UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À

L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN GÉNIE INDUSTRIEL

PAR

ERIC LACROIX

PROPOSITION D'UNE NOUVELLE STRUCTURE D'ÉVALUATION PROBABILISTE DE SÛRETÉ POUR LES RÉACTEURS CANDU PHW 600

AVRIL 1999

PROPOSITION D'UNE NOUVELLE STRUCTURE D'ÉVALUATION PROBABILISTE DE SÛRETÉ POUR LES RÉACTEURS CANDU-PHW 600

Eric Lacroix

(Sommaire)

Ce mémoire a pour objet la comparaison des pratiques internationales en matières d'évaluation probabiliste de sûreté (EPS) pour les centrales nucléaires avec celles utilisées pour les réacteurs CANDU-PHW 600 en exploitation au Canada, afin de proposer une nouvelle structure d'EPS pour ces derniers. L'analyse est appliquée à un cas concret soit celui de la centrale nucléaire Gentilly-2, propriété d'Hydro-Québec.

L'étude débute par la description de l'état de l'art en matière d'EPS. Cette partie de l'étude constitue le cadre de référence avec lequel l'EPS de Gentilly-2 est comparée.

Par la suite une présentation de l'EPS de Gentilly-2 et de son évolution est effectuée. Celle-ci est composée de quinze (15) études matricielles de sûreté (EMS) avec, en support, plusieurs études de fiabilité de système. Une analyse de l'évolution des EMS de la centrale nucléaire Gentilly-2 a démontré que celles-ci, quoique différentes au début, sont maintenant très semblables à l'approche internationale.

Par la suite, les besoins de Gentilly-2 en matière d'EPS ont été déterminés afin d'identifier les lacunes que la nouvelles structure devra combler. Les principales lacunes identifiées sont le manque d'informatisation des anciens modèles et une évaluation de la sûreté opérationnelle avec ces modèles et des données de fiabilité spécifiques à la centrale.

Finalement, trois hypothèses ont été émises sur la durée d'exploitation restante de la centrale nucléaire Gentilly-2. Pour chacune de ces hypothèses, ce mémoire propose une solution représentant la meilleure approche d'EPS en fonction des besoins et ressources d'Hydro-Québec. Une des solutions comprend une estimation des coûts, des efforts et de la structure requis pour la réalisation et le maintien à jour de l'approche proposée.

REMERCIEMENTS

L'auteur souhaite remercier tous les individus ayant contribué, de près ou de loin, à la réalisation de la présente étude par leurs commentaires et leur support. En particulier, M. Georges Abdul-Nour et M. René Rochette, directeur et co-directeur de ce projet de maîtrise, de l'Université du Québec à Trois-Rivières. Dans un deuxième temps, M. Raynald Vaillancourt, de la centrale nucléaire Gentilly-2, pour m'avoir permis de réaliser la présente étude, en plus d'y avoir contribué significativement par des commentaires pertinents lors de nos nombreuses discussions. Je remercie aussi tous les membres de l'équipe Fiabilité pour leur aide et leurs commentaires, en particulier M. Réjean Comeau, pour ses précieux conseils tout au long de l'étude. Je remercie enfin la direction de la centrale nucléaire Gentilly-2 pour m'avoir octroyé le temps et les ressources humaines et matérielles nécessaires à la réalisation de cette étude. Finalement, je désire souligner l'appui moral que mes parents, Gilles et Diane Lacroix, et ma fiancée, Julie Hébert, m'ont prodigué durant tout le déroulement de ce travail.

AVERTISSEMENT

Hydro-Québec se dégage de toute responsabilité quant à l'utilisation ou l'interprétation qui pourrait être faite des informations contenues dans ce rapport par une tierce partie. En aucun cas, Hydro-Québec ne saurait être tenu responsable de tout dommage ou préjudice quelconque lié à une utilisation ou une interprétation fautive de tout ou partie du contenu de ce rapport.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

PAGE

LISTE DES SYMBOLES ET ABRÉVIATIONS

AECL	:Energie Atomique du Canada Limitée
AMDEC	: Analyse des Modes de Défaillance de leurs Effets et Criticité
CAFTA	: Computer Aided Fault Tree Analysis
CANDU	: CANada Deutérium-Uranium
CCEA	: Commission de Contrôle de l'Énergie Atomique
CDF	: Core Damage Frequency
D_2O	: Symbole chimique de l'eau lourde
EMS / SDM	:Étude Matricielle de Sûreté / Safety Design Matrice
EPRI	: Electrical Power Research Institute
EPS	:Évaluation Probabiliste de Sûreté
IAEA	: International Atomic Energy Agency
MW	: Méga-Watt
NEA	: Nuclear Energy Agency
OECD	: Organisation for Economic Cooperation and Development
PEH	: Probabilité d'Erreur Humaine
PEI	: Procédure d'Exploitation sur Incident
PERCA	: PERte de CAloporteur
PHW	: Pressurized Heavy Water
P.P.	: Pleine Puissance
RAW	: Risk Achievement Worth
RMQS	: Risk Management Query System
RRW	: Risk Reduction Worth
RTS	: Responsable Technique de Système
SAIC	: Science Application International Corporation
SKI	: Statens KärnkraftInspektion

SRS	: Système Relié à la Sûreté
SSC	: Structure, Système et Composant
SSS	: Système Spécial de Sûreté
TMI	: Three Miles Island
USNRC	: United State Nuclear Regulatory Commission

LEXIQUE DES TERMES UTILISÉS

Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC): Méthode d'analyse qualitative d'un système ayant pour but d'identifier les modes de défaillance des composants du système, leurs causes, leurs effets et leur criticité.

Arbre d'événement: Diagramme logique utilisant une structure arborescente et montrant les conséquences d'un événement initiateur.

Arbre de défaillance: Diagramme logique utilisant une structure arborescente et montrant les causes de défaillance et/ou de panne (et leurs combinaisons) conduisant à un événement indésirable.

Cause de défaillance: Circonstances liées à la conception, la fabrication ou l'emploi et qui ont entraîné la défaillance.

Composant: La plus petite partie d'un système qu'il est nécessaire et suffisant de considérer pour l'analyse du système.

Composant critique: Composant dont la défaillance, dans un état de fonctionnement donné du système, entraîne la défaillance du système.

Confinement: Le système de confinement constitue une enveloppe qui entoure les composantes nucléaires du système caloporteur.

Coupe (d'événement): Combinaison d'événement de base conduisant à l'événement indésirable.

Coupe minimale (d'événement): Coupe telle que, un quelconque des événements de base de la coupe ne se réalisant pas, la combinaison des événements de base restants ne constitue pas une nouvelle coupe.

Défaillance: Cessation de l'aptitude d'une entité à accomplir une fonction requise.

Défense en profondeur: Selon ce principe, il faut en premier lieu prévenir les accidents en fonctionnement normal. Si on ne peut les éviter, il faut empêcher que les accidents prennent de l'ampleur et, à défaut, traiter les conséquences de façon à minimiser les émission radioactives sous les niveaux admissibles.

Disponibilité: Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné.

Erreur humaine: Écart entre le comportement de l'opérateur humain et ce qu'il aurait dû être, cet écart dépassant des limites d'acceptabilité dans des conditions données.

Essais de fiabilité en exploitation: Essai de conformité ou de détermination de la fiabilité effectué dans des conditions d'essai enregistrées d'utilisation en exploitation.

Essai de maintenance: Essai effectué périodiquement sur un dispositif ou un équipement et destiné à vérifier que ses caractéristiques de fonctionnement se maintiennent dans des limites spécifiés, après que l'on ait procédé, le cas échéant, aux ajustements nécessaires.

Ligne de conduite pour l'exploitation (LCE): Document de support au Permis d'exploitation définissant les principes, règles et limites à l'intérieur desquels l'exploitation de la centrale sera réalisée.

Maintenance préventive: Maintenance effectuée à intervalles prédéterminés ou selon des critères prescrits et destinés à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'une entité.

Mode de défaillance: Effet par lequel une défaillance est observée.

Système: Un système est un ensemble déterminé d'éléments discrets (ou composants) interconnectés ou en interaction.

Système caloporteur: Ce système transporte la chaleur produite dans le combustible vers les générateurs de vapeur.

Système de sûreté: Systèmes ayant pour but d'assurer que les quatre fonctions suivantes puissent être remplies en condition anormale:

- L'arrêt du réacteur;
- Le refroidissement du combustible;
- La limitation des rejets radioactifs;
- La surveillance de la centrale.

Systèmes reliés à la sûreté: Systèmes, composants et structures qui advenant leur défaillance d'agir tel que le prévoit leur conception ou les analyses de sûreté, ont un impact potentiel sur la sûreté radiologique du public ou du personnel de la centrale.

Systèmes spéciaux de sûreté (SSS): Systèmes de sûreté ayant comme particularité d'être indépendants les uns des autres et d'être aussi indépendants des systèmes de production.

CHAPITRE 1

INTRODUCTION

1.0 Les méthodes d'évaluation de la sûreté

Les installations industrielles complexes, produisant ou utilisant des produits reconnus dangereux pour l'environnement et la population, (par exemple, les complexes pétrochimiques et les centrales nucléaires), présentent un risque advenant un accident majeur. Afin d'évaluer ce risque, des méthodes ont été mises au point. Ces méthodes sont appliquées généralement au stade de la conception, à un stade ultérieur s'il est prévu d'apporter des changements à la configuration de l'installation, et lors de l'évaluation de l'expérience d'exploitation afin de vérifier que la sûreté de l'installation reste garantie.

Deux méthodes, l'une déterministe et l'autre probabiliste sont actuellement utilisées. Ces méthodes sont employées pour évaluer et améliorer la sûreté de la conception et de l'exploitation.

1.0.1 Méthode déterministe

Dans la méthode déterministe, des événements de référence sont choisis comme enveloppe d'une série d'événements initiateurs qui pourraient mettre en danger la sûreté de l'installation. Une analyse est faite pour montrer que la réaction de l'installation et de ses systèmes de sûreté aux événements de référence satisfait à des spécifications prédéterminées en ce qui concerne à la fois le comportement de l'installation elle-même et les buts de sûreté à atteindre. (IAEA,1990)

1.0.2 Méthode probabiliste

L'analyse probabiliste, mieux connue sous le nom d'évaluation probabiliste de sûreté (EPS), est employée pour évaluer la probabilité de tout scénario particulier d'événements et de ses conséquences. Cette évaluation peut prendre en considération les effets des mesures d'atténuations prises à l'intérieur et à l'extérieur de l'installation. L'EPS est utilisée pour estimer le risque et spécialement pour repérer toute faiblesse possible, dans la conception et l'exploitation qui pourrait représenter une contribution excessive au risque. (IAEA, 1990)

1.1 L'EPS dans les centrales nucléaires

Dans une centrale nucléaire, d'importantes mesures de sûreté sont mises en oeuvre afin de prévenir tout accident pouvant avoir de graves conséquences. Le niveau de sûreté correspondant est démontré et contrôlé par les analyses de sûreté (probabilistes et déterministes) et le retour d'expérience. Le présent mémoire se limite cependant à l'utilisation des EPS dans les centrales nucléaires.

L'EPS se différencie des analyses déterministes traditionnelles par son approche méthodologique d'identification des séquences d'accidents suite à un large éventail d'événements initiateurs. Elle permet aussi une détermination réaliste et systématique des fréquences et conséquences d'accidents ainsi que la quantification des incertitudes liées à celles-ci. Finalement, il a été démontré que l'EPS procure d'importants enseignements qui complètent ceux des analyses déterministes.

1.1.1 Historique

En 1975, la United State Nuclear Regulatory Commission (USNRC) complétait la première étude quantitative sur les probabilités et conséquences d'accidents majeurs dans les centrales nucléaires commerciales publiée sous le

nom de WASH-1400. Ce rapport utilisait pour la première fois les techniques de l'EPS à l'étude d'accidents majeurs dans deux réacteurs commerciaux. Le risque associé à de tels accidents fut estimé relativement faible en comparaison avec les risques naturels ou résultant de l'activité humaine.

Suite à l'achèvement du WASH-1400, des efforts de recherche furent initiés pour développer des méthodes avancées d'évaluation de fréquences d'accidents et améliorer les moyens de collecte et d'analyse des données. Des méthodes furent lancées pour améliorer l'habileté à quantifier l'effet des erreurs humaines et des études pour mieux prédire la nature et les effets des causes communes commencèrent.

L'accident de Three Miles Island (TMI) en 1979 changea le caractère des analyses d'accidents majeurs à travers le monde. En effet, avant cet incident, les croyances voulaient que les contributeurs majeurs au risque soient les accidents de grandes importances, comme les grandes pertes de caloporteur (PERCA), même si selon le WASH-1400 les contributeurs majeurs étaient les petites PERCA et les changements d'état d'exploitation. L'accident de TMI démontra l'utilité du WASH-1400 et il fut recommandé dans les divers rapports d'enquête, Kemeny et al. (1979) et Rogovin et al. (1980), sur cet accident que les techniques de l'EPS devraient être utilisées pour compléter les méthodes déterministes traditionnelles d'analyse de sûreté des centrales nucléaires.

Un grand nombre de centrales nucléaires ont été ou sont analysées à l'aide de techniques probabilistes à travers le monde dans le but d'identifier leurs faiblesses potentielles et pour déterminer la fréquence des accidents majeurs. D'important enseignements ont été obtenus relativement aux actions devant être prises pour maintenir ou améliorer les enveloppes de sûreté tout en procurant une augmentation de la flexibilité de l'exploitant.

Au cours des dernières années, le développement d'outils informatiques puissants et spécifiques aux techniques d'EPS a amené le concept d'EPS vivante. En effet, une EPS peut, en plus de l'évaluation statique de la sûreté qu'elle fournit, être maintenue pour procurer une mise à jour continue des évaluations qui complète la gestion de l'exploitation de la centrale et des modifications apportées à l'installation.

1.1.2 Approche d'EPS

Il existe actuellement deux approches d'EPS pour les centrales nucléaires. La plus connue et répandue est celle décrite dans les "Safety Series" de l'International Atomic Energy Agency (IAEA). Cette approche, majoritairement développée par les américains, est présentée et décrite dans ce mémoire sous le nom d'approche internationale.

Parallèlement à l'approche internationale, une approche EPS similaire, développée au Canada, a vu le jour au milieu des années 70. Cette approche est composée d'un nombre d'études spéciales, appelées Études matricielles de sûreté (EMS). Ces études furent produites pour l'octroi de permis d'exploitation des réacteurs CANDU-PHW 600 dont celui de la centrale nucléaire Gentilly-2 propriété d'Hydro-Québec.

1.2 Présentation du présent mémoire

1.2.1 Mise en contexte

La centrale nucléaire Gentilly-2, exploitée commercialement depuis octobre 1983, est une centrale de type CANDU-PHW 600 d'une puissance nominale de 675 MW. Pour l'obtention de son premier permis d'exploitation, Hydro-Québec a dû démontrer à la Commission de Contrôle de l'Énergie Atomique (CCEA), organisme fédéral réglementant et contrôlant l'industrie nucléaire,

que l'exploitation de la centrale nucléaire Gentilly-2 ne comportera pas de risques injustifiés pour la santé et la sécurité du personnel, de la population ou pour l'environnement.

À cet effet, Hydro-Québec a produit, entre autres, une évaluation probabiliste de la sûreté se composant principalement de quinze (15) études matricielles de sûreté avec, en support, plusieurs études de fiabilité de système. Ces études datent de 1982 à l'exception de trois : deux furent mise à jour en 1986 et une en 1996. La mise à jour d'une autre étude est en cours de réalisation et devrait être terminée pour la fin de l'année 1998.

1.2.2 Problématique

Les études matricielles de sûreté de 1982 constituaient une approche très innovatrice tant par leur contenu que par les techniques de modélisation utilisées. Cependant, à l'époque, l'utilisation d'outils informatiques afin d'aider à la modélisation, à l'évaluation et à l'analyse n'était pas généralisée. De ce fait, les calculs ont été exécutés de façon manuelle et donc plusieurs hypothèses simplificatrices ont du être faites, après analyse, afin de faciliter les évaluations. Également, on disposait de peu d'historique d'exploitation pour les CANDU-PHW 600. Donc, plusieurs des probabilités numériques utilisées provenaient de banques très génériques ou de jugements d'experts. Finalement, il n'existait pas au Canada ou dans le monde de normes pour la réalisation et l'analyse d'une EPS.

Les études matricielles de 1982 ont été réalisées afin de démontrer la sûreté de la conception de la centrale et non pas comme outils utiles durant l'exploitation. Le fait que ces modèles n'étaient pas informatisés rendait difficile leur utilisation pour évaluer différentes configurations de la centrale et les interroger pour vérifier l'impact de changements dans les activités d'exploitation (ex.: entretiens préventifs, intervalles d'essais, etc.).

De nos jours, certaines des lacunes, identifiées par le passé, ont été comblées:

a) des outils informatiques puissants et spécifiques aux techniques utilisées dans les EPS ont été développés;
b) on dispose d'une certaine expérience d'exploitation tant spécifique à la centrale nucléaire Gentilly-2 que générique pour les CANDU-PHW 600;
c) finalement, des guides internationaux et nationaux ont été rédigés.

Afin d'être en mesure de suivre l'évolution de la sûreté de la centrale nucléaire Gentilly-2, d'optimiser l'utilisation de l'EPS actuelle et dans une certaine mesure, satisfaire aux attentes toujours croissantes de la CCEA, Hydro-Québec désire développer une nouvelle approche EPS en gardant et en améliorant les acquis des études matricielles de sûreté. D'autant plus qu'elle est aussi consciente que la CCEA exigera probablement que son EPS soit mise entièrement à jour dans l'option où elle désirerait prolonger la durée de vie utile de la centrale nucléaire Gentilly-2.

1.2.3 But et objectifs

Le développement d'une nouvelle approche d'EPS est un long processus dont le présent mémoire se veut être la première étape. Ce mémoire a pour objet de comparer les pratiques internationales en matière d'évaluation probabiliste de sûreté pour les centrales nucléaires avec celles utilisées pour les réacteurs CANDU 600 en exploitation au Canada, dont Gentilly-2, afin de proposer une nouvelle structure d'EPS pour ces derniers. La nouvelle structure d'EPS devra combler les lacunes mentionnées ci-dessus afin de pouvoir être utilisée comme outil de gestion. Les principales utilisations visées par la nouvelle structure sont:

- l'évaluation du risque moyen causé par l'exploitation d'une centrale,
- la surveillance du risque instantané durant son exploitation et
- l'évaluation de la sévérité des incidents survenus durant l'exploitation.

1.2.4 Méthodologie

Pour retirer tous les bénéfices d'une démarche intégrée vers une nouvelle approche EPS, il faut comprendre, structurer et planifier celle-ci. Suivant cet ordre de pensée, la première étape fut la familiarisation avec la centrale nucléaire Gentilly-2 et l'accumulation des informations sur les EPS (recherche bibliographique). Divers travaux et études ont aussi été effectués afin de bien saisir l'importance et l'utilité de l'EPS de Gentilly-2. Les enseignements découlant de ces travaux et études sont analysés et résumés dans le présent mémoire. Les chapitres de ce mémoire ont été divisés et écrits de façon à respecter les étapes réalisées afin de déterminer la nouvelle structure d'EPS de Gentilly-2:

- Le concept de risque, chapitre 2, est défini afin de fournir au lecteur les notions de base nécessaires à la compréhension du présent mémoire.
- L'état de l'art en matière d'EPS, présenté et expliqué au chapitre 3, constitue le cadre de référence avec lequel l'EPS de Gentilly-2 est comparée. Le but de ce chapitre est de tracer un portrait général de l'approche EPS internationale sans mettre l'emphase sur un type d'application ou une application particulière d'EPS.
- Le chapitre 4 décrit et analyse les études matricielles de sûreté et le chapitre 5 présente leur évolution et utilisation à Gentilly-2.
- L'analyse des besoins de Gentilly-2 en matière d'EPS, chapitre 6, permet d'identifier les lacunes que la nouvelle structure d'EPS devra combler.
- Finalement, le chapitre 7 propose les options représentant les meilleures approches d'EPS pour Gentilly-2 en fonction de ses besoins et de ses ressources. La présentation des options comprend une estimation des coûts, des efforts et de la structure requis pour la réalisation et le maintien à jour de celles-ci.

1.3 Recherche bibliographique

Dans les dernières années, les EPS ont fait l'objet d'une attention particulière tant de la part des organismes de contrôle que des exploitants. C'est ainsi que s'est développé un corpus de connaissance de plus en plus structuré circonscrivant la problématique des EPS. Diverses publications font état de ces connaissances; pour la plupart, ces publications sont soit des études de cas ou des analyses conceptuelles. C'est sur la base d'une revue la plus complète possible de ces publications que ce mémoire fut produit.

Cette section présente les principaux éléments de la recherche bibliographique. Le lecteur trouvera en référence une liste plus exhaustive des documents consultés.

1.3.1 Documents réglementaires

L'objectif premier des ces guides est d'assister les spécialistes effectuant ou supervisant la réalisation d'une EPS. Ils procurent à l'exploitant des directions sur la préparation, l'application, l'interprétation et la maintenance de leur EPS. Un objectif plus particulier à ces guides est de normaliser le cadre de réalisation, la terminologie et la documentation des EPS afin de faciliter les revues externes de celles-ci.

La USNRC a réalisé un grand nombre de ce type de document. Étant donné la réglementation américaine, ces documents sont extrêmement détaillés et par le fait même sont grandement utilisés et cités dans les autres pays. En plus de guides généraux sur la réalisation d'EPS (NUREG/CR-2815, NUREG/CR-2300, NUREG-1050, NUREG/CR-3485), plusieurs guides spécifiques à des activités liés à l'EPS ont aussi été réalisés comme, par exemple, le NUREG/CR-1278 sur la fiabilité humaine et le NUREG/CR-4780 sur les causes communes de défaillance.

L'IAEA a réalisé une séries de documents basés sur la littérature existante. Cette série de documents établit le rôle d'une EPS (IAEA, 1992) et offre des directions quant à la réalisation d'une EPS de niveau 1 (IAEA,1992), de niveau 2 (IAEA, 1995) et de niveau 3 (IAEA, 1996).

1.3.2 EPS vivante

Les EPS vivantes sont relativement récentes, les premières publications sur ce sujet datent de la fin des années 1980 lorsqu'on était encore au stade de développement du concept. Les premières publications nous proviennent essentiellement des ateliers organisés par TÜV Norddeutsschland e.V. en 1988, 1990, 1992 et 1994. La centaine d'articles publiés lors de ces ateliers constitue la base de toutes les applications qui se développent de nos jours. Tous les aspects d'une EPS vivante furent abordés lors de ces ateliers: définition, bénéfices, problèmes, applications, développement de codes et systèmes informatiques, etc.

Parallèlement à ces ateliers, SKI a débuté un projet en 1990 dont le principal objectif est la démonstration de l'utilité des EPS vivantes pour l'évaluation de la sûreté et l'identification d'amélioration possible de la sûreté opérationnelle. Les publications liées à ce projet fournissent une définition claire du concept d'EPS vivante ainsi que des cas pratiques de réalisation et d'utilisation de celle-ci. (SKI, 1994)

1.3.3 Exemples d'application

Beaucoup d'exploitants ont écrit des articles sur la réalisation de leur EPS et/ou sur les applications découlant de celle-ci. Les applications les plus courantes sont les suivante:

- Modification à la conception: Ces articles traitent de modifications (physiques) apportées à l'installation suite à la réalisation d'une EPS.
  Ex.: NEA (1997)
- EPS en état d'arrêt (shutdown PSA) et planification de la maintenance: Dans ces articles, il est question de la réalisation d'une EPS pour l'état d'arrêt d'une centrale et de son utilisation pour planifier les travaux de maintenance.
  Ex.: IAEA-TECDOC-751 (1994), OH (1996)
- Modifications des activités d'exploitation: Ces articles traitent de modifications apportées aux spécifications techniques, à la ligne de conduite d'exploitation, aux intervalles d'essais, etc.
  Ex.: Deriot (1992), Raina (1998)

1.3.4 Études matricielles de sûreté

Il existe peu de documents traitant des études matricielles de sûreté. Le seul document externe à Gentilly-2 retracé est celui de Gumley (1979). Les informations sur celles-ci furent donc obtenues en révisant tous les documents internes disponibles de Gentilly-2 traitant des EMS (EMS, correspondances avec la CCEA, procédures de fiabilité, etc.) et en discutant avec les personnes ayant participé à leur réalisation et celles les utilisant.

1.4 Originalité de la présente étude

Les études matricielles de sûreté étant très peu répandues, la présente étude est, à la connaissance de l'auteur, la première à comparer celles-ci à l'approche d'EPS préconisée internationalement.

De plus, le résultat de la démarche utilisée est la création d'une nouvelle structure d'EPS développée en améliorant les acquis des EMS par l'intégration des règles de l'art actuelles en matière d'EPS.

1.5 Extension de la recherche

L'utilisation de l'EPS est encore limitée aux domaines du nucléaire et de l'aérospatiale. Plusieurs autres domaines comportent des dangers pour le public (ex.: les complexes pétro-chimiques) et par conséquent devraient évaluer la possibilité d'utiliser un tel outil. C'est pourquoi plusieurs aspects de l'EPS font encore l'objet de développements importants et que celle-ci bénéficierait beaucoup de recherches visant à:

- éliminer ou réduire certaines de ses lacunes;
- développer de nouvelles applications d'EPS;
- développer de nouvelles méthodes de modélisation;
- améliorer l'évaluation de la fiabilité humaine, etc.

De plus, l'étude probabiliste de sûreté effectuée au Royaume-Uni sur des installations pétrolières et chimiques de l'île de Canvey a démontré l'applicabilité de cette méthode à un domaine en dehors du nucléaire (CANVEY, 1978 et 1981). Cette étude, prenant en compte toutes les interactions possibles entres les sites, a permis d'identifier les principaux dangers des installations, d'évaluer les risques associés (individuel et collectif) et de proposer des modifications pour les réduire. La réalisation d'une telle étude devrait être envisagée pour plusieurs parcs industriels existants notamment celui de Bécancour, voisin de la centrale Gentilly-2, constitué de plusieurs installations comportant des dangers.

CHAPITRE 2

CONCEPT DE RISQUE

Ce chapitre constitue une brève introduction au concept de risque. Pour plus de détails, le lecteur est invité à lire l'annexe A.

2.0 Définition du risque

Selon Nieuwhof (1985), le risque peut être défini comme la perte ou le dommage envisagé et considéré qui est associé à l'occurrence d'un événement indésirable possible. L'expression mathématique du risque (R) d'un événement est le produit de la probabilité d'occurrence (P) de cet événement par le coût[1] de ses conséquences (C).

$$R = P \times C$$

2.1 Perception du risque et risque acceptable

La perception des risques dépend de nombreux facteurs moraux et psychosociologiques qui apparaissent difficilement quantifiables ou mêmes explicables. Par exemple les événements de caractère exceptionnel (inondation, tornade) sont considérés comme beaucoup plus meutriers qu'ils ne le sont en réalité. En effet, il semble que le public juge "moins dangereux" une activité qui fait 1 mort tous les jours que 300 morts une fois par an. De plus, il n'existe pas de définition précise de ce qui constitue un risque acceptable, une notion essentiellement

[1] Lorsqu'on parle de coût ce n'est pas uniquement l'aspect financier qui est considéré.

subjective. Dans sa plus simple forme, le risque dénote un niveau d'incertitude associé à une action individuelle donnée. L'acceptation du risque est généralement gouvernée par le degré pour lequel il est considéré relativement improbable et de conséquence limitée.

2.2 Évaluation

Pour une installation industrielle, l'évaluation du risque fait une distinction entre les dangers potentiels qui peuvent être rencontrés en l'absence de mesures protectrices et les risques individuels qui demeurent en dépit des mesures prises. Il n'existe aucun moyen pour s'assurer que les risques résiduels ont complètement été éliminés ou que toutes les sources de dangers potentiels ont été identifiées.

Pour une centrale nucléaire, les accidents ou événements pouvant entraîner la libération de grandes quantités de matières radioactives à l'environnement présentent un danger pour la santé publique. Elle doit donc être conçue pour que le risque associé à son exploitation demeure à l'intérieur de limites acceptables pour le public et l'environnement. Le concept de la probabilité des événements avec les conséquences associées a rapidement été incorporé à l'intérieur des analyses de sûreté en prenant en compte le fait que la probabilité d'un accident doit être inversement proportionnelle à la sévérité des conséquences potentielles.

2.2.1 Méthode d'évaluation du risque

En général, l'évaluation du risque s'effectue selon les étapes suivantes comme citées dans Tanguay et Guyonnet (1978):

1. Rechercher les événements initiateurs d'accidents

Établir la liste de toutes les défaillances envisageables, sur les composants et sur les organes de liaison, susceptibles de faire sortir le système de son fonctionnement normal et de créer un accident.

2. Étudier les scénarios d'accidents

À partir des événements initiateurs, on doit ensuite établir l'ensemble des séquences accidentelles qui peuvent en découler

3. Évaluation de la probabilité d'accident

Le scénario d'accident ayant été établi, il est possible de calculer la probabilité de voir arriver l'événement indésirable à partir de la probabilité des événements initiateurs et des probabilités respectives des événements successifs. Généralement, on s'appuie sur les statistiques disponibles sur les types d'événements considérés pour évaluer leur probabilité.

4. Exposition de l'environnement

Pour évaluer les conséquences du scénario, il est nécessaire de connaître l'état de l'environnement du système au moment où se produit l'événement indésirable.

5. Calcul des conséquences

Pour chaque type d'environnement, l'événement indésirable conduira à des dommages résultant de l'événement considéré et de l'environnement dans lequel il se produit. Pour chaque événement on dispose donc d'un spectre de conséquences dont chaque élément sera affecté du temps d'exposition dans l'environnement considéré.

6. Évaluation du risque

La quantification du danger est généralement représentée par une grandeur à plusieurs dimensions (nombre de victimes, dommages financiers, etc.) fonction du couple défaillances-environnement retenu. Cette grandeur sera toujours bornée supérieurement, le danger potentiel maximal correspondant à la défaillance totale du système survenant dans l'environnement le plus critique.

2.2.2 Limites

Indépendamment de ces nombreux avantages, l'évaluation du risque présentera toujours des limites intrinsèques à la méthodologie d'évaluation:

- le manque d'exhaustivité des événements initiateurs;
- l'insuffisance des connaissances sur certains phénomènes;
- la difficulté d'appréhender les probabilités cherchés;
- la difficulté d'évaluation des conséquences possibles.

Ces limites sont approfondies à la section 3.0.6 du chapitre suivant.

CHAPITRE 3

DESCRIPTION D'UNE EPS

Ce chapitre présente et explique ce qu'est une évaluation probabiliste de sûreté. Son but est d'offrir une vision générale du rôle, de la méthodologie et des principales caractéristiques d'une EPS. Pour des informations plus spécifiques, le lecteur est invité à consulter les documents cités en références.

3.0 EPS de base

L'expression "de base" est utilisée ici pour faire la distinction entre le contenu (structure statique) d'une EPS et son processus de mise à jour appelé: "EPS vivante". Ce dernier concept est présenté à la section 3.1 du présent chapitre. Cette section a pour but de tracer un portrait général des EPS sans mettre l'emphase sur un type d'application ou une application particulière d'EPS.

Au cours des dernière années, plusieurs documents traitant des EPS ont été produits. L'IAEA a synthétisé la majorité de ceux-ci dans ses "Safety Series": IAEA (1992), IAEA (1995) et IAEA (1996). Ces derniers documents réflètent l'état de l'art actuel et conséquemment ont grandement été utilisés pour la création de cette section.

3.0.1 Définition

L'évaluation probabiliste de la sûreté[1] d'une centrale nucléaire a pour but d'évaluer et de juger de sa sûreté pour tous les états potentiels d'exploitation

[1] Initialement, ce genre d'évaluation était dénommée aux États-Unis : "Évaluation probabiliste du risque (EPR)". Le terme "risque" ayant une connotation négative et celui de "sûreté" une connotation positive, les

(marche normale et arrêt). Elle est utilisée pour estimer le risque et spécialement pour repérer toute faiblesse possible dans la conception et l'exploitation qui pourrait représenter une contribution excessive du risque.

Il s'agit d'une analyse probabiliste menant à l'obtention d'un ou plusieurs modèles, employés pour évaluer la probabilité de tout enchaînement particulier d'événements et de leurs conséquences. Cette évaluation peut prendre en considération les effets des mesures d'atténuations prises à l'intérieur et à l'extérieur de la centrale. (IAEA, 1992)

3.0.2 Buts et objectifs

Dans son sens le plus large, une EPS vise à :

- identifier et décrire les combinaisons d'événements pouvant entraîner de graves accidents;
- estimer la probabilité d'occurrence de chacune de ces combinaisons;
- évaluer leurs conséquences.

Pour atteindre ces buts, la méthodologie d'une EPS incorpore les renseignements relatifs (IAEA,1992):

- à la conception des installations;
- à leur fonctionnement depuis leur mise en service;
- aux pratiques d'exploitation;
- à la fiabilité des constituants;
- au comportement humain;
- aux phénomènes d'accident;
- aux incidents potentiels sur l'environnement et la santé.

---

européens et l'IAEA ont dénommé ce genre d'évaluation "Évaluation probabiliste de sûreté (EPS)". Cette appellation est maintenant généralisée à l'échelle mondiale, incluant les États-Unis.

3.0.3 Envergure

Il est coutume de distinguer trois niveaux d'EPS selon l'envergure de l'analyse (IAEA, 1992, 1995 et 1996):

1. EPS niveau 1: cette EPS fournit une évaluation de la conception et de l'exploitation de la centrale avec une insistance particulière sur les séquences pouvant entraîner une dégradation du coeur.

2. EPS niveau 2: en plus des analyses effectuées dans une EPS niveau 1, cette EPS aborde également les phénomènes qui suivraient une dégradation accidentelle du coeur, la réaction du confinement aux charges qui en résulteraient et le transport de corps radioactifs jusque dans l'environnement (de telles analyses fournissent des informations sur les probabilités de rejets radioactifs accidentels).

3. EPS niveau 3: en plus des analyses effectuées dans une EPS niveau 2, cette EPS envisage également la dispersion de radionucléides hors de l'enceinte et leurs incidences sur l'environnement et la santé.

