Titre: Title:	Intérêt et applications potentielles des systèmes experts au domaine de la santé et de la sécurité du travail
Auteurs: Authors:	Christian Fortin, & Robert Gilbert
Date:	1987
Type:	Rapport / Report
Référence: Citation:	Fortin, C., & Gilbert, R. (1987). Intérêt et applications potentielles des systèmes experts au domaine de la santé et de la sécurité du travail. (Rapport technique n° EPM-RT-87-37). https://publications.polymtl.ca/9838/

Institution:	École Polytechnique de Montréal
Numéro de rapport: Report number:	EPM-RT-87-37
URL officiel: Official URL:	
Mention légale: Legal notice:	

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

INTÉRÊT ET APPLICATIONS POTENTIELLES DES SYSTÈMES EXPERTS AU DOMAINE DE LA SANTÉ ET DE LA SÉCURITÉ DU TRAVAIL

PAR

CHRISTIAN FORTIN, ing., M.Sc.A.,

CANDIDAT AU Ph.D.,

DÉPARTEMENT DE GÉNIE ÉLECTRIQUE

ET

ROBERT GILBERT, Ph. D.

PROFESSEUR AGRÉGÉ

DÉPARTEMENT DE GÉNIE INDUSTRIEL

(1987)

Table des matières

Sommaire

Le champ de la santé et de la sécurité du travail constitue un domaine idéal pour l'approche par les systèmes experts, si on en juge par les critères habituellement utilisés dans la littérature. La création d'un tel système entraînerait dans ce domaine des retombées positives majeures : développement et mise en application d'un cadre conceptuel clair et approprié, disparition du plafonnement actuel de l'efficacité de la prévention, découverte d'un nouveau paradigme, ainsi que d'autres retombées majeures. Pour maximiser les retombées attendues, un tel système devrait être développé d'abord dans le domaine de la sécurité du travail, être doté d'une base de faits et de règles tirés du domaine de l'ergonomie, contenir un certain nombre de connaissances et de scénarios sur la survenue de l'erreur humaine, et être capable de traiter les problèmes de fiabilité des systèmes. À partir de ce noyau, et à l'aide d'une stratégie de validation appropriée, il devrait être possible d'élaborer un système expert extrêmement utile comme aide dans l'étude des risques et des accidents ou des maladies du travail.

1.0 Introduction

Les objectifs de ce travail consistent à :

- définir ce que pourrait être un système expert pouvant aider à l'analyse des risques, des accidents et des maladies du travail, particulièrement s'il pouvait suggérer des causes et des scénarios d'erreur humaine à partir de ce qui est connu en ergonomie;

- indiquer les principales retombées positives attendues de la création d'un tel système;

- circonscrire le problème de la fiabilité humaine;

- préciser les grandes lignes d'une stratégie appropriée de développement et de validation.

La méthodologie consistera simplement à réaliser une synthèse des connaissances acquises :

- dans le cadre du cours d'Introduction aux systèmes experts 9.6984 de l'École polytechnique de Montréal;

- dans les références citées dans la bibliographie;

- à l'occasion de nos travaux antérieurs dans le domaine de l'ergonomie appliquée aux problèmes de santé et de sécurité du travail.

En particulier,

- nous définirons les notions de fiabilité et de sécurité d'un système, ainsi que les rapports entre ces deux notions;

- nous indiquerons les principales difficultés rencontrées dans l'évaluation de la fiabilité des systèmes hommes-machines, par suite des caractéristiques propres à l'être humain;

- nous évaluerons sommairement et à l'aide de quelques exemples l'intérêt qu'il pourrait y avoir à utiliser les langages de l'intelligence artificielle dans les études de fiabilité et de sécurité.

2.0 Intérêt des systèmes experts en santé et sécurité du travail

Le domaine de la santé et de la sécurité du travail constitue un champ idéal pour l'approche par les systèmes experts, si on en juge par les critères habituellement utilisés dans la littérature et, notamment, par A. Bonnet (1984) et E.A. Feigenbaum et P. McCorduck (1984) :

a) existence d'un levier économique important;

b) niveau des connaissances utiles suffisamment techniques;

c) appartenance de nombreux problèmes du domaine à l'une des classes de problèmes qui se prêtent bien à la résolution par les systèmes experts, en l'état actuel de l'art :

- gestion, interprétation et mise à jour rapide d'un ensemble complexe de données,
- diagnostic (dans les domaines notamment de la sécurité, de l'hygiène industrielle, de la toxicologie et de la médecine industrielle),
- détection d'anomalies dans la conception ou le

fonctionnement d'un système,

- classification,
- évaluation de situations actuelles et de solutions proposées,
- gestion de crise (dans le contrôle de réacteurs chimiques ou de puissance, par exemple).

Plus précisément, l'utilité et l'intérêt évidents des systèmes experts en santé et sécurité du travail sont fondés sur les considérations suivantes :

1) Les accidents et les maladies reliés au milieu de travail entraînent des coûts fantastiques. On évalue à 14 milliards de dollars ce qu'il en a coûté aux Canadiens, en 1984 seulement, en frais de mortalité, d'accidents et de maladies reliés au milieu de travail, sans compter la souffrance, la peine et l'inquiétude qui s'ensuivent inévitablement (source : Travail Canada, in Travail et Santé, volume 2, no 1, 1986). Il suffirait donc que les systèmes experts contribuent un tant soit peu à une augmentation de l'efficacité de la prévention, pour que le coût de leur développement, de leur diffusion et de leur entretien soit remboursé plusieurs fois.

2) Les problèmes de santé et sécurité du travail sont essentiellement multidisciplinaires. Ils ne peuvent souvent être résolus efficacement que par l'interaction de plusieurs spécialistes, ou éventuellement par une fusion intelligente de leurs compétences respectives dans un système expert.

3) Les problèmes de sécurité impliquent souvent tant de possibilités à explorer qu'on peut facilement passer à côté de causes importantes d'accident ou de maladie ou les mal comprendre. Il est donc nécessaire d'utiliser une procédure systématique d'examen et d'analyse, reposant sur une représentation aussi exhaustive que possible de la réalité. Un système expert ne se fatigue pas. Il n'est pas sujet à des oublis ou à des distractions. Il peut être beaucoup plus systématique et efficace que l'être humain dans un travail de routine.

4) Les connaissances utiles en santé et en sécurité du travail sont très nombreuses, très techniques et très spécialisées. L'essentiel de ces connaissances et, en particulier, les règles de l'art sont déjà codifiées dans les encyclopédies techniques, dans les manuels de référence et les fiches techniques

qui sont publiés et régulièrement remis à jour par les divers organismes nationaux et internationaux de prévention et de normalisation. Dans certains domaines, comme en toxicologie, il existe déjà d'immenses banques de données informatisées. Il serait très avantageux de pouvoir explorer les informations pertinentes à l'aide d'un système intelligent.

5) Les connaissances utiles en santé et sécurité du travail évoluent très rapidement. Les systèmes experts présentent d'intéressantes possibilités de mise à jour automatique.

6) Les experts en santé et sécurité du travail d'une entreprise ou d'un milieu industriel donné peuvent au fil des années accumuler une réserve énorme et précieuse de savoir expert. Ce dernier peut disparaître à mesure que les gens oublient, s'en vont à la retraite ou changent de milieu. Un système expert pourrait servir à stocker l'expertise collective de l'entreprise ou du milieu. Cette spécialisation, propre à un milieu d'usagers, accroîtrait sûrement la facilité d'utilisation et l'efficacité

du système expert. Elle présenterait ainsi pour la prévention dans ce milieu un avantage important.

7) Il y a actuellement à travers le monde et notamment au Québec, une pénurie d'experts qualifiés et de haut niveau en santé et sécurité du travail et, plus particulièrement, en ergonomie et en sécurité. Contrairement à ce qu'on prétend parfois, l'écart entre l'offre et la demande ne tendra pas à se résorber dans un proche avenir, mais augmentera au contraire rapidement dans le présent contexte. Les programmes actuels de formation intensive, de recyclage accéléré et de développement de ressources humaines auront d'abord pour effet de stimuler la demande en permettant l'identification de besoins plus nombreux et sophistiqués.

Par ailleurs, la complexité et l'intégration croissantes des technologies actuelles ainsi que leur développement accéléré, génèrent de nouveaux besoins en matière de prévention et nécessitent, malgré la transparence également croissante de ces technologies, une approche préventive à plus long terme, plus exhaustive et plus profonde; bref : une approche permettant de mieux appréhender la complexité

des situations réelles de travail. Cette nécessité entraîne à son tour une augmentation accrue de la demande en experts qualifiés et de haut niveau en santé et sécurité du travail dans tous les secteurs de l'activité humaine. On aura aussi remarqué que toute cette dynamique entraîne naturellement une accélération de l'évolution, déjà rapide, des connaissances en ce domaine, ainsi qu'une intensification des besoins de mise à jour rapide.

Il nous apparaît donc essentiel et urgent, de ce point de vue :

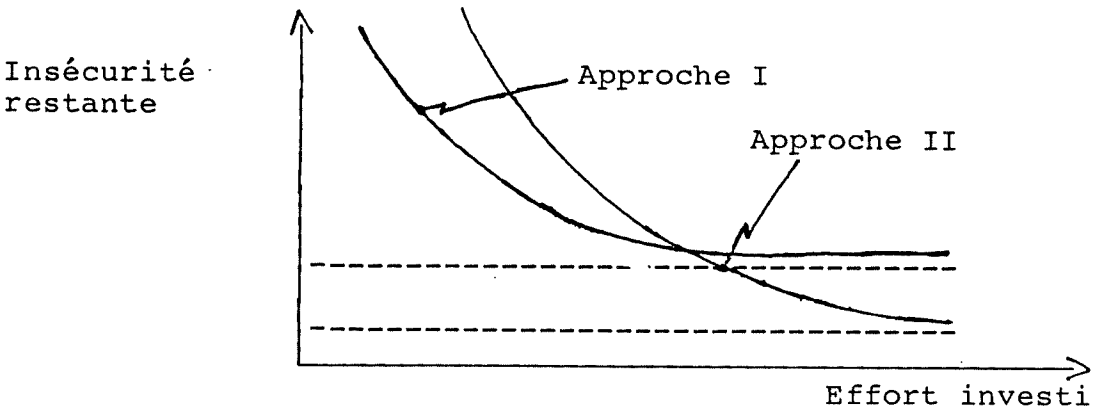
- de mettre à la portée du plus grand nombre possible le maximum des connaissances et des compétences des experts dans les nombreuses sous-spécialités reliées à la santé et à la sécurité du travail;
- de développer des outils, des méthodes et moyens de solution des problèmes, ainsi que des méthodes et moyens de conception sécuritaire des équipements, du travail et de l'environnement de travail, pour les mettre à la disposition des principaux intervenants en ce domaine.

8) L'élaboration d'un système expert exige d'abord un cadre conceptuel clair afin de :

- définir les bases de données pertinentes;
- choisir les règles de raisonnement utiles sur les données, y compris les règles pour régler les conflits de règles ou de critères;
- retenir les concepts et les méthodes de résolution de problèmes qui sont réellement efficaces dans le domaine considéré.

En prévention, on reconnaît et regrette l'absence d'un tel cadre depuis plus de vingt ans (De Cock, 1964; Faverge, 1967; Leplat et Cuny, 1974; Cuny et Grawsky, 1972; Raouf, 1972; Surry, 1974; Gilbert, 1975, 1981, 1982, 1983; Fortin, 1983; Fortin et al., 1983a, b, c et d). Un tel cadre présenterait de nombreux avantages importants en prévention. En particulier, il permettrait de définir une procédure systématique de diagnostic des risques, d'analyse des accidents et de leurs sources déterministes et non déterministes. Il pourrait servir de schéma général de référence, fournir une grille d'analyse et suggérer des hypothèses qui pourraient aider très efficacement à l'élaboration d'un bon diagnostic.

Par ailleurs, on remarque depuis plusieurs années un plafonnement de l'efficacité de la prévention. L'abaissement de la fréquence et de la gravité des accidents et des maladies du travail dans les pays industrialisés est loin d'être en rapport avec les efforts investis. Ceci est peut être tout à fait naturel, dans la mesure où le rendement d'une approche donnée, pour la réduction de la fréquence et de la gravité des accidents, est nécessairement décroissant. Il est toujours plus facile d'améliorer une situation mauvaise qu'une très bonne. En conséquence, si les efforts de prévention sont engagés dans un ordre de priorité correspondant à leur rendement effectif, le rendement global d'une approche donnée sera une fonction monotone décroissante. Ainsi, la valeur absolue de la dérivée d'un indice d'insécurité, par rapport à un indice d'effort ou d'investissement en prévention, est décroissante lorsque l'indice d'effort augmente. Ceci peut être illustré par un graphique du type suivant :



Il arrive donc un moment où une augmentation, même considérable, des efforts investis ne produit plus d'amélioration significative du niveau de la sécurité. À notre avis, nous sommes actuellement arrivés à un point où, pour progresser encore, il nous faut développer et utiliser de nouvelles approches, de nouvelles méthodes et de nouveaux moyens (Fortin, 1984). Les approches de type statique sont maintenant dépassées depuis longtemps, et il faut désormais utiliser des approches qui tiennent réellement compte de la complexité et de la dynamique des relations entre les personnes, les machines, les tâches, les espaces et les environnements de travail.

