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.

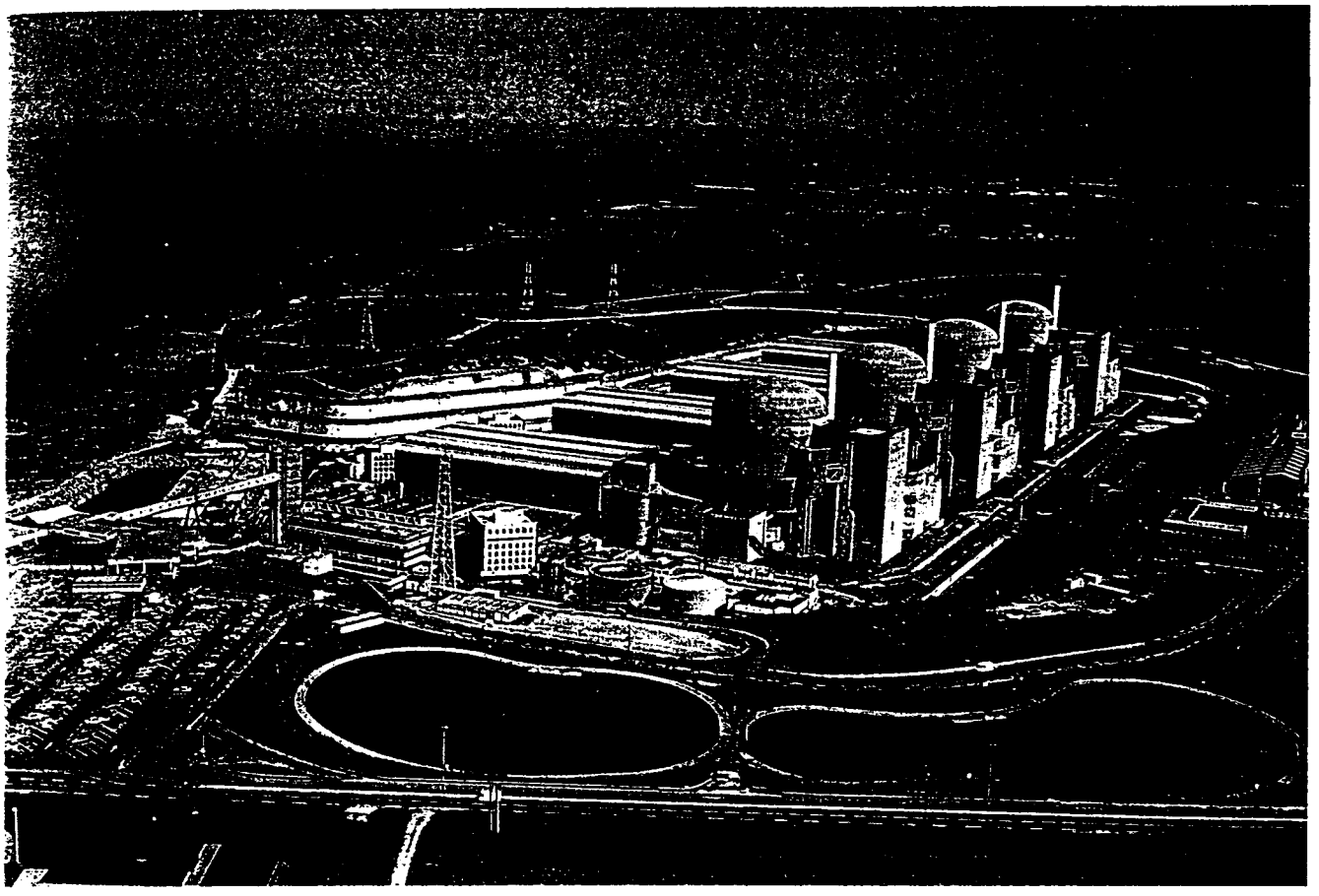
Ces études ont notamment permis d'évaluer la fiabilité et la disponibilité des systèmes de sûreté des centrales nucléaires, la probabilité de scénarios d'accidents, et d'aider à définir des spécifications techniques (notamment les délais de fonctionnement autorisés en cas d'indisponibilité partielle 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.

