Les études probabilistes de sûreté des centrales nucléaires françaises de 900 et 1 300 MW

Par Jacques BRISBOIS
Commissariat à l'Energie Atomique,
Institut de Protection et de Sûreté Nucléaire

Jeanne-Marie LANORE
Commissariat à l'Energie Atomique,
Institut de Protection et de Sûreté Nucléaire

Alain VILLEMEUR
Electricité de France,
Direction des Etudes et Recherches

Jean-Pierre BERGER
Electricité de France, Direction de l'Equipement

Jean-Marc De GUIO
Electricité de France,
Direction de la Production et du Transport

1. Introduction

Deux Etudes Probabilistes de Sûreté (EPS) des réacteurs à eau sous pression français ont vu leur aboutissement en 1990.

La première de ces études (EPS 900) concerne un réacteur standard du palier de 900 MWe et a été réalisée au Département d'Analyse de Sûreté de l'Institut de Protection et de Sûreté Nucléaire du Commissariat à l'Energie Atomique (CEA/IPSN/DAS) avec la participation de la société Framatome. Elle a été financée par le Service Central des Installations Nucléaires.

La seconde (EPS 1 300) a été menée par Electricité de France sur la tranche 3 (1 300 MWe) du Centre de Production Nucléaire de Paluel (fig. 1), le constructeur Framatome étant également associé à l'étude EPS 1 300.

Une Etude Probabiliste de Sûreté d'un réacteur nucléaire a pour objet, d'une part, d'identifier les scénarios d'accident susceptibles de se produire et d'endommager gravement le réacteur et, d'autre part, d'en évaluer les fréquences d'occurrence. Ces scénarios d'accident, encore appelés séquences accidentelles, sont identifiés en utilisant des méthodes appropriées ; ces séquences accidentelles sont généralement des successions de défaillances de matériels et/ou d'erreurs humaines d'opérateurs comme le sont, la plupart du temps, les véritables accidents.

Imaginer le pire pour mieux le prévenir ! Tel sont en définitive l'objet et l'objectif d'une EPS, tant il est évident que l'évaluation des points forts et faibles de la sûreté peut conduire à d'éventuelles améliorations de la sûreté au niveau de la conception ou de l'exploitation d'une installation nucléaire. Cette démarche permet ainsi de mieux apprécier les risques potentiels, et de hiérarchiser les efforts de sûreté.

Les EPS 900 et 1 300 sont, selon la terminologie généralement utilisée, des EPS de niveau 1, c'est-à-dire une évaluation de la fréquence de fusion du cœur. La poursuite de ces études jusqu'à l'évaluation de la fréquence des différents niveaux de rejet correspondrait à une étude de niveau 2 et l'évaluation des conséquences humaines et socio-économiques se ferait dans des études dites de niveau 3.

La première Etude Probabiliste complète a été réalisée aux Etats-Unis, en 1975 par une équipe dirigée par le professeur Rasmussen. Après diverses critiques, l'intérêt de l'étude et des méthodes associées apparut de plus en plus clairement, notamment après l'accident de Three Mile Island (1979).

En effet, cette approche fournit non seulement des résultats quantifiés de probabilité, mais elle constitue aussi une modélisation du fonctionnement du réacteur en situation accidentelle, intégrant un très grand nombre d'informations relatives à la conception et à l'exploitation des tranches.

Depuis lors, de nombreuses études de même type ont été réalisées dans la plupart des pays ayant un programme nucléaire, avec des retombées multiples tant pour la conception que pour l'exploitation des réacteurs.

Bien que la conception des réacteurs repose essentiellement sur des bases déterministes, l'approche probabiliste a été considérée en France, depuis le début des années 1970, comme une aide importante pour l'analyse de la sûreté. Diverses études probabilistes partielles ont été réalisées par Electricité de France, par l'IPSN et par Framatome pour différents types de réacteurs.

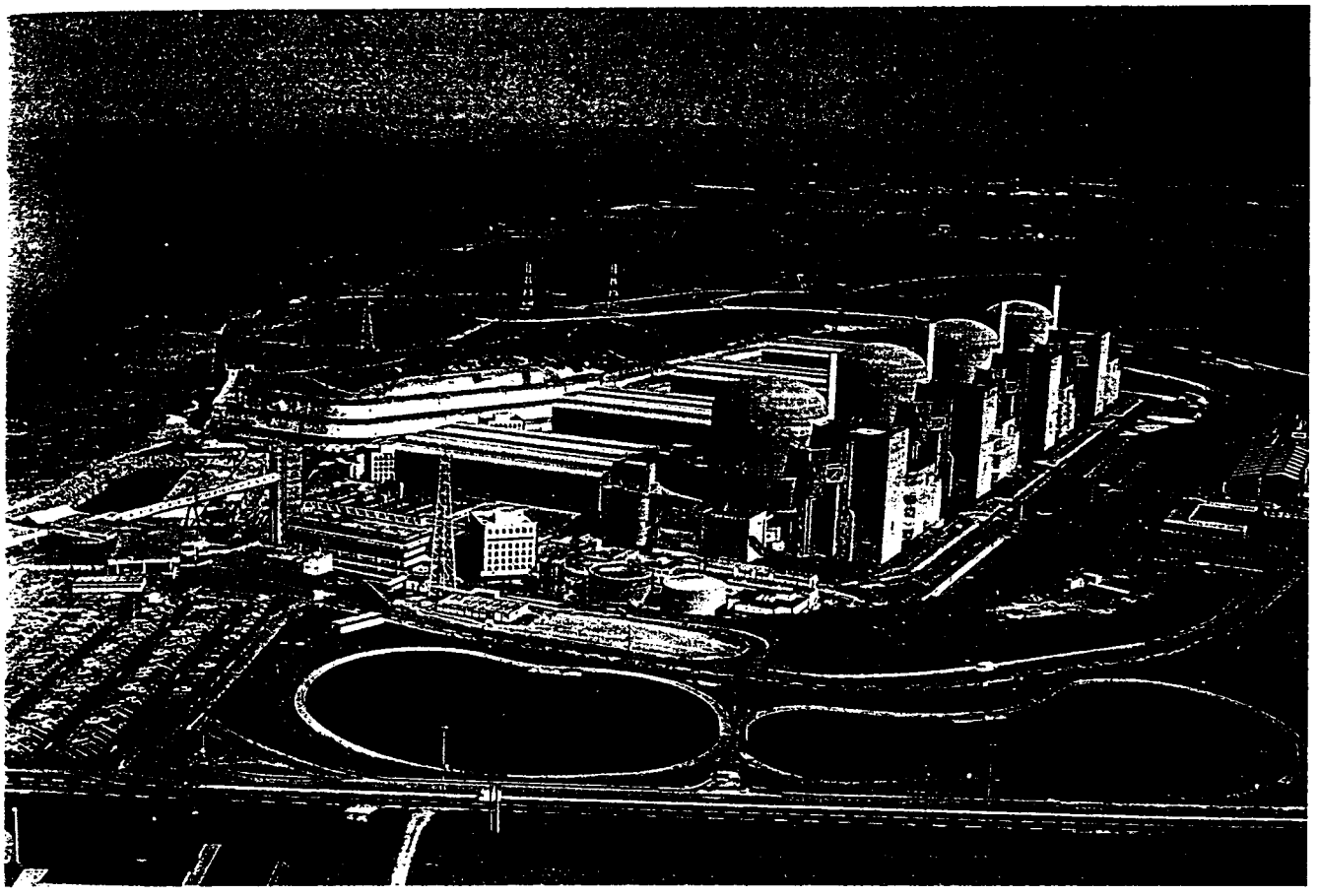
Ces études ont notamment permis d'évaluer la fiabilité et la disponibilité des systèmes de sûreté des centrales nucléaires, la probabilité de scénarios d'accidents, et d'aider à définir des spécifications techniques (notamment les délais de fonctionnement autorisés en cas d'indisponibilité partielle de systèmes de sûreté). En parallèle, les méthodes d'évaluation et les logiciels correspondants ont été largement développés. En outre, EDF a mis en place le Système de Recueil de Données de Fiabilité (SRDF) permettant un suivi du comportement des matériels sur toutes les tranches en exploitation, et en a déduit une base de données particulièrement représentative.