À chacun des niveaux, une EPS fournit les probabilités (ou fréquences) de conséquences défavorables. Les résultats dépendent, dans une certaine mesure, d'éléments subjectifs intervenant dans le déroulement de l'analyse. L'annexe B présente l'envergure des différents éléments d'une EPS. L'annexe C, quant à lui, présente les principales étapes de réalisation d'une EPS selon les documents de l'IAEA.

3.0.4 Utilisation

D'une façon générale, on peut classer les utilisations des EPS en quatre catégories en fonction de la manière dont les informations sont rassemblées et les résultats évalués.

Il existe deux manières de rassembler les données nécessaires à la conduite d'une EPS (IAEA,1992):

- Analyses a posteriori: les données d'entrée utiles, telles que événements initiateurs, taux de défaillance et interactions des systèmes, peuvent être liées à des observations opérationnelles spécifiques à la centrale. Ces analyses constituent un excellent moyen de contrôler la sûreté en exploitation.

- Analyses a priori: il est possible d'effectuer des analyses sans ou avec très peu de données relevant de l'expérience spécifique d'une centrale. Celles-ci sont particulièrement utiles lorsqu'on a affaire à une nouvelle technologie sans expérience notable. Dans ce cas, une EPS pose les jalons qui permettront d'agencer d'une manière pondérée les connaissances se rapportant aux caractéristiques de sûreté et de procéder à un examen quantitatif de ces caractéristiques.

Il existe deux manières fondamentales différentes d'évaluer dans la pratique les résultats d'une EPS (IAEA,1992):

- Conclusions techniques: cette possibilité consiste à tirer des conclusions techniques à partir de l'importance relative avec laquelle les différentes séquences d'accident, équipements et modes de fonctionnement contribuent au risque. De telles conclusions relatives s'avèrent d'un intérêt capital pour

l'amélioration de la sûreté du fait qu'elles indiquent la pertinence et les priorités des démarches à entreprendre.

- Conclusions absolues: cette possibilité consiste à tirer des conclusions absolues sur les risques relatifs à une installation et sur la tolérabilité de ces risques. En principe, cela peut se faire pour les risques techniques (probabilité d'une grave dégradation accidentelle du coeur, probabilités de termes sources inacceptables) ou pour les risques sanitaires liés à de tels accidents.

L'utilité d'une EPS dépend en grande partie de l'envergure et notamment du niveau et de la catégorie des recherches effectuées. La part de subjectivité, préjugés et incertitudes des résultats augmente grandement lorsque l'on passe d'une étude de niveau 1 à une étude de niveau 3. En outre, l'incidence de ces facteurs sur les résultats est beaucoup plus grande dans des analyses a priori que dans des analyses a posteriori, dont les résultats sont difficilement comparables.

3.0.5 Avantages

Dans l'ensemble, les EPS se sont révélées utiles pour (IAEA, 1992):

- vérifier que la conception est complète et cohérente (y compris l'identification des risques liés aux différents états de la centrale et des effets vis-à-vis des conséquences d'un accident);
- évaluer les modifications apportées à la conception du point de vue sûreté;
- évaluer les stratégies de gestion et d'exploitation;
- aider la direction de la centrale à établir des stratégies utiles en matière d'entretien, d'essai et de formation (EPS vivante validée en permanence sur l'expérience d'exploitation);

- aider à se prononcer sur l'opportunité de réaliser des interventions pour amélioration;
- évaluer les stratégies de réponse aux accidents;
- aider à l'amélioration des règles d'exploitation;
- assurer un contrôle systématique du niveau de sûreté en évaluant, par exemple, des événements précurseurs en fonction de leur importance pour la sûreté;
- établir des priorités pour la recherche future en identifiant les secteurs où les connaissances sont les plus incomplètes;
- aider à créer de nouveaux concepts de réacteurs.

La plupart de ces avantages s'obtiennent à partir d'EPS niveau 1 et de niveau 2 (analyses a posteriori visant à tirer des conclusions techniques). De telles recherches sont aptes à servir de méthodologie standard pour les examens de sûreté périodiques des centrales nucléaires.

3.0.6 Limites

L'utilisation d'une EPS présente des limites, comme citée dans le chapitre 2 au point 2.2.2, dont la plupart sont intrinsèques à la méthodologie utilisée. En effet, celle-ci est tributaire :

- de la conception déterministe,
- d'incertitudes dans les données et les modèles,
- de difficultés à analyser correctement certaines questions et,
- des conclusions sélectives de l'équipe qui réalise l'EPS.

Les principales critiques de la méthode concernent principalement (Tanguy et Guyonnet, 1978):

- le manque d'exhaustivité des événements initiateurs: on ne sera jamais sûr d'avoir pensé à tous les scénarios possibles pouvant engendrer les événements;

- l'insuffisance des connaissances sur certains phénomènes: le calcul des probabilités s'appuie toujours sur une bonne connaissance des systèmes en question et une compréhension bien formulée des phénomènes qui s'y passent. C'est loin d'être toujours le cas, pour le physicien s'efforçant de comprendre les phénomènes et pour l'ingénieur s'efforçant de les manoeuvrer;

- la difficulté d'appréhender les probabilités recherchées: la rigueur des méthodes de calcul n'est pas toujours acquise, les données de base nécessaires au calcul de la probabilité des événements en fonction des probabilités de ses causes ne sont pas toujours accessibles (quand elles existent, le plus souvent les données n'existent pas!), le facteur humain qui est essentiel dans tous les scénarios est difficilement quantifiable;

- la difficulté d'évaluation des conséquences possibles: l'extension spatiale sur des centaines de kilomètres, la multiplicité des formes prises par les dommages, l'influence différée sur des années, le mode pernicieux de l'agression (invisibilité des radiations), le comportement irrationnel des humains en groupe important (panique), tous ces facteurs rendent une évaluation exacte des conséquences très difficiles, voire impossibles sans une marge d'erreur d'un facteur 2, 4, 10 ou plus.

L'annexe D donne plus de détails sur les limites d'une EPS.

3.1 EPS vivante

Cette section définit le concept d'EPS vivante. Elle est basée principalement sur le rapport de la Staten Kärnkraftinspektion (1994) sur l'utilisation des EPS vivantes pour l'évaluation de la sûreté. Les enseignements découlant des applications des EPS vivantes dans les diverses utilités à travers le monde ont aussi été intégrés.

3.1.1 Définition

Une EPS vivante est un programme comprenant comme élément de base une EPS bien structurée, bien documentée, revue et possédant un haut niveau de détail. L'EPS est maintenue vivante en la mettant à jour périodiquement pour refléter tous les changements pertinents. L'EPS est aussi mise à jour pour refléter l'augmentation de la compréhension des systèmes de la centrale, les avancements dans les méthodes et pour rehausser l'achèvement des modèles.

Un programme EPS surveille et influence les changements du profil de sécurité de la centrale en fonction du temps. Cette habileté à surveiller les effets de changements dans la configuration et les procédures et d'influencer les changements améliorant la sûreté, fait d'une EPS vivante un outil puissant pour supporter les décisions qui affectent la sûreté de la centrale (SKI, 1994).

L'annexe E décrit plus en détails le concept d'EPS vivante. L'annexe F donne les différentes caractéristiques du modèle d'EPS vivante et ses limites.

3.1.2 Buts et objectifs

Le concept d'EPS vivante implique une description de la manière dont l'EPS originelle peut être utilisée d'une manière plus dynamique, continuellement mise à jour selon les états des systèmes reliés à la sûreté de la centrale. Les principaux buts du développement d'une EPS vivante sont (SKI, 1994):

- procurer un outil d'évaluation du risque pour l'analyse des effets sur la sûreté des changements dans la conception de la centrale, les procédures et spécifications techniques,
- supporter la planification de la maintenance et la gestion d'exploitation en procurant un outil de recherche des stratégies optimales d'exploitation, de maintenance et d'essais du point de vue de la sûreté.

Un programme d'EPS vivante deviendra, suivant ce concept, un système journalier de gestion de la sûreté basé sur une EPS spécifique à la centrale et supportant un système d'information.

3.1.3 Envergure

Les applications d'une EPS vivante peuvent être divisées en trois catégories (SKI, 1994):

1. Évaluation du risque : Il s'agit de l'évaluation du risque moyen causé par l'exploitation de la centrale, l'objectif premier étant de vérifier le niveau moyen de risque de la centrale, et d'en identifier les contributeurs majeurs. Les résultats de cette évaluation sont applicables à la planification à long terme afin d'améliorer les faiblesses identifiées de la centrale.

2. Surveillance du risque : Il s'agit de calculer le risque instantané durant l'exploitation de la centrale. Elle diffère de l'évaluation du risque, dans laquelle une configuration moyenne de la centrale est utilisée, par l'utilisation de la configuration observée au moment présent.

3. Le suivi du risque : Il s'agit de calculer le risque rétrospectif c'est-à-dire l'évaluation du risque expérimenté durant l'exploitation de la centrale. Un des objectifs est d'évaluer la sévérité des incidents du point de vue de la

sûreté. Un autre objectif est la recherche d'améliorations convenables et efficaces dans l'exécution technique et organisationnelle de la centrale.

3.1.4 Utilisations

Les applications d'une EPS vivante peuvent être divisées en domaines spécifiques pour mieux refléter les utilisations des résultats. La figure 1 présente ces domaines d'application. Une EPS vivante peut aussi servir d'outil de communication entre les autorités et les exploitants (SKI, 1994).

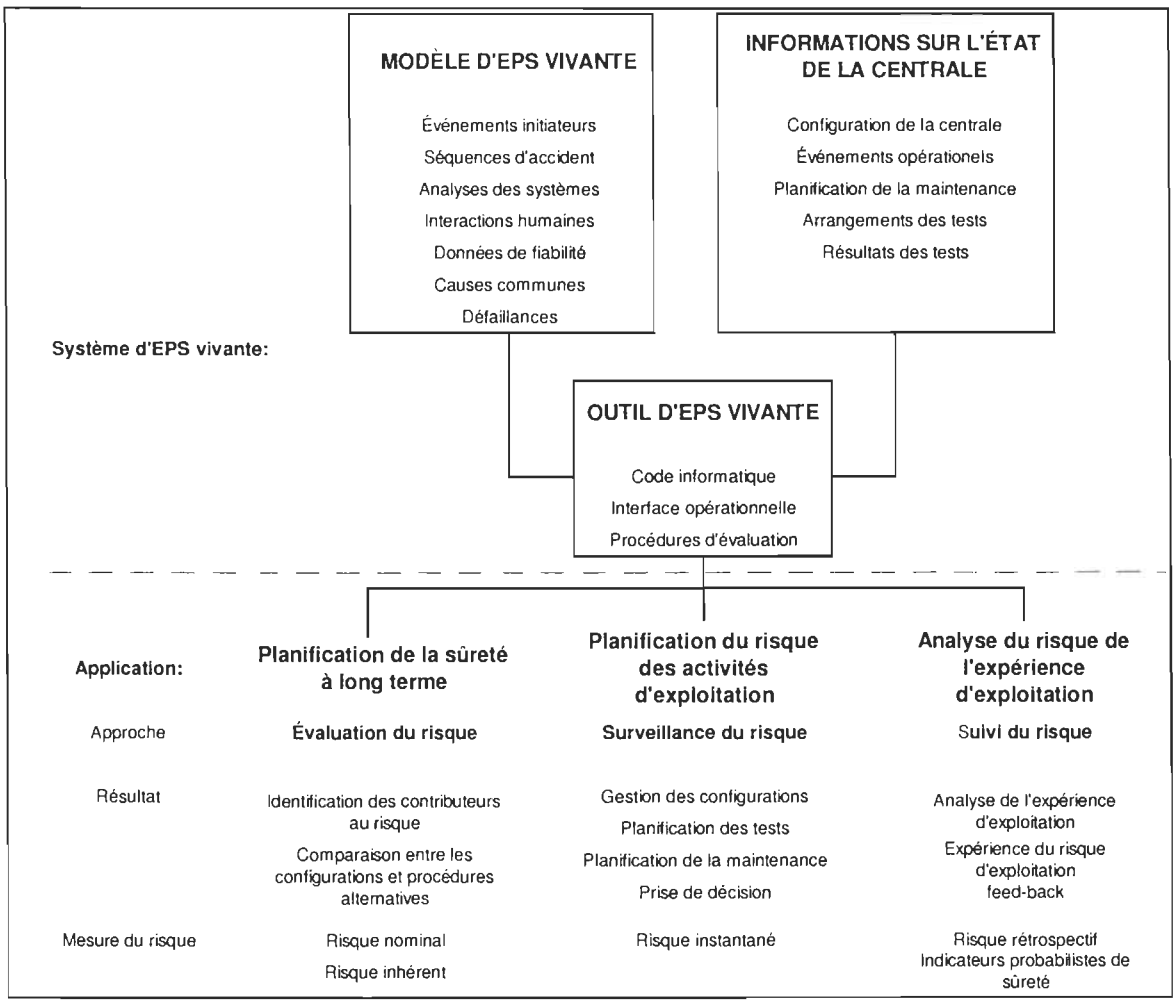

Figure 1. Concept d'EPS vivante (source: SKI, 1994)

3.1.5 Mise à jour

Les modèles développés, lors de la réalisation d'une EPS, reflètent la conception, l'exploitation et la maintenance de la centrale au début de sa réalisation. Au fur et à mesure que l'EPS est utilisée, il est probable qu'elle reflète de moins en moins le niveau de sûreté de la centrale dû aux changements dans la conception, l'exploitation et la maintenance de celle-ci.

La fréquence de mise à jour nécessaire selon les applications de l'EPS doit être déterminée. On distingue généralement trois types de fréquences selon son utilisation :

- Arrêt planifié: L'EPS est mise à jour à chacun des arrêts planifiés en considérant les changements pertinents dans la conception, l'exploitation et la maintenance de la centrale depuis l'arrêt précédent.
- EPS: L'EPS est mise à jour lorsqu'un changement dans la conception, l'exploitation ou la maintenance a le potentiel d'affecter l'EPS.
- Temps réel: L'EPS reflète continuellement l'état de la centrale en temps réel.

3.1.6 Principales activités requises

Les principales activités requises pour supporter un programme d'EPS vivante sont les suivantes (OECD, 1992):

1. La réalisation d'une EPS spécifique à la centrale de niveau 1.
2. L'établissement et la maintenance d'un programme d'EPS vivante. Cette activité comprend certains ou tous les éléments suivants dépendamment de la maturité du programme:
   - Un énoncé des utilisations et applications projetées. Cet énoncé définit les buts et bénéfices attendus et définit les caractéristiques du

programme, incluant les caractéristiques de l'EPS, les ressources nécessaires et les exigences organisationnelles.

- Un système de collecte de données assurant un flux continue d'information entre la centrale et l'EPS, afin de permettre des mises à jour périodiques de l'EPS pour refléter les changements de configurations et les données spécifiques de défaillances des composants. Ceci requiert que toutes les procédures gouvernant les activités de la centrale qui peuvent en modifier la configuration comprennent des dispositions pour rapporter ces changements à l'équipe d'EPS.
- Un cadre de travail pour guider les utilisations de l'EPS dans le support des activités de la centrale, cohérent avec les directives administratives et réglementaires, les procédures et les réglements.
- Un processus de communication interne à l'exploitant afin de communiquer les hypothèses des EPS et permettre la coopération des différents départements lors de conditions critiques.
- Un protocole de communication entre l'exploitant et l'organisme de contrôle afin de partager certaines informations.
- Un cadre de travail pour les prises de décision établissant ce qu'est une condition critique du point de vue de l'EPS, procurant une latitude pour les changements sous certaines limites et établissant clairement les responsabilités lors de prise de décision.
- Une équipe d'EPS interne dédiée au support du programme d'EPS vivante.

3.1.7 Bénéfices d'une EPS vivante

Les principaux bénéfices reconnus par les utilisateurs d'EPS vivante sont les suivants (OECD, 1992):

⇒ Bénéfices pour l'exploitation de la centrale:

- Amélioration des procédures et spécifications techniques
- Amélioration de la performance des opérateurs à travers les amélioration des procédures d'exploitation sur incidents (PEI) et de la formation
- Augmentation de la disponibilité des équipements à travers l'optimisation des intervalles d'essais et d'entretien préventif
- Justification pour continuer l'exploitation

⇒ Communication avec l'organisme de contrôle:

- Exemption d'exigences réglementaires sans effets
- Remplacement de modifications requises par des modifications plus efficaces
- Support à l'interaction réglementaire
- Augmentation de l'habileté à négocier avec les aspects techniques des exigences réglementaires
- Rehaussement de la crédibilité auprès de l'organisme de contrôle

⇒ Amélioration du processus de décision interne

- Base pour les priorisation des modifications
- Élimination de modifications inefficaces
- Optimisation de la stratégie d'exploitation
- Évaluation des effets du vieillissement

3.1.8 Outils

Les outils d'EPS vivante sont des codes informatiques pour gérer les modèles, les données et les informations nécessaires à la gestion et l'évaluation de la sûreté de la centrale par l'EPS. Ce sujet est abordé en détails dans l'annexe G.

CHAPITRE 4

LES ÉTUDES MATRICIELLES DE SÛRETÉ

Le présent chapitre a pour objet de présenter et d'expliquer les différents éléments constituant une EMS. Il présente ce qu'on peut appeler la "philosophie" des EMS i.e. leurs buts, objectifs, méthodologie, contenu, hypothèses générales, avantages, limites, etc.

4.0 Historique

Au début des années 1970, il est devenu évident, avec l'augmentation de la complexité des centrales nucléaires, que les analyses de défaillances simples/doubles traditionnelles n'étaient plus suffisantes, par elles-mêmes, pour complètement et proprement évaluer la sûreté d'une centrale nucléaire. Plusieurs discussions ont eu lieu entre le personnel de la CCEA et les exploitants afin de déterminer comment aborder les aspects tels que:

- Le traitement des fonctions de support de sûreté dans les analyses d'accidents;
- Le traitement des effets à long terme de certains accidents;
- Le traitement d'événements non couverts par les analyses traditionnelles, lesquels ne requièrent pas une réponse immédiate des systèmes de sûreté mais, au lieu, une série ordonnée d'actions correctives soit automatiques ou initiées par l'opérateur.
- Le traitement d'événements de cause commune (ex.: tremblements de terre) lesquels peuvent mettre hors de service plus d'un procédé ou système de sûreté.

En partie comme résultat des requêtes et commentaires faits par le personnel de la CCEA au cours de ces discussions et en partie de la propre initiative des exploitants

pour améliorer la couverture d'analyse d'accident dans certaines régions, une matrice d'accident modifiée fut proposée à la CCEA en 1975 pour l'octroi de permis des réacteurs de 600 MW. En plus des analyses de défaillances simples/doubles traditionnelles qui étaient considérées pour les centrales nucléaires précédentes, la demande de permis devait inclure un nombre d'études spéciales (appelées Études matricielles de sûreté) dont le but spécifique est d'évaluer la sûreté de la centrale dans les régions identifiées ci-dessus. Pendant que des EMS furent produites pour des problèmes spécifiques à la centrale Bruce A d'Ontario-Hydro, les centrales de 600 MW furent les premières pour lesquelles elles furent systématiquement préparées sur un large étendu de sujets. (AECB, 1982)

4.1 Buts et objectifs

Une étude matricielle de sûreté peut se définir comme une étude probabiliste de sûreté étudiant, lors de l'occurrence d'un événement initiateur donné, la réponse d'une installation nucléaire. Un événement initiateur est défini comme une défaillance d'un système de procédé pouvant entraîner:

- une perte de capacité de refroidissement du combustible
- ou, une augmentation de la puissance du réacteur au-delà de la capacité de refroidissement du combustible

Elle vise, premièrement, à identifier, à décrire et à évaluer la fréquence d'occurrence des combinaisons d'événement causant l'occurrence de l'événement initiateur donné et, deuxièmement, les combinaisons d'événements (aussi appelées séquences d'événements) qui découlent de cet événement majeur non désiré. Les EMS ont été développées afin de faciliter la compréhension des modes de défaillance et d'analyser plus en profondeur les séquences d'événement consécutives à un accident (AECB,1982; PF-EMS-001; PFP-MFE-005). Ces objectifs sont réalisés en:

- identifiant les causes d'occurrence des événements initiateurs;

- procurant des informations sur la fréquence attendue des événements analysés et des défaillances de composants pouvant causer ces événements; habituellement, la technique de l'arbre de défaillance est utilisée pour obtenir cette information;
- procurant des informations sur les réponses des divers systèmes de la centrale (incluant les systèmes spéciaux de sûreté) à ces événements;
- montrant que les séquences d'événements résultantes n'entraînent pas de conséquences inacceptables en termes de relâche de produits de fission ou que la probabilité de telles relâches soit extrêmement petite;
- identifiant, dans les séquences d'événement, les actions requises des opérateurs pour atteindre et maintenir des conditions de centrale stables et sécuritaires.

4.2 Méthodologie

La technique d'analyse recommandée pour une étude matricielle de sûreté est celle des arbres de défaillance et des séquences d'événements. Ces techniques sont présentées et expliquées à l'annexe H.

4.3 Hypothèses

Les hypothèses énoncées ci-après sont des hypothèses générales qui ont été retenues pour les études matricielles (Gumley, 1979). Les contraintes et les hypothèses applicables à une étude particulière sont indiquées dans l'annexe I.

- Puissance initiale: La puissance du réacteur avant la défaillance ou l'événement initiateur est présumée être de 100% P.P., ce qui permet de définir les exigences relatives à la conception des systèmes de sûreté et des systèmes reliés à la sûreté, afin d'assurer une mise à l'arrêt sûre du réacteur et l'extraction de la chaleur résiduelle.

- Conditions initiales d'exploitation: Les conditions initiales d'exploitation sont présumées correspondre aux conditions normales d'exploitation lorsque le

réacteur est à pleine puissance. Les défaillances qui se produisent en situation anormale d'exploitation sont prises en considération seulement lorsque cela est nécessaire, selon les conséquences prévues pour l'étude matricielle.

- Intervention de l'exploitant: Il est présumé, dans tous les cas, que l'exploitant n'intervient pas pendant les quinze (15) premières minutes suivant le moment où il prend connaissance de la défaillance. On attribue un degré de probabilité au comportement de l'exploitant après les quinze (15) premières minutes, selon le temps écoulé après l'événement initiateur et la précision des renseignements présentés.

- Comportement du système fonctionnel: Le comportement du système fonctionnel, y compris les effets provoqués par le système de régulation du réacteur, sert à déterminer la séquence d'événements prévue.

- Indisponibilité des systèmes spéciaux de sûreté: L'indisponibilité des systèmes spéciaux de sûreté est présumée être de 10^{-3} dans tous les cas, à moins qu'il existe un lien avec l'événement initiateur.

- Séquences d'événements: Les séquences d'événements prennent fin lorsque les conditions d'exploitation se stabilisent ou que la fréquence de la séquence est inférieure ou égale à une valeur de 10^{-7} événements / année.

4.4 Envergure

Un programme d'études matricielles de sûreté est développé pour chaque centrale. Celui de Gentilly-2 est présenté au chapitre suivant. La portée de ces études n'est pas fixe car l'expérience nous enseigne que pendant la préparation des séquences d'événements, de nouvelles conséquences doivent être prises en considération et incorporées aux études.

L'ampleur et l'objet de chaque étude sont indiqués dans l'annexe I. Lorsque les conséquences des études se recoupent, des correspondances sont établies entre celles-ci.

Les séquences d'événements prennent fin lorsque les conditions d'exploitation se sont stabilisées et que s'amorce le processus de rétablissement des conditions normales ou que la fréquence de la séquence est inférieure ou égale à 10^{-7} événements/année.

4.5 Avantages

Les études matricielles de sûreté offrent, bien entendu, les avantages généraux liés aux évaluations probabilistes de sûreté comme cités à la section 3.0.5 du chapitre 3. De façon plus spécifique, les principaux avantages des études matricielles de sûreté sont les suivants:

⇒ Avantages reliés au nombre d'études:

- Analyse qualitative et quantitative offrant une bonne compréhension des causes et conséquences d'un événement initiateur donné.
- L'analyse d'une seule famille d'accident par étude donne une meilleure compréhension de la réponse de la centrale et un degré de raffinement qui permet de mettre en lumière des situations qui pourraient passer plus facilement inaperçues dans une étude plus volumineuse.
- Les réponses développées suite à un événement initiateur prennent en considération les effets différents entraînés par les différentes causes de l'événement initiateur.
- Les causes, importances relatives et principaux contributeurs des événements initiateurs sont clairement identifiés.
- Le niveau de détail des études est très élevé.

- Offre la possibilité de créer une liste des hypothèses et des activités d'exploitation (essais, entretien préventif, etc.) crédités dans le modèle.
- Étude plus petite donc plus facile à utiliser et réviser.

⇒ Avantages reliés aux séquences d'événements:

- Considère le déroulement de la réponse de la centrale dans le temps. Cette caractéristique constitue un avantage majeur car il est bien connu que la perte d'un équipement a un impact différent selon le moment auquel elle se produit.
- Le rôle de l'opérateur est clairement identifié. Les actions requises par celui-ci afin de stabiliser ou récupérer une situation sont très bien définies.
- La représentation graphique des séquences d'événement facilite la compréhension et la visualisation de la réponse de la centrale par le personnel d'exploitation.

4.6 Limites

Les études matricielles de sûreté n'échappent malheureusement pas aux limites générales reliées aux EPS (exhaustivité, incertitudes, etc.) que l'on retrouve à la section 3.0.6. En plus de ces limites générales, ce type d'étude comporte certaines limites plus spécifiques:

⇒ Limites reliées au nombre d'études

- L'analyste n'a pas de vision globale liée à l'ensemble des événements initiateurs.
- Il est impossible de calculer un CDF (Core Damage Frequency) sans adapter l'approche actuelle.

⇒ Limites reliées à l'analyse

- Les erreurs d'exploitation pouvant causer un événement initiateur ou entraîner l'indisponibilité d'un système de mitigation ne sont pas considérées.
- L'étude matricielle sur le confinement n'est pas aussi détaillée qu'une EPS de niveau 2.

⇒ Limites reliées à la situation actuelle

- Il n'existe pas de guides, normes et encadrements clairs pour la réalisation et la documentation des EMS.
- Méthodologie unique aux CANDU donc difficilement comparable avec les autres pratiques internationales.

CHAPITRE 5

ÉVOLUTION DE L'EPS DE GENTILLY-2

Dans un premier temps, ce chapitre retrace l'évolution des études matricielles de sûreté à Gentilly-2, depuis sa demande de permis jusqu'à aujourd'hui. Cette partie est axée sur les modifications et ajouts apportés à la méthodologie des EMS par le personnel de Gentilly-2 et non sur le contenu des études matricielles de Gentilly-2. En second lieu, une courte présentation des études de fiabilité est fournie. Finalement, les outils (programmes informatiques) disponibles à la centrale nucléaire Gentilly-2 sont décrits brièvement.

5.0 1982 (Études matricielles de sûreté originales)

Deux types d'analyse d'accident furent soumises en appui au permis d'exploitation de la centrale nucléaire Gentilly-2: le rapport de sûreté et les études matricielles de sûreté. Hydro-Québec a produit quinze (15) études de ce dernier type, cependant deux de celles-ci n'ont été soumises à la CCEA que pour informations seulement (voir tableau I). L'envergure de ces études correspond à celle présentée à l'annexe I du présent document. (HQ, 1981)

Le Tableau I fournit la liste des études matricielles de sûreté actuellement en vigueur (NM-9.09).

Tableau I

Liste des études matricielle de sûreté de Gentilly-2

Numéro	Titre	Date
66-SDM-1	Inadvertent addition of positive reactivity (Second Edition)	Février 1981
66-SDM-2	Loss of steam generator as a heat sink (Second Edition)	Février 1982
66-SDM-3	Large LOCA and ECC operation	Octobre 1980
66-SDM-4	Operation after an earthquake Addendum 1: Consideration of partial failures of non-qualified systems	Juillet 1980 Avril 1982
66-SDM-5	Flooding of turbine and service buildings*	Octobre 1980
66-SDM-6	Reactor building flooding (Second Edition)*	Juin 1982
66-SDM-7	Small LOCA and ECC operation	Septembre 1980
66-SDM-8	Containment operation (Second Edition)	Juin 1982
66-SDM-9	Moderator as a heat sink	Avril 1981
66-RS-4	Dual computer failure (Second Edition)	Mars 1981
66-RS-5	Moderator and shield cooling system failures	Mai 1980
66-RS-7	Loss of shutdown cooling Addendum #1 Addendum #2	Mai 1981 Juin 1982 Décembre 1982
66-RS-8	Perte complète de l'alimentation d'air d'instrument	Février 1986
66-RS-9	Perte complète de l'eau de service	Février 1986
66-RS-10	Perte complète de l'alimentation électrique de catégorie IV	Mai 1996

* Ces études ne sont pas des documents d'appui au permis d'exploitation

5.1 1986

Afin de combler les lacunes des études originales, dont certaines soulevées par la CCEA (voir annexe J), les révisions de trois études matricielles de sûreté originales furent publiées en 1986. Ces études étaient :

- Perte complète de l'alimentation d'air d'instrument (66 RS-8)
- Perte complète de l'eau de service (66 RS-9)
- Perte complète de l'alimentation électrique de catégorie IV (66 RS-10)

⇒ Les principaux objectifs de ces révisions étaient de (DEVA, 1997):

- s'assurer de la conformité avec les installations de la centrale. Autrement dit, s'assurer que la description des composants (nomenclatures, nombre, performance, fréquences d'essai, durée des réparations en tenant compte de l'accessibilité, etc.) et le fonctionnement du système (conditions d'opération, points de consigne, capacité, état des composants (relève, arrêt, etc.) sont représentatifs des installations actuelles de la centrale.
- s'assurer de l'inclusion dans l'étude de tous les modes de défaillance (ex. : perte de débit, de fluide, de pression, etc.) pouvant occasionner un fonctionnement inadéquat du système étudié.
- s'assurer que tous les liens croisés entre les événements initiateurs et les systèmes de mitigation et entre les systèmes de mitigation eux-mêmes, sont identifiés.
- s'assurer que le rôle de l'opérateur dans les modèles est réaliste en considérant les procédures existantes ainsi que le temps et les informations disponibles pour le diagnostic de l'incident.
- réduire le conservatisme de certaines contraintes d'exploitation (ex. : arrêter le réacteur en moins de 8 heures après une perte du transformateur du réseau).
- lister les hypothèses utilisées dans les études matricielles de manière plus compréhensive que dans les études originales.

⇒ Les résultats de ces révisions ont démontré les bénéfices de l'approche :

- Certaines contraintes d'exploitation furent réduites.
- Quelques procédures d'essais furent modifiées pour s'assurer que les essais correspondaient bien aux modèles.
- Un programme de suivi obligatoire des essais et de la maintenance fut implanté.
- Durant l'exploitation de la centrale, plusieurs décisions furent basées sur les études révisées pour justifier les indisponibilités maximum, avant la réduction de la puissance du réacteur, de certains équipements ou fonctions importantes.

⇒ Cependant, ces révisions possèdent quelques faiblesses :

- Seulement les équipements ou fonctions considérées comme importantes par l'analyste furent modélisés.
- Les liens croisés entre les équipements et systèmes sont très dépendants de la perspective de l'analyste.
- Puisque les calculs ne sont pas informatisés, les études de sensibilité, pour évaluer l'impact de défaillances d'équipement ou fonction, prennent beaucoup de temps i.e. que les résultats peuvent prendre quelques jours avant d'être obtenus.

5.2 1996

La construction de la centrale de Bécancour a amené l'obligation de réviser l'étude matricielle RS-10 « Perte complète de l'alimentation électrique de catégorie IV ». Cette étude publiée en mai 1996 est la première étude matricielle à être informatisée. La méthodologie utilisée tente de rendre les EMS plus faciles d'utilisation pour le personnel d'exploitation.

Les principaux objectifs de cette étude étaient (DEVA, 1997):

⇒ Objectifs probabilistes de sûreté

- Démontrer que 90% des pertes d'alimentation électrique de catégorie IV sont rétablies en moins de 30 minutes.
- Démontrer que la probabilité de la séquence où le réacteur ne déclenche pas suite à l'événement initiateur est inférieure à 1 $x10^{-7}$ événements /année.
- Démontrer que la probabilité de la séquence où la chaleur résiduelle du combustible n'est pas enlevée suite à l'événement initiateur est inférieure 1 $x10^{-7}$ événements /année.
- Démontrer que la probabilité de la séquence où la chaleur de l'eau du modérateur ou des boucliers n'est pas enlevée après l'événement initiateur

est inférieure 1 x10^{-7} événements /année.

⇒ Objectifs reliés à l'exploitation de la centrale :

- Présenter les modes de défaillances amenant l'événement initiateur, les transitoires suivant l'événement initiateur et la réponse de la centrale
- Examiner les actions de l'opérateur créditées en tenant compte des procédures approuvées utilisées pour la formation des opérateurs. En plus, identifier clairement les actions de l'opérateur non créditables selon le modèle de l'opérateur conventionnel. (Exemple: les actions devant être exécutées en moins de 15 minutes)

En plus des arbres de défaillances et des séquences d'événements que l'on retrouve dans les EMS, un arbre global de défaillances fut développé. Cet arbre, construit après les séquences d'événements, intègre les arbres de défaillance afin d'effectuer une évaluation de l'ensemble des scénarios et pour tenir compte d'éventuels modes communs de défaillance entre divers systèmes.

5.3 Actuellement (1998)

Hydro-Québec procède actuellement à la révision de l'étude matricielle de sûreté 66RS-7 «Perte du refroidissement en temps d'arrêt ». La révision de cette étude permet de mettre à jour la modélisation par l'utilisation des méthodes informatiques et de tenir compte des modifications apportées au système de refroidissement en temps d'arrêt (RTA) et aux pratiques d'exploitation depuis la réalisation de l'étude précédente. (St-Denis et Comeau, 1998)

Cette étude vise l'atteinte de deux objectifs principaux :

- Démontrer la sûreté des installations actuelles de la centrale durant les arrêts planifiés où la source froide est assurée par le système RTA.
- Développer un outil facilitant la prise de décision lors de la planification et la

réalisation des arrêts planifiés de la centrale.

