EDF
Electricité de France

EPS 1300

Etude Probabiliste de Sûreté

d'une tranche du
Centre de Production Nucléaire de PALUEL (1300 MWe)

RÉSUMÉ

31 MAI 1990

ELECTRICITE DE FRANCE

DER
RNE
6, QUAI WATIER
78401 CHATOU
CEDEX
30.87.72.44

DPT
SPT
IMMEUBLE PB 26
92060 PARIS-LA-DEFENSE
CEDEX 57
49.02.01.11

DE
SEPTEN
12-14, AV. DUTRIEVOZ
69628 VILLEURBANNE
CEDEX
78.94.44.44

Etude Probabiliste de Sûreté de la tranche 3 du Centre de Production Nucléaire de PALUEL

RESUME

31 mai 1990

CHEFS DE PROJET

M. VILLEMEUR
Direction des Etudes et Recherches

M. BERGER
Direction de l'Equipement

MEMBRES DE L'EQUIPE EPS-1300

EDF - Direction de l'Equipement (DE) :
M. ANTONIUCCI, Mme BOURBONNAIS, M. CHAMBON, Mme DALIGAUT, MM. DESCOMBES, GIVAUDAN, HEROU, KAPPLER, PINET

EDF - Direction des Etudes et Recherches (DER)
M. MORONI, Mme ANCELIN
MM. ARENY, BOUISSOU, BOURGADE, CARRE, DERIOT, DEWAILLY, DUBREUIL-CHAMBARDEL, LE, MAGNE, MOLINERO, MOSNERON-DUPIN, Melle de SAINT-QUENTIN, Mme SALIOU, Melle VILLATTE, M. AUPIED, M. LANNOY

EDF - Direction de la Production et du Transport (DPT) :
M. DE GUIO, M. MESLIN
MM. BROGNIART, GAUTHIER, HEBEISEN, ZANETTI

FRAMATOME
Mme ELLIA-HERVY
M. FAUGERAS, Mme HERSKOVITZ

COMITE DIRECTEUR

Président : M. TANGUY Inspecteur Général pour la Sûreté Nucléaire à EDF

Membres :

. EDF - Direction de l'Equipement (DE)	:	MM. BACHER VIGNON puis REYNES
. EDF - Direction des Etudes et Recherches (DER)	:	MM. GODIN puis MENJON MALHOUITRE puis BOULOT
. EDF - Direction de la Production et du Transport (DPT)	:	MM. BERTRON puis MIRA NOC

COMITE TECHNIQUE

EDF - Direction de l'Equipement (DE)	:	M. BERGER
EDF - Direction des Etudes et Recherches (DER)	:	MM. VILLEMEUR MORONI Mme ANCELIN
EDF - Direction de la Production et du Transport (DPT)	:	MM. MESLIN puis DE GUIO
EDF - Inspection Générale pour la Sûreté Nucléaire (IGSN)	:	Mme CARNINO
FRAMATOME	:	Mme ELLIA-HERVY

RESUME

Auteurs LES CHEFS DE PROJET
et
MM. MORONI
DE GUIO
Mme CARNINO

Ce rapport est le résumé du Rapport de Synthèse de l'Etude Probabiliste de Sûreté d'une tranche du Centre de Production Nucléaire de PALUEL.

Rapport EDF - 31 mai 1990 (Auteurs : Les Chefs de Projet et MM. MORONI, DE GUIO, Mmes CARNINO, ANCELIN, BOURBONNAIS, MM. DUBREUIL-CHAMBARDEL, MOSNERON-DUPIN).

SOMMAIRE

Page

AVERTISSEMENT 7

0. PREAMBULE (OU QU'EST-CE QU'UNE EPS ?) 9

0.1. INTRODUCTION 9

0.2. CONTENU D'UNE ETUDE PROBABILISTE DE SURETE 11

1. PRESENTATION DE L'EPS-1300 13

1.1. BUTS ET OBJECTIFS GENERAUX DE L'EPS-1300 13

1.2. PRINCIPALES CARACTERISTIQUES ET SPECIFICITES 14

1.3. ORGANISATION ET MOYENS 16

1.4. QUALITE, ASSURANCE-QUALITE ET CONTROLE EXTERNE 17

2. RESULTATS 19

2.1. LES LIMITES DES ETUDES PROBABILISTES 19

2.2. RESULTATS D'ENSEMBLE 20

2.3. INTERPRETATION DES PRINCIPAUX RESULTATS 29

3. DONNEES 33

3.1. INTRODUCTION 33

3.2. PROFIL DE FONCTIONNEMENT 37

3.3. INITIATEURS 39

3.4. DONNEES DE FIABILITE DES COMPOSANTS 40

4. METHODES ET INFORMATISATION 43

4.1. METHODES 43

4.2. INFORMATISATION 50

5. FACTEURS HUMAINS 55

5.1. FACTEURS HUMAINS DANS LES EVALUATIONS DE SYSTEMES 55

5.2. FACTEURS HUMAINS DANS LES EVALUATIONS DE SEQUENCES ACCIDENTELLES 55

6. ENSEIGNEMENTS ET PERSPECTIVES 61

6.1. ENSEIGNEMENTS RELATIFS A LA CONCEPTION 61

6.2. ENSEIGNEMENTS RELATIFS A L'EXPLOITATION 63

6.3. ENSEIGNEMENTS RELATIFS AUX METHODES ET A L'INFORMATISATION 65

6.4. PERSPECTIVES 68

REFERENCE 69

ANNEXE 1 : Principaux sigles et abréviations figurant dans ce rapport

ANNEXE 2 : Résultats de l'EPS - 1300

ANNEXE 3 : Séquences accidentelles prépondérantes

AVERTISSEMENT

Ce document est un résumé du Rapport de Synthèse de l'Etude Probabiliste de Sûreté d'une tranche REP 1300 MWe (EPS-1300). De même que ce dernier, il présente les résultats et les enseignements de cette étude obtenus à la date du 31 mai 1990.

Des compléments d'analyse, relatifs à la séquence de perte totale du système de refrigération à l'arrêt lorsque le réacteur est en arrêt pour intervention, sont en cours. Leurs conclusions donneront lieu à une éventuelle actualisation de l'étude.

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.

0. PREAMBULE (OU QU'EST-CE QU'UNE EPS ?)

0.1. INTRODUCTION *

Une Etude Probabiliste de Sûreté (EPS) a été menée à partir de 1986, pendant une période de quatre ans, sur le Centre de Production Nucléaire (CPN) français de PALUEL. Ce CPN comprend quatre réacteurs nucléaires à eau pressurisée d'une puissance unitaire de 1 300 MWe qui ont été mis en service entre 1983 et 1987. La tranche n° 3 a été retenue comme objet de cette étude. Ce CPN est le premier du palier de 1 300 MWe et fait suite au palier de 900 MWe dont une quarantaine de réacteurs a été mise en service entre 1976 et 1989.

Une Etude Probabiliste de Sûreté d'un réacteur nucléaire a pour objet d'identifier tous les scénarios d'accident susceptibles de se produire avec endommagement du réacteur et d'en évaluer les fréquences d'occurrence. Ces scénarios d'accident, encore appelés séquences accidentelles, sont élaborés par des ingénieurs utilisant des méthodes appropriées ; ce sont généralement des successions de défaillances de systèmes ou/et d'erreurs humaines d'opérateurs comme le sont souvent dans la réalité les véritables accidents. Les accidents auxquels on s'intéresse sont ceux qui peuvent potentiellement endommager gravement le réacteur nucléaire - tout particulièrement le coeur du réacteur - et être source, si l'accident n'est pas maîtrisé, de rejets de produits radioactifs dans l'environnement.

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, leur durée de réparation ou les fréquences d'erreurs humaines sont déduites autant que possible de l'analyse du retour d'expérience des autres réacteurs nucléaires.

Imaginer le pire pour mieux le prévenir ! tels 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 tant au niveau de la conception que de l'exploitation d'une installation nucléaire.

Les premières évaluations probabilistes du risque lié à une installation industrielle furent menées sur des centrales nucléaires (un réacteur à eau pressurisée et un réacteur à eau bouillante) aux Etats-Unis et publiées en 1975 ; la première étude, effectuée à la demande des Autorités de Sûreté américaines dans un contexte de fort développement du nucléaire, fut dirigée par le professeur Rasmussen (rapport WASH-1400). Elle ouvrit le champ des Etudes Probabilistes de Sûreté (EPS) et des Etudes Probabilistes de Risque (EPR) ; alors que les EPS se limitent à l'évaluation des accidents compromettant la sûreté (exemple : fusion du coeur du réacteur), les EPR prolongent les EPS en cherchant à caractériser le risque que fait courir aux populations environnantes une telle installation : ce risque peut être caractérisé par la fréquence annuelle de décès (par mort immédiate, par cancer) de personnes des populations environnantes ou par toute autre mesure de dommage, à la suite d'un accident conduisant à une dispersion de produits radioactifs.

Basée sur des méthodes d'évaluation de la sûreté de fonctionnement des systèmes (c'est-à-dire de la fiabilité, disponibilité, maintenabilité, sécurité), développées auparavant dans les domaines industriels de pointe, cette première étude avait un caractère de prototype et d'action de recherche. Ses conclusions furent très critiquées par les Autorités de Sûreté américaines quelques années plus tard, compte tenu des importantes marges d'incertitude sur les données de fiabilité, le comportement humain, les défauts de cause commune et en conséquence sur les résultats ; néanmoins, les méthodes étaient recommandées compte tenu de leur intérêt.

A la suite de l'accident de la centrale nucléaire de Three Mile Island (1979) qui ne fit pas de victime mais suscita une forte émotion, les attitudes vis-à-vis des méthodes probabilistes de risque évoluèrent de nouveau. Notamment, on s'aperçut que le rapport "Rasmussen" avait mis en évidence un accident ressemblant par son scénario à celui de la centrale de Three Mile Island ; la

* Il convient de noter que l'annexe 1 définit les principaux sigles et abréviations figurant dans ce rapport.

commission créée par le Président des Etats-Unis à la suite de cet accident recommanda l'utilisation croissante des méthodes d'analyse probabiliste de risque dans le cadre de la sûreté nucléaire. La décennie des années 80 verra les études se multiplier dans la plupart des pays ayant des centrales nucléaires en construction ou en service.

Abordons maintenant le contexte à EDF ; dès le début des années 70, EDF et le support technique de l'Autorité de Sûreté française, l'Institut de Protection et de Sûreté Nucléaire (IPSN) expérimentèrent, à titre de recherche, les méthodes d'analyse probabiliste. Au lancement du programme électro-nucléaire en 1974, EDF entreprit un effort particulier de développement de ces méthodes et d'application à la centrale de Fessenheim, la première centrale nucléaire à eau pressurisée d'une puissance de 900 MWe qui fut mise en service à partir de 1977. La sûreté nucléaire repose en grande partie sur la fiabilité des systèmes de sûreté chargés de maîtriser des accidents pris en compte dans le dimensionnement des centrales nucléaires ; aussi les premières études furent-elles utilisées pour évaluer les points forts et faibles de la fiabilité des systèmes de sûreté et ceci dans un cadre de recherche et en dehors de tout aspect réglementaire.

De nombreuses considérations ont été tirées de ces études sur l'importance des systèmes de sûreté et sur leur niveau de fiabilité ; elles ont guidé le concepteur pour améliorer la fiabilité de ces systèmes sur la centrale de Fessenheim et les centrales suivantes. Par ailleurs, elles ont aussi conduit le concepteur à approfondir la démarche suivie et à prévoir des parades à certains accidents situés en dehors de la liste réglementaire des situations de dimensionnement. Ainsi, à titre d'illustration, citons la perte totale des alimentations électriques secourues qui deviendra une situation complémentaire de dimensionnement ; des parades particulières seront mises en oeuvre pour pallier cet accident.

Dès 1978 EDF mit en place le "Système de Recueil de Données de Fiabilité" (SRDF) sur les centrales nucléaires de Fessenheim et de Bugey ; ce système sera étendu à partir de 1983 à toutes les centrales nucléaires françaises à eau pressurisée. Cette banque a pour vocation de permettre un suivi aussi exhaustif que possible du comportement en exploitation d'un grand nombre de matériels ; cette connaissance permet d'en déduire des estimateurs des données de sûreté de fonctionnement.

A partir du début des années 1980, des évaluations probabilistes de sûreté furent systématiquement effectuées pour les centrales nucléaires de 900 MWe pour définir de manière rationnelle les règles d'exploitation en cas d'indisponibilité partielle des systèmes de sûreté ; des méthodes originales avaient été précédemment développées et mises au point. En effet, lorsqu'un système de sûreté est partiellement indisponible (exemple : perte d'une file alors que le système redondant en comporte deux) deux stratégies peuvent généralement se présenter : soit continuer à fonctionner dans certaines conditions, soit procéder à un arrêt. Les études probabilistes de sûreté permettent d'estimer les temps autorisés de fonctionnement des tranches en quantifiant les scénarios d'accident pertinents.

Pour le CPN de PALUEL, tête de série du palier de 1300 MWe, EDF a effectué (1981-83) des évaluations probabilistes de la fiabilité de tous les systèmes de sûreté, dans le cadre du processus réglementaire conduisant à l'autorisation de démarrage des centrales nucléaires.

Pour le projet de centrale nucléaire de 1400 MWe, EDF a entrepris (1983-86) des évaluations probabilistes de scénarios d'accident afin de démontrer que ceux qui débutent par des situations complémentaires respectent les objectifs fixés ; elles permettent ainsi de valider les choix faits dans la conception. De manière plus précise, la probabilité de fusion du coeur débutant par une situation complémentaire de dimensionnement (exemple : perte des alimentations électriques secourues) ne doit pas excéder en ordre de grandeur 10^{-7}/an par tranche. Pour ces études, des méthodes et des logiciels originaux furent développés.

Bien évidemment, toutes ces études furent examinées, discutées et entérinées par l'Autorité de Sûreté.

Ainsi, fin 1985, EDF pouvait se prévaloir d'une expérience importante dans le champ des évaluations probabilistes de sûreté, d'une grande maîtrise des méthodes et logiciels

correspondants, et également d'un important retour d'expérience d'un parc homogène de centrales nucléaires ; dans ce contexte, EDF décida de lancer à partir de janvier 1986 le projet EPS-1300, projet d'Etude Probabiliste de Sûreté de la tranche 3 du CPN de PALUEL. Le constructeur FRAMATOME des chaudières nucléaires françaises à eau pressurisée fut associé à ce projet dès son lancement.

Des objectifs ambitieux et originaux furent fixés :

- évaluation de la fréquence d'endommagement du coeur en identifiant tous les scénarios qui y contribuent ; cette évaluation devait être aussi détaillée que possible et couvrir tous les états standards du réacteur,

- fourniture d'un outil informatique (appelé LESSEPS et développé par EDF), aisément exploitable et permettant d'obtenir la réalisation d'une EPS "vivante", c'est-à-dire facilement révisable en fonction de l'évolution des données et des connaissances.

Ainsi, pour la première fois, une EPS "vivante" a été réalisée, gage d'une future utilisation aisée de cette étude grâce à l'existence d'un outil informatique contenant toutes les données et tous les scénarios d'accident identifiés et permettant d'en recalculer tous les résultats. Bien évidemment les données tirées du retour d'expérience des centrales nucléaires évolueront dans les prochaines années ; le logiciel LESSEPS aidera à en mesurer l'impact sur la sûreté des centrales nucléaires et sur les scénarios précédemment identifiés.

Une grande attention a été accordée à la qualité des travaux menés dans le cadre de l'EPS-1300 ; tout particulièrement, un contrôle externe de cette évaluation probabiliste de la sûreté a été assuré par l'IPSN. Notons que, par ailleurs, l'IPSN avait engagé une EPS sur une centrale du palier 900 MWe et qu'EDF en a effectué le contrôle externe ; on peut noter que l'IPSN utilise le logiciel LESSEPS pour l'EPS-900 depuis 1988.

Ainsi, d'une manière générale, dans le cadre du projet EPS-1300 ont été réalisés :

- des rapports techniques détaillant toutes les parties de l'étude, des données aux études de scénarios d'accident ; le volume de ces rapports est d'environ 15 000 pages,

- un logiciel (LESSEPS-1300) et la documentation associée.

Un Rapport de Synthèse du projet EPS-1300 a été élaboré [1] ; ce rapport en constitue le résumé.

Après une rapide description du projet, seront présentés et examinés les résultats de l'étude ainsi que les éléments principaux qui sous-tendent l'étude, à savoir les données, les méthodes, l'informatisation et les facteurs humains. Les enseignements marquants de l'étude et les perspectives sont abordés à la fin de ce rapport.

0.2. CONTENU D'UNE ETUDE PROBABILISTE DE SURETE

Une EPS comprend 3 grandes parties :

- l'évaluation probabiliste des initiateurs,
- l'évaluation probabiliste des systèmes de sûreté,
- l'évaluation probabiliste 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 coeur 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 (parfois la disponibilité ou la maintenabilité) des systèmes qui interviennent sur le plan de la sûreté. Les systèmes de sûreté sont généralement des systèmes redondants sollicités pour maîtriser les 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 (défaillance de matériel, erreur humaine lors de maintenance, etc.) 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 décroissante. Les éventuels points faibles de ces systèmes sont ainsi 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 menant à un accident grave c'est-à-dire à un accident endommageant le coeur 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. La séquence accidentelle sera donc une succession de défaillances de systèmes de sûreté ou/et de défaillances humaines.

Les défaillances de systèmes de sûreté sont liées aux échecs des missions identifiées dans la partie précédente.

Les défaillances humaines sont généralement des erreurs humaines commises durant la phase qui suit l'initiation de l'accident (exemples : erreur de diagnostic de l'accident, erreur dans l'application d'une procédure de conduite accidentelle).

1. PRESENTATION DE L'EPS-1300

1.1. BUTS ET OBJECTIFS GENERAUX DE L'EPS-1300

Deux buts ont été assignés au projet EPS-1300 ; ils sont inséparables et d'égale importance :

1 - évaluer la probabilité d'endommagement du coeur de la tranche n° 3 du CPN de PALUEL , dans tous ses états et ceci de manière aussi détaillée que possible ;

2 - fournir un logiciel d'évaluation, le logiciel LESSEPS-1300 afin de réaliser une EPS "vivante".

Ces buts précis s'apprécient en tenant compte des objectifs généraux poursuivis par ce projet afin d'en favoriser au maximum les retombées. Précisons maintenant les objectifs généraux qui ont fortement influencé ce projet et ses caractéristiques :

1 - évaluation de la démarche de sûreté française
Il s'agit de vérifier le niveau réel de sûreté des centrales nucléaires françaises. D'importantes améliorations de la sûreté ont été apportées à ces types de centrales tant au niveau de la conception (optimisation de la conception des systèmes de sûreté, prise en compte de situations complémentaires et de procédures ultimes, optimisation des procédures incidentelles et accidentelles...) qu'au niveau de l'exploitation (présence permanente d'un Ingénieur de Sûreté Radioprotection...).

Par la mise en évidence des points forts et des points faibles de la conception des systèmes ou fonctions de sûreté, cette étude devrait ainsi contribuer à apprécier la complétude et l'homogénéité de la démarche de sûreté française.