C'est en 1982 que la décision fut prise à l'IPSN de réaliser une EPS complète pour un réacteur standard du palier 900 MWe, et en 1986 qu'EDF lançait une étude équivalente sur un réacteur de 1 300 MWe en prenant comme référence la tranche de Paluel 3.

Ces EPS ont été achevées au cours du premier trimestre 1990. Elles ont été examinées par le Groupe Permanent chargé des réacteurs nucléaires qui étudie les problèmes techniques que posent, en matière de sûreté, la création, la mise en service, le fonctionnement et l'arrêt des réacteurs nucléaires ; suite à la réunion du 26 avril 1990, le Groupe Permanent chargé des réacteurs nucléaires a recommandé au Chef du Service Central de Sûreté des Installations Nucléaires que les résultats des Etudes Probabilistes de Sûreté soient pris en compte dans l'analyse de la sûreté des réacteurs à eau sous pression et que le développement de ces études soit poursuivi.

2. Qu'est-ce qu'une EPS ?

Les EPS s'intéressent à tous les accidents qui peuvent potentiellement endommager gravement le réacteur nucléaire — tout particulièrement le cœur du réacteur — et être source, si l'acci-



(M. BRIGAUD – SODEL)

Fig. 1. — **Centre de Production Nucléaire de Paluel.**

dent n'est pas maîtrisé, de rejets de produits radioactifs dans l'environnement.

Cette prévision des scénarios d'accident est basée sur des méthodes d'évaluation de la sûreté de fonctionnement (c'est-à-dire de la fiabilité, disponibilité, maintenabilité, sécurité) des systèmes développés auparavant dans les domaines industriels de pointe (aéronautique, spatial, nucléaire, etc.).

Afin de mesurer le caractère plus ou moins probable de ces scénarios, la fréquence de ces derniers est calculée à l'aide de méthodes utilisant la théorie des probabilités. Les données élémentaires, par exemple les fréquences des événements initiateurs d'accident, les fréquences de panne des matériels ou leur durée de réparation et les fréquences d'erreurs humaines sont déduites autant que possible de l'analyse du retour d'expérience des réacteurs nucléaires.

Une EPS comprend trois grandes parties, relatives à l'évaluation probabiliste :

- des initiateurs,
- des systèmes de sûreté,
- des séquences accidentelles.

L'évaluation probabiliste des initiateurs : elle a pour objet d'identifier et d'évaluer la fréquence des événements initiateurs ; ces événements encore appelés « initiateurs » sont des événements susceptibles d'entraîner une fusion du cœur soit directement soit parce que les systèmes de sûreté ne fonctionnent pas, par exemple pour des causes matérielles ou des causes humaines.

L'évaluation probabiliste des systèmes de sûreté : elle a pour objet d'évaluer la fiabilité (aptitude à fonctionner sans panne) ou la disponibilité (aptitude à être en état de fonctionner) ou la maintenabilité (aptitude à être réparée après une panne) des systèmes qui interviennent sur le plan de la sûreté. Les systèmes de sûreté sont généralement des systèmes redondants, sollicités pour maîtriser des situations de dimensionnement. Habituellement, une douzaine de systèmes répondent à ces critères ; ces systèmes ont été conçus pour des missions spécifiques, parfois fort différentes.

L'évaluation consiste, dans un premier temps, à identifier pour chacune des missions recensées les défaillances ou/et leurs combinaisons entraînant l'échec de ces missions ; dans un deuxième temps, les probabilités d'échec de ces missions sont calculées. Les causes de défaillances de ces systèmes sont ainsi identifiées et classées par ordre de probabilité décroissant. Les éventuels points faibles de ces systèmes sont mis en évidence.

L'évaluation probabiliste des séquences accidentelles : elle a pour objet de recenser et d'évaluer les séquences accidentelles ou scénarios d'accident conduisant à un accident grave c'est-à-dire à un accident endommageant le cœur du réacteur et pouvant conduire à sa fusion.

L'évaluation consiste, pour chaque initiateur retenu, à construire les séquences accidentelles. En règle générale, par des méthodes appropriées, on imagine l'échec des fonctions de sûreté sollicitées par l'occurrence de l'initiateur. Les défaillances des systèmes de sûreté correspondent aux échecs identifiés dans la partie précédente. Les défaillances humaines sont généralement des erreurs humaines commises durant la phase qui suit le début de l'accident (exemples : erreur de diagnostic de l'accident, erreur dans l'application d'une procédure de conduite accidentelle).

Ces trois grandes parties reposent ainsi sur l'analyse du retour d'expérience et sur l'évaluation de la fiabilité humaine, comme le représente la figure 2.

3. Caractéristiques et spécificités des EPS

On présente tout d'abord les caractéristiques majeures des EPS puis les spécificités des études françaises au regard de celles effectuées sur le plan international.

3.1. Caractéristiques majeures de l'EPS 900

Le réacteur considéré est un réacteur à eau sous pression de type CP2 (deuxième contrat pluriannuel des tranches de 900 MWe) prenant en compte l'ensemble des modifications décidées à la date du 1er janvier 1990. Le modèle correspond donc aux tranches des centrales de Saint-Laurent-des-Eaux, Cruas ou Chinon, peu différentes des autres tranches nucléaires de 900 MWe.

L'objectif général qui a été donné à l'EPS 900 est la création d'un outil d'aide à l'analyse de sûreté. Cet outil doit permettre d'évaluer l'importance des problèmes de sûreté en exploitation et de juger l'intérêt d'éventuelles modifications. On peut citer par exemple :

– la mise en évidence des éventuels points faibles de conception ;

– l'analyse des spécifications techniques d'exploitation et des procédures de conduite ;

– l'analyse des essais périodiques et de la maintenance en exploitation ;

– l'identification de domaines de recherche.

Pour atteindre cet objectif général, il a été décidé d'effectuer l'étude avec les objectifs plus particuliers suivants :

– réaliser une EPS aussi complète et détaillée que possible ;

– construire un modèle informatisé permettant d'effectuer rapidement, à partir de l'étude de base, des calculs de variation de risque et des remises à jour de l'étude en fonction de l'évolution des données et des connaissances.

Les travaux se sont déroulés de 1983 à 1990 en trois phases :

– de 1983 à 1987 : une phase préliminaire. Elle a fait l'objet d'une revue externe complète et détaillée effectuée par EDF ;

– de 1987 à 1989 : une phase provisoire. Elle a permis de prendre en compte qualitativement l'ensemble des remarques effectuées par EDF, ainsi que les résultats des études complémentaires et les améliorations jugées nécessaires. De plus, certaines modifications des tranches de 900 MWe, décidées entre temps, ont été introduites. C'est également lors de la phase provisoire qu'il a été décidé d'utiliser le système informatique LESSEPS développé par EDF ;

– de 1989 à 1990 : une phase définitive. Elle a permis d'effectuer la quantification finale, ainsi que la rédaction de la documentation définitive.