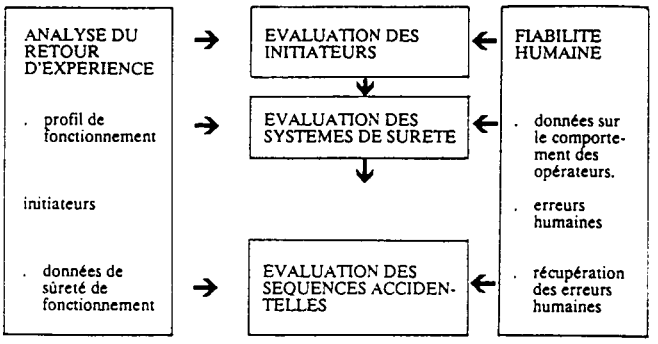


Fig. 2. – **Démarche générale des EPs 900 et 1 300.**

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-

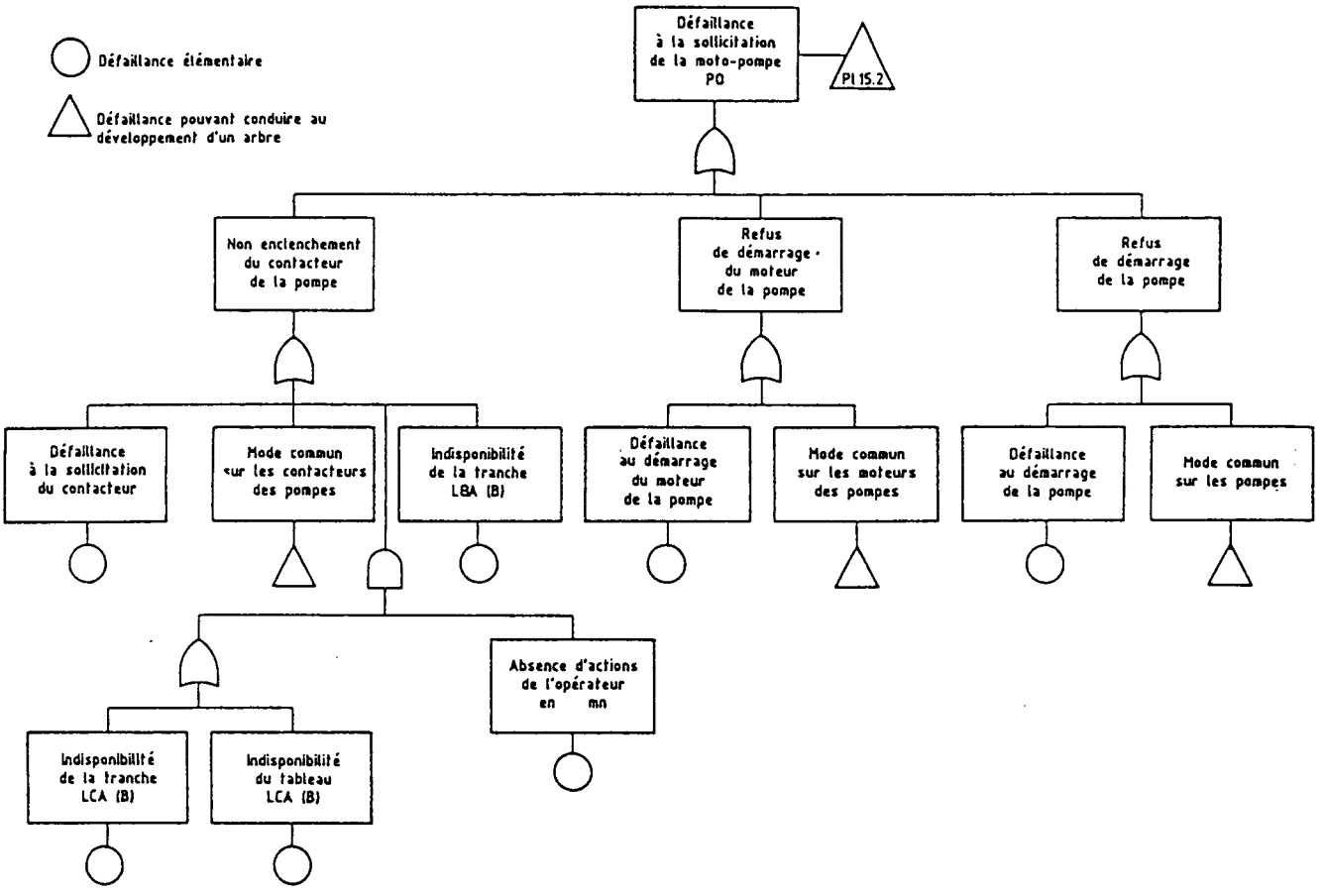
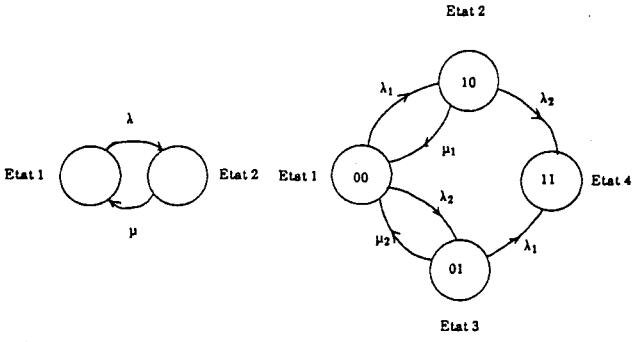


Fig. 3. — **Exemple d'un arbre de défaillance.**



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).

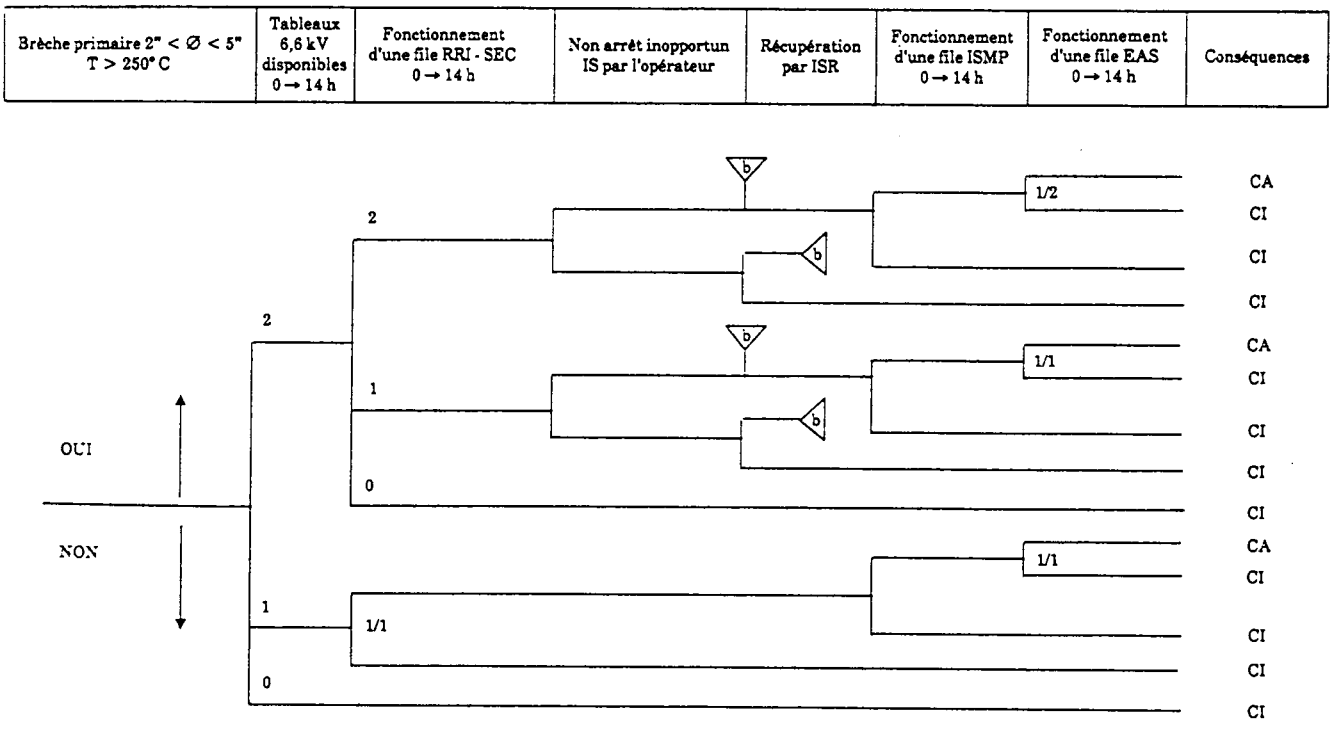
Dans le cas d'un système non redondant ou en redondance active (tous les composants fonctionnent simultanément) et lorsque le système est considéré comme non réparable (système inaccessible, contaminé par exemple), la méthode de l'arbre de défaillance est retenue.