2 - Aide à la conception et à l'exploitation des centrales nucléaires
Les résultats du projet EPS-1300 doivent pouvoir être utilisés par les concepteurs et les exploitants des tranches nucléaires dans les domaines suivants :

. aide à la conception : l'évaluation de la démarche de sûreté française et l'existence d'un outil informatique d'évaluation devrait puissamment aider le concepteur pour les futurs réacteurs nucléaires envisagés (projet REP 2000),

. aide à l'exploitation : quatre principales utilisations devraient être envisagées dans l'avenir,

a) aide à la définition des spécifications techniques : les délais autorisés de fonctionnement en cas d'indisponibilité partielle fortuite de matériels de sûreté étant calculés à l'aide des méthodes probabilistes, le logiciel LESSEPS devrait permettre de les actualiser, compte tenu de l'évolution des données,

b) aide à l'analyse de l'évolution des données : le logiciel LESSEPS pourrait être utilisé pour mesurer l'impact de l'évolution des données sur le plan sûreté. Il n'est en effet pas toujours évident d'en juger la répercussion sur ce plan (exemple : taux de défaillance qui diminue, temps de réparation qui augmente). D'où l'intérêt de connaître la répercussion de cette évolution sur les probabilités de défaillance des systèmes, d'échecs des fonctions de sûreté et de fusion du coeur,

c) aide à l'amélioration des procédures de conduite : la mise en évidence des erreurs humaines envisageables et contribuant au risque permettra, si nécessaire, d'optimiser ces procédures,

d) aide à la formation des opérateurs : l'identification des scénarios d'accident les plus probables et des erreurs humaines envisageables pourra contribuer à orienter la formation des opérateurs.

1.2. PRINCIPALES CARACTERISTIQUES ET SPECIFICITES

1.2.1. CARACTERISTIQUES LIEES AU CONTENU DE L'ETUDE

- **Tranche nucléaire choisie :**
  Le CPN de PALUEL, tête de série du palier REP-1300 MWe 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-1300 et d'être la première tranche REP-1300 MWe sur laquelle certains matériels améliorant la sûreté (les soupapes SEBIM au pressuriseur par exemple) venaient d'être installés avant d'être généralisés aux autres tranches nucléaires.

- **Niveau d'étude :**
  L'EPS-1300 est, ce qu'il est convenu d'appeler, une étude de niveau 1, à savoir une étude ayant pour objet l'évaluation de la fréquence de la fusion du coeur du réacteur. La notion de fusion du coeur ou de conséquences inacceptables est définie par le biais de critères (propres à chaque famille d'initiateurs) permettant de simplifier les études : critère de gaine supérieure à 1204°C, dénoyage du coeur, etc. En cas d'accident, ces critères sont atteints avant le début de fusion du coeur : les études correspondantes présentent donc un certain degré de conservatisme. Ainsi, on évalue, en réalité, la fréquence annuelle d'endommagement du coeur de réacteur et il ne s'agit donc pas nécessairement de la fusion du coeur du réacteur.

  Dans le cadre de ce projet, il n'a pas été jugé opportun de poursuivre l'étude au niveau 2 (évaluation de la fréquence des divers types de rejets de produits-radioactifs hors de l'enceinte) et au niveau 3 (évaluation des risques vis-à-vis de l'environnement et des populations environnantes). En effet, l'existence de grandes incertitudes sur les phénomènes qui suivent une fusion du coeur limite actuellement l'intérêt d'une évaluation probabiliste des scénarios d'accident au-delà de la fusion du coeur pour l'aide à la conception ou à l'exploitation. Une étude de niveau 1 étant une étape obligée avant d'éventuels prolongements, il a donc paru prioritaire de réaliser une étude de niveau 1 de grande qualité et de grande ampleur afin d'en maximaliser les enseignements.

  Les agressions externes (inondations externes, chutes d'avions, risques liés aux activités humaines...) ont fait l'objet d'une démarche probabiliste dès la conception afin qu'elles ne représentent qu'un risque résiduel.

  Les agressions internes (exemples : incendies, inondations) n'ont pas été prises en compte dans l'étude ; des travaux de recherche méthodologique sont néanmoins en cours dans ce domaine, compte tenu des problèmes très spécifiques posés par la prise en compte de ces agressions dans les EPS.

- **Etats du réacteur :**
  Le risque est étudié dans tous les états de la tranche, 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 ont été en partie développées, avant le projet EPS-1300, dans le cadre des évaluations probabilistes des situations complémentaires qui avaient déjà traité tous les états du réacteur.

- **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 : en effet, les ISR sont spécialement formés à la sûreté nucléaire et à la maîtrise des accidents. Ils assurent ainsi, par rapport à l'équipe de quart, une véritable redondance humaine d'autant plus efficace qu'ils interviennent

sur la base d'un panneau de contrôle et de procédures (Surveillance Permanente après Incident -SPI- et refroidissement ultime du coeur - U1) qui leur sont spécifiques.

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 post-accidentelle 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 (déjà citée) et U_3 (secours des systèmes d'injection de sécurité et d'aspersion de l'enceinte par du matériel mobile) sont prises en compte.

1.2.2. CARACTERISTIQUES LIEES AUX METHODES RETENUES

Deux contraintes ont fortement influencé le choix des méthodes retenues et leur condition d'utilisation, à savoir les nécessités :

- de réaliser une EPS de grande ampleur (exemple : prise en compte de tous les états du réacteur) et très détaillée (exemple : prise en compte des défaillances de cause commune au niveau des composants élémentaires) : il en résulte l'obtention de très nombreuses modélisations d'événements indésirables à l'aide de méthodes fort diverses (exemples : arbre de défaillance, arbre d'événements, graphe d'états...). Cette dernière méthode a été retenue pour permettre une prise en compte fine et réaliste de la maintenance, même si elle complique notablement la modélisation globale,

- d'informatiser l'ensemble de l'EPS-1300, le logiciel LESSEPS 1300 devant permettre à la fois le calcul de l'EPS-1300 et les futures études de sensibilité aux données. Pour ces dernières, afin de faciliter le plus large spectre d'études, les modélisations devaient être aussi fines que possible. Rappelons que cet objectif augmente considérablement la complexité de l'étude : en effet, d'habitude pour faciliter le traitement des modélisations par les logiciels d'évaluation probabiliste, les modélisations traitent des macro-composants (ensemble de composants ayant certaines propriétés) qui rendront cependant plus complexes les études de sensibilité. D'où l'option, dans ce projet, de modéliser les défaillances (y compris les défaillances de cause commune) au niveau des composants élémentaires.

  Les modélisations de grande taille qui en résultent nécessitent d'utiliser des logiciels d'évaluation probabiliste très performants dans le cadre de LESSEPS-1300. En outre, l'objectif de réaliser de manière aisée des études de sensibilité aux données a imposé une architecture logicielle de LESSEPS-1300 permettant de ne relancer que les calculs strictement indispensables.

De plus, une grande attention a été accordée aux points faibles reconnus comme tels dans ces évaluations, à savoir les défaillances de cause commune et la fiabilité humaine :

- les défaillances de cause commune : un effort a été fait pour identifier ces défaillances qui sont souvent à la limite du savoir-faire actuel, effort enrichi par une analyse systématique de ces défaillances dans l'expérience française. Puis une innovation a été réalisée en prenant en compte ces défaillances au niveau des composants élémentaires par l'adaptation de la méthode dite des chocs,

- la fiabilité humaine : une méthode performante a été mise au point pour identifier des erreurs humaines susceptibles d'être commises ; cette méthode est basée sur les dernières méthodes proposées et expérimentées sur le plan international.
  Là aussi ces méthodes se sont appuyées sur l'analyse d'un retour d'expérience sans précédent au niveau des simulateurs de formation. Rappelons qu'EDF les utilise depuis de nombreuses années pour simuler des incidents ou accidents avec de véritables équipes de quart, dans des conditions aussi réalistes que possible ; les données de toute nature (temps de diagnostic, type

d'erreur humaine commise, fréquence d'erreurs...) tirées de l'observation du comportement des opérateurs ont été très largement utilisées dans l'EPS-1300.

1.2.3. CARACTERISTIQUES LIEES AUX DONNEES INTRODUITES

La quasi-totalité des données utilisées dans l'EPS-1300 sont issues de l'analyse de l'expérience d'EDF liée aux centrales REP en exploitation.

Dès 1986 l'important retour d'expérience accumulé pour les centrales REP, représentant environ 200 années x 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, Fichier de Données Statistiques...) Des enquêtes sur sites ont également été menées pour compléter ces données et tenir compte des spécificités du site étudié ; des sytèmes 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.

1.3. ORGANISATION ET MOYENS

La lourdeur des moyens requis, l'étalement inévitable sur plusieurs années, la mise en oeuvre de nombreuses techniques (fonctionnement en situation accidentelle, sûreté de fonctionnement, statistiques, facteurs humains, informatique...), impliquant le recours à de nombreux spécialistes d'unités différentes, le contrôle externe par l'IPSN, tout a concourru à ce qu'une grande attention soit accordée, dès le lancement du projet, à l'organisation mise en place pour le mener à bien.

Ce projet a été conduit par EDF, la société FRAMATOME ayant été associée à des tâches spécifiques.

L'étude a été assurée par une équipe intégrée, constituée d'ingénieurs des différentes Directions d'EDF concernées, à savoir :

- la Direction de l'Equipement (DE) : Service Etudes et Projets Thermiques et Nucléaires (SEPTEN),

- la Direction des Etudes et Recherches (DER) : Service Réacteurs Nucléaires et Echangeurs (RNE),

- la Direction de la Production et du Transport (DPT) : Service de la Production Thermique (SPT).

Dans son rôle de maître d'ouvrage, le SEPTEN a été assisté par un Comité Directeur, présidé par l'Inspecteur Général pour la Sûreté Nucléaire et comprenant des représentants de la DE, de la DER et de la DPT.

Dans son rôle de maître d'oeuvre, le Service RNE a été assisté par un Comité Technique ; deux Chefs de Projet ont assuré le pilotage du projet EPS-1300.

D'importants moyens humains et financiers ont été consacrés à l'EPS-1300 ; précisons les moyens humains (ingénieurs de l'EDF et de FRAMATOME) engagés dans les grandes tâches de l'EPS-1300 (de 1986 à 1990).

TACHES	MOYENS HUMAINS
Evaluation Probabiliste	≃ 30 I x AN
Analyse du Retour d'Expérience	≃ 10 I x AN
Logiciel LESSEPS-1300	≃ 10 I x AN

Ces moyens humains se sont répartis de la manière suivante sur environ cinq ans :

	1986	1987	1988	1989	1990
MOYENS HUMAINS	≃ 13 I x AN	≃ 13 I x AN	≃ 13 I x AN	≃ 10 I x AN	1 I x AN

Ainsi un effort d'environ 50 ingénieurs x an a été effectué et le coût du projet EPS-1300 peut être évalué à environ 50 MF.

1.4. QUALITE, ASSURANCE-QUALITE ET CONTROLE EXTERNE

Une grande attention a été accordée à la construction de la qualité de l'EPS-1300. Citons les principaux facteurs de qualité de type organisationnel, les autres facteurs techniques ayant été décrits par ailleurs :

- L'équipe EPS-1300 a fait appel aux spécialistes des diverses disciplines concernées (fonctionnement accidentel, sûreté de fonctionnement, évaluation probabiliste, statistiques, sûreté en conception, sûreté en exploitation, informatique...). La présence d'un ingénieur d'exploitation de la centrale de PALUEL qui s'est consacré à temps plein aux enquêtes spécifiques à PALUEL a beaucoup contribué au réalisme de l'étude.

- L'organisation mise en place (Comité Directeur, Chefs de Projets, Comité Technique, équipe) a contribué à bien définir les niveaux de responsabilité et à permettre aux divers points de vue de s'exprimer et de se compléter.

- L'existence de trois phases successives dans le projet EPS-1300 (phases préliminaire, provisoire et définitive) a permis de réactualiser et de compléter les études de manière structurée et ordonnée en tenant compte des avis ou des critiques formulés par de nombreuses unités.

- Un contrôle externe a été effectué par l'IPSN .

En ce qui concerne l'écriture et la diffusion des rapports techniques de l'EPS-1300, une procédure d'Assurance Qualité (AQ) a été mise en place en plus des procédures propres à chaque Direction ; ainsi les rapports techniques étaient soumis à la procédure d'AQ de la Direction concernée et à la procédure qui suit.

On distingue trois niveaux d'acteurs de l'AQ pour l'EPS-1300 :

- Premier niveau : c'est l'équipe rédactionnelle qui après un auto contrôle diffuse un rapport en prédiffusion pour avis. Après recueil des avis, une fois signée par les deux chefs de projet, le rapport est diffusé.

- Deuxième niveau : c'est le Comité Technique. Ce niveau est responsable des actions formalisées au titre de l'AQ et dénommées vérifications indépendantes. Le contrôle externe par l'IPSN entre dans cette catégorie.

- Troisième niveau : c'est le Service RNE (DER) qui contrôle le bon déroulement de la procédure.

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 cet organisme dans les différentes phases de l'EPS-1300.

Compte tenu de la réalisation par l'IPSN d'une étude équivalente, l'EPS-900, un Comité de liaison comprenant des responsables des deux études s'est régulièrement réuni à partir de 1986. Dans ce cadre, les remarques formulées par l'IPSN sur les rapports techniques EPS-1300 ont été régulièrement discutées.

Après discussion et approbation des rapports de méthodes d'analyse (notamment ceux sur la prise en compte des défaillances de cause commune et des facteurs humains) en 1986 et 1987, les discussions ont porté sur les rapports d'évaluation probabiliste et le jeu de données. Les rapports d'évaluation probabiliste ont été examinés deux fois par l'IPSN, dans la phase préliminaire et dans la phase provisoire. En outre un jeu de données approuvé par l'IPSN a été obtenu en juin 1989.

Compte tenu des remarques formulées par l'IPSN lors des deux phases (préliminaire et provisoire), sur la base du jeu de données approuvé, la troisième phase et dernière phase de l'EPS-1300 s'est déroulée de juillet à décembre 1989. Les résultats de l'EPS-1300 présentés dans ce rapport sont ceux de cette dernière phase.

2. RESULTATS

2.1. LES LIMITES DES ETUDES PROBABILISTES

On ne peut présenter les résultats de l'EPS-1300 sans dire quelques mots des difficultés rencontrées dans l'étude, non pas les difficultés bien naturelles inhérentes à tout projet important mais celles résultant des cas où l'on se heurte aux limites de la connaissance : limites méthodologiques, connaissance limitée des phénomènes physiques... On peut d'ailleurs remarquer que ce ne sont pas généralement des problèmes dus à l'aspect probabiliste des études mais des problèmes induits par les difficultés de modélisation d'un matériel, d'un système, du comportement de la tranche.

2.1.1. LES INITIATEURS

Seuls les incidents d'origine interne ont été traités. Les initiateurs tels les incendies, les inondations, les agressions externes n'ont pas été étudiés. Rappelons cependant que la démarche suivie à la conception vis-à-vis des agressions externes liées à l'activité humaine est de nature probabiliste et que les estimations réalisées font apparaître que le risque dû à ces initiateurs est faible.

Pour d'autres initiateurs tels le séisme, la démarche suivie par EDF à la conception est déterministe ; dans l'état actuel des connaissances les évaluations probabilistes qui pourraient être faites seraient fort longues et trop imprécises pour qu'un réel enseignement puisse en être tiré.

Par ailleurs, il subsiste le problème bien connu de l'exhaustivité des initiateurs. Malgré l'effort très important fourni dans ce domaine tant au niveau des recherches bibliographiques que dans l'analyse du retour d'expérience des tranches 900 MWe et 1300 MWe il n'est pas possible de garantir que tous les initiateurs sont étudiés (par exemple, pour les cumuls de perte de source électrique) ; d'où l'intérêt à l'avenir, d'une part, d'une recherche des précurseurs d'accidents par l'analyse du retour d'expérience et, d'autre part, d'une révision de l'EPS-1300 en fonction de ces enseignements.

2.1.2. LES INCERTITUDES

Elles interviennent à plusieurs niveaux :

- problèmes liés aux données :

* certaines fréquences d'occurrence d'initiateurs sont difficiles à quantifier :

  . les grosses brèches,
  . les cumuls (ruptures de tuyauterie vapeur et de tube de générateur de vapeur, ruptures multiples de tubes de générateur de vapeur, pertes de sources électriques,...),
  . la perte de la source froide.

* le jugement de l'ingénieur (tant au niveau de la collecte qu'au niveau de l'analyse des données de fiabilité) ne peut être totalement éliminé,

* les données relatives aux défaillances de cause commune et aux erreurs humaines font l'objet d'importantes incertitudes.

- problèmes liés aux hypothèses fonctionnelles : la modélisation elle-même est souvent rendue difficile parce que la réalité est complexe ou mal connue : dans ce dernier cas, la modélisation retenue est toujours enveloppe de la réalité. Dans le cadre de l'EPS, des études complémentaires

ont été réalisées sur certaines séquences pour affiner la connaissance physique des phénomènes : cela a permis de réduire les marges d'incertitude fonctionnelle.

L'ensemble de ces éléments doit en être pris en compte dans les conclusions que l'on peut tirer de ces études.

Notons d'ores et déjà que les incertitudes liées aux données ont fait l'objet d'un calcul : la connaissance (sous forme d'une distribution statistique) des incertitudes sur ces données permet d'en déduire les incertitudes qui pèsent sur la fréquence calculée d'endommagement du coeur.

2.2. RESULTATS D'ENSEMBLE

La fréquence annuelle d'endommagement du coeur sur la tranche 3 de PALUEL est de l'ordre de

10^{-5} /tranche x an

pour l'ensemble des initiateurs internes retenus.

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

[2,2 10^{-6}/tranche x an ; 2,1 10^{-5}/tranche x an]

Les bornes de cet intervalle sont telles que la vraie valeur de la fréquence annuelle d'endommagement du coeur a 90 chances sur cent d'appartenir à cet intervalle.

Dans les paragraphes suivants on explicite les contributions à ce risque des différentes familles d'initiateurs selon les divers états du réacteur. Ensuite, afin de mieux interpréter ces résultats, sont examinés certains facteurs qu'il paraît intéressant de regrouper par thèmes :

- les états d'arrêt du réacteur,
- les poids des erreurs de conduite,
- les incertitudes,
- l'apport des spécificités de la démarche de sûreté française,
- les systèmes de sûreté,
- les différents modes de fusion du coeur.

Avant de présenter ces résultats détaillés, il convient de rappeler que tous les événements initiateurs ont été regroupés selon 10 familles d'initiateurs :

- 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
- PDS : pertes de sources
- TGTA : transitoires secondaires

- TRCP : transitoires primaires
- H1 : perte totale de la source froide
- H2 : perte totale de l'eau alimentaire des générateurs de vapeur
- H3 : perte totale des alimentations électriques secourues

En outre, cinq états initiaux de la tranche ont été considérés (voir chapitre 3.2.1.). Ce sont les états suivants :

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

Par commodité, l'état a sera qualifié "état en puissance ou à l'arrêt à chaud" et les autres états (b, c, d,e) "états d'arrêt".

2.2.1. RESULTATS SELON LES ETATS ET LES FAMILLES D'INITIATEURS

La répartition de la fréquence annuelle d'endommagement du coeur selon les états et les familles d'initiateurs figure dans les deux tableaux qui suivent. Elle est également illustrée par les figures 1 et 2 ci-après.