L'étude a nécessité la participation d'un nombre important d'ingénieurs de l'IPSN/DAS et de la société Framatome, dans des domaines de compétence variés (fonctionnement, physique, méthodes de fiabilité, facteur humain). L'investissement total de l'étude peut être estimé à 50 ingénieurs × an.

3.2. Caractéristiques majeures de l'EPS 1 300

Pour l'EPS 1 300, le CPN de Paluel tête de série du palier REP 1 300, a été retenu ; la tranche n° 3 est l'objet de l'étude car elle présentait le double avantage d'être en exploitation au début de l'EPS 1 300 et d'être la première tranche REP 1 300 MWe sur laquelle certains matériels améliorant la sûreté (les soupapes SEBIM du pressuriseur par exemple) venaient d'être installés avant d'être généralisés aux autres tranches nucléaires.

Deux buts ont été assignés au projet EPS 1 300 ; ils sont inséparables et d'égale importance :

• Evaluer la fréquence d'endommagement du cœur de la tranche n° 3 du CPN de Paluel, dans tous les états de fonctionnement de la tranche et ceci de manière aussi détaillée que possible.

• Fournir un logiciel d'évaluation, le logiciel LESSEPS afin de réaliser une EPS « vivante », c'est-à-dire révisable en fonction de l'évolution des données et des connaissances.

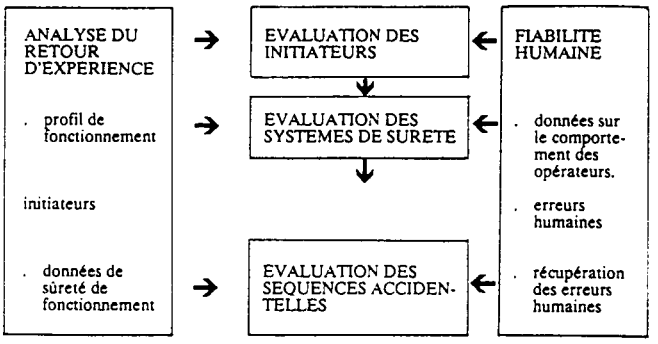


Fig. 2. – **Démarche générale des EPs 900 et 1 300.**

Ces buts s'apprécient en tenant compte des objectifs généraux poursuivis par ce projet afin d'en favoriser au maximum les retombées.

Le premier objectif était d'évaluer la démarche de sûreté française et notamment de vérifier et de confirmer le haut niveau de sûreté des centrales nucléaires françaises, d'importantes améliorations de la sûreté ayant été apportées ces dernières années à ces types de centrales tant au niveau de la conception qu'au niveau de l'exploitation.

Le deuxième objectif était d'aider à la conception et à l'exploitation des centrales nucléaires françaises (exemples : définition du projet REP 2000, calcul des spécifications techniques, amélioration des procédures de conduite et de la formation des opérateurs, etc.).

L'EPS 1 300 a été menée par trois directions d'EDF, à savoir la Direction des Etudes et Recherches, la Direction de l'Equipement et la Direction de la Production et du Transport. La société Framatome a été associée au projet EPS 1 300 dès son lancement.

Trois phases ont été successivement distinguées dans le projet EPS 1 300 : phase préliminaire (1986-88), provisoire (1988-89) et définitive (1989). Elles ont permis de réactualiser et de compléter les études de manière structurée et ordonnée en tenant compte des avis ou des critiques formulées par de nombreuses unités. Notamment, toutes les données ont fait l'objet d'un contrôle par IPSN et le jeu de données commun, finalisé en juin 1989, a permis de réaliser la phase définitive.

Un contrôle externe de l'évaluation probabiliste a été conduit par l'IPSN ; tous les rapports techniques relatifs aux évaluations probabilistes (des systèmes de sûreté, des séquences accidentelles), aux méthodes d'analyse et aux données tirées de l'analyse du retour d'expérience ont été diffusés à l'IPSN dans les différentes phases de l'EPS 1 300.

D'importants moyens humains et financiers ont été consacrés à l'EPS 1 300 ; ainsi un effort d'environ 50 ingénieurs × an a été effectué et le coût du projet EPS 1 300 peut être évalué à environ 50 MF.

3.3. Spécificités des études françaises

Abordons maintenant les spécificités des EPS qui permettent de les positionner sur le plan international, tant au niveau du contenu que de l'ampleur.

• Niveau d'étude

Les EPS françaises sont donc des études de niveau 1, à savoir des études ayant pour objet l'évaluation de la fréquence de la fusion du cœur du réacteur. Cependant, dans leur état actuel, les deux EPS ne prennent pas en compte les agressions externes et internes comme l'incendie, l'inondation ou le séisme ; des travaux de recherche méthodologique sur la prise en compte des agressions dans les EPS ont été lancés pour pallier cette limitation actuelle.

Tableau 1. — **Profil de fonctionnement d'une tranche REP.**

	Etat	Description	Durée de l'état (en jours)	Pourcentage
Etat de puissance	a	— Réacteur en puissance — Réacteur en arrêt à chaud ou en partie supérieure du domaine d'arrêt intermédiaire	312	85,5
Etats d'arrêt	b	— Réacteur en partie inférieure du domaine d'arrêt intermédiaire Réacteur en refroidissement aux conditions RRA	8	0,5
	c	— Arrêt RRA, circuit primaire plein	11	3
	d	— Circuit primaire partiellement vidangé ou ouvert	19	5,2
	e	— Piscine réacteur pleine	9	2,5
	f	— Etat du primaire, le combustible étant entièrement déchargé	12	3,3

• Etats du réacteur

Tous les états de la tranche sont étudiés, y compris les arrêts à froid ; habituellement, les EPS ne considèrent que l'état de fonctionnement en puissance, les risques dans les autres états étant supposés négligeables. Il a semblé important de vérifier cette hypothèse.

Cette originalité rend l'étude plus longue mais également plus complexe. Les méthodes correspondantes avaient été en partie développées dans le cadre des évaluations probabilistes des situations complémentaires qui avaient déjà traité tous les états du réacteur.

Le tableau 1 donne le profil de fonctionnement d'une tranche REP pris en compte dans les EPS ; notons dès maintenant que le risque est évidemment nul dans l'état f où le combustible est entièrement déchargé.

• Rôle de l'Ingénieur de Sûreté Radioprotection (ISR)

L'introduction dans les centrales françaises, ces dernières années, d'un Ingénieur de Sûreté Radioprotection, en complément de l'équipe de quart et des ingénieurs d'exploitation, est une caractéristique fondamentale de la sûreté en exploitation.

Ceci a conduit à innover au niveau de la fiabilité humaine, pour prendre en compte cette « redondance humaine », tant au niveau des modèles de la fiabilité humaine qu'au niveau des données à introduire.

• Procédures U

La démarche de sûreté française a conduit à introduire de nouvelles procédures dites Ultimes (procédures U). Les procédures U ayant un impact sur l'étude, à savoir les procédures U_1 (refroidissement ultime du cœur) et U_3 (secours des systèmes d'injection de sécurité et d'aspersion de l'enceinte par du matériel mobile) sont prises en compte.

• Situations accidentelles à long terme

L'analyse des séquences a été menée soit jusqu'à la fusion du cœur, soit jusqu'à un état dans lequel le risque puisse être considéré comme négligeable. Cette dernière condition a conduit à prendre en compte des situations post-accidentelles de longue durée, en particulier dans le cas des brèches du circuit primaire pour lesquelles on a étudié une phase à long terme pouvant durer jusqu'à un an.

4. Méthodologie

La figure 2 décrit la démarche générale des EPS. La méthodologie utilisée pour réaliser les EPS françaises est basée sur des méthodes relatives aux domaines suivants :

— analyse du retour d'expérience,

— évaluation probabiliste,

— fiabilité humaine,

— informatisation.