L'approche de base utilisée dans cette étude est celle des études matricielles de sûreté. Cette approche a surtout été privilégiée à cause des avantages pour la compréhension, l'illustration et la documentation de la réponse de la centrale lors de la défaillance d'un équipement ou d'un système. Par contre, l'approche présentée dans l'étude tire aussi avantage des bénéfices des outils développés pour la réalisation des évaluations probabilistes de sûreté (EPS) américaines et internationales. Ces outils facilitent grandement l'informatisation de l'évaluation de la fréquence des scénarios d'incident. C'est pourquoi l'étude utilise à la fois la technique des séquences d'événements et des arbres d'événements. Les avantages de ces deux méthodes d'analyse sont donc exploités pour répondre le mieux possible aux objectifs fixés.

Le développement d'un outil facilitant les décisions durant l'exploitation (second objectif) est basé sur une modélisation des systèmes qui offre la flexibilité pour interroger les modèles, sur l'intégration des essais prescrits et des entretiens préventifs, sur l'utilisation à la fois des séquences d'événements et des arbres d'événements, et sur la réalisation d'études de sensibilité. On peut ainsi modifier la configuration d'un système (par exemple, retirer un équipement pour entretien préventif) et observer l'impact sur les différents scénarios potentiels d'accident.

Les arbres d'événements sont utilisés pour intégrer les différents arbres de défaillance de l'événement initiateur et des systèmes de mitigation. La modélisation détaillée des systèmes par arbre de défaillance et l'intégration des arbres de défaillance permet d'avoir une meilleure assurance que les modes communs de défaillance seront considérés.

5.4 Réalisation d'une EMS

Les principales étapes de réalisation d'une EMS, selon la réalisation actuelle de

l'étude matricielle 66 RS-7, consistent à (St-Denis et Comeau, 1998):

a) Définir l'événement indésirable (ou les événements) à considérer (ex.: perte de refroidissement du combustible dans le coeur);
b) identifier les limites de l'analyse (limites des systèmes), les états initiaux traités, les exclusions, etc.;
c) identifier les modes de défaillance du système étudié, l'impact sur les autres systèmes, l'impact d'autres systèmes sur le système étudié (par revue systématique des liens entre les systèmes);
d) définir les événements initiateurs à traiter pouvant conduire à l'événement indésirable et les classer selon la réponse des systèmes de mitigation et de l'opérateur;
e) modéliser par arbres de défaillance ces événements initiateurs, déterminer la fréquence de ces événements initiateurs;
f) pour chaque état et événement initiateur considéré, réaliser les séquences d'événements: identifier les systèmes de mitigation et les actions d'opérateur requis, et évaluer de façon préliminaire les scénarios potentiels d'accident;
g) modéliser, par arbre de défaillance, les systèmes de mitigation requis, intégrer l'indisponibilité donné par ces arbres aux portes conditionnelles des séquences d'événement;
h) construire, pour chacun des états initiaux, les arbres de défaillance des systèmes de support communs (alimentation électrique, eau de service, air d'instrumentation, eau brute de refroidissement, etc.);
i) à l'aide des séquences d'événements, réaliser les arbres d'événements;
j) identifier et évaluer les scénarios pertinents;
k) analyser les résultats, les contribuants importants, les modes communs de défaillance;
l) revoir la modélisation et raffiner le modèle si requis, élaborer les conclusions.

5.5 Utilisations des EMS

Les EMS de Gentilly-2 sont principalement utilisées pour:

- démontrer que la conception de la centrale nucléaire Gentilly-2 est sûre.
- déterminer les essais et entretiens nécessaire pour maintenir les systèmes et composants étudiés dans un état analysé.
- identifier les activités d'exploitation requises, ainsi que leur fréquence, afin de démontrer la disponibilité des équipements et des systèmes en attente.
- spécifier ou aider à spécifier les règles d'exploitation qui se retrouvent dans la LCE.
- aider à la prise de décision lors de cas particuliers (événement, modification, entretien, etc.)
- identifier les actions requises de l'opérateur (développement des PEI).
- aider à la compréhension des événements.
- identifier les contributeurs de risque et ainsi identifier et fixer les priorités des mesures d'amélioration de sûreté.
- identifier les équipements et fonctions nécessaires à la suite de certains incidents étudiés.

Le modèle de l'étude matricielle de sûreté 66 RS-7 ainsi que ceux des études de fiabilité sont développés de façon à permettre de planifier le risque des activités d'exploitation:

- planification de la maintenance corrective
- planification de la maintenance préventive
- planification des essais et de leurs combinaisons

5.6 Études de fiabilité

Les études de fiabilité évaluent la probabilité et la fréquence de défaillance des systèmes et de leurs composants. Elles sont requises pour démontrer la fiabilité des systèmes spéciaux de sûreté (SSS) et celles des systèmes reliés à la sûreté (SRS) crédités dans les études matricielles de sûreté. Elles identifient les activités techniques importantes nécessaires au maintien de la fiabilité telles les activités d'entretien préventif et d'essais prescrits. Les études matricielles de sûreté se basent sur les données, les hypothèses et les résultats des études de fiabilité. Hydro-Québec a réalisé, jusqu'à maintenant, une quarantaine d'études de ce type. (NM-9.09)

5.6.1 But et objectifs

Une étude de fiabilité analyse la défaillance d'un système, d'une fonction d'un système ou d'un groupe de systèmes interactifs et évalue leurs performances respectives anticipées. (PF-EFP-003)

Les principaux objectifs d'une étude de fiabilité sont de:

a) refléter l'état réel d'exploitation du système;
b) évaluer l'indisponibilité ($\overline{A}$) et/ou la fiabilité (R) et la fréquence d'occurrence des défaillances (W);
c) déterminer les contributeurs majeurs à l'indisponibilité et à la fréquence de défaillance du système (composants critiques);
d) identifier les activités d'exploitation requises (essais, entretien préventif, inspection, contrôle chimique, etc.) pour assurer une indisponibilité minimale, et;
e) fixer les règles d'exploitation lors de certaines défaillances partielles.

5.6.2 Contenu

Une étude de fiabilité fournit une description du système analysé, de ses sous-

systèmes et circuits, les principales hypothèses de conception, d'exploitation et de modélisation ainsi que les données de fiabilité utilisées pour l'étude. Elle présente également une analyse détaillée des résultats et une série d'étude de sensibilité. Le modèle de défaillance du système analysé est généralement basé sur la technique des arbres de défaillance. Toutefois, avec l'accord du coordinateur de l'étude de l'Équipe Fiabilité, une autre technique, plus appropriée dans certains cas, peut-être utilisée.

5.7 Outils disponibles

La majorité des outils disponibles à la centrale nucléaire Gentilly-2 sont des logiciels développés par Science Application International Corporation (SAIC). Une très brève description de ces outils est fournie à l'annexe K. Pour plus d'informations, le lecteur est invité à consulter les manuels d'utilisateur cités dans la bibliographie.

CHAPITRE 6

ANALYSES DE L'EPS DE GENTILLY-2

Ce chapitre a pour objet l'identification des raisons justifiant et motivant des changements à apporter à l'EPS actuelle de la centrale nucléaire Gentilly-2.

Dans un premier temps, une courte analyse de la réglementation en matière d'EPS à laquelle Gentilly-2 doit se soumettre est effectuée. En second lieu, les lacunes de l'EPS actuelle sont identifiées par la présentation des besoins d'Hydro-Québec en matière d'EPS. Finalement, quelques améliorations non indispensables mais offrant certains avantages sont présentées.

6.0 Réglementation en matière d'EPS

C'est la responsabilité d'Hydro-Québec, en tant qu'exploitant, d'assurer la sûreté de la centrale nucléaire Gentilly-2. Cependant la manière dont Hydro-Québec s'y prend ainsi que les outils utilisés doivent être jugés acceptable par la CCEA. Selon la réglementation actuelle de l'industrie nucléaire canadienne, Hydro-Québec n'a pas d'obligation de réaliser une EPS de niveau 1, 2 ou 3.

Suite à de nombreuses conversations avec le personnel de la CCEA et à la lecture de certains projets de documents réglementaires, on s'aperçoit clairement que la CCEA préconise une approche probabiliste de sûreté correspondant à l'approche internationale. Ainsi, en cas de prolongement de la durée de vie utile de Gentilly-2, il est fort probable que la CCEA oblige Hydro-Québec à réviser son EPS actuelle et à l'adapter à l'approche internationale.

Actuellement, il n'existe aucune exigence réglementaire pour la mise à jour périodique des études matricielles de sûreté.

6.1 Besoins d'Hydro-Québec

"Hydro-Québec aspire à devenir une référence dans le domaine de la sûreté" (Politique de la sûreté nucléaire de la DPTN) et en même temps elle veut réduire ses coûts de production afin d'augmenter son profit. Il existe une certaine dualité entre les termes "sûreté" et "production rentable". En effet, certaines situations acceptables d'un point de vue de production peuvent ne pas l'être du point de vue de la sûreté (ex.: un arrêt du réacteur ou une réduction de sa puissance dus à un défaut d'un composant d'un SSS). Le contexte actuel de rationalisation des ressources met donc en évidence la nécessité pour Hydro-Québec de se doter d'un outil d'évaluation de la sûreté lui permettant d'optimiser sa production tout en ne dépassant pas un certain niveau de risque.

6.1.1 Besoins liés à l'exploitation

Conscient de la problématique présentée ci-dessus, la présente section identifie donc les principaux besoins d'hydro-Québec en matière d'EPS en fonction des demandes, provenant de l'exploitation, des responsables techniques de système (RTS) ou de l'unité Sûreté et Permis, auxquelles l'Équipe Fiabilité de Gentilly-2 est appelée à répondre. La majorité de ces demandes concernent les délais admissibles et les actions à prendre lors de retrait d'équipement pour entretien ou dû à la découverte d'un défaut. Beaucoup des réponses fournies proviennent de l'analyse de l'EPS de Gentilly-2. L'expérience a donc fait ressortir les lacunes et besoins suivants.

6.1.1.1 Études à jour

Les études originales ont été réalisées pour démontrer la sûreté de la conception de la centrale et la plupart n'ont pas été mises à jour suite à diverses modifications de systèmes et/ou de méthodes d'exploitation. Les modèles doivent donc être révisés afin de refléter l'état actuel d'exploitation et pouvoir être utilisés comme outils de gestion du risque. En effet, quelle valeur peut-on attribuer à la réponse fournie si la situation évaluée ne correspond pas à celle existant en centrale?

En plus de la révision des études actuelles, un programme de mise à jour périodique doit être mis en place afin de s'assurer que l'EPS reflétera tous les changements pertinents à venir au niveau de la conception, des pratiques d'exploitation et des caractéristiques (ex.: taux de défaillance) des systèmes. Afin de vérifier ce dernier point, Hydro-Québec devra donc implanter un programme d'évaluation de la sûreté opérationnelle comprenant la création d'une banque de données spécifiques à Gentilly-2. Cette banque permettra de comparer les données génériques utilisées dans les modèles avec celles colligées en centrale et ainsi permettre la validation des performances prévues des systèmes.

6.1.1.2 Efficience

Le fait que les modèles ne soient pas informatisés rend difficile leur utilisation pour évaluer différentes configurations de la centrale et leur interrogation pour vérifier l'impact de changements de méthodes d'exploitation. En plus, les calculs ayant été en majorité effectués à la main, de nombreuses hypothèses simplificatrices furent utilisées, après analyse, et la modélisation des systèmes fut peu détaillée.

Compte tenu de son ampleur, afin de faciliter la prise de décision et ainsi réduire les délais de réponse, l'EPS de Gentilly-2 devrait être entièrement informatisée. En effet, les outils informatiques disponibles de nos jours facilitent grandement la création et l'évaluation des modèles et ainsi permettent une analyse plus détaillée et plus rapide des systèmes modélisés.

Une analyse des différents outils informatiques disponibles à Gentilly-2 (annexe K) montre que la majorité des fonctions nécessaires (annexe G) sont comblées. Malheureusement, certains des outils disponibles sont utilisés à seulement une fraction de leurs capacités ou pas du tout (ex.: UNCERT) du aux directions et priorités choisies par l'équipe Fiabilité.

6.1.1.3 Critère d'acceptabilité

Toute décision doit être basée sur des critères. Dans le présent cas, nous parlons de critères probabilistes d'acceptabilité du risque. Actuellement, les situations sont analysées cas par cas. Il n'existe pas de critères probabilistes d'acceptabilité du risque bien définis, à part l'objectif de fiabilité suivant: l'indisponibilité des SSS doit être inférieure à 10^{-3}an/an.

Le critère probabiliste d'acceptabilité du risque le plus connu et commun à la majorité des centrales nucléaires est le Core Damage Frequency (CDF). Hydro-Québec devrait probablement évaluer la possibilité de calculer un tel critère et de se fixer des objectifs de fiabilité pour tous les systèmes modélisés dans son EPS.

Afin de calculer un CDF pour Gentilly-2, les études actuelles devraient être adaptées et regroupées. Le regroupement des études permettrait aussi d'avoir une vision globale reliée à l'ensemble des événements initiateurs et d'obtenir une meilleure assurance quant à la mesure de

l'impact réel d'éventuels modes communs de défaillances entre les systèmes.

6.1.1.4 État du réacteur

À part l'étude matricielle de sûreté RS-07, les EMS évaluent la réponse de la centrale suite à un événement initiateur ayant lieu lorsque le réacteur est à 100% de sa pleine puissance. L'expérience démontre cependant que plusieurs demandes concernent un autre état du réacteur soit celui d'arrêt. Une évaluation probabiliste de la sûreté en situation d'arrêt devrait donc être produite afin que l'Unité Analyse et Fiabilité puisse répondre adéquatement à ces demandes.

6.1.1.5 Personnel formé et études bien documentées

Finalement, en plus de posséder les bons modèles et outils, le personnel en place à Gentilly-2 doit connaître les modèles et outils à sa disposition. Actuellement, plusieurs études probabilistes de Gentilly-2 sont effectuées par ou avec l'aide de consultants externes sous supervision d'une personne à l'interne. Il arrive souvent que, pour répondre à certaines questions, les consultants externes soient consultés, ce qui ne peut se faire en cas de situation d'urgence. Ce problème peut cependant être réglé en documentant très bien les études.

Les études datant d'avant 1992 ne sont malheureusement pas assez bien documentées. Certaines informations comme les hypothèses de modélisation sont difficilement retraçables et un temps considérable d'analyste, non-présent lors de la réalisation de ces études, serait requis pour les retrouver.

Les études futures, du moins la majorité, devraient donc être réalisées par le personnel d'Hydro-Québec. En plus de faciliter la cohérence entre les études cela permettrait de maintenir les connaissances à l'interne. Il ne faudrait pas oublier que ce sont les employés d'Hydro-Québec qui devront utiliser ces études futures.

6.1.2 Besoins liés à la sûreté

Cette section identifie les lacunes et besoins en matière d'EPS en fonction de ses principales utilisations liées à la sûreté de la centrale nucléaire Gentilly-2. La section précédente, quant à elle, faisait ressortir plusieurs lacunes de l'EPS en fonction de son analyse afin de répondre aux demandes de l'exploitation.

6.1.2.1 Identification des contributeurs de risque

Un des premiers objectifs d'une EPS est l'identification des contributeurs de risque afin d'identifier et de fixer les priorités des mesures d'amélioration de la sûreté. Par contributeurs de risque, on ne parle pas seulement des défaillances ou erreurs d'exploitation pouvant causer un événement initiateur mais aussi de celles causant l'indisponibilité d'un système de mitigation. Il n'existe aucune liste formelle identifiant et affectant une priorité à ces contributeurs à Gentilly-2. Les spécialistes connaissent cependant la majorité de ces contributeurs de risque. Pour obtenir cette liste, ils devront néanmoins analyser chacune des études réalisées.

6.1.2.2 Évaluation des objectifs de sûreté

Les seuls systèmes possédant des objectifs fixes de sûreté sont les quatre (4) SSS. Ils sont donc les seuls pour lesquelles une évaluation systématique de la sûreté opérationnelle est effectuée afin de s'assurer

que les objectifs sont respectés. Il n'existe pas de processus pour l'évaluation opérationnelle des autres systèmes. Les performances de ces derniers sont évaluées et comparées avec les paramètres de fiabilité utilisés dans les études matricielles de sûreté et dans celles de fiabilité que lors de situation problématique. Hydro-Québec devrait envisager la possibilité de fixer des objectifs de sûreté pour tous les systèmes/composants considérés comme critiques pour la sûreté et naturellement effectuer un suivi de ces systèmes/composants.

6.1.2.3 Détermination des activités d'exploitation

Les EPS permettent l'identification des activités d'exploitation (essais et entretiens) requises, ainsi que leur fréquence, afin de maintenir les systèmes et composants étudiés dans l'état analysé. Ces activités ont été déterminées mais, malheureusement, pour l'instant elles ne sont pas toutes suivies de façon systématique. La mise en service prochaine du logiciel "Essais" devrait permettre de combler cette lacune du point de vue des essais. Hydro-Québec travaille à l'instauration d'un meilleur programme de suivi des entretiens préventifs au cours de la prochaine année.

6.1.2.4 Analyse de la fiabilité humaine

Les séquences d'événements des EMS ont l'avantage d'identifier clairement le rôle de l'opérateur. Les actions requises par celui-ci afin de stabiliser ou récupérer une situation sont très bien définies. Ce pourquoi, les EMS ont été grandement consultées pour la création des procédures d'exploitation sur incident (PEI) lesquelles servent à la formation des opérateurs et à l'exploitation de la centrale.

La fiabilité humaine observée à Gentilly-2 devrait être évaluée afin de valider le modèle d'opérateur actuellement utilisé dans les EMS. Ce modèle est très ancien et la possibilité d'utiliser un autre modèle devrait être évaluée Une évaluation de la fiabilité humaine de Gentilly-2 permettrait aussi d'insérer dans les modèles les erreurs d'exploitation augmentant la probabilité d'un événement initiateur ou entraîner l'indisponibilité d'un système de mitigation.

Il faut cependant noter que la fiabilité humaine est difficilement quantifiable et que les méthodes d'évaluation actuelles sont très controversées internationalement.

6.1.2.5 Compréhension des événements

Les études matricielles remplissent très bien cette mission. En effet, la représentation graphique des séquences d'événements facilite la compréhension et la visualisation de la réponse de la centrale par le personnel de fiabilité et d'exploitation.

Afin d'améliorer leur compréhension et leur facilité d'utilisation, les EMS bénéficieraient beaucoup d'une meilleure documentation. Un bon moyen pour y arriver serait la production des listes suivantes:

- liste des hypothèses,
- liste des événements initiateurs,
- listes des équipement critiques et de leur fonction,
- liste des actions créditées de l'opérateur, etc.

6.1.2.6 Suivi de la sûreté (EPS vivante)

Finalement, la principale lacune de l'EPS de Gentilly-2 est qu'elle ne possède pas de programme d'EPS vivante. Quelques unes des études

matricielles ont été révisées mais il n'existe pas de mise à jour périodique et systématique de celles-ci.

Les avantages et l'importance de maintenir son EPS à jour ont été discutés à la section 3.1 du présent mémoire et les principales activités requises pour supporter un programme d'EPS vivante sont énumérées à la section 3.1.6. L'auteur ne juge donc pas nécessaire de répéter ces points ici. Le lecteur est aussi invité à relire la section 6.1.1.1 démontrant qu'une EPS à jour est nécessaire pour répondre aux besoins de sûreté ainsi qu'à ceux de l'exploitation.

6.2 Améliorations souhaitables

Les éléments présentés dans cette section ne sont pas considérés comme des éléments indispensables à l'EPS de Gentilly-2 mais cependant constituent des améliorations souhaitables à celle-ci.

6.2.1 Niveau de détail

Les études matricielles de sûreté, principalement les plus anciennes, bénéficieraient beaucoup d'une modélisation plus détaillée. En plus d'éliminer plusieurs hypothèses simplificatrices, un nombre plus élevé d'événements initiateurs pourraient aussi être évalué. On obtiendrait ainsi une meilleure assurance que les modèles représentent bien les conditions de centrale. Les modèles pourraient aussi subir plusieurs analyses de sensibilité afin d'optimiser les règles d'exploitation de la Ligne de Conduite pour l'Exploitation (LCE).

6.2.2 Analyse de région

Les informations comprises dans les analyses de région permettent de produire des coupes par région (ex.:par salle d'équipement) au lieu de coupes par équipement. Ce type d'analyse permet de répondre à la question suivante: "Quels composants sont affectés par un incendie dans cette salle?". Ce type d'analyse est donc très utile lorsque l'on veut produire une évaluation probabiliste de sûreté qui tient compte d'événements initiateurs comme des feux ou des tremblements de terre.

6.2.3 Planification de la maintenance

Les modèles d'EPS peuvent être utilisés pour planifier les activités de maintenance et s'assurer ainsi qu'un certain niveau de risque n'est pas dépassé. Il existe divers outils sur le marché (EOOS, ORAM, etc.) permettant d'intégrer les cédules de maintenance aux modèles d'EPS. Hydro-Québec pourrait donc envisager l'achat d'un tel outil afin de faciliter la gestion des arrêts planifiés de Gentilly-2. Cependant, il faudra au préalable, que l'état d'arrêt du réacteur soit modélisé et informatisé.

CHAPITRE 7

SOLUTIONS PROPOSÉES

La direction d'Hydro-Québec évalue actuellement la possibilité de prolonger la durée de vie utile de la centrale nucléaire Gentilly-2. La décision concerne principalement le remplacement des canaux de force du réacteur. Si l'on décide de ne pas les changer, la centrale cessera d'être exploitée en 2008. Dans le cas contraire, sa durée de vie pourrait être prolongée de plusieurs années.

Le nombre d'années d'exploitation restantes a un impact significatif sur le choix des améliorations à apporter à l'EPS de Gentilly-2. En effet, en fonction du temps de réalisation et des ressources requises, certains changements ne peuvent offrir les bénéfices escomptés pour une durée de temps déterminée.

Le présent chapitre propose donc trois solutions en fonction de la durée de vie restante de la centrale nucléaire Gentilly-2.

7.0 Option 2008

Hypothèses: La centrale nucléaire Gentilly-2 cessera d'être exploitée en 2008.

Le peu de temps d'exploitation restant permet peu de changements et oblige à se concentrer sur les activités les plus bénéfiques à court terme. Celles-ci sont:

- le développement d'outils qualitatifs (listes, tableaux, etc.) consistant à l'identification des événements initiateurs, de leurs principales causes, des équipements critiques, de leurs fonctions et des séquences d'événements.

- l'implantation d'un suivi de la fiabilité opérationnelle des principaux équipements et systèmes incluant le suivi des essais, de la maintenance, des inspections et des contrôles chimiques.

7.1 Option 2013

Hypothèses: La centrale nucléaire Gentilly-2 cessera d'être exploitée en 2013.

Étant donné le temps d'exploitation restant, il n'est pas économiquement rentable de répondre à tous les besoins mentionnés au précédent chapitre comme, par exemple, réviser entière l'EPS de Gentilly-2. En plus des activités mentionnées pour l'option 2008, il est préférable de concentrer les efforts et ressources sur le suivi de la sûreté par l'entremise des études de fiabilité. Pour ce faire, les étapes suivantes sont proposées:

1. L'identification et priorisation des systèmes qui advenant leur défaillance d'agir tel que le prévoit leur conception ou les analyses de sûreté, ont un impact potentiel sur la sûreté de la centrale.

2. La réalisation d'études de fiabilité informatisées pour les principaux systèmes identifiés ci-dessus. Dans la majorité des cas, cette étape sera plutôt une étape de révision puisque plusieurs systèmes sont déjà modélisés.

3. La production d'arbres de défaillance dit "simplifiés" à partir des arbres de défaillance détaillés des études existantes. Un arbre simplifié est un arbre qui regroupe plusieurs défaillances présentées dans les arbres détaillés. Les arbres simplifiés en plus de permettre une réévaluation rapide des systèmes comportent les avantages suivants:
    - facilitent l'illustration des principaux blocs potentiellement responsables de la défaillance des systèmes;
    - mettent en évidence les interrelations entre les différents systèmes;

- facilitent l'analyse des arbres de défaillance;
- peuvent être réutilisés dans d'autres études probabilistes de sûreté, par exemple les EMS.

4. Comparaison des résultats des études de fiabilité avec les paramètres crédités dans les EMS.
   a) si les données concordent: Aucune action à prendre.
   b) si les données ne concordent pas: On doit analyser les situations cas par cas.

5. Détermination d'objectifs probabilistes de fiabilité pour chacun des systèmes modélisés.

6. Suivi de la fiabilité afin de s'assurer que les études de fiabilité reflètent bien tous les changements pertinents.
   a) Modification de la conception: Toutes les modifications à la conception devront être évaluées au préalable afin de s'assurer que les objectifs de fiabilité continueront d'être rencontrés. Lorsque ces modifications seront réalisées en chantier, les modèles devront être mis à jour afin de respecter ces changements.
   b) Suivi des activités d'exploitation: Les essais et les entretiens préventifs devront être planifiés et suivis de façon systématique afin de respecter les conditions modélisées dans les études de fiabilité de système. Le logiciel "Essais" actuellement en développement devrait combler ce besoin pour les essais et donc la création d'un logiciel similaire pour les entretiens préventifs devrait être envisagée.
   c) Suivi des performances: Les données de fiabilité devront être colligées et les performances des systèmes calculées. Une mise à jour des paramètres de fiabilité des études devrait avoir lieu à chaque année. La solution la plus efficace et économique serait que les RTS s'occupent de colliger les données pour leur système et que les spécialistes des études probabilistes analysent ces données et calculent les performances des systèmes grâce à un logiciel.

Pour retirer tous les bénéfices d'une telle démarche, les cinq premières étapes doivent être réalisées le plus rapidement possible. Il faudrait absolument qu'elles soient terminées pour le début de l'année 2003. Les coûts et ressources reliés à la réalisation de ces étapes dépendent grandement du nombre de systèmes à modéliser et de la qualité des études de fiabilité existantes. L'évaluation précise de ces facteurs est en dehors des limites du présent mémoire. Une brève analyse permet cependant de supposer que cette option n'engendrerait aucune dépense supplémentaire significative pour Hydro-Québec. En effet, les premières étapes nécessiteront peut-être plus de ressources pour les quatres prochaines années mais par la suite ces coûts diminueront grandement puisque le suivi de la fiabilité de systèmes ne devrait pas nécessiter plus de deux personnes par année pour l'Équipe Fiabilité.

7.2 Option prolongement de la durée de vie

Hypothèse: La durée de vie de la centrale nucléaire Gentilly-2 sera prolongée au delà de 2013.

Étant donné le nombre d'années d'exploitation restantes et la situation actuelle de l'EPS de Gentilly-2, la meilleure solution envisagée est la révision complète de celle-ci et la mise en place d'un programme d'EPS vivante.

7.2.1 Révision de l'EPS

Comparons les étapes de réalisation d'une EPS selon l'IAEA (figure C.2) avec celles de l'étude matricielle de sûreté 66RS-7 présentées à la section 5.4. On constate que les étapes de réalisation sont sensiblement les mêmes. Une analyse de cette situation permet donc d'affirmer que la liaison des études matricielles de sûreté offre la même structure qu'une EPS de type international tout en conservant les avantages liés aux EMS. C'est donc cette structure qui apparaît être le meilleur choix. Les étapes de réalisation seront donc les

mêmes que celles effectuées actuellement, à la différence que le tout devra être construit de façon à pouvoir joindre les études ensemble.

Dans un premier temps, toutes les études matricielles seront révisées sauf celle sur le confinement (66-SDM-8) et celle sur la perte de refroidissement en temps d'arrêt (66-RS-7). En second lieu, l'étude matricielle de sûreté 66-RS-7 sera révisée et modifiée de façon à obtenir une EPS en état d'arrêt. Suite à la réalisation de ces études, une EPS de niveau 2 sera produite en s'inspirant de l'étude matricielle de sûreté 66-SDM-8. Le résultat escompté est une EPS entièrement révisée et informatisée qui répond aux différents besoins mentionnés au chapitre précédent.

Selon le jugement d'experts d'hydro-Québec et d'EACL, les ressources requises afin d'obtenir une telle structure d'EPS sont évaluées à 55 personnes-année. La composition de l'équipe chargée de ce projet devrait correspondre à celle présentée au tableau II.

Tableau II

Composition de l'équipe requise pour réviser l'EPS de Gentilly-2

Composition de l'équipe	**Personnel requis (personnes)***
Chargé de projet	1
Analyste de système	4-6
Spécialiste d'EPS	3-4
Analyste de fiabilité humaine	1-2
Analyste des données	1-2
Analyste des événements externes	1-2
Spécialiste en progression d'accident	2-3
Spécialiste des structures	1-2

* Certaines de ces personnes peuvent ne pas être requises pour la durée complète de la révision ou peuvent être impliquées dans plus d'une tâche.

Le coût moyen de révision par EMS est évalué à 500 000$ et celui de réalisation d'une EPS de niveau 2 est évalué à 1,5 millions. Donc la révision

entière de celles-ci devrait se chiffrer aux alentours de 8 500 000$.

Lorsque la révision de l'EPS sera terminée, de nouvelles EMS concernant des événements initiateurs non-traités dans la révision (ex.: un incendie dans le bâtiment réacteur) pourront être envisagées.

7.2.2 Base de données

Hydro-Québec doit se doter d'une base de données spécifique à la centrale nucléaire Gentilly-2 afin de réviser son EPS et d'en faire le suivi. Les étapes de création d'une telle base de données sont présentées à la figure 2.

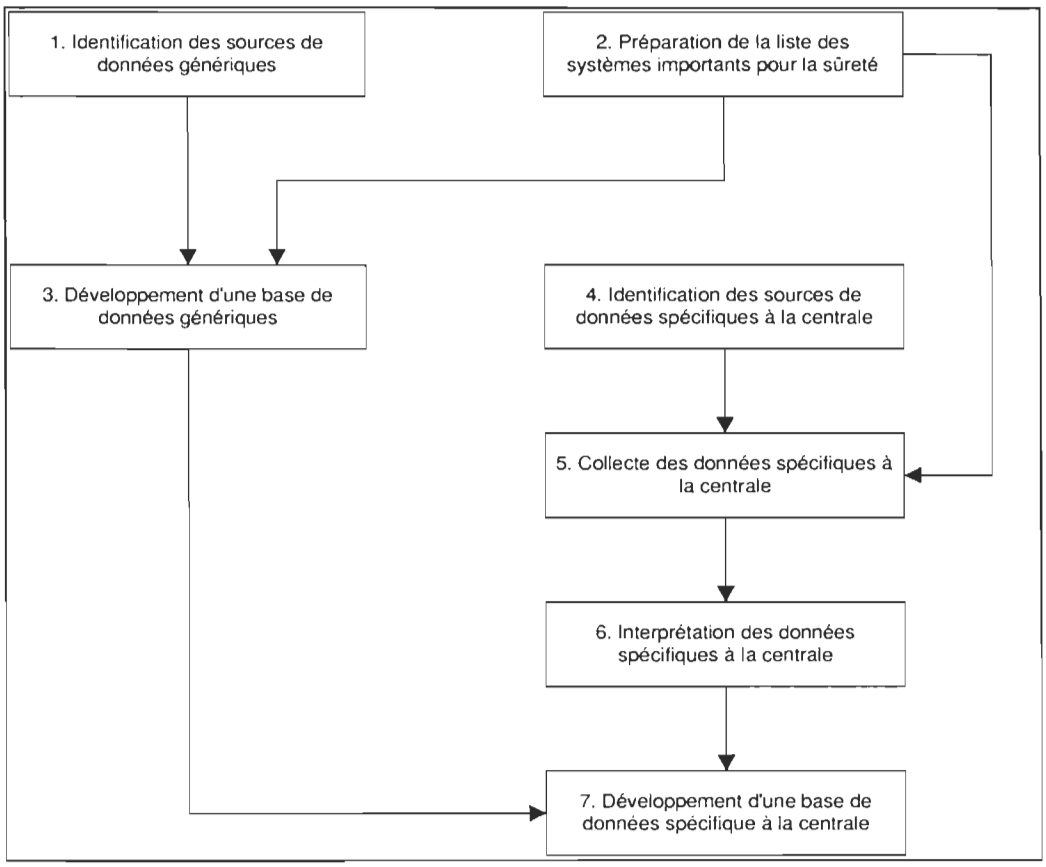

Figure 2. Étapes de création d'une base de données spécifique

La collecte et l'analyse des données disponibles à Gentilly-2 afin de produire un historique des systèmes débutant en 1992 devraient nécessiter environ 10 personnes-année. Le maintien d'une telle base afin d'effectuer un suivi des performances des systèmes modélisés est évalué à 5 personnes-année/année dont 2 personnes-année en fiabilité.

7.2.3 Programme d'EPS vivante

Un programme d'EPS vivante requiert des ressources pour utiliser et maintenir le modèle ainsi que des procédures répondant aux points suivants:

- Décider quand mettre à jour le modèle et/ou la documentation;
- Décider quelles informations doivent être inclues;
- Décider du niveau de détail;
- Décider des méthodes et personnes qui seront utilisées pour modéliser la centrale;
- Réviser l'analyse des données de fiabilité;
- Documenter les hypothèses et simplifications utilisées dans le modèle;
- Documenter les interdépendances dans le modèle;
- Faire des copies de sûreté;
- Contrôler l'accès au système d'EPS;
- Conserver des archives sur le contenu du modèle d'EPS;
- Fournir du feed-back au personnel;
- Documenter les carences de l'outils d'EPS et fournir du feed-back aux développeurs du système;
- Former le personnel d'EPS;
- Former le personnel d'exploitation à l'utilisation des outils et/ou des résultats d'EPS.

La structure du programme d'EPS vivante devra être mise en place dès que la révision de l'EPS sera achevée. L'établissement d'une telle structure devrait nécessiter environ 5 personnes-année. Par la suite, un minimum de trois personnes dans l'organisation devront être nommées responsables du suivi des modèles d'EPS.

7.2.4 Ressources requises

Le tableau III offre un estimé des ressources nécessaires à la révision et au maintien de l'EPS de Gentilly-2.

Tableau III

Estimé des ressources nécessaire à la révision et au maintien de l'EPS de Gentilly-2

Activités	Révision (personnes-année)	Maintien (personnes/année)
Révision des modèles	55	0
Création d'une base de données	10	5
Établissement d'un programme d'EPS vivante	5	3
Total	70	8

7.3 Option évolutive

Hypothèse: Cette situation correspond à la situation actuelle soit: la décision de prolonger ou non la durée de vie de la centrale nucléaire Gentilly-2 n'est pas encore connue.