• **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.**

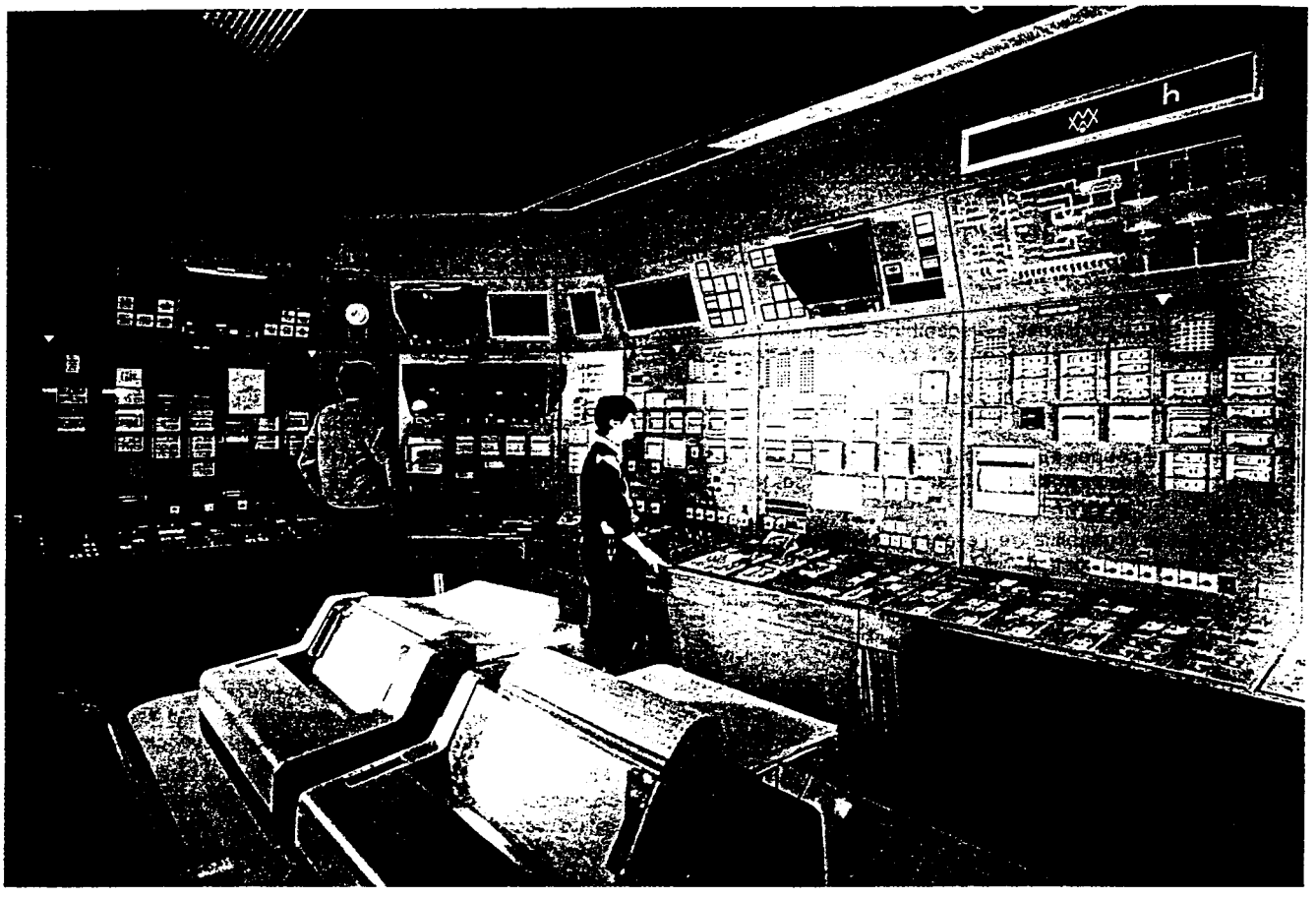


Fig. 6 - **Simulateur de formation d'EDF.**

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-

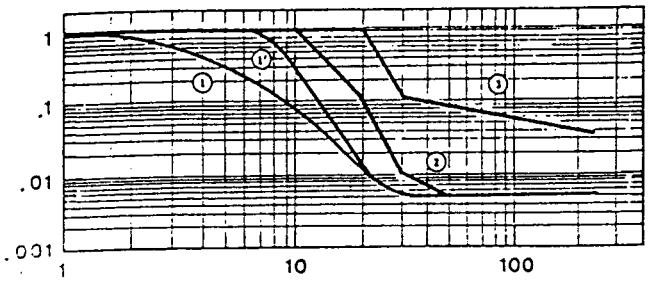


Fig. 7 - **Probabilité d'échec du diagnostic par l'opérateur.**

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 ;

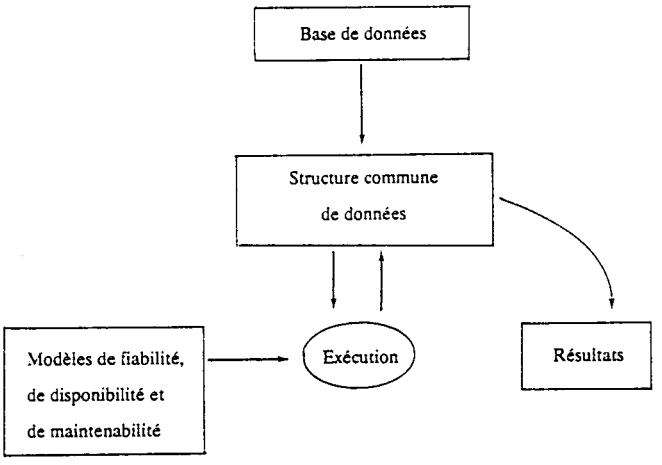


Fig. 8 - **Structure de LESSEPS.**

– 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

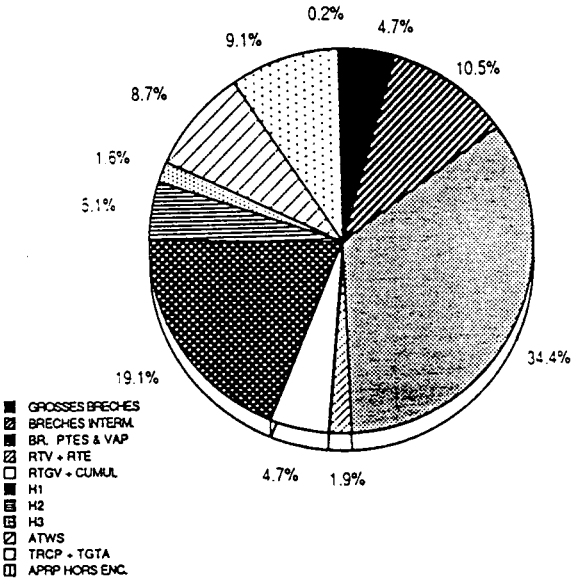
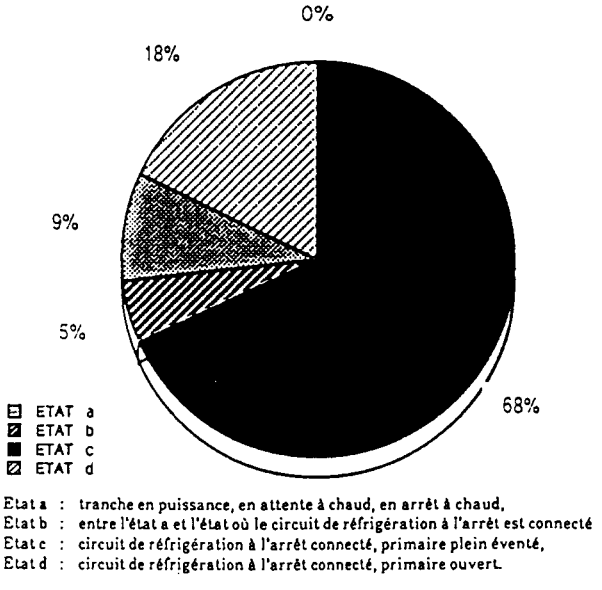


Fig. 9 - **EPS 900 : fréquence d'endommagement du cœur par famille d'initiateurs.**



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

boucles). Si l'opérateur n'intervient pas assez vite pour arrêter la dilution et effectuer un appoint, il y a ébullition de l'eau primaire et découvrement du cœur. La probabilité de la séquence est estimée à $3{,}2 \cdot 10^{-6}$/tranche × an ;

– la deuxième séquence, de probabilité $1{,}3 \cdot 10^{-6}$/tranche × an, est un cas de dilution brutale par un bouchon d'eau non borée qui peut se former pendant un arrêt des pompes primaires. L'arrivée brutale de ce front d'eau dans le cœur peut provoquer un accident de réactivité. Bien qu'il y ait de grandes incertitudes relatives aux phénomènes physiques, cette séquence a été jugée suffisamment importante pour qu'une modification des tranches ait été décidée par EDF durant le cours des études probabilistes.