On aborde successivement les éléments méthodologiques marquants de chacun de ces domaines. Enfin on traite de l'important problème de la prise en compte des incertitudes dans les EPS.

4.1. Analyse du retour d'expérience

La quasi-totalité des données utilisées dans les EPS sont issues de l'analyse de l'expérience d'EDF liée aux centrales REP en exploitation.

Dès 1986, l'important retour d'expérience accumulé (représentant environ 200 années × réacteur) permettait d'engager une analyse détaillée de ce retour d'expérience en vue d'obtenir des données avec un niveau de confiance suffisant.

L'existence d'un parc homogène de réacteurs nucléaires et donc la présence de matériels quasi-identiques, sans équivalent de par le monde, a beaucoup contribué à l'obtention de données de grande qualité.

L'analyse du retour d'expérience a eu recours aux nombreuses banques nationales de données d'EDF (Système de Recueil de Données de Fiabilité, Fichier des Evénements, Fichiers de Données Statistiques...). Des enquêtes sur sites ont également été menées pour compléter ces données et tenir compte des spécificités du site étudié ; des systèmes informatiques ont été utilisés ou développés pour le recueil d'informations locales. Pour certaines données particulières il a été fait appel à quelques bases de données étrangères.

La base de données comprend principalement :

— **les données d'exploitation** concernant les durées moyennes des états standard de la tranche : durée du fonctionnement en puissance, en arrêt à chaud, en arrêt à froid. Le tableau 1 illustre le profil de fonctionnement retenu pour les tranches françaises ;

— **la liste des événements initiateurs** ainsi que les fréquences d'occurrence associées. Cette liste est élaborée à partir des résultats d'exploitation et complétée par une recherche bibliographique ou par des études pour les situations à la limite du dimensionnement, de fréquence rare ou hautement improbable ;

— **les données de sûreté de fonctionnement** (encore appelées communément « données de fiabilité ») de tous les matériels comme les taux de défaillance en fonctionnement (nombre de défaillances en fonctionnement rapporté à la durée cumulée d'heures de fonctionnement), les taux de défaillance à la sollicitation (nombre de défaillances à la sollicitation rapporté au nombre total des sollicitations), les durées moyennes de réparation associées, ainsi que les durées d'indisponibilité des maté-

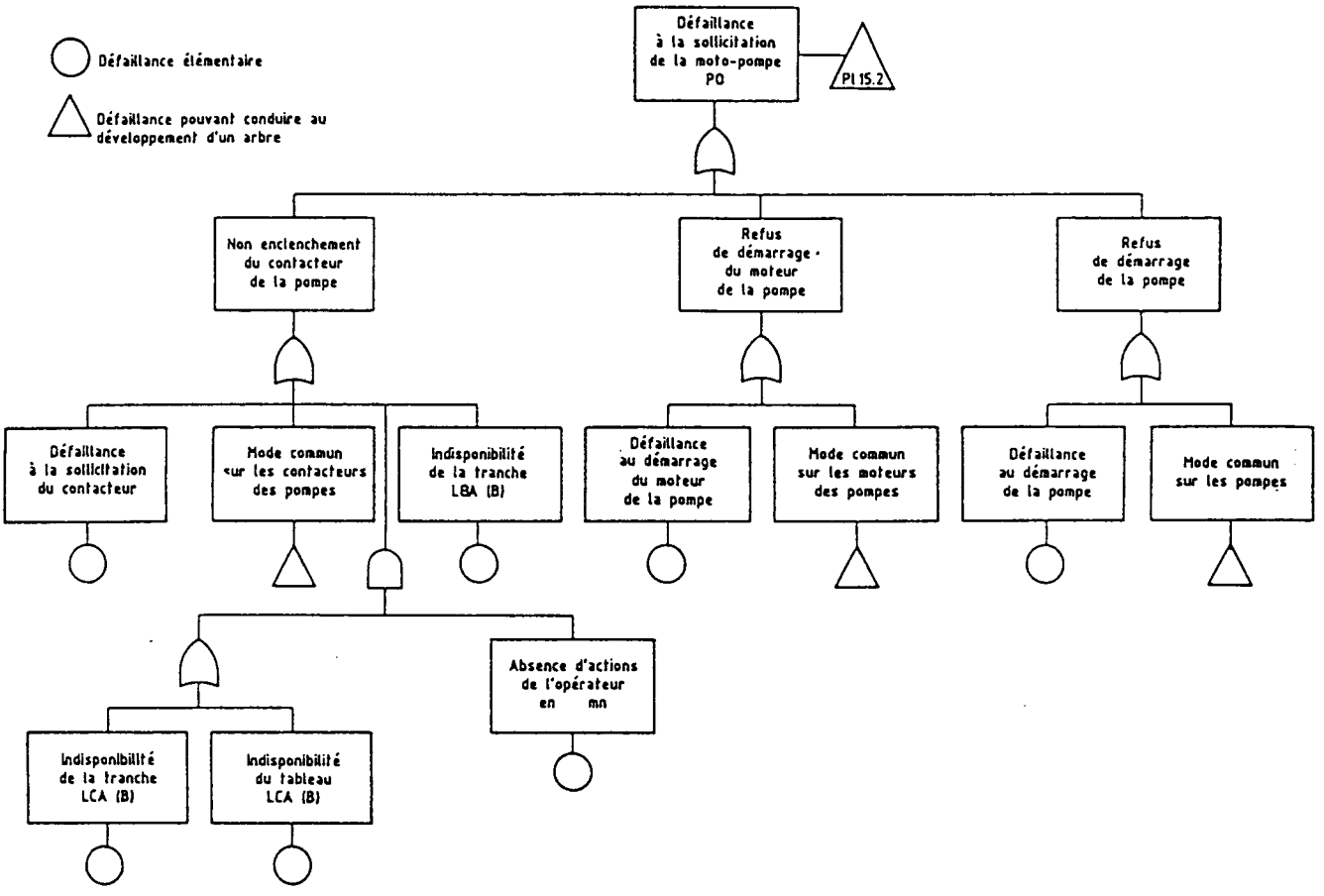
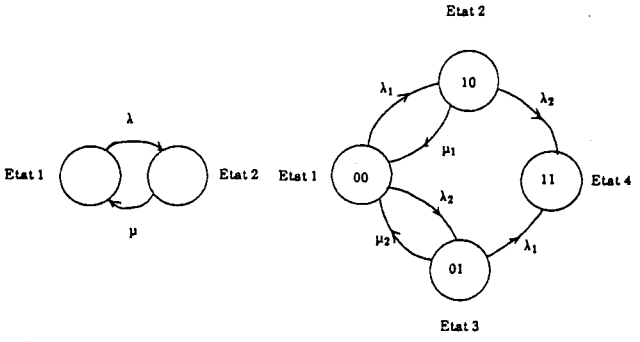


Fig. 3. — **Exemple d'un arbre de défaillance.**



Graphes d'états d'un système à un composant
Etat 1 : état de fonctionnement
Etat 2 : état de panne
λ : taux de défaillance
μ : taux de réparation

Graphe d'états d'un système à deux composants (en redondance)
Etat 1 (00) : les deux composants fonctionnent
Etat 2 (10) : le composant 1 est en panne, le composant 2 est en fonctionnement
Etat 3 (01) : le composant 1 est en fonctionnement, le composant 2 est en panne
Etat 4 (11) : les deux composants sont en panne
Etat de fonctionnement : Etats 1, 2, 3
Etat de panne : Etat 4

Fig. 4. — **Exemple de graphes d'états.**

riels dans les différents états définis ci-dessus, intégrant les indisponibilités pour maintenance corrective, préventive ou pour essai périodique.