La problématique de cette situation est liée au fait quand plus de ne pas connaître la décision, on ne connaît pas non plus le moment où elle sera prise. Sera-t-elle prise en l'an 2000 ou 2006?

Afin de remédier à cette situation, la solution proposée consiste à réaliser l'option 2008 et l'option 2013 ensemble. Cependant la réalisation de cette dernière option s'effectuera beaucoup plus lentement. En effet, la solution proposée consiste à réviser l'EPS de Gentilly-2 scénario par scénario, autrement dit, EMS par EMS. Le rythme envisagé serait de réviser une EMS aux trois années. La base de données ne serait construite que pour les systèmes modélisés.

Dans le cas où la durée de vie ne sera pas prolongée; on peut arrêter la révision après n'importe quel scénario et la base de données est construite seulement pour les systèmes modélisés.

Dans le cas où la durée de vie est prolongée, certains scénarios sont déjà modélisés, une partie de la base de données est construite, le personnel est formé et la structure du programme d'EPS vivante est déjà définie.

CONCLUSION

Le but de ce mémoire était de comparer les pratiques internationales en matière d'évaluation probabiliste de sûreté pour les centrales nucléaires avec celles utilisées pour les réacteurs CANDU 600 en exploitation au Canada afin de proposer une nouvelle structure d'EPS pour ces derniers.

Plus particulièrement, le présent mémoire a comparé l'approche internationale avec les études matricielles de sûreté (EMS) de la centrale nucléaire Gentilly-2. Une analyse de l'évolution de ces EMS a démontré que celles-ci, quoique différentes au début, sont maintenant très semblables à l'approche internationale. En effet, les EMS utilisent les mêmes outils informatiques et conséquemment les mêmes méthodes de modélisation. Les principales différences restantes sont liées au niveau de détails de séquences d'événements et au fait que les EMS évaluent une seule famille d'accident par étude. Ce dernier point rend impossible le calcul d'un CDF sans adaptation et regroupement de celles-ci. Il est à noter aussi qu'il n'existe pas d'EMS équivalentes à une EPS de niveau 2 ou 3.

L'analyse de l'EPS de Gentilly-2 a aussi fait ressortir certaine lacunes et besoins ayant traits au éléments suivants :

- Informatisation de l'EPS
- Documentation des études
- Suivi de la sûreté
- Formation du personnel

- La direction d'Hydro-Québec évalue actuellement la possibilité de prolonger la durée de vie utile de la centrale nucléaire Gentilly-2. La décision n'ayant pas encore été prise, trois hypothèses ont été émises quant à la durée restante d'exploitation de Gentilly-2 et une solution a été développée et proposée pour chacune d'elles:

- La centrale nucléaire Gentilly-2 cessera d'être exploitée en 2008 :
  La solution proposée consiste à développer des outils qualitatifs (liste, tableaux, etc.) et implanter un suivi de la fiabilité opérationnelle.

- La centrale nucléaire Gentilly-2 cessera d'être exploitée en 2013 :
  En plus des activités de l'hypothèse précédente, Hydro-Québec devrait concentrer ses efforts et ses ressources sur le suivi de la sûreté par l'entremise des étude de fiabilité

- La durée de vie de la centrale nucléaire Gentilly-2 sera prolongée au-delà de 2013 :
  Suite à l'analyse de l'EPS de Gentilly-2, la solution proposée est l'adoption d'une nouvelle structure d'EPS, combinant les forces et avantages des deux approches (EMS et internationale). La base de cette nouvelle structure est celle des EMS. Cette approche a surtout été privilégiée à cause des avantages pour la compréhension, l'illustration et la documentation de la réponse de la centrale lors de la défaillance d'un équipement ou d'un système. La nouvelle structure tire aussi avantage des outils développés pour l'approche internationale. Ces outils facilitent grandement l'informatisation de l'évaluation de la fréquence des scénarios d'accident. C'est pourquoi la nouvelle structure utilise à la fois la technique des séquences d'événement et des arbres d'événement. De plus, afin d'obtenir une meilleure assurance quant à la mesure de l'impact réel d'éventuels modes communs de défaillances entre les systèmes, les EMS sont intégrées ensemble, formant ainsi une seule étude. Sans oublier, le développement d'une base de données spécifiques et l'implantation d'un programme d'EPS vivante.

Les solutions proposées dans ce mémoire n'ont cependant pas été révisées par un organisme externe. Cette lacune devrait donc constituer la prochaine étape à réaliser. Par la suite, lorsqu'Hydro-Québec aura déterminé la durée restante d'exploitation de Gentilly-2, il faudra réaliser un plan d'action pour la solution qui sera choisie.

De nos jours, l'EPS est un outil reconnu d'évaluation et de gestion de la sûreté. La recherche bibliographique effectuée regorge d'exemples d'applications démontrant les avantages et bénéfices de cette méthode. Cependant, son utilisation est encore limitée aux domaines du nucléaire et de l'aérospatiale. Plusieurs autres domaines comportent des dangers pour le public (ex. : les complexes pétro-chimiques). Par conséquent, l'adaptation et la réalisation de ce type d'étude devrait être envisagée pour l'évaluation de la sûreté dans plusieurs autres domaines.

BIBLIOGRAPHIE

[1] AECL. Safety Design Matrix Probability Calculations. TTR-14, december 1981.

[2] AFNOR. AMDEC/AMDE/AEEL l'essentiel de la méthode. février 1994.

[3] CANVEY. An investigation of Potential Hazards from Operation in the Canvey ISland/Thurrock Area. Healt and Safety Executive, HMSO, 1978.

[4] CANVEY. A Second Report. Health ans Safety Executive, HMSO, 1981.

[5] Deriot, S. Impact of Shutdown Risk on Risk-Based Assessment of Technical Specifications. Collection de notes internes de la Direction des Etudes et Recherches, EDF. 93NB000610. octobre 1992.

[6] Dubreuil-Chambardel, A. Villemeur, A. Berger, J.P. Moroni, J.M. Living Probabilistic Safety Assessment of French 1300 Mwe PWR Nuclear Power Plant Unit : Methodology, Results and Teaching. Collection de notes internes de la Direction des Etudes et Recherches, EDF. 92NB00030. Février 1991.

[7] EPRI. PSA Applications Guide. Rapport EPRI TR-105396, August 1995.

[8] Gumley, P. Safety Design Matrices. File: XX-68000-130-000, august 1979.

[9] Hickman, et al. PRA Procedure Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants. Rapport NUREG/CR-2300 Vol. 1, 1983.

[10] Hurst, D.G. Boyd, F.C. Reactor Licensing and Safety requirements. Article 72-CNA-102. Présenté à la 12^{e} Conférence Annuelle de l'Association Nucléaire Canadienne, Ottawa juin 1972.

[11] IAEA. The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Plant Safety. Safety Series No. 106, Vienna 1992.

[12] IAEA. Probabilistic Safety Assessment. 75-INSAG-6, Vienna 1992.

[13] IAEA. Procedures for Conducting Probabilistic Safety Nuclear Power Plants (Level 1). Safety Series No. 50-P-4, Vienna 1992.

[14] IAEA. Procedures for Conducting Probabilistic Safety Nuclear Power Plants (Level 2). Safety Series No. 50-P-4, Vienna 1995.

[15] IAEA. Procedures for Conducting Probabilistic Safety Nuclear Power Plants (Level 3). Safety Series No. 50-P-4, Vienna 1996.

[16] IAEA. PSA for the Shutdown Mode for Nuclear Power Plants Proceedings of the Technical Committe meeting held in Stockholm, 30 november-3 december 1992. IAEA-TECDOC-751. 1994.

[17] NEA. Probabilistic Safety Assessment : An Analytical Tool For Assessing Nuclear Safety. NEA Issue Brief No 8, January 1992.

[18] NEA. Living PSA Development and Application in Member Countries: Summary of TÜV Workshops held from 1988 to 1994. OCDE/GD(96)24, 1996.

[19] Nieuwhof, G.W.E. Risk : A Probabilistic Concept. Reliability Engineering, vol. 10, n° 3. 1985.

[20] OECD. L'évaluation probabiliste de la sûreté dans la gestion des centrales nucléaires. Paris 1989.

[21] OECD. Living Probabilistic Safety Assessment for Nuclear Power Plant Management. Paris 1992.

[22] Otway, H.J. Erdmann, R.C. Reactor Safety and Design from a Risk View Point. Nuclear Engineering Design, 13, 365. 1970.

[23] Pagès et Gondran. Fiabilité des systèmes. Éditions Eyrolles. 1980.

[24] Raina, V.M. Experience with PRA Application in Ontario Hydro Nuclear. Communication presented at the 11th Pacific Basin Nuclear Conference held in Banff, may 3-7 1998.

[25] Riggs, J.L. Rentz, W.F. Kahl, A.L. West, T.M. Engineering Economics. First canadian Edition. McGraw-Hill Ryerson. 1986.

[26] Santamaura et al. Severe Core Damage Frequency and Insights from CANDU 6 level 1 Probabilistic Safety Assessment. Paper presented at the11th Pacific Basin Nuclear Conference held in Banff, may 3-7 1998

[27] SKI. Safety Evaluation by Living Probabilistic Safety Assessment. Procedures and Applications for Risk Planning of Operational Activities and Risk Analysis of Operating Experience. SKI Report 94:2. NKS/SIK-1(93)16, january 1994.

[28] SKI. NKS/SIK-1 Reports and Publications on LPSA Development. Supporting documentation for: Safety Evaluation by Living Probabilistic Safety Assessment. Procedures and Applications for Risk Planning of Operational Activities and Risk Analysis of Operating Experience. SKI-Report 94:3.

[29] Slovic, P. and All. The Assessment and Perception of Risk. The royal society of London. 1980.

[30] Tanguy, P. Guyonnet, J.F. La prévision rationnelle des grands risques. Le progrès technique, n^{os} 11-12. décembre 1978.

[31] USNRC Fault Tree Handbook. Rapport NUREG-0492, 1981.

[32] USNRC. Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, 1983.

[33] USNRC. Probabilistic Risk Analysis Reference Document. Rapport NUREG-1050, 1984.

[34] USNRC. Probabilistic Risk Analysis Review Manual. Rapport NUREG/CR-3485, 1985.

[35] USNRC. Probabilistic Safety Analysis Procedures Guide. Rapport NUREG/CR-2815, Vol. 1 Rev.1, 1985.

[36] USNRC. Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Rapport NUREG/CR-4780 Vol.1, 1988.

[37] USNRC. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants. Rapport NUREG-1150 Vol.1 Rev.2, 1989.

[38] Villemeur, A. Sûreté de fonctionnement des systèmes industriels. Éditions Eyrolles, Paris 1988.

Documents Hydro-Québec

[39] DEVA Services Inc. Probabilistic Safety Assessment Options for Gentilly-2 CANDU 600 Station. september 1997

[40] NM-9.09. Études probabilistes de sûreté. Rév. 1, octobre 1998.

[41] PF-EFP-008. Guide pour la préparation des arbres de défaillances simplifiés. février 1997

[42] PF-EMS-000. Les études probabilistes d'évaluation de la fiabilité et de la sûreté nucléaire. novembre 1992.

[43] PF-GEN-001. Glossaire de fiabilité. septembre 1997.

[44] PSP-MFE-005. Guide de rédaction des études matricielles de sûreté. 1994

[45] Saint-Denis, M. Comeau, R. Contenu de l'étude matricielle de sûreté 66RS-7 (rev. 2): Perte de refroidissement en temps d'arrêt. février 1998.

[46] 66 SDM-1. Inadvertent Addition of Positive Reactivity. février 1981.

[47] 66 SDM-2. Loss of Steam Generator as a Heat Sink. février 1982

[48] 66 SDM-3. Large Loss Coolant Accident and Emergency Core Cooling System. octobre 1980.

[49] 66 SDM-4. Operation after a Eartquake. juillet 1980.

[50] 66 SDM-5. Flooding of Turbine and Service Buildings. avril 1982.

[51] 66 SDM-6. Reactor Building Flooding. juin 1982.

[52] 66 SDM-7. Small Loss of Coolant Accident and Emergency Core Cooling Operation. septembre 1980.

[53] 66 SDM-8. Containement Operation. juin 1982.

[54] 66 SDM-9. Moderator as a Heat Sink. avril 1981.

[55] 66 RS-4. Dual Computer Failure. mars 1981.

[56] 66 RS-5. Moderator and Shield Cooling System Failures. mai 1980.

[57] 66 RS-7. Perte de refroidissement en temps d'arrêt. (DRAFT).

[58] 66 RS-8. Perte complète de l'alimentation d'air d'instrument. février 1986.

[59] 66 RS-9. Perte complète de l'eau de service. février 1986.

[60] 66 RS-10. Perte complète de l'alimentation électrique de catégorie IV. mai 1996.

Manuels d'utilisateur

[61] SAIC. RMQS User's Manual. 1993.

[62] SAIC.GTPROB Reference Guide.1993.

[63] SAIC/EPRI. CAFTA for Windows: Fault Tree Analysis System Version 3.2. User's Manual. 1996.

[64] SAIC. Uncert for Windows: PSA Uncertainty Analysis Tool Version 1.0B. User's Manual. 1997.

[65] SAIC/EPRI. ETA for Windows: Event Tree Analysis System Version 3.1. User's Manual. 1997.

[66] SAIC/EPRI. PRAQUANT for Windows: Accident Sequence Quantification Version 3.3. User's Manual. 1997.

[67] STAR Inc. Logiciel GSEAO. 1993.

Sites WEB consultés

PLG Nuclear Energy Services. (Page consultée le 16 juillet 1998). *PLG Nuclear Energy Services*, adresse URL:http://www.plg.com/pages/nucset1.html

SAIC. (Page consultée le 16 juillet 1998). *Risk & Reliability Tools*, adresse URL: http://fsg.saic.com/html/risk___reliability_tools.html

RELCON AB. (Page consultée le 16 juillet 1998). *Risk Spectrum - Main*, adresse URL: http://www.riskspectrum.com/

Lockheed Martin. (Page consultée le 16 juillet 1998). *SAPHIRE - Systems Analysis Programs for Hands-on Integrated Reliability Evaluations,* adressse URL: http://sageftp.inel.gov/saphire/saphire.asp

ERIN Software. (Page consultée le 16 juillet 1998). *OVERVIEW OF ERIN SOFTWARE*, adresse URL: http://www.erineng.com/software.htm

Documents d'informations publiques d'Hydro-Québec

Hydro-Québec, Glossaire des termes nucléaires, 1992. ISBN 2-550-26834-2. HQ DE-92-106-F-2.

Hydro-Québec, La sûreté à la centrale nucléaire Gentilly-2, 1992. ISBN 2-550-26883-4. HQ DE-92-106-F-1.

Hydro-Québec, Le fonctionnement de la centrale nucléaire Gentilly-2, 1994. ISBN 2-550-29323-1.

ANNEXE A

DEFINITION DU CONCEPT DE RISQUE[1]

A.1 Introduction

Définir précisément le concept de risque est une tâche difficile étant donné le grand nombre d'acceptations différentes de ce concept (aussi bien dans le langage courant que dans le langage technique) et de la confusion souvent faite avec le concept de probabilité. Il existe plusieurs propositions de définitions pour ce concept qui visent toujours à associer deux aspects d'un même événement soit: sa probabilité d'occurrence et ses effets ou conséquences.

Cette annexe a pour objet de présenter le concept de risque par la présentation de résumés ou d'extraits de lectures. En premier lieu, la définition ainsi que les expressions mathématiques du risque décrites par Nieuwhof (1985) sont exposées. Cette définition, tout en étant générale (champ d'application large), utilise une terminologie précise éliminant les incompréhensions. Par la suite, ce document introduit les aspects de la perception et du niveau d'acceptabilité du risque tels que présentés dans le livre de Villemeur (1988). Ils sont suivis par la méthodologie d'évaluation du risque ainsi que sa critique comme présentées par Tanguy et Guyonnet (1978). La notion de bénéfice attendu qui est utilisée pour les comparaisons économiques impliquant des risques (Riggs et al. (1986)) est aussi présentée et, finalement, une transposition du concept de risque aux centrales nucléaires de type CANDU a été effectuée.

---

[1] Cette annexe est la copie de l'article suivant: Lacroix, E. Définition du concept de risque. Bulletin de la Société Nucléaire Canadienne, hiver 1997.

A.2 Définition du risque

Le risque peut être défini comme suit : *"La perte ou le dommage envisagé et considéré qui est associé à l'occurrence d'un événement indésirable possible."*

Certains termes de cette définition demandent quelques explications supplémentaires:

1. « événement indésirable »

Ce terme inclut :

- l'occurrence de conditions indésirables ;
- un accident (ex.: une défaillance, une destruction, une désintégration, etc.) ;
- une action défavorable particulière (dangereuse ou coûteuse).

2. « la perte ou le dommage envisagé»

Ce terme sera traité avec une attente mathématique:

Si p est la probabilité qu'une personne perdra une somme d'argent S durant une action particulière de jeu d'argent (gambling), alors l'attente mathématique de la perte d'argent est définie comme le produit de p et S, c'est-à-dire $p \times S$.

Nous pouvons présenter cette situation de la manière suivante:
La perte attendue par une personne qui parie une somme d'argent S dans un jeu particulier est :

$$\text{Prob.}\{\text{perdre la somme S}\} \times [\text{la somme d'argent S}]$$

Dans cet exemple l'événement indésirable est l'action défavorable de perdre la somme d'argent S.

3. « considéré »

Si nous évaluons le risque associé à un type particulier de perte causée par un événement indésirable particulier, alors nous ne devons pas inclure les pertes causées par d'autres événements. Le concept de risque, comme défini ci-dessus, est pratique seulement si l'événement et les pertes sont définis précisément.

À partir de la définition du risque et de sa discussion et avant que le risque d'une perte particulière associé avec l'occurrence d'un événement particulier puisse être établi, il est clair qu'un modèle probabiliste valide doit être confirmé. De la théorie de base des probabilités, il est reconnu qu'un modèle probabiliste demande :

> "Une expérience bien définie, laquelle détermine tous les résultats possibles et permet de différencier un résultat qualifié de "succès" ou "d'échec"."

Par « une expérience bien définie » nous entendons une description précise du système, son opération ou action, et les conditions sous lesquelles il est supposé fonctionner. Le terme « système » est utilisé dans un sens très général. Il inclut les systèmes techniques, biologiques, organiques, etc. En association avec le risque il est évident qu'un "échec" est la perte ou le dommage causé, si l'événement indésirable possible se produit.

A.3 Les expressions mathématiques du risque

L'expression mathématique la plus générale du risque est :

$$\text{Risque} = [\text{Prob.}\{\text{événement se produise}\}] \times [\text{le coût probable si l'événement se produit}]$$

ou

$$\text{Risque} = [\text{Prob.}\{\text{événement}\}] \times [\text{Estimé}\{\text{coût par événement}\}]$$

Avec ceci en tête, trois types de modèle de risque peuvent être distingués.

1. Risque associé avec l'incertitude de l'occurrence d'un événement indésirable et ses conséquences fixes ou déterministes.

   Risque I = [Prob.{événement}] × [Estimé{coût / événement} = C]
   Risque I = [Prob.{événement}] × C

2. Risque associé avec l'incertitude de l'importance des conséquences d'un événement indésirable d'occurrence fixe ou déterministe.

   Risque II = [Prob.{événement}=1] × [Estimé{coût/événement}]
   Risque II = Estimé{coût/événement}

3. Risque associé avec l'incertitude de l'occurrence de l'événement indésirable et l'incertitude de l'importance de ses conséquences.

   Risque III = [Prob.{événement}] × [Estimé{coût/événement}]

A.4 Exemples

Il est très important de bien comprendre, premièrement, la distinction entre le concept de risque et celui de probabilité et, deuxièmement, de définir de façon très précise l'événement indésirable et ses conséquences. Voici quelques exemples que l'on peut entendre dans la vie courante et qui peuvent présenter certaines difficultés.

1. Le risque de se briser la jambe pour un skieur inexpérimenté est plus élevé que celui d'un skieur expérimenté.

   Dans ce cas, la conséquence est fixe et c'est la probabilité d'occurrence qui varie. On considère que le skieur inexpérimenté tombera plus souvent et conséquemment il est plus probable qu'il se blesse. Ici l'événement indésirable

est une chute en ski et non se briser une jambe. Le fait de se briser une jambe est la conséquence de la chute.

2. Le risque de mort ou de blessure est plus élevé pour ceux conduisant une automobile sans ceinture de sécurité que pour ceux la portant.

   Ici, la probabilité d'accident est théoriquement la même pour les deux types de conducteur. Cependant, les conséquences ne sont pas les mêmes. L'événement indésirable est un accident et ses conséquences sont la mort ou des blessures.

3. Le risque de blessure à la tête et/ou au visage des joueurs de hockey professionnels est plus faible aujourd'hui qu'auparavant.

   Dans cet exemple l'événement est de jouer au hockey et ses conséquences sont d'être blessé à la tête et/ou au visage. La probabilité d'occurrence a augmenté (les joueurs jouent plus de parties qu'avant) mais les conséquences ont diminué (le port du casque avec visière).

Comme on peut le constater, l'augmentation du risque n'est pas nécessairement associée avec une augmentation de la probabilité d'occurrence d'un événement. Il ne faut donc pas mélanger le concept de risque et celui de probabilité. La description de l'événement et de ses conséquences doit être la plus précise possible pour éviter les erreurs. L'exemple numéro 1 n'a de sens que lors d'une descente en ski car dans la vie quotidienne le fait d'être un skieur expérimenté ne nous protège point des accidents.

A.5 Acceptation du risque

L'acceptation du risque par les individus et par la société est influencée par de nombreux facteurs. Le plus important d'entre eux est lié au caractère volontaire ou involontaire du risque couru; on accepte ainsi de courir des risques plus importants

lorsqu'ils sont volontairement pris. Citons d'autre facteurs : les effets immédiats ou retardés du danger, la présence ou l'absence d'alternatives, la connaissance précise ou imprécise du risque, le danger commun ou particulier à certaines personnes, la réversibilité ou l'irréversibilité des conséquences.

Les activités volontaires et involontaires se définissent de la manière suivante :

Activité volontaire : l'individu décide librement d'exercer cette activité en fonction de son expérience, de ses goûts, etc. (exemples : alpinisme, tabagisme).

Activité involontaire : l'individu est soumis à ce risque dont généralement le choix, le contrôle ou la maîtrise lui échappe.

Dans les pays occidentaux industrialisés, le risque de décès provenant de maladie est d'environ 10^{-2}/an. C'est une référence pour les plus hauts niveaux de risque involontairement acceptés. Le plus bas niveau de risque involontairement accepté est celui qui résulte d'événements naturels tels que la foudre, les inondations, les piqûres d'insectes, etc. Il est d'environ 10^{-6}/an. Entre ces deux extrêmes, le public semble accepter des risques involontairement courus en fonction des bénéfices escomptés. L'enquête menée par Otway et Erdmann (1970) aboutit schématiquement aux conclusions suivantes sur les niveaux annuels de risque individuel de décès :

- 10^{-3}/an : Ce niveau de risque est inacceptable ; dès qu'un risque approche ce niveau, des mesures immédiates sont prises pour le réduire.
- 10^{-4}/an : Le public réclame des dépenses publiques pour contrôler et réduire ce risque (ex. : trafic automobile, incendies, etc.).
- 10^{-5}/an : Les risques de ce niveau sont identifiés par le public (ex.: noyade, arme à feu, etc.). Des conseils sont donnés pour les réduire (ex. : ne jamais nager seul en mer).

- 10^{-6}/an : Les risques de ce niveau n'inquiètent pas l'individu moyen; l'individu est au courant de ces accidents mais pense que ça arrive uniquement aux autres; il se montre résigné face à de tels risques.

Les auteurs de cette enquête en concluaient que le risque individuel de décès de 10^{-7}/an est une limite supérieure acceptable pour le risque issu d'accidents de centrales nucléaires.

A.6 Perception du risque

De très nombreux facteurs affectent la perception des risques par les individus. Une intéressante enquête aux Etats-Unis menée par Slovic et all (1980) a montré la relation entre le risque perçu par le public et le risque réel. Il apparaît ainsi que:

- Les causes de décès du type « maladie » et « accident de la route » sont considérées comme équivalentes alors que les premières sont dix fois plus nombreuses.
- Les risques qui contribuent de manière importante au nombre de morts sont sous-estimés.
- Les risques qui contribuent peu au nombre de morts sont surestimés ; ainsi les événements de caractère exceptionnel (inondations, tornades) sont considérés comme beaucoup plus meurtriers qu'ils ne le sont en réalité.

Cette enquête semble confirmer le fait que le public juge « moins dangereux » une activité qui fait 1 mort tous les jours que 300 morts une fois par an. La perception des risques dépend de nombreux facteurs moraux et psychosociologiques qui apparaissent difficilement quantifiables ou même explicables.

A.7 Prévision du risque

Pour les événements indésirables se produisant avec des fréquences relativement élevées, il est possible de partir des observations du passé pour fonder une évaluation prévisionnelle qui prenne en compte l'évolution du niveau d'activité et des techniques employées. Par contre, pour ceux dont la probabilité d'occurrence est faible, il faut adopter une approche entièrement différente.

A.7.1 Méthode d'évaluation du risque

1. Rechercher les événements initiateurs d'accidents

Établir la liste de toutes les défaillances envisageables, sur les composants et sur les organes de liaison, susceptibles de faire sortir le système de son fonctionnement normal et de créer un accident.

2. Étudier les scénarios d'accidents

À partir des événements initiateurs, on doit ensuite établir l'ensemble des séquences accidentelles qui peuvent en découler. On est donc amener à tracer ce qu'on appelle un "arbre ou séquence d'événements". Dans certains cas, on peut partir d'événements indésirables rencontrés et remonter aux différentes causes initiales qui peuvent en être l'origine, ce qui correspond à la méthode de "l'arbre de défaillance".

3. Évaluation de la probabilité d'accident

Le scénario d'accident ayant été établi, il est possible de calculer la probabilité de voir arriver l'événement indésirable à partir de la probabilité des événements initiateurs et des probabilités respectives des événements successifs. Généralement, on s'appuie sur les statistiques disponibles sur les types d'événements considérés pour évaluer leur probabilité.

4. Exposition de l'environnement

Pour évaluer les conséquences du scénario, il est nécessaire de connaître l'état de l'environnement du système au moment où se produit l'événement indésirable.

5. Calcul des conséquences

Pour chaque type d'environnement, l'événement indésirable conduira à des dommages résultant de l'événement considéré et de l'environnement dans lequel il se produit. Pour chaque événement on dispose donc d'un spectre de conséquences dont chaque élément sera affecté du temps d'exposition dans l'environnement considéré.

6. Évaluation du risque

La quantification du danger est généralement représentée par une grandeur à plusieurs dimensions (nombre de victimes, dommages financiers, etc.) fonction du couple défaillances-environnement retenu. Cette grandeur sera toujours bornée supérieurement, le danger potentiel maximal correspondant à la défaillance totale du système survenant dans l'environnement le plus critique.

Remarque: Il faut signaler qu'il peut y avoir une corrélation entre le scénario d'accident et l'environnement et qu'il faut porter une attention particulière aux causes communes de défaillances

A.7.2 Critique de la méthode

1. Le manque d'exhaustivité des événements initiateurs

On ne sera jamais parfaitement sûr d'avoir pensé à tous les scénarios possibles pouvant engendrer l'événement indésirable considéré.

2. L'insuffisance des connaissances sur certains phénomènes

Le calcul des probabilités des événements s'appuie toujours sur une bonne connaissance des systèmes en question et une compréhension bien formulée des phénomènes qui s'y passent. C'est loin d'être toujours le cas, pour le physicien s'efforçant de comprendre les phénomènes et pour l'ingénieur s'efforçant de les manoeuvrer.

3. La difficulté d'appréhender les probabilités cherchées

- La rigueur des méthodes de calcul n'est pas toujours acquise. Il faut interpréter avec prudence les valeurs de probabilités obtenues.
- Les données de base nécessaires au calcul de la probabilité de l'événement indésirable en fonction des probabilités de ses causes ne sont pas toujours accessibles quand elles existent, parce que les rapports d'exploitation n'ont pas été conçus en vue de la gestion des risques. Le plus souvent ces données n'existent pas.
- Le facteur humain qui est essentiel dans tous les scénarios est difficilement quantifiable.

4. La difficulté d'évaluation des conséquences possibles

L'extension spatiale sur des centaines de kilomètres, la multiplicité des formes prises par les dommages, l'influence différée sur des années, le mode pernicieux de l'agression (invisibilité des radiations), le comportement irrationnel des humains en groupe important (panique), tous ces facteurs rendent une évaluation exacte des conséquences très difficile, voire impossible sans une marge d'erreur d'un facteur 2, 4, 10 ou plus?

A.8 Le bénéfice attendu

Le bénéfice attendu est la mesure standard utilisée pour les comparaisons économiques impliquant des risques. Il prend en considération les effets des risques sur les résultats potentiels grâce à une moyenne pondérée. Les résultats sont

pondérés en fonction de leur probabilité d'occurrence. La somme des produits de chaque résultat, multipliée par sa probabilité respective, est le bénéfice attendu.

Prenons comme exemple le jeu suivant: On doit payer 1$ pour avoir la chance de lancer deux pièces de monnaie. Si l'on obtient deux "face" on reçoit 2$, pour deux " pile" on reçoit 1$ et rien pour les autres résultats. Le calcul du bénéfice attendu est le suivant:

$$BA = P(F,F)*(2\$-1\$) + P(P,P)*(1\$-1\$) + P(P,F)*(-1\$) + P(F,P)*(-1\$)$$
$$= 0,25*1\$ + 0,25*0\$ + 0,25*-1\$ + 0,25*-1\$ = -0,25\$$$

Ce calcul démontre que ce jeu n'est pas payant car la perte moyenne par partie est de 0,25$. Cependant pour chaque partie que l'on jouera, le risque de perdre la somme misée sera de :

$$Risque = P \text{ (perdre 1\$)} * 1\$ = 0,5 *1\$ = 0,50\$$$

Si pour deux "face" l'on obtiendrait 10$ au lieu de 2$, le bénéfice attendu deviendrait 1,75$ mais le risque de perdre la somme misée demeure le même.

Le bénéfice attendu est une notion liée au risque. Il peut altérer la perception que l'on a d'un risque et servir de critère d'acceptabilité. Dans l'exemple ci-dessus, le risque est le même mais cependant un joueur avisé choisira le 2^{e} jeu.

A.9 Évaluation du risque des centrales nucléaires de type CANDU

Toute activité implique un certain degré de risque et la plupart des activités industrielles comportent certains dangers publics. Certains de ces risques sont chroniques, comme le dégagement continu de produits chimiques toxiques provenant des camions, fonderies et centrales au charbon ainsi que l'échappement continu de petites quantités de matières radioactives provenant des centrales

nucléaires. Certains de ces risques sont aigus (accidents) comme par exemple, les explosions, les ruptures de barrages et l'écroulement de bâtiments. Pour une centrale nucléaire les accidents pouvant entraîner la libération de grandes quantités de matières radioactives présentent un danger pour la santé publique.

Dans le cas de la sûreté nucléaire, la probabilité d'occurrence de l'événement est d'habitude la fréquence annuelle c'est-à-dire "le nombre de fois par an" et la mesure de conséquence est généralement "la dose d'irradiation reçue par le public".

Au Canada, la Commission de Contrôle de l'Énergie Atomique (CCEA) établit les directives sous une forme numérique pour la fréquence et les conséquences des accidents. Le tableau A-1 extrait de Hurst et Boyd (1972) présente ces directives.

Tableau A-1

Directives de la CCEA pour des conditions accidentelles

Situation	Fréquence maximale	Environnement	Dose-limite individuelle	Dose-limite de la population
Exploitation normale		Pondérer selon l'effet (fréquence multipliée par la dose pour obtenir le dégagement unitaire)	0,5 rem/an (corps entier) 3 rem/an (thyroïde)	10^4 homme-rem/an (corps entier) 10^4 rem/an (thyroïde)
Défaillance simple	1/3 ans	La pire température prévalant au plus 10% du temps ou la condition F de Pasquill si les données locales sont incomplètes	0,5 rem (corps entier) 3 rem (thyroïde)	10^4 homme-rem (corps entier) 10^4 rem (thyroïde)
Défaillance double	1/3000 ans	La pire température prévalant au plus 10% du temps ou la condition F de Pasquill si les données locales sont incomplètes	25 rem (corps entier) 250 rem (thyroïde)	10^6 homme-rem (corps entier) 10^6 rem (thyroïde)

A.10 Conclusion

Peu importe ce que nous faisons, il existe toujours un risque. Il est irréductible à zéro quoi que l'on fasse. La sécurité absolue n'existe pas. Cependant, on peut s'efforcer de fixer des critères d'acceptabilité pour chaque catégorie de risque par

référence aux risques admis dans des activités existantes et en fonction des bénéfices attendus, individuels ou collectifs. Ces critères ne peuvent pas avoir de valeur objective absolue. La fixation des niveaux de risques acceptables restera toujours en définitive du ressort du pouvoir politique.

ANNEXE B

CONTENU D'UNE EPS

Cette annexe identifie les différents éléments constituants une EPS ainsi que leur niveau de détails. Les techniques d'analyse (arbre de défaillances, séquences et arbres d'événements), dont il est question dans cette annexe, sont expliquées plus en détails à l'annexe H.

B.1 Éléments d'une EPS

Une EPS de niveau 1 comprend les trois (3) éléments essentiels suivant :

- L'identification des événements qui, si non prévenus, peuvent résulter en une dégradation du cœur et une relâche potentielle de radionucléides.
- Le développement de modèles représentant les événements amenant une dégradation du cœur.
- La quantification des modèles dans l'estimation de la fréquence de dégradation du cœur.

B.1.1 Identification

Le premier élément d'une EPS de niveau 1 est la détermination des événements qui, si non prévenus, peuvent résulter en une dégradation du cœur et une relâche potentielle de radionucléides. Ce processus, généralement référé comme « analyse des séquences d'événements », est typiquement divisé en deux parties : l'identification des événements initiateurs et le développement

des séquences d'accident de dégradation potentielle du cœur associées avec les éléments initiateurs.