<table>
<tr><td colspan="5">Fréquence d'endommagement du coeur
dans l'état initial considéré (/tranche x an)</td></tr>
<tr><td>Etat en puissance
ou à l'arrêt à chaud</td><td colspan="4">Etats d'arrêt</td></tr>
<tr><td>état a</td><td>état b</td><td>état c</td><td>état d</td><td>état e</td></tr>
<tr><td rowspan="2">$4,7\ 10^{-6}$</td><td>$5,8\ 10^{-7}$</td><td>$2,1\ 10^{-6}$</td><td>$3,4\ 10^{-6}$</td><td>//</td></tr>
<tr><td colspan="4">Pour tous les états d'arrêt $6,1\ 10^{-6}$</td></tr>
<tr><td colspan="5">Pour tous les états de la tranche $1,08\ 10^{-5}$</td></tr>
</table>

Note : // signifie négligeable

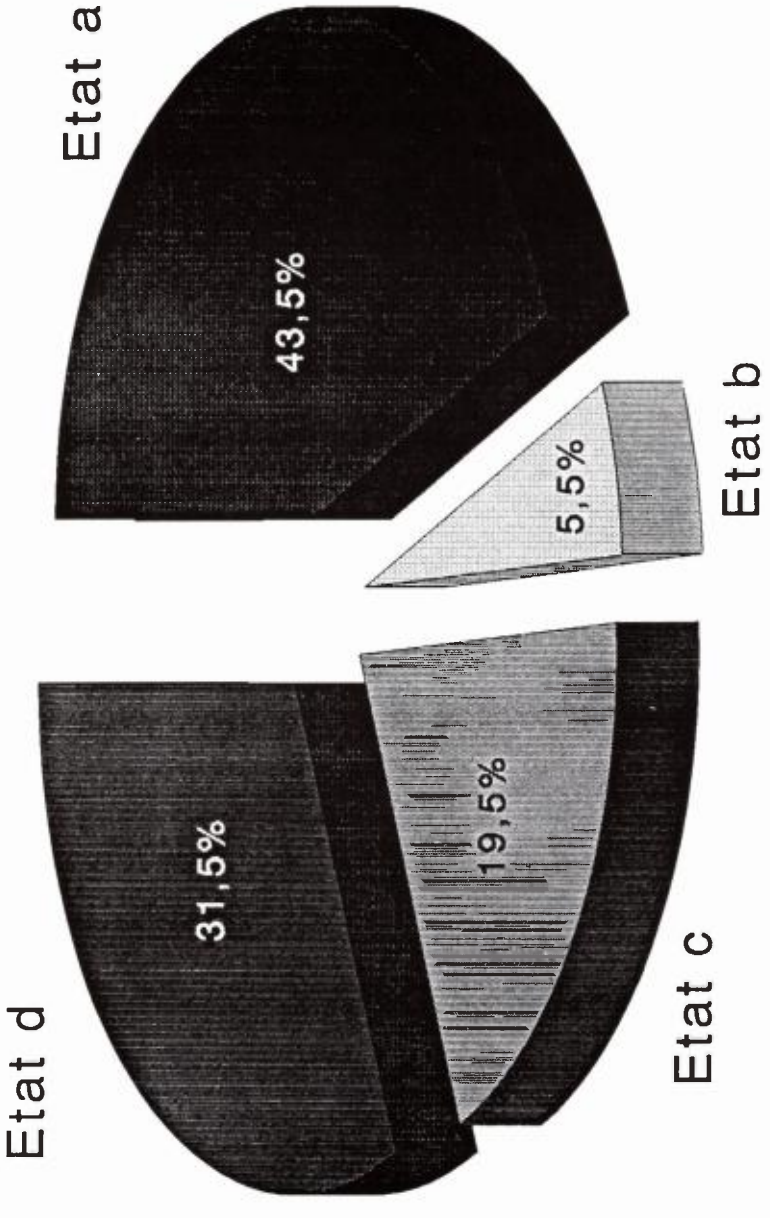
Dans le tableau ci-après, les familles d'initiateurs y sont classées par contribution décroissante.

Famille d'initiateurs	Fréquence d'endommagement du coeur dans l'état initial considéré (/tranche x an)		
	Etat en puissance ou à l'état d'arrêt à chaud	Etats d'arrêt	Total par famille
Accidents par perte de réfrigérant primaire (APRP)	$1,5\ 10^{-6}$	$5,3\ 10^{-6}$	$6,8\ 10^{-6}$
Transitoire suivis d'une défaillance de l'arrêt d'urgence (ATWS)	$1,2\ 10^{-6}$	//	$1,2\ 10^{-6}$
Transitoires primaires (TRCP)	$2,4\ 10^{-7}$	$6,7\ 10^{-7}$	$9,1\ 10^{-7}$
Ruptures de tuyauterie secondaire : eau ou vapeur (RTS)	$7,6\ 10^{-7}$	$5,7\ 10^{-9}$	$7,6\ 10^{-7}$
Ruptures de tube(s) de générateur de vapeur (RTGV)	$4,6\ 10^{-7}$	$1,2\ 10^{-9}$	$4,6\ 10^{-7}$
Perte totale de l'eau alimentaire des générateurs de vapeur (H2)	$2,5\ 10^{-7}$	$1,0\ 10^{-8}$	$2,6\ 10^{-7}$
Pertes de sources (PDS)	$1,3\ 10^{-7}$	//	$1,3\ 10^{-7}$
Perte totale de la source froide (H1)	$8,7\ 10^{-8}$	$3,3\ 10^{-8}$	$1,2\ 10^{-7}$
Perte totale des alimentations électriques secourues (H3)	$2,5\ 10^{-8}$	$4,7\ 10^{-8}$	$7,2\ 10^{-8}$
Transitoires secondaires (TGTA)	$4,5\ 10^{-8}$	//	$4,5\ 10^{-8}$
Toutes familles confondues	$4,7\ 10^{-6}$	$6,1\ 10^{-6}$	$1,08\ 10^{-5}$

Note : // signifie négligeable

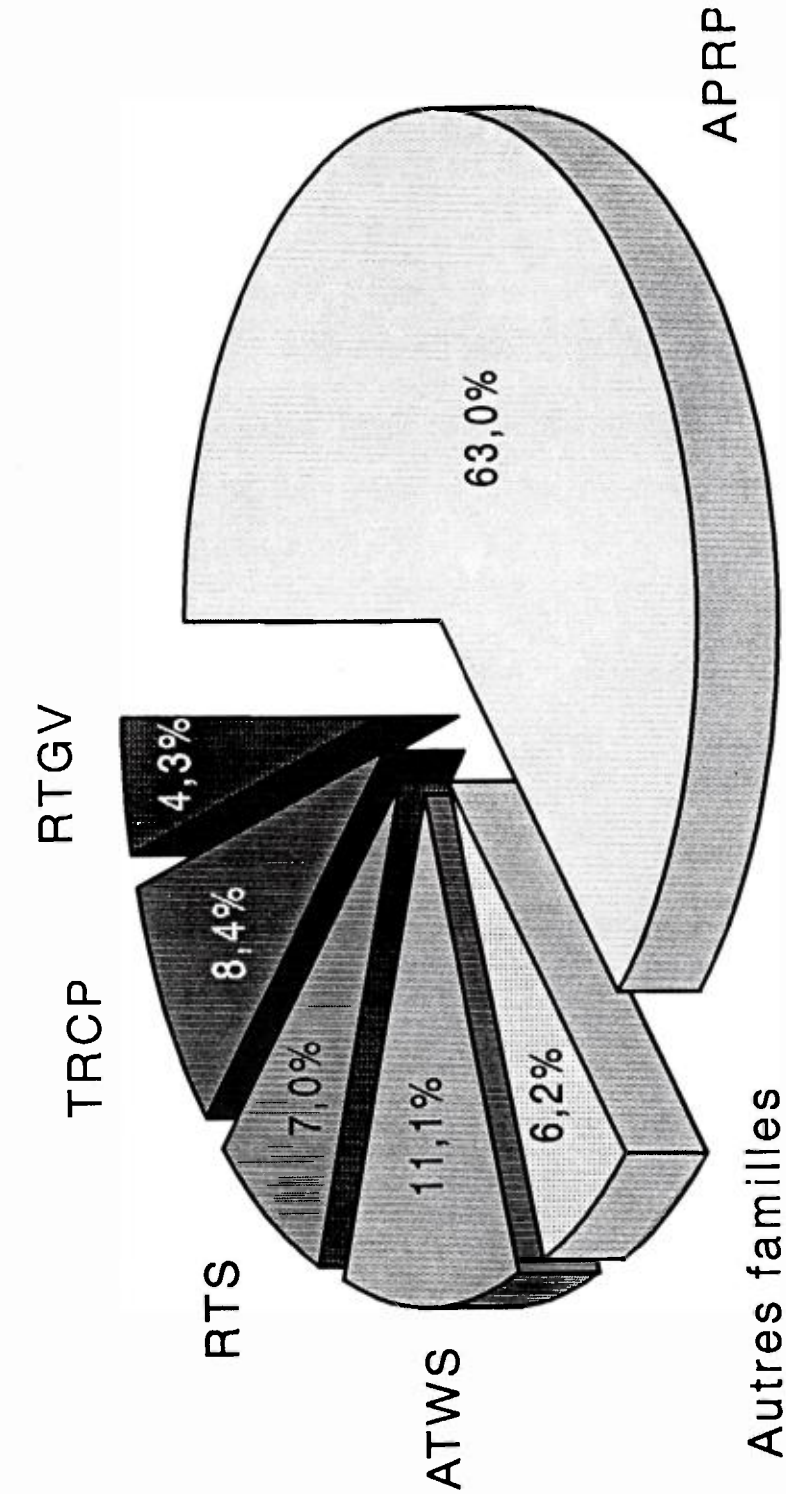
L'annexe 2 donne les résultats détaillés selon les familles d'initiateurs et selon les divers états de la tranche.

FIGURE 1. : FREQUENCE D'ENDOMMAGEMENT DU COEUR PAR ETAT DE LA TRANCHE



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.

FIGURE 2. : FREQUENCE D'ENDOMMAGEMENT DU COEUR PAR FAMILLE D'INITIATEURS



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

2.2.2. COMMENTAIRES

La fréquence annuelle d'endommagement du coeur sur la tranche 3 de Paluel est de l'ordre de 10^{-5}/an pour l'ensemble des initiateurs internes. L'incertitude associée à cette valeur point a été calculée à l'aide d'un modèle simplifié (représentant environ 90 % du poids total du risque). L'intervalle de confiance à 90 % obtenu par ce modèle simplifié est le suivant : [2,2 10^{-6} ; 2,1 10^{-5}]. La valeur médiane, la valeur moyenne et le facteur d'erreur correspondants sont respectivement : 6,1 10^{-6}, 8,4 10^{-6} et 3,5. Rappelons que le facteur d'erreur est le maximum des rapports suivants : borne supérieure/médiane et médiane/borne inférieure.

Il n'est pas question de se situer ici par rapport aux résultats d'autres EPS ; les comparaisons sont toujours très délicates et peuvent être largement discutées.

Le risque global est de 10^{-5}/tranche x an mais le résultat quantitatif en lui-même ne signifie pas tout, l'intérêt des études probabilistes résidant largement dans l'interprétation des résultats ou dans la connaissance acquise pour les obtenir.

La première conclusion importante vient du poids important des états d'arrêt du réacteur (environ 55 %). Ainsi la faible durée de ces états d'arrêt est plus que compensée par l'importance du risque horaire couru dans ces états ; à titre indicatif le risque est de 75.10^{-10}/heure dans les états c ou d contre 6.10^{-10}/heure dans l'état a.

Cela confirme les observations qui avaient été faites lors des études probabilistes traitant des pertes totales de systèmes redondants fréquemment sollicités pour le palier N_4 (source froide RRI-SEC (H1), alimentations électriques (H3)) et justifie a posteriori le choix retenu pour l'étude française de traiter tous les états initiaux possibles de la tranche.

A priori loin d'être évident, ce fait mérite pour le moins d'être commenté ; c'est pourquoi il sera repris dans les enseignements.

Un autre élément mérite d'être souligné : la famille des accidents par perte de réfrigérant primaire représente 60 % du risque global. Cependant, comme on l'indique au paragraphe suivant, il n'y a pas de séquence accidentelle nettement prépondérante ; les deux séquences les plus importantes représentent en effet chacune environ 10 % du total. Par ailleurs, le risque est également réparti entre l'état a et les états d'arrêt.

On peut également constater que les familles accidentelles identifiées sont du même type que celles couramment identifiées dans les EPS étrangères ; en effet, ces dernières font généralement apparaître la prédominance des petites brèches primaires, des transitoires suivis d'une défaillance de l'arrêt d'urgence et de la situation de perte totale des alimentations électriques secourues (H_3). Ces résultats sont très proches de ceux de l'EPS-1300, à l'exception de la famille H3 dont le poids est beaucoup plus faible, compte tenu des dispositions prises pour faire face à cette situation.

2.2.3. SEQUENCES ACCIDENTELLES PREPONDERANTES

Le tableau qui suit présente la liste des dix séquences accidentelles prépondérantes. Ces dernières sont repérées par la famille d'initiateurs, puis décrites de façon succincte ; leur fréquence d'occurrence ainsi que leur contribution (en pourcentage du risque total) sont ensuite données.

Liste des dix séquences prépondérantes de l'EPS

Famille d'initiateurs	Description succincte	Fréquence d'occurrence (/tranche x 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	$1,45\ 10^{-6}$	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	$1,14\ 10^{-6}$	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	$7,7\ 10^{-7}$	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	$5,9\ 10^{-7}$	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	$5,8\ 10^{-7}$	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	$4,6\ 10^{-7}$	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	$3,6\ 10^{-7}$	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 oeuvre de la procédure U1 par l'ISR	$3,5\ 10^{-7}$	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	$3,0.10^{-7}$	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 oeuvre de la procédure U1 par l'ISR	$2,6.10^{-7}$	2,4

On peut remarquer que :

- deux séquences seulement pèsent plus de 10 % du risque total,
- cinq familles interviennent dans les dix premières séquences (APRP, ATWS, TRCP, RTGV, RTS).

Il convient néanmoins de noter que les brèches du circuit primaire dans l'état d'arrêt d ont une contribution de l'ordre de 26 % du risque total.

En outre, les séquences prépondérantes de l'état a font toutes moins de 13 % du risque dans cet état (4,7 10-6/tranche x an).

On trouvera dans l'annexe 3 la liste des vingt séquences prépondérantes ; on verra que les conclusions précédentes ne sont pas sensiblement modifiées par la considération d'une liste plus étendue de séquences.

2.2.4. QUELQUES SEQUENCES ACCIDENTELLES INTERESSANTES

Certaines séquences accidentelles méritent une attention particulière à un titre ou à un autre (poids important, conséquences, incertitude...).

2.2.4.1. BRECHES DANS LES ETATS D'ARRET

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'initiateur prises en compte (le taux horaire de brèche primaire est le même qu'en puissance). Cependant il faut noter qu'une fois l'initiateur survenu, le système d'injection de sécurité doit être mis en service par l'opérateur. Dans la plupart des cas en effet, la seule protection opérationnelle (haute pression enceinte) interviendrait trop tard.

2.2.4.2. DILUTION

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 oeuvre 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 boriquée. Cette poche, si elle n'est pas désagrégée lors du redémarrage d'une pompe primaire, est propulsée à travers le coeur. 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 oeuvre sur les tranches un automatisme d'isolement de la dilution lors de la perte des pompes primaires ; il a été tenu compte de cet automatisme dans le calcul de la fréquence d'occurrence de la séquence correspondante.

2.2.4.3. PERTE DU SYSTEME DE REFRIGERATION A L'ARRET (RRA) DANS L'ETAT d

Un initiateur, qui peut s'apparenter à la perte totale de la source froide, s'est révélé important ; il s'agit de la perte du RRA quand la tranche est dans l'état d.

Les séquences qui en découlent sont intéressantes à plus d'un titre mais leurs caractéristiques principales sont :

- le délai court avant conséquences inacceptables : une demi-heure environ quand le circuit primaire est peu ouvert et le RRA définitivement perdu ;

- la probabilité de perdre le RRA (au moins momentanément) est non négligeable. En effet, du fait du manque de précision de la mesure du niveau visible d'eau dans le circuit primaire, le refroidissement par RRA a été momentanément interrompu plusieurs fois sur les tranches françaises.

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

Cette séquence n'a pas encore été quantifiée définitivement. Elle sera intégrée ultérieurement dans une révision de l'EPS-1300.

2.2.4.4. BRECHES INTERFACES

Ces séquences accidentelles, qui conduisent à une fuite de fluide primaire à l'extérieur de l'enceinte de confinement, sont difficiles à quantifier. Elles supposent la défaillance successive de trois clapets d'isolement du circuit primaire en série. Compte tenu de la conception des circuits, des essais périodiques, on a considéré qu'il n'existe pas de mode commun d'ordre 3 en fonctionnement sur ces clapets. La probabilité de cette séquence est donc très faible ; elle est très sensible à l'hypothèse faite. Si de tels modes communs existaient, elle serait beaucoup plus élevée.

Compte tenu de ces différents éléments une réflexion approfondie est engagée ; des enseignements en seront tirés notamment dans le cadre de la conception des futures tranches REP françaises (REP 2000).

2.2.4.5. LES PERTES DE SOURCE DE CONTROLE COMMANDE

Les pertes de source 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.

Lors d'un incident survenu en 1984 sur la tranche Bugey 5, par suite d'une dégradation progressive de tension continue non détectée immédiatement, des actionneurs ont manoeuvré 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) de fréquence globale égale à environ 10^{-6}/tranche x an. Compte tenu de

l'existence de la procédure 113, on peut estimer que ces séquences conduisent à un risque très faible. Il faut toutefois remarquer qu'il subsiste des incertitudes importantes sur la quantification des erreurs humaines dans de telles situations.

Ce genre de cumuls a fait l'objet d'une première réflexion. Il n'est pas possible de couvrir chaque cas 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.

2.3. INTERPRETATION DES PRINCIPAUX RESULTATS

2.3.1. LES ETATS D'ARRET DU REACTEUR

Il convient d'approfondir un des enseignements majeurs de l'étude : le poids important des états d'arrêt. En fait ceci 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 aux conditions nominales.

- ensuite du fait que, 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 sont conçus pour protéger les tranches en fonctionnement.

Il est évident que le souci majeur des concepteurs doit rester l'état en puissance. Il convient de plus de remarquer que la qualité des protections dans ces états conduit à un abaissement du risque tel qu'il n'est pas prépondérant devant celui provenant des états d'arrêt.

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 (et ses dangers potentiels par exemple vis-à-vis des erreurs de conception),

- 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 par ailleurs tenir compte du fait (difficilement quantifiable) que du personnel est souvent présent dans le bâtiment réacteur et à ce titre peut signaler directement en salle de commande l'impact des phénomènes perturbateurs (vapeur, etc.). La quantification des séquences présente donc une marge d'incertitude importante.

Il faut s'interroger tout particulièrement sur la durée passée dans un tel état (~ 15 jours) même si le circuit primaire n'est pas en permanence dans la plage de travail basse du RRA et voir quelle mesure pourrait être prise pour raccourcir cette durée au minimum ou pour au moins renforcer la surveillance de l'installation dans cet état.

2.3.2. LE POIDS DES ERREURS DE CONDUITE

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".

Est-ce à dire qu'il n'y a plus rien à faire pour améliorer les matériels et le processus de fonctionnement des tranches si ce n'est par des programmes accrus de formation des opérateurs ? Certainement pas.