Ces données comprennent également celles relatives aux défaillances de cause commune (voir paragraphe 4.2.2) déterminées par une méthode spécifique.

Pour la plupart de ces données, il est calculé un facteur d'erreur représentant les limites de l'intervalle de confiance associées à la valeur estimée.

Cette base de données a fait l'objet d'une analyse critique de la part de l'IPSN ; en juin 1989, une base de données commune à l'IPSN et à EDF a été obtenue.

4.2. Evaluation probabiliste

4.2.1. Evaluation probabiliste des initiateurs

L'expérience française et internationale a déjà conduit au recensement de ce type d'événements. La liste a été complétée au vu des évaluations probabilistes de systèmes réalisés dans les premières phases des EPS. L'évaluation de leurs fréquences d'occurrence résulte d'une analyse du retour d'expérience lorsqu'ils se sont déjà produits ou d'une analyse prévisionnelle dans les autres cas.

4.2.2. Evaluation probabiliste des systèmes de sûreté

La démarche, suivie pour l'étude de ces systèmes, environ treize pour chaque EPS, comprend principalement les étapes suivantes :

— **identification des missions ;** toutes les missions (ou fonctions) sont identifiées compte tenu des scénarios d'accident dans lesquels ces systèmes peuvent intervenir ;

— **analyse préliminaire par Analyse des Modes de Défaillances et de leurs Effets (AMDE) ;** cette analyse consiste à identifier les modes de défaillance des composants du système (exemples : pompe, vanne, etc.) et à étudier tous les effets de l'occurrence de ces modes de défaillance sur les fonctions du système, la salle de commande, les opérateurs, etc. ;

— **modélisation des missions :** l'ensemble des défaillances ou pannes (et leurs combinaisons) est identifié par des méthodes comme l'arbre de défaillance (ou arbre des causes) et le graphe d'états markovien.

Rappelons succinctement quelques caractéristiques de ces méthodes.

La méthode de l'arbre de défaillance consiste à :

– déterminer les diverses combinaisons possibles d'événements qui entraînent la réalisation d'un événement indésirable unique ;

– représenter graphiquement ces combinaisons au moyen d'une structure arborescente.

L'arbre de défaillance est ainsi formé de deux niveaux successifs d'événements tels que chaque événement est généré à partir des événements de niveau inférieur par l'intermédiaire de portes logiques (OU et ET) ; ces événements sont généralement des défaillances de matériels, des indisponibilités de matériels, des erreurs humaines... pouvant conduire à l'événement indésirable.

Des programmes informatiques de calcul appropriés permettent :

– d'identifier les coupes minimales, c'est-à-dire les plus petites combinaisons d'événements conduisant à l'événement indésirable ;

– de calculer la probabilité de l'événement indésirable et des coupes minimales associées.

Un exemple d'arbre de défaillance est présenté à la figure 3.

La méthode du graphe d'états consiste à :

– recenser et classer tous les états du système en états de fonctionnement ou en états de panne ;

– recenser toutes les transitions possibles entre ces différents états et identifier toutes les causes de ces transitions ; celles-ci sont généralement l'apparition d'une défaillance d'un composant du système ou l'existence d'une réparation d'un composant ;

– calculer les probabilités de se trouver dans les différents états ou d'autres caractéristiques de sûreté de fonctionnement (durée moyenne de fonctionnement du système avant la première défaillance, durée moyenne de réparation, taux de défaillance équivalent, etc.).

Des exemples de graphes d'états sont présentés à la figure 4.

D'une manière générale, la méthode du graphe d'états est retenue pour modéliser l'échec d'une mission d'un système réparable ou présentant des changements de configuration au cours du temps (dans le cadre de la mission considérée).

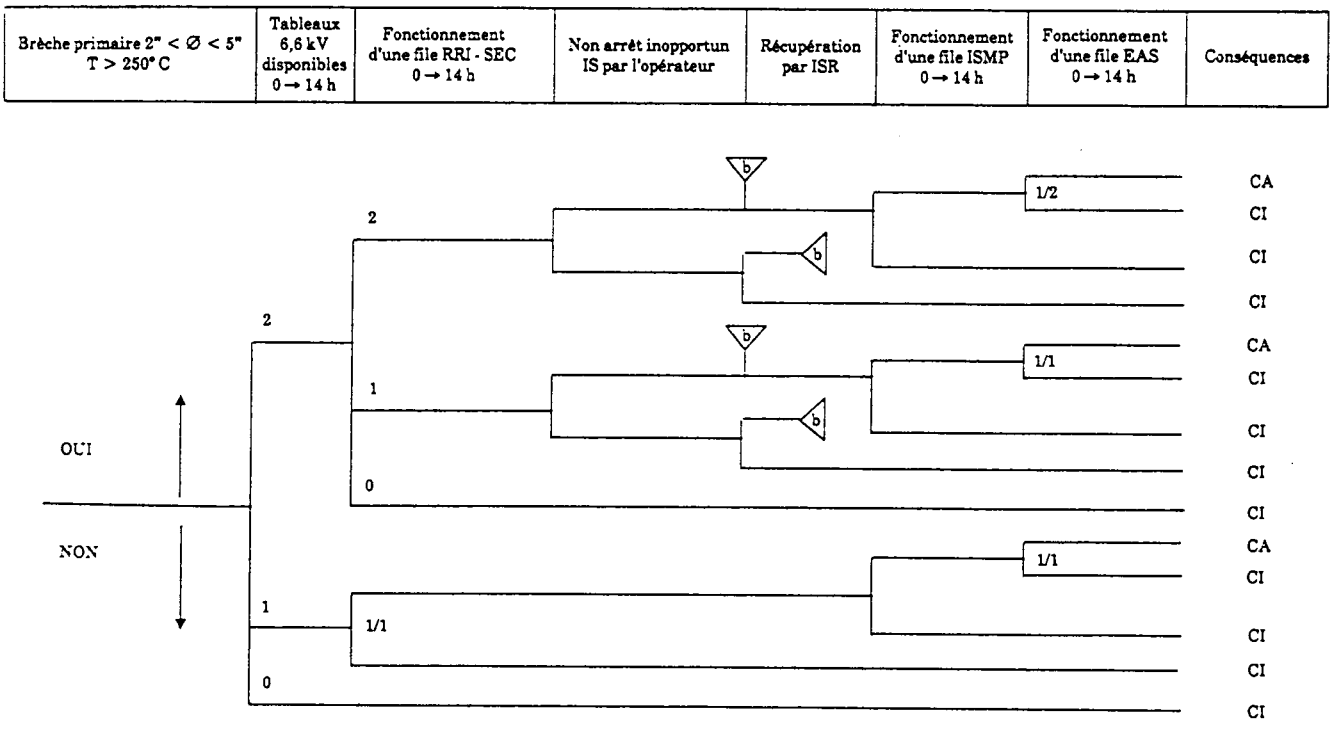
Dans le cas d'un système non redondant ou en redondance active (tous les composants fonctionnent simultanément) et lorsque le système est considéré comme non réparable (système inaccessible, contaminé par exemple), la méthode de l'arbre de défaillance est retenue.

• **Analyse quantitative** : les coupes minimales des arbres de défaillances ont été systématiquement calculées ainsi que les fréquences d'échec des missions des systèmes. Les probabilités des états de panne des graphes d'états markoviens ont également été calculées. On en déduit ainsi les points faibles de ces systèmes.