Les événements initiateurs généralement modélisés dans une EPS sont les pertes de caloporteur (PERCA) et les pertes des systèmes de services (eau, air, électricité). Des arbres d'événement sont développés pour chacun de ces événements initiateurs. Les séquences d'accident comprennent les séquences d'événement (c'est-à-dire, les succès et défaillances des fonctions et systèmes) qui, si elles se produisent, résulteront en une dégradation du cœur. Par conséquent, les événements initiateurs et les séquences d'accident identifient les différents systèmes pour lesquels un modèle mathématique (algèbre booléenne) est requis.

B.1.2 Développement des modèles

Les modèles de la centrale sont développés dans le second élément d'une EPS de niveau 1. Ces modèles représentent les différents chemins de défaillance associés à chaque système dans la détermination de leur indisponibilité et fiabilité.

Deux types différents d'arbre de défaillance sont généralement utilisés pour modéliser la performance potentielle d'un système. Le concept de « grand arbre de défaillance » implique le développement d'un seul arbre de défaillance qui modélise chacune des différentes configurations de défaillance d'un système. Des événements spéciaux, appelés « house events » sont modélisés dans l'arbre de défaillance pour activer chacune des configurations. Le concept d'« arbre de défaillance par configuration » implique le développement d'arbres de défaillance séparés pour chacune des configurations différentes de défaillance.

B.1.3 Estimation de la fréquence de dégradation du coeur

Le troisième élément d'une EPS de niveau 1 estime la fréquence de dégradation du cœur et son incertitude statistique. Cette estimation est exécutée en quantifiant :

- les probabilités de défaillance et les indisponibilités des différents structures, systèmes, et composants;
- les fréquences des événements initiateurs;
- et les probabilités d'erreurs humaines associées avec les différentes actions des opérateurs.

La fréquence de chaque séquence d'accident est ensuite calculée en intégrant les probabilités de défaillance des structures, systèmes, et composants (SSC) et les probabilités d'erreurs humaines (PEH) avec les fréquences d'événements initiateurs dans les modèles booléens. Ces fréquences sont additionnées pour obtenir une fréquence générale moyenne de dégradation du cœur. Cette valeur représente la fréquence moyenne annuelle de dégradation du cœur associée avec la conception, l'exploitation et la maintenance de la centrale analysée.

Une partie de l'estimation de la fréquence de dégradation du cœur est la quantification de son incertitude statistique. Cette incertitude reflète le manque de précision dans les données et le manque de compréhension détaillée des phénomènes physiques modélisés.

B.2 Étendue et niveau de détail de l'EPS

L'EPS examine les conséquences des événements qui impliquent un arrêt d'urgence du réacteur ou un arrêt forcé avec la nécessité d'un enlèvement subséquent de la chaleur du cœur. Ces événements peuvent se produire à différents états d'exploitation, de la pleine puissance aux différents modes d'arrêts.

B.2.1 Analyse des événements initiateurs

Les événements initiateurs sont généralement incorporés dans les EPS courantes par un seul événement qui représente la fréquence moyenne annuelle de cet événement. La majorité des fréquences sont développées à partir des données d'exploitation. Malgré qu'un modèle logique expliquant en détail les différents systèmes et composants contribuant à la fréquence d'occurrence puisse être développé et quantifié, ils n'est généralement pas incorporé dans le modèle d'EPS.

Rappelons que les événements initiateurs généralement modélisés dans une EPS courante sont les pertes de caloporteur (PERCA) et les pertes des systèmes de services (eau, air, électricité).

B.2.2 Analyse des arbres d'événement (séquences d'accident)

Les séquences d'accident sont généralement présentées au niveau de détail fonctionnel ou systémique. Les fonctions ou systèmes sélectionnés sont dépendants de l'étendue de l'analyse des critères de succès. Les critères de succès déterminent les fonctions ou systèmes, ou combinaisons de fonctions ou systèmes, lesquels si opérant dans des conditions définies, maintiendront le cœur dans une condition sécuritaire (c'est-à-dire préviendront l'occurrence de dégradation du cœur).

Inversement, les critères de succès identifient les combinaisons de fonctions ou systèmes, qui s'ils n'opèrent pas dans des conditions spécifiques, résulteront en une condition non sécuritaire. Généralement, dans la plupart des EPS, le cœur est assumé être en condition sécuritaire quand les conséquences de relâche de radionucléides en provenance du combustible endommagé est négligeable.

Les besoins d'un état défini de dégradation du cœur sont déterminés à partir des analyses d'ingénierie du comportement du cœur et de la centrale sous différentes conditions d'accidents. Les critères de succès définis et les analyses d'ingénierie déterminent les fonctions et systèmes qui sont identifiés comme capable de prévenir une dégradation du cœur. Cependant, il existe plusieurs systèmes n'ayant pas de relations avec les fonctions désirées ou qui ne rencontrent pas nécessairement les critères de succès. Ces systèmes ne sont pas évalués ni modélisés dans l'EPS.

B.2.3 Analyse des systèmes

Les arbres de défaillance construits pour les différents systèmes peuvent être développés selon les différents niveaux de résolution suivants :

- Niveau du composant :

  Les composants individuels compris dans la fonction ou système et les modes de défaillances possibles de chaque composant sont explicitement représentés dans le modèle d'arbre de défaillance comme événements de base uniques. Il doit cependant être noté que tous les composants de systèmes et les modes de défaillance ne sont pas modélisés. Généralement, seulement les composants dont le mode de défaillance résulte en la perte d'une fonction du système avec une probabilité relativement significative ($\geq 10^{-6}$) sont modélisés.

  Un composant dans une EPS est généralement la pièce principale d'un équipement qui est essentielle à la fonction du système comme des pompes, valves, échangeurs de chaleur, générateurs diesel, etc. Les pièces qui sont essentielles à la fonction du composant (ex.: disque de valve) ne sont pas explicitement modélisées comme événements de base uniques mais sont inclues dans les limites du composant (ex.: valve).

- Niveau mode de défaillance :

  Seulement les modes de défaillance de chaque système sont modélisés comme événements de base uniques (perte d'alimentation électrique, maintenance préventive, etc.).

- Niveau du système :

  La fonction ou système est représenté par un seul événement. Ce niveau de résolution peut être référé aux modèles de "boîte noire".

B.2.4 Analyse des données

L'analyse des données implique la quantification des différentes probabilités des modes de défaillances associées avec les SSC modélisés dans les arbres de défaillance. Les modes de défaillance généralement considérés dans les EPS courantes sont :

- Défaillance matérielle :

  Ce mode de défaillance examine les défaillances, selon le nombre de demande et le temps de service, associées avec les défaillances aléatoires du matériel.

- Défaillance d'essais et de maintenance :

  Ce mode de défaillance examine le potentiel pour un composant, équipement ou système d'être indisponible lorsque nécessaire parce qu'il est hors service pour un essai ou pour une activité de maintenance.

- Cause commune de défaillance :

  Ce mode de défaillance examine le potentiel pour plusieurs composants de faire défaillance dû à une même cause spécifique comme le remplacement de la même pièce dans plusieurs composants où les pièces de rechange sont défectueuses.

L'analyse des données implique aussi la quantification des fréquences des événements initiateurs. Cette quantification examine les modes de défaillance ci-dessus qui peuvent causer l'occurrence des événements initiateurs.

Les événements identifiés et les modes de défaillances définis dictent les informations requises pour quantifier les taux de défaillance, les indisponibilités et les fréquences des événements initiateurs. Si des informations adéquates de la centrale existent, on pourra donc calculer les taux de défaillance, les indisponibilités et les fréquences des événements initiateurs spécifiques à la centrale. Cependant, si les informations sont inadéquates, des données génériques doivent être utilisées, lesquelles limitent les applications de l'EPS. Il est important que les données reflètent, autant que possible, la performance actuelle de la centrale.

B.2.5 Analyse de la fiabilité humaine

L'estimation des probabilités des événements implique aussi la quantification des performances humaines. Cette tâche est très diversifiée, et une normalisation n'existe pas. Cette tâche, cependant, a la possibilité de changer les séquences d'accident, donc changer les résultats de l'EPS.

Les événements humains comprennent les actions de l'opérateur qui exécutées lors de l'exploitation normale de la centrale peuvent rendre un équipement inopérable sans causer d'événements initiateurs. Ils comprennent aussi les activités de l'opérateur qui sont requises pour obtenir un arrêt sécuritaire de la centrale.

B.2.6 Quantification

La fréquence de dégradation du cœur est généralement basée sur la somme des séquences d'accident dominantes seulement, et non toutes les séquences. Les séquences d'accidents dont la fréquence calculée de dégradation du cœur est moindre que 10^{-7} évé./année sont généralement tronquées ; elles ne sont pas intégrées dans le modèle général d'EPS.

B.2.7 Analyse d'incertitude

Les incertitudes associées avec les valeurs des paramètres sont définies en assignant une distribution de probabilités aux taux de défaillance et indisponibilités des composants, aux fréquences d'événements initiateurs, et aux probabilités d'erreurs humaines. Les incertitudes reliées aux phénomènes physiques sont estimées en assignant des distributions de probabilités aux différentes hypothèses de modélisation. Les données et les distributions de modélisation sont insérées dans la quantification de la fréquence de dégradation du cœur en utilisant généralement les techniques de Monte Carlo.

B.3 Résultats de l'EPS

En plus de la fréquence de dégradation du cœur calculée, il y a de nombreux résultats qui peuvent être quantifiés dans une EPS. Un modèle d'EPS comprend une centaine de séquences d'accident qui peuvent potentiellement résulter en une dégradation du cœur. Les résultats d'une EPS de niveau 1 indiquent les séquences d'accident dominantes qui généralement comprennent 95 % de la fréquence totale de dégradation du cœur et représentent moins d'une douzaine de séquences. Ces séquences dominantes sont les séquences d'accident les plus susceptibles de se produire. Les événements dominants de ces fréquences sont aussi identifiés. Ces événements sont ceux qui sont les plus susceptibles de se produire et de résulter en une dégradation du cœur.

Les résultats probablement les plus importants sont les mesures d'importance. Ces mesures fournissent différents renseignements sur la fréquence de dégradation du cœur en regard de la fiabilité et de l'indisponibilité définies pour les SSC.

Les mesures d'importance généralement vue dans les EPS sont les suivantes :

- Facteur d'augmentation du risque
- Facteur de diminution du risque
- Mesure d'importance de Fussel-Vesely

ANNEXE C

LES PRINCIPALES ÉTAPES DE RÉALISATION D'UNE EPS

Cette annexe présente de façon très générale les principales étapes de réalisation d'une EPS. Pour des informations plus spécifiques, le lecteur est invité à consulter les documents de l'IAEA et la littérature existante.

C.1 Réalisation d'une EPS de niveau 1

La réalisation d'une EPS de niveau 1 implique les six (6) étapes majeures suivantes (IAEA, 1992):

1. Gestion et organisation

   Cette étape comprend les actions et activités nécessaires à la gestion et organisation de l'étude. Elle comprend la définition des objectifs, l'étendue et la gestion de projet de l'EPS, la sélection des méthodes et l'établissement des procédures, la sélection du personnel et l'organisation de l'équipe qui réalisera l'EPS, la formation de cette équipe, la préparation de la cédule du projet, l'estimation et l'obtention des fonds nécessaires, et l'établissement de procédures d'assurance qualité et de revue par les pairs.

2. Identification des sources de relâche radioactive et initiateurs d'accident

   Dans cette étape, les sources potentielles de relâche radioactive à l'environnement sont identifiées, les états potentiels de la centrale sont analysés et déterminés, et les fonctions de sûreté incorporées à la centrale sont identifiées. Les événements initiateurs qui peuvent solliciter ces fonctions ainsi que les systèmes qui les remplissent sont identifiés. Les relations entre les événements initiateurs, les

fonctions de sûreté et les systèmes sont établies et catégorisées. Au cours de cette étape, l'équipe d'analyse devient familière avec la centrale à analyser et les méthodes qui seront utilisées, et elle collecte la majorité des informations requises sur lesquelles se basera l'analyse subséquente.

3. Modélisation des séquences d'accident

   La troisième étape compose avec la construction d'un modèle qui simule l'initiation d'accident et la réponse de la centrale. Ce modèle consiste principalement en la combinaison d'événements (comprenant les événements initiateurs, possiblement quelques externes, les défaillances de systèmes et les erreurs humaines) amenant des conséquences indésirables. Ces combinaisons d'événements sont appelées séquences d'accident et l'objectif de cette étape est de les définir. Des modèles pour une analyse détaillée des défaillances des systèmes et des erreurs humaines seront développés. Une analyse de dépendance qualitative pour l'inclusion de dépendances possibles dans le modèle sera aussi exécutée.

4. Évaluation des données et estimation des paramètres

   Cette étape acquiert et/ou génère toutes les informations nécessaires pour quantifier le modèle construit à la troisième étape. En particulier, les éléments fondamentaux du modèle de la centrale et les paramètres qui ont besoin d'être estimés sont identifiés. Les données nécessaires à la production de ces estimations et leurs incertitudes associées sont colligées et traitées convenablement. Les paramètres pouvant être estimés sont divisés en trois catégories: fréquences des événements initiateurs, indisponibilités des composants et probabilités d'erreurs humaines. Les paramètres nécessaires à la modélisation des dépendances potentielles à travers les différents événements (événements initiateurs, défaillances de systèmes ou erreurs humaines) sont aussi estimés.

5. Quantification des séquences d'événements

   Dans cette étape, le modèle (construit dans la troisième) est quantifié utilisant les

résultats de la quatrième étape. Le résultat de cette étape est l'évaluation de la fréquence des séquences d'accident. Normalement ceci est accompagné par l'évaluation des incertitudes associées. Des études de sensibilité sont faites pour les hypothèses importantes et les importances relatives des différents contributeurs au résultat calculé sont indiquées.

6. Documentation de l'analyse

   Les résultats de l'analyse sont complètement documentés dans chaque étape. Dans cette étape les résultats sont présentés de la façon qui rencontre le mieux les besoins des utilisateurs. Ceci comprend l'interprétation des résultats, en accord avec les objectifs de l'EPS

Le flux général des informations/travaux est présenté à la figure C.1. Il est important de reconnaître que ce flux n'est pas toujours linéaire et qu'il y a plusieurs boucles itératives à travers ces étapes. Les étapes ont été divisées en tâches lesquelles constituent le cadre de travail de réalisation d'une EPS (Figure C.2).

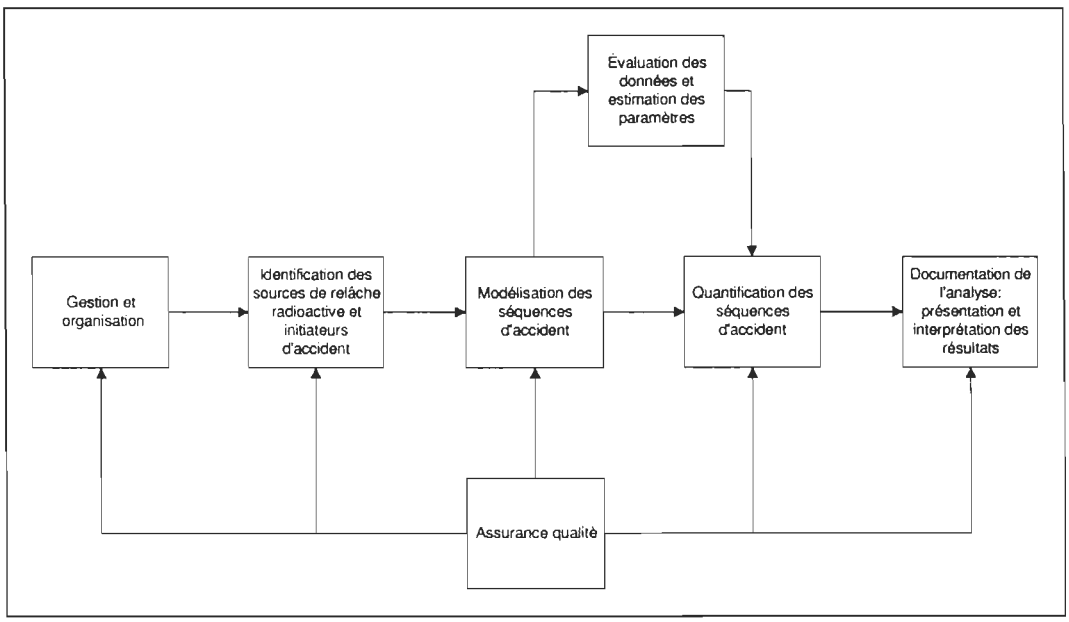

Figure C.1. Principales activités de réalisation d'une EPS de niveau 1
(Source: IAEA,1992)

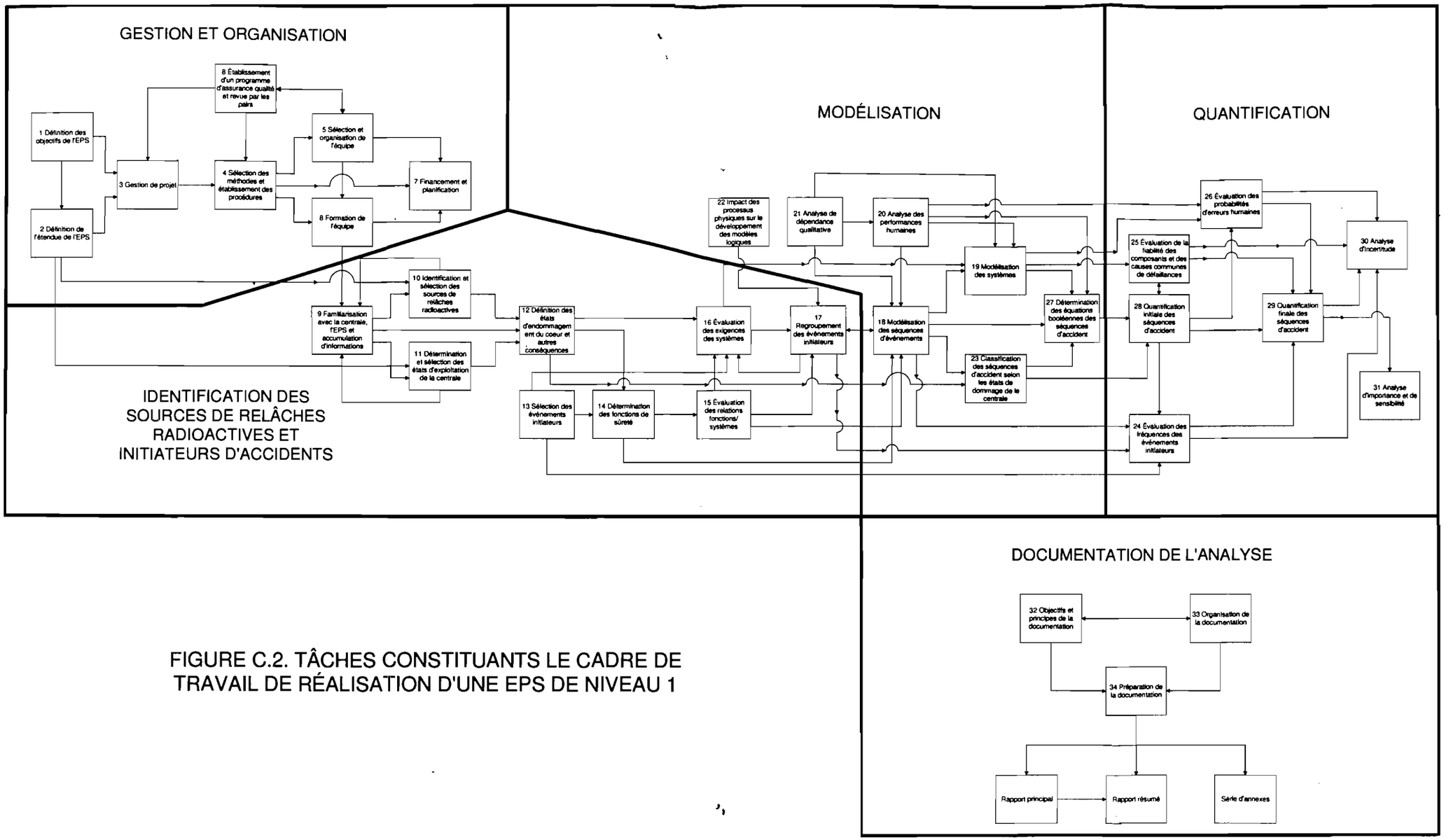

FIGURE C.2. TÂCHES CONSTITUANTS LE CADRE DE TRAVAIL DE RÉALISATION D'UNE EPS DE NIVEAU 1

C.2 Réalisation d'une EPS de niveau 2

La réalisation d'une EPS de niveau 2 implique, elle aussi, six (6) étapes majeures (Figure C.3). Les différentes tâches constituants ces étapes ont aussi été énumérées ci-dessous. (IAEA, 1995)

1. Gestion et organisation

   Les aspects organisationnels présentés dans l'EPS de niveau 1 s'appliquent aussi à l'EPS de niveau 2.

   Tâches: 1. Définition des objectifs de l'EPS de niveau 2.
   2. Définition de l'étendue de l'EPS de niveau 2.
   3. Gestion de projet.
   4. Sélection et organisation de l'équipe.
   5. Établissement d'un programme d'assurance qualité et revue par les pairs.

2. Familiarisation avec la centrale et identification des aspects de conception reliés aux accidents sévères

   Tâches: 6. Familiarisation avec la centrale.
   7.Identification des aspects de la conception reliés aux accidents sévères.

3. Interface avec l'EPS de niveau 1: Regroupement des séquences

   L'EPS de niveau 1 identifie un très grand nombre de séquences d'accident lesquelles conduisent à un dommage du coeur potentiel. Il n'est pas pratique ou nécessaire de traiter chacune d'elles individuellement lorsqu'on évalue la progression de l'accident, la réponse du confinement et la relâche de produits de fission. Les séquences sont groupées dans des états de dommage de centrale de sorte que tous les accidents aboutissant a un état de dommage de centrale donné puissent être traités en groupe.

   Tâches: 8.États de dommage de centrale pour les initiateurs internes en puissance
   9. États de dommage de centrale de l'EPS de niveau 1 existante.

10. Extension aux autres initiateurs.
11. Extension aux autres états de puissance.

4. Progression d'accident et analyse du confinement

Tâches: 12. Performance du confinement.
13. Analyse de la progression d'accidents sévères.
14. Développement et quantification des arbres d'événements, de la progression d'accident et du confinement.
15. Regroupement des états finaux des arbres d'événements dans des catégories de relâche.
16. Traitement de l'incertitude dans la progression d'accident.
17. Résumé et interprétation des résultats de la performance du confinement.

5. Sources d'accidents sévères

Plusieurs caractéristiques et phénomènes des systèmes de la centrale et du confinement ont été démontrés comme influençant l'amplitude et les caractéristiques des sources pour les accidents sévères. En général, il est recommandé de faire plusieurs calculs sur les sources de la centrale avec un code informatique approprié.

Tâches: 18. Regroupement des produits de fission.
19. Relâche de produits de fission provenant du combustible pendant la phase "dans les tubes".
20. Rétention des produits de fission à l'intérieur du système caloporteur.
21. Relâche des produits de fission pendant la phase "hors-tube".
22. Rétention des produits de fission à l'intérieur du confinement.
23. Traitement des incertitudes dans les sources estimées.
24. Présentation et interprétation des sources estimées.

6. Documentation de l'analyse

Les détails de l'analyse d'une EPS de niveau 2 sont rapportés de façon à présenter les informations sur les méthodes utilisées, le processus d'EPS, et les conclusions selon un développement logique. Le rapport lui-même doit être soumis à la revue des pairs et procurer une structure favorisant les liens avec le matériel (plus détaillé) de support.

Tâches: 25. Objectifs et principes de la documentation.

26. Organisation de la documentation.

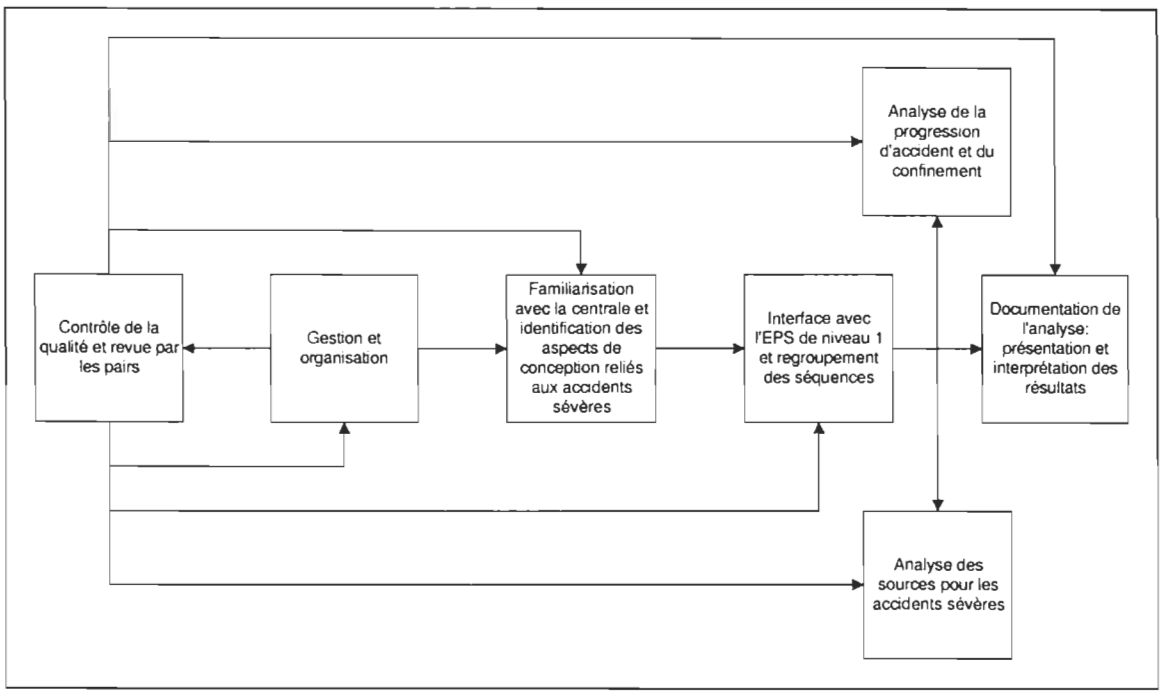

Figure C.3. Principales activités de réalisation d'une EPS de niveau 2

(Source: IAEA, 1995)

C.3 Réalisation d'une EPS de niveau 3

Pour ce qui est de l'EPS de niveau 3, nous nous contentons seulement d'énumérer les différentes tâches nécessaires à sa réalisation dans la figure suivante (Figure C.4).

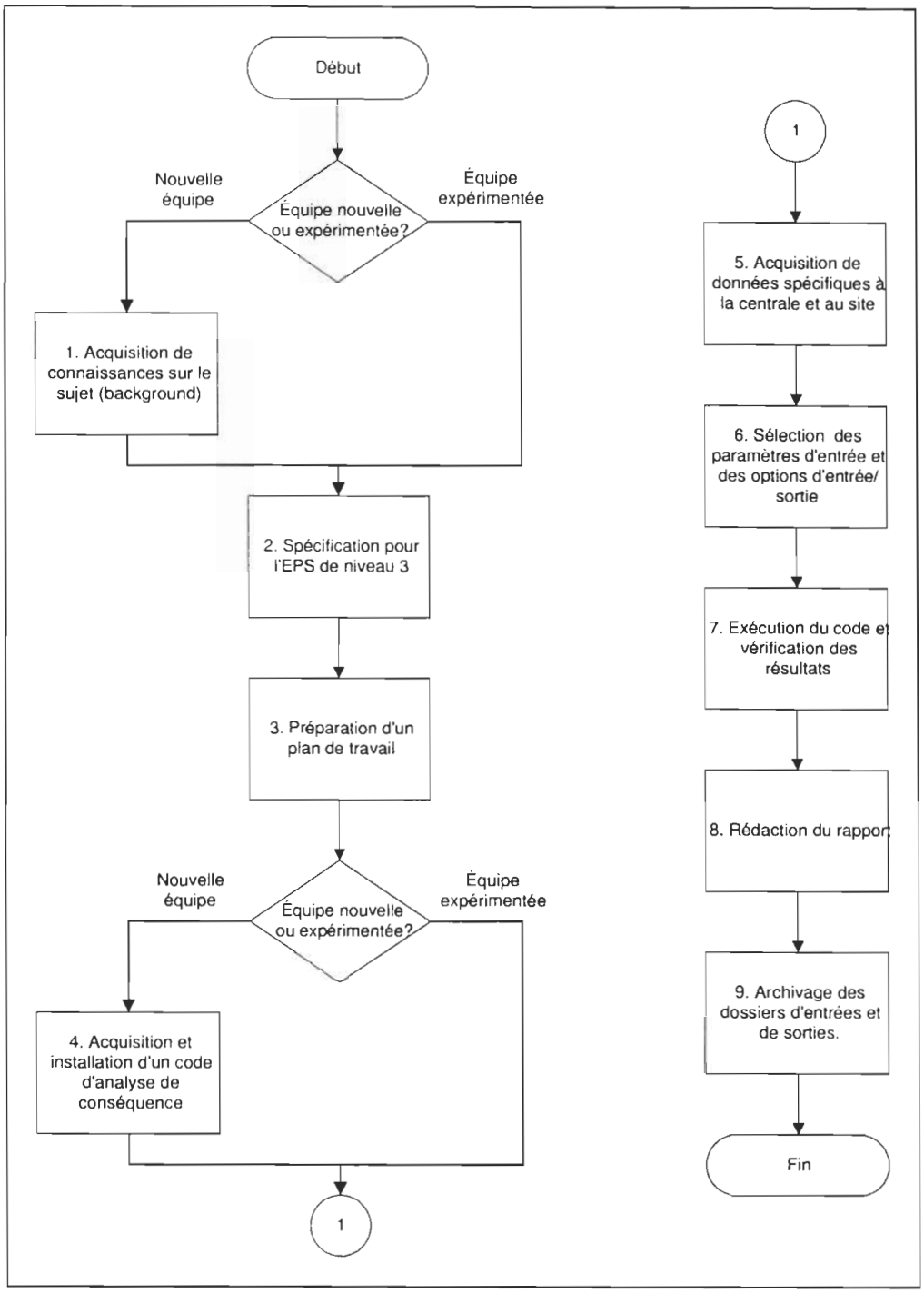

Figure C.4. Principales activités de réalisation d'une EPS de niveau 3.

(Source: IAEA, 1996)

ANNEXE D

LIMITES D'UNE EPS

L'utilisation des résulats d'une EPS comme aide à la décision doit absolument tenir compte des limites de celle-ci. Cette annexe a pour but d'identifier et d'expliquer ces limites.

D.1 Introduction

L'utilisation d'une EPS présente des limites dont la plupart sont intrinsèques à la méthodologie utilisée. En effet, celle-ci est tributaire (Birkhofer, 1991):

- de la conception déterministe,
- d'incertitudes dans les données et les modèles,
- de difficultés à analyser correctement certaines questions et,
- des conclusions sélectives de l'équipe qui réalise l'EPS.

D.2 Tributaire de la conception

Une limite fondamentale d'une EPS tient au fait que ses possibilités dépendent du niveau de défense en profondeur résultant de la conception déterministe de la centrale. Une prévision fiable des probabilités de défaillance exige des données tirées de l'expérience. De très faibles probabilités d'accident ne peuvent être élaborées avec une précision raisonnable que si elles résultent de combinaisons de probabilités conditionnelles de défaillances plus importantes, lesquelles peuvent être tirées de l'expérience. Cela exige l'indépendance de ces probabilités conditionnelles de défaillances par des niveaux de protection indépendants, à l'intérieur d'une bonne réalisation de défense en profondeur. Une conception qui permet à des événements

isolés ou à des modes de défaillances particuliers (par exemple, erreur humaine) de déjouer simultanément tous les niveaux de protection ne fournit pas cette base nécessaire à une étude probabiliste.

Il est en outre des aspects difficiles à estimer quantitativement. Citons, par exemple, les influences de l'organisation de la centrale et la culture en matière de sûreté, ainsi que certains aspects décrit ci-après. C'est une tâche essentielle de la conception déterministe de la centrale que de limiter et de réduire l'influence de ces aspects.

D.3 Incertitudes dans la création des modèles

En raison des limites dans la précision des données, les résultats d'une EPS sont, dans une certaine mesure, incertains. La méthodologie probabiliste permet de quantifier les incertitudes. On peut propager l'incertitude des données aux résultats, puis y ajouter un avis d'expert afin d'évaluer l'influence des incertitudes introduites par la modélisation. Ces incertitudes sont représentées par des distributions de probabilités des résultats calculés.

Pour les EPS de niveau 1 portant sur des conceptions de réacteur éprouvées, les incertitudes (définies pour 90% de l'intervalle de confiance) couvrent environ un ordre de grandeur. Les résultats disponibles montrent que l'incertitude du niveau 2 s'étend sur plusieurs ordres de grandeur en raison des difficultés de modéliser la tenue et les défaillances du confinement. Dans les analyses de niveau 3, d'autres incertitudes viennent s'ajouter avec l'inclusion de relations dose-effet, en particulier pour l'incidence d'une irradiation à très faible dose sur la santé de populations importantes.

D.4 Limite de champ d'application

Une EPS prend en compte un nombre limité de défaillances et de séquences. Certaines peuvent être négligées parce qu'estimées peu importantes (elles peuvent le

devenir quand l'importance de d'autres séquences se trouve réduite suite à l'amélioration de la technologie), ou pour la raison qu'on ne peut pas facilement les inclure dans la structure des modèles d'EPS. Par exemple, le champ des analyses de séquences accidentelles se limite généralement aux défaillances d'éléments d'un type donné et aux erreurs d'un opérateur dans la bonne conduite des tâches décrites. La prise en compte des événements initiateurs est également limitée dans son étude.

Certaines limites spécifiques du champ d'application d'une EPS sont décrites plus en détail ci-après.

D.5 Facteur humain

Il est difficile de créer un modèle du comportement humain. L'influence du facteur humain compte parmi les questions les plus difficiles à quantifier dans une EPS. Les conceptions, dont la sûreté dépend pour une grande part, de l'intervention humaine sont particulièrement sensibles à cet égard.

Pour les conceptions éprouvées, l'influence de l'erreur humaine a été grandement réduite par l'automatisation et par l'amélioration de l'interface homme-machine. Toutefois, bien qu'elle ne cesse de s'accroître, la fiabilité d'ensemble de la technologie des centrales n'empêche pas l'erreur humaine de constituer un facteur de risque important.