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 :

- Ce que nous appelons "erreur" dans une étude de séquences n'est qu'un échec dans la récupération d'un accident. Le risque serait généralement plus élevé en l'absence d'opérateurs (l'impact de l'opérateur dépendant cependant de l'accident : nécessité de réaliser des actions, possibilités d'actions inopportunes...). Ce sont en fait surtout les actions inopportunes et les erreurs de maintenance (à l'origine d'initiateurs et de défaillances de systèmes) qui sont à mettre au "passif" de l'opérateur.

- 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 coeur 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, de la formation, et, dans certains cas, par l'automatisation. Ces actions seront détaillées dans le paragraphe relatif aux enseignements. Il ne faut pas cependant oublier leurs limites ; l'importance de l'organisation de l'exploitation normale et de la maintenance ne doit pas être sous-estimée.

2.3.3. LES INCERTITUDES

L'EPS 1300 a donné lieu à un calcul de propagation des incertitudes sur les données. Le facteur d'erreur obtenu par ce calcul est de 3,5 sur la fréquence d'endommagement du coeur.

Il faut noter que les incertitudes sur les données se "compensent" si bien que l'incertitude sur le résultat global est comparable à l'incertitude moyenne sur les données élémentaires ; cependant le facteur d'erreur peut être beaucoup plus important pour certaines séquences accidentelles.

Un tel facteur d'erreur ne doit pas être pris comme une faiblesse des études probabilistes mais comme un fait et à ce titre il doit en être tenu compte dans les conclusions qui peuvent être tirées d'une telle étude.

Il convient également de souligner les incertitudes très importantes qui peuvent provenir de la modélisation. L'étude a comporté trois phases ; par chacune d'entre elles, de nombreuses études complémentaires ont été réalisées pour mieux comprendre et mieux connaître le comportement de l'installation dans des situations qui ne sont pas de dimensionnement. Outre le fait qu'il convient de souligner l'intérêt des enseignements de ces études, il faut remarquer que certaines séquences jugées inacceptables dans un premier temps ont pu être revues à la lumière de ces enseignements.

L'approfondissement de la connaissance a donc permis de diminuer de façon sensible les incertitudes que l'on pourrait appeler fonctionnelles : ce fait est très important d'un point de vue méthodologique.

En outre, on notera que les études de sensibilité, qui pourront être effectuées à l'avenir avec LESSEPS-1300, peuvent permettre d'apprécier le poids du taux de défaillance d'un composant que l'on connaît mal ou l'importance d'une hypothèse incertaine.

2.3.4. L'APPORT DES SPECIFICITES DE LA DEMARCHE DE SURETE FRANCAISE

Il convient en premier lieu de citer les procédures et les matériels associés. 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 coeur 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 et réduit le risque d'endommagement du coeur.

- H3 : Le LLS, (turbogénérateur entraînant une pompe et alimentant l'instrumentation indispensable) permet de poursuivre l'injection aux joints des pompes primaires.

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 ces dispositions (ISR et SPI-U1) est d'environ 6 (en l'absence de ces dispositions, le risque serait 6 fois plus élevé).

2.3.5. LES SYSTEMES DE SURETE

Il convient de citer ici quelques points importants mis en évidence par les évaluations probabilistes des systèmes de sûreté.

a) <u>La prise en compte des défaillances de cause commune</u>

L'évaluation probabiliste des défaillances de cause commune (DCC) fait appel à des données spécifiques dites "facteurs β" (voir chapitres 3.4.4. et 4.1.1. ci-après). Les DCC contribuent fortement à la défiabilité des systèmes redondants. A titre indicatif le poids des DCC dans la défiabilité des systèmes d'injection de sécurité et d'alimentation de secours des générateurs de vapeur peut atteindre 50 à 80 % selon la mission considérée.

Malgré les incertitudes importantes sur les facteurs β, en particulier pour 3 ou 4 composants, cela souligne l'intérêt de la diversification fonctionnelle et confirme le fait qu'il faut s'interroger sur la meilleure façon de procéder à l'entretien ou au réglage des systèmes redondants.

Le retour d'expérience nous enseigne que le fait d'avoir trois ou quatre composants en parallèle n'est pas une garantie absolue vis-à-vis de ce type d'incidents ; d'où la nécessité d'une réflexion approfondie sur l'intérêt de la diversification lorsqu'il s'avère encore nécessaire d'améliorer la haute fiabilité des systèmes de sûreté.

b) <u>La prise en compte des essais périodiques et de la maintenance</u>

Il est confirmé que les indisponibilités de matériels dues à un essai périodique en cours ont un poids très faible.

Les indisponibilités pour maintenance ont une importance non négligeable principalement dans les états d'arrêt à froid où leur taux est souvent supérieur aux taux de défaillance à la sollicitation des composants concernés. Leur contribution à la défiabilité d'un système redondant est toutefois fortement minimisée par le fait que la maintenance se fait de façon décalée dans le temps entre les voies des systèmes.

L'enquête ponctuelle menée sur le CPN de Paluel afin d'obtenir des taux d'indisponibilités pour maintenance mériterait d'être étendue à d'autres tranches REP de façon à améliorer sensiblement la précision de ces données.

c) La fiabilité des composants

L'analyse détaillée des défaillances des composants et l'élaboration d'une base de données validée ont mis en lumière le fait que certains composants ont des taux de défaillance élevés (voir le chapitre 3 : données). C'est par exemple le cas des taux de défaillance en fonctionnement des diesels et des pompes du système d'alimentation de secours des générateurs de vapeur.

Bien que leur impact sur le risque global ne soit pas très important, il convient de s'interroger sur la signification profonde de ces données et voir dans quelle mesure pour les paliers futurs, il serait souhaitable de faire des choix plus industriels (en gardant bien sûr, la "qualité nucléaire") ayant un champ d'application plus vaste que le strict cadre des centrales.

d) Les interactions entre systèmes

Grâce à la diversification fonctionnelle, les interactions entre systèmes ont un poids très faible.

Les seules interactions réellement significatives sont les sources de puissance électrique (tableaux LH 6,6 kV secouru), les tableaux LB (125 V équipement) associés ainsi que la source froide (RRI - SEC).

2.3.6. LES DIFFERENTS MODES DE FUSION DU COEUR

On peut distinguer :

- les fusions avec intégrité de l'enceinte (c'est la quasi-totalité des cas),

- les fusions avec fuite directe hors de l'enceinte de confinement.

Pour ce dernier cas, deux séquences principales sont identifiées :

- les brèches interfaces dont il a déjà été question précédemment et pour lesquelles une réflexion est engagée,

- la séquence accidentelle liée à une rupture de tube de générateur de vapeur (RTGV) suivie d'un remplissage du générateur de vapeur, puis d'une sollicitation et d'un blocage ouvert d'une soupape secondaire, puis ultérieurement de l'endommagement du coeur. Cette séquence est d'un poids faible vis-à-vis du risque total mais elle serait à examiner avec plus d'attention dans le cadre d'une étude de niveau 2 (évaluation de la fréquence annuelle de rejet dans l'environnement).

L'optimisation de la procédure de conduite à appliquer en cas de RTGV et la formation réduisent la probabilité de remplissage du générateur de vapeur : l'application de la procédure SPI-U1 permet de conduire la tranche en cas de cumul RTGV - soupape du générateur de vapeur bloquée ouverte.

3. DONNEES

3.1. INTRODUCTION

3.1.1. GENERALITES

A quelques exceptions près, les données utilisées dans l'EPS-1300 sont issues de l'expérience d'EDF liée aux centrales REP en exploitation.

Cette démarche a été rendue possible grâce à l'importance du retour d'expérience d'un parc homogène de tranches REP représentant plus de 200 années x réacteur, sans équivalent dans le monde.

En effet le parc français des centrales REP se caractérise par son homogénéité au niveau de la conception, de l'exploitation et de la maintenance.

Même si des différences notables existent entre paliers, comme par exemple entre le palier 900 MWe et le palier 1300 MWe en ce qui concerne les systèmes de sauvegarde, les matériels composant ces systèmes sont à quelques exceptions près pratiquement identiques.

De plus, parmi les caractéristiques de cette étude, figure la prise en compte de tous les états de tranche, depuis les états d'arrêt à froid pour rechargement jusqu'à l'état de tranche à pleine puissance.

L'étude est de ce fait plus complexe et nécessite une analyse plus approfondie des données d'exploitation.

La base de données a fait l'objet d'une analyse critique de la part de l'IPSN en tant que contrôle externe, ce qui a permis l'obtention d'une base commune de données de très grande qualité.

Elle comprend principalement :

- Les données d'exploitation concernant les durées moyennes passées dans les états standards de la tranche (durée du fonctionnement en puissance, en arrêt à chaud, en arrêt à froid...,) et permettant ainsi de définir le profil de fonctionnement de la tranche.

- 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 pour les situations à la limite du dimensionnement, de fréquence rare ou hautement improbable.

- Les données de sûreté de fonctionnement 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 de sollicitations), les durées moyennes de réparation associées ainsi que les durées d'indisponibilité des matériels dans les différents états définis ci-dessus, intégrant les indisponibilités pour maintenance corrective, préventive ou pour essai périodique. Par commodité toutes ces données sont aussi dénommées "données de fiabilité".

- Les données relatives aux défaillances de cause commune déterminées par la méthode des chocs (encore appelée méthode de la loi binomiale).

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. Ce calcul est réalisé selon la loi adoptée généralement dite du Khi-Deux.

3.1.2. METHODES ET OUTILS DE COLLECTE DES DONNEES

Dans la perspective d'obtenir un nombre important de données, le recours aux banques de données nationales a été maximal : ainsi ont été analysées les banques S.R.D.F. et F.E. (respectivement Système de Recueil de Données de Fiabilité et Fichier des Evénements) et le fichier des données statistiques sur le fonctionnement des tranches nucléaires françaises.

De plus, il est apparu nécessaire de compléter ces études par des enquêtes sur site pour tenir compte de certaines spécificités du site étudié et pour apporter un plus grand réalisme à l'étude.

Enfin il a été fait appel à quelques bases de données étrangères pour compléter et comparer certaines données particulières.

Cette démarche à 3 niveaux - local - national - international est explicitée ci-après.

3.1.2.1. NIVEAU LOCAL

a) La méthode :

- Sur le site, les enquêtes et observations ont permis de mieux prendre en compte la réalité d'exploitation et de proposer des données complémentaires spécifiques. Par ailleurs les analyses locales de l'exploitation ont amené à préciser un certain nombre d'événements non envisagés à l'origine dans les études de fiabilité de systèmes ou de séquences.

  Des données de fonctionnement et de fiabilité ont été recueillies, en particulier sur des matériels pour lesquels on ne disposait pas de données génériques ou sur ceux pour lesquels l'expérience d'exploitation sur site conduisait à supposer que les résultats seraient notablement différents des résultats génériques.

  Dans le cas très particulier d'un retour d'expérience restreint, il a été fait appel à des méthodes d'agrégation de type bayesiennes pour prendre en compte différents types d'informations concernant des matériels de même nature, dans le but d'obtenir des données plus valides.

  En outre un suivi particulier de plusieurs arrêts annuels pour rechargement de types différents a été effectué.

  Un planning général mettant en évidence les différentes phases des niveaux et des mouvements d'eau du circuit primaire a été établi.

b) Les outils :

Tous les systèmes informatiques locaux ont été utilisés pour le recueil d'informations. Des programmes de dépouillement automatique ont été développés pour faciliter l'extraction d'informations pertinentes.

C'est ainsi que 3 importants fichiers locaux ont été utilisés :

- Les données établies à partir du calculateur de tranche qui enregistre en permanence le fonctionnement de la tranche. Tout changement d'état d'un composant ou toute variation de grandeur analogique est ainsi mémorisé et traité au moyen d'un outil informatique .

- Les données relatives aux retraits d'exploitation des matériels qui sont effectuées à l'aide d'un outil informatique : AIC (Aide Informatique aux Consignations) et qui constituent l'historique de toutes les opérations de maintenance.

- Les données, enregistrées dans un fichier historique local, relatives aux anomalies constatées sur le fonctionnement d'un matériel et qui ont conduit à l'établissement d'une demande de travaux pour corriger cette anomalie.

Ces moyens informatisés ou automatisés ont été complétés dans quelques cas particuliers par des recherches dans les rapports d'exploitation des équipes de conduite et des Ingénieurs de Sûreté Radioprotection, et par de nombreux entretiens avec les équipes d'exploitation et de maintenance.

3.1.2.2. NIVEAU NATIONAL

Sur le plan national, la recherche des données a été réalisée essentiellement à partir des banques de données S.R.D.F. et F.E. (respectivement Système de Recueil de Données de Fiabilité et Fichier des Evénements).

Quant au fichier de données statistiques, il a été utilisé pour la recherche des données d'exploitation des tranches : coefficients de disponibilité et de production.

a) Le S.R.D.F.

Présentation du fichier

Environ 500 matériels électriques et mécaniques par tranche sont suivis (pompes, appareils de robinetterie, groupes diesels, moteurs électriques, transformateurs...) depuis la première mise en service du S.R.D.F. sur le site de Fessenheim en 1978. La collecte des défaillances est réalisée au niveau local sous forme de fiche descriptive comprenant un résumé de la défaillance, le mode de défaillance et son degré de gravité ainsi que les conséquences sur la tranche. Par ailleurs les paramètres de fonctionnement sont régulièrement collectés pour chaque matériel. Un ordinateur central permet la gestion et le traitement des données au niveau national en offrant la possibilité d'une interrogation-analyse à partir de chaque terminal.

Le fichier comprend en moyenne plus d'une centaine de fiches par an et par tranche (environ 20 000 fiches à fin 88).

Par ailleurs la spécificité du matériel électronique utilisé dans le contrôle commande des tranches 1300 MWe a nécessité le développement d'un système de suivi particulier : le S.R.D.F. A (environ 5000 fiches à fin 88).

Méthodologie utilisée

Excepté pour les données du S.R.D.F. A pour lesquelles le contrôle est réalisé à l'échelon central, les données brutes ne sont pas systématiquement analysées par l'échelon central avant traitement.

En conséquence, à partir de l'ensemble des éléments descriptifs de la défaillance, recueilli dans un contexte d'exploitation normale, il a été nécessaire de s'assurer de la cohérence, de l'homogénéité et de la représentativité des données dans le cadre de l'EPS.

Le contrôle centralisé des fiches par des ingénieurs ayant une bonne connaissance d'exploitation a assuré l'obtention de données homogènes et réalistes grâce à une faible dispersion des interprétations liées au jugement de l'ingénieur et à un choix rigoureux des défaillances critiques au sens de la sûreté.

Par ailleurs, l'étude d'environ 5000 fiches de défaillances a été complétée par une analyse d'identification de défaillances de cause commune.

La plupart des données de fiabilité ont été ainsi élaborées sur une période d'observation s'échelonnant généralement de 78 à 86 environ en fonction de la mise en place progressive du S.R.D.F. sur les sites.

b) Le fichier des événements

Présentation du fichier

En ce qui concerne le F.E., les données collectées correspondent principalement aux incidents d'exploitation (arrêts, baisse de charge, non respect des spécifications techniques...), aux incidents concernant la sûreté et l'environnement, aux incidents d'origine humaine.

La mise en service de cette banque de données a été entreprise en 1978. La collecte des événements est réalisée au niveau local sous forme de fiche descriptive d'événement comprenant en plus d'un résumé de l'événement, l'origine et la nature de l'événement ainsi que la situation de la tranche et les données de fonctionnement.

Un ordinateur central assure la gestion et le traitement des données au niveau national. Une interrogation-analyse est possible à partir de chaque terminal.

Le fichier comprend environ 20 000 fiches à fin 88.

Méthodologie utilisée :

Un grand nombre de fiches (environ 5 000) ont fait l'objet d'une analyse détaillée et ont permis :

- de compléter dans certains cas les données de fiabilité S.R.D.F. en analysant les événements en fonction de leurs conséquences plutôt qu'en fonction de leurs causes,
- de fournir des données de fonctionnement,
- de compléter et valider la quantification du profil de fonctionnement,
- de réaliser la quantification d'un grand nombre d'événements initiateurs.

3.1.2.3. NIVEAU INTERNATIONAL

a) Les outils utilisés :

- La consultation de certaines banques de données étrangères a permis de compléter la recherche des données. Deux sont à citer :

  . NPRDS : (Nuclear Plant Reliability Data System). Cette banque de données américaines réalisée par l'INPO (Institute of Nuclear Power Operation) est équivalente au S.R.D.F.,

  . le fichier incidents des centrales étrangères, élaboré par la Direction des Etudes et Recherches d'EDF.

  Ce fichier comporte plus de 20 000 événements d'exploitation à fin 87 représentant une expérience équivalente à 500 années x réacteur.

b) Méthodologie :

L'analyse de ces bases de données a fourni dans quelques cas particuliers des données non suivies par ailleurs comme par exemple la fréquence des initiateurs de type rupture de tuyauterie mais a aussi permis d'utiliser le retour d'expérience mondial pour comparer et valider certaines données.

3.1.3. LIMITES DE LA DEMARCHE

Basée sur l'analyse du retour d'expérience, cette démarche est naturellement limitée lorsque le retour d'expérience est insuffisant ou n'existe pas. Elle doit alors être complétée par d'autres études et être accompagnée par l'utilisation d'autres méthodes.

Parmi celles qui sont utilisées dans le cadre de cette étude, il faut mentionner :

- la recherche bibliographique et le jugement d'expert avec les incertitudes inhérentes pour l'élaboration de données relatives à des événements rares,

- la méthode d'agrégation type estimation bayesienne déjà citée qui permet de mieux prendre en compte le retour d'expérience,

- les études théoriques de sûreté de fonctionnement prévisionnelle pour compléter la recherche et la quantification de certaines données. Un exemple d'application concerne la transposition d'une donnée recueillie à l'occasion des essais périodiques en une donnée à utiliser pour le fonctionnement accidentel prolongé.

Une autre limitation est liée aux caractéristiques des bases de données. En effet même en donnant des critères de recueil précis, il n'est pas possible d'éliminer totalement la part de jugement de l'ingénieur tant au niveau de la collecte qu'au niveau de l'analyse.

On peut toutefois penser que cette limitation n'introduit pas de biais significatif dans les résultats compte tenu d'une part de la taille généralement importante des échantillons statistiques, d'autre part du nombre d'ingénieurs ou d'experts qui ont été impliqués dans l'analyse a posteriori de ces données.

3.1.4. RESULTATS DE L'ANALYSE DU RETOUR D'EXPERIENCE

L'analyse du retour d'expérience a permis :

- de déterminer le profil type de fonctionnement des tranches, c'est-à-dire le temps passé en moyenne dans les différents états de tranche,

- d'identifier et de quantifier un grand nombre d'événements initiateurs, situation à partir de laquelle peut se développer une séquence accidentelle,

- d'élaborer l'ensemble des données de fiabilité (taux de défaillance, durée de réparation, etc.) nécessaires aux évaluations quantitatives des missions des systèmes de sûreté et des séquences accidentelles.

3.2. PROFIL DE FONCTIONNEMENT

3.2.1. OBJECTIFS

La prise en compte de tous les états initiaux possibles de la chaudière, nécessite de disposer d'un profil type de fonctionnement des tranches REP, applicable au cas particulier de la tranche 3 du CPN de Paluel.

L'expérience d'exploitation du palier 1300 MWe étant encore trop faible, l'établissement de ce profil-type est fait essentiellement à partir de l'expérience d'exploitation du palier 900 MWe, confortée par quelques enquêtes spécifiques effectuées à Paluel.