5.2.4. Autres familles

Dans les autres familles, aucune séquence n'a une contribution supérieure à 10^{-6}/tranche × an. On peut néanmoins citer une séquence de poids plus faible ($8 \cdot 10^{-7}$/tranche × an) mais aux conséquences potentiellement graves : il s'agit d'une rupture de tube de générateur de vapeur, combinée avec une fuite secondaire et un échec du refroidissement. Une telle séquence conduit à l'endommagement du cœur avec by-pass de l'enceinte de confinement.

6. EPS 900 : enseignements

La fréquence totale d'endommagement du cœur est estimée à $5 \cdot 10^{-5}$/tranche × an. Bien qu'il soit difficile de comparer entre eux des résultats d'EPS, on peut signaler que ce chiffre se situe dans la fourchette des résultats généralement obtenus à l'étranger. Bien évidemment, la comparaison nécessite une analyse détaillée de toutes les hypothèses et données. En particulier, l'EPS 900 prend en compte les états du réacteur hors puissance, ainsi que les situations post-accidentelles à long terme, ce qui n'est pas le cas dans les études similaires.

Si l'on exclut les séquences accidentelles dans les états d'arrêt, et si l'on limite la durée des séquences à 24 h, la fréquence d'endommagement du cœur devient $2 \cdot 10^{-5}$/tranche × an. Il faut néanmoins rappeler que, dans son état actuel, l'EPS 900 ne tient pas compte des incendies ou inondations internes, ni des agressions externes, qui peuvent avoir une contribution significative.

Le résultat total se répartit entre un grand nombre de séquences et de familles. Aucune séquence ne contribue pour plus de 13 % au risque total. Ceci indique une certaine homogénéité de l'ensemble de la sûreté des tranches de 900 MWe.

6.1. Poids des états d'arrêt

Une constatation intéressante est le poids important des situations à l'arrêt, qui contribuent pour 32 % du chiffre total. Cette valeur élevée provient du fait qu'en général il n'y a pas d'automatisme pour faire face à une situation accidentelle et que l'intervention humaine est nécessaire. On peut cependant noter que l'incertitude associée est importante, tant sur la probabilité d'erreur humaine que sur la fréquence des initiateurs.

Notons que l'état e (arrêt pour rechargement piscine pleine) a une contribution négligeable au risque total.

6.2. Importance du facteur humain

Le facteur humain joue un rôle très important ; en effet, les séquences contenant au moins une erreur humaine contribuent pour près de 70 % au résultat. De plus, le facteur humain intervient aussi dans la probabilité de défaillance des systèmes et dans la fréquence des initiateurs. Cependant, il faut bien noter que, dans la plupart des cas, l'intervention humaine a été introduite comme la possibilité de restauration ou de récupération d'une situation dégradée, et la séquence conduisant à la fusion du cœur passe donc par l'échec de l'opérateur à effectuer cette restauration. Sans prise en compte du facteur humain, la probabilité de fusion du cœur serait plus élevée, et on ne peut pas conclure de façon simple que 70 % du risque est dû à des erreurs humaines.

On peut remarquer que le facteur humain a un poids particulièrement important dans les séquences pour lesquelles une action est nécessaire dns un délai court, comme dans le cas des brèches dans l'état d'arrêt pour intervention (état d) ou dans le cas de perte totale de la source froide (situation H1).

Les défaillances de cause commune ont une contribution dominante à la probabilité de défaillance des systèmes. ce qui était prévisible. Certains équipements non redondants comme la prise d'eau ont également un poids important.

6.3. Types d'endommagement de cœur possibles

Bien que l'étude ne traite pas actuellement du problème de la tenue de l'enceinte et des rejets de produits de fission, on peut cependant distinguer parmi les séquences d'endommagement du cœur trois types de situations aux conséquences potentiellement très différentes :

– les endommagements du cœur à basse pression dans le circuit primaire qui contribuent pour $3{,}8 \cdot 10^{-5}$ soit 77 % du résultat ;

– les endommagements à haute pression qui ont une probabilité de $9{,}5 \cdot 10^{-6}$ soit 18 % du total. Les contributions proviennent essentiellement des familles H2 (perte totale de l'eau alimentaire des générateurs de vapeur), H3 (perte totale des alimentations électriques secourues) et ATWS (transitoires avec échec de l'arrêt d'urgence). Il faut cependant préciser que cette estimation ne tient pas compte des actions de dépressurisation du circuit primaire prévues dans les procédures de gestion des accidents graves lorsque la fusion du cœur est inévitable. Il s'agit donc d'une évaluation pessimiste ;

– les endommagements du cœur avec by-pass de l'enceinte (perte de réfrigérant primaire extérieure à l'enceinte ou rupture de tube de générateur de vapeur cumulée avec une rupture de tuyauterie de vapeur) qui ont une probabilité de $2{,}4 \cdot 10^{-6}$ soit 5 % du total. Dans ce dernier cas, l'incertitude est particulièrement importante.

6.4. Prise en compte des actions de restauration

La prise en compte des actions de restauration définies dans les procédures accidentelles complémentaires H et ultimes U permet de réduire la probabilité d'endommagement du cœur de façon significative par rapport au niveau atteint par la seule utilisation des procédures événementielles I et A :

– les séquences de brèches avec défaillance de systèmes à long terme ont une contribution qui, bien que non négligeable, n'est pas dominante. Par contre, si l'on ne prend pas en compte le dispositif de secours mutuel des moyens de pompage entre injection de sécurité et aspersion dans l'enceinte qui permet également l'envoi d'eau dans le cœur par des moyens mobiles extérieurs (dispositif H4-U3), le risque à long terme est multiplié par un facteur de l'ordre de 10 et le risque total par un facteur 1,6 ;

– les moyens complémentaires relatifs à la procédure H3 de perte totale des alimentations électriques secourues (groupe turbogénérateur LLS - turbine à gaz) rendent négligeables les séquences conduisant à une fuite aux joints des pompes primaires ;

– la prise en compte de la procédure de refroidissement en « gavé-ouvert » (procédure H2) réduit la probabilité d'endommagement du cœur, en cas de perte d'alimentation des générateurs de vapeur, de plus d'un facteur 10 ;

– l'intervention de l'Ingénieur de Sûreté Radioprotection a été introduite dans tous les cas où les procédures SPI (Surveillance Permanente après Incident) et U1 peuvent permettre de récupérer une situation dégradée. L'introduction de l'ISR et des procédures SPI - U1 conduit à réduire d'un facteur 3 à 10 la probabilité d'un grand nombre de séquences, par exemple les séquences de petite brèche primaire ou de rupture de tube de générateur de vapeur avec défaillance de l'injection de sécurité à haute pression, et toutes les séquences impliquant une défaillance de l'alimentation de secours des générateurs de vapeur.