• **Analyse du retour d'expérience** : pour chaque système de sûreté, les incidents sur les matériels ont été collectés et analysés. On a notamment vérifié que ces incidents étaient pris en compte dans les analyses prévisionnelles et que ces dernières étaient cohérentes avec les enseignements tirés de ces incidents.

L'application de cette démarche a conduit à l'obtention d'environ quatre cents modèles (arbres de défaillance et graphes d'états). Les plus complexes des arbres de défaillances pouvaient comprendre plusieurs centaines d'événements.

Mentionnons qu'une grande attention a été accordée aux défaillances de cause commune. On rappelle que les défaillances de cause commune sont des défaillances survenant de manière simultanée ou concomitante sur plusieurs composants et provenant de la même cause. De possibles défaillances de cause commune ont été systématiquement envisagées sur les



La perte d'un tableau LH ou LB rend la file RRI-SEC de la même voie indisponible. La perte d'un tableau LH ou LB ou la perte d'une file RRI-SEC rend la file des systèmes RIS (ISMP et ISBP) et EAS de la même voie indisponible. Le fonctionnement des tableaux LH-LB est donc examiné en premier, puis celui des files RRI-SEC en fonction de la disponibilité des tableaux électriques, puis enfin celui des systèmes RIS et EAS en fonction de la disponibilité des systèmes supports.

Fig. 5 - **Exemple d'un arbre d'événements.**

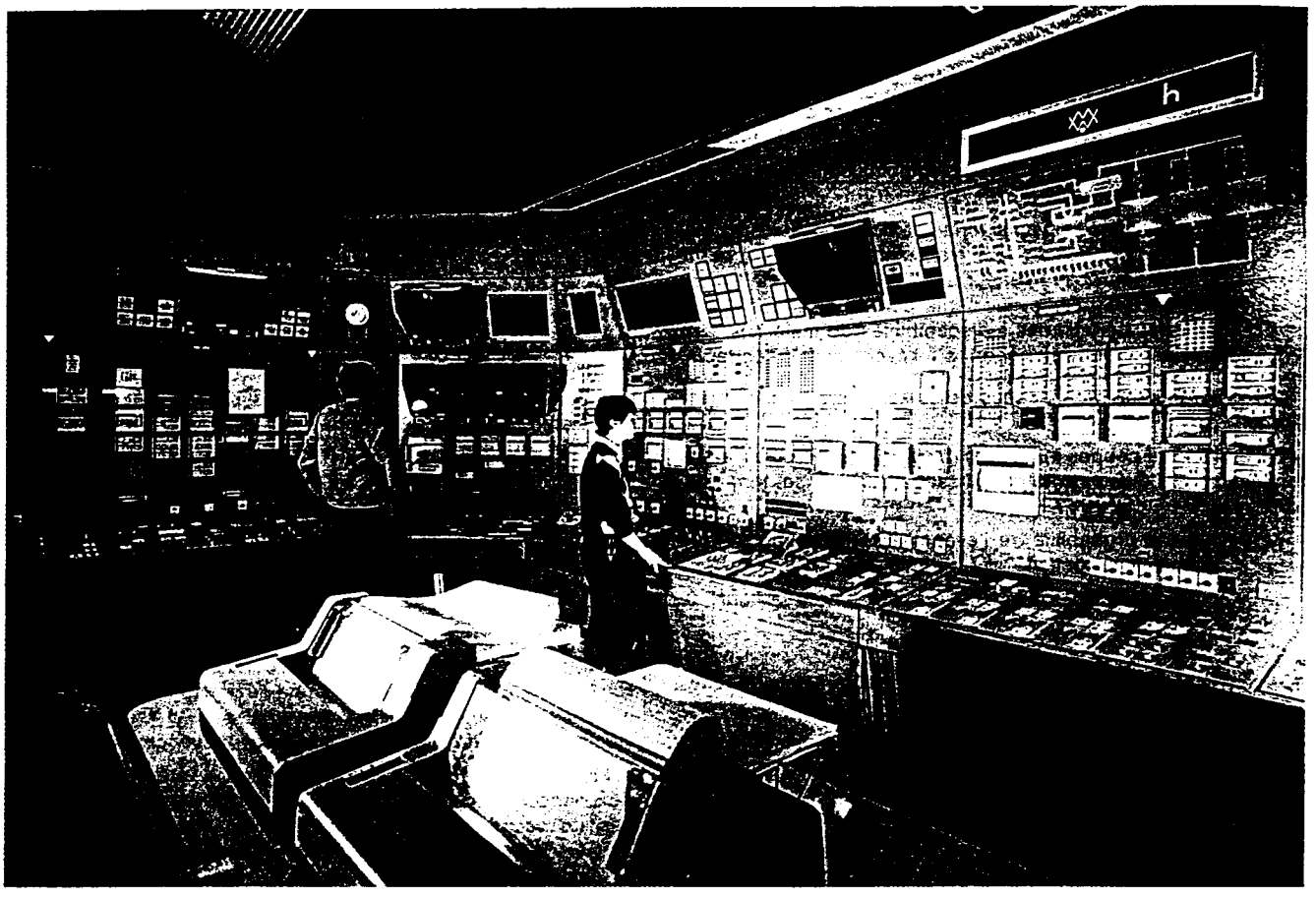


Fig. 6 - **Simulateur de formation d'EDF.**

composants de systèmes de sûreté tels que pompes, moteurs, diesels, turbines, vannes, clapets, soupapes, contacteurs, disjoncteurs, capteurs. Dans les modèles (par exemple arbre de défaillance), ces défaillances de cause commune ont été introduites pour tous les composants en redondance. La quantification a été réalisée à l'aide d'une méthode spécifique ; les paramètres de la loi ont été tirés de l'analyse de l'expérience française.

4.2.3. Evaluation probabiliste des scénarios d'accident

La méthode de l'arbre des événements (ou arbre des conséquences) a généralement été utilisée. Rappelons que la méthode de l'arbre d'événements consiste principalement à :

– identifier les séquences menant à un accident (ou séquences accidentelles). Ceci se fait par l'étude des conséquences de l'initiateur ;

– à représenter graphiquement ces séquences au moyen d'une structure arborescente ;

– à calculer les probabilités des séquences accidentelles.

Une séquence est une succession d'événements dont le premier est l'événement initiateur ; les autres sont appelés « événements génériques ». Ces derniers correspondent habituellement aux missions des systèmes requis après l'apparition de l'initiateur ou à des actions de l'opérateur.

Les conséquences des séquences sont classées en différentes catégories : acceptables ou inacceptables. Les séquences aux conséquences inacceptables (CI) sont bien évidemment celles qui entraînent généralement un endommagement du cœur. Seules les probabilités de ces séquences sont calculées.

Un exemple d'arbre d'événements est présenté à la figure 5.

Cette méthode a été utilisée pour modéliser la plupart des scénarios. Ceux-ci sont en effet de courte durée (au plus quelques jours après l'apparition de l'initiateur) et l'on peut supposer que les systèmes requis pour maîtriser l'initiateur ne sont pas réparables.

Lorsque les scénarios d'accident à long terme font intervenir des systèmes dont les composants peuvent être réparés durant le déroulement du scénario, une autre méthode a été utilisée : les graphes d'états markoviens.

Environ 200 arbres d'événements et 50 enchaînements de graphes markoviens (soit environ 900 graphes différents) ont ainsi été construits pour l'ensemble des événements initiateurs susceptibles de se produire dans tous les états du réacteur.

4.3. Fiabilité humaine

Un gros effort a été fait pour prendre en compte les erreurs humaines susceptibles de se produire après occurrence de l'événement initiateur.