Ainsi donc, le développement et la mise en application d'un cadre conceptuel approprié pourrait fort bien constituer la contribution la plus importante des systèmes experts au domaine de la prévention des accidents et maladies du travail. Parmi les autres retombées positives, on peut mentionner ici l'élaboration, à court ou à moyen terme :

- d'une terminologie cohérente dans le domaine de la sécurité;
- de méthodes plus efficaces d'identification et d'analyse des risques en milieu de travail;

- de méthodes plus efficaces pour l'analyse des accidents;
- de méthodes plus efficaces en prévention;
- d'outils de gestion de la recherche et du développement en matière de santé et sécurité du travail.

Les systèmes experts sont généralement conçus pour être capables d'expliquer les lignes de raisonnement qui les ont amenés à prendre leurs décisions. Certains peuvent même dire pourquoi ils ont rejeté tel raisonnement pour en choisir un autre. Cette transparence est un trait dominant de ces systèmes. C'est d'ailleurs un trait nécessaire. Pour être capable de juger s'il peut avoir ou non confiance en une certaine conclusion, l'usager doit être capable de comprendre non seulement cette conclusion, mais aussi les faits et le raisonnement qui y conduit. En cas de doute, il sera par ailleurs davantage en mesure de fournir de nouveaux faits ou de tester d'autres lignes de raisonnement.

À plus long terme, il sera possible aussi de concevoir ces systèmes de façon à ce que leurs explications s'adaptent au niveau et au type de formation de l'usager (A. Bonnet, 1984). Un expert dans un domaine donné a besoin de moins de détails dans son domaine qu'un autre

pour comprendre un raisonnement donné et surtout pour en voir les limites. On peut aussi les doter d'une capacité pédagogique très intéressante, dans la mesure où on peut facilement les modifier de façon à ce qu'ils puissent suivre et comprendre les raisonnements et les solutions imaginées par les usagers (A. Bonnet, 1984). Ils peuvent alors expliquer ce qui va ou ne va pas dans une solution donnée, et ils peuvent même être capables de retenir de bonnes idées pour un usage futur. Ils peuvent donc constituer une forme très intéressante de formation interactive et adaptée aux besoins individuels. En outre, les concepteurs de tels systèmes investissent actuellement beaucoup de temps pour les doter de la capacité de comprendre et de s'exprimer en langage naturel. Les progrès de la recherche sont très rapides et certains systèmes sont actuellement très performants dans des domaines bien précis, si on veut bien accepter de passer par un clavier. La synthèse de la parole est très avancée mais le déchiffrage de la parole pose encore de grandes difficultés.

En résumé, les objectifs d'un système expert en santé et sécurité du travail seraient :

1° <u>à un premier niveau de</u> :

a) capter, copier et distribuer la compétence des

experts du domaine;

b) fusionner la connaissance détenue par plusieurs experts, dans un contexte multidisciplinaire;

c) gérer et mettre à jour la connaissance pertinente;

d) former des usagers et élargir leur expertise particulière et générale dans le domaine;

e) améliorer l'efficacité de la prévention à l'aide d'une meilleure approche ou d'une approche plus systématique des facteurs potentiellement impliqués (plusieurs milliers).

2° <u>à un second niveau, de</u> :

a) diagnostiquer les problèmes en exploitant systématiquement toute la connaissance pertinente;

b) proposer des solutions;

c) évaluer des solutions et les comparer entre elles;

d) orienter l'usager dans la mesure des informations disponibles;

e) proposer des stratégies d'observations et de prise de données;

f) aider à la gestion de problèmes complexes ou de situations de crise.

Il s'agit là d'un programme ambitieux, mais vraisemblablement réaliste, dans la mesure où il pourrait être réalisé par étapes et dans la mesure où il existe déjà plusieurs systèmes experts dans des domaines connexes tels :

- la conception de postes de travail;
- la médecine;
- la sécurité (militaire et financière);

ainsi qu'on peut le constater en parcourant la liste placée à la fin de l'ouvrage de E.A. Feigenbaum et P. McCorduck.

En fait, dans certains sous-domaines comme la médecine du travail et la toxicologie industrielle, il suffirait peut-être d'utiliser directement l'un des systèmes existant actuellement en médecine, en modifiant ou en changeant sa base de règles et de faits et en ajoutant un certain nombre de termes et d'expressions (éventuellement grand dans le cas de la toxicologie) dans le dictionnaire de l'interface en langage naturel.

On pourrait éventuellement procéder de la même façon en sécurité, en ingénierie ou en ergonomie. Cependant, parce que les accidents proviennent essentiellement de l'interaction défectueuse entre plusieurs composantes d'un

système, il nous apparaît préférable mais aussi plus intéressant, de procéder autrement.

En effet, un système résultant d'une telle adaptation, ne pourrait que contribuer très peu à la problématique des accidents du travail ou des accidents en général. Une telle adaptation permettrait sans doute d'améliorer l'efficacité de la prévention et du diagnostic des maladies du travail, mais elle n'est certainement pas très apte à générer la plupart des retombées positives que nous avons mentionnées précédemment.

3.0 Sécurité, ergonomie et fiabilité

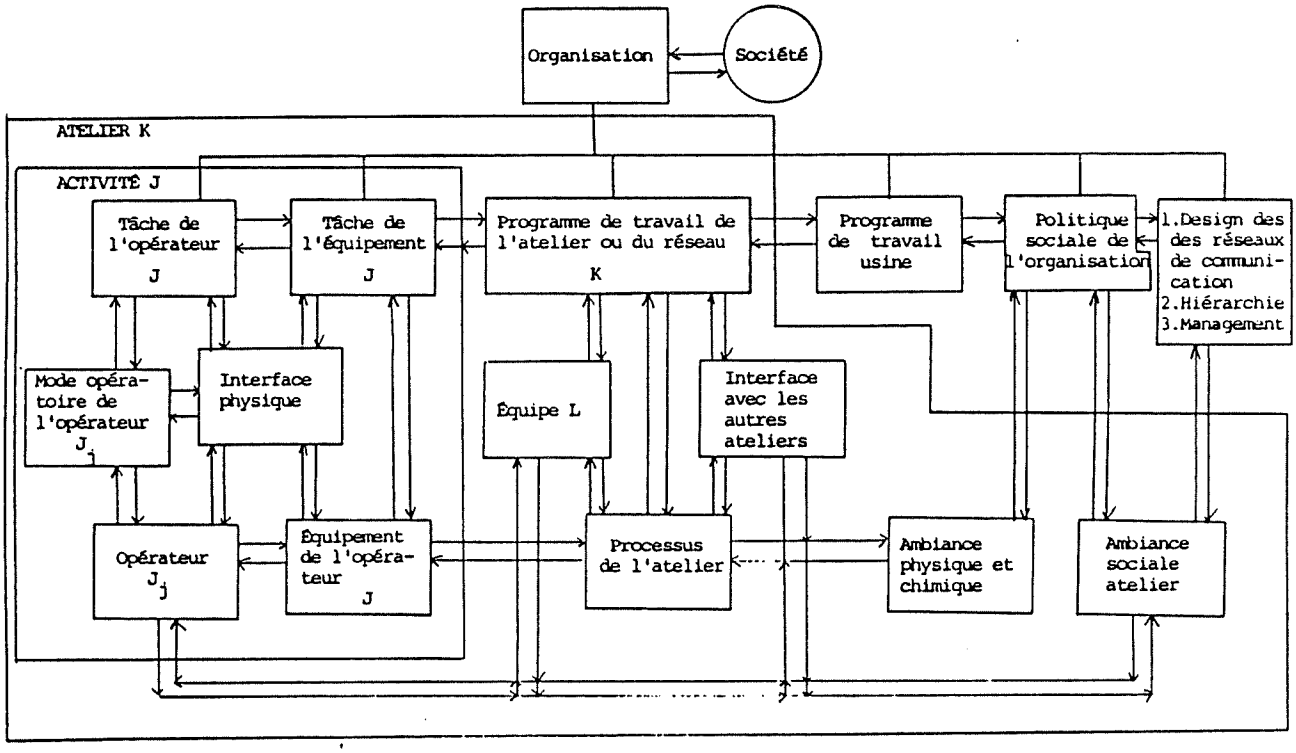
Les accidents et les maladies du travail peuvent être définis, d'une façon générale, comme le résultat de relations défectueuses dans un système de production entre les personnes, leur travail et le matériel utilisé au cours de ce dernier (Fortin, 1983). La figure 1, à la page suivante, constitue un exemple de découpage d'un système de production en blocs intereliés. Cette figure est tirée de Fortin (1983).

L'objet de l'ergonomie est justement d'étudier ces relations en termes de sécurité, de confort et de productivité. L'étude de telles relations amène inévitablement à reviser la conception des équipements et des méthodes de travail. L'ingénierie et l'ergonomie deviennent ainsi indissociables dans le diagnostic des problèmes de santé et, plus spécifiquement, de sécurité du travail, ainsi que dans l'élaboration, l'adaptation et l'implantation de solutions efficaces à ces problèmes.

Un système expert en santé et sécurité du travail devra donc être doté d'une base de faits et de règles tirés du domaine de l'ergonomie. En particulier, un tel système devra contenir les nombreuses connaissances

Découpage par blocs des composantes d'un système hommes-machines

Figure 1



disponibles en ergonomie sur les mécanismes de la survenue de l'erreur humaine, et être capable d'évaluer l'effet des diverses erreurs sur le fonctionnement du système considéré, les possibilités de récupération précoce ou tardive, ainsi que les moyens de prévention utiles.

Ce point est d'une extrême importance. Déjà en 1959, dans une étude portant sur 75 000 cas d'accidents variés dans divers secteurs industriels, Heinrich a trouvé que 98% de tous les accidents auraient pû être prévenus et que 88% avaient été causés par des actions dangereuses. Par la suite, de nombreux travaux démontrèrent l'importance de l'erreur humaine dans l'arrivée des accidents. Avec le temps cependant, l'interprétation du rôle de l'erreur humaine s'est progressivement modifiée, au fur et à mesure qu'on tentait de clarifier la signification et les mécanismes de la survenue de l'erreur humaine.

Aujourd'hui, celle-ci n'est plus perçue uniquement comme une cause d'accident, mais principalement comme l'indice de relations défectueuses ou de dysfonctionnements au niveau de l'interface entre la personne, sa tâche, son matériel, son environnement de travail et ses méthodes de travail. Les travaux de Fitts et Jones (1947), en particulier, avaient clairement démontré que

dans la majorité des accidents, les erreurs humaines prenaient leur source dans la conception inadéquate des interfaces personne-machine.

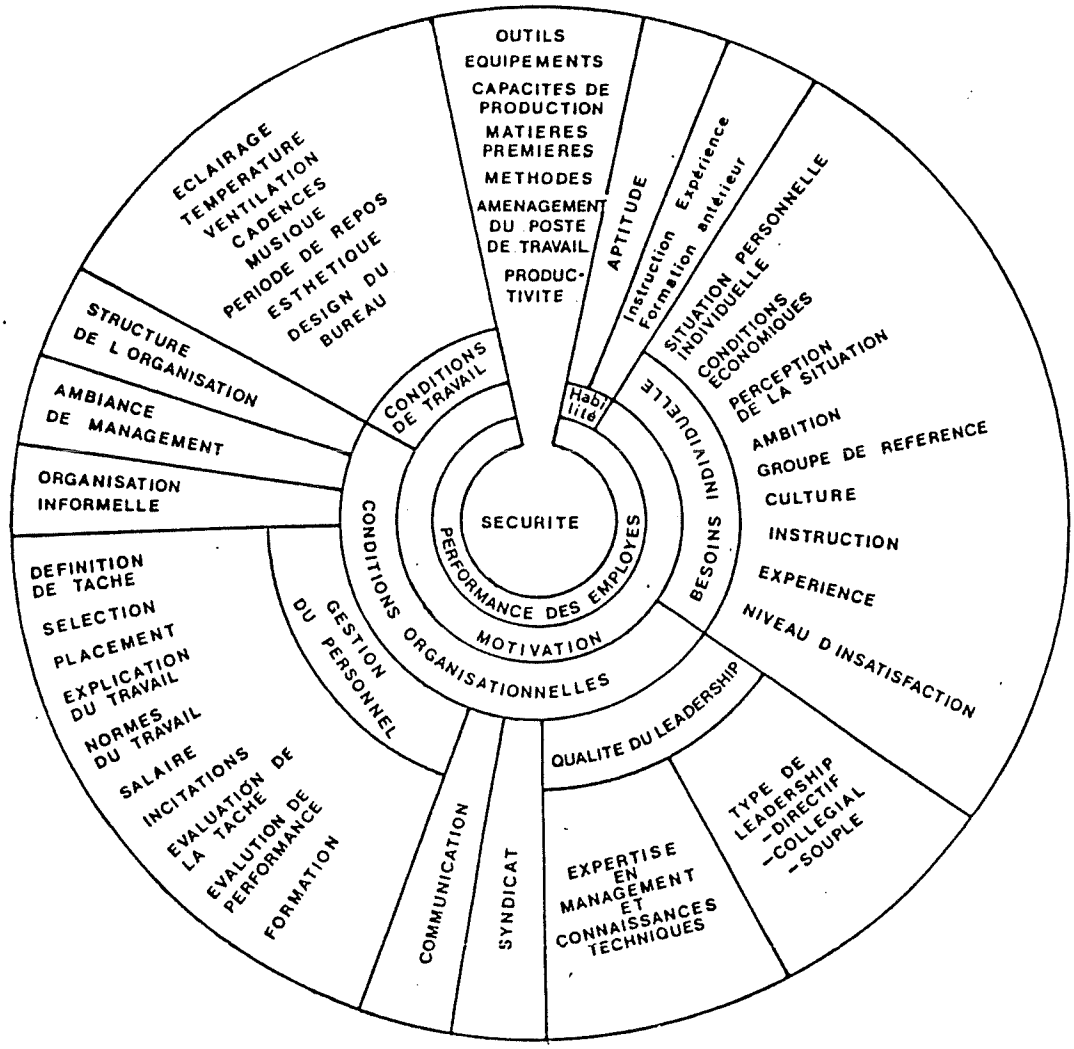
On ne peut demander à aucun être humain de ne jamais faire d'erreur, à quelque niveau que ce soit. En termes techniques, on dit que sa fiabilité n'est pas de 100%. Ainsi, on sait par exemple que dans les actions répétitives le taux d'erreur résiduel d'un opérateur humain oscillera entre 0,001 et 0,0001 par cycle, alors qu'un mauvais design ou une mauvaise organisation fera grimper ce taux à 0,01 et même à 0,1 (Swain et Guttmann, 1983). Les machines non plus ne peuvent être fiable à 100%. Cependant, dans les cycles répétitifs, leur fiabilité sera en général beaucoup plus élevée. Par ailleurs, ce ne sont pas toutes les pannes ou tous les dysfonctionnements qui conduiront à des accidents, pas plus que ce ne sont toutes les erreurs humaines dans l'exécution du travail. Parmi celles-ci, certaines n'ont pas de conséquences importantes du point de vue de la sécurité, alors que d'autres en ont ou peuvent en avoir mais sont récupérées à temps.