7. EPS 1 300 : Résultats

7.1. Résultats d'ensemble

La fréquence totale d'endommagement du cœur obtenue pour la tranche 3 de Paluel est de :

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

Les bornes de l'intervalle de confiance à 90 % sont les suivants :

$$[2{,}2\cdot10^{-6}/\text{tranche} \times \text{an} ;\ 2{,}1\cdot10^{-5}/\text{tranche} \times \text{an}]$$

Si l'on ne s'intéresse qu'à l'état de puissance (état a), la fréquence d'endommagement du cœur est égale à $4{,}7\cdot10^{-6}$/tranche × an.

Les contributions des familles d'initiateurs et des états sont données par les figures 11 et 12.

7.2. Commentaires sur les familles et séquences dominantes

Le tableau 2 présente la liste des dix séquences accidentelles prépondérantes.

Les trois premières séquences sont des brèches primaires dans les états d'arrêt à froid. On peut considérer que le poids de ces séquences est enveloppe, du fait des fréquences annuelles d'initiateurs prises en compte ; le taux horaire de brèche primaire est en effet le même dans ces états que dans l'état de puissance. Il faut noter qu'une fois l'initiateur survenu, le système d'injection de sécurité doit être mis en service par l'opérateur et une procédure de conduite existe actuellement sur les tranches en service pour couvrir cet accident ; en effet, dans la plupart des cas, la seule protection opérationnelle (haute pression enceinte) interviendrait trop tard.

Plusieurs séquences de dilution se traduisent par des risques non négligeables. La plus significative d'entre elles a conduit au lancement d'une modification qui est en cours de mise en œuvre sur les tranches. L'initiateur est une perte de l'alimentation électrique principale (conduisant à la perte des pompes primaires) pendant une dilution. Si l'opérateur n'arrête pas rapidement cette dilution, il peut y avoir formation d'une poche d'eau non borique. Cette poche, si elle n'est pas désagrégée lors du redémarrage d'une pompe primaire, est propulsée à travers le cœur. Cela conduit à l'endommagement des éléments combustibles par suite d'une redivergence.

Des incertitudes importantes subsistent sur les phénomènes physiques mis en jeu :

— lors de la création (ou non) de la poche d'eau (quel est l'impact du débit de thermosiphon ?) ;

— lors du démarrage de la pompe primaire (quel est le comportement de la poche ? n'est-elle pas désagrégée ?).

Pour améliorer la connaissance du comportement de l'installation, EDF a décidé de réaliser un programme d'essais. De plus, sans attendre les résultats, il a été décidé de mettre en œuvre sur les tranches un automatisme d'isolement de la dilution lors de la perte des pompes primaires ; les calculs probabilistes effectués dans l'EPS 1 300 sur cette séquence ont pris en compte l'existence de ce dispositif.

Un initiateur appartenant à la famille de la perte totale de la source froide s'est révélé également important : il s'agit de la perte du circuit de réfrigération à l'arrêt (RRA) quand la tranche est dans l'état d (RRA connecté, primaire ouvert). Ces séquences sont intéressantes à plus d'un titre mais leurs caractéristiques principales sont les suivantes :

— le délai est court entre la perte RRA et l'apparition de conséquences inacceptables : moins d'une heure quand le circuit primaire est peu ouvert ;

— la probabilité de perdre le RRA, au moins momentanément, n'est pas négligeable.

Il existe des procédures qui permettent à l'opérateur de conduire la tranche dans une telle situation. De plus, il a été mis en place des mesures de niveau adaptées qui devraient permettre de diminuer la fréquence de tels incidents et d'en faciliter le diagnostic.

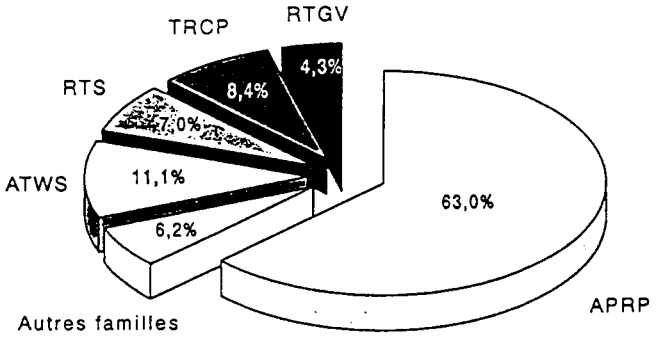
Les pertes de sources simples, clairement identifiées par des alarmes spécifiques, sont conduites grâce à des procédures spécifiques. Elles ne présentent pas de risque significatif. Compte tenu du retour d'expérience, EDF s'est plus particulièrement intéressé à deux types d'incidents :

— les dégradations lentes et progressives des tensions de contrôle-commande ;

— les cumuls de pertes de source électrique.

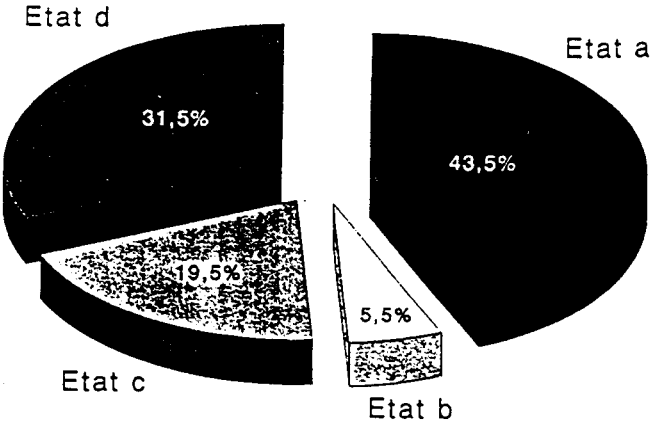
Le premier type d'incidents est déjà connu par un incident survenu en 1984 sur la tranche Bugey 5 ; compte tenu d'une dégradation progressive de tension continue non détectée immédiatement, des actionneurs ont manœuvré de façon intempestive. Les modifications réalisées tant au niveau des alarmes que des déclenchements automatiques des tableaux « sensibles » ont permis de ramener le risque résultant de ces incidents à des valeurs très faibles.

