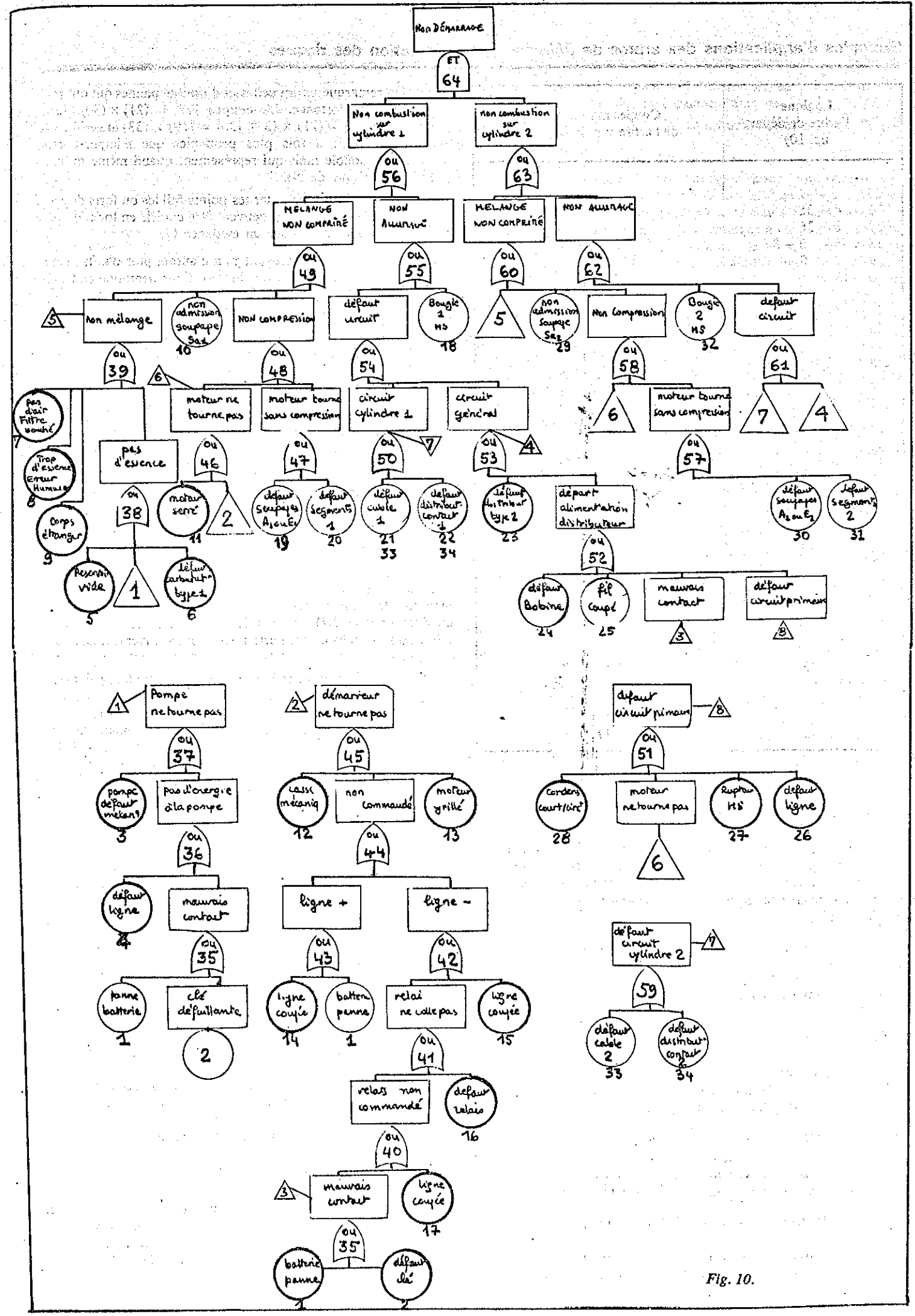

Non Démarrage
ET 64
Non combustion sur cylindre 1
non combustion sur cylindre 2
ou 56
ou 63
MELANGE NON COMPRIMÉ
NON ALLUMAGE
MELANGE NON COMPRIMÉ
NON ALLUMAGE
ou 49
ou 55
ou 60
ou 62
Non mélange
non admission soupape Sa1
NON COMPRESSION
défaut circuit
Bougie 1 HS
18
5
non admission soupape Sa2
29
Non Compression
Bougie 2 HS
32
défaut circuit
ou 39
ou 48
ou 54
ou 58
ou 61
6
moteur ne tourne pas
moteur tourne sans compression
circuit cylindre 1
circuit général
6
moteur tourne sans compression
7
4
pas d'air Filtre bouché
pas d'essence
ou 46
ou 47
ou 50
ou 53
ou 57
7
Trop d'essence Erreur Humaine
8
ou 38
moteur serré
2
défaut soupapes A1 ou E1
19
défaut segments 1
20
défaut culbuto 1
21
33
défaut distribut-contact 1
22
34
défaut distributeur type 2
23
départ alimentation distributeur
défaut soupapes A2 ou E2
30
défaut segments 2
31
Corps étranger
9
Réservoir vide
5
1
défaut carburateur type 1
6
11
ou 52
défaut Bobine
24
fil coupé
25
mauvais contact
3
défaut circuit primaire
8
1
Pompe ne tourne pas
2
démarreur ne tourne pas
défaut circuit primaire
8
ou 37
ou 45
ou 51
pompe défaut mécan?
3
pas d'énergie à la pompe
Lassi mécaniq
12
non commandé
moteur grillé
13
Cordons court/circ
28
moteur ne tourne pas
Rupteur HS
27
défaut ligne
26
ou 36
ou 44
6
défaut ligne
4
mauvais contact
ligne +
ligne -
ou 35
ou 43
ou 42
défaut circuit cylindre 2
7
panne batterie
1
clé défaillante
2
ligne coupée
14
batterie panne
1
relais ne colle pas
ligne coupée
15
59
défaut câble 2
33
défaut distribut-contact 2
34
ou 41
relais non commandé
défaut relais
16
ou 40
3
mauvais contact
ligne coupée