La question se pose donc aujourd'hui de la manière suivante : comment concevoir ou modifier :

- les équipements
- le travail, c'est-à-dire :
  - . l'organisation du travail
  - . les méthodes de travail
  - . les modes opératoires
  - . les informations utilisées pendant le travail
  - . les conditions d'exécution du travail
- le matériel
- l'individu (aptitudes, état et autres caractéristiques)
- d'autres facteurs (voir figure 2, page suivante, tirée de Fortin, 1983) afin de :
  - . minimiser, dans un premier temps, la probabilité d'erreur
  - . interdire, dans un deuxième temps, la transformation des erreurs en accidents.

Ou, en plus bref : comment concevoir des systèmes qui réduisent le plus possible les fréquences d'erreur humaine, et qui soient robustes vis-à-vis de ces erreurs. Mais comment, par ailleurs, reconnaître ou évaluer de tels systèmes? Il y a tellement de facteurs qui peuvent être impliqués dans les séquences ou les mécanismes déclencheurs des accidents! Plusieurs milliers, en fait (Fortin, 1983; Fortin et al., 1983a, b, c, d).

Figure 2



Principaux facteurs déterminant la sécurité au travail

La première phase consistera donc à présélectionner soigneusement les facteurs à considérer, puis à établir un diagnostic et à valider ce dernier. Un système expert pourrait être très utile déjà au niveau de la première étape. En effet, il pourrait effectuer cette présélection à l'aide d'une description du risque ou de l'accident envisagé par l'usager et d'un certain nombre de métarègles dans sa banque de règles. Il se trouverait ainsi à établir un prédiagnostic qui devra être évalué et éventuellement révisé ultérieurement. Il pourrait aussi établir ce prédiagnostic en conversant avec l'usager ou en complétant celui que lui aurait fourni l'usager au préalable. Plus simplement encore, l'usager pourrait se contenter d'indiquer, par exemple dans un menu structuré, les variables, les composantes et le niveau du système qui l'intéressent pour que le système expert lui suggère d'autres composantes ou d'autres variables, reliées aux premières, ainsi que des sous-variables et des indicateurs pertinents. Selon le niveau de détails désiré, le but de l'étude et les moyens disponibles, l'analyste pourra refuser certaines variables et en accepter d'autres. Après un certain nombre de choix, il aura découpé dans le réseau global un sous-réseau de variables correspondant à ses besoins. Ce dernier constituera alors un modèle réduit particulier qui pourra être approfondi, raffiné, traité ou développé de diverses façons par l'usager.

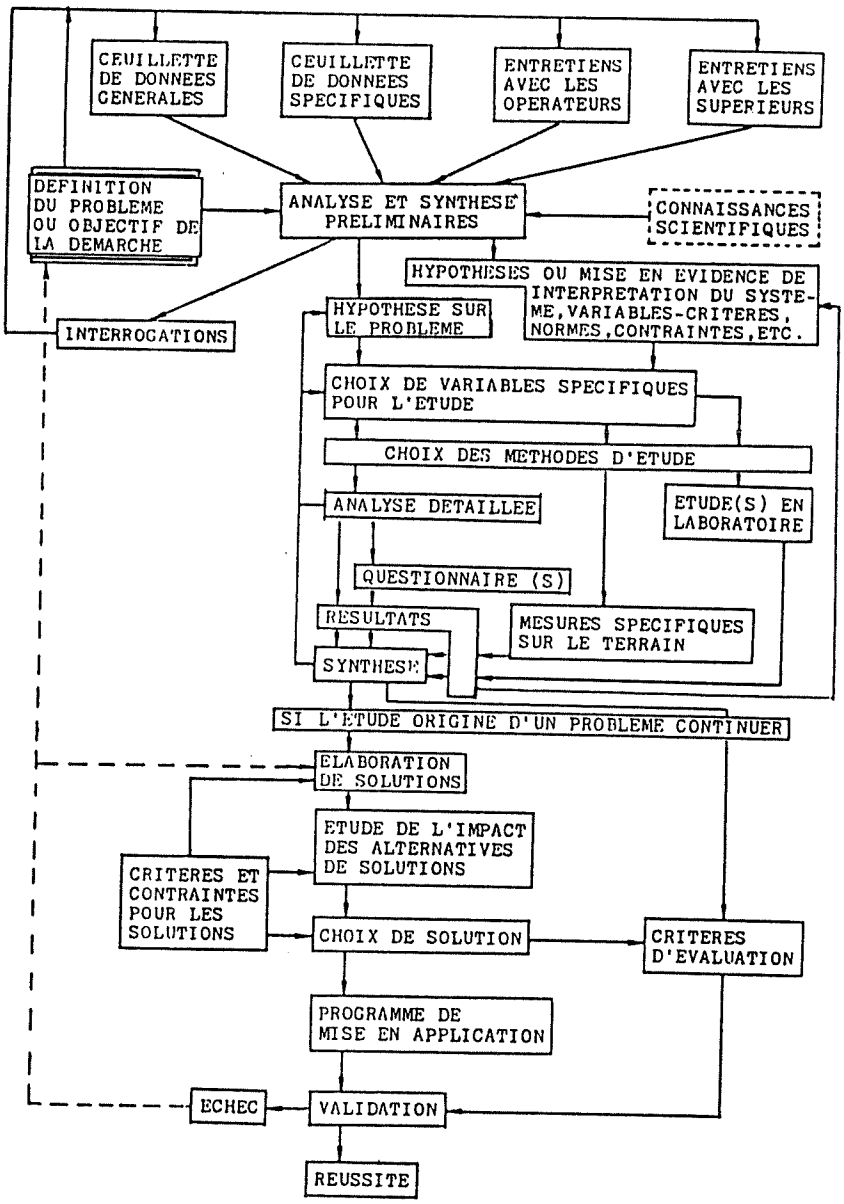
Toute la première phase se déroulerait itérativement en s'inspirant de la démarche méthodologique générale illustrée par la figure 3 à la page suivante (tirée de Gilbert, 1985).

La seconde phase consisterait à appliquer les outils connus en fiabilité des systèmes et, plus spécifiquement, les diverses techniques reliées aux arbres de défaillance. Cette phase permettrait ainsi d'évaluer et de comparer quantitativement divers systèmes (ou diverses versions d'un même système). En particulier, elle pourrait permettre à l'usager d'évaluer les probabilités a priori et a posteriori des accidents, c'est-à-dire avant qu'ils ne se soient produits (les risques) et après, surtout quand il s'agit d'une instantiation qui n'avait pas été envisagée a priori ou qui ne l'avait pas été de cette manière.

Cette démarche est assez naturelle si on se rappelle ici la définition que nous avons donnée au début de ce chapitre de l'accident ou de la maladie du travail, et si on la rapproche de la définition suivante de la fiabilité.

La fiabilité d'un système est habituellement définie comme sa probabilité de bon fonctionnement dans des conditions données pendant un temps donné. En conséquence, tout événement indésirable, toute perturbation dans le

Figure 3


CEUILLETTE DE DONNEES GENERALES
CEUILLETTE DE DONNEES SPECIFIQUES
ENTRETIENS AVEC LES OPERATEURS
ENTRETIENS AVEC LES SUPERIEURS
DEFINITION DU PROBLEME OU OBJECTIF DE LA DEMARCHE
ANALYSE ET SYNTHESE PRELIMINAIRES
CONNAISSANCES SCIENTIFIQUES
HYPOTHESES OU MISE EN EVIDENCE DE INTERPRETATION DU SYSTE-ME,VARIABLES-CRITERES, NORMES,CONTRAINTES,ETC.
INTERROGATIONS
HYPOTHESE SUR LE PROBLEME
CHOIX DE VARIABLES SPECIFIQUES POUR L'ETUDE
CHOIX DES METHODES D'ETUDE
ANALYSE DETAILLEE
ETUDE(S) EN LABORATOIRE
QUESTIONNAIRE (S)
RESULTATS
MESURES SPECIFIQUES SUR LE TERRAIN
SYNTHESE
SI L'ETUDE ORIGINE D'UN PROBLEME CONTINUER
ELABORATION DE SOLUTIONS
ETUDE DE L'IMPACT DES ALTERNATIVES DE SOLUTIONS
CRITERES ET CONTRAINTES POUR LES SOLUTIONS
CHOIX DE SOLUTION
CRITERES D'EVALUATION
PROGRAMME DE MISE EN APPLICATION
ECHEC
VALIDATION
REUSSITE

fonctionnement du système, pourra être considéré comme un dysfonctionnement, c'est-à-dire comme un défaut de fiabilité. Toutefois, comme dans les systèmes complexes de tels événements sont continuels, nous sommes amenés à ne considérer comme tels que les événements ayant au moins un certain degré d'indésirabilité.

Dans ce contexte, les accidents et les maladies du travail appartiennent à la classe des événements indésirables à un certain degré et sont donc justiciables des méthodes de la fiabilité des systèmes, comme l'a d'ailleurs montré Faverge (1967). Le degré d'indésirabilité est relié à la gravité des conséquences de l'événement. L'acceptabilité d'un risque est relié à sa probabilité de réalisation, à sa gravité, ainsi qu'aux possibilités existantes de prévention en fonction de leur coût ou leur contribution au bon fonctionnement du système.

Par ailleurs, nous devons considérer qu'il n'y a pas de différence qualitative entre l'accident et la maladie du travail, car seuls l'échelle des temps et le niveau des énergies diffèrent. L'accident, en effet, arrive soudainement et libère beaucoup d'énergie (relativement aux capacités d'absorption ou de résistance des surfaces de transfert concernées) durant un temps bref et les dommages

qu'il peut causer à l'organisme apparaissent rapidement. La maladie industrielle, par contre, n'apparaît que progressivement, à la suite d'une exposition plus ou moins longue à des niveaux d'énergie relativement faibles, mais nocifs, et les dommages causés à l'organisme ne se révèlent souvent qu'à long terme. La surdité industrielle, par exemple, provient de l'exposition à des niveaux trop élevés de bruit (énergie sonore), alors qu'une intoxication chronique peut provenir, par exemple, d'une exposition à des concentrations trop élevées de certains contaminants dans l'air (énergie chimique), tels les solvants, l'oxyde de carbone, les poussières de plomb ou d'autres contaminants.

Ainsi donc, un système expert en sécurité du travail pourrait être utilisé aussi en santé du travail, et particulièrement s'il s'agit de concevoir (ou de reconcevoir, à des fins de correction ou d'amélioration) un système de production.