Un problème particulier réside dans l'estimation des erreurs commises par l'opérateur. Ces erreurs sont des actes intentionnels que les opérateurs effectuent en contradiction avec les procédures existantes et qui peuvent tenir du caractère imprécis de ces dernières, à une instrumentation pouvant induire en erreur, ou simplement des omissions de la part des opérateurs. L'inclusion de telles erreurs dans une EPS est extrêmement difficile en raison du nombre pour ainsi dire illimité d'actions possibles qu'il faudrait envisager.

Un autre aspect difficile à estimer concerne le sabotage. Ce dernier diffère de l'erreur commise par un opérateur en ce sens qu'il s'agit d'un acte délibéré pour endommager une installation. Un sabotage n'est pas un accident et on le considère généralement comme intrinsèquement différent des événements figurant normalement dans une EPS. Un sabotage dépend pour une grande part de facteurs sociaux et politiques complexes. Il ne doit pas être traité dans une EPS mais par une approche spécifique basée sur le concept de défense en profondeur.

D.6 Défaillance par mode commun

Étant donné la haute qualité des équipements des centrales nucléaires, il est extrêmement rare de constater des défaillances de mode commun dans les systèmes de sûreté redondants. De telles défaillances peuvent avoir pourtant une contribution prépondérante dans le taux de défaillance du système dans un système fortement redondant.

La difficulté de prédire les probabilités de défaillances de mode commun peut entraîner une surestimation de leur contribution. Cependant, en raison de la grande incertitude dans la prédiction de tels effets, il est nécessaire que les centrales soient protégées par conception contre les défaillances de mode commun.

D.7 Événements de faible probabilité

En général, les événements de très faible probabilité sont négligés en raison du jugement que l'on porte sur leur contribution au risque. À cet égard, il est d'usage, et cela ne semble n'avoir aucune influence significative sur le résultat d'une analyse, de ne pas tenir compte d'événements dont les probabilités d'occurrence sont de deux ou trois ordres de grandeur inférieurs aux probabilités globales du résultat défavorable considéré. Étant donné que la plupart des EPS prévoient une probabilité de dégradation du coeur entre 10^{-5} et 10^{-4} par réacteur par an, un seuil correspondant à une probabilité de 10^{-7}/an semble appropriée à cet égard.

Indépendamment du seuil de probabilité, il faut envisager certains événements dont les probabilités sont inférieures au seuil, si ces événements peuvent amener des changements radicaux dans les conséquences. Il convient toutefois de traiter ces événements séparément.

ANNEXE E

UN PROGRAMME D'EPS VIVANTE

Cette annexe décrit ce qu'est un programme d'EPS vivante ainsi que ces diverses application. (SKI, 1994)

E.1 EPS vivante dans la gestion de la sûreté

La première étape d'un programme typique d'EPS appelée EPS de base est l'exécution d'une étude de niveau 1 concentrée sur les événements internes et les séquences d'accidents amenant une dégradation du coeur. L'EPS de base est un modèle statique. Elle est créée pour l'évaluation de la probabilité moyenne dans le temps de dégradation du coeur.

Afin d'augmenter la disponibilité de l'EPS de base pour la gestion opérationnelle de la sûreté, le modèle ainsi que le programme entier d'EPS doivent être développés pour devenir un outil plus dynamique. On appelle programme EPS vivante le processus de mise à jour du modèle EPS pour représenter la configuration actuelle ou planifiée et pour utiliser le modèle pour évaluer les changements directs dans la configuration.

La première version d'une EPS spécifique à une centrale n'est habituellement pas adéquate pour toutes les possibilités envisagées d'une EPS. En effet, le modèle EPS de base et les données ne supportent pas complètement une évaluation flexible du niveau de sûreté de la centrale. Peu de codes informatiques sont convivials et assez rapides, et il y a peu de procédures d'utilisation et de maintenance d'EPS pour la

gestion quotidienne de la sûreté. Une EPS n'est vivante que lorsqu'elle a été complètement intégrée dans la gestion opérationnelle de la sûreté.

Une partie importante du concept d'EPS vivante est de définir comment les résultats de l'évaluation seront interprétés dans la prise de décision reliée à la sûreté. Dans ce contexte, nous avons à définir les mesures de risque utilisées pour présenter les résultats de ces applications. L'aspect fondamental des résultats d'une EPS vivante est qu'ils expriment le risque de dommage au coeur à un certain temps et état donnés de la centrale. Cette structure change dans les différents modes d'exploitation ainsi que les probabilités d'événement de base varient suivant la connaissance des états des composants. Un modèle EPS doit être capable de suivre ces changements.

E.2 Buts et objectifs

Le concept d'EPS vivante implique une description du comment le modèle originel d'EPS peut être utilisé d'une manière plus dynamique, continuellement mis à jour selon les états des systèmes reliés à la sûreté de la centrale. Les principaux buts de développement d'une EPS vivante sont:

- procurer un outil d'évaluation du risque pour l'analyse des effets sur la sûreté des changements dans la conception de la centrale, les procédures et spécifications techniques,

- supporter la planification de la maintenance et la gestion d'exploitation en procurant un outil de recherche des stratégies optimales d'exploitation, de maintenance et d'essais du point de vue de la sûreté.

Un programme d'EPS vivante deviendra, suivant ce concept, un système journalier de gestion de la sûreté basé sur une EPS spécifique à la centrale et supportant un système d'information.

E.3 Envergure et utilisation

Les applications d'une EPS vivante peuvent être divisées en trois catégories (voir figure E.1):

1. évaluation du risque
2. surveillance du risque
3. suivi du risque

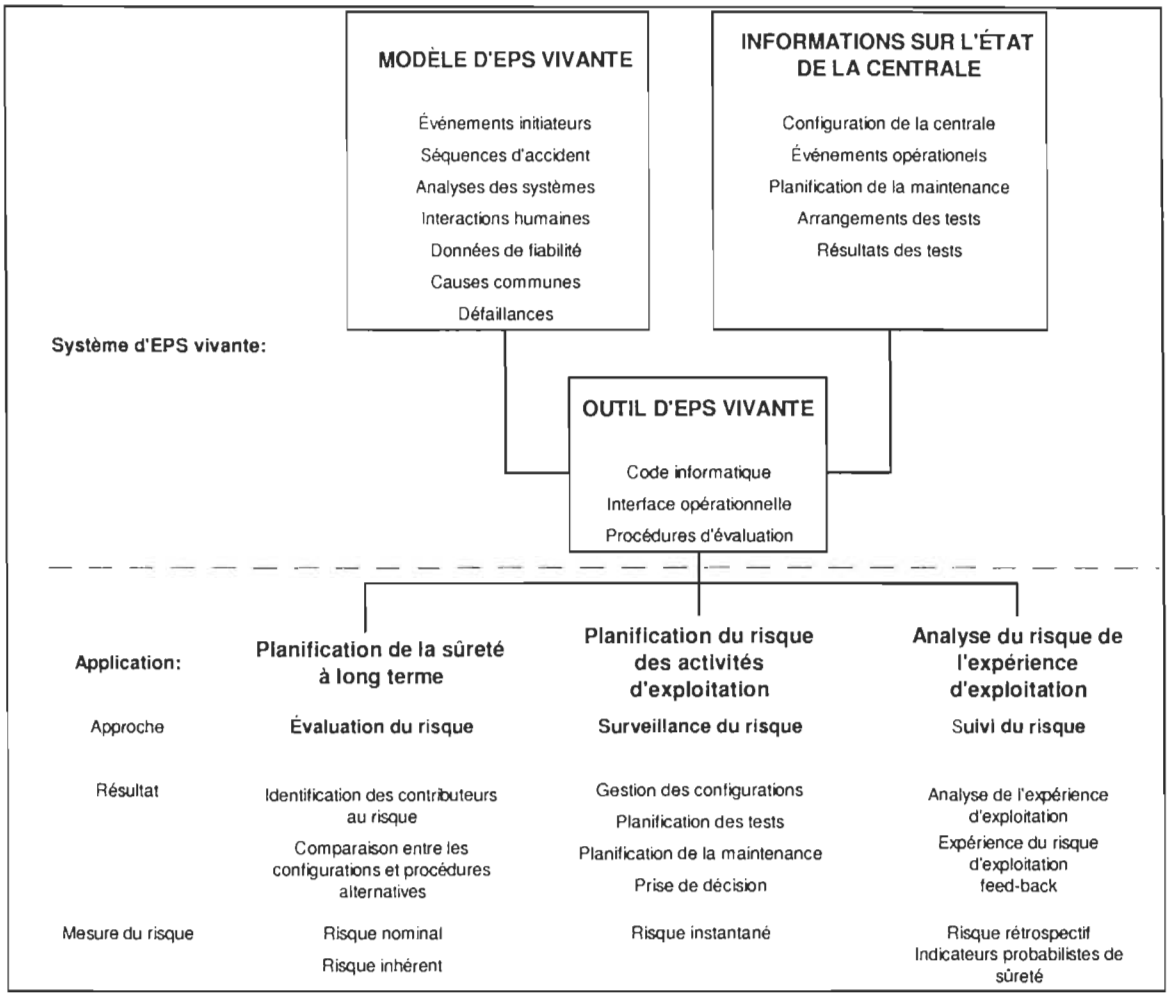

Figure E.1. Concept d'EPS vivante (Source: SKI, 1994)

E.3.1 Évaluation du risque

L'évaluation du risque se rapproche beaucoup de l'idée des EPS de base, soit l'évaluation du risque moyen causé par l'exploitation de la centrale. L'objectif premier est de vérifier le niveau moyen de risque de la centrale et d'en identifier les contributeurs majeurs. Les résultats de cette évaluation sont applicables à la planification à long terme afin d'améliorer les faiblesse identifiées de la centrale.

La planification à long terme inclut les évaluations statiques et les comparaisons des effets sur le risque des changements dans la conception de la centrale, la maintenance, les essais, les procédures et les spécifications techniques. Le but de ces études est d'optimiser l'exploitation de la centrale, la maintenance et la conception tout en respectant la minimisation du risque et la flexibilité opérationnelle.

E.3.2 Surveillance du risque

L'idée de la surveillance du risque est de calculer le risque instantané durant l'exploitation de la centrale. Elle diffère de l'évaluation du risque, dans laquelle une configuration moyenne de la centrale est utilisée, par l'utilisation de la configuration observée au moment présent.

La surveillance du risque peut être exécutée de façon "on-line", "off-line" ou pour la planification. La surveillance "on-line" du risque est effectuée par les opérateurs qui possèdent les informations mises à jour de l'état de la centrale. La surveillance "off-line" est exécutée en se basant sur l'expérience opérationnelle. Dans la planification, des configurations hypothétiques sont évaluées au préalable pour identifier les configurations dangereuses pour la sûreté.

La surveillance du risque signifie que le personnel de planification de la maintenance ou d'exploitation utilise une EPS vivante comme outil de consultation pour compléter les spécifications techniques. Ceci est mené à bonne fin en contrôlant le niveau de risque des décisions et alternatives opérationnelles et en identifiant les moyens de contrôle de hautes variations du risque. Les résultats de la surveillance du risque sont applicables dans la planification à court terme afin de sélectionner les stratégies d'exploitation ou de maintenance dans une situation donnée ou planifiée.

Seulement quelques exemples de surveillance du risque appliqués de façon "on-line" existent.

E.3.3 Le suivi du risque

L'idée du suivi du risque est de calculer le risque rétrospectif c'est-à-dire l'évaluation du risque expérimenté durant l'exploitation de la centrale. Un objectif du suivi du risque est d'évaluer la sévérité des incidents du point de vue de la sûreté. Un autre objectif est la recherche d'améliorations convenables et efficaces dans l'exécution technique et organisationnelle de la centrale. L'analyse des expériences soutient les vérifications ainsi que l'achèvement des modèles EPS et des données.

Le suivi du risque est considéré comme le premier pas dans le développement d'un système d'EPS vivante car les exigences d'un modèle d'EPS vivante sont semblables aux applications de la surveillance du risque

E.4 Applications de l'EPS vivante dans la gestion de la sûreté

Les applications d'une EPS vivante peuvent être divisées en domaines spécifiques pour mieux refléter les utilisations des résultats. Le tableau E-1 présente ces domaines d'application et leurs usagers. En plus de ces usagers, les ingénieurs fiabilistes et les développeurs de codes informatiques sont toujours nécessaires au

maintien du système. Une EPS vivante peut aussi servir d'outil de communication entre les autorités et les exploitants.

Tableau E-1

Domaines d'applications de l'EPS vivante et leurs utilisateurs

Applications	**Utilisateurs**				
	Gestion de la sûreté	Gestion de l'exploitation	Planification de la maintenance	Conception	Autorité
Planification du risque à long terme					
Évaluation des objectifs de sûreté	X			X	X
Identification des contributeurs de risque	X			X	X
Comparaisons des conceptions et procédures alternatives	X	X		X	X
Optimisation des conditions limites d'exploitation	X	X			X
Formation des opérateurs		X			
Planification de la gestion des accidents	X	X		X	X
Planification du risque des activités opérationnelles					
Planification de la maintenance préventive			X		
Planification de la maintenance corrective			X		
Planification des essais et de leurs combinaisons	X	X			
Gestion des incidents	X	X	X		
Exemption aux spécifications techniques	X	X			X
Analyse du risque de l'expérience d'exploitation					
Indicateurs probabilistes et rétrospective du suivi du risque	X	X			X
Analyse des incidents	X	X			X
Études des événements précurseurs	X	X			X
Analyse du vieillissement		X	X		X

(Source: SKI, 1994)

E.4.1 Planification du risque à long terme

Évaluation des objectifs de sûreté

Dans l'évaluation des objectifs de sûreté les résultats sont utilisés de manière absolue. La fréquence nominale de dégradation du coeur est comparée avec un critère national ou international. Le critère est considéré plus comme une cible car les résultats d'une EPS sont sensibles à l'approche utilisée dans l'évaluation du risque. Spécifiquement, le niveau de détails de l'EPS affecte grandement les résultats.

Identification des contributeurs de risque

L'identification des contributeurs de risque permet d'identifier et de fixer les priorités des mesures d'amélioration de la sûreté. Ces résultats sont utilisés de façon relative. Les mesures d'importance du risque des événements de base sont les premiers résultats à utiliser dans l'identification des contributeurs de risque.

Comparaisons des conceptions et procédures alternatives

Quand des changements dans la conception ou les procédures ont une influence sur l'état de sûreté, l'EPS vivante procure un support pour la comparaison des alternatives. Les incertitudes et les aspects économiques doivent aussi être pris en considération.

Optimisation des conditions limites d'exploitation

Les limites d'exploitation et les conditions données par les spécifications techniques sont analysées en évaluant les effets sur le risque des exigences des alternatives. La planification de stratégies est aussi reliée à cette activité. Le but est de balancer les exigences en respectant la flexibilité opérationnelle et l'économie de la centrale. Les situations de haut risque permises par les spécifications techniques sont identifiées et remplacées par d'autres donnant un risque minimum, ainsi que les exigences trop strictes sont substituées par d'autres plus flexibles.

Formation des opérateurs

Les résultats de l'identification des contributeurs de risque peuvent être utilisés dans la planification des séquences d'accidents devant être mis en emphase dans la formation des opérateurs. Vice versa, la formation des opérateurs peut être utilisés pour vérifier le réalisme des modèles d'interactions humaines considérés dans les séquences d'accidents.

Planification de la gestion des accidents

Généralement, les contributeurs de risque identifiés, les séquences d'accidents dominantes, les chemins de succès et de rétablissement, ainsi que les états finals peuvent supporter la planification du programme de gestion des accidents.

E.4.2 Planification du risque des activités opérationnelles

Planification de la maintenance préventive

Le département de maintenance évalue les impacts sur le risque du programme de maintenance préventive. L'isolation de systèmes ou composants importants à la sûreté augmente temporairement le niveau de risque. La durée des travaux de maintenance et la combinaison des systèmes isolés ou indisponibles sont contrôlés. Les facteurs d'augmentation du risque, les marges de sûreté et les marges de dégradation de la sûreté indiquent les effets des actions de maintenance cédulées.

Planification de la maintenance corrective

Au contraire des arrêts dus à la maintenance préventive, les arrêts dus à la maintenance corrective sont aléatoires. En se basant sur l'expérience, la fréquence de tels événements peut être prédites et, subséquemment, on peut contrôler leur contribution à la durée de vie de l'équipement en ajustant son temps admissible de mise hors service.

Planification des essais et de leurs combinaisons

La surveillance du risque produit une courbe de la fréquence instantanée laquelle suit les changements dans la configuration de la centrale. Dû au probabilités dépendantes du temps des défaillances cachées ou des systèmes de sûreté en réserve, la courbe du risque a une forme en dents de scie. Les essais des composants ou systèmes en réserve diminuent ou augmentent la fréquence instantanée de risque parce que certaines défaillances cachées peuvent être détectées lors des essais. Une indisponibilité évidente, comme la maintenance préventive d'un système, d'un autre côté, augmente immédiatement la fréquence de risque.

La gestion de l'exploitation peut de cette façon analyser les risques et bénéfices des différentes stratégies d'essais. Les essais doivent être planifiés de façon à ce que les défaillances considérées soit détectées mais que l'introduction de modes de défaillance additionnels soit évitée. L'effet des intervalles d'essais et de l'échelonnage possible de certains essais redondants peut être évalué à partir d'un point de vue de fiabilité par des modèles de défaillances de composant dépendant du temps.

Gestion des incidents

Le but de la surveillance "on-line" du risque est d'évaluer la fréquence instantanée du risque, ou la probabilité de dommage au coeur durant un court intervalle de temps donné, selon les informations sur la configuration de la centrale. La gestion des incidents négocie avec des situations de défaillance à la centrale où des décisions rapides sont nécessaires. La sévérité des incidents est contrôlée par la surveillance "on-line". Les résultats fournissent un support dans la prise de décision à court terme. Les actions de maintenance peuvent être priorisées de façon à ce que les systèmes les plus critiques soit réparés en premier. L'importance des chemins de succès, c'est-à-dire les facteurs de diminution du risque, peuvent être utilisés pour classer ces actions.

Exemption aux spécifications techniques

Une exemption aux spécification techniques a habituellement une influence sur la sûreté de la centrale. Le risque causé par l'exemption est comparé avec les risques d'autres alternatives. Cette application est similaire au contrôle des configurations et à l'optimisation des temps de mise hors service admissibles.

E.4.3 Analyse du risque de l'expérience d'exploitation

Indicateurs probabilistes et rétrospective du suivi du risque

Les résultats du suivi du risque forment une courbe historique de la fréquence du risque, laquelle peut générer des indications de sûreté probabilistes. Les principaux indicateurs sont:

- Les sommets de la courbe de fréquence instantanée
- Les probabilités de dégradation du coeur lors des sommets
- La fréquence moyenne durant la période observée

Les résultats peuvent être utilisés pour identifier les situations possibles de haut risque et classer les événements survenus selon le point de vue de la sûreté et ainsi obtenir du feed-back sur l'identification des contributeurs de risque et sur la vérification du modèle EPS.

Les résultats peuvent servir de données pour des applications plus avancées de suivi du risque et pour calculer le risque rétrospectif. En plus de l'analyse de l'expérience opérationnelle dans la surveillance "off-line" du risque, le suivi du risque rétrospectif considère les événements cachés aussi précisément que possible étant donné les informations disponibles. Les combinaisons de défaillances exceptionnelles, les dépendances entre les défaillances, les réparations, les modes de maintenance ou d'exploitation peuvent être identifiés.

Analyse des incidents

Les événements importants pour la sûreté sont analysés aussi profondément que nécessaire afin d'identifier les causes (racines) des événements et évaluer leur sévérité.

Études des événements précurseurs (évaluation d'événements)

Il y a deux types d'événements pouvant être regardés comme précurseurs:

- les événements déclencheurs possibles suivi d'une défaillance d'un système de sûreté
- l'indisponibilité d'un système de sûreté

L'évaluation d'événements identifie les événements significatifs à partir d'un grand nombre de données d'exploitation. La sévérité est évaluée en calculant la probabilité conditionnelle d'un accident étant donné un certain événement. Les études de séquences d'accidents d'événements précurseurs fournissent deux types de résultats:

- fréquence générique d'événement précurseur
- marge de sûreté durant des événements individuels

Analyse du vieillissement

Les analyses du vieillissement ont pour but d'identifier l'effet du vieillissement des systèmes ou composants. Du point de vue de la fiabilité, les indications d'incidents prochains et de changements dans la fréquence de défaillance sont surveillées de sorte que la durée de vie planifiée de la centrale puisse être atteinte, et si possible, prolongée. Les composants vieillissant peuvent être classés selon leur criticité pour la sûreté de la centrale. La planification des programmes de maintenance et d'essais doit prendre en compte les effets du vieillissement.

ANNEXE F

MODÈLE D'EPS VIVANTE

Cette annexe présente les caractéristiques nécessaires pour qu'un modèle d'EPS vivante soit capable de répondre aux diverses applications qui lui sont demandées. Un modèle d'EPS vivante doit être assez flexible pour représenter les changements dans les conditions des systèmes de sûreté de la centrale. Le modèle doit traiter les dépendances du au temps de façon plus complète qu'un modèle de base. Le réalisme des modèles et des données est aussi très important. (SKI, 1994)

Cette annexe présente aussi les limites liés au modèle et à son utilisation.

F.1 Caractéristiques du modèle d'EPS vivante

Représentation de l'état de sûreté de la centrale

L'état de sûreté de la centrale dépend des conditions des systèmes et composants. Le modèle doit refléter notre connaissance des conditions dans lesquelles chaque système se trouve et comment cela affecte le niveau de risque de la centrale

Un modèle EPS peut être considéré comme un arbre de défaillance avec "dégradation du coeur" comme événement indésirable. L'événement indésirable est causé par les événements déclencheurs et les défaillances des systèmes de sûreté c'est-à-dire la réponse de la centrale.

Les événements de base peuvent être divisés en "évident" et "caché" (Tableau F-1). Les événements évidents sont ceux que l'observateur sait avec certitude être vrai ou non. Les autres demeurent cachés.

Tableau F-1

Classification des événements de base d'un modèle d'EPS

Type d'événement de base	Observation
Composant indisponible pour maintenance	Évident
Composant indisponible pour réparation	Évident
Défaillance d'un composant en réserve	Caché
Défaillance en fonction du temps ou des demandes	Caché
Erreur lors de test et/ou maintenance	Caché
Erreur humaine dans la réponse d'accident	Caché

(Source: SKI, 1994)

Modélisation des systèmes et composants

Du point de vue de la surveillance et du suivi du risque, la modélisation des événements de base la plus intéressante est celle reliée aux défaillances des composants en relève testés périodiquement. Le modèle doit tenir compte que certaines défaillances peuvent ne pas être détectées durant l'essai et causer une défaillance non voulue lors d'une demande réelle. Un modèle général, couvrant toutes les combinaisons des modes de défaillance dépendants et indépendants du temps, les possibilités de détection selon les modes, etc. est difficile à créer, et encore plus difficile à appliquer. Le tableau F-2 présente les formules utilisées pour quantifier les composants en réserve.

Tableau F-2

Résumé des formules de quantification des composants en réserve

	Évaluation du risque	**Surveillance du risque**	**Suivi du risque**
Sans défaillance	$q_{ave} = q_0 + 0{,}5\lambda_s TI + (q_0 + \lambda_s TI)\,TR/TI + \lambda_d TM + TPM/TPMI$	$q(t) = q_0 + 1 - \exp\{-\lambda_s (t - TL)\} + \lambda_d TM$	a) avec mémoire de défaillance seulement $q(t) = q_0 + 1 - \exp\{-\lambda_s (t - TL)\} + \lambda_d TM$ b) avec mémoire totale $q(t) = q_{00}$
Avec défaillance	Comme sans défaillance, pas de crédit pour restauration	Événement caché jusqu'à la détection $q(t) = q_0 + 1 - \exp\{-\lambda_s (t - TL)\} + \lambda_d TM$ Événement évident lors des actions correctives : $q(t) = 1$ Possibilité de rétablissement	Événement caché jusqu'à la détection a) indisponibilité latente $q(t) = 1$, ou b) indisponibilité linéaire $q(t) = (q_0 + \lambda_s (t - TL))/(q_0 + \lambda_s TI)$ Événement évident lors des actions correctives : $q(t) = 1$ Possibilités de rétablissement

(Source: SKI, 1994)

Où: q_0 est la probabilité de défaillance sur demande (indépendante du temps) du composant,
q_{00} est la probabilité de défaillance sur demande mais non sur test,
λ_s est le taux de défaillance en attente,
TL est le moment du dernier essai,
λ_d est le taux de défaillance en fonctionnement,
TM est le temps moyen de demande,
TI est l'intervalle d'essais,
TR est le temps moyen de réparation,
TPM est le temps moyen de maintenance préventive,
TPMI est l'intervalle moyen de maintenance préventive.

Cause commune de défaillance

La dépendance du temps introduit par les EPS vivante produit de nouvelles exigences pour les modèles de cause commune de défaillance. Un modèle de cause

commune de défaillance dépendant du temps, peut être créé en tenant compte de la dépendance des points d'essai où des défaillances latentes peuvent être détectées et enlevées, ou de nouvelles défaillances introduites. Les hypothèses suivantes ont été posées :

1. Les défaillances latentes peuvent se produire à un point du temps aléatoire pendant que le composant est en réserve
2. Si plusieurs composants sont affectés par le même mécanisme de défaillance latent pendant qu'ils sont en réserve, les composants entre en état de défaillance au même point du temps
3. Les défaillances introduites en testant ou autre activation du composant, rendent le composant défaillant peu après être retourné en réserve.
4. Les défaillances détectées dans le prochain essai avec une probabilité de 1, sont subséquemment réparées parfaitement.

Ces hypothèses mènent à un modèle linéaire dépendant du temps pour les événements à causes partagées.

$$P\left\{C_{A_1 \ldots A_k}(t) = 1\right\} \approx q_0^{k/n} + \lambda_s^{k/n}(t - TL_{A_1 \ldots A_k})$$

Où $A_1 \ldots A_k$ est un sous-groupe spécifique de k dans n composant et $TL_{A1 \ldots Ak}$ est le dernier moment où quelques composants ont été testés. Les paramètres de défaillance de groupe, $q_0{}^{k/n}, \lambda_s{}^{k/n}$, peuvent être développé par des modèles paramétriques comme SHACAM (shared cause model).

Quand des défaillances sont détectées ou les composants sont indisponibles, les probabilités de cause communes de défaillances doivent être recalculées en adaptant les causes d'événement partagées à la situation détectée. En pratique, il est cependant raisonnable d'appliquer les modèles de causes communes de défaillance dépendant du temps seulement aux systèmes d'intérêt et, autrement, appliquer les indisponibilités moyennes dans le temps.

Erreurs humaines

Les erreurs humaines sont incluses dans la modélisation de la centrale pour représenter les différents types d'interactions humaines durant le cours des événements. Les interactions humaines peuvent être catégorisées en cinq (5) types différents selon l'indisponibilité du composant et les événements déclencheurs :

1. Avant un événement déclencheur, le personnel peut affecter l'indisponibilité d'un système ou composant
2. Action humaine amenant un événement déclencheur
3. Erreur d'omission ; après un événement déclencheur, le personnel n'exécute pas l'action requise
4. Erreur de commission ; après un événement déclencheur, le personnel ne suit pas les procédures
5. Action de récupération ; après un événement déclencheur, le personnel, en improvisant, retourne à la situation initiale.

F.2 Données

Données de défaillance

Une exigence de base est que les données doivent être spécifiques à la centrale, et le concept d'EPS vivante demande que les données de défaillance soit régulièrement mise à jour et vérifiées. Pour augmenter la crédibilité des résultats d'EPS vivante, l'estimation des données de défaillance doit être validée. Ceci requiert des analyses pour clarifier les problèmes affectant la validité comme :

1. Problèmes lors des essais : conditions d'essai différentes de la demande réelle, essais ne couvrant qu'une partie du composant, ne couvrant qu'une partie des défaillances possibles, de nouvelles défaillances peuvent être introduites, etc.
2. Problèmes dans le signalement des défaillances : étendue du rapport, exactitude du rapport, les informations rapportées, etc.

3. Problèmes dans la préparation des données quantitative de défaillances : définition des limites, des groupements de composants, du nombre de demandes, des traitements statistiques, etc.
4. Problèmes dans la modélisation de fiabilité : le vieillissement, l'inefficacité des essais, hypothèses sur le degré de dépendance selon le temps, etc.

Données d'exploitation

Les données sont nécessaires dans les approches de surveillance et de suivi du risque. Dans la surveillance du risque, les données d'exploitation incluent les informations au sujet des états des systèmes et composants. Basés sur les données d'exploitation, les événements de base évidents sont mis à vrai ou faux. Dépendamment de la réalisation du système d'EPS vivante, les modèles sont mis à jour par les personnes responsables en suivant les procédures. Dans un système "on-line", les opérateurs gardent les modèles à jour tout le temps. Si l'utilisation de l'EPS est moins fréquente, les informations sont rassemblées chaque fois qu'une évaluation est faite. Les principales informations nécessaires sont :

- les modes d'exploitation de la centrale;
- les modes d'opération des principaux systèmes;
- les modes d'opération des composants;
- les enregistrements des derniers essais.

F.3 Incertitudes

Il y a trois sortes d'incertitude à prendre en considération dans le contexte d'EPS vivante.

- l'incertitude reliée au degré de compréhension et d'exhaustivité des phénomènes à être modélisés;
- l'incertitude reliée au degré de validité des modèles utilisés;

- l'incertitude paramétrique : concernant les valeurs de la multitude des paramètres utilisés dans les modèles EPS.

F.4 Limites

Même si un travail approfondi a été réalisé pour améliorer les modèles d'arbre de défaillance et d'événement pour les rendre plus complet et enlever le conservatisme, il reste plusieurs manques et incertitudes.

1. Exhaustivité

   Le problème d'exhaustivité apparaît car un modèle maniable ne peut renfermer tous les événements et séquences concevables c'est-à-dire que le risque n'est pas couvert en entier dans le modèle. Le fait de ne pas être exhaustif peut aussi résulter en de mauvaises importances relatives des défaillances individuelles.

2. Conservatisme

   Dans plusieurs cas les modèles d'EPS sont construits avec des hypothèses conservatrices. La raison est habituellement pour simplifier le modèle tout en faisant des estimations conservatrices. Le conservatisme peut amener de fausses importances relatives et de mauvaises décisions et ainsi amener des actions non-conservatrices.

3. Cause commune de défaillance

   Les indisponibilités des systèmes dépendants du temps et les causes communes de défaillances ne sont pas complètement modélisées dans les EPS conventionnelles. Le problème est d'éviter le conservatisme et de permettre des arrangements non-symétriques d'essais. Un modèle de cause commune de défaillance dépendant du temps peut être créé en tenant compte de la dépendance des moments d'essais où des erreurs latentes peuvent être détectées et enlevées ou de nouvelles erreurs introduites. Des analyses plus poussées sont nécessaires avant que des recommandations concernant ce problème puissent être données.

4. Vérification et efficacité des essais

   En pratique, une hypothèse simplifiée est posée disant que les conditions d'essai sont égales aux exigences de la demande (l'essai est parfait). Si l'efficacité des essais est prise en considération, le modèle d'indisponibilité dépendant du temps d'un composant doit être changé, plus de paramètres sont nécessaires. Il y a aussi un manque de données en regard de l'efficacité des essais.

5. Contrainte de temps

   Dans le contexte d'une EPS vivante avec ses fréquentes mises à jour, il y a trop peu de temps pour exécuter une évaluation avec le modèle entier, au lieu de cela des calculs simplifiés ou diminués sont faits. Une façon de réduire le temps de calcul est d'utiliser une liste de coupes minimales précalculées et de mettre à jour les probabilités d'événements de base seulement. Naturellement les changements dans les événements évidents peuvent donner des résultats fortement biaisés. La limite de temps est le facteur de motivation pour l'utilisation d'analyse d'incertitude intégrée, car la simulation de Monte Carlo nécessite trop de temps.

6. Approche simplifiée pour les évaluations dépendantes du temps

   Plusieurs programmes informatiques utilisés dans l'analyse d'EPS appliquent seulement les indisponibilités nominales aux événements de base. Ce qui est requis pour une implantation pratique est une routine qui lit les fichiers d'événement et qui trouve les moments où des calculs sont nécessaires. À chaque moment, de nouvelles probabilités sont calculées pour les coupes du composant. Comme résultat, un registre du risque avec des points du temps et la fréquence de risque correspondante est obtenu.

ANNEXE G

SYSTÈME INFORMATISÉ D'EPS VIVANTE

Cette annexe se veut un document d'introduction à l'informatisation des EPS. Elle énonce les concepts et principes généraux à respecter. L'implantation d'un système informatisé d'EPS vivante nécessite d'autres analyses plus spécifiques et détaillées mais doit être basée sur les enseignements découlant de cette annexe.

Les informations présentées dans cette annexe proviennent majoritairement du rapport de la Statens Karnkraftinspektion (1994) et des outils informatiques existants (Cafta, Riskman, Riskspectrum, Saphire, etc.).

Un système d'EPS vivante se définit comme toute la structure informatisée (logiciel et matériel) liée à la construction, l'évaluation et la documentation d'une EPS.

G.1 Objectif du système

Le concept d'EPS vivante met l'accent sur le réalisme de l'analyse appliquée aux situations courantes de la centrale. Fondamentalement, la question est: "Comment le modèle d'EPS peut être mis à jour pour refléter les changements et s'adapter aux besoins de l'évaluation continue de sûreté?" L'établissement d'un modèle d'EPS vivante est pratiquement possible de nos jours. À en juger par les applications existantes, c'est plus une question de ressources que de développement de solutions techniques. Cependant, les implantations pratiques requièrent des développements

des codes EPS existants afin d'exécuter et de minimiser les temps des réévaluations basées sur les coupes.