17
ou 35
batterie panne
1
défaut clé
2

Fig. 10.

Logique de l'arbre de départ fig. 10)	**Coupes** minimales de l'arbre simplifié = 58	
	dont 22 coupes de longueur 1	et 36 coupes de longueur 2
35 = 1 + 2	4	10 × 29 10 × 31
36 = 4 + 35	13	22 × 32 18 × 30
37 = 3 + 36	7	20 × 32 22 × 29
38 = 5 + 6 + 37	15	10 × 32 20 × 29
39 = 7 + 8 + 9 + 38	24	18 × 31 10 × 34
40 = 17 + 35	1	21 × 30 18 × 33
41 = 16 + 40	16	19 × 30
42 = 15 + 41	25	18 × 29
43 = 1 + 14	11	18 × 34
44 = 42 + 43	8	21 × 33
45 = 12 + 13 + 44	9	19 × 33
46 = 11 + 45	5	21 × 31
47 = 19 + 20	2	19 × 31
48 = 46 + 47	14	22 × 30
49 = 10 + 39 + 48	17	20 × 30
50 = 21 + 22	27	18 × 32
51 = 26 + 27 + 28 + 46	28	21 × 34
52 = 24 + 25 + 35 + 51	12	19 × 34
53 = 23 + 52	6	22 × 33
54 = 50 + 53	3	20 × 33
55 = 18 + 54	23	10 × 30
56 = 49 + 55	26	22 × 31
57 = 30 + 31		20 × 31
58 = 46 + 57		21 × 29
59 = 33 + 34		22 × 34
60 = 29 + 39 + 58		20 × 34
61 = 53 + 59		19 × 29
62 = 32 + 61		10 × 33
63 = 60 + 62		21 × 32
64 = 56 × 63		19 × 32

Fig. 11.

Ce développement peut être limité aux premiers termes et même à S_1 qui est une borne supérieure de la valeur de $p(64)$ d'autant plus proche que les probabilités q_l sont petites, soit $p(64) < S_1$. L'égalité est vérifiée s'il n'y a aucun événement répété dans les coupes. On trouve ici $S_1 \cong 0{,}096$ et $p(64) = 0{,}093$, la différence est donc faible.

Si la loi de répartition des pannes est connue dans le temps il est possible de tenir compte des taux de panne λ, constants ou non dans le temps, et de plus, on peut envisager le cas d'un système avec des composants réparables au bout d'un temps moyen de réparation τ (12).