Enfin, l'analyse par les arbres de défaillance est à l'heure actuelle et malgré ses défauts à peu près la seule méthode valable d'analyse a priori et a posteriori des accidents (Henley et Kumamoto, 1983; Bruun, Rasmussen et Taylor; 1979). Par ailleurs, depuis que l'on a appris à

les construire et à les traiter par informatique, ces défauts ont commencé à s'estomper, et les progrès de la recherche sont à ce niveau très rapides (Henley et Kumamoto, 1981, 1985). Ceci s'explique par le fait que dans l'ordinateur on représente l'arbre par des tables de décision et que celles-ci permettent beaucoup de flexibilité à divers niveaux tels que :

- le nombre d'états que peut prendre une composante donnée;
- le nombre, le type et l'organisation des relations qu'une composante peut avoir avec d'autres, étant donné son état et les états des autres composantes avec lesquelles elle interagit;
- la structuration des tables et les méthodes de réduction logique des rapports entre composantes;
- l'application des algorithmes de la recherche opérationnelle pour découvrir les ensembles de coupe minimale ou les chemins critiques de défaillance;
- la possibilité d'étudier les risques d'accident dans l'ordre des probabilités décroissantes.

De plus, on peut noter ici qu'il a eu beaucoup de progrès depuis quelques années concernant le codage et le traitement des tables de décision, en termes des gains

réalisés en temps de traitement et en espace-mémoire nécessaire (Maurice Queyranne, communication personnelle).

Ainsi, l'avancement en ce domaine provient essentiellement des progrès en programmation logique et en traitement des réseaux de composantes et en traitement des arbres d'événements. Or, les langages utilisés en intelligence artificielle étant spécialement conçus pour être efficaces dans ces domaines, on peut certainement supposer que leur utilisation pourrait être très profitable dans les analyses de fiabilité. Cette impression se renforce quand on examine les principales étapes de la construction d'un arbre de défaillance. Ces étapes sont les suivantes :

1- Identification des modes de défaillance des composantes à partir de plusieurs points de vue. (Une composante est un sous-système du système considéré. Elle correspond au niveau le plus élémentaire de la hiérarchie des sous-systèmes figurant dans l'analyse).

2- Identification des modes de défaillance reposant sur les interrelations entre les composantes, sous diverses conditions. Dans le cas d'un opérateur, on considérera, par exemple : son état de santé et de stress, ses conditions de travail, etc.

3- Identification des modes de défaillance reliés aux interrelations entre sous-systèmes.

4- Identification des modes de défaillance reliés aux interactions entre les personnes et les équipements, et notamment au niveau des communications, à celui des contrôles et à celui des méthodes de travail.

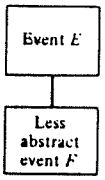
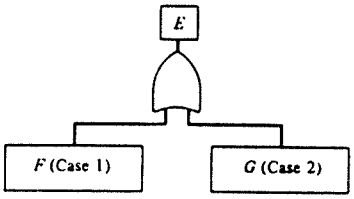
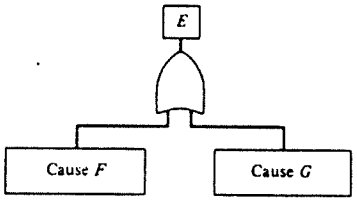
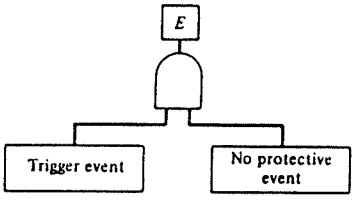
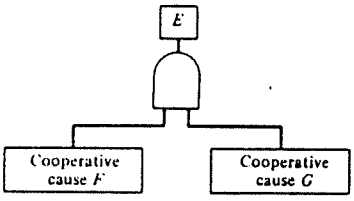
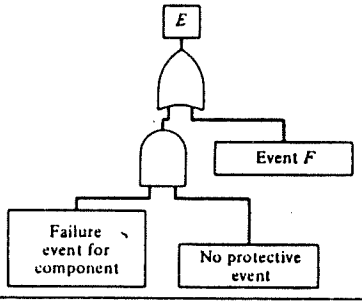
5- Réalisation d'une analyse des modes et conséquences des défaillances.

6- Construction de l'arbre des défaillances.

Les cinq premières étapes correspondent à l'élaboration de la base de faits et de règles spécifiques au système à évaluer, tandis que la sixième correspond aux procédures utilisées par l'expert en fiabilité (ou, plus généralement, par l'équipe d'experts) pour construire l'arbre des défaillances, effectuer les calculs requis et simuler l'écoulement du temps. Ces procédures incluent un certain nombre d'heuristiques dont on pourrait certainement s'inspirer pour diriger les échanges entre un système expert et un usager et pour construire systématiquement les arbres de défaillance. Le tableau 1 à la page suivante indique les principales étapes de l'une de ces heuristiques, alors que les figures 4 et 5 illustrent une autre heuristique. Bien entendu, la construction d'un arbre de

Tableau 1

HEURISTIC GUIDELINES FOR FAULT TREE CONSTRUCTION

	Development Policy	Corresponding Part of Fault Tree
1	Equivalent but less abstract event F	
2	Classification of event E	
3	Distinct causes for event E	
4	Trigger versus no protective event	
5	Cooperative cause	
6	Pinpoint a component failure event	

Ernest J. Henley
Hiromitsu Kumamoto

Figure 4

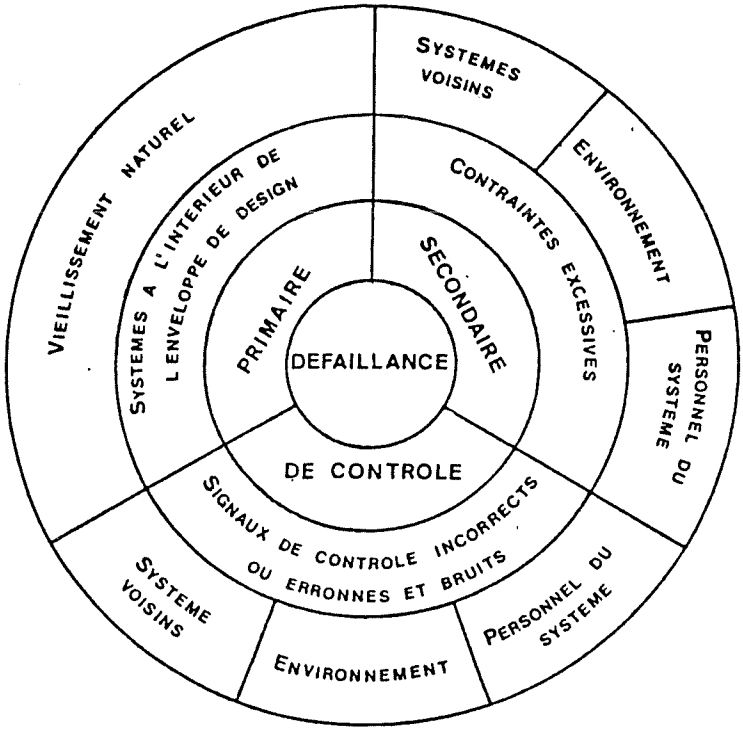
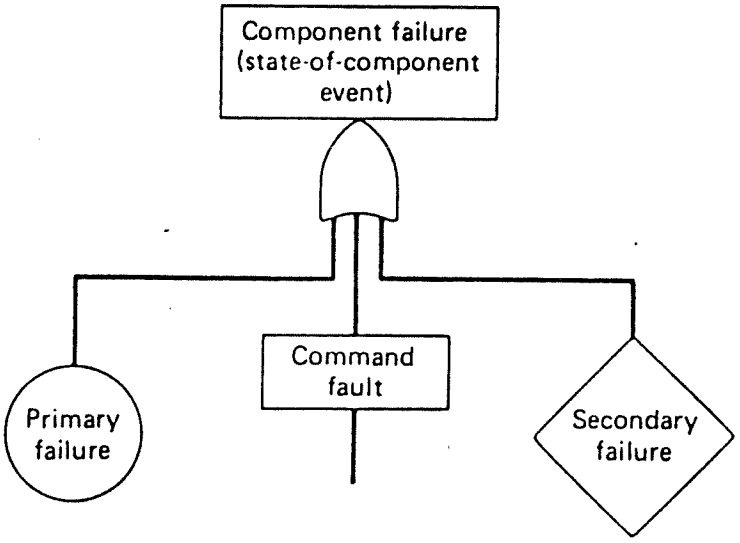

SYSTEMES VOISINS
ENVIRONNEMENT
PERSONNEL DU SYSTEME
PERSONNEL DU SYSTEME
ENVIRONNEMENT
SYSTEME VOISINS
VIEILLISSEMENT NATUREL
SYSTEMES A L'INTERIEUR DE L ENVELOPPE DE DESIGN
CONTRAINTES EXCESSIVES
PRIMAIRE
SECONDAIRE
DEFAILLANCE
DE CONTROLE
SIGNAUX DE CONTROLE INCORRECTS OU ERRONNES ET BRUITS

Figure 5



Development of a component failure (state-of-component event).

Ernest J. Henley

Hiromitsu Kumamoto

défaillance, ainsi que son évaluation quantitative, exigent que soient d'abord définis au moins les principales portes logiques. Mais, cela ne devrait pas être un bien grand problème dans les langages de l'intelligence artificielle. En fait, nous pensons qu'il serait même particulièrement intéressant d'utiliser pour cela un langage tel que PROLOG. En effet, dans les arbres de défaillance, le nombre d'entrées d'une porte logique donnée est variable, selon l'événement considéré à la sortie : une porte "et" par exemple, peut avoir un nombre quelconque d'entrées et il en est de même pour le "ou-ordinaire", le "ou-exclusif", le "ou-à-k-entrées-positives-parmi-n", et ainsi de suite. En PROLOG, ces portes pourraient être aisément définies à l'aide de règles récursives sur des listes de longueur variable. Ensuite, pour les calculs, on pourrait traiter ces portes comme des opérateurs multinaires et utiliser :

- des procédures de simplification, utiles pour notamment :
  - . enlever des portes "et" les événements hautement probables;
  - . enlever des portes "ou" les événements hautement improbables;
  - . remplacer les portes plus compliquées par une

combinaison de portes plus simples, lorsque nécessaire;

. générer les arbres conditionnels nécessaires lorsque certains événements se répètent dans diverses branches ou s'excluent mutuellement, et les relier par un "ou-exclusif";

. simplifier les super arbres, de manière à éviter l'explosion combinatoire des événements et des calculs;

- des procédures de distribution des opérateurs "et" sur les "ou" de traitement de l'opérateur "négation", de réarrangement des termes dans une forme normale, et d'application de l'opérateur espérance mathématique.

Or, toutes ces procédures sont courantes en PROLOG et on peut en trouver des exemples dans la plupart des livres, notamment dans celui de F. Giannesini et coll. (1985).

4.0 Le problème de la fiabilité humaine

Le seul problème apparent, mais il est de taille, avec les analyses par les méthodes actuelles de la fiabilité, c'est qu'on ne sait pas encore comment tenir compte de la fiabilité humaine dans ces analyses (Swain et Guttmann, 1983). Il s'agit là d'un problème fondamental, car ce que nous voulons vraiment c'est justement évaluer la fiabilité réelle d'un système personnes-machines, en tenant compte du comportement et des possibilités d'erreur de ses opérateurs, ou de ses usagers. Or, le plus souvent on se contente encore de nos jours de supposer que les opérateurs ou les usagers humains agissent comme des relais parfaits, en faisant exactement ce qu'ils sont supposés faire au bon moment (Henley et Kumamoto, 1981 et 1985; Swain et Guttmann, 1983; Leplat, 1985). Le problème est donc ainsi complètement évacué et on parle alors strictement de fiabilité technique. Dans les approches les plus récentes et les plus modernes, on tend à traiter les humains comme s'ils étaient des ensembles assez compliqués de relais dont on connaîtrait les probabilités de défaillance (Henley et Kumamoto, 1981 et 1985; Swain et Guttmann, 1983; Leplat, 1985). La tâche d'un opérateur, par exemple, sera décomposée en opérations élémentaires pour chacune desquelles on indiquera quelles sont les informations et les décisions à prendre. Alors, à partir

du réseau semi-ordonné des précédences de ces opérations, de ces prises d'information et de ces décisions, on tracera l'arbre des réussites et des échecs en attribuant à chaque prise d'information, à chaque décision et à chaque exécution d'une opération ou d'un groupe d'opérations élémentaires une certaine probabilité de réussite ou d'échec. Cette démarche peut paraître séduisante à première vue. Elle permet de combiner les données relatives au fonctionnement de la composante humaine à celles relatives au fonctionnement des installations ou du matériel technique et d'obtenir ainsi une évaluation de la fiabilité du système. En fait, cette démarche pose de sérieuses difficultés et présente des insuffisances graves (Leplat, 1985). Les principales proviennent :

- de la variabilité des procédures effectives;
- de l'instabilité du découpage en sous-tâches;
- des difficultés de l'évaluation de la probabilité des erreurs humaines.