L'étude permet de déterminer pour chacun des états retenus, qui peuvent être différents des états standards, la fréquence et la durée par tranche et par an.

Les états du réacteur définis pour l'EPS sont les suivants :

ETAT	DESCRIPTION
Etat a	Point de fonctionnement (pression, température) au-dessus de (139 bar, 295 °C à Paluel) ce qui correspond aux états standards : - réacteur en puissance groupe couplé ou non - réacteur en arrêt à chaud - partie supérieure du domaine d'arrêt intermédiaire
Etat b	Point de fonctionnement (pression, température) entre (139 bar, 295 °C) et les conditions RRA (30 bar, 177 °C)
Etat c	Arrêt sur RRA, circuit primaire plein, fermé et éventé
Etat d	Circuit primaire partiellement vidangé ou ouvert. Par conservatisme tous les états d seront assimilés à l'état où le niveau du circuit primaire est dans la plage de travail basse du RRA (initialement défini par "état plan médian") et pour lequel la masse de réfrigérant primaire est minimale
Etat e	Piscine réacteur pleine avec au moins un élément combustible en cuve
Etat f	Tout état du primaire où le combustible est entièrement déchargé. Il correspond aux épreuves hydrauliques et épreuves enceintes, aux passages en génératrice inférieure et toutes autres interventions nécessitant le déchargement complet (inspection cuve, interventions sur les internes inférieurs etc.). Cet état n'a pas lieu d'être pris en compte dans l'EPS

3.2.2. DUREES ANNUELLES DES ETATS PRIS EN COMPTE DANS L'EPS-1300

ETAT	SOUS-ETAT	TEMPS EN JOURS	POURCENTAGE SUR L'ANNEE
Etat a	Puissance > 60 % PN	268	73,4 %
	Puissance < 60 % PN	17	4,7 %
	Réacteur critique		
	Groupe non couplé	12	3,3 %
	Réacteur sous-critique	15	4,1 %
Etat b		2 (38 heures)	0,5 %
Etat c		11	3 %
Etat d	Sans dénoyage des épingles des générateurs de vapeur	2	0,6 %
	Avec dénoyage des épingles des générateurs de vapeur	17	4,6 %
Etat e		9	2,5 %
Etat f		12	3,3 %
TOTAL		365	100 %

Les durées ont été déterminées en tenant compte de la fréquence de passage dans chaque état, de la durée de fonctionnement dans l'état et du temps nécessaire pour passer d'un état à un autre.

En ce qui concerne ce dernier point, de nombreuses observations sur site ont permis d'évaluer les durées de transitoires.

3.3. INITIATEURS

3.3.1. DEFINITION

Un événement initiateur est un événement à partir duquel peut se développer une séquence accidentelle. L'évaluation du risque de fusion du coeur passe par la détermination et l'évaluation de ces événements initiateurs. Aussi a-t-il été nécessaire de définir une démarche comportant plusieurs phases comme indiqué ci-après.

3.3.2. METHODOLOGIE

Une première liste a été établie à partir :

- des situations de dimensionnement,
- de l'analyse des incidents et accidents déjà observés sur les tranches françaises et étrangères,
- d'une recherche bibliographique afin de s'inspirer des études déjà réalisées,
- des résultats d'analyse prévisionnelle des systèmes ou de séquences accidentelles qui mettent en évidence certains initiateurs.

Une fois la liste établie, les événements initiateurs de cette liste doivent être quantifiés et, lors de l'analyse du retour d'expérience, cette liste peut être modifiée par la mise en évidence de séquences non prises en compte au départ.

Pour les événements rares (exemple : rupture de tuyauteries), la quantification est principalement réalisée à partir de jugements d'experts, compte tenu du retour d'expérience mondial. Pour cela sont utilisés les rapports publiés au plan international ainsi que l'interrogation du fichier des événements des centrales étrangères créé par la Direction des Etudes et Recherches et constitué à partir des rapports publiés depuis 1974 sur les réacteurs nucléaires de plus de 400 MWe.

Pour les événements plus fréquents, donc plus observables, le retour d'expérience a été utilisé systématiquement en utilisant principalement le retour d'expérience des tranches françaises. En effet la richesse du retour d'expérience du parc due au nombre de tranches, à la standardisation et à l'organisation mises en place pour la collecte des données et des informations permet de quantifier avec un ordre de grandeur réaliste les initiateurs.

3.3.3. RESULTATS

La mise en oeuvre de la méthodologie résumée ci-dessus a permis d'obtenir, pour chaque événement initiateur considéré dans l'EPS-1300 (exception faite des initiateurs du type perte de système redondant dont les fréquences d'occurrence sont calculées par l'intermédiaire d'études de sûreté de fonctionnement) :

- sa fréquence annuelle d'occurrence dans les différents états initiaux du réacteur où il est susceptible de ce produire,

- l'intervalle de confiance correspondant.

Ainsi, à titre d'exemple, la fréquence annuelle d'occurrence d'une perte du vide au condenseur au-dessus de 40 % PN est égale à 5,0 10^{-2}/tranche x an ; les bornes inférieure et supérieure de l'intervalle de confiance à 90 % associé à cette valeur sont respectivement 2,5 10^{-2}/tranche x an et 9,0 10^{-2}/tranche x an.

3.4. DONNEES DE FIABILITE DES COMPOSANTS

3.4.1. OBJECTIFS

Après modélisation de la sûreté de fonctionnement des systèmes de la tranche et identification des défaillances pertinentes, il est nécessaire, pour la quantification, de connaître les paramètres de sûreté de fonctionnement des composants modélisés :

- lambda : taux de défaillance en fonctionnement (/heure)

- gamma : taux de défaillance à la sollicitation (/demande)

- tau : durée moyenne de réparation (heure)

- I : taux d'indisponibilité d'un composant en fonction de l'état du réacteur

- béta : facteur béta de données de défaillance de cause commune.

L'élaboration de cette base de données a donc été étroitement liée à la réalisation des études de manière à adapter la recherche aux besoins et vice-versa.

Ceci a conduit à la définition de composants qui dépendent des limites de la modélisation et de celles de l'observation. De même, pour chaque composant, les modes de défaillances modélisés sont fonction des modes de défaillances observables.

3.4.2. TAUX DE DEFAILLANCE

La richesse du retour d'expérience actuel liée, d'une part au nombre d'années x réacteur sur un parc REP homogène et d'autre part à l'organisation mise en place pour la collecte (fichiers nationaux), a permis de s'orienter vers une base de données entièrement EDF.

A chaque valeur est associé un intervalle de confiance. En ce qui concerne les taux de défaillance en fonctionnement les valeurs obtenues sont fonction du type de matériel, avec quelques points singuliers pour certains composants.

Les pompes se situent entre 5,5 10^{-6}/h et 5,5 10^{-5}/h sauf la pompe d'alimentation de secours des générateurs de vapeur (ASG) qui a une valeur de fiabilité égale à 3,2 10^{-4}/h.

En ce qui concerne les turbines, type ASG, et les diesels les valeurs sont comprises entre 3 10^{-3}/h et 10^{-2}/h.

Les taux de défaillance en fonctionnement des composants passifs ou électroniques sont compris entre 10^{-7}/h et 10^{-6}/h.

La fiabilité des moteurs, quant à elle, est indépendante de leur puissance et se situe autour d'une valeur de 4 10^{-6}/h.

En ce qui concerne les taux de défaillance à la sollicitation, on remarque la bonne fiabilité des moteurs (7,5 10^{-6}/d) et les valeurs élevées pour la turbine ASG et les diesels (respectivement 8,6 10^{-3}/d et 3,4 10^{-3}/d). La robinetterie se situe entre 10^{-4}/d et 10^{-3}/d (sauf les clapets qui, avec une valeur de 10^{-5}/d se situent 10 fois plus bas) tandis que les différentes pompes s'échelonnent entre 2 10^{-5}/d et 10^{-3}/d.

3.4.3. TAUX D'INDISPONIBILITE

Toutes les indisponibilités sont prises en compte qu'elles soient dues à la maintenance corrective, à la maintenance préventive, à un "régime d'essai" ou même à un "régime de consignation pour exploitation".

Cet exercice a été effectué sur le CPN de Paluel, sur une période limitée représentant environ 8,3 années x réacteur et a permis d'obtenir tous les taux d'indisponibilité utilisés dans l'EPS 1300.

3.4.4. DEFAILLANCES DE CAUSE COMMUNE

Les défaillances de cause commune (DCC) sont des défaillances survenant de manière simultanée ou concomitante sur plusieurs composants et provenant de la même cause.

Pour caractériser les défaillances de cause commune, de deux composants par exemple, on évalue le facteur β de la manière suivante :

$$\beta = \frac{\text{taux de défaillance de cause commune}}{\text{taux de défaillance indépendante} + \text{taux de défaillance de cause commune}}$$

La détermination de ces facteurs β repose, d'une part, sur une analyse détaillée des fichiers du retour d'expérience des tranches REP et, d'autre part, sur l'utilisation de la méthode des chocs (loi binomiale).

Les études faites sur ces bases concernent plusieurs types de matériels :

- instrumentation (capteurs, transmetteurs, chaînes de mesures analogiques,...),
- pompes,
- robinetterie primaire et secondaire (vannes électriques pneumatiques, clapets, vannes manuelles),
- disjoncteurs et contacteurs (en particulier matériels 6,6 kV, disjoncteurs d'arrêt d'urgence).

Les facteurs β se situent entre 10^{-2} et 10^{-1}.

4. METHODES ET INFORMATISATION

Les méthodes employées dans l'EPS-1300 appartiennent à un très large spectre de disciplines : sûreté de fonctionnement, informatique, statistiques, facteurs humains, etc.

Dans ce chapitre on se limite aux méthodes relevant de la sûreté de fonctionnement et de l'informatique, des chapitres spécifiques étant consacrés aux données (voir chapitre 3) et aux facteurs humains (voir chapitre 5).

4.1. METHODES

On aborde ici les méthodes d'évaluation probabiliste utilisées tant au niveau des systèmes de sûreté que des séquences accidentelles.

4.1.1. EVALUATION PROBABILISTE DES SYSTEMES DE SURETE

4.1.1.1. GENERALITES

Treize systèmes de sûreté ont fait l'objet d'une évaluation probabiliste ; compte tenu des dépendances entre certains de ces systèmes, dix études ont été réalisées. Généralement, la fiabilité de ces systèmes a été évaluée, mais aussi parfois leur disponibilité ou leur maintenabilité.

Une démarche systématique a été appliquée pour l'évaluation probabiliste de ces systèmes, les principales étapes de cette démarche étant les suivantes :

- définition des missions à analyser,
- modélisation des événements indésirables avec :
  - . choix et justification des méthodes employées,
  - . choix et justification des outils employés,
  - . élaboration des modèles.
- prise en compte des défaillances de cause commune,
- prise en compte du facteur humain,
- prise en compte des tests et de la maintenance,
- prise en compte du contrôle commande,
- quantification des résultats,
- comparaison avec les incidents réellement survenus sur le système (analyse du retour d'expérience des tranches françaises).

Ces étapes sont résumées ci-après ; on se contente d'indiquer les éléments marquants.

4.1.1.2. DEFINITION DES MISSIONS A ANALYSER

L'examen des séquences accidentelles impliquant un système donné permet, pour le système considéré, de dresser une liste exhaustive de toutes les missions pour lesquelles il est requis.

Par mission, nous entendons :

- les critères de fonctionnement (exemple : nombre de lignes d'injection requises, débit nécessaire...),

- la durée de fonctionnement du système,

- l'état des systèmes supports (sources électriques de puissance et de commande, source froide),

- les indisponibilités liées à la situation accidentelle (générateur de vapeur indisponible après une rupture de tuyauterie vapeur...).

Bien évidemment, cette étape a nécessité une itération à partir d'une liste préliminaire obtenue dans la première phase de l'EPS-1300, la liste définitive ayant été obtenue dans la dernière phase de l'EPS-1300.

4.1.1.3. MODELISATIONS DES EVENEMENTS INDESIRABLES

Deux méthodes sont principalement retenues : la méthode de l'arbre de défaillance et la méthode du graphe d'états. 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 niveaux successifs d'événements tels que, chaque événement est généré à partir des événements de niveau inférieur par l'intermédiaire de portes logiques (OU ou ET) ; ces événements sont généralement des défaillances de matériels, des indisponibilités de matériels, des erreurs humaines ... pouvant conduire à l'événement indésirable.

Des codes 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.

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 ; les causes de ces transitions 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.).

Dans l'EPS-1300, deux types de quantification de ces graphes d'états sont utilisés :

- un traitement matriciel pour les systèmes multiphasés. Un graphe est alors décrit par sa matrice des taux de transition. Une inversion de cette matrice donne la probabilité de présence du système (en fonction du temps) dans les différents états,

- un traitement par recherche de séquences dans le graphe pour les systèmes dont la défaillance participe à un événement initiateur. Le graphe d'états n'a pas toujours besoin d'être décrit ; seules des règles de production définissant les transitions allant de l'état de bon fonctionnement à un état de panne sont données et suffisent pour permettre le calcul du graphe d'états.

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 généralement retenue.

4.1.1.4. PRISE EN COMPTE DES DEFAILLANCES DE CAUSE COMMUNE

Des défaillances de cause commune sont des défaillances survenant de manière simultanée ou concomitante sur plusieurs composants et provenant de la même cause.

Des défaillances de cause commune sont systématiquement prises en compte dans chaque étude de système, au niveau des composants analogues redondants de ce système. La méthode employée pour la quantification est inspirée de la méthode des chocs (encore appelée méthode de la loi binomiale). Des défaillances de cause commune entre composants de systèmes différents ne sont pas considérées, à l'exception de celles clairement identifiées comme la perte d'un système support commun (tableau électrique, source froide, ...) ; celles-ci sont introduites directement comme événements génériques dans les évaluations probabilistes de séquences accidentelles .

Les composants pour lesquels des défaillances de cause commune sont considérées sont les suivants :

- pompes (à la sollicitation et en fonctionnement),

- moteurs (à la sollicitation et en fonctionnement),

- diesels (à la sollicitation et en fonctionnement),

- turbines (à la sollicitation et en fonctionnement),
- vannes (à la sollicitation),
- clapets (à la sollicitation et en fonctionnement pour les ruptures),
- soupapes (à la sollicitation),
- contacteurs 6,6 kV et 380 V (à la sollicitation),
- disjoncteurs (à la sollicitation),
- capteurs (à la sollicitation et en fonctionnement).

Pour chaque composant affecté par des défaillances de cause commune, toutes celles-ci sont distinguées. Par exemple pour le composant A appartenant à la famille de composants analogues (A, B, C, D), les différentes défaillances de cause commune sont les suivantes :

- défaillance affectant les composants A et B
- défaillance affectant les composants A et C
- défaillance affectant les composants A et D
- défaillance affectant les composants A, B et C
- défaillance affectant les composants A, B et D
- défaillance affectant les composants A, C et D
- défaillance affectant les composants A, B, C et D

4.1.1.5. PRISE EN COMPTE DU FACTEUR HUMAIN

La méthode utilisée est explicitée dans le chapitre 5. Succinctement, mentionnons que des erreurs humaines sont introduites comme événements de base dans les arbres de défaillance ou comme transitions dans les graphes d'états. Les probabilités associées sont déterminées au cas par cas selon la méthodologie générale développée à cet effet.

4.1.1.6. PRISE EN COMPTE DES TESTS ET DE LA MAINTENANCE

Les tests et tout particulièrement les essais périodiques sont pris en compte de la manière suivante :

- dans les indisponibilités cachées :

  Certaines défaillances peuvent n'être détectées que lors des essais périodiques. Les matériels concernés peuvent donc être indisponibles lorsqu'on les sollicite. Le taux d'indisponibilité est pris égal à $\lambda_a * T / 2$ (T étant la durée de l'intervalle entre tests), λ_a étant le taux de défaillance à l'arrêt. Cette méthode a été employée pour le calcul des indisponibilités cachées des capteurs et des composants électroniques.

- dans les indisponibilités liées à la mise en configuration du système pour l'essai périodique :

  Certains systèmes ou composants nécessitent une reconfiguration pour effectuer un essai périodique. S'ils ne disposent pas d'une mise en configuration automatique, ils peuvent alors être indisponibles durant toute la durée de l'essai. Dans ce cas, on a pris une indisponibilité du système ou du composant de taux égal à la durée de l'essai divisée par la périodicité de celui-ci.

En outre, des indisponibilités dues à des composants "laissés" en mauvaise configuration après un essai périodique sont prises en compte.

Les indisponibilités pour maintenance sont prises en compte. Celles-ci sont généralement introduites sous forme de "bulle" (ensemble de composants rendus indisponibles par la maintenance) dont les taux correspondants sont calculés à l'aide du retour d'expérience de la centrale de Paluel.

Pour des matériels fonctionnant en permanence et dont la défaillance est détectée immédiatement ou très rapidement, le taux d'indisponibilité est pris égal au produit du taux de défaillance en fonctionnement par le temps moyen de réparation (cas des baies Controbloc).

Pour les systèmes fonctionnant en permanence et modélisés par graphes d'états, les indisponibilités sont, de fait, prises en compte par les passages dans les états dégradés du graphe d'états.

4.1.1.7. PRISE EN COMPTE DU CONTROLE-COMMANDE

Le contrôle-commande est intégré dans chaque étude de système, jusqu'aux MAI (Modules Amplificateurs Intégrateurs) inclus pour le système SPIN et jusqu'aux baies incluses pour le système Controbloc.

Sont aussi introduites dans chaque étude de système les indisponibilités et les pertes en fonctionnement :

- du système d'air comprimé SAR,

- des tableaux électriques 125 V LBC et LBD,

- des tableaux électriques 30 V LDA et LDC,

- des tableaux électriques 380 V LLA à LLJ

Les tableaux 125 V équipement LBA et LBB sont traités comme les tableaux 6,6 kV secourus LHA et LHB et comme la source froide, en tant que systèmes supports.

Ils font donc l'objet d'études spécifiques et sont placés comme événements génériques en tête des arbres d'événements (voir ci-après chapitre 4.1.2.).

4.1.1.8. QUANTIFICATION DES RESULTATS

Les probabilités des événements indésirables sont calculées en utilisant des codes de calcul appropriés (voir ci-après chapitre 4.2.). Ces derniers permettent en outre une analyse qualitative des résultats obtenus : coupes minimales lorsqu'on utilise la méthode de l'arbre de défaillance et séquences dominantes lors de l'emploi des graphes d'états.

4.1.1.9. COMPARAISON AVEC LES INCIDENTS REELS

Les incidents réellement survenus jusqu'à fin 1987 sur les systèmes de sûreté des tranches nucléaires françaises de type à eau pressurisée ont été analysés et situés par rapport aux évaluations probabilistes de ces systèmes ; on a notamment vérifié que les causes et les fréquences de ces incidents n'étaient pas respectivement en contradiction avec les modèles qualitatifs et quantitatifs.

4.1.2. EVALUATION PROBABILISTE DES SEQUENCES ACCIDENTELLES

Pour étudier les scénarios possibles consécutifs à une situation incidentelle ou accidentelle, la principale méthode retenue a été la méthode des arbres d'événements. Elle consiste à :

- identifier les séquences d'événements menant à un accident (ou séquences accidentelles),
- 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. Le premier de ces événements est appelé "événement initiateur" ; les autres sont appelés "événements génériques". Ces derniers correspondent généralement aux missions des systèmes requis après l'apparition de l'événement 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 un endommagement du coeur. Seules les probabilités de ces séquences sont calculées.