Ce calcul de $p(64)$ fournit, en résultats intermédiaires, la liste des probabilités des 58 coupes ce qui permet de les classer et d'évaluer plus précisément ensuite l'importance des événements. On constate ainsi que la onzième coupe de longueur 1, donc une panne simple avec l'événement (8), qui correspond à un excès d'essence dans le carburateur dû à une erreur humaine vaut $2 \cdot 10^{-2}$ soit plus de 2/10 de la probabilité de ND. On constate aussi que 9,5 fois sur 10, les causes de ND viennent seulement de 10 coupes de longueur 1 soit 10 événements qui sont classés dans un ordre décroissant d'importance [(8)], [(2), (14), (4), (1)], [(25)], [(1), (16), (17), (6)]; en effet $\sum_{10} \prod q_l = 8{,}8 \cdot 10^{-2}$. Le premier type de panne simple (8) est déjà 40 fois plus probable qu'un des 4 derniers. Le poids total des 36 coupes restantes de longueur 2 reste donc faible. On remarque parmi celles-ci 4 double-pannes qui ont relativement de l'importance, les coupes $\{28\} = (21) \times (30)$, $\{29\} = (19) \times (30)$, $\{32\} = (21) \times (33)$, $\{33\} = (19) \times (33)$ toutes 4 de probabilité $6{,}4 \cdot 10^{-5}$, 8 fois plus probables que n'importe quelle autre panne double mais qui représentent quand même moins de 3/1000° du risque de ND.

d) Il est possible de détecter les points faibles ou forts du système à l'aide d'indicateurs qui peuvent être choisis en fonction de ce qui doit être mis d'avantage en évidence (7).

1° Par exemple le composant y_l a d'autant plus d'influence sur le comportement du moteur que le taux d'augmentation de fiabilité du système dû à l'augmentation de fiabilité du composant y_l est plus grand. Cet effet se calcule à partir de la dérivée de $f(q)$ par rapport à la variation de q_l. En notant $f(q)$ la probabilité de non démarrage du moteur qui peut être écrite sous la forme :

$$f(q) = aq_l + b \text{ d'où } \frac{\partial f}{\partial q_l} = a.$$

Cette grandeur permet d'apprécier également l'importance des conséquences d'une erreur commise sur l'appréciation d'une probabilité et il s'agit en fait d'un calcul de sensibilité.

2° Le fait que le système tombe en panne lorsque le composant y_l tombe en panne est une caractéristique de sa criticité par rapport à cet événement, elle est mesurée par :

$$\frac{\partial f}{\partial q_l} \cdot q_l = Ci \text{ ou bien par } [f(1_l, q) - f(0_l, q)] \cdot q_l$$

Ce sont les événements (19), (21), (30), (33) qui sont, après (8) bien sûr, les plus critiques pour le ND. En effet, la probabilité conditionnelle de ND qui vaut $1{,}5 \cdot 10^{-4}$ est nettement plus élevée (10 à 20 fois) dans ce cas particulier, comparativement aux autres événements.

3° Si l'on veut apprécier l'influence d'une défaillance élémentaire cachée non fatale y_l sur le risque de ND, il suffit de considérer comme certaine cette défaillance y_l et calculer $p(64) = f(1_l, q)$ c'est-à-dire pour $y_l = 1$. On trouvera par exemple quand une bougie sur deux est en mauvais état c'est-à-dire en posant $p(18) = 1$ que $p(64) = 1{,}1 \cdot 10^{-1}$ soit 1,15 fois plus qu'avant. Le risque de ND a légèrement augmenté. On constaterait une influence du même ordre de grandeur en cas de défaut de segmentation sur un des deux cylindres.

Second Cas. Effet des règles pour les gardes-côte dans la réduction de la probabilité de collision dans le port de Boston d'un bateau citerne (BC) transportant du gaz naturel liquéfié GNL (8) (voir figure 11)

a) L'objectif est de voir l'effet des règles, définies au cours de l'étude, sur la réduction du risque. L'AdD ici commence par décrire les séquences possibles d'événements qui sont nécessaires à l'apparition de l'événement redouté. Le modèle ainsi trouvé décrit qualitativement et quantitativement des milliers de scénarios d'accidents. Le fait d'avoir ou non des règles s'interprète en affirmant comme vrai ou faux des événements dans l'AdD, c'est pourquoi cet arbre est non cohérent, car il contient cette fois en particulier des événements complémentaires (fig. 12) ou ce qui s'y ramène des portes OU exclusif du type C = A + B — AB (le signe — veut dire « mais pas »).