La variabilité des procédures effectives

L'application des méthodes actuelles de fiabilité exige que le rôle de l'opérateur humain (ou de l'usager) dans le système soit très précisément défini, c'est-à-dire que la procédure d'exécution soit très clairement explicitée dans des instructions formelles. Le cas le plus typique est celui où l'opérateur dispose d'une liste de

contrôle qu'il a pour consigne de suivre très fidèlement. L'existence d'une procédure normalisée définie dans les consignes ne garantit pas que cette procédure soit suivie. Au contraire, souligne Leplat (1985), de nombreuses études du travail ont montré que la tâche prescrite ne coïncide que rarement avec celle qui est réellement exécutée par l'opérateur. De plus, selon les opérateurs ou les moments pour un même opérateur, les procédures permettant d'atteindre un même but peuvent différer : les opérations peuvent n'être pas faites dans le même ordre, ou avoir une structure différente, ou être différentes. Au niveau des décisions, en particulier, un même opérateur n'utilisera pas nécessairement les mêmes critères dans la même situation, ou ne leur accordera pas le même poids. Par ailleurs, on peut noter que même lorsque la procédure normalisée semble être suivie, les processus logiques de l'activité mentale en cause pour la prise d'une décision demeurent difficilement accessibles.

Les écarts entre les procédures sont favorisés par un certain nombre de facteurs. La qualification est l'un des plus importants : si des opérateurs sont peu qualifiés, ils devront se reposer plus fortement sur les instructions pour réaliser leur travail; par contre, s'ils sont qualifiés, ils auront tendance à avoir une activité orientée vers un but (Leplat, 1985). Leur démarche

variera alors en fonction de ce but et de leur connaissance, ainsi que de leur expérience, du dispositif. Les comportements dirigés par des buts sont moins prévisibles, mais ils ont l'avantage d'être adaptatifs et de pouvoir répondre à des cas non prévus dans les instructions. Ils font appel à une plus grande compétence. Ce sont par ailleurs ces comportements qui sont le plus vivement recherchés dans le contrôle des situations de crise. Ce sont eux aussi qu'on cherche à développer dans les nouvelles formes d'organisation du travail prônées par des mouvements tels celui de l'enrichissement du travail ou celui de la qualité de la vie en milieu de travail.

On peut aussi remarquer avec Leplat et Chenais (1985), que l'opérateur qualifié est susceptible de corriger ses erreurs, si bien que l'erreur commise n'aura pas alors de conséquences sur la sortie du système. Ce rôle autorégulateur de l'opérateur rend beaucoup plus difficile toute prédiction précise fondée sur une procédure stable. Il faut en effet estimer alors la probabilité que l'erreur passe inaperçue et, dans le cas contraire, la probabilité qu'elle soit corrigée à temps en inventant au besoin les modifications appropriées à la procédure effective. Les tentatives de correction n'étant pas toutes réussies et certaines conduisant parfois à une aggravation de la situation (Faverge, 1967), les erreurs de l'opérateur sont

donc reliées à une diminution de la fiabilité du système, du moins, pour les erreurs qui ont ou peuvent avoir des conséquences suffisamment importantes du point de vue de la sécurité.

Les écarts entre les procédures peuvent aussi s'expliquer par les aléas des processus de production, ainsi qu'aux imprévus de toute nature qui peuvent entacher normalement le design d'une procédure donnée. Une telle procédure est semblable à un programme informatique : tout paraît parfait sur le papier jusqu'au moment où on l'essaie dans la réalité; alors, toutes sortes d'imprévus et de fautes (les fautes de sémantique et de logique, notamment) se manifestent tout à coup. En informatique, on est amené lorsqu'on élabore un gros programme, à le diviser en modules qui seront testés séparément, puis on teste leur intégration. Les changements nécessaires sont souvent faits au fur et à mesure, de façon ad hoc, et sont rarement documentés; de telle sorte que le programme devient incompréhensible au point que si on désire plus tard le modifier, il sera vraisemblablement plus facile mais peut être trop coûteux de recommencer à partir du début. Au niveau des procédures de travail c'est la même chose : les changements nécessaires sont faits à un niveau local, au fur et à mesure des besoins et paraissent souvent trop peu importants pour qu'on se donne la peine de

les documenter; cependant, ils s'accumulent et souvent très rapidement au début de la vie d'un système. Cette dynamique explique sans doute une bonne partie de l'écart entre les procédures prescrites et effectives, même si d'autres facteurs importants y contribuent aussi notablement. En particulier, l'opérateur est capable de s'adapter et d'apprendre : il peut donc redéfinir une fonction ou une tâche qui lui est assignée et ceci, autre caractéristique importante, en fonction de buts multiples dont la pondération peut être variable et qui ne coïncident pas tous avec ceux du concepteur ou du pilote du système.

L'instabilité du découpage en sous-tâches

L'application des méthodes actuelles de fiabilité exige que les procédures à analyser soient découpées en tâches élémentaires. Ce qui présente plusieurs difficultés importantes :

- d'abord, pour une même procédure, ce découpage peut :
  - être plus ou moins fin;
  - correspondre plus ou moins bien à l'organisation mentale de l'activité;
- ensuite, des études expérimentales ont montré depuis longtemps (Ombredane et Faverge, 1954) que le temps d'exécution de la tâche globale ne peut être estimé par la somme des temps élémentaires. Ceci est

attribuable en particulier :

. au fait que les opérations élémentaires ne sont pas indépendantes, comme le suppose le modèle, et ce d'autant moins que l'opérateur est expérimenté;

. au fait que les conditions de travail sont loin d'être stables, contrairement à ce que suppose le modèle, en raison des aléas de la production tels les variations dans les taux de production, les défauts du matériel, les insuffisances de l'approvisionnement, etc. L'opérateur répond souvent à l'ensemble d'une situation plutôt qu'à des événements individuels ou à des états du système. L'être humain est très habile pour reconnaître des patterns complexes d'information et modéliser ses réponses en fonction d'une situation d'ensemble;

- enfin, le découpage mental de la tâche est variable du point de vue de l'opérateur, en fonction de son expérience et de son état de stress ou de fatigue. En effet, avec l'apprentissage et l'expérience, l'activité s'automatise tout en correspondant progressivement, du moins dans une première phase à un schéma de plus en plus large et complexe. Inversement, la fatigue et les situations de stress ou de surcharge induisent un retour à des schémas qui

seront d'autant plus élémentaires et morcelés que la fatigue, le stress ou la surcharge seront marquées (Leplat et Chenais, 1985; Fortin, 1983; Leplat et Cuny, 1974).

Les difficultés de l'évaluation de la probabilité des erreurs humaines

En admettant qu'on ait réussi à définir une procédure, il faudrait être capable de déterminer sa probabilité d'utilisation dans des conditions et par des opérateurs donnés; il faudrait surtout être capables de déterminer les probabilités de ses erreurs d'exécution puis, à partir de celles-ci, de ses probabilités de succès ou d'échec, et, dans ce dernier cas, la probabilité de succès de la procédure de récupération.

Or, d'après Leplat et Chenais (1985), il n'existe pas actuellement de moyens valables pour effectuer ces évaluations. Ils justifient ce jugement par le fait que les principaux moyens actuellement utilisés consistent à :

- utiliser les jugements indépendants d'experts à qui on a demandé leur estimation pour une même erreur, après leur avoir fait lire une description détaillée de la tâche comprenant :
  - . des instructions écrites
  - . des photographies des commandes, du tableau de

signalisation, des valves et autres éléments qui doivent être lus ou manipulés par le personnel. Ce qui est certainement très subjectif, très imprécis et, surtout, invérifiable;

- utiliser des estimations obtenues à partir de données existant dans des situations similaires, à supposer qu'elles n'aient pas été obtenues comme précédemment. Ce qui pose d'autres problèmes, en particulier celui des critères permettant de juger de la similitude des tâches, celui de la précision de ces critères et celui de leurs rapports et de leurs poids respectifs;
- utiliser, enfin, les résultats d'expériences psychologiques de laboratoire. Ce qui ne vaut certes pas mieux que les deux précédents moyens par suite de la simplification abusive habituelle des tâches effectuées en laboratoire par rapport aux tâches réelles, par suite des autres grandes différences entre les deux types de tâches (elles seront souvent loin d'être similaires) et par suite aussi du fait que ces expériences sont habituellement réalisées dans des conditions idéales très éloignées des conditions réelles d'opération des systèmes de production.

5.0 Les systèmes experts : nouveau paradigme en sécurité du travail?

En termes de risques, tel que signalé précédemment, il existe tellement de facteurs qui peuvent être impliqués dans les séquences ou les mécanismes déclencheurs des accidents, qu'il est essentiel, pour tout travail efficace de prévention, de présélectionner soigneusement les facteurs à considérer.

Cette présélection doit être réalisée principalement en fonction d'un cadre général d'interprétation ou, si on préfère, en fonction d'un modèle général de la causalité des accidents. Malheureusement, ainsi que nous l'avons souligné plus haut, un tel modèle est actuellement manquant. Son élaboration éventuelle ne saurait être guidée par le paradigme actuel du domaine, car ce dernier est inexistant. En effet, le domaine des accidents du travail est présentement en plein flottement : l'ensemble de ses archétypes correspond plus ou moins à l'ensemble de ses paradigmes successifs, mais il y en a aucun qui soit encore dominant et qui serve à réinterpréter les autres plus ou moins fortement. On sait seulement qu'ils sont inadéquats ou trop limités, mais on ne sait pas encore comment les intégrer ou quels archétypes ou quel paradigme

nouveaux adopter. Les paradigmes passés furent successivement :

- (avant 1925) l'accident, synonyme de hasard, de risque inhérent à un métier, une activité, une profession ou une industrie;

- (entre 1925 et 1945) l'accident, synonyme de prédisposition individuelle, qu'on peut donc prévenir par la sélection basée sur les méthodes de la psychométrie;

- (entre 1940 et 1950) l'accident, synonyme d'événement imprévu (mais non nécessairement imprévisible) causé par une chaîne ou un arbre d'événements ou de causes, et qu'on peut donc prévenir en agissant sur ces causes;

- (entre 1945 et 1960) l'accident, synonyme d'erreur humaine occasionnée par de mauvaises conditions de travail ou une mauvaise conception des équipements ou des tâches;

- (entre 1960 et 1970) l'accident, synonyme d'erreur humaine, qu'on peut prévenir à l'aide d'une meilleure sélection et d'une meilleure formation du personnel (retour aux méthodes de la psychométrie);

- (entre 1960 et 1975) l'accident, synonyme d'un défaut de fonctionnement d'un système, défaut qu'on peut étudier à l'aide des méthodes de la cybernétique;

- (entre 1975 et aujourd'hui) l'accident, synonyme d'un défaut de fonctionnement d'un système, défaut qu'on peut étudier à l'aide des méthodes de la fiabilité.

Au niveau de la recherche, un grand nombre de modèles et de méthodes ont été étudiés ou proposés dans ces divers contextes pour l'analyse des accidents (Fortin, 1983; Fortin et autres, 1983a, b, c, d). Toutes ces études ont permis de comprendre un peu mieux les différents mécanismes d'accident, mais elles ont introduit aussi beaucoup de bruit dans les connaissances, par suite principalement de problèmes de terminologie; même le terme accident est loin d'avoir une définition acceptée universellement. Chacune de ces études implique en général seulement un petit nombre de concepts ou de facteurs qui ont la mauvaise habitude de différer d'une étude à l'autre. De nombreuses autres différences, souvent mal explicitées, existent entre ces études au niveau des orientations ou des hypothèses sous-jacentes, tant explicites qu'implicites. La valeur d'un nombre considérable d'observations et de découvertes empiriques ne repose

souvent que sur la validité mal éprouvée d'une série de propositions théoriques mal reliées (concept d'accident, concept d'erreur humaine, dynamique des éléments du système, concept de risque, critères de risque, biais des données statistiques, stratégies en prévention, etc.) (Fortin, 1983). Malgré ces difficultés, on pourrait songer à construire un modèle général suffisamment exhaustif en rassemblant un certain nombre de ces études et en tentant de les intégrer. En fait, nous avons déjà réalisé un tel effort (Fortin, 1983; Fortin et al., 1983a, b, c, d; Gilbert et al., 1982). Nous étions ainsi parvenu à un modèle comprenant plusieurs milliers de variables et plusieurs centaines de relations entre ces variables. Par "variables" nous entendions les divers facteurs relatifs à la sécurité, aux moyens techniques, aux équipements, aux méthodologies, au design, aux caractéristiques humaines, ainsi que les caractéristiques de ces facteurs et les informations de diverses natures nécessaires pour comprendre les accidents, car ils sont tous susceptibles en effet de varier au cours du temps ou d'un système de production à un autre. Cet ensemble de variables a de plus été muni des diverses structures suivantes :

- une structure hiérarchisée d'agrégation comprenant plusieurs niveaux du point de vue du système (système, atelier, activité, composantes; groupe, équipe,

opérateur; tâches; équipements et matériel, machines, produits; environnements; etc.) et en termes de catégories de variables (nous faisons alors appel à la terminologie suivante : super variables, variables, sous-variables, indicateurs);

- un découpage par blocs fonctionnels représentant les composantes d'un système "personnes-machines";
- une typologie des défaillances d'un système "personnes-machines" en fonction de leur origine;
- une structure en forme de réseau suggérant des relations d'influence ou causales, non nécessairement déterministes, entre les divers facteurs;
- un sous-modèle (modèle de poste) ayant comme centre un opérateur.