Dans le second type d'incidents, si l'on écarte certains cumuls conduisant à des conséquences graves mais de probabilité négligeable, il reste des initiateurs de type H3 (perte totale des alimentations électriques secourues) de fréquence globale égale à environ 10^{-6}/tranche × an. Compte tenu de l'existence de la procédure H3, on peut estimer que ces séquences conduisent à



APRP : accidents par perte de réfrigérant primaire
ATWS : transitoires suivis d'une défaillance de l'arrêt d'urgence
RTGV : ruptures de tube(s) de générateur de vapeur
RTS : ruptures de tuyauterie secondaire (eau ou vapeur)
TRCP : transitoires primaires
Autres familles : pertes de sources transitoires secondaires, perte de la source froide, perte totale de l'alimentation des générateurs de vapeur, perte totale des alimentations électriques secourues

Fig. 11 - **EPS 1 300 : 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. 12 - **EPS 1 300 : fréquence d'endommagement du cœur par état de la tranche.**

Tableau 2. — **Liste des dix séquences prépondérantes de l'EPS 1300.**

Famille d'initiateurs	Description succincte	Fréquence d'occurrence (par tranche × an)	Contribution au risque total
APRP	Brèche de 1" à 2" du circuit primaire (dans l'état d) suivie d'une non-mise en service par l'opérateur du système d'injection de sécurité	$1{,}45 \cdot 10^{-6}$	13,5
APRP	Brèche au pressuriseur (dans l'état c) suivie d'une non-mise en service par l'opérateur du système d'injection de sécurité	$1{,}14 \cdot 10^{-6}$	10,6
APRP	Brèche de 3/8" à 1" du circuit primaire (dans l'état d) suivie d'une non-mise en service par l'opérateur du système d'injection de sécurité	$7{,}7 \cdot 10^{-7}$	6,8
ATWS	Perte partielle du poste d'eau (la puissance de la tranche étant supérieure à 30% de la puissance nominale) suivie d'une défaillance de l'arrêt d'urgence	$5{,}9 \cdot 10^{-7}$	5,5
APRP	Brèche de 2" à 3" du circuit primaire (dans l'état d) suivie d'une non-mise en service par l'opérateur du système d'injection de sécurité	$5{,}8 \cdot 10^{-7}$	5,4
APRP	Brèche au pressuriseur (dans l'état b) suivie d'une non-mise en service par l'opérateur du système d'injection de sécurité	$4{,}6 \cdot 10^{-7}$	4,3
TRCP	Dilution dans l'état d qui n'est pas interrompue ou qui ne fait pas l'objet d'une mise en service de l'appoint par l'opérateur	$3{,}6 \cdot 10^{-7}$	3,4
RTGV	Rupture d'un tube de générateur de vapeur suivie d'une perte totale de l'alimentation de secours en eau puis d'un échec de mise en œuvre de la procédure U1 par l'ISR	$3{,}5 \cdot 10^{-7}$	3,3
APRP	Brèche de 3/8" à 1" du circuit primaire (dans l'état a) suivie d'un arrêt inopportun du système d'injection de sécurité par l'opérateur	$3{,}0 \cdot 10^{-7}$	2,8
RTS	Petite rupture de tuyauterie secondaire en eau suivie d'une perte du système d'alimentation de secours des générateurs de vapeur puis d'un échec de mise en œuvre de la procédure U1 par l'ISR	$2{,}6 \cdot 10^{-7}$	2,4

un risque très faible. Il faut toutefois remarquer les incertitudes importantes sur la quantification des erreurs humaines compte tenu de la complexité de telles situations. Ce genre de cumuls fait l'objet d'une réflexion qui sera poursuivie. En effet, il n'est pas possible de couvrir chaque cas de cumul par une procédure spécifique (trop de combinaisons). C'est notamment pour couvrir ces situations qu'une nouvelle approche de conduite est en cours de développement à EDF.

8. EPS 1 300 : enseignements

On distingue les enseignements relatifs à la conception et à l'exploitation des tranches nucléaires et ceux relatifs aux méthodes et à l'informatisation de l'EPS 1 300.

8.1. Enseignements relatifs à la conception et à l'exploitation

8.1.1. Les états d'arrêt du réacteur

Il convient d'approfondir un des enseignements majeurs de l'étude : le poids important des états d'arrêt. Il provient de plusieurs éléments :

— tout d'abord d'une incertitude : le taux horaire des brèches primaires dans ces états a été pris égal à celui retenu aux pressions et températures nominales du circuit primaire. Cela peut sembler conservatif. En réalité les ruptures sont souvent la conséquence de phénomène d'érosion ou de corrosion et surviennent plus souvent lors de transitoires que lors de régimes établis. A ce titre il n'a pu être démontré qu'à basse pression ou basse température, le taux de défaillance est sensiblement inférieur au taux défini par les conditions nominales ;

— mais aussi d'une réalité : dans les états d'arrêt, la tranche n'est pas complètement protégée par le démarrage automatique des systèmes de sauvegarde. En outre, des pompes sont débrochées pour la protection des personnes lors des opérations de maintenance. La conception actuelle des tranches est en effet basée sur le principe que les états d'arrêt sont peu dangereux ; à ce titre les systèmes et les automatismes ont généralement été conçus pour protéger les tranches en fonctionnement.

Il faut néanmoins souligner que cet enseignement n'est pas totalement nouveau. EDF étend largement aux états d'arrêt l'applicabilité des procédures de conduite accidentelle et des spécifications techniques d'exploitation. Cet effort devra être complété par une réflexion approfondie selon deux axes principaux :

— l'augmentation éventuelle du niveau d'automatisation ;

— la sensibilisation de l'exploitant au risque dans les états d'arrêt (formation).

Il convient en particulier de s'intéresser à l'état d (niveau du circuit primaire dans la plage de travail basse du RRA). L'inventaire en eau disponible est faible. Les délais dont dispose l'opérateur pour réagir sont courts et l'identification des incidents est souvent malaisée (nombreuses alarmes déjà présentes en salle de commande). Il faut en outre tenir compte du fait (difficilement quantifiable) que le personnel est souvent présent dans le bâtiment réacteur et à ce titre peut signaler directement en salle de commande l'impact des phénomènes (vapeur, etc.). La quantification des séquences présente donc une marge d'incertitude importante.

Enfin, le problème des états d'arrêt précédemment évoqué concerne bien entendu également les équipes de maintenance qui elles aussi doivent être sensibilisées et formées.

En outre, compte tenu de l'importance des défaillances de cause commune, l'organisation des interventions sur les voies A et B d'un même système devrait faire l'objet d'une réflexion toute particulière destinée à définir des axes d'amélioration.

8.1.2. Le facteur humain

C'est une évidence de dire que le facteur humain est important, encore faut-il définir précisément ce que cela signifie. Le poids des séquences où intervient au moins une erreur de conduite (mauvais diagnostic, non-réalisation d'une action, action trop tardive...) est d'environ 80% ; ceci ne tient pas compte d'autres erreurs (de type oubli d'une vanne en position fermée ou

erreur de maintenance) prises en compte au niveau des défaillances des systèmes élémentaires, ou de type « erreurs initiatrices ».