La construction de l'AdD reproduit le découpage en 4 secteurs géographiques du système étudié ce qui correspond aux 4 phases principales du transit du B.C. On a ensuite identifié 6 mécanismes possibles de rejet de GNL et c'est à partir de 2 de ces 6 événements qu'est poursuivie l'analyse.

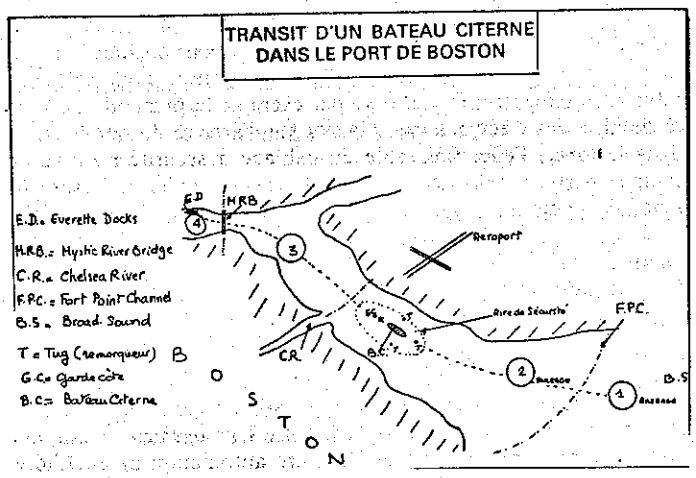


Fig. 12.

b) L'analyse qualitative trouve 600 combinaisons en présence de règles et 198 sans. On identifie un scénario général d'accident valable dans tous les cas :

1. Un autre bateau agresseur (BA) doit se trouver dans l'aire de manœuvre du BC cela veut dire que les règles ont été violées par erreur, par désobéissance ou par défaillance fatale d'équipements.

2. Les mécanismes de défense des 2 bateaux doivent faire défaut ce qui n'est possible que par la combinaison d'actions humaines et d'opérations matérielles qui échouent toutes.

3. Le BA doit peser plus de 1 000 tonnes, ce qui correspond à une vitesse critique d'impact indépendante de l'angle.

4. Le garde-côte (GC) et le remorqueur concerné sont inefficaces.

c) L'analyse quantitative indique pour un transit une $P = 4{,}6 \cdot 10^{-7}$ avec règles, contre $P = 1{,}4 \cdot 10^{-5}$ ce qui représente un facteur d'amélioration = 30. Dans les calculs faisant intervenir l'erreur humaine (EH) une forte dépendance a été prise en considération, c'est-à-dire que la probabilité de la séquence d'erreur $(EH) = (EH)_1 \times (EH)_2 \times (EH)_3$ est plus forte que le produit des 3 supposées statistiquement indépendantes (13). Aussi en situation opérationnelle normale, le risque d'erreur a été estimé $p(EH)_1 = 10^{-2}$ par opération, en cas de tension $p(EH)_2 = 10^{-1}$ et en cas de détresse ou panique $p(EH)_3 = 1$ soit une probabilité de l'erreur humaine globale de 10^{-3} au lieu de 10^{-6}.

On constate que dans tous les cas la probabilité conditionnelle de l'EH dans l'accident est de 0,99 et celle d'une vitesse excessive à l'impact de 0,70. Lorsqu'il y a des règles le scénario le plus probable d'accident, $p = 0{,}96 \cdot 10^{-7}$, soit une fois sur 5, est le suivant :

1. A cause d'EH, le BA ne respecte pas les mises en garde faites par radio $p = 10^{-2}$.

2. Il pénètre donc dans l'aire de manœuvre du BC.

3. A cause d'une EH, le BC n'entreprend pas de mesure d'évitement $p = 10^{-2}$.

4. Les remorqueurs échouent dans leurs manœuvres aussi par EH $p = 10^{-1}$.

5. La vitesse d'impact est critique $p = 1{,}6 \cdot 10^{-2}$.