Naturellement, d'autres chercheurs avant nous avaient entrepris une telle démarche. Mais ils ont abandonné en cours de route devant la complexité et surtout l'apparente inapplicabilité du modèle éventuel (Maurice De Montmollin, communication personnelle, 1982). Ce dernier paraissait d'ailleurs inapplicable à juste titre, car on pensait alors en termes de fonction de transfert. La complexité du modèle paraissait aussi être un défaut

important, ne serait-ce qu'à cause du nombre de variables et d'interrelations considérées, par suite des moyens informatiques très lourds que cela aurait exigé à l'époque.

Aujourd'hui, une telle complexité ne nous apparaît plus comme un obstacle, mais comme une nécessité en matière de prévention. Par ailleurs, si on pense en termes de faits et de règles (plutôt qu'en termes de fonctions de transfert), un modèle comme celui que nous avons développé pourrait présenter sous la forme d'un système-expert de très intéressantes et très avantageuses possibilités d'application.

L'un des avantages les plus grands consisterait probablement à pouvoir mieux étudier et prédire le comportement d'un opérateur en fonction de son niveau de connaissances. En effet, un système expert peut en principe utiliser les mêmes connaissances, les mêmes règles que l'opérateur et fonctionner comme lui en étant dirigé par des buts ou des sous-buts. Un tel système peut ou pourrait copier plus ou moins bien le comportement d'un opérateur. Il suffirait pour cela de donner au système les règles qui relient les variables spécifiques du cas ou du système à l'étude à notre concept de variables communes, ainsi que les règles qui lui permettent d'interroger convenablement l'utilisateur à ce sujet. En effet, pour l'application à

des cas concrets, il faudra toujours traiter de variables et de règles spécifiques. Cependant ces variables pourront généralement être considérées comme des cas particuliers (des instantiations) de nos variables générales ou communes. En conséquence, un tel système pourra, comme l'opérateur, entreprendre une séquence d'opérations avant de se rendre compte qu'elle est mauvaise. En donnant au système un certain nombre de problèmes à résoudre (perturbations ou pannes de système à régler), on pourrait même repérer un certain nombre de bons et de mauvais comportements et, après analyse, modifier en conséquence le système, ou les instructions aux opérateurs ou les deux. Ce qui constituerait une utilisation des plus intéressante, à des fins préventives, d'un tel système.

Nous pensons donc que l'approche par les systèmes experts présenterait, pour le domaine de la sécurité du travail, en plus des grandes sources d'intérêt déjà mentionnées au chapitre 1, un intérêt bien particulier et fondamental : celui de lui fournir un nouveau paradigme. Ce dernier serait alors capable à notre avis d'intégrer tous les précédents et il serait en outre suffisamment fertile et évolutif pour constituer un outil durable et fondamental de recherche appliquée.

6.0 Exemples de divers problèmes en fiabilité technique

6.1 Généralités

Un système à n composantes peut être représenté par un réseau à n noeuds, où les arcs représentent les circuits possibles entre les n composantes du système. Une telle représentation sera souvent suffisante pour nous permettre d'évaluer plus ou moins directement la fiabilité d'un système, ainsi que nous le montrons à l'aide des prochains exemples. Cette représentation sera également utile même dans les cas les plus complexes, ne serait-ce que comme guide nous permettant de nous poser (ou de nous faire poser par un système expert) les questions pertinentes à la réalisation des cinq premières étapes de l'analyse par les arbres de défaillance. Ensuite, selon la complexité du problème considéré, le système pourra construire l'arbre de défaillance plus ou moins automatiquement ou aider l'usager à le faire.

6.2 Structures et fonctions de structure

6.2.1 Définitions

Un réseau composé de n noeuds sera appelé une structure d'ordre n où les noeuds seront appelés composantes de la structure.

À un tel réseau, on associera un vecteur d'état ayant autant de composantes qu'il y en a dans le système. Chacune pourra prendre la valeur 1 ou la valeur 0, selon que la composante correspondante dans le système fonctionne bien ou non. Il y aura donc 2^n vecteurs d'état possibles pour un système à n composantes. Le nombre de composantes en opération à un instant donné sera alors obtenu par la somme des composantes du vecteur d'état à cet instant. Certains de ces vecteurs représenteront le fait que notre structure fonctionne bien, et les autres le fait qu'elle ne fonctionne pas bien.

Pour chaque structure d'ordre n, on peut associer une fonction binaire Q(X(t)) qu'on appelle la fonction de structure, telle que :

$$Q(X(t)) = \begin{cases} 1, & \text{si } X(t) \text{ est un état de bon fonctionnement} \\ 0, & \text{autrement} \end{cases}$$

Alors, puisque R(t) est égale par définition à la probabilité que Q(X(t)) = 1, on aura que :

$$E[Q(X(t))] = R(t)$$

où E est l'opérateur espérance mathématique

R(t) est la fiabilité de notre structure.

On appellera structure (k,n) tout réseau d'ordre n tel :

- qu'il est en état de bon fonctionnement pour tout vecteur d'état comprenant au moins k composantes en bon état de fonctionnement :

$$\sum_{i=1}^{n} x_i \geqslant k$$

- qu'il est en état de mauvais fonctionnement dans le cas contraire :

$$\sum_{i=1}^{n} x_i < k$$

L'intérêt des systèmes d'ordre (k,n) est double :

a) de nombreux systèmes peuvent être ramenés ou décomposés en sous-systèmes de type (k,n).

b) la fiabilité d'un système quelconque à n composantes indépendantes et identiquement distribuées a une limite supérieure donnée par un système (k,n) où k=L, le plus petit nombre de composantes pour lequel le système fonctionne.

6.2.2 Problèmes simples

- **Structure série**

Une structure série est une structure (k,n) avec k=n. Sa fonction de structure est telle que :

$Q(X(t)) = 1$, si $x_i(t) = 1$, $i=1,\ldots,n$.

Elle peut donc être représenté par :

$$Q(X(t)) = \prod_{i=1}^{n} x_i(t)$$

Par conséquent, $R_s(t)$, la fiabilité de cette structure sera donnée par :

$$R(t) = E[\prod_{i=1}^{n} x_i(t)] = \prod_{i=1}^{n} E(x_i(t))$$

$$R(t) = \prod_{i=1}^{n} R_i(t)$$

où $R_i(t)$ est la fiabilité de la ième composante.

- **Structure parallèle**

Une structure parallèle est une structure (k,n) avec k=1. Sa fonction de structure est telle que :

$Q(X(t)) = 0$ ssi $x_i(t) = 0$, $i=1,\ldots,n$

Elle peut donc être représentée par :

$$Q(X(t)) = 1 - \prod_{i=1}^{n} (1 - x_i(t)$$

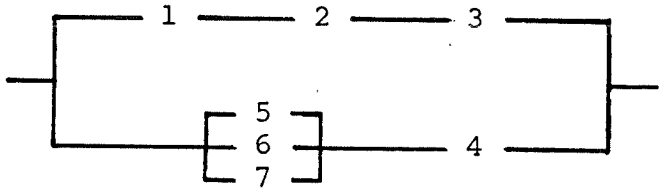
et :

$$R(t) = 1 - \prod_{i=1}^{n} (1 - E(x_i(t)))$$

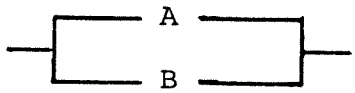
$$= 1 - \prod_{i=1}^{n} (1 - R_i(t))$$

- **Structure décomposable**

Soit la structure suivante :



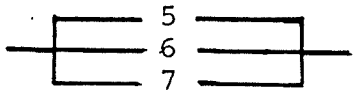
On peut la décomposer d'abord en deux branches en parallèle dont chacune peut être considérée comme un système série :



A = 1 — 2 — 3

B = C — 4

et où la branche inférieure est constituée d'un sous-système parallèle en série avec une composante :

C = 

Pour trouver la fonction de structure du réseau initial, il suffit d'appliquer systématiquement les règles pour les systèmes séries et les systèmes parallèles :

a) $Q[X(t)] = 1 - (1-Q_A(X_A(t)))(1-Q_B(X_B(t)))$

b) $Q_A(X_A(t)) = \prod_{i=1}^{n} x_i(t)$

c) $Q_B(X_B(t)) = x_t(t)\ Q_C(X_C(t))$

d) $Q_C(X_C(t)) = 1 - \prod_{i=5}^{7} (1-x_i(t))$

d'où, par remplacement :

$$Q(X(t)) = 1 - (1- \prod_{i=1}^{3} x_i(t))\ (1-x_t(t)(1- \prod_{i=5}^{7} (1-x_i(t))))$$

- **Traitement de ces problèmes dans un système expert**

Le traitement le plus simple consisterait à déclarer la nature des sous-systèmes (série, parallèle ou composite) et à indiquer la liste de ses éléments, chacun d'eux étant associé à une probabilité ou à une fonction de probabilité, exactement comme nous l'avons fait plus haut.

Par exemple :

SYSTÈME'1 → Parallèle (AA.BB.nil);

SSYST (AA) → Série (C1.C2.C3.nil);

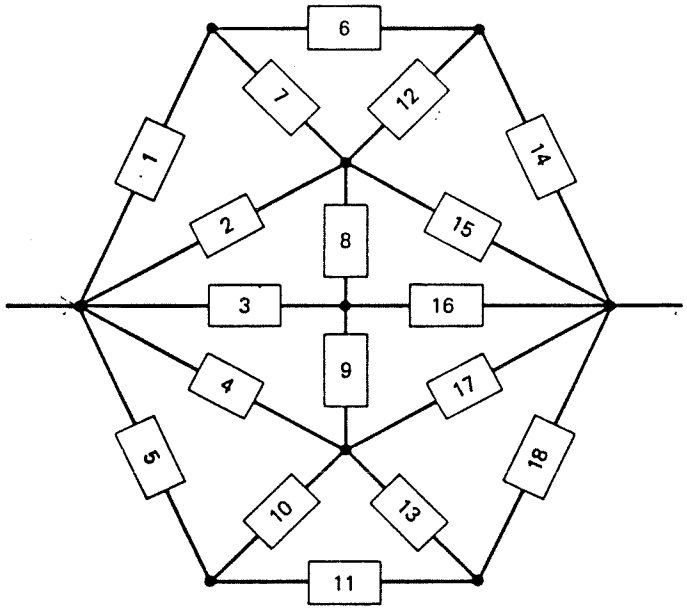
SSYST (BB) → Série (CC.C4.nil);

SSYST (CC) → Parallèle (C5.C6.C7.nil);

Il suffirait alors que le système contienne les règles qui associent les systèmes série et parallèle à leurs fonctions de structure, ainsi que la procédure de remplacement et celle de distribution de l'espérance mathématique quand les pannes des composantes sont indépendantes. On pourrait envisager aussi de donner au système les règles qui lui permettraient d'effectuer lui-même les décompositions nécessaires. Il suffirait alors de lui donner la liste des composantes et leurs relations de connexité.

6.3 Problèmes plus compliqués

Certains graphes ne peuvent être décomposés en sous-graphes de systèmes d'ordre (k,n). Par exemple, on pourrait fort bien avoir un graphe ayant l'allure suivante :



Dans ce diagramme, chaque ligne est en fait un arc double. La suite 3, 9, 17 est un chemin, de même que la suite 4, 9, 16. On aura aussi remarqué que, pour traiter les points d'intersection des sentiers, on devra soit ajouter des sommets intermédiaires (composantes fictives de fiabilité 1), soit des sentiers élémentaires (règles).

Pour traiter un tel problème, on peut envisager plusieurs méthodes.

1ère méthode : Analyse des vecteurs d'état

La première méthode est peut-être la plus simple. Elle consiste à :

- Générer la liste de tous les cas possibles à partir du fait que chaque composante peut être soit en état de bon fonctionnement soit en état de mal fonctionnement ("panne").

- Trier cette liste en deux sous-listes dont l'une correspond aux cas où le système est en état de bon fonctionnement et l'autre où le système est en état de mal fonctionnement (en "panne"). Évaluer au préalable chaque cas.

- Évaluer les probabilités de chaque cas d'au moins une sous-liste.

- Pour évaluer la fiabilité du système, additionner les probabilités de la liste des cas pour lesquels le système est en état de bon fonctionnement.

- Pour évaluer l'infiabilité, faire de même sur l'autre liste, ou retrancher la valeur précédente de 1.

La méthode la plus pratique pour réaliser ce programme utilisera le vecteur d'état associé au système.

Pour savoir si un vecteur particulier correspond à une panne ou non, il suffit de vérifier s'il existe ou non un chemin de la source au puit, passant uniquement par des composantes en état de bon fonctionnement.

Le programme PROLOG pour faire ce travail pourrait sans doute être assez simple. Il suffirait, par exemple :

. de caractériser d'abord chaque composante du système par trois variables :
  - une pour le numéro d'identification
  - une pour la probabilité de bon fonctionnement
  - une pour repérer l'état

. d'écrire les instructions pour l'exécution des étapes mentionnées précédemment. Intégrer en particulier dans ces instructions, un programme de recherche d'un chemin sans boucle entre la source et le puit.