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.

Dans le cas de scénarios de très longue durée (1 an), où les changements de configuration sont nombreux et où les séquences bouclées (défaillance, réparation, défaillance d'un même matériel) n'ont pas une probabilité négligeable, on a utilisé la méthode des graphes d'états enchaînés qui est la seule à pouvoir traiter ce genre de problème.

4.1.2.1. UTILISATION DE LA METHODE DES ARBRES D'EVENEMENTS

La construction et l'évaluation probabiliste d'un arbre d'événements peuvent s'avérer relativement longues et complexes et nécessitent habituellement une démarche itérative.

Une analyse fonctionnelle détaillée facilite la construction de l'arbre d'événements : elle consiste à identifier de manière précise toutes les fonctions de sûreté sollicitées par l'apparition de l'initiateur ou impliquées dans la maîtrise de l'accident. Des arbres d'événements "fonctions", où les événements génériques sont, en première analyse, des fonctions de sûreté, peuvent s'avérer très utiles dans une étape intermédiaire.

La construction définitive puis l'évaluation probabiliste dépendent étroitement des aspects suivants :

- la prise en compte des interactions fonctionnelles et temporelles,

- la quantification des séquences accidentelles,

- les renvois entre arbres d'événements.

On aborde successivement et succinctement ces trois aspects.

Les événements initiateur et génériques constitutifs d'un arbre d'événements ne sont pas nécessairement indépendants : il peut exister des interactions entre eux. Celles-ci sont de deux types :

- Interactions fonctionnelles

  Les événements génériques correspondant à la défaillance de systèmes sont généralement modélisés par des arbres de défaillance. Les événements de base constituant ces arbres peuvent être communs à plusieurs d'entre eux (composants communs, tableaux électriques alimentant des composants de systèmes différents, source froide refroidissant plusieurs systèmes...).

  Les probabilités d'occurrence de ces événements ne sont alors pas indépendantes.

- Interactions temporelles

  L'instant de démarrage d'un système, sa durée de fonctionnement peuvent être fonction de la durée de bon fonctionnement et de la durée d'indisponibilité d'un autre système dans le cas de systèmes fonctionnant en normal-secours.
  De plus, il peut y avoir un délai entre la défaillance d'un système et l'atteinte de conséquences inacceptables qui peut être mis à profit pour réparer le ou les systèmes dont la défaillance intervient dans la séquence accidentelle étudiée.
  La probabilité de défaillance d'un système ne peut dans ce cas être calculée indépendamment des séquences où sa défaillance est envisagée.
  La non prise en compte des interactions temporelles peut conduire à des calculs exagérément conservatifs : d'où le grand intérêt qu'il y a à les modéliser et à les calculer de manière réaliste.

Pour permettre sa quantification par un code de calcul, chaque arbre d'événements est décrit séquence par séquence ; seules les séquences à quantifier sont décrites (ce sont généralement celles qui mènent aux conséquences inacceptables). Pour chacune des séquences on précise :

- l'intervalle de temps sur lequel on examine le fonctionnement des systèmes,

- le délai avant conséquences inacceptables après l'occurrence des événements de la séquence,

- pour chaque système, son instant de démarrage ou son mode de fonctionnement (en normal secours de tel ou tel autre système) ou pour chaque erreur humaine, son instant d'apparition.

Dans les rares cas où il n'existe ni dépendances temporelles, ni dépendances fonctionnelles entre les événements génériques de l'arbre, la probabilité de chaque séquence est égale au produit des probabilités des événements génériques qui la constituent.

Une méthode a été développée pour calculer la probabilité de certains événements initiateurs des arbres d'événements. Ces événements initiateurs correspondent à la perte de systèmes redondants (cas des accidents de type H). Leur probabilité d'occurrence a été calculée par graphes d'états.

On obtient ainsi des séquences initiatrices qui s'étalent généralement sur une durée significative : un certain laps de temps peut s'écouler entre la première défaillance par laquelle débute la séquence et la dernière dont l'apparition provoque l'entrée dans la situation accidentelle. Ce laps de temps peut être mis à profit pour passer la tranche dans un état de repli où les conséquences de l'événement initiateur seront moindres.

Il convient alors d'établir un arbre d'événements pour une tranche en puissance et un autre pour une tranche en état de repli et donc de calculer la probabilité qu'une séquence débutée tranche en puissance se termine dans le même état ou se termine en état de repli. Dans des cas plus complexes, il peut y avoir, en outre, des états intermédiaires ; la répartition des séquences initiatrices se fait alors entre plusieurs arbres d'événements.

Les conséquences d'une séquence accidentelle d'un arbre d'événements peuvent être analogues à celles résultantes d'un événement initiateur étudié par ailleurs. Par exemple, un transitoire primaire peut provoquer la sollicitation d'une soupape du pressuriseur qui, si elle ne se ferme pas, provoque une brèche primaire qui fait l'objet d'une autre étude. Afin de ne pas refaire l'étude d'une telle situation, l'arbre relatif au transitoire primaire renvoie à l'arbre relatif à la brèche primaire correspondante. Cette démarche permet de calculer la totalité du risque résultant d'un événement initiateur donné (ici un transitoire primaire) sans avoir à dupliquer les modélisations.

4.1.2.2. UTILISATION D'UN ENCHAINEMENT DE GRAPHES D'ETATS

Pour étudier des scénarios à très long terme (par exemple un an pour les brèches primaires) où les changements de configuration, les possibilités de réparations multiples d'un même composant sont nombreuses et où les conditions minimales requises évoluent dans le temps, la seule méthode applicable est celle des graphes d'états enchaînés.

Les systèmes dont le mode de fonctionnement (redondance active ou passive...) évolue dans le temps, systèmes encore qualifiés de systèmes multiphasés, nécessitent de telles méthodes.

On découpe la période pendant laquelle les scénarios sont examinés en différentes phases où les configurations minimales sont constantes. Sur chacune des phases, on établit des graphes d'états modélisant le fonctionnement des systèmes. Chacun de ces graphes d'états peut être relatif à un ou plusieurs systèmes et correspondre à l'échec d'une ou plusieurs configurations minimales. Les graphes d'états ici considérés sont de type markovien.

Les conditions finales d'une phase servent au calcul des conditions initiales de la suivante. Cette méthode nécessite de connaître en fin de chaque phase la probabilité d'être dans les différents états du graphe et impose ainsi un traitement matriciel du graphe d'états.

Précisons que la première phase est traitée par arbres d'événements ; toutes les dépendances fonctionnelles pertinentes entre systèmes sont ainsi prises en compte. Les autres phases sont traitées par enchaînement de graphes d'états.

4.1.3. CALCUL D'INCERTITUDE

Le calcul d'incertitude a pour objet d'évaluer les incertitudes qui existent sur les résultats finaux, compte tenu des incertitudes affectant les données élémentaires.

On a retenu la méthode de simulation de Monte Carlo globale. Cette méthode a l'avantage d'être

très simple sur le plan du principe et rigoureuse. Elle a cependant le gros inconvénient d'être très coûteuse en temps calcul. C'est pourquoi cette simulation a été faite sur un modèle simplifié.

Un modèle simplifié de l'EPS-1300 a été élaboré. Pour chaque famille d'accidents, les séquences prépondérantes ont été conservées. Pour chacune de ces séquences, des modèles simplifiés des événements génériques concernés ont été élaborés (coupes prépondérantes pour un arbre de défaillance et séquences prépondérantes pour un graphe). Les critères d'élimination des séquences ou des coupes ont été choisis de façon à garantir la représentativité du modèle simplifié. Dans presque tous les cas le modèle simplifié représente plus de 90 % du modèle complet.

On a ainsi déterminé pour le risque global, pour celui lié à chaque famille d'accident ainsi que pour le risque par état standard de la tranche, un intervalle de confiance à 90 %, la moyenne, la médiane, la variance et le facteur d'erreur associés à chacun de ces risques.

4.2. INFORMATISATION

L'EPS-1300 devant rester, malgré sa complexité, révisable en fonction de l'évolution des données et des connaissances, son automatisation complète s'est imposée dès son lancement.

Le projet LESSEPS (Logiciel d'Etudes de Sensibilité basé sur des Systèmes Experts pour une EPS) fut donc mené, dès 1986, en parallèle des études.

L'ensemble des logiciels permettant l'informatisation de l'EPS-1300 se décompose comme suit :

- les codes de calcul (PHAMISS, MARKSMP, GSI et ISA) permettant le traitement qualitatif et quantitatif des modèles de sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité),

- le logiciel LESSEPS dont l'objectif principal est d'assurer l'enchaînement des codes de calcul précités,

- les systèmes experts EXPRESS et EXPGSI permettant la génération automatique de modèles (respectivement arbres de défaillance et graphes d'états),

- le logiciel LESSEPS-1300 (ou l'EPS-1300 informatisée) ou application du logiciel LESSEPS à l'EPS-1300.

4.2.1. LES CODES DE CALCUL

Quatre codes de calcul sont utilisés dans le cadre de l'EPS 1300 :

PHAMISS

Développé par l'organisme hollandais ECN (Stichting Energieonderzoek Centrum Nederland), ce code permet le traitement des arbres de défaillance. Après une étape de réduction booléenne dont le résultat est un ensemble de coupes minimales, celles-ci sont quantifiées pour aboutir au calcul de la défiabilité et/ou de l'indisponibilité du système. La recherche des coupes minimales peut être limitée par l'introduction d'un seuil sur l'ordre de ces coupes.

MARKSMP

Développé par la société ELF-AQUITAINE (FRANCE), ce code de calcul assure le traitement des graphes d'états de petite taille. La méthode mise en oeuvre s'appuie sur une résolution matricielle

des graphes de Markov. Ce code de calcul a été essentiellement utilisé pour traiter des enchaînements de graphes.

GSI

Développé par EDF, ce code est particulièrement adapté au traitement des systèmes séquentiels de grande taille. S'appuyant sur la théorie des graphes semi-markoviens, il permet en effet d'explorer localement un modèle de type graphe d'états sans que la construction complète de ce modèle ne soit nécessaire.
GSI peut chercher directement à partir de ce modèle l'ensemble de séquences d'événements menant à la panne du système. La recherche de ces séquences peut être limitée par l'introduction de seuils sur leur longueur ou sur leur probabilité.

Par ailleurs, GSI permet aussi de construire complètement le graphe lorsque celui-ci est de taille raisonnable, le traitement quantitatif associé étant alors de type matriciel.

ISA

Développé par EDF, ce code permet le traitement des arbres d'événements selon la méthode présentée au chapitre 4.1.2.

4.2.2. LE LOGICIEL LESSEPS

Conçu pour assurer la gestion automatisée des études de sûreté de fonctionnement, le logiciel LESSEPS a pour objectifs principaux :

- la gestion des données (données de fiabilité, résultats intermédiaires, résultats finaux),
- la gestion des modèles fournis par les études,
- l'enchaînement des exécutions, une exécution étant le traitement d'un modèle par un code de calcul,
- l'optimisation des études de sensibilité.

Les principes fonctionnels que les choix de conception informatique se sont ensuite astreints à respecter sont les suivants :

- regrouper dans un même catalogue les données relatives aux composants élementaires (modes de défaillance, temps de réparation ...),
- tirer profit du caractère modulaire d'une étude comme l'EPS-1300, en assurant tout à la fois :
  - . l'autonomie d'une étude partielle,
  - . la possibilité de fusionner ou d'enchaîner l'ensemble des résultats issus de cette étude avec ceux d'une autre (ou de l'ensemble des autres),
- assurer un stockage centralisé et codifié de l'ensemble des données nécessaires à la communication entre codes de calcul,
- conserver un historique des calculs réalisés en associant à chaque donnée la notion de version (référence horodatée).

Parmi les principaux choix de conception il convient de citer :

- l'utilisation des notions de réseau (formalisation des liens entre les diverses quantifications d'une étude) et de structure commune de données (structure d'accueil de l'ensemble des données) nécessaires à la réalisation d'une étude ou produites par cette étude : données amont, données d'interface entre codes, résultats ...,

- le développement d'un ensemble de logiciels destinés à la gestion automatisée des études (CHEF D'ORCHESTRE, EXTRACT, ...) et à l'optimisation des études de sensibilité.

4.2.3. LES SYSTEMES EXPERTS : EXPRESS ET EXPGSI

Les systèmes experts EXPRESS et EXPGSI ont été développés dans le cadre du "projet EPS-1300", pour faciliter l'étude des systèmes élémentaires les plus complexes.

Leur objectif est la génération automatique de modèles de sûreté de fonctionnement. Dans le cadre général de l'automatisation des études, ces systèmes experts se situent en amont du logiciel LESSEPS : leur but est de générer des modèles informatisés qui seront ensuite gérés par LESSEPS.

Le principe général de ces systèmes experts repose sur les deux constatations suivantes :

1) La plupart des systèmes étudiés peuvent être considérés comme des ensembles de "lignes" véhiculant un "fluide" (énergie thermohydraulique ou électrique, information, etc.).

2) La plupart des modes de défaillance des composants de ces systèmes peuvent être regroupés en deux types de "modes de défaillance principaux", en fonction de leurs conséquences sur le fluide véhiculé :

   - obstruction du fluide (circuit ouvert dans le cas électrique),

   - fuite externe du fluide (court-circuit dans le cas électrique).

Les modèles sont générés en deux étapes :

La première dite "inférence topologique" a pour but le regroupement des composants du système étudié en macro-composants, selon les conséquences de leurs défaillances principales.

La deuxième dite "inférence génératrice" a pour but de relier les causes de défaillance des composants aux modes de défaillance principaux et de déduire les conséquences sur le système, en termes de pertes de "chemins" (lignes de fluide).

EXPRESS est utilisé pour les systèmes statiques, et génère un modèle PHAMISS de type arbre de défaillance. EXPGSI est utilisé pour les systèmes séquentiels, et génère un modèle GSI (description en règles équivalentes à un graphe d'états).

4.2.4. LESSEPS-1300 (OU L'EPS-1300 INFORMATISEE)

L'entrée, dans le logiciel LESSEPS, d'une part de la base de données de l'EPS-1300 et, d'autre part, de tous les modèles issus des évaluations probabilistes de systèmes et de séquences accidentelles, a abouti à la création de LESSEPS-1300 (EPS-1300 informatisée). LESSEPS-1300 contient ainsi environ 200 arbres de défaillance, 150 graphes d'états et 200 arbres d'événements.

Notons que LESSEPS-1300 fonctionne sur un gros ordinateur de type IBM 3090 et qu'il est exécuté en environ 2 heures, ce temps ne comprenant pas le temps de génération des modèles par systèmes-experts.

5. FACTEURS HUMAINS

Le développement des méthodes d'Evaluation Probabiliste de la Fiabilité Humaine (EPFH) s'est appuyé sur les travaux antérieurs, et, plus particulièrement, ceux menés par l'Autorité de Sûreté américaine (NRC) et l'Electric Power Research Institute (EPRI).

Néanmoins, ces méthodes assez générales ne pouvaient être opérationnelles sans une adaptation au contexte de l'EPS-1300. Un important travail a donc été réalisé à cet effet.

De plus (et surtout), les bases expérimentales des données proposées par les méthodes antérieures n'étaient pas assez complètes. De toutes façons, ces données n'auraient pas été transposables directement au contexte d'EDF. C'est pourquoi, un gros effort de recueil de données de "terrain" en centrales et sur simulateurs a été mené. Le rôle considérable joué dans les EPFH de l'EPS 1300 par les données relevées sur simulateur en constitue d'ailleurs une des originalités.

Dans les paragraphes qui suivent, on explicite les éléments marquants de la prise en compte des facteurs humains dans les évaluations probabilistes de systèmes puis de séquences accidentelles, en insistant tout particulièrement sur ces dernières compte tenu de leur importance dans les résultats de l'EPS-1300.

5.1. FACTEURS HUMAINS DANS LES EVALUATIONS DE SYSTEMES

Les erreurs humaines se produisant en exploitation normale, mais susceptibles de contribuer à un accident ou de gêner sa récupération sont traitées dans les études de systèmes.

Certaines de ces erreurs sont prises en compte de manière implicite dans les données de fiabilité des matériels et, surtout, dans les données relatives aux défaillances de cause commune ; les fréquences d'initiateurs intègrent également des erreurs humaines. D'autres ne le sont pas et pour celles-ci, il est donc nécessaire d'utiliser une méthode d'analyse complémentaire.

Les erreurs sont modélisées dans les arbres de défaillances des études de systèmes, à l'aide d'événements de base standardisés. La création de ces événements de base est régie par des règles simples, qui permettent notamment de tenir compte des dépendances introduites par les pratiques d'exploitation (intervention sur des composants redondants lors d'un même quart, par exemple).

Les erreurs sont classées en quatre catégories en fonction des facteurs de récupération. Une probabilité comprise entre quelques 10^{-2} et 10^{-5} leur est alors affectée, en fonction de ces mêmes facteurs.

5.2. FACTEURS HUMAINS DANS LES EVALUATIONS DE SEQUENCES ACCIDENTELLES

5.2.1. DEMARCHE D'ENSEMBLE

La démarche décrite ci-après a été menée pour chaque famille d'initiateurs. Elle est itérative. Les familles les plus importantes ont donc fait l'objet de plusieurs EPFH successives. Les méthodes et modèles présentés ici sont ceux utilisés lors de la dernière phase de l'EPS-1300.

Les étapes d'une itération sont les suivantes :

a) Recherche et sélection des erreurs potentielles significatives

Les erreurs potentielles des opérateurs durant un accident donné sont recherchées par un examen systématique :

- des résultats d'essais sur simulateur,
- des consignes de conduite accidentelle disponibles sur la tranche.

En particulier, on envisage l'arrêt inopportun de tous les systèmes de sûreté requis. Une première sélection est alors faite par jugement, le critère principal étant la gravité des conséquences des erreurs. Puis, une première quantification de chaque famille d'initiateurs permet de mettre en évidence les erreurs significatives, qui seules sont soumises à une analyse approfondie.

b) Représentation des erreurs significatives

Sauf dans les cas très simples, on construit des arbres d'événements propres au Facteur Humain.

Après simplification éventuelle, les arbres relatifs au Facteur Humain sont incorporés dans les arbres d'événements des études de séquences accidentelles. Ces derniers font apparaître explicitement les erreurs humaines, pour assurer une bonne lisibilité des modèles de l'EPS-1300.

c) Analyse qualitative des erreurs significatives

L'analyse qualitative des erreurs significatives est menée en parallèle avec leur quantification. Elle consiste à recueillir des informations sur les facteurs susceptibles d'influer sur la réalisation de chaque tâche étudiée : caractéristiques de la tâche, interface homme-machine, organisation, formation des opérateurs.

Ces informations sont indispensables pour la quantification (orientation du jugement, données "d'entrée" des modèles de quantification). En aidant à mettre en évidence les principaux facteurs d'erreur, elles permettent également souvent de suggérer des améliorations de l'interface homme-machine.