L'accès à un modèle adaptable procurant une représentation réaliste de l'état de sûreté, lequel est en principe disponible sous forme informatique pour les analyses en profondeur, ouvre les possibilités pour un champ plus large d'utilisation de l'EPS dans les décisions reliées à la sûreté. Ceci peut être réalisé en construisant un système d'EPS vivante renfermant le modèle et les analyses et les rendant plus accessibles pour l'évaluation de la conception de la centrale, des procédures, de la planification de l'exploitation et du retour d'expérience. Le noyau d'un système d'EPS vivante est le modèle, mais en plus un environnement informatique doit être créé avec les buts suivants en tête :

- supporter l'utilisateur dans l'extraction de toutes les informations pertinentes de l'EPS vivante
- intégrer l'EPS vivante avec les informations existantes sur les systèmes de la centrale
- établir un rapport entre les résultats de l'EPS vivante et les critères déterministes

De telles applications doivent cependant être introduites seulement après s'être assuré que les résultats d'EPS vivante sont correctement compris et utilisés. Ceci requiert une évaluation des domaines où l'EPS vivante peut contribuer à améliorer la sûreté avec une emphase particulière sur comment les résultats d'EPS vivante doivent être présentés au personnel possédant une connaissance limitée des EPS.

L'exigence principale d'un outil informatique d'EPS est de fournir un moyen flexible pour gérer le modèle, les données et les informations nécessaires à l'évaluation de l'EPS et à la gestion de la sûreté. La fonction de calcul de base est de générer les coupes minimales et de calculer la fréquence d'accident. En plus de cela, un nombre d'autres exigences peut être produit pour améliorer l'utilisation des résultats et enseignements d'une EPS. Un aspect important est le temps de calcul nécessaire à la réévaluation des modèles, étant donné certaines conditions

spécifiques. Le système informatique doit aussi supporter les spécifications flexibles des composants ou systèmes c'est-à-dire hors service ou reconfiguré, afin de mettre à jour l'état du risque de la centrale.

G.2 Exigence de base

Un système d'EPS vivante doit être logique, facile d'utilisation, efficient et capable de manipuler un modèle détaillé. Par définition, une EPS vivante est destinée à être utilisée sur une base journalière. Ceci implique une exigence commune à tous les systèmes d'EPS vivante soit la mise à jour du modèle. Il doit être possible de mettre à jour le modèle EPS et ses résultats de façon simple.

Logique : L'outil et le modèle d'EPS vivante doivent être cohérents, compactes et les informations présentées sous forme logique de haut en bas (structure hiérarchique). L'utilisateur doit être capable de trouver l'endroit désiré de façon logique. Toutes les connections entre les entités doivent être claires malgré un grand nombre de mises à jour. L'utilisateur doit avoir accès à toutes les informations nécessaires à la compréhension du modèle. Les entités doivent être répétées le moins possible. Un mécanisme doit assurer que lorsqu'un changement est fait à un endroit, il est effectué aux autres endroits pertinents.

Facilité d'utilisation : Un outil d'EPS vivante doit être convivial (user-friendly) et pratique, ainsi il n'y a pas de pertes de temps associées au programme et à ses limites, les efforts sont dirigés sur le modèle lui-même. Il doit posséder des fonctions flexibles pour trouver et pour insérer des informations dans le modèle. L'éditeur de modèle doit posséder une fonction de vérification d'erreur et permettre le retour en arrière. Une caractéristique importante est que le programme doit être capable de prendre en considération par lui-même les changements qui n'ont pas encore été calculés. Le programme doit prendre soin des informations mise à jour à partir d'autres informations et ainsi avertir lorsque les résultats ne sont pas à jour.

Efficient : Les calculs doivent être assez rapides pour permettre une utilisation journalière. Afin de guider l'utilisateur vers une utilisation plus efficiente du modèle et du programme, les informations doivent lui être présentées de façon hiérarchique. L'outil doit guider l'utilisateur à travers le modèle en partant d'une vue générale vers les détails les plus importants.

Exigences du modèle : Les exigences de base d'un modèle EPS sont l'étendue, l'exhaustivité et le réalisme. Les modèles de risque nominal ne peuvent pas être utilisés pour la surveillance et les applications de contrôle du risque à court terme. Un approfondissement sur les besoins de développement de modèles dépendant du temps pour les calculs du risque instantané est nécessaire car les modèles ne doivent pas contenir d'événements basés sur des indisponibilités nominales.

Exigences des données : Il faut appliquer les données spécifiques à la centrale lorsqu'elles sont disponibles. Les modèles dépendant du temps nécessitent des analyses sur les données spécifiques de défaillances pour identifier les mécanismes dépendants et indépendants du temps.

G.3 Caractéristique d'un outil d'EPS vivante

Les outils d'EPS vivante sont des programmes informatiques permettant de gérer les modèles, données et informations nécessaires à la gestion et l'évaluation de la sûreté d'une centrale nucléaire par son EPS. Le concept d'EPS vivante implique un modèle de la centrale adaptable afin qu'il puisse être mis à jour en parallèle avec les modifications et reconfigurations de la centrale. Une interface conviviale, une rapidité d'exécution et la capacité d'emmagasiner et manipuler un grand nombre d'informations de toutes sortes sont requis afin de rencontrer ce concept. Cette section fournit la description d'un outil d'EPS vivante idéal (théorique).

G.3.1 Fonctions nécessaires

Un des principaux buts d'un outil d'EPS vivante est qu'il doit contenir un éventail complet de fonctions permettant la réalisation et le maintien d'une EPS de niveau 1 pour une centrale nucléaire. La présente section résume les fonctions nécessaires.

Le gestionnaire de modèles est le coeur de l'outil. C'est lui qui possède les fonctions d'édition et d'analyse des modèles. La capacité du gestionnaire de modèles est le paramètre le plus restrictif d'un outil d'EPS vivante. Le gestionnaire de modèles peut se diviser selon les quatre (4) parties suivantes:

1. Construction

   La construction de modèles consiste en des éditeurs graphiques et tabulaires d'arbres de défaillances et d'arbres d'événements. En plus des fonctions d'édition de base (ajouter, enlever, lier, etc.) les éditeurs doivent permettre:

   - d'identifier les causes communes;
   - de gérer et d'évaluer les paramètres des événements de base;
   - de classer et d'identifier les événements initiateurs;
   - d'identifier et de gérer les séquences d'événements;
   - d'accéder à toutes les informations nécessaires (système de documentation et base de données de fiabilité);
   - de construire des AMDE. Cette fonction est généralement exécutée par un logiciel ou module autre que celui de construction d'arbre de défaillance et d'événement. Cependant, il est préférable que l'information soit accessible par l'éditeur de modèle.

2. Évaluation

   L'évaluation d'un arbre de défaillance s'effectue généralement par la génération de coupes. En plus d'un générateur de coupes, les fonctions d'analyse suivantes sont requises:

- Analyse qualitative et quantitative des coupes minimales;
- Analyse en fonction du temps;
- Analyse d'importance: calcul des mesures d'importance pour les événements individuels ou groupés;
- Analyse de sensibilité: vérification de la sensibilité du modèle en regard des conditions limites ou d'hypothèses dans les modèles;
- Analyse d'incertitude paramétrique (ex.: Monte-Carlo).

3. Traitement et évaluation à posteriori

   Cette partie consiste principalement en un éditeur de coupes permettant d'étendre l'analyse des résultats. Dans un contexte d'EPS vivante, une fonction permettant d'effectuer et d'évaluer des changements temporaires (alignements, essais, etc.) est aussi nécessaire. Une fonction d'analyse de coûts est recommandée.

4. Gestion des résultats

   Cette fonction s'occupe de l'emmagasinage et de la documentation des analyses, résultats et spécifications. Il est important que la récupération d'informations provenant de la base de données de l'EPS soit efficiente. Un utilisateur doit rapidement et aisément être capable de localiser et combiner les informations d'intérêt, et présenter ces informations sur l'écran ou des rapports imprimés.

G.3.2 Informations et données

Tous les arbres de défaillances, arbres d'événements, événements de base, résultats d'analyse, etc. doivent être maintenus et intégrés dans une base de données communes comprenant des façons flexibles d'ajouter des informations. Ceci afin de faciliter la mise à jour, la gestion des modèles et données, la traçabilité et le contrôle de la qualité.

Informations de base à emmagasiner dans la base de données: Les informations de base à emmagasiner dans une base de données d'EPS vivante consistent aux données de base utilisées pour construire et quantifier le modèle (tableau G-1). Une base de données comprend le modèle complet avec les données de chacune de ses parties ainsi que les résultats obtenus. Ces données de base doivent être emmagasinées afin de garantir que les différents résultats obtenus sont reproductibles.

Tableau G-1

Informations de base d'une banque de données d'EPS vivante

Éléments du modèle	Informations
Analyse de séquence d'accident	Événement de tête (conséquence, séquence, fonction, etc.), description et données
Analyse des arbres d'événement	Description et données, événements initiateurs, événements fonctionnels et états dangereux
Analyse des arbres de défaillance	Description de la logique, des portes et des événements de base
Donnée des événements de base	Définitions, limites et paramètres
Données paramétriques	Spécifications des paramètres, source des données de spécifications ou analyse des données de défaillances
Spécification des attributions	Définition des groupements (pour les analyses d'importance et de sensibilité)
Spécifications des "house event"	Conditions limites des spécifications
Données d'exploitation	Schéma des essais, alignements, etc.
Bibliothèque des données de la centrale	Rapport de sûreté, description des systèmes, schéma fonctionnel, informations sur les composants (localisation, type, mode de défaillance, manufacturier, etc.), spécifications techniques, etc.

(Source: SKI, 1994)

Informations prétraitées et classements: Avec les informations prétraitées et les classements emmagasinés dans la base de données (tableau G-2), l'utilisateur peut rapidement et aisément localiser, combiner et présenter les résultats de quantifications spécifiques.

Tableau G.2

Informations prétraitées et classements d'une banque de données d'EPS vivante

Données prétraitées et classement	Informations
Résultats nominaux	
Évaluation du risque de base (moyen)	Résultats précalculés et importances des contributeurs. Description des séquences d'accidents dominantes. Résultats d'événements de tête (conséquence, séquence, fonction, systèmes, etc.). Résultats des analyses de sensibilité et d'incertitude.
Données sur la propagation des défaillances et leurs dépendances	AMDE basée sur la logique des arbres de défaillance. Informations sur les interfaces entre les composants et systèmes de support.
Classements	Mesures d'importance (RAW, RRW) pour les scénarios, fonctions, systèmes, composants, modes de défaillances, etc. Classements selon les résultats d'analyse de sensibilité et d'incertitude.
Résultats instantanés	
Évaluation du suivi du risque	Résultats générés suite à des observations en exploitation ou résultats générés suite à des scénarios planifiés.
Données d'exploitation	Données d'exploitation et activités d'essais et de maintenance. Données sur les transitoires, indisponibilités des composants, etc.
Classements conditionnels	Classement des situations d'exploitation et des scénarios de défaillance importants. Classement des composants selon leur contribution relative au risque instantané. Classement conditionnel en situation de défaillance i.e. classement de l'équipement défectueux en fonction du bénéfice de le remettre en service.

(Source: SKI, 1994)

Les principaux résultats d'un système d'EPS vivante comprennent les coupes minimales, les fréquences moyennes et instantanées de dommage du coeur, les mesures d'importance, les analyses de sensibilité et d'incertitude. Les résultats doivent être immédiatement disponibles sans besoin d'autres calculs. Le programme doit être capable d'attirer l'attention sur les résultats qui ont changé depuis la dernière évaluation. Il devrait être possible de faire une comparaison entre les résultats du modèle de base et le modèle changé. Le programme doit être capable de fournir des résultats résumés, des résultats détaillés et une variété entre les deux. Les extrants doivent contenir assez d'information pour identifier leur provenance afin qu'on ne puisse pas mélanger ceux-ci.

G.4 Principes d'une interface d'EPS vivante

Une modélisation flexible et compréhensible de la centrale est la clé si l'on veut que l'EPS devienne un outil pratique d'aide à la décision en exploitation. Le développement et les exigences des modèles sont discutés dans le chapitre 3 du présent document. En assumant qu'un modèle comportant toutes les qualités nécessaires est disponible, la prochaine étape consiste à clarifier son utilisation pour la gestion et l'exploitation de la centrale. Cette tâche est différente du développement du modèle puisqu'elle tient compte de l'applicabilité des résultats de l'EPS dans différents domaines, des connaissances des utilisateurs d'EPS et du comment intégrer l'EPS vivante avec les systèmes d'informations existant dans la centrale.

Pour faire la meilleure utilisation du potentiel de l'EPS vivante, sans aller au-delà des limites de l'EPS, requière que les résultats de l'EPS soient présentés selon un contexte et accompagnés des principes de sûreté et des exigences d'exploitation. L'accès au modèle d'EPS vivant doit être facilité en établissant des liens avec les autres sources d'informations et en procurant une interface homme-machine adaptable aux différents utilisateurs. L'interface opérationnelle doit créer une structure informatisée enveloppant le modèle d'EPS vivante et être conçue de façon à maximiser les bénéfices reliés à l'utilisation des modèles et des analyses sous-jacentes.

En se basant sur le point de vue présenté ci-dessus, les principes pour la conception d'une interface opérationnelle d'EPS vivante sont les suivants:

- L'opération du système ne doit pas nécessiter une expertise des données ou une connaissance approfondie des modèles d'EPS;
- La préparation des données doit être facile et rapide, une prédéfinition et/ou une génération automatique sont possible;
- La sélection des calculs à être exécutés et la présentation des résultats doivent être flexibles et couvrir une grande variété d'applications;

- Le lancement et l'exécution des calculs du modèle doivent nécessiter peu d'opérations lorsque les données d'entrées et de sorties sont définies;
- Lorsque les résultats d'EPS vivantes doivent être présentés dans un contexte avec d'autres informations et conditions limites, le système d'EPS vivante doit communiquer avec les sources d'informations ou base de données de la centrale;
- Lorsque possible, le système doit être équipé d'un programme interactif d'extraction et de traitement des informations contenues dans le modèle EPS et la documentation.

ANNEXE H

TECHNIQUES D'ANALYSE D'EPS

Cette annexe décrit et explique brièvement les trois (3) techniques d'analyse complémentaires que l'on retrouve généralement dans une EPS. Celles-ci sont:

- les arbre de défaillance;
- les séquences d'événements;
- les arbres d'événements.

Jusqu'à maintenant les EMS se limitaient à l'utilisation des arbres de défaillance et des séquences d'événements. Il faut cependant mentionner que les séquences d'événements sont très détaillées dans le cas des EMS et ce sont donc celles-ci qui sont décrites dans cette annexe. La prochaine EMS révisée à Gentilly-2 utilise quant à elle les trois (3) techniques comme les EPS de type "internationale".

H.1 Arbre de défaillance

La technique de l'arbre de défaillance est une analyse déductive des événements qui provoquent un état indésiré pour un système. Elle est utilisée pour estimer la fréquence des défaillances fonctionnelles. Les analyses portent aussi bien sur les défaillances aléatoires de l'équipement et les erreurs de l'exploitant que sur les défauts de régulation et de contrôle. Une analyse caractéristique par arbre de défaillance est illustrée à la figure H.1. Afin de mieux comprendre cette figure, il est fortement conseillé de consulter le "Fault Tree Handbook" du USNRC (1981).

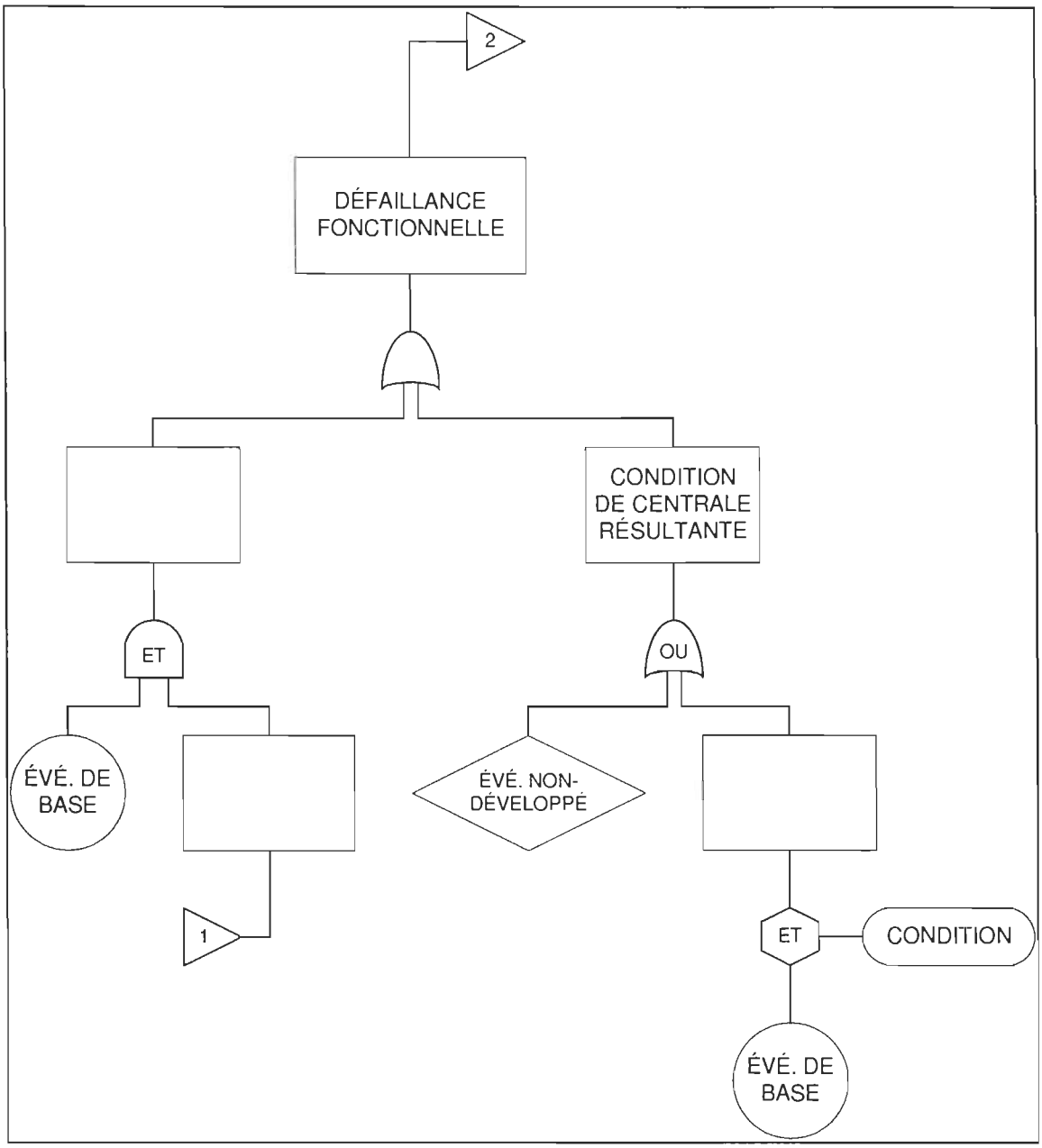

Figure H.1. Logique des arbres de défaillance (Source: Gumley, 1979)

Les modes de défaillance pouvant entraîner la perte du système fonctionnel visé par l'étude doivent être examinés afin de permettre la définition des conditions d'exploitation prévues au moment de la défaillance. Dans certains cas, la nature des événements précédant la défaillance dicte celle des événements subséquents. La fréquence de la défaillance doit être estimée, afin de pouvoir déterminer si les mesures de protection du réacteur sont appropriées. Les formules mathématiques

utilisées pour les fins de la technique de l'arbre de défaillance sont présentées dans plusieurs documents dont les suivants: USNRC (1981) et AECL (1981).

L'application de la technique de l'arbre de défaillance pour analyser une défaillance fonctionnelle permet de détecter les modes de défaillance. Une défaillance fonctionnelle correspond, dans de nombreux cas, non pas à la défaillance spontanée d'une importante installation de la centrale pouvant entraîner des conséquences graves, mais plutôt à la conjugaison de divers événements ou incidents hautement probables qui, pris individuellement, ont une incidence négligeable sur la sûreté de la centrale.

H.2 Séquence d'événements

Après avoir déterminé le déroulement et la fréquence des défaillances fonctionnelles, une analyse des différentes séquences d'événements est amorcée afin d'établir la mesure dans laquelle les systèmes de sûreté et les systèmes reliés à la sûreté sont disponibles à partir du moment où se produit la défaillance fonctionnelle. Ces séquences se terminent lorsque leur fréquence est inférieure ou égale à 10^{-7} événements/année ou dès que les conditions d'exploitation se sont stabilisées. La possibilité de relever divers événements initiateurs plausibles constitue l'un des avantages de ce processus analytique; on peut ainsi déterminer si la conception est appropriée. Il est aussi possible de détecter les défaillances croisées (cross-linked) touchant d'autres systèmes de support et, le cas échéant, de justifier dans une certaine mesure la prolongation ou l'interruption éventuelle des séquences.

Un exemple de séquence d'événements est présenté à la figure H.2.

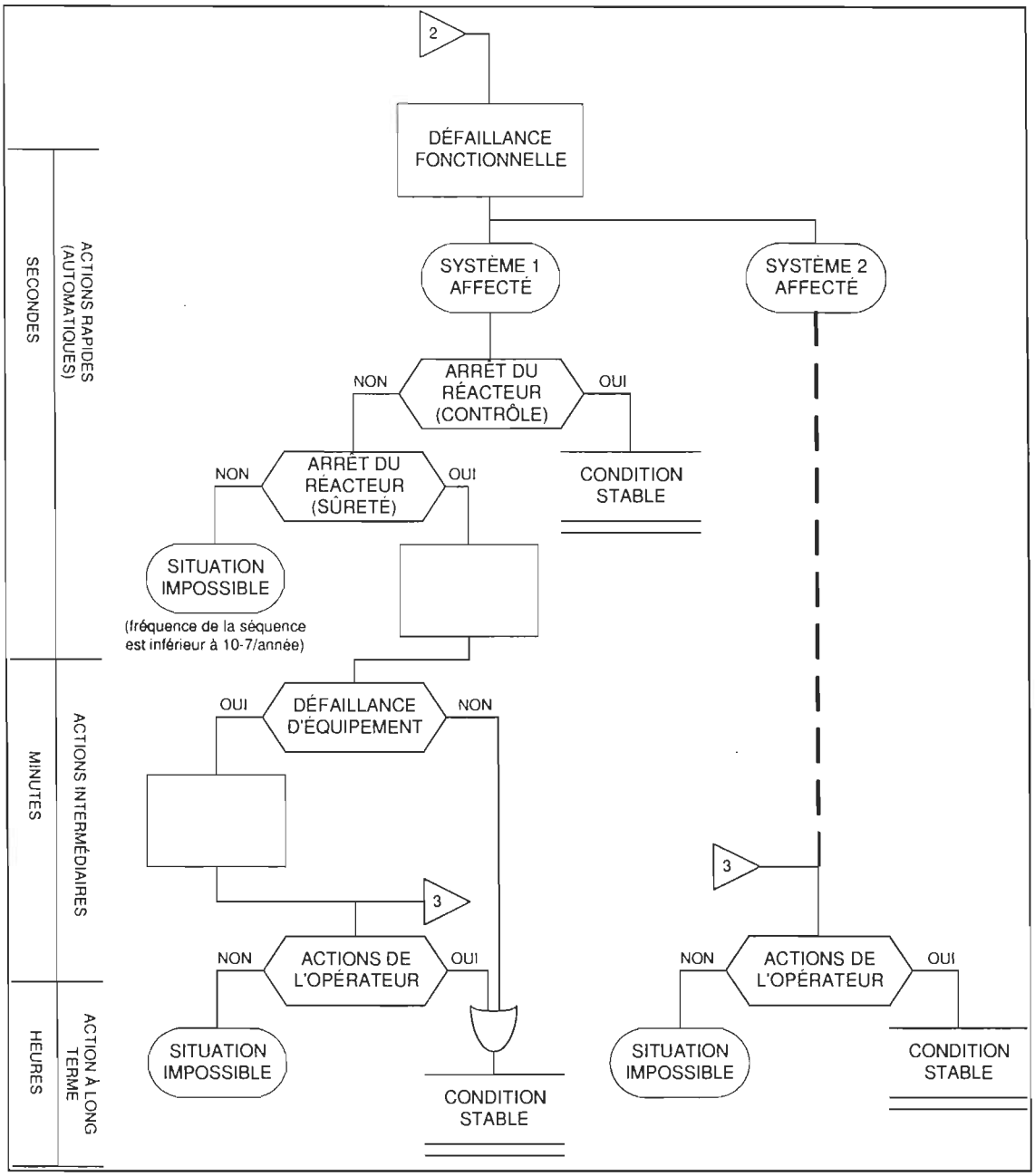

Figure H.2. Logique des séquences d'événement (Source: Gumley, 1979)

Le mode de présentation des séquences a été élaboré de façon à faciliter la compréhension des événements et à refléter l'importance accordée aux limites de temps, ce qui permet de prévoir les conditions d'exploitation et le rôle de l'exploitant. Les scénarios concevables sont d'ordinaire définis en fonction du temps nécessaire à la sollicitation des systèmes de sûreté par l'exploitant et de l'aptitude de

ce dernier à remédier à la situation. Pour les systèmes automatiques, cela correspond à une évaluation de leur aptitude à réagir, à court terme, aux conditions résultantes, à mettre le réacteur à l'arrêt de façon sûre et à assurer le refroidissement du cœur. Dans la plupart des cas, cela revient à dissocier les systèmes spéciaux de sûreté de la défaillance et de ses conséquences immédiates, et à indiquer que les paramètres de déclenchement sont appropriés.

L'adéquation des paramètres de déclenchement avec les événements initiateurs concevables doit être établie au moyen d'analyses de transitoires détaillées à court terme (d'une durée de quelques secondes). Ces données sont d'ordinaire utilisées seulement à titre indicatif dans le cadre de l'étude matricielle.

La situation relève davantage de l'exploitant à mesure que le temps passe (moyen ou long terme: minutes, heures ou jours). En règle générale, la puissance résiduelle est plutôt faible pendant ces périodes, sans compter que dans la plupart des situations à long terme, l'exploitant dispose de plusieurs heures pour prendre une décision. Toutefois, il est généralement admis que des défaillances aléatoires peuvent se produire à long terme; celles-ci sont donc représentées dans les séquences d'événement.

H.3 Arbre d'événements

Une fois les séquences d'événements déterminées, l'arbre d'événements est utilisé pour les identifier, les représenter et les évaluer de manière qualitative et quantitative. La démarche généralement utilisée comporte les cinq étapes suivantes (Villemeur, 1988):

1. Détermination des fonctions de sûreté

   Les fonctions de sûreté sont définies par un ensemble d'actions empêchant la fusion du coeur, la perte de l'intégrité de l'enceinte ou minimisant les relâchement de produits radioactifs. De telles actions peuvent résulter d'une

mise en oeuvre automatique ou manuelle de systèmes liés à la sûreté. La liste des fonctions de sûreté à considérer dépend du but de l'étude, des moyens mis en oeuvre pour l'analyse, etc.

2. Détermination des événements initiateurs

   Par définition, un événement initiateur est le premier événement d'une séquence d'événements. On reprend donc les événements initiateurs déterminés lors de l'élaboration des séquences d'événements.

3. Élaboration de l'arbre d'événement "fonctions"

   Dans un premier temps, on élabore un arbre d'événements avec pour événements génériques des fonctions de sûreté. Un tel arbre est développé pour chaque événement initiateur puisque chacun d'entre eux génère une réponse fonctionnelle particulière de la centrale en sollicitant différemment les fonctions de sûreté. Pour faciliter sa construction, on s'aide des séquences d'événements réalisées précédemment.

4. Élaboration de l'arbre d'événements "systèmes"

   Chaque fonction de sûreté identifiée comme événement générique est accomplie par un système ou parfois par un ensemble de systèmes. On obtient un arbre d'événement "systèmes" en remplaçant dans l'arbre d'événement "fonctions", les fonctions par les systèmes de sûreté correspondants. Il faut bien évidemment modifier l'arbre d'événements et revoir éventuellement l'ordre des événements génériques. Ceci est généralement dû aux nombreuses interaction entres fonctions de sûreté, entre systèmes, à l'existence de systèmes accomplissant plusieurs fonctions de sûreté, etc.

   L'ordre des événements génériques, très important, est souvent le résultat d'une pratique itérative. Trois facteurs aident à en déterminer l'ordre:

- le temps: Dans l'arbre d'événement, les systèmes sont placés dans l'ordre dans lequel ils sont sensés intervenir dans le cadre de la réponse de la centrale.
- les interactions fonctionnelles: citons les exemples suivants:
    - les systèmes qui dépendent du fonctionnement d'autres systèmes doivent être considérés après ces systèmes.
    - si l'échec d'une fonction entraîne nécessairement l'échec d'autres fonctions, le succès de ces dernières n'est évidemment plus à considérer.
- les interactions entre les systèmes: les systèmes auxiliaires communs à différents systèmes de sûreté doivent être considérés avant ces derniers.

5. Quantification

   Le calcul de la probabilité des séquences de l'arbre d'événements n'est simple que si tous les échecs ou succès des missions des différents systèmes sont des événements indépendants les uns des autres; dans le cas contraire, toutes les probabilités à considérer sont des probabilités conditionnelles. Aussi, est-il nécessaire d'obtenir un arbre d'événements réduit. Les simplifications déjà opérées, lorsqu'on prend en compte les interactions fonctionnelles et les interactions entre systèmes vont dans ce sens.

La figure H.3 présente un exemple d'arbre d'événements.

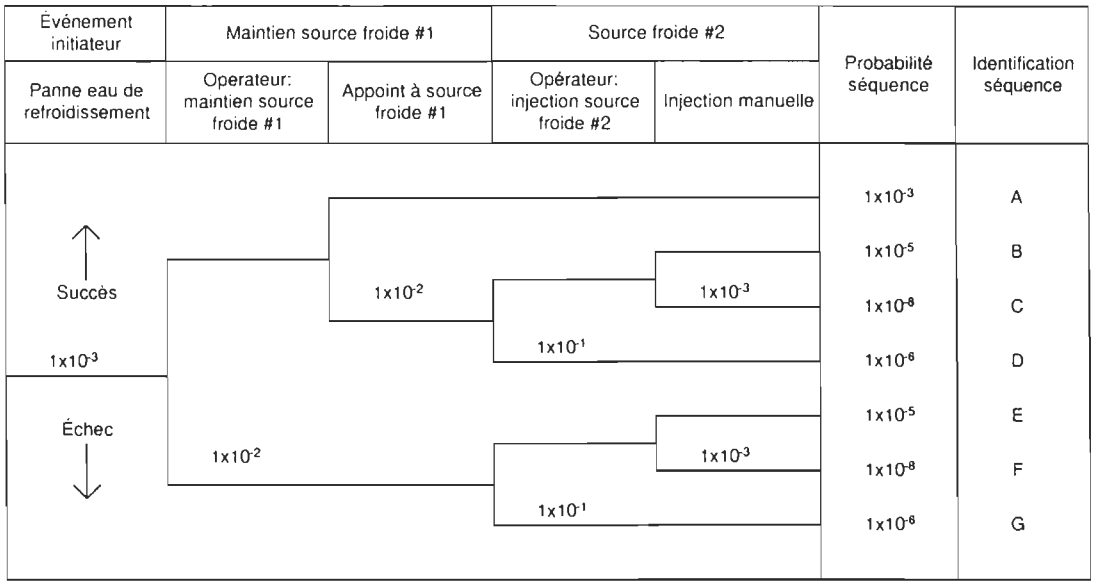

Figure H.3. Logique des arbres d'événements

ANNEXE I

ENVERGURE DES ÉTUDES MATRICIELLES DE SÛRETÉ

Cette annexe décrit l'ampleur et l'objet des études matricielles de sûreté. Les numéros inscrits entre les parenthèses correspondent aux numéros d'identification utilisés à Gentilly-2. La compréhension de cette annexe nécessite une certaine connaissance de la conception des réacteurs CANDU-PHW 600. Cette annexe offre cependant aux non-initiés une idée des scénarios d'accident modélisés.

Les informations présentées sont extraites de Gumley (1979) et on été validées, et quelque peu modifiées, avec les études matricielles de sûreté de Gentilly-2 afin de refléter le contenu réel de celles-ci.

I.1 Surcriticité imprévue (66-SDM-1)

Une surcriticité imprévue se produit lorsqu'un réacteur à l'arrêt ou un réacteur critique à faible puissance devient surcritique indépendamment de la volonté de l'exploitant. Une telle situation peut comporter des risques de rejets de produits de fission si les protections prévues sont inaptes à ramener le réacteur à un état sous-critique. Les divers événements initiateurs susceptibles de produire une surcriticité sont répertoriés. Des arbres de défaillance sont utilisés pour déterminer la fréquence de ces événements.

Les délais d'intervention de l'exploitant en cas de surcriticité imprévue varient selon la capacité de réactivité à l'arrêt et le taux de changement de la réactivité correspondant à l'enlèvement du poison. Ce dernier paramètre varie selon que le

combustible utilisé est neuf ou à l'équilibre et selon que le circuit de purification enlève à la fois le gadolinium et le bore ou seulement l'un de ces deux poisons.

En cas de surcriticité imprévue, l'exploitant est présumé être alerté au moyen d'alarmes et de messages, et non par les tableaux d'affichage normalement utilisés.

Les séquences d'événements pour chaque cas de surcriticité imprévue sont préparées, et les modalités d'intervention de l'exploitant sont définies.

I.2 Perte des générateurs de vapeur comme source froide (66-SDM-2)

La perte de générateurs (GV) de vapeur comme source froide est examinée en situation normale et en situation anormale (accident).

I.2.1 Conditions normales d'exploitation

Cette partie de l'étude a pour objet d'examiner les modes de défaillance, en situation normale d'exploitation et à l'arrêt, entraînant la perte des générateurs de vapeur comme source froide. Les événements initiateurs les plus fréquents sont les suivants : défaillances du système de régulation entraînant une perte de régulation de la pression ou du niveau des GV; défaillances dans le circuit d'eau d'alimentation (défaillance des pompes d'alimentation ou des vannes de régulation); erreurs commises par l'exploitant. Initialement, la circulation dans le circuit primaire de caloportage est présumée être assurée par les pompes de ce circuit ou par celles du circuit de refroidissement à l'arrêt. Les défaillances qui réduisent la capacité du caloporteur à céder de l'énergie calorifique aux GV sont examinées.

Les séquences d'événement permettent de déterminer les délais dont dispose l'exploitant pour prendre les mesures qui s'imposent et d'indiquer les sources

froides de remplacement qui peuvent être utilisées pour chaque mode de défaillance.