Cependant, on voit bien que cette méthode exige de longs temps de calcul et beaucoup mémoire. En particulier, elle exige qu'on génère et qu'on évalue tous les événements possibles, même lorsqu'on ne s'intéresse qu'à l'une des sous-listes. Déjà, pour un système à 20 composantes, il faut évaluer plus de 10^6 vecteurs d'état.

De plus, si on examine de près ce qui se passe, on verra que de nombreux vecteurs d'état ont en commun un ou plusieurs chemins, dans le cas de la sous-liste des bons fonctionnements, et une ou plusieurs coupes dans le cas de la sous-liste des pannes du système.

Dans un système donné ou dans un arbre de défaillance donné, un ensemble de coupe est un ensemble d'événements élémentaires (feuilles) tels que s'ils se réalisent tous, alors l'événement au sommet de l'arbre (la panne) est certain. L'ensemble est minimal si le sommet de l'arbre ne se réalise pas quand n'importe quel événement de l'ensemble ne se réalise pas.

Dans les arbres de défaillance, les relations entre les composantes peuvent être très complexes et être fonction notamment de leurs états et de l'état du système. Ainsi, les effets d'une panne particulière peuvent être bloqués par la panne d'une certaine composante et, au contraire, transmis et même amplifiés par le fonctionnement normal de cette même composante.

Cependant, dans le cas de notre exemple, un événement d'un ensemble de coupe sera nécessairement une panne

d'une composante. Par exemple, si on désigne par $\overline{i}$, i=1, ...,18, la panne de la ième composante, alors :

$$E = [\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\ ]$$

sera un ensemble de coupe minimal.

Une notion duale de la notion de coupe est la notion de chemin. Dans un arbre de défaillance, un chemin est un ensemble d'événements élémentaires (feuilles) tels que s'ils se réalisent tous, alors l'événement au sommet de l'arbre (la panne) ne se réalise pas. Le chemin est minimal si l'événement au sommet de l'arbre se réalise quand n'importe quel événement du chemin ne se réalise pas.

Ces notions sont intéressantes car on peut montrer que si toutes les coupes minimales ne se réalisent pas (Henley et Kumamoto, 1981), alors aucune autre coupe ne se réalise. On peut aussi montrer que tout chemin est constitué d'au moins un chemin minimal. Il n'est donc pas nécessaire, en particulier à des fins de prévention, d'examiner tous les cas possibles.

On peut donc envisager d'utiliser plutôt l'une des deux méthodes suivantes.

2ième méthode : Recherche des chemins minimaux

Cette méthode consistera simplement à :

- Faire la liste de tous les chemins sans boucle menant de la source au puit.
- Calculer, pour chacun de ces chemins, la probabilité que le système fonctionne par le biais de ce seul chemin.
- Calculer la probabilité que le système fonctionne par le biais d'au moins un chemin.

Pour que dans la liste des chemins il n'y ait que des chemins minimaux, il n'est pas nécessaire d'effectuer un tri. Il suffit de définir un chemin sans boucle comme un chemin où aucun sommet (plutôt qu'aucun arc) ne figure plus d'une fois.

On voit que cette méthode exige moins d'espace mémoire que la précédente. Elle permet de générer rapidement la liste des chemins minimaux. Il est également facile de générer à partir de ceux-ci la liste des coupes minimales. Il suffit, en effet, qu'au moins un événement sur chaque chemin ne se réalise pas pour que chaque ensemble de ces non réalisations soit un ensemble de coupe. Il suffira donc de :

- prendre la liste des chemins minimaux ordonnés par ordre croissant de longueur
- prendre le complément du premier événement du premier chemin
- prendre le complément d'un autre événement sur le chemin suivant où ne figurent ni le premier événement ni aucun des événements complémentés par la suite en réitérant la présente étape. N'utiliser que des événements associés aux sommets du graphe dont le numéro de précédence est plus grand que ceux des sommets associés aux événements déjà complémentés. Si on atteint le dernier chemin, alors la liste des événements complémentés est une coupe à mettre dans la liste des coupes.
- recommencer les étapes précédentes avec l'événement suivant du premier chemin.
- recommencer successivement avec les chemins suivants.
- ordonner les coupes par ordre croissant de longueur.
- enlever les coupes qui en contiennent au moins une autre. Si deux coupes sont identiques, en garder une et enlever l'autre.

- garder le résultat : c'est l'ensemble des coupes minimales.

Si on compare cette deuxième méthode à la première, il n'est pas du tout certain que les temps de calcul seront moins longs lorsqu'il s'agira d'évaluer la fiabilité ou l'infiabilité du système : ceci, parce que, dans l'arbre de défaillance équivalent, on n'aura plus au sommet de l'arbre un "ou exclusif" où un seul événement est possible à la fois, mais un "ou inclusif." Les calculs seront donc beaucoup plus complexes. Il faudra soit utiliser intensivement le théorème de Bayes, soit construire la fonction de structure et l'utiliser correctement (voir 4ième méthode).

Bref, cette seconde méthode est meilleure que la première s'il s'agit d'analyser qualitativement des systèmes et de construire leurs arbres de défaillance. Elle n'est pas plus efficace par contre s'il s'agit d'évaluer quantitativement la fiabilité d'un système.

On peut ici remarquer que l'intérêt de cette méthode réside en partie en ce que, fréquemment, les défaillances d'un système donné originent du fait que les événements d'un ensemble de coupe peuvent avoir une cause commune.

Dans l'industrie américaine des réacteurs de puissance, par exemple, on a trouvé dans une analyse portant sur 379 pannes que 78 avaient été occasionnées par la réalisation d'un ensemble de coupe de mode commun (Henley et Kumamoto, 1981). Il est donc important d'identifier de telles coupes.

Or, on peut supposer que ceci pourrait être fait aisément en PROLOG. Il suffirait d'ajouter les règles correspondantes aux pannes de mode commun et puis de vérifier pour chaque ensemble de coupe s'il peut être réalisé par une cause commune (ou par plusieurs en coïncidence). On pourrait dans certains cas se contenter de lister de tels ensembles de coupe dans les règles si on en a repérés d'une manière ou d'une autre.

3ième méthode : Recherche des coupes minimales

Cette troisième méthode est duale de la deuxième. Au lieu de rechercher l'ensemble des chemins minimaux, on recherche les ensembles de coupe minimaux. On a déjà expliqué plus haut son intérêt pour la prévention.

Cette méthode n'est pas utilisable directement sur un graphe, à moins qu'il ne s'agisse d'un arbre.

Néanmoins elle peut être utilisée en même temps que la première méthode afin d'épargner de l'espace mémoire. En effet, il n'est pas nécessaire de conserver les vecteurs d'état qu'on génère pour évaluer la fiabilité d'un système. Il suffit d'évaluer la probabilité de chacun au fur et à mesure qu'on les génère et de sommer ces probabilités selon qu'elles correspondent à de la fiabilité ou à de l'infiabilité. On peut donc se contenter de ne garder pour fins d'analyses ultérieures que les vecteurs d'état qui correspondent à des coupes minimales. Il suffit de comparer chaque nouveau vecteur avec ceux qu'on a déjà pour décider s'il représente ou non une coupe minimale. Si l'ensemble des zéros de l'un des anciens vecteurs est contenu dans celui du nouveau, alors ce dernier n'est pas minimal et on le laisse tomber. Sinon on le conserve et on examine si, au contraire, l'ensemble de ses zéros n'est pas contenu dans celui de chacun des anciens. On laissera alors tomber chacun des anciens vecteurs pour lequel l'examen sera positif et on gardera les autres.

4ième méthode : Recherche et utilisation de la fonction de structure

Pour calculer la fiabilité d'un système, après avoir trouvé l'ensemble de ses chemins minimaux, on peut utiliser la fonction de structure de l'arbre résultant :

$$R_S = E[Z(Y)] = \bigvee_{j=1}^{n} \left[\bigwedge_{i=1}^{n_j} Y_{i,j} \right]$$

où n est le nombre de chemins minimaux

n_j est le nombre de composantes sur le jième chemin

$Y_{i,j}$ est une variable binaire prenant la valeur 1 quand la ième composante sur le jième chemin est en état de bon fonctionnement et 0 sinon.

Il faut remarquer qu'en général plusieurs événements élémentaires figureront sur plus d'un chemin. En conséquence, même si ces événements sont indépendants, on aura que :

$$E\,[Z(Y)] = E\left[1 - \prod_{j=1}^{n} \left(1 - \prod_{i=1}^{n_j} Y_{i,j}\right)\right]$$

$$E\,[Z(Y)] \neq 1 - \prod_{j=1}^{n} \left[1 - E\left[\prod_{i=1}^{n_j} Y_{i,j}\right]\right]$$

Pour calculer E[Z(Y)] il sera donc nécessaire de faire l'expansion de Z(Y), puis de simplifier le résultat à l'aide de la loi d'absorption, avant de distribuer l'opérateur d'espérance. On peut éviter ce long processus en utilisant la méthode de décomposition partielle à pivot.

La fonction de structure Z(Y) peut être réécrite sous la forme :

$$Z(Y) = Y_i\, Z(1_i,Y) + (1-Y_i)\, Z(0_i,Y)$$

où $Z(1_i,Y)$ et $Z(0_i,Y)$ sont des fonctions binaires obtenues en forçant la ième variable indicatrice à, respectivement, un ou zéro. On pivote ces fonctions binaires d'une variable indicatrice à l'autre jusqu'à ce que les fonctions binaires résultantes ne contiennent plus que des facteurs indépendants. L'E[Z(Y)] peut alors être calculée facilement.

Exemple :

$$\begin{aligned} Z(Y) &= (Y_1+Y_2-Y_1Y_2)(Y_2+Y_3-Y_2Y_3)(Y_3+Y_1-Y_3Y_1) \\ &= Y_1Z(1_1,Y)+(1-Y_1)Z(0_1,Y) \\ &= Y_1(Y_2+Y_3-Y_2Y_3)+(1-Y_1)Y_2(Y_2+Y_3-Y_2Y_3)Y_3 \end{aligned}$$

Le premier terme est constitué de facteurs indépendants mais pas le second. On effectue donc une autre transformation mais seulement sur ce second terme :

$$\begin{aligned} Z(Y) &= Y_1Z(1_1,Y)+(1-Y_1)Y_2Z(0_1,1_2,Y) \\ &\quad +(1-Y_1)(1-Y_2)Z(0_1,0_2,Y) \\ &= Y_1(Y_2+Y_3-Y_2Y_3)+(1-Y_1)Y_2Y_3+(1-Y_1)(1-Y_2).0 \\ &= Y_1(Y_2+Y_3-Y_2Y_3)+(1-Y_1)Y_2Y_3 \end{aligned}$$

D'où :

$$E[Z(Y)] = E[Y_1](E[Y_2]+E[Y_3]-E[Y_2]E[Y_3]) + (1-E[Y_1])E[Y_2]E[Y_3]$$

en supposant les événements élémentaires statistiquement indépendants.

Autres méthodes

De nombreuses autres méthodes peuvent sans doute être envisagées. Lorsque les temps de calcul deviennent trop longs, par exemple, il faut recourir à des méthodes fournissant plutôt des bornes inférieures et supérieures pour la fiabilité (ou l'infiabilité) d'un système. On peut aussi, au lieu de générer tous les vecteurs d'état, n'en générer qu'un échantillon représentatif à partir de la méthode de Monte Carlo.

Une méthode, en particulier, apparaît intéressante. Elle consiste à construire à partir de la liste des vecteurs d'état (ou d'un échantillon représentatif) le graphe des transitions entre ces vecteurs. À chaque arc on associe le logarithme, multiplié par moins un, de la probabilité de transition. On peut alors appliquer un algorithme des plus courts chemins pour obtenir successivement toutes les défaillances du système, par ordre de probabilité décroissante. On peut alors arrêter l'énumération

à partir d'un seuil, fixé à l'avance, en dessous duquel les probabilités individuelles ou l'ensemble des probabilités restantes n'est plus considéré comme significatifs.

6.4 Problèmes encore plus compliqués

Dans de nombreux systèmes, les relations entre les diverses composantes peuvent être nombreuses, complexes et sujettes à de nombreuses conditions, relatives notamment à l'état du système, aux états d'autres composantes, aux conditions physiques et chimiques présentes, à l'ordre des séquencements des événements en cours, à l'évolution du système, et ainsi de suite. Le graphe des relations entre les composantes ne peut plus servir à représenter réellement toutes ces relations, sous peine de devenir incompréhensible, voire ingérable. Il faudra donc se contenter d'un schéma très simplifié mais utilisable comme guide dans l'exploration de ces relations. Ces dernières pourront certainement être représentées alors sous la forme de règles PROLOG. On pourra ainsi vraisemblablement utiliser les mêmes méthodes que pour les cas précédents. Ce qui présente un intérêt certain, dans la mesure où ces règles pourront accepter facilement plus de deux états (bon ou mauvais) par composante. On pourra avoir toute une gradation d'états entre le bon et le mauvais fonctionnement. De plus, à l'aide de règles adéquates, il ne

devrait pas être difficile de traiter les cas où des événements s'excluent mutuellement l'un l'autre. Enfin, tel qu'expliqué précédemment, il sera nécessaire dans les cas les plus compliqués de construire finalement l'arbre de défaillance du système étudié.