Ce chiffre de 80 % peut donner une image très négative des interventions humaines en cours d'accident. En fait, il doit être interprété à la lumière des éléments suivants :

— comme on l'a déjà souligné au paragraphe 6.4., ce que nous appelons « erreur » dans une étude de séquences n'est qu'un échec dans la récupération d'un accident ;

— si l'on calculait, de la même façon que pour les erreurs de conduite, le pourcentage des séquences incluant au moins une « défaillance matérielle » (rupture d'une tuyauterie, défaillance d'un composant) on arriverait à une proportion de 100 % dans la mesure où toute séquence conduisant à l'endommagement du cœur fait intervenir au moins une défaillance de matériel.

Le chiffre obtenu signifie donc simplement que l'opérateur a un rôle essentiel dans la récupération des accidents.

La réduction de la contribution de la conduite accidentelle, et plus généralement du facteur humain passe par une amélioration de l'interface homme-machine et de la formation, et, dans certains cas, par l'automatisation.

Les essais sur simulateur « MSR » et l'analyse systématique des consignes de conduite accidentelle réalisés pour l'EPS 1 300 ont permis d'identifier les difficultés potentielles d'utilisation des consignes. Leur importance a également pu être évaluée. Ces informations ont été utilisées lors de la révision des consignes. Les modifications ont principalement porté sur :

— la conception des « tests logiques » servant à orienter les opérateurs dans les consignes en fonction des valeurs des paramètres de la tranche ;

— la formation et la présentation des actions demandées ;

— la répartition des tâches entre les différents opérateurs ;

— la mise en évidence des actions-clés.

Des actions ont également été menées afin de réduire les délais d'appel de l'ISR par l'équipe de conduite en cas d'incident (notamment l'amélioration des dispositifs d'appel).

Des efforts importants sont consentis pour améliorer de façon permanente la compétence des opérateurs. L'EPS peut servir à parfaire cette formation. Ainsi, les instructeurs pourront faire approfondir aux stagiaires, aussi bien sur le plan théorique que sur le plan pratique (sur simulateur), les séquences prépondérantes ; néanmoins les modalités de cette formation sont bien évidemment à définir avec attention, ne serait-ce que pour éviter les effets de focalisation, par exemple.

8.1.3. L'apport des spécificités de la démarche de sûreté française

Il convient en premier lieu de citer les procédures. Même s'il est toujours difficile de chiffrer le gain apporté par la bonne application d'une procédure, il est indéniable que les procédures H améliorent sensiblement la sûreté des tranches françaises.

• H1 : permet de ramener le risque d'endommagement du cœur à une valeur faible malgré une fréquence d'initiateurs élevée ;

• H2 : le gavé-ouvert est maintenant largement utilisé pour tous les réacteurs à eau pressurisée ;

• H3 : le LLS (turbogénérateur entraînant une pompe et alimentant l'instrumentation indispensable) permet de poursuivre l'injection aux joints.

Il faut insister sur l'intérêt de la présence d'un ingénieur (ISR) appliquant une nouvelle technique de la conduite accidentelle : l'approche par états (SPI-U1) en complément de l'approche événementielle classique. Le gain global apporté par cette disposition (présence d'un ISR et des procédures SPI-U1 associées) est d'environ 6.

8.1.4. Aide à la décision en matière de Spécifications Techniques d'Exploitation

Les Spécifications Techniques d'Exploitation (STE) représentent un ensemble de règles que doit suivre l'exploitant pour assurer la sûreté des installations. Ainsi en cas de défaillance d'un matériel important pour la sûreté, les STE précisent la conduite à tenir en définissant un état de repli de la tranche et un délai pour atteindre cet état.

Ces délais de repli sont calculés conformément aux exigences de sûreté pour limiter l'accroissement du risque consécutif à une indisponibilité. L'établissement de ces délais est basé sur des calculs probabilistes. Les EPS sont des outils indispensables pour la détermination des STE ; les résultats obtenus, basés sur les données du retour d'expérience, doivent être accompagnés d'une analyse critique intégrant les aspects liés à l'exploitation et à la maintenance.

8.1.5. Aide à la définition des priorités d'études sur les matériels

Les résultats issus des études probabilistes peuvent aider à apprécier les poids relatifs des composants ou des systèmes dans le risque global. Ceci permettrait de hiérarchiser les efforts et de définir les axes d'études prioritaires.

Les activités menées dans le cadre de l'EPS 1 300 ont permis d'élaborer un ensemble complet de données de fiabilité établi à partir de l'analyse des fichiers nationaux et d'enquêtes spécifiques sur sites.

Il est nécessaire à présent d'étudier les possibilités de réactualisation de cette base de données. Ces études permettront d'apprécier des écarts dans le comportement des matériels ou des tendances d'évolution.

Parmi les axes de réflexion qui peuvent être dégagés, on peut citer également :

— l'amélioration des programmes de base de maintenance préventive : ces programmes ont un impact direct sur la fiabilité et doivent ainsi prendre en compte, d'une part la fiabilité spécifique constatée des matériels et son évolution potentielle, d'autre part le poids spécifique de ces matériels dans le risque global ;

— l'analyse des éventuels effets du vieillissement des composants : cet axe de travail est un axe difficile car les effets de la maintenance préventive ou corrective, voire des remplacements périodiques de composants ou de matériels, viennent contrebalancer les effets directs liés au vieillissement ; un programme de recherche est néanmoins lancé à EDF qui devra tenir compte de tous les facteurs entrant en jeu ;

— l'amélioration des programmes d'essais périodiques des matériels importants pour la sûreté : à l'origine, ces programmes ont été définis sur des bases déterministes et à partir des jugements d'experts ; les EPS pourront apporter ici des enseignements permettant d'améliorer et d'homogénéiser si nécessaire ces programmes d'essais, tant sur le plan des matériels concernés que sur les périodicités et/ou la nature des essais.

8.2. Enseignements relatifs aux méthodes et à l'informatisation

8.2.1. Méthodes

Les systèmes experts ont été utilisés pour l'évaluation de plusieurs systèmes de sûreté, thermohydrauliques et électriques. L'expérience a montré que l'ajout de missions supplémentaires était facilement effectué, le système expert générant rapidement les arbres de défaillance complémentaires à partir de la base commune de faits et de règles.

L'emploi pour la première fois dans une EPS de la méthode des graphes d'états a confirmé tout l'intérêt de la méthode pour la prise en compte fine du fonctionnement séquentiel et du caractère réparable des systèmes. Cette méthode oblige l'analyste à identifier tous les états de fonctionnement et de panne. Elle permet de prendre en compte des stratégies de maintenance complexe ; ainsi elle a permis de tenir compte de manière réaliste de l'existence d'un nombre d'équipes de réparateurs parfois inférieur au nombre de réparations à effectuer. En outre, elle donne généralement des résultats rigoureux et non approchés.