Menée sans précautions, cette étape pourraît être très lourde. La sélection préalable des erreurs significatives, et l'utilisation intensive des résultats d'essais sur simulateur la facilitent considérablement.

d) Quantification des erreurs significatives

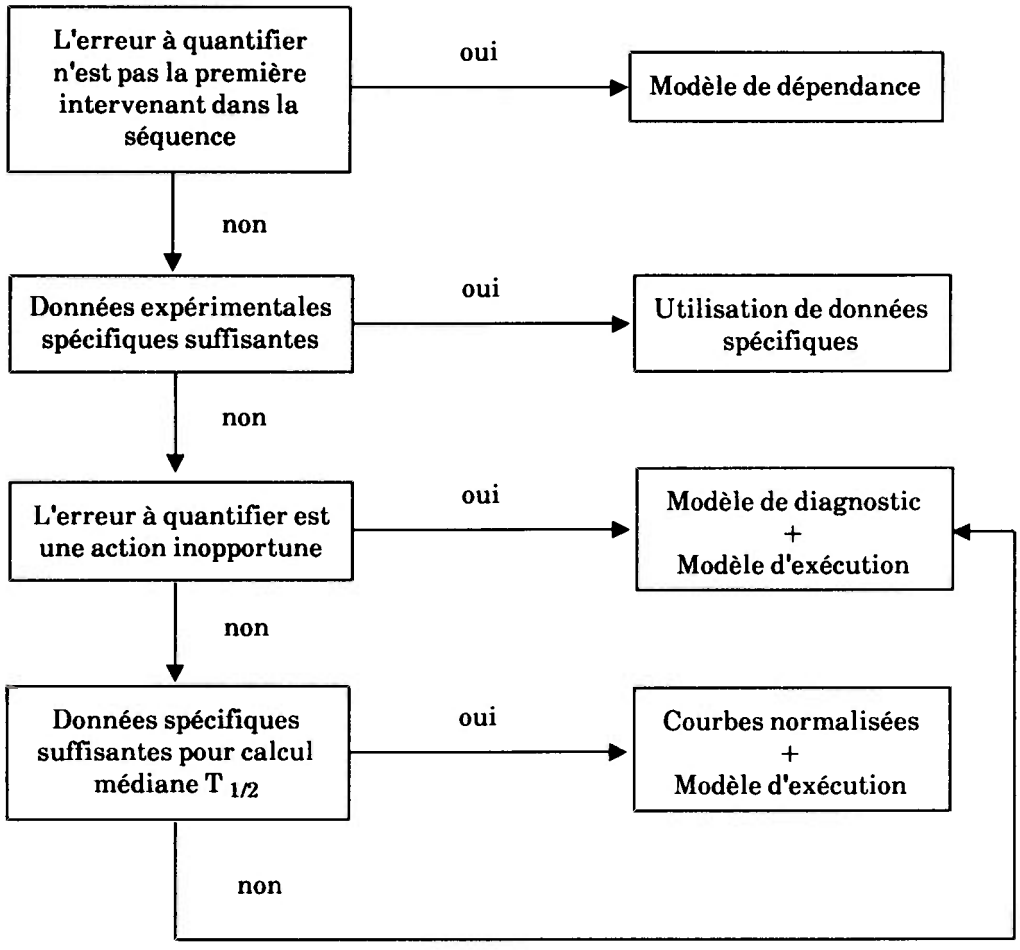
Il s'agit d'attribuer à chaque erreur une probabilité. La figure suivante guide le choix du modèle de quantification.

e) Prise en compte de l'organisation de crise et de l'approche SPI-U1 (ISR)

On admet que grâce à l'Organisation de Crise, aucune erreur de stratégie ne pourra se prolonger ou être commise au-delà de 4 heures après un accident, cette hypothèse étant compatible avec les délais de mise en place observés lors des exercices de crise.

L'ISR n'est pris en compte que pour son rôle principal de récupération des séquences les plus dégradées, menant au dépassement de critères de sa consigne de surveillance (SPI). Son éventuelle action de récupération d'anomalies moins graves est négligée. Les conduites selon les consignes événementielles (opérateurs), d'une part, et selon SPI et U1 (ISR), d'autre part, font l'objet d'événements génériques spécifiques dans les arbres d'événements. Ceci permet de mettre clairement en évidence l'impact de "l'approche SPI-U1".

CHOIX DES METHODES DE QUANTIFICATION



f) Evaluation de l'incertitude

Dans les EPFH, on a tenu compte des incertitudes liées :

- aux modèles de quantification du Facteur Humain (hors écart entre comportements sur simulateur et en réel),

- à l'utilisation de ces modèles (choix des modèles, jugements divers nécessaires à leur utilisation...),

- à l'écart entre le comportement des opérateurs sur simulateur et en réel.

L'incertitude est évaluée par jugement selon la méthode suivante. Chaque modèle de quantification est considéré comme le produit de trois lois log-normales associées aux trois sources d'incertitude ci-dessus. On estime par jugement les bornes (Bs et Bi) entre lesquelles se situerait le modèle pour chaque source d'incertitude, en l'absence des autres. On en déduit alors par calcul un facteur d'erreur pour chacune des trois lois associées, puis pour le modèle lui-même, qui est leur produit.

5.2.2. SOURCES D'INFORMATION

L'équipe EPS-1300 a pu en permanence s'appuyer sur les compétences d'un ingénieur de la centrale de Paluel. Cet ingénieur a fourni au jour le jour de nombreuses informations et il a réalisé des enquêtes systématiques très précieuses pour les EPFH, notamment pour améliorer leur réalisme.

Par ailleurs, l'EPS-1300 a fait largement appel aux données issues des essais sur simulateurs (ou essais de Mise en Situation Recréée - MSR) ; ces essais sont spécialement organisés par EDF pour permettre l'observation du comportement des opérateurs en situation perturbée. Un essai dure entre une à trois heures et vise à recréer des conditions, aussi réalistes que possible, d'occurrence de l'incident ou de l'accident retenu et du comportement des opérateurs ; bien évidemment les opérateurs ne connaissent pas la nature de l'incident ou de l'accident qui est simulé. 204 essais ont été réalisés de 1982 à fin 1988 sur les simulateurs des salles de commande 900 MWe et 1300 MWe. 78 équipes d'opérateurs y ont participé.

5.2.3. MODELES QUANTITATIFS

Ces modèles servent à attribuer une probabilité à une erreur humaine en conduite accidentelle, en fonction des caractéristiques de la situation fournies par l'analyse qualitative.

On distingue les modèles relatifs aux interventions de l'équipe d'opérateurs hors ISR, et ceux spécifiques aux actions de récupération propres à l'ISR. Des modèles ont ainsi été élaborés pour :

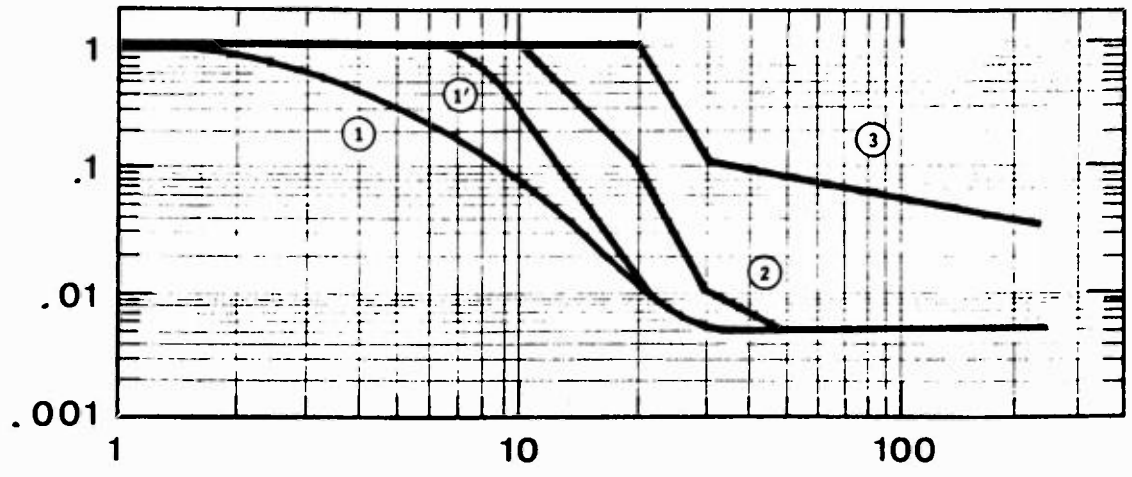
- le diagnostic de l'accident
- l'exécution des actions après le diagnostic
- les actions propres à l'ISR (dans le cadre de l'approche SPI-U1)

On a également utilisé le modèle de SWAIN pour la prise en compte des dépendances entre actions. On se contente ici, dans un souci d'illustration, de décrire succinctement un modèle de diagnostic et le modèle relatif à l'ISR.

a) <u>Modèle de diagnostic (opérateurs, hors ISR)</u>

La probabilité d'échec du diagnostic $P_{\bar{D}}$ est déterminée à l'aide du modèle de diagnostic présenté ci-après.

PROBABILITE D'ECHEC DU DIAGNOSTIC $P_{\bar{D}}$



Délai disponible pour effectuer le diagnostic (minutes)

Les courbes proposées correspondent à différents niveaux de difficulté du diagnostic. Les courbes 1 et 1' s'appliquent aux diagnostics les plus faciles (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.

Des 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 simulateur "MSR" pour les délais inférieurs à 20 mn, et extrapolées des résultats d'essais au-delà. Les courbes 2 et 3 sont inspirées de celles généralement utilisées aux Etats-Unis : elles demeurent néanmoins, tout en étant plus conservatives, assez hypothétiques.

b) Modèle relatif à l'approche SPI-U1 (ISR)

Un modèle spécifique est utilisé pour prendre en compte les actions de récupération propres à l'ISR, dans le cadre de l'approche SPI-U1. En effet, la mise en oeuvre de l'approche SPI-U1 repose principalement sur l'ISR. Ce dernier n'étant pas en permanence en salle de commande, la probabilité d'échec de SPI-U1 peut s'écrire :

$$P = A(T) + (1 - A(T)) \cdot P_{\bar{E}I\bar{A}}$$

- A (T) probabilité d'absence de l'ISR à T, instant au-delà duquel il est trop tard pour mettre en oeuvre les récupérations selon SPI-U1.

- $P_{\bar{E}I\bar{A}}$ probabilité d'échec, l'ISR étant présent, toutes causes confondues.

A (T) est obtenue à partir des distributions :

- du délai pour décider d'appeler l'ISR suite à l'accident initiateur,

- du délai pour joindre l'ISR,

- du délai de déplacement de l'ISR.

La première distribution est issue des essais "MSR", les deux autres d'une enquête spécifique en centrale.

P_{EIA} est basée à la fois sur les essais "MSR" et un "modèle de dépendance" et est fonction du type d'action à entreprendre.

- $P_{\bar{E}I\bar{A}} = 5 \times 10^{-2}$ lorsqu'il suffit d'effectuer des actions de récupération décrites par SPI,

- $P_{\bar{E}I\bar{A}} = 3 \times 10^{-1}$ ou 10^{-1} (en fonction du délai disponible) lorsque la situation est si dégradée que l'application de U1 est nécessaire.

Au total, la probabilité P est souvent assez élevée (de l'ordre de 10^{-1}), car elle prend en compte les inévitables phénomènes de dépendance entre l'équipe d'opérateurs et l'ISR. La probabilité finale d'échec des interventions humaines d'une séquence accidentelle est le produit des probabilités d'échec de l'équipe et de l'ISR.

6. ENSEIGNEMENTS ET PERSPECTIVES

L'interprétation des résultats a déjà fait apparaître un certain nombre d'enseignements généraux ou ponctuels qui ont été déjà largement abordés mais qui peuvent être regroupés par grands thèmes (la conception, l'exploitation, les méthodes et l'informatisation). Les perspectives sont ensuite présentées de manière succincte.

6.1. ENSEIGNEMENTS RELATIFS A LA CONCEPTION

Plusieurs enseignements majeurs sont à souligner.

Le risque de 10^{-5}/tranche x an, est réparti entre différentes familles et différents états de la tranche.

Cela signifie que le dimensionnement classique - qui reste indispensable - complété par les spécificités de l'approche française a permis d'obtenir un niveau de sûreté homogène.

Cela signifie également que pour progresser des réflexions doivent être menées pour renforcer les efforts déjà entrepris et pour s'interroger sur les points difficiles identifiés.

6.1.1. ENSEIGNEMENTS GENERAUX

a) Les états d'arrêt méritent une attention toute particulière. L'extension du domaine couvert par les procédures accidentelles à ces états est une amélioration sensible. Il convient de poursuivre les réflexions dans les domaines suivants :

- procédures de conduite (amélioration, extension de la conduite accidentelle par états de la tranche),
- aides-opérateurs (aides informatiques par exemple),
- amélioration de la conception (introduction de mesures adaptées aux états d'arrêt),
- protection automatisée ou conception différente pour les paliers futurs,
- analyse des différentes configurations d'exploitation.

b) La fiabilité moyenne de certains composants importants doit inciter le concepteur à s'interroger sur les causes de certains problèmes. Tout composant peut connaître des défaillances ; la mise en place d'une organisation efficace au niveau du retour d'expérience permet d'identifier ces défauts et d'y remédier. Deux de ces causes mériteraient cependant d'être approfondies

Le matériel nucléaire ne correspond pas toujours à du matériel standard car il doit répondre à des normes précises, en particulier dans le cadre de l'assurance-qualité. Il ne faut pas pour autant que ce matériel soit totalement spécifique, déconnecté de l'expérience générale des constructeurs : en un mot, il serait bon de s'attacher à obtenir et exploiter un matériel industriel et non des prototypes (sauf bien entendu pour des besoins spécifiques impératifs).

Le caractère impératif de ces besoins mérite également d'être souligné. Il est souvent la conséquence de l'application de règles strictes. Cela conduit à un cahier des charges très dur à respecter et à des contraintes lourdes pour le matériel lui-même. Le temps de démarrage des diesels (quelques secondes) peut être cité à titre d'exemple ; l'exigence à ce niveau est la conséquence du cumul entre un accident donné et la perte des alimentations électriques externes (il n'est pas question de discuter du bien fondé ou non de cette règle ici).

En conclusion, il serait très certainement opportun d'étudier non seulement les modifications matérielles remédiant aux défaillances mais également de s'interroger sur les causes profondes de ces défaillances.

c) L'EPS-1300 confirme l'importance des Facteurs Humains pour la sûreté. La prise en compte de ces facteurs au niveau de la conception est donc importante.

Il paraît essentiel d'orienter la conception des systèmes dans le sens d'une moindre complexité et d'une plus grande tolérance aux erreurs.

L'automatisation peut apporter dans des cas précis certaines solutions. Cependant, elle est susceptible d'accroître la complexité. Il est de plus impossible de tout prévoir et optimiser, a priori, depuis le bureau d'études. Par ailleurs, l'EPS-1300 a montré que les actions inopportunes peuvent avoir un poids significatif, notamment dans les états où existent des protections automatiques (par exemple l'arrêt inopportun de l'injection de sécurité lors des accidents de perte de réfrigérant primaire en puissance). L'automatisation ne saurait donc dispenser le concepteur de la nécessité de faciliter le diagnostic et la récupération des incidents. Et ceci d'autant plus que la plupart des erreurs importantes mises en évidence sont des erreurs où intervient l'interprétation de la situation et non de simples erreurs de manipulation (arrêt inopportun des systèmes de sûreté, diagnostic tardif, ...).

L'EPS-1300 peut guider certaines actions dans ce domaine, car elle a mis en évidence des informations essentielles pour l'interprétation et la récupération de séquences importantes : alarme de "très bas niveau bâche ASG" (brèches sur le secondaire), alarme "flux élevé à l'arrêt" (dilution intempestive dans l'état d), alarmes et mesures de niveau primaire dans l'état d (APRP)...

d) Un autre élément général est le poids important des défaillances de cause commune dont l'incertitude est élevée.

Le concepteur a résolu ce problème dans certains cas, par la diversification. Citons en exemple, pour mémoire, les groupes de pompage de l'alimentation de secours des générateurs de vapeur : motopompes et turbopompes. Il convient, pour les paliers futurs, de réfléchir au meilleur moyen de mettre en oeuvre ce principe et d'en évaluer le bénéfice même si cela est difficile au vu du seul retour d'expérience.

e) Les apports de l'Approche par Etats : les études probabilistes mettent en évidence le fait qu'une situation dégradée ne peut résulter que d'un cumul d'événements.

Actuellement, EDF développe (et a déjà implanté sur deux tranches 1300 P'4) l'approche par états généralisée qui vise à remplacer l'approche événementielle classique de la conduite post-accidentelle. Basée non plus sur le diagnostic d'un événement précis mais sur celui de l'état de la tranche représentée par des paramètres physiques (primaire, secondaire et enceinte), elle permet non seulement d'apporter une réponse à l'opérateur en cas de cumuls d'incidents mais également grâce à des réorientations, de rattraper des erreurs éventuelles.

Le gain apporté par cette nouvelle approche n'a pu être évalué dans le cadre de l'EPS-1300 ; il est cependant clair qu'elle devrait apporter certaines réponses aux problèmes posés par les erreurs humaines.

6.1.2. SEQUENCES SPECIFIQUES

Des enseignements plus ponctuels peuvent être tirés de l'examen de certaines séquences particulières. Ces séquences ont déjà été décrites précédemment et ont, pour certaines d'entre elles, induit des modifications en cours sur les tranches nucléaires ; de plus la réflexion générale faite sur les états d'arrêt couvrira certaines d'entre elles.

Il conviendra d'engager des réflexions approfondies sur la séquence des brèches interfaces, en particulier pour les réacteurs futurs. Il est également nécessaire de s'interroger sur les accidents de dilution, dans la mesure où ces initiateurs n'apparaissent pas de façon habituelle dans les EPS.

Citons comme dernier exemple les transitoires suivis d'une défaillance de l'arrêt d'urgence (ATWS). Une séquence dominante est liée au mode commun de refus d'ouverture des disjoncteurs d'arrêt d'urgence. D'ores et déjà, il a été décidé que, sur le palier futur N4, une diversification serait mise en place, en envoyant également un ordre d'ouverture aux disjoncteurs des groupes d'alimentation électrique des mécanismes de manoeuvre des grappes.

6.2. ENSEIGNEMENTS RELATIFS A L'EXPLOITATION

6.2.1. ENSEIGNEMENTS DANS LE DOMAINE DE LA CONDUITE

a) Aide à la formation des équipes de conduite

- Identification des séquences prépondérantes

  Des efforts importants sont consentis pour améliorer de façon permanente la compétence des opérateurs. L'EPS peut servir à parfaire cette formation. Les instructeurs feront approfondir aux stagiaires aussi bien sur le plan théorique que sur le plan pratique (sur simulateur) les séquences prépondérantes.

- Mise en évidence de l'importance des états d'arrêt

  Le deuxième enseignement fondamental est la nécessité de sensibiliser les opérateurs à l'importance des états d'arrêt. Ce ne sont d'ailleurs pas seulement les opérateurs qui doivent être sensibilisés. Des réflexions pourraient être entreprises sur l'organisation des arrêts pendant lesquels les spécifications techniques doivent être respectées avec autant de rigueur qu'en puissance. Il faudrait en particulier voir dans quelle mesure la durée de l'état d pourrait être réduite.

- Amélioration de l'interface homme-machine

  Les essais sur simulateur "MSR" et l'analyse systématique des consignes de conduite accidentelle réalisés pour l'EPS-1300 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 formulation 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).

b) Développement d'outils d'analyse

- Outil d'analyse des données

Les résultats, aussi bien qualitatifs que quantitatifs obtenus sur le site, ont permis de fournir à l'EPS-1300 des données de qualité et de conférer aux études un réalisme nécessaire.

Des systèmes informatiques locaux ont été utilisés pour le recueil d'informations. Des programmes de dépouillement automatique ont été développés pour faciliter l'extraction d'informations pertinentes d'une très grande quantité de données disponibles. Non seulement ils ont permis d'obtenir des données de fonctionnement et d'indisponibilité des matériels mais ils ont donné aussi des informations sur le dysfonctionnement des tranches.