La méthode d'identification des erreurs humaines est dérivée de la méthode SHARP (Systematic Human Action Reliability Procedure), méthode éprouvée sur le plan international. De nombreux modèles de fiabilité humaine ont été élaborés, notamment au niveau des diagnostics et de l'exécution des actions. D'une manière générale, ces méthodes et ces modèles se sont très largement appuyés sur une expérience originale en matière d'essais sur simulateur (fig. 6) ; ainsi, plus de deux cents essais ont été réalisés ces dernières années par EDF sur ses simulateurs de formation.

Rappelons que ces essais sur simulateur (ou essais de Mise en Situation Recréée - MSR) permettent l'observation du comportement des opérateurs en situation incidentelle ou accidentelle simulée. De très nombreux enseignements ont été tirés de ces essais (exemples : type d'erreurs, temps moyen de diagnos-

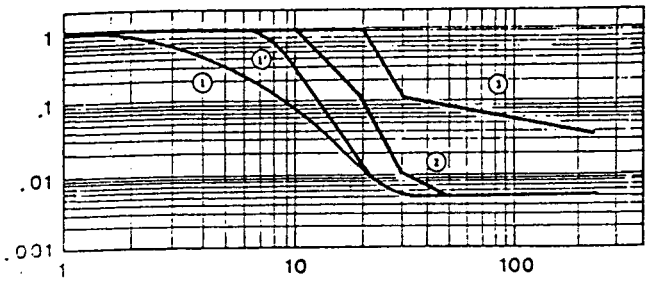


Fig. 7 - **Probabilité d'échec du diagnostic par l'opérateur.**

tic, temps moyen de récupération d'une erreur, etc.) et ont été intégrés dans les EPS.

De nombreux modèles ont été créés afin d'attribuer une probabilité à une erreur humaine en conduite incidentelle ou accidentelle en fonction des caractéristiques de la situation fournie par l'analyse qualitative. A titre d'exemple explicitons un de ces modèles, celui de la probabilité qu'un diagnostic ne soit pas effectué ou soit mal effectué par l'opérateur (ou l'équipe), dans le délai disponible t pour le réaliser. La figure 7 présente un tel modèle.

Les courbes proposées correspondent à différents niveaux de difficulté du diagnostic. Les courbes 1 et 1' s'appliquent aux diagnostics les plus faciles, c'est-à-dire aux incidents et accidents « classiques » dont le diagnostic est facilité par des consignes de diagnostic, et qui sont couramment pratiqués par les opérateurs en formation et recyclage. La courbe 3 s'applique aux situations les plus délicates, aux caractéristiques inverses des précédentes (incidents et accidents « non classiques »...). La courbe 2 correspond à un niveau intermédiaire.

Ces règles ont été définies pour guider le choix de la courbe à utiliser. Ce choix peut être facilité si l'on dispose de quelques données expérimentales propres au cas étudié.

Les courbes 1 et 1' sont directement issues des essais sur simulateurs « MSR » pour les délais inférieurs à 20 mn, et extrapolées des résultats d'essais au-delà de 20 mn. Les courbes 2 et 3 sont inspirées de celles généralement utilisées aux Etats-Unis ; elles demeurent néanmoins, tout en étant plus conservatrices, assez hypothétiques.

Ainsi, d'une manière générale, le facteur humain intervient dans les EPS sous deux grandes formes : la modélisation du comportement des opérateurs (opérateur de l'équipe de quart, équipe de quart, ISR, etc.) dans le cadre d'interventions et celle des erreurs humaines de ces acteurs.

4.4. Informatisation

Environ 600 modèles ont été construits. Leur traitement a été réalisé par le logiciel LESSEPS qui a été élaboré par EDF. Celui-ci permet :

– le calcul des probabilités d'échec des missions des systèmes ;

– le calcul des probabilités des scénarios d'accident ;

– les études de sensibilité aux données : les données de fiabilité peuvent être modifiées et le logiciel recalcule toutes les probabilités pertinentes en optimisant le calcul, c'est-à-dire en ne relançant que les calculs strictement nécessaires.

Schématiquement, les logiciels LESSEPS 900 et LESSEPS 1 300, qui sont des applications du logiciel LESSEPS aux EPS 900 et 1 300, comprennent (fig. 8) :

– une base de données (données de sûreté de fonctionnement, profils de fonctionnement, etc.) ;

– des programmes informatiques d'évaluation de modèles élémentaires : PHAMISS pour les arbres de défaillances, ISA pour les arbres d'événements, MARK SMP et GSI pour les graphes d'états ;

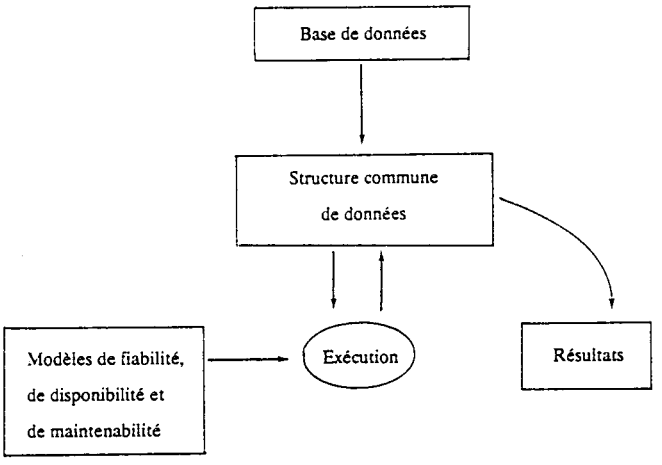


Fig. 8 - **Structure de LESSEPS.**

– un programme-maître (chef d'orchestre) pour permettre l'enchaînement des modèles et la recherche des données dans la base ;

– des systèmes-experts pour l'évaluation de certains systèmes de sûreté en ayant recours aux techniques de l'intelligence artificielle : EXPRESS pour des systèmes thermohydrauliques et EXPGSI pour des systèmes électriques. Mentionnons ainsi, à titre d'illustration, que le logiciel EXPRESS construit l'arbre de défaillance à partir d'une description formalisée de la topologie et du fonctionnement d'un système thermohydraulique.

Le logiciel LESSEPS fonctionne sur IBM 3090. Le calcul de l'ensemble de l'étude demande quelques heures de temps calcul. Une version LESSEPS sera bientôt disponible sur station de travail.

4.5. Prise en compte des incertitudes

Les résultats de l'EPS sont entachés d'une inévitable incertitude qu'il est indispensable de préciser. Les sources majeures d'incertitude peuvent être regroupées en trois catégories :

• Les incertitudes provenant d'un manque d'exhaustivité à l'intérieur même du domaine étudié. Il est clair qu'on ne peut réellement démontrer l'exhaustivité d'une telle étude, même si, comme dans le cas des EPS françaises, les travaux ont été menés avec un souci constant de prendre en compte le plus grand nombre possible de situations, notamment en traitant les états du réacteur hors puissance, et les initiateurs du type pertes de sources ou transitoires.

• Les incertitudes liées aux données : données de fiabilité des composants, fréquence des initiateurs, défaillances de cause commune, fiabilité humaine. Le facteur d'erreur associé à chacune de ces données, qui indique les bornes d'un intervalle à 90 % de confiance, peut être estimé entre 3 et 10 selon les données. Les valeurs les plus incertaines sont les fréquences des initiateurs très rares, comme les grosses brèches primaires, les brèches dans les états d'arrêt, les cumuls de rupture de tuyauterie de vapeur et de tubes de générateurs, ou la perte de la prise d'eau, et également les données relatives au facteur humain, notamment dans les situations qui ne corrrespondent pas à des observations réelles (diagnostic de situations complexes, avec des délais importants).