Les défaillances de cause commune ont été systématiquement prises en compte au niveau des composants élémentaires (pom-

pes, vannes, disjoncteurs, etc.) à l'aide d'une méthode spécifique. Les modèles comme les arbres de défaillance qui les intègrent sont devenus plus complexes ; cette complexité est restée néanmoins compatible avec les capacités de traitement des programmes de calcul. Ce niveau de prise en compte permet de tirer des enseignements précis sur l'importance des contributions des défaillances de cause commune et facilite les études de sensibilité aux données.

La méthode d'identification des erreurs humaines s'est révélée fort utile pour identifier des erreurs humaines susceptibles de se produire et difficiles à imaginer a priori sans méthode. Il a été possible d'évaluer le gain apporté par l'Ingénieur de Sûreté Radioprotection par une modélisation adéquate, très exigeante cependant en données pertinentes issues des centrales nucléaires ou des simulateurs. D'une manière générale, l'existence d'un retour d'expérience du comportement d'opérateurs sur simulateurs en situation incidentelle ou accidentelle (plus de deux cents essais) a considérablement aidé les analystes dans leurs travaux de modélisation et de quantification du comportement humain et a beaucoup contribué au réalisme de l'étude. La base de données de fiabilité humaine ainsi obtenue constitue une importante référence pour les études à venir. Néanmoins le jugement d'expert a une place significative tant au niveau des données que des modèles ; il serait important à l'avenir d'en réduire l'influence.

8.2.2. Informatisation

Le logiciel LESSEPS et les logiciels probabilistes associés sont apparus irremplaçables pour gérer la complexité de l'étude et tout particulièrement :

- les interactions entre la base de données et les très nombreux modèles ;
- les enchaînements entre codes de calcul ;
- le grand nombre de données de toute nature (3 000) ;
- le caractère modulaire des études.

Les logiciels LESSEPS 900 et LESSEPS 1 300 contiennent, pour chacun d'eux, environ 400 modèles d'arbres de défaillance et de graphes d'états ainsi que 200 arbres d'événements. Le nombre et l'ampleur de ces modèles invitent à lancer des réflexions méthodologiques sur les possibilités de simplifier les modèles. LESSEPS, grâce à sa structure, a permis de construire les modèles EPS 900 et 1 300, étude par étude ; les études de systèmes de sûreté et les études de séquences accidentelles ont été « entrées » successivement et le logiciel a fusionné les bases de données communes.

Ainsi il s'avère facile de rajouter une étude de système ou de séquences accidentelles.

LESSEPS 1 300 a confirmé son grand intérêt lors de la phase définitive ; l'ensemble des résultats de l'EPS 1 300 a été recalculé avec une nouvelle base de données issue de l'accord avec l'IPSN Le travail de calcul et d'analyse des nouveaux résultats a été accompli en moins de trois semaines, le calcul ayant été effectué en une journée.

En définitive, le logiciel LESSEPS permet de calculer et de gérer toute étude probabiliste nécessitant de combiner et d'enchaîner les nombreuses méthodes (et modèles) de la sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité et sécurité). Ces enseignements augurent bien de l'intérêt d'une adaptation en cours de LESSEPS à d'autres gammes d'ordinateurs et notamment aux stations de travail.

9. Comparaison entre les deux études

La comparaison des résultats des deux études montre que la différence entre les fréquences d'endommagement du cœur entre les REP 900 et 1 300 est proche du facteur 5, en faveur des tranches les plus récentes.

Cet écart n'est pas surprenant, même si on peut noter qu'il provient en partie de différences entre certaines données et hypothèses de modélisation.

La conception des tranches de 1 300 MWe a été faite, en effet, avec le souci d'améliorer la fiabilité et les performances de certaines fonctions dont on peut maintenant chiffrer le bénéfice. On peut noter parmi certaines de ces différences :

- l'aspiration des pompes du système d'injection à moyenne pression (REP 1 300) se fait directement dans les puisards de l'enceinte, assurant ainsi une redondance plus complète ;
- le système d'alimentation de secours des générateurs de vapeur des tranches de 1 300 MW comporte deux turbopompes ;
- l'indépendance des deux voies du circuit de réfrigération à l'arrêt est mieux assurée sur les tranches de 1 300 MWe ;
- l'automatisme d'isolement de la décharge du circuit de contrôle volumétrique et chimique (en cas de température élevée de l'eau du circuit primaire) protège les pompes du circuit qui aspirent alors l'eau froide de la bâche de réserve des piscines (bâche PTR).

On notera que ces améliorations s'adressent pour la plupart à des systèmes qui interviennent lors d'accidents initiés pendant la phase de fonctionnement. Ceci explique l'augmentation du poids des états d'arrêt dans le résultat global de l'EPS 1 300.

10. Conclusions et perspectives

L'importance des enseignements déjà tirés des EPS 900 et 1 300 montre l'intérêt du travail effectué par Electricité de France et l'Institut de Protection et de Sûreté Nucléaire dans le domaine des Etudes Probabilistes de Sûreté. Des avancées significatives dans la compréhension de la sûreté des réacteurs à eau sous pression ont été obtenues par rapport aux études équivalentes réalisées à l'étranger ; ces études apportent ainsi une contribution significative dans les domaines suivants :

- recherche de l'exhaustivité des séquences accidentelles ;
- prise en compte du facteur humain ;
- prise en compte de l'expérience d'exploitation ;
- mise en œuvre d'une informatisation complète.

La prise en compte des situations d'arrêt ainsi que des situations à long terme après un accident sont des éléments particulièrement novateurs et riches d'enseignements.

Bien que les résultats des études probabilistes dépendent à l'évidence des hypothèses utilisées, les valeurs de fréquence d'endommagement du cœur calculées pour les réacteurs à eau sous pression exploités en France, qui toutefois ne prennent pas en compte certaines agressions spécifiques, se situent, toutes choses égales par ailleurs, dans la fourchette basse des valeurs comparables à l'étranger.

En outre, les Etudes Probabilistes de Sûreté effectuées sur les tranches de 900 MWe et de 1 300 MWe constituent, d'une part, une base de connaissances importantes permettant d'aider à apprécier la sûreté des réacteurs à eau sous pression et en particulier à hiérarchiser les problèmes et, d'autre part, un outil de base et de référence pour des études ultérieures dont certaines nécessiterons des recherches et des développements importants. Ces EPS pourront notamment être utilisées dans les domaines suivants :

- réévaluation de la sûreté des tranches de 900 et de 1 300 MWe ;
- évaluation de la sûreté des tranches du palier N4 ;
- procédures de conduite en situation accidentelle ;
- spécifications techniques d'exploitation ;
- fiabilité des équipements.

L'effort sera poursuivi, d'une part, pour intégrer dans ces études les connaissances nouvelles qui seront générées par l'expérience d'exploitation et les études de sûreté et, d'autre part, pour en diminuer les incertitudes.

Enfin, les méthodes et les outils informatiques continueront à faire l'objet de développement et de recherches afin d'en améliorer les performances ou d'en réduire les limites.

En tout état de cause, l'étude sera révisée à l'avenir pour tenir compte de l'évolution de l'expérience d'exploitation des tranches REP et des connaissances nouvelles issues des études de fonctionnement.