7.0 Conclusion

Le développement d'un système expert en santé et sécurité du travail présente pour ce domaine, pour les domaines connexes et pour celui des systèmes experts un intérêt majeur. Le développement d'un tel système devra débuter par le domaine de la sécurité, plutôt que par celui de la santé : ce sera plus difficile ainsi, mais les retombées positives seront bien plus nombreuses et considérables. En effet, si on commence par le domaine de la santé, on pourra vraisemblablement se contenter d'adapter aux maladies du travail un système existant actuellement pour un autre type de maladie; mais, un tel système ne pourra que contribuer très peu à la problématique des accidents du travail ou des accidents en général. Une telle adaptation permettrait sans doute d'améliorer l'efficacité de la prévention et du diagnostic des maladies du travail, mais elle n'est certainement pas très apte à générer la plupart des retombées positives que nous avons mentionnées précédemment.

Le domaine de la sécurité du travail est cependant encore beaucoup trop vaste. Il faudra donc circonscrire beaucoup plus précisément le domaine d'intérêt initial. Tel que suggéré dans le corps du texte, on pourrait se

concentrer, par exemple, sur les mécanismes de la survenue de l'erreur humaine, en liaison avec les caractéristiques des interfaces entre l'opérateur et sa machine ou ses coéquipiers, ainsi qu'avec les caractéristiques de sa tâche, notamment la structure générale et variable de celle-ci. Ce dernier problème est cependant très difficile, et il conviendrait de l'aborder plutôt dans la seconde ou la troisième étape du développement du système envisagé. Pour être plus réaliste, la première étape pourrait consister à construire un système d'aide à la conception ou à l'analyse de la conception des équipements ou des postes de travail : adaptation anthropométrique, articulaire et biomécanique des postes, respect des stéréotypes, disposition et aménagement des postes de travail et autres éléments de base. La seconde étape, qui pourrait être réalisée en parallèle avec la première, consisterait à élaborer un système d'aide à l'analyse des risques ou des accidents s'inspirant des techniques de l'analyse qualitative par les arbres de défaillance, mais restreint au niveau du poste de travail, ou restreint à un certain type de poste de travail dans une industrie donnée. On serait prêt alors pour la troisième étape et pour les étapes suivantes. Ces dernières auraient évidemment pour objectifs :

- d'élargir la base de règles et de faits;
- d'élargir, plus spécialement, l'ensemble des sous-domaines couverts;
- d'offrir des possibilités d'assistance intelligente dans la recherche de données pertinentes, notamment dans les banques de données informatisées;
- de fournir la possibilité de mise à jour automatique des données;
- de fournir une aide à l'adaptation du système aux besoins spécifiques d'un secteur industriel donné, voire d'une entreprise particulière;
- de créer une interface la plus naturelle possible entre le système et les divers usagers visés.

Quant à la validation du système comme tel, au fur et à mesure de son élaboration, nous pourrions appliquer la stratégie suivante, stratégie que nous avions déjà proposée (Fortin, 1983; Fortin et collaborateurs, 1983a, b, c, d) à la suite de Gilbert (1974, 1975), pour la validation de notre modèle général (Fortin, 1983; Fortin et coll., 1983a, b, c, d), et qui permettrait, par l'étude d'accidents et de postes de travail, d'arriver à un degré de validation raisonnable.

Bibliographie

1. AUTEURS DIVERS. Accidents et sécurité du travail. Préface de Jacques Leplat, Collection du Travail Humain, les Éditions Presses Universitaires de France, Paris 1972, 287 pages.

2. BRID, Frank E. Le guide du contrôle des pertes à l'intention de la direction. Institute Press, Atlanta, Georgia, 1974. Traduit de l'anglais par l'Association de prévention des accidents industriels du Québec.

3. BONNET, Alain. L'intelligence artificielle, Promesses et réalités. Inter Éditions, 1983.

4. BROWNSTON, Lee, Robert FARRELL, Elaine KANT et Nancy MARTIN. Programming Expert Systems in OPS5 : An Introduction to Rule-Based Programming. Addison Wesley Publishing Company, 1985.

5. CAZAMIAN, Pierre. Leçons d'ergonomie industrielle, Une approche globale. Éditions Cujas, 1974, Paris, 158 pages.

6. CAZAMIAN, P., Y. CHICH, G. DEVEZE et F. FAVRE. Approche scientifique de la sécurité du travail (son ambiguïté, ses fausses routes, ses espoirs). Dans Accidents et sécurité du travail, 1972, p. 38 et suivantes.

7. CHARNIAK, Eugène et Drew Mc PERMOTT. Introduction to Artificial Intelligence. Addison Wesley, 1985.

8. CUNY, Xavier et G. GRAWSKY. Pratique de l'analyse d'accidents du travail dans la perspective socio-technique de l'ergonomie des systèmes. Accidents et sécurité du travail, p. 46 et suivantes.

9. DE COCK, Dr. Gaston. Une nouvelle approche dans la prévention des accidents. Les Presses de l'Université de Louvain, Bruxelles, 1964.

10. DE MONTMOLLIN, Maurice. Les systèmes hommes-machines. PUF, 1967, 252 pages.

11. DE MONTMOLLIN, Maurice. 1981. Communication personnelle.

12. DUBOIS, Didier et Henri PRADE. Théorie des possibilités. Applications à la représentation des connaissances en informatique, Éditions Masson, Collection Méthode et Programmes, 1985.

13. FAVERGE, Jean-Marie. Psychosociologie des accidents du travail. Les Éditions des Presses Universitaires de France, Collection SUP, 1967, 160 pages.

14. FIESCHI, Marius. Intelligence artificielle en médecine. Des systèmes experts, Éditions Masson, Collection Méthode et Programmes, 1984.

15. FITTS, Paul M. et R.E. JONES. Analysis of factors contributing to 460 "Pilot Error" Experiences in Operation Aircraft Controls. Memorandum. Report TSEAA-694-12 Aero Medical Laboratory. Air Material Commande, Wright-Patterson Air Force Base, Dayton, Ohio, July 1, in H.W. Sinaiko (1961).

16. FITTS, Paul M. et R.E. JONES. Psychological Aspects of Instrument Display I : Analysis of 270 "Pilot Error" Experiences in reading and interpreting Aircraft Instruments. Memorandum Report TSEAA-694-12A, Aero Medical Laboratory, Air Material Command, Wright-Patterson Air Force Base, Dayton, Ohio, October 1, 1947 in H.W. Sinaiko (1961).

17. FORTIN, C. La causalité des accidents. Mémoire de maîtrise, Département de génie industriel, École Polytechnique de Montréal, Montréal, août 1983, 547 pages.

18. FORTIN, C., R. GILBERT et J.C. WARMOES. Typologie des causes d'accidents. (Listes et interelations). Rapport technique numéro EP 83-R.27, École Polytechnique de Montréal, Montréal, 1983, 483 pages.

19. FORTIN, C., R. GILBERT et J.C. WARMOES. Revue des modèles concernant les systèmes H-Ms et la sécurité. Rapport technique numéro EP 83-R.28, École Polytechnique de Montréal, Montréal, 1983a, 286 pages.

20. FORTIN, C., R. GILBERT et J.C. WARMOES. Schéma des interelations entre les diverses variables impliquées dans les accidents. Rapport technique numéro EP 83-R.29, École Polytechnique de Montréal, Montréal, 1983c, 18 plans.

21. FORTIN, C., J.C. WARMOES et R. GILBERT. Mathématiques applicables à l'analyse de la causalité des accidents. Rapport technique numéro EP 83-R.26, École Polytechnique de Montréal, Montréal, 1983d, 150 pages.

22. GILBERT, R. Les fondements de l'ergonomie. Colloque organisé par le Comité associé du Conseil national de recherche du Canada pour l'application industrielle des recherches en ergonomie. 22 février 1985, Hôtel Méridien, Montréal, 14 pages.

23. GASCUEL, Olivier. Un système expert dans le domaine médical. Thèse de 3ième cycle. Institut de programmation, Université Pierre et Marie Curie. Centre National de la Recherche Scientifique, 1981.

24. GILBERT, R., D. MUKHEDKAR, C. FORTIN et J.C. WARMOES. Logistics of Accident Causes and Prevention. École Polytechnique de Montréal, National Scientific and Technical Conference on Electrical Safety, 1982, Bulgary.

25. GILBERT, R., D. MUKHEDKAR, C. FORTIN et J.C. WARMOES. École Polytechnique de Montréal. Interactive Computer Approach to Accident Analysis suitable for Field Application. National Scientific and technical conference on Electrical Safety, 1982, Bulgary.

26. GILBERT, R., D. MUKHEDKAR, J.C. WARMOES, C. FORTIN et G. TOULOUSE. École Polytechnique de Montréal. The state of the art and future developements in accident research and risk evaluation. "Human factors and New Technology", 15th Annual HFAC Conference, Toronto, Ontario, Canada, 1982.

27. GILBERT, R., B. VO-NGOC et P. ROHAN. Une nouvelle approche en recherche sur les accidents. Rapport, Université du Québec, (IRNS), 1975, 46 pages.

28. GILBERT, R., B. VO-NGOC et P. ROHAN. Les accidents vus du dedans. Rapport pour l'O.C.Q. Université du Québec, (IRNS), 1976, 26 pages.

29. HENLEY, Ernest J. et Hiromitsy KUMAMOTO. Reliability Engineering and Risk Assessment. Prentice-Hall Inc., 1981, Englewood Cliffs, N.J.

30. HENLEY, Ernest J. et H. KUMAMOTO. Designing for Reliability and Safety Control. Prentice-Hall Inc., 1985, Englewood Cliffs, N.J.

31. KUHN, Thomas S. La structure des révolutions scientifiques. Flammarion, 1983, 288 pages.

32. LEPLAT, Jacques. Erreur humaine, fiabilité humaine dans le travail. Armand Collin, Paris, 1985, 200 pages.

33. LEPLAT, Jacques et Xavier CUNY. Les accidents de travail. Presses Universitaires de France, 1974, Collection Que sais-je?, 126 pages.

34. NEGOITA, Virgil Constantin. Expert Systems and Fuzzy Systems. The Benjamin/Cummings Publishing Co., 1985.

35. POIRIER, Michel. Énergie et sécurité. Études d'économie de l'énergie, publiées par l'Institut Économique et Juridique de l'Énergie, Cahier no 8, Essais et travaux de l'Université de Grenoble. Ed. : Mouton et Co., 1969, 353 pages.

36. PRADE, Henri. A Computational Approach to Approximate and Plausible Reasoning with Applications to Expert Systems. IEEE Transactions on Pattern Analysis and Machine Intelligene, Vol. PAMI-7, No 3, May 1985.

37. RICH, Elaine. Artificial Intelligence. McGraw Hill, 1983.

38. SCHMUCKER, Kurth et J. Fuzzy Sets, Natural Language Computations, and Risk Analysis, Computer Science Press, 1984.

39. SHAFFER, G. A Mathematical Theory of Evidence. Princeton University Press, 1976.

40. SINAIKO, H. Wallace. Selected Papers on Human Factors in the Design and Use of Control Systems. Dover Publications Inc., New-York, 1961, 406 pages.

41. SINAIKO, H. Wallace et E.P. BUCKLEY. Human Factors in the Design of Systems. NRL Report 4996, Naval Research Laboratory, Washington, D.C. August 29, 1957 in H. Wallace Sinaiko (1961).

42. SINGLETON. W.T., R.S. EASTERBY and D.C. WHITEFIELD. The Human Operator in Complex System. On behalf of the University of Aston in Birmingham and the Industrial Section of the Ergonomics Research Society. Ed. : Taylor & Francis Ltd., London, 1971, 198 pages.

43. SINGLETON, W.T. Introduction à l'ergonomie. Organisation mondiale de la santé, Genève, 1974, p. 109.

44. SURRY, Jean. An Annoted Bibliography for Industrial Accident Research and Related Fields. A companion volume to "Industrial Accident Research : A human Engineering Appraisal". Ed. : Labour Safety Council of Ontario, April, 1969, 159 pages.

45. SURRY, Jean. Industrial Accidents Research : A Human Engineering Appraisal. University of Toronto. Department of Industrial Engineering, June 1969, 203 pages.

46. SWAIN, A.D. and H.E. GUTTMANN. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report NUREG/CR-1278, U.S. Nuclear Regulatory Commission 1983.

47. WILDE, Gérard J.S. Evidence refuting the theory of risk homeostasis? A rejoinder to Frank P. McKenna. Ergonomics, 1984, Vol. 27 no 3, p. 297-304.

48. WILDE, Gérard J.S. The theory of risk homeostasis : implications for safety and health. Risk Analysis 2, p. 209-225.

49. WINSTON, Patrick Henry. Artificial Intelligence. Second Edition, Addison-Wesley Publishing Co Inc., 1984.

50. WINSTON, Patrick Henry, Berthold KLAUS et Paul HORN. Lisp. Second Edition, Addison Wesley, 1984.

DES SYSTEMES EXPERTS...

19