Ces outils informatiques développés pour l'EPS-1300 sont actuellement des maquettes opérationnelles. Leur industrialisation pourrait être faite pour apporter une aide dans des domaines tels que :

- l'analyse des transitoires importants d'exploitation, calcul des durées de fonctionnement des différents composants, élaboration des taux d'indisponibilité des matériels et systèmes sous l'angle des consignations ;

- l'élaboration et le suivi d'indicateurs locaux de performances en matière de sûreté.

- Outil d'analyse des événements

L'objectif dans cet axe de réflexion pourrait être de créer un outil permettant d'analyser de manière probabiliste, en favorisant l'aspect qualitatif, les divers événements pouvant survenir en centrale et ce faisant de favoriser une démarche individuelle et collective dans le cadre de la culture de sûreté.

Au niveau des centrales, cet outil pourrait permettre d'analyser de manière homogène un même incident ou événement et donc d'apporter une meilleure connaissance de l'installation en situation perturbée.

En outre, il pourrait permettre de mettre en évidence les matériels contribuant fortement à la sûreté dans une situation donnée et pouvant nécessiter une surveillance particulière.

Dans les centres de formation, un tel outil basé sur la méthode des arbres d'événements pourrait être utilisé :

- pour introduire et expliquer la démarche d'analyse probabiliste de sûreté,

- pour mettre en évidence les matériels et les erreurs humaines faisant partie des séquences prépondérantes pouvant conduire à des conséquences inacceptables.

L'application informatique LESSEPS-1300, développée dans le cadre de l'EPS-1300, a pour rôle de générer l'ensemble des enchaînements complexes des codes de calcul et de permettre le traitement d'un volume important de données. Elle contient toute la base de connaissance, la logique et les résultats. Il pourrait être intéressant de développer un modèle simplifié sur micro-ordinateur pouvant être utilisé, en fonction d'objectifs préalablement définis, et donnant aux utilisateurs une démarche automatisée et d'une constante rigueur dans l'analyse d'une situation.

6.2.2. ENSEIGNEMENTS DANS LE DOMAINE DE LA MAINTENANCE

a) Réflexions sur les problèmes d'interventions relatives à des voies redondantes

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.

b) 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-1300 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 ; ceci permettra là encore de hiérarchiser les besoins et de focaliser les efforts d'études ;

- 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 qu'aurait le 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 les matériels concernés que sur les périodicités et/ou la nature des essais.

6.3. ENSEIGNEMENTS RELATIFS AUX METHODES ET A L'INFORMATISATION

Un certain nombre d'enseignements majeurs peuvent être d'ores et déjà mis en évidence sur le plan des méthodes et des logiciels d'analyse probabiliste. Ces enseignements sont à replacer dans le cadre des défis méthodologiques et informatiques que contenaient le projet EPS 1300, à savoir principalement :

- innover sur certains aspects méthodologiques,

- développer des méthodes pour une étude de grande ampleur,

- créer le logiciel LESSEPS-1300.

6.3.1. METHODES

a) Méthodes d'analyse probabiliste des systèmes de sûreté

La méthodologie générale utilisée s'est révélée très complète et adaptée à des analyses très détaillées. Insistons tout particulièrement sur deux enseignements importants.

Les systèmes-experts ont été utilisés pour l'évaluation de plusieurs systèmes de sûreté, thermo-hydrauliques et électriques. Prenons le cas du système d'alimentation de secours des générateurs de vapeur ; le système-expert "EXPRESS" a été employé pour la construction d'arbres de défaillance liées à une cinquantaine de missions différentes. Ce système-expert a permis de réaliser une analyse fine de toutes les missions du système et ainsi de diminuer le conservatisme de l'analyse. L'expérience a montré que l'ajout de missions supplémentaires était facilement effectué, le système-expert générant rapidement les arbres de défaillance supplémentaires à partir de la base commune de faits et de règles.

D'une manière générale, la révision des études réalisées, notamment par suite de l'idendification des nouvelles missions à considérer dans le cadre des études de séquences accidentelles, s'est ainsi trouvée facilitée par l'emploi des systèmes-experts EXPRESS et EXPGSI.

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'équipe de réparateurs parfois inférieur au nombre de réparations à effectuer. En outre, elle donne généralement des résultats rigoureux et non approchés.

b) Méthodes d'analyse probabiliste des séquences accidentelles

La méthodologie générale utilisée s'est révélée adaptée à l'évaluation de scénarios d'accident, parfois fort complexes, et dans tous les états du réacteur. La méthode de l'arbre d'événements a pris en compte les dépendances de tous types entre événements génériques ; l'introduction dans l'arbre de l'éventuelle disparition de l'événement initiateur (par suite, par exemple, d'une réparation) a permis le calcul direct de la probabilité des séquences accidentelles. La méthode des graphes d'états a confirmé son intérêt pour la modélisation des phases accidentelles à long terme lorsque les composants sont réparables ; le développement de codes de calculs permettant d'enchaîner les calculs liés à différentes phases de mission à long terme a été très utile.

c) Méthodes de prise en compte des défaillances de cause commune

Les défaillances de cause commune ont été systématiquement prises en compte au niveau des composants élémentaires (pompes, vannes, disjoncteurs, etc.) à l'aide d'une démarche combinant la méthode des chocs (loi binomiale) et le facteur β. Les modèles comme les arbres de défaillance qui les intégrent 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.

d) Méthodes de prise en compte du Facteur Humain

La méthode d'identification des erreurs humaines, méthode éprouvée sur le plan international, 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 200 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.

6.3.2. 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 (3000),
- le caractère modulaire des études.

LESSEPS-1300 contient environ 350 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 le modèle EPS-1300 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 très facile de rajouter une étude de système ou de séquences accidentelles.

LESSEPS a confirmé son grand intérêt lors de la phase définitive ; l'ensemble des résultats de l'EPS-1300 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.

L'utilisation de LESSEPS par l'IPSN pour une tranche nucléaire du palier 900 MWe a conduit à l'obtention de LESSEPS-900 et a confirmé les mêmes avantages.

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 actuellement de LESSEPS à d'autres gammes d'ordinateurs et notamment aux stations de travail.

6.4. PERSPECTIVES

Le projet EPS-1300 n'a pas été conduit pour rester une étude sans lendemain. Outre la modélisation de la tranche, la quantification, les conclusions et les enseignements qui ont pu en être tirés, un outil informatique a été élaboré. Il va permettre de réaliser des études d'application dans plusieurs domaines et sur différents paliers.

Citons simplement quelques exemples :

- les études du palier N4,

- la révision des spécifications techniques d'exploitation,

- le programme de travail relatif au projet REP 2000, futures tranches d'EDF.

Les modèles seront donc applicables aux tranches en service, en construction ou en projet ; dans chaque cas ils peuvent apporter un éclairage nouveau, des enseignements, qui combinés à d'autres éléments, feront progresser la sûreté des tranches.

Il faut également garder en mémoire le fait que l'ensemble de ces études repose sur des bases de données et une analyse du retour d'expérience qu'il faudra poursuivre et enrichir.

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

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.

REFERENCE

[1] Etude Probabiliste de Sûreté d'une tranche du Centre de Production Nucléaire de PALUEL
Rapport de synthèse - EDF - 31 mai 1990

ANNEXE 1

PRINCIPAUX SIGLES ET ABREVIATIONS FIGURANT DANS CE RAPPORT

3 pages

1. ORGANISMES, ORGANISATIONS

CPN : Centre de Production Nucléaire
DE : Direction de l'Equipement d'EDF
DER : Direction des Etudes et Recherches d'EDF
DPT : Direction de la Production et du Transport d'EDF
EDF : Electricité de France
ELC : Equipe Locale de Crise
ENC : Equipe Nationale de Crise
EPRI : Electric Power Research Institute (USA)
IGSN : Inspection Générale pour la Sûreté Nucléaire d'EDF
INPO : Institute of Nuclear Power Operation (USA)
IPSN : Institut de Protection et de Sûreté Nucléaire
ISR : Ingénieur de Sûreté Radioprotection
NRC : Nuclear Regulatory Commission (USA)
ONC : Organisation Nationale de Crise
PCC : Poste de Commandement de Contrôles
PCD : Poste de Commandement Direction
PCL : Poste de Commandement Local
RNE : Réacteurs Nucléaires et Echangeurs
SCSIN : Service Central de Sûreté des Installations Nucléaires
SEPTEN : Service Etudes et Projets Thermiques et Nucléaires
SPT : Service de la Production Thermique

2. SYSTEMES ET MATERIELS

ARE : Alimentation Régulée en Eau des GV
ASG : Alimentation de Secours des GV
BC : Branche Chaude
BF : Branche Froide
EAS : Circuit d'aspersion de l'enceinte
GCT : Contournement turbine
GMPP : Groupe Motopompe Primaire
GV : Générateur de Vapeur
IS : Injection de Sécurité (voir RIS)
LAi : Distribution électrique 230 V continu

LBi	:	Distribution électrique 125 V continu
LCi	:	Distribution électrique 48 V continu
LDi	:	Distribution électrique 30 V continu
LGi	:	Distribution électrique 6,6 kV
LHi	:	Distribution électrique 6,6 kV secouru
LLi	:	Distribution électrique 380 V secouru
LNi	:	Distribution électrique 220 V
MAI	:	Module Amplificateur - Inverseur
MRB	:	Module Relais Bistable
MRM	:	Module Relais Monostable
RCP	:	Circuit Primaire
RCV	:	Circuit de contrôle volumétrique et chimique
REA	:	Circuit d'appoint en eau et en bore
RIS	:	Circuit d'injection de sécurité
(R)ISBP	:	Circuit d'injection de sécurité basse pression
(R)ISMP	:	Circuit d'injection de sécurité moyenne pression
RPR	:	Système de protection du réacteur
RRA	:	Circuit de réfrigération à l'arrêt
RRI	:	Circuit de réfrigération intermédiaire
SAR	:	Distribution d'air comprimé de régulation
SEC	:	Circuit d'eau brute secourue
SPIN	:	Système de Protection Intégré Numérique
TA	:	Transformateur Auxiliaire
TP	:	Transformateur Principal
TS	:	Transformateur de Soutirage

3. RETOUR D'EXPERIENCE

AIC	:	Aide Informatisée aux Consignations
DCC	:	Défaillance de Cause Commune
DF	:	Donnée de Fiabilité
EI	:	Evénement Initiateur
F.E.	:	Fichier des Evénements
MSI	:	Mise en Service Industriel
NPRDS	:	Nuclear Plant Reliability Data System
PF	:	Profil de Fonctionnement
S.R.D.F.	:	Système de Recueil de Données de Fiabilité

4. METHODES ET INFORMATISATION

AMDE : Analyse des Modes de Défaillance et de leurs Effets
BDF : Base de Données de Fiabilité
EPFH : Evaluation Probabiliste de la Fiabilité Humaine
MSR : Mise en Situation Recréée
SCD : Structure Commune de Données

5. SEQUENCES ACCIDENTELLES

APRP : Accident par Perte de Réfrigérant Primaire
ATWS : Transitoire suivi d'une défaillance de l'arrêt d'urgence
PDS : Perte de Source
RTE : Rupture de Tuyauterie d'Eau
RTGV : Rupture de Tube(s) de Générateur de Vapeur
RTS : Rupture de Tuyauterie Secondaire (eau ou vapeur)
RTV : Rupture de Tuyauterie Vapeur
TGTA : Transitoire Secondaire
TRCP : Transitoire Primaire
H1 : Perte totale de la source froide
H2 : Perte totale de l'eau alimentaire des générateurs de vapeur
H3 : Perte totale des alimentations électriques secourues

ANNEXE 2

RESULTATS DE L'EPS-1300

1 page

Les résultats d'ensemble de l'EPS-1300 sont présentés ci-après sous la forme d'un tableau où figurent les risques d'endommagement du coeur par famille et par état ainsi que les bornes de l'intervalle de confiance à 90 %.

Rappelons que cinq états de la tranche sont considérés :

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

Famille d'initiateurs	Fréquence d'endommagement du coeur dans l'état initial considéré (/tranche x an)							
	a	b	c	d	e	Total par famille	Bornes de l'intervalle de confiance à 90 % inf.	sup.
APRP	$1{,}5\ 10^{-6}$	$5{,}2\ 10^{-7}$	$2{,}0\ 10^{-6}$	$2{,}8\ 10^{-6}$	//	$6{,}8\ 10^{-6}$	$4{,}7\ 10^{-7}$	$1{,}8\ 10^{-5}$
ATWS	$1{,}2\ 10^{-6}$	//	//	--	--	$1{,}2\ 10^{-6}$	$3{,}1\ 10^{-7}$	$3{,}0\ 10^{-6}$
TRCP	$2{,}4\ 10^{-7}$	$4{,}3\ 10^{-10}$	$8{,}7\ 10^{-8}$	$5{,}8\ 10^{-7}$	//	$9{,}1\ 10^{-7}$	$2{,}1\ 10^{-8}$	$2{,}1\ 10^{-6}$
RTS	$7{,}6\ 10^{-7}$	$5{,}7\ 10^{-9}$	--	--	--	$7{,}6\ 10^{-7}$	$6{,}3\ 10^{-8}$	$2{,}3\ 10^{-6}$
PDS	$1{,}3\ 10^{-7}$	//	//	//	//	$1{,}3\ 10^{-7}$	$3{,}8\ 10^{-9}$	$2{,}7\ 10^{-7}$
RTGV	$4{,}6\ 10^{-7}$	$1{,}2\ 10^{-9}$	//	--	--	$4{,}6\ 10^{-7}$	$5{,}4\ 10^{-8}$	$1{,}0\ 10^{-6}$
TGTA	$4{,}5\ 10^{-8}$	//	--	--	--	$4{,}5\ 10^{-8}$	$2{,}1\ 10^{-9}$	$1{,}1\ 10^{-7}$
H1(*)	$8{,}7\ 10^{-8}$	$2{,}5\ 10^{-8}$	$7{,}1\ 10^{-9}$	$5{,}3\ 10^{-10}$	//	$1{,}2\ 10^{-7}$	$1{,}5\ 10^{-8}$	$9{,}6\ 10^{-7}$
H2	$2{,}5\ 10^{-7}$	$1{,}0\ 10^{-8}$	--	--	--	$2{,}6\ 10^{-7}$	$1{,}4\ 10^{-8}$	$3{,}8\ 10^{-7}$
H3(*)	$2{,}5\ 10^{-8}$	$2{,}1\ 10^{-8}$	$1{,}0\ 10^{-8}$	$1{,}6\ 10^{-8}$	//	$7{,}2\ 10^{-8}$	$1{,}0\ 10^{-8}$	$5{,}0\ 10^{-7}$
Total par état	$4{,}7\ 10^{-6}$	$5{,}8\ 10^{-7}$	$2{,}1\ 10^{-6}$	$3{,}4\ 10^{-6}$	//	$1{,}08\ 10^{-5}$		
TOTAL	$1{,}08\ 10^{-5}$						$2{,}2\ 10^{-6}$	$2{,}1\ 10^{-5}$

// : négligeable
--- : sans objet
(*) : résultats des études réalisées pour le palier N4, antérieurement à l'EPS-1300.

ANNEXE 3

SEQUENCES ACCIDENTELLES PREPONDERANTES

2 pages

Le tableau qui suit présente la liste des vingt séquences accidentelles prépondérantes de l'EPS-1300 ; ces dernières sont repérées par la famille et le numéro de la sous-famille concernée (1ère colonne), le libellé (2ème colonne), leur fréquence d'occurrence par tranche et par an (3ème colonne), le pourcentage par rapport au total (4ème colonne).

On peut remarquer que :

- deux séquences seulement pèsent plus de 10 % de l'ensemble,

- cinq familles interviennent dans les vingt premières séquences (APRP, ATWS, TRCP, RTGV, RTS).

Le même "phénomène" peut être mis en évidence pour l'état a, les séquences prépondérantes ATWS 2 ($5{,}9.10^{-7}$), RTGV 2 ($3{,}5.10^{-7}$), APRP 2 ($3{,}0.10^{-7}$) et RTS 4 ($2{,}6.10^{-7}$) faisant toutes moins de 13 % de la fréquence d'endommagement du coeur du réacteur dans l'état a ($4{,}7.10^{-6}$/tranche x an).

Famille d'initiateurs	Libellé de la séquence	Fréquence d'occurrence (/ tranche x an)	%
APRP 8	Brèche 1"- 2" état d - non mise en service de l'IS par l'opérateur	$1{,}45\ 10^{-6}$	13,5
APRP 9	Brèche pressuriseur état c - non mise en service de l'IS par l'opérateur	$1{,}14\ 10^{-6}$	10,6
APRP 8	Brèche 3/8" - 1" état d - non mise en service de l'IS par l'opérateur	$7{,}7\ 10^{-7}$	6,8
ATWS 2	Perte partielle du poste d'eau P > 30 % PN - Défaillance AU + coefficient modérateur > 93 %	$5{,}9\ 10^{-7}$	5,5
APRP 8	Brèche 2"- 3" état d - non mise en service de l'IS par l'opérateur	$5{,}8\ 10^{-7}$	5,4
APRP 9	Brèche pressuriseur état b - non mise en service de l'IS par l'opérateur	$4{,}6\ 10^{-7}$	4,3
TRCP 2	Dilution état d - non interruption de la dilution ou non mise en service de l'appoint par l'opérateur	$3{,}6\ 10^{-7}$	3,4
RTGV 2	RTGV - 1 tube - perte ASG - échec U1	$3{,}5\ 10^{-7}$	3,3

Famille d'initiateur	Libellé de la séquence	Fréquence d'occurrence (/tranche x an)	%
APRP 2	Brèche 3/8" - 1" état a arrêt inopportun de l'IS par l'opérateur	$3,0.10^{-7}$	2,8
RTS 4	Petite RTE état a - Perte ASG - échec U1	$2,6.10^{-7}$	2,4
APRP 8	Grosse brèche état c non isolable - Non mise en service de l'IS par l'opérateur	$2,2\ 10^{-7}$	2
APRP 8	Brèche intermédiaire état c non isolable - Non mise en service de l'IS par l'opérateur	$2,1.10^{-7}$	2
ATWS 3	Fermeture 1 VIV, P > 30 % PN - défaillance AU, coeff. mod. > 93 %	$1,6.10^{-7}$	1,5
TRCP2	Dilution dans l'état a	$1,3.10^{-7}$	1,3
APRP 2	Brèche 3/8" - 1" - perte RIS	$1,25.10^{-7}$	1,2
APRP 2	Brèche 1" - 2" - perte RIS	$1,25.10^{-7}$	1,2
APRP 2	Brèche 1" - 2" - arrêt inopportun de l'IS par l'opérateur	$1,2.10^{-7}$	1,1
APRP8	Brèche 3/8" - 2" état c isolable - Perte du RCV et non mise en service de l'IS par l'opérateur	$1,2.10^{-7}$	1,1
TRCP 2	Dilution non interruptible état d - défaillance de l'alarme de flux - non mise en service d'un appoint par l'opérateur	$1,2.10^{-7}$	1,1
APRP 3	Brèche 3"- 5" branche froide état a - arrêt inopportun de l'IS par l'opérateur	$9,510^{-8}$	0,8
	TOTAL (sur un total de $1,08.10^{-5}$)	$7,63.10^{-6}$	71