• Les incertitudes provenant de la modélisation, dont l'impact sur le résultat peut être très important, sont de plus, très difficiles à estimer quantitativement. Diverses études de sensibilité ont permis d'identifier certaines hypothèses de modélisation pouvant être à l'origine d'incertitudes significatives. En premier lieu, on peut citer les hypothèses concernant la tenue des matériels en situation accidentelle, par exemple le comportement des soupapes de générateur de vapeur sollicités en eau, la tenue des joints des pompes primaires en cas de défaillance de l'injection et du refroidissement, le fonctionnement des équipements au-delà de

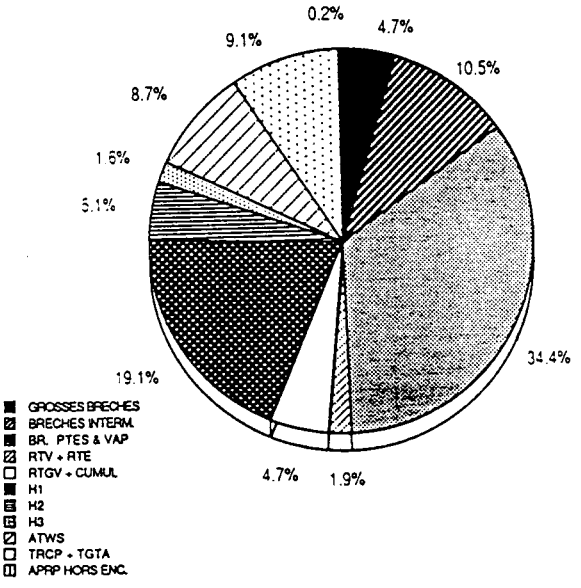
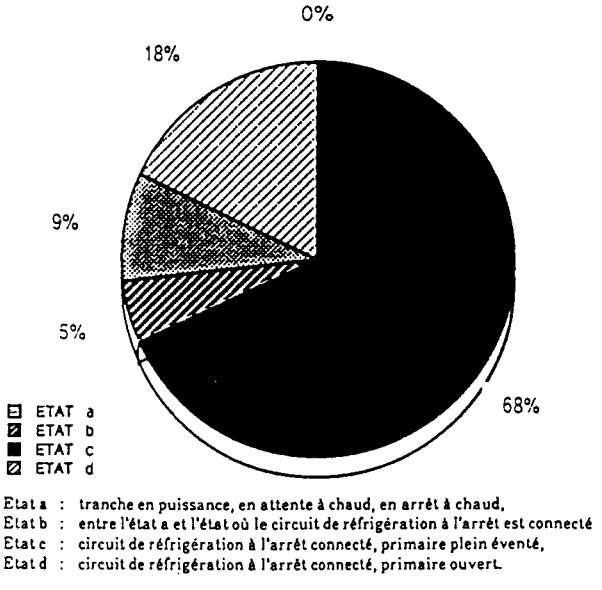


Fig. 9 - **EPS 900 : fréquence d'endommagement du cœur par famille d'initiateurs.**



Etat a : tranche en puissance, en attente à chaud, en arrêt à chaud,
Etat b : entre l'état a et l'état où le circuit de réfrigération à l'arrêt est connecté
Etat c : circuit de réfrigération à l'arrêt connecté, primaire plein éventé,
Etat d : circuit de réfrigération à l'arrêt connecté, primaire ouvert.

Fig. 10 - **EPS 900 : fréquence d'endommagement du cœur par état de la tranche.**

leurs limites de spécification ou de qualification (exemple : les pompes d'injection de sécurité à basse pression lors de la défaillance du circuit d'aspersion dans l'enceinte assurent le refroidissement de l'eau d'injection). D'autres incertitudes proviennent d'un manque de connaissance de certains phénomènes physiques, comme les conditions de mélange lors de dilutions intempestives.

Face à ces différents problèmes, les hypothèses adoptées dans les EPS sont conservatrices.

De plus, notons que les incertitudes ne sont pas inhérentes aux EPS, mais proviennent d'une manière générale de la limitation des connaissances. Et dans ce sens, l'intérêt des EPS est de mettre en évidence les domaines dans lesquels un approfondissement des connaissances serait particulièrement utile.

5. EPS 900 : résultats

5.1. Résultats d'ensemble

La fréquence totale d'endommagement du cœur obtenu dans cette étude est de :

$$5{\cdot}10^{-5}/\text{tranche} \times \text{an}$$

Les contributions des familles d'initiateurs et des états sont données par les figures 9 et 10.

5.2. Commentaires sur les familles et séquences dominantes

5.2.1. Accidents de Pertes de Réfrigérant Primaire

L'ensemble des APRP contribue pour environ 50 % du risque total, avec la répartition suivante :

	En puissance	A l'arrêt
Grosses brèches	$1{,}2{\cdot}10^{-6}$	$1{,}1{\cdot}10^{-6}$
Brèches intermédiaires	$4{,}1{\cdot}10^{-6}$	$1{,}1{\cdot}10^{-6}$
Petites brèches	$9{,}4{\cdot}10^{-6}$	$7{,}6{\cdot}10^{-6}$

Les séquences dominantes sont :

– une brèche en puissance suivie à court ou moyen terme de la défaillance du système d'injection de sécurité basse pression. Le poids de cette séquence est de $6{\cdot}10^{-6}$/tranche × an pour les petites brèches dans l'état a ;

– une brèche dans un état d'arrêt (états c, d ou e dans lesquels le démarrage de l'injection de sécurité n'est pas automatique), suivi de l'échec de l'opérateur dans la mise en service manuelle de ce système. Cette séquence intervient pour $3{,}6{\cdot}10^{-6}$/tranche × an dans l'état c et $5{\cdot}10^{-6}$/tranche × an dans l'état d.

On peut noter quelques points marquants :

– les états d'arrêt ont un poids élevé, dû essentiellement à l'absence d'automatisme et au risque d'erreur humaine. Cependant l'incertitude est importante, notamment en ce qui concerne la fréquence des initiateurs ;

– le long terme, c'est-à-dire la phase post-accidentelle au-delà de quinze jours après l'accident, contribue pour 16 % du résultat, ceci en prenant en compte les procédures H4-U3. Ces procédures permettent le secours mutuel des systèmes d'injection et d'aspersion de l'enceinte à l'aide de moyens mobiles. Sans ces procédures le risque à long terme est multiplié par environ un facteur 10 ;

– le facteur humain intervient dans 55 % des séquences liées aux APRP, soit à court terme (mise en service manuelle de l'injection de sécurité), soit à long terme (mise en œuvre des procédures H4-U3).

5.2.2. Perte totale de la source froide

La séquence dominante est une perte de la source froide par perte de la prise d'eau, suivie d'une erreur humaine dans la mise en œuvre de la procédure H1 ; cette erreur conduit à la défaillance de l'injection aux joints des pompes primaires, donc à une fuite primaire. Si la source froide n'est pas restaurée à terme, un mauvais refroidissement entraînera la perte des pompes d'injection de sécurité basse pression, et par conséquent l'endommagement du cœur.

Cette séquence présente d'importantes incertitudes, notamment en ce qui concerne la tenue des matériels (joints, pompes) au-delà de leurs conditions de qualification. Le poids de cette séquence est de $5{\cdot}10^{-6}$/tranche × an, soit 10 % du résultat total.

5.2.3. Dilutions intempestives

Les accidents de dilution intempestive font partie de la famille des transitoires. Deux séquences significatives ont été mises en évidence :

– la première séquence est celle d'une dilution progressive se produisant dans l'état d (niveau primaire au plan médian des