I.2.2 Conditions anormales d'exploitation (accident)

Cette partie de l'étude a pour objet d'examiner les scénarios d'accident prévoyant l'utilisation des GV comme source froide, après coup, lorsque ces derniers n'ont pas contribué à l'accident. L'aptitude des GV à constituer une source froide est examinée. Voici des situations où les GV sont nécessaires :

a) perte du circuit principal de vapeur;
b) faible perte de caloporteur;
c) perte prolongée d'alimentation de catégories III et IV; l'aptitude de l'exploitant, dans un tel cas, à établir et à maintenir l'alimentation en eau des GV, à l'aide du circuit d'eau d'urgence et du système d'alimentation électrique d'urgence, est examinée.

I.3 Importante perte de caloporteur (PERCA) et refroidissement d'urgence du coeur (RUC) (66-SDM-3)

La fréquence utilisée pour cette étude provient de l'arbre de défaillance d'une PERCA importante. Cette étude porte sur les séquences d'événement consécutives à une dépressurisation du circuit de caloportage pour diverses fuites concevables dans le circuit.

Ces séquences permettent d'évaluer l'efficacité du RUC, l'accent étant mis sur le rôle de l'exploitant pendant la transition devant déboucher sur le refroidissement d'urgence du coeur à long terme. L'étude permet également d'examiner les alarmes et les indications susceptibles d'être transmises à l'exploitant à la suite de bris à divers endroits dans le circuit.

Les défaillances pouvant toucher l'équipement ou l'instrumentation des systèmes utilisés dans le bâtiment-réacteur à la suite d'une PERCA, ainsi que leurs conséquences éventuelles, sont examinées.

On accorde une importance particulière à la disponibilité des systèmes de sûreté et des systèmes reliés à la sûreté ainsi qu'aux renseignements qui sont communiqués à l'exploitant afin de lui permettre de prendre les mesures de sûreté qui s'imposent.

La disponibilité d'une source froide de remplacement est présumée être nécessaire pour la définition du rôle de l'exploitant dans les séquences d'événement consécutives à une PERCA. La disponibilité de cette source froide est examinée dans toutes les séquences consécutives à l'accident.

Si les séquences d'événement font état de conditions qui sont abordées dans d'autres études matricielles, un renvoi à ces données est proposé.

Comme l'équipement essentiel peut fonctionner pendant des mois pour assurer le refroidissement à long terme, il faut examiner les conséquences de défaillances éventuelles.

Les séquences d'événement pour cette étude prennent fin lorsque s'amorce l'opération de nettoyage.

I.4 Exploitation de la centrale à la suite d'un tremblement de terre (66-SDM-4)

Cette étude a pour objet d'examiner les conséquences que peut entraîner l'exploitation de la centrale après un tremblement de terre. Pour les fins de l'étude, l'équipement ayant une qualification parasismique est présumé être disponible immédiatement après le séisme. Les modes de défaillance des systèmes non qualifiés dans le bâtiment-réacteur, le bâtiment des services et le bâtiment de la turbine sont examinés afin de déterminer les conditions éventuelles d'exploitation.

Ces modes de défaillance comprennent les pertes partielles de systèmes non qualifiés pouvant entraver le processus de mise à l'arrêt automatique du réacteur immédiatement après le séisme et avant l'intervention de l'exploitant.

Des séquences d'événement sont préparées pour chaque condition d'exploitation. Pour chaque séquence, la sûreté de la salle de commande est examinée et le rôle de l'exploitant est défini; on détermine également si ce dernier peut exploiter efficacement la centrale depuis la salle de commande principale ou s'il vaudrait mieux qu'il s'installe dans la salle de commande d'urgence. Cette analyse porte sur les mesures que doit prendre l'exploitant pour assurer le fonctionnement du système d'eau d'urgence (SEU) et du système d'alimentation électrique d'urgence (AEU), et sur l'équipement de régulation dont il dispose pour chaque séquence.

Les séquences prennent fin lorsque les conditions d'exploitation se sont stabilisées.

I.5 Inondation du bâtiment des services ou du bâtiment de la turbine (66-SDM-5)

Cette étude a pour objet d'examiner les conséquences de l'inondation du bâtiment des services et du bâtiment de la turbine. La technique de l'arbre de défaillance est utilisée pour analyser les modes de défaillance pouvant entraîner une inondation de ces bâtiments. De telles inondations seraient vraisemblablement causées par le bris d'une conduite ou d'une vanne; dans les centrales où ces bâtiments sont situés à un niveau inférieur à celui de la prise d'eau, le bris de brides du circuit d'eau de circulation du condenseur pourrait causer une inondation. La vitesse d'élévation du niveau de l'eau est évaluée, afin de déterminer les modalités d'intervention de l'exploitant.

Les risques que pose l'inondation de ces bâtiments sont liés à la perte éventuelle d'équipement de soutien, notamment des compresseurs du circuit d'air d'instrumentation, des groupes électrogènes de secours, des pompes d'alimentation des générateurs de vapeur, de la turbine et de ses accessoires.

Les conséquences de la perte de ces équipements sont évaluées à l'aide de séquences d'événement. Les intervalles de temps prévus entre l'accident initial et la perte de cet équipement sont pris en considération.

Les moyens (régulation et instrumentation) dont dispose l'exploitant pour réduire la puissance du réacteur et refroidir le coeur sont examinés.

I.6 Conséquences d'un arrosage intempestif et de l'inondation du bâtiment-réacteur (66-SDM-6)

Cette étude a pour objet d'examiner les conséquences d'un arrosage intempestif lorsque le réacteur est en marche ainsi que celles de l'inondation du sous-sol du bâtiment-réacteur, causée par une défaillance d'un circuit d'eau de refroidissement à l'intérieur de l'enceinte étanche.

La technique de l'arbre de défaillance est utilisée pour déterminer la fréquence des arrosages intempestifs. Les défaillances touchant les éléments suivants sont prises en considération : conduites, vannes et collecteurs du circuit d'arrosage; régulation et instrumentation.

Les conséquences d'un arrosage intempestif et les modes de défaillance des systèmes touchés par cette anomalie à l'intérieur de l'enceinte étanche sont examinés à l'aide de la technique des séquences d'événement. Seuls les systèmes qualifiés pour fonctionnement dans un milieu détrempé sont présumés être disponibles. On accorde une importance particulière au fonctionnement des pompes du circuit primaire de caloportage, à l'intégrité de ce circuit, aux défaillances de la machine de chargement, à la perte du circuit de refroidissement du modérateur et des boucliers, et à la disponibilité des systèmes de sûreté.

La technique de l'arbre de défaillance est utilisée pour déterminer la fréquence de ces inondations. Seuls les circuits d'eau de refroidissement situés à l'intérieur du bâtiment-réacteur sont pris en considération pour l'analyse des pertes de régulation ou d'équipement attribuables à un niveau élevé d'eau dans le sous-sol. Le circuit de refroidissement des boucliers, qui renferme une faible quantité d'eau, présente peu de risques d'inondation. Par contre, le circuit d'eau de service est beaucoup plus susceptibles d'inonder le sous-sol du bâtiment. Même un bris limité peut entraîner le déversement d'importantes quantités d'eau s'il n'est pas détecté rapidement.

Des séquences d'événement sont préparées. La taille des bris est prise en considération pour déterminer la vitesse à laquelle le niveau de l'eau est susceptible de monter dans les cas extrêmes. Pour les situations où une intervention de l'exploitant est nécessaire, les alarmes et les indications liées à chaque mode de défaillance sont répertoriées, et les délais d'intervention de l'exploitant sont précisés.

I.7 Faible perte de caloporteur (PERCA) et refroidissement d'urgence du coeur (RUC) (66-SDM-7)

Une faible PERCA consiste en une perte de caloporteur entraînant une dépressurisation du circuit primaire qui peut être neutralisée par le circuit secondaire (GV). Dans un tel cas, la puissance du réacteur est réglée à l'aide du système de régulation.

Bien que l'emplacement de la fuite ait une incidence limitée sur les conséquences d'une faible PERCA, au début de la dépressurisation du circuit primaire, les conséquences à plus long terme varient en fonction des hypothèses d'isolement des boucles, de la disponibilité des pompes du circuit de caloportage, de l'appoint prévu et de l'intervention de l'exploitant. La technique de l'arbre de défaillance est utilisée pour déterminer la fréquence de ces accidents et, subséquemment, pour définir les

conditions initiales en fonction desquelles les séquences d'événement seront préparées.

Des séquences d'événement sont préparées en nombre suffisant pour permettre de relever les principales différences existant entre les conditions initiales prévues pour chaque faible PERCA concevable. Ces séquences complètent l'analyse du transitoire pendant les premières étapes de la défaillance concevable. Après la sollicitation du circuit de refroidissement d'urgence du coeur, le rôle de l'exploitant est défini pour chaque événement consécutif à l'accident. Les défaillances des systèmes de sûreté essentiels sont analysées et incorporées aux séquences d'événement. Une importance particulière est accordée à la qualification de l'équipement essentiel, à l'instrumentation et à la régulation de cet équipement après l'accident.

La perte d'alimentation de catégorie IV consécutive au déclenchement du réacteur ou de la turbine doivent être incorporée à chaque séquence. Les résultats d'analyses en cours visant à définir les conditions optimales de thermosiphon sont aussi pris en considération.

Les séquences d'événement prennent fin lorsque les conditions d'exploitation se sont stabilisées ou que la probabilité d'autres événements est inférieure a 10^{-7} évé./année. Si la séquence d'événements comprend un rejet de produits de fission dans l'enceinte étanche, la fréquence prévue et les délais approximatifs pour un tel rejet sont indiqués. Ces données sont utilisées pour une étude similaire portant sur le confinement.

I.8 Confinement (66-SDM-8)

Cette étude sert de fondement à d'autres études ayant pour objet de définir les besoins en matière de confinement.

Deux types de défaillances fonctionnelles sont examinés :

1) celles qui entraînent un rejet radioactif dans l'enceinte étanche;
2) celles qui peuvent endommager l'enveloppe de confinement.

Les défaillances de type 1) qui sont examinées sont les suivantes : perte importante de caloporteur, faible perte de caloporteur, défaillance spontanée des tubes de force, défaillance des raccords d'extrémité, réduction du débit dans les canaux du réacteur, défaillance de la machine de chargement lorsque celle-ci est raccordée au réacteur, défaillance de la machine de chargement lorsque celle-ci n'est pas raccordée au réacteur.

Les défaillances de type 2) comprennent la perte du circuit principal de vapeur et la dépressurisation des deux boucles du circuit de caloportage.

Les données sur la fréquence de ces défaillances sont extraites des documents pertinents; la technique de l'arbre de défaillance est utilisée pour les cas où de telles données ne sont pas disponibles.

Les séquences d'événement sont préparées. Celles-ci ont pour objet d'examiner les défaillances éventuelles du confinement après l'accident.

Les modalités d'intervention de l'exploitant sont définies, y compris le temps dont il dispose pour maintenir le confinement ou, en cas de perte d'étanchéité du confinement, pour limiter l'ampleur du rejet de produits de fission, à l'aide des systèmes de filtration d'air.

Les séquences d'événement pennent fin lorsque s'amorce le processus de rétablissement des conditions normales d'exploitation. Pour les fins de la présente analyse, ce moment est présumé coïncider avec l'interruption du refroidissement d'urgence du coeur à long terme et le début de l'enlèvement du combustible.

I.9 Modérateur utilisé comme source froide (66-SDM-9)

Cette étude porte sur l'utilisation du modérateur comme source froide à la suite d'une perte de caloporteur accompagnée d'une indisponibilité du système de refroidissement d'urgence du coeur.

Après la dépressurisation du circuit primaire, le combustible, qui est alors à découvert, surchauffe et se déforme dans les tubes de force, qui à leur tour s'affaissent et entrent en contact avec les tubes de la calandre. Dans un tel cas, le transfert de chaleur du combustible au modérateur sous-refroidi atténue les contraintes mécaniques dans le coeur.

La fréquence pour une perte de caloporteur accompagnée d'une indisponibilité du système de refroidissement du coeur est déterminée à l'aide de la technique de l'arbre de défaillance. L'analyse porte sur deux types de fuites dans le circuit primaire : celles qui sont attribuables au bris d'un tube de force à l'intérieur du coeur et celles qui résultent d'un bris à l'extérieur du coeur. Tous les bris à l'extérieur du coeur sont pris en considération, quelle que soit leur importance.

Les conditions prévues après l'accident sont analysées pour chaque scénario concevable. L'accent est mis sur la qualification de l'équipement essentiel, sur l'instrumentation et sur la régulation, notamment sur l'aptitude de cet équipement à demeurer disponible.

Des séquences d'événement sont préparées pour chacune des étapes consécutives à l'accident. Le rôle joué par l'exploitant pour établir et assurer le maintien du refroidissement est défini au besoin.

Compte tenu du caractère anormal de ce mode d'exploitation, les alarmes et les indications reçues pendant cette période sont analysées afin de relever les sources

éventuelles d'information erronée; ces données sont utilisées pour l'évaluation des erreurs d'exploitation.

Pour les fins de l'analyse, la puissance du réacteur avant l'accident est présumée être de 100 % P.P. Les transitoires prévus à la fin de la période de dépressurisation servent à définir les conditions initiales pour cette analyse.

I.10 Perte des deux ordinateurs (66-RS-04)

Les deux ordinateurs sont présumés être indisponibles lorsque l'un et l'autre sont inaptes à exécuter une des fonctions de régulation jumelées. Les ordinateurs sont dotés de protections permettant l'envoi de signaux «sûrs» aux dispositifs faisant l'objet de la régulation. En effet, lorsqu'une fonction de régulation ne peut être exécutée par l'ordinateur, celui-ci détecte l'anomalie par autocontrôle et coupe le circuit qui le relie au dispositif visé. En outre, si la coupure du circuit ne se fait pas, le signal de sortie de l'ordinateur est réglé de façon à mettre le dispositif dans un état sûr. L'étude matricielle de sûreté portant sur la perte des deux ordinateurs a pour objet d'analyser la séquence d'événement consécutive à une indisponibilité similaire à celle qui est décrite ci-dessus. Les autres modes de défaillance ne sont pas visés par cette étude.

L'indisponibilité des deux ordinateurs peut être attribuable :

1) à une défaillance complète des deux ordinateurs;
2) à l'inaptitude des deux ordinateurs à exécuter au moins une des fonctions de régulation jumelées;
3) à une défaillance complète de l'ordinateur principal, suivie d'une défaillance du mécanisme de transfert des fonctions de régulation;
4) à la défaillance d'au moins une fonction de régulation jumelée dans l'ordinateur principal, suivie de la défaillance du mécanisme de transfert des fonctions de régulation.

Des arbres de défaillance sont utilisés pour déterminer la fréquence de ces événements.

Dans le cadre de l'étude sur la perte des deux ordinateurs, les conséquences de l'inaptitude de ceux-ci à exécuter au moins une fonction de régulation jumelée sont examinées, et les modalités d'intervention de l'exploitant sont définies. En outre, les séquences d'événement correspondant aux divers modes de défaillance prévus sont préparées.

I.11 Perte de refroidissement du modérateur et des boucliers (66-RS-05)

Cette étude porte sur les modes de défaillance des circuits de refroidissement du modérateur et des boucliers. Les défaillances entraînant une perte de circulation, de source froide et de fluide sont examinées, et les arbres de défaillance correspondants sont élaborés. Le fonctionnement du réacteur lorsque la quantité de modérateur est réduite (dans la calandre) constitue, pour les fins de l'étude, une condition normale d'exploitation, puisqu'il s'agit d'une exigence normale visant à limiter la quantité de D_2O devant être transférée pendant le réchauffage ou l'arrêt du réacteur. Un bilan de réactivité est établi afin de déterminer le niveau critique du modérateur permettant de maintenir le réacteur en puissance tant en régime stable qu'en régime transitoire (perte de modérateur). L'absence de refroidissement de la calandre par atomisation peut accroître les contraintes et la température dans les tubes et l'enveloppe.

Il est prévu que dans les huit minutes qui suivent une perte de refroidissement ou de débit du modérateur, celui-ci entre en ébullition. Dans un tel cas, le rejet d'importantes quantités de deutérium et de tritium dans l'enceinte étanche constitue la préoccupation principale.

L'apport de chaleur relativement faible et l'inertie thermique relativement importante du circuit de refroidissement des boucliers donnent lieu à des transitoires

plutôt lents pouvant nécessiter la prise de nombreuses mesures correctives par l'exploitant.

Les séquences d'événement pour la perte de ces circuits sont élaborées. Des analyses sont effectuées dans le but de déterminer les contraintes et la température de la cuve dans de telles conditions. Les résultats de ces analyses devraient montrer que de telles pertes n'ont aucune incidence sur le fonctionnement des systèmes d'arrêt d'urgence et sur l'intégrité du circuit primaire.

La contribution de l'exploitant à la mise à l'arrêt du réacteur et à l'établissement d'une autre source froide est définie dans les séquences d'événement.

I.12 Perte de refroidissement à l'arrêt (66-RS-07)

I.12.1 Conditions normales d'exploitation

Le circuit de refroidissement à l'arrêt a pour fonction de refroidir le caloporteur et de le maintenir à une basse température pendant une période indéfinie. En situation normale, le circuit de refroidissement à l'arrêt réduit la température du caloporteur seulement lorsque celle-ci a atteint une valeur intermédiaire (et non la valeur maximale à pleine puissance), soit environ trente (30) minutes après l'arrêt. D'ordinaire, les pompes principales du circuit de caloportage sont utilisées pour faire circuler le caloporteur et le faire passer dans les échangeurs de chaleur; les pompes du circuit de refroidissement à l'arrêt ne sont sollicitées que plus tard au cours du processus de refroidissement, lorsque la chaleur produite par les pompes du caloporteur devient la principale source thermique dans le circuit.

Le circuit de refroidissement à l'arrêt est aussi conçu pour assurer le refroidissement du coeur lorsque le circuit de caloportage est drainé (au niveau

des collecteurs) afin de permettre l'entretien des générateurs de vapeur et des pompes du circuit de caloportage.

Dans la première partie de cette étude, la technique de l'arbre de défaillance est utilisée afin de déterminer la fréquence des pertes du circuit de refroidissement à l'arrêt. Les défaillances et les défauts de fonctionnement qui se produisent au début du processus de refroidissement à l'arrêt ou en mode normal de refroidissement à l'arrêt sont incorporés à l'arbre de défaillance. La séquence d'événement faisant suite à une défaillance ou à un défaut de fonctionnement de ce circuit est préparée.

I.12.2 Conditions anormales d'exploitation

Il est prévu que le circuit de refroidissement à l'arrêt sera utilisé en situation anormale. Il constitue une source froide de remplacement en cas d'indisponibilité du circuit de vapeur, du circuit principal d'eau d'alimentation ou de l'alimentation électrique de catégorie IV.

Il est proposé d'utiliser le circuit de refroidissement à l'arrêt comme source froide dès après l'arrêt du réacteur (et non après que la température du caloporteur a atteint une valeur intermédiaire).

Des arbres de défaillance et des séquences d'événement sont préparés pour ces conditions anormales. Les défaillances et les défauts de fonctionnement qui se produisent au début du processus de refroidissement à l'arrêt en situation anormale ou en mode anormal de refroidissement à l'arrêt sont incorporés à l'arbre de défaillance.

Note :Le fonctionnement du circuit de refroidissement à l'arrêt en cas de tremblement de terre n'est pas visé par cette étude

I.13 Perte de l'alimentation d'air (66-RS-08)

Dans une centrale, l'air comprimé alimente normalement trois ou quatre circuits, soit un circuit d'air d'instrumentation, un circuit d'air de service, un circuit d'air pour respirateurs (air à masque) et, dans les centrales multitranches, un circuit d'air servant à la régulation et au fonctionnement des systèmes communs. La technique de l'arbre de défaillance est utilisée pour déterminer la fréquence des pertes de chaque circuit d'air lorsqu'il est prévu que celles-ci compromettent la sûreté de la centrale. L'élaboration de l'arbre de défaillance pour une perte d'air comprimé comprend une évaluation des défaillances des compresseurs et des sécheurs, afin de pouvoir déterminer les liens d'interdépendance entre l'air comprimé et divers systèmes auxiliaires (ex.: eau de service). L'aptitude de l'exploitant à maintenir ou procurer une autre source d'air comprimé est incorporée à l'arbre de défaillance. Les pertes d'air comprimé prévues dans les arbres de défaillance comprennent les bris de conduites, les bris de vannes, les pertes de régulation et les erreurs de l'exploitant. La fréquence des pertes partielles ou totales d'air comprimé est examinée dans les cas où le circuit est doté de réservoirs d'air permettant d'assurer une alimentation d'appoint à la suite d'une brève indisponibilité d'un compresseur. Les réservoirs d'air, qui sont destinés à des systèmes particuliers, ne sont pas pris en considération pour l'élaboration des arbres de défaillance des circuits d'air. Ils sont toutefois incorporés à des séquences d'événement subséquentes. L'examen de chacun des systèmes fonctionnels et des systèmes de sûreté touchés permet de déterminer l'incidence des pertes d'air sur la sûreté de la centrale et de faire état des conditions résultantes. Des séquences mixtes (composite event sequence diagram) sont préparées et examinées afin de relever les modes de défaillances croisés. On accorde une importance particulière au maintien de l'alimentation en eau des générateurs de vapeur et à la disponibilité de sources froides de remplacement.

L'air d'instrumentation est largement utilisé pour la régulation de la centrale. Lorsque la régulation est liée à la sûreté, des réservoirs d'air sont disponibles. Le

rôle de ces réservoirs et celui de l'exploitant, à long terme, sont incorporés à la séquence d'événement.

I.14 Perte de l'eau de service (66-RS-09)

La fonction de refroidissement est assurée d'ordinaire par trois ou quatre circuits d'eau. Un seul de ces circuits, soit le circuit d'eau de circulation du condenseur, peut être considéré comme étant fonctionnellement indépendant, puisqu'il ne partage que la source d'eau avec les autres circuits. Un circuit d'eau brute est utilisé pour refroidir le circuit d'eau de service recirculée. Les centrales multitranches sont dotées d'une source commune d'eau de service d'appoint, l'eau étant acheminée à chaque tranche à l'aide de conduites vannées.

Les défaillances entraînant une perte d'eau de service sont examinées au moyen de la technique de l'arbre de défaillance, afin de déterminer la fréquence de la perte de chaque circuit. D'ordinaire, les pertes d'eau de service sont attribuables à l'encrassement des tamis, à la perte du circuit de lavage des tamis, à une perte de régulation, à une perte d'équipement (pompe, vanne, conduite, etc.), à une perte d'alimentation électrique ou à une erreur de l'exploitant.

La défaillance d'une barre omnibus constitue une perte d'alimentation pour les fins de l'étude. Une perte d'alimentation de catégorie IV se traduit par une baisse automatique des charges du circuit d'eau de service, afin de permettre aux groupes électrogènes de secours de satisfaire aux besoins essentiels. Dans les séquences d'événement, une perte d'alimentation électrique peut être considérée comme étant la cause ou la conséquence d'une perte d'eau de service (ex.: un arrêt du réacteur entraînant une perte d'alimentation du réseau).

En règle générale, les circuits d'eau de refroidissement satisfont aux besoins essentiels de refroidissement des pompes et des échangeurs de chaleur des divers

systèmes de sûreté ou systèmes reliés à la sûreté. Les modes de défaillance croisés (cross-linked) sont indiqués.

Les séquences d'événement sont préparées afin de déterminer les conséquences des pertes d'eau de service. Les défaillances croisées sont prises en considération pour l'élaboration du modèle; celui-ci comprend les hypothèses les plus plausibles quant au temps écoulé avant la défaillance, aux systèmes touchés et aux conséquences éventuelles. Voici des exemples de systèmes qui seraient touchés par une perte d'eau de service: eau d'alimentation des générateurs de vapeur, air d'instrumentation, refroidissement du modérateur et des boucliers, garnitures d'étanchéité des pompes du circuit primaire de caloportage, alimentation électrique.

Le rôle de l'exploitant est évalué pour les cas où il doit intervenir. On examine notamment l'aptitude de l'exploitant à maintenir une source froide suffisante, à réduire la pression du circuit primaire et à assurer l'intégrité de celui-ci.

I.15 Perte d'alimentation électrique (66-RS-10)

Cette étude porte sur les conséquences des pertes d'alimentation électrique de catégorie III ou IV. La fréquence des pertes d'alimentation de catégorie IV est établie en fonction des données sur la stabilité du réseau, des pertes d'équipement et de la réaction de la turbine en cas d'instabilité du réseau. Deux périodes de référence sont utilisées pour évaluer les pertes d'alimentation de catégories IV: moins de trente (30) minutes, période pendant laquelle l'alimentation peut être rétablie par l'exploitant; plus de trente (30) heures, période pendant laquelle des éléments importants de la centrale peuvent être touchés par des défaillances (ex.: un transformateur ou une ligne de transport d'énergie).

L'aptitude des groupes électrogènes de secours à rétablir et à maintenir l'alimentation électrique de catégorie III peut être évaluée, et la fréquence des défaillances déterminée, en fonction de ces deux périodes de référence. Lorsque l'alimentation de

catégorie III ne peut être rétablie dans les trente (30) minutes suivant une défaillance, il s'ensuit une perte d'alimentation de catégorie I et II, alimentation assurée par des accumulateurs. Les pertes d'alimentation de catégorie I et II attribuables à des défaillances aléatoires de barres omnibus ne sont pas visées par la présente étude. Comme ces sources d'alimentation sont triplées et séparées, il est peu probable que la défaillance d'une seule barre omnibus de catégorie I ou II ait une incidence sur la sûreté de la centrale.

Les conséquences d'une perte d'alimentation de catégorie IV de longue durée sont examinées au moyen d'une séquence d'événements. Le rôle de l'exploitant y est défini, et l'aptitude de ce dernier à maintenir l'alimentation en eau des générateurs de vapeur, à l'aide de l'alimentation électrique d'urgence et du circuit d'eau d'urgence, y est examinée.

Les pertes partielles d'alimentation de catégorie III ou IV attribuables à la défaillance d'une barre omnibus sont aussi examinées et, s'il y a lieu, les séquences d'événement correspondantes sont élaborées. La division des sources d'alimentation selon un système de numérotation pair et impair signifie que les barres omnibus de catégorie III et IV sont doublées. Or, comme il n'en est pas ainsi des charges, il s'ensuit que la défaillance varie selon que la perte d'alimentation est attribuable à une barre paire ou impaire.

I.16 Exploitation de la centrale à la suite d'autres événements de mode commun

Cette étude a pour objet d'examiner les conséquences éventuelles de divers événements, naturels ou provoqués par l'homme, n'ayant aucun lien avec l'exploitation de la centrale.

Voici des exemples d'événements provoqués par l'homme : accidents routiers, ferroviaires, aériens ou maritimes; accidents industriels. Les incendies, les inondations, les tornades et les tempêtes de neige constituent des événements

naturels. Les tremblements de terre ne sont pas compris dans cette étude, étant donné que l'exploitation de la centrale à la suite d'un séisme fait l'objet d'une autre étude matricielle.

La fréquence de chaque événement est estimée et une séquence reflétant les conditions d'exploitation après l'accident est préparée. Chaque séquence prend fin lorsque les conditions se sont stabilisées.

ANNEXE J

COMMENTAIRES DE LA CCEA

Les demandes de permis d'exploitation pour les centrales nucléaires CANDU-PHW 600 devaient inclure, en plus des analyses déterministes traditionnelles, un nombre d'études spéciales appelées Études Matricielles de Sûreté (EMS). Suite à leur vérification, une liste de critère à remplir et les méthodes pour y arriver fut développée par le personnel de la CCEA afin d'améliorer et d'assurer la cohérence, la vérification et l'état complet des EMS et des études de fiabilité. Elle fut communiquée à EACL et aux exploitants comme des critiques sur les EMS originales (lettre du 12 décembre 1980 de J.G. Waddington à A. Duchesne-R. McKenzie-P. Gumley). Ces critères sont présentés ci-dessous.

1- Limites des systèmes:

(a) Les limites déterminant l'interaction et/ou l'interface entre le système analysé et les autres systèmes doivent être clairement définies. La définition des limites doit être fonctionnelle et physique et ne pas créer de chevauchements ou d'écarts entre les systèmes adjacents.

(b) Les probabilités utilisées dans les EMS mais qui sont validées dans les études de fiabilité doivent être clairement identifiées. De tels croisements de références entre les EMS et les études de fiabilité sont acceptables s'il est démontré que les événements auxquels ces probabilités sont assignées sont exactement les mêmes dans les deux documents (i.e. même limites de système). Si ce n'est pas le cas, l'utilisation de même probabilité doit être justifiée sur une base cas par cas.

2- Définition de la défaillance d'un système

L'exploitant doit compiler une liste des défaillances de système qui ont été considérées, incluant celles qui ont été identifiées mais écartées pour différentes raisons. Les critères ou modes de défaillance doivent être énoncés de façon précise et mesurable. La liste doit demeurer à jour et si une définition change, l'effet de ce changement doit être étudié et signalé.

Les défaillances de systèmes comprennent :

a) Les défaillances sur demande, ceci inclut l'incapacité d'un système de fonctionner au moment de la requête et au cours de la période pendant laquelle son fonctionnement est requis.
b) Les défaillances empêchant un système de cesser de fonctionner sur commande
c) Les défaillances causant l'entrée en fonction d'un système sans en avoir eu la commande.
d) Les défaillances conduisant à de nouveaux événements initiateurs

3- Information sur la conception

Les informations de conception utilisées lors des analyses doivent clairement être identifiées. Par exemple, le numéro de révision d'un dessin ou d'un manuel de conception doit être identifié afin que chaque changement ainsi que son effet sur les résultats de l'analyse soient correctement expliqués.

4- Liste des hypothèses

Les hypothèses utilisées dans l'analyse doivent être énoncées clairement. Il arrive que le manque d'informations ou de ressources oblige l'analyste à poser des hypothèses. Ces hypothèses doivent être résumées dans un annexe afin de faciliter leur validation et la revue de l'étude par d'autres experts.

5- Informatisation des arbres de défaillances

Les défaillances identifiées dans les séquences d'événement doivent être résumées sous la forme d'arbres de défaillance. Le format des arbres de défaillance doit permettre leur

informatisation. L'informatisation est nécessaire pour manipuler un nombre élevé d'information provenant de diverses analyses et d'extraire de celles-ci toutes les contradictions entre les différentes analyses.

6-Codification des événements

Chaque événement présenté dans les arbres de défaillance doit se faire assigner un code unique et garder celui-ci dans toutes les analyses. Le but de cette exigence est de procurer un moyen d'identification pour les liens croisés entre les systèmes et identifier les exigence contradictoires.

7- Méthode d'évaluation

- Les arbres de défaillance doivent inclure les sources de contrôle et d'énergie.
- Les liens entre les analyses de deux systèmes différents doivent être clairement identifiés dans chaque analyse par des codes communs.
- Les événements considérés non pertinents doivent être exclus et clairement identifiés comme tel dans les arbres de défaillances.
- Les séquences d'événement ne peuvent être utilisées pour définir le taux de défaillance d'événements combinés.
- Une hypothèse sur l'indépendence de systèmes et composants sans validation (preuve) n'est pas acceptable.
- Les arbres de défaillance peuvent être utilisé directement comme des modèles mathématiques seulement à l'intérieur des limites de leur usage.

8- Modèle de l'opérateur

- L'analyse des effets des actions de l'opérateur doit être basée sur les procédures d'exploitation et doit tenir compte de la conception et disposition des instruments de contrôle et d'indications.
- Le modèle de l'opérateur est un outil adéquat pour juger de l'importance relative des actions de l'opérateur dans les séquences d'événement.

- Les probabilités associées avec ce modèle ne sont pas nécessairement conservatrices et donc une probabilité totale de 10^{-7} évé/année ne doit jamais être considérée comme ce terminant à un point impliquant une action de l'opérateur.
- La conséquence d'un comportement irrationnel de l'opérateur doit être considérée comme en dehors des limites de l'étude.
- Cependant on doit tenir compte des actions que l'opérateur est raisonnablement attendu de prendre dans une séquence particulière en plus des actions correctes qu'il est supposé effectuer.

ANNEXE K

OUTILS D'EPS DISPONIBLES À GENTILLY-2

Ce chapitre décrit très brièvement les outils d'EPS disponibles à Gentilly-2.

K.1 CAFTA

CAFTA pour Windows est un programme de développement d'arbre de défaillance qui fonctionne sous un environnement Microsoft Windows. CAFTA permet de:

- construire un modèle d'arbre de défaillance
- construire une base de données de fiabilité
- évaluer l'arbre de défaillance afin d'obtenir des coupes
- réviser et analyser les résultats des coupes

La figure K.1 présente les fonctions majeures de CAFTA lesquelles correspondent aux étapes d'une analyse d'arbre de défaillance.

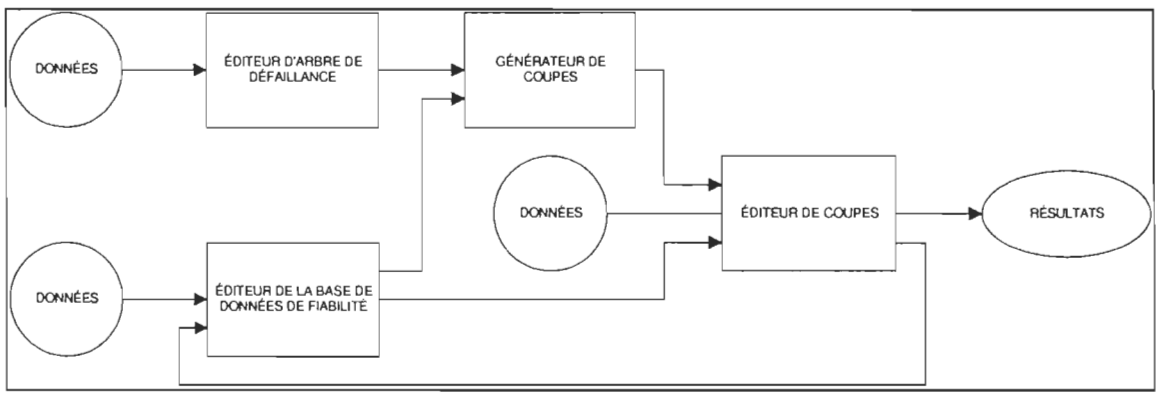

Figure K.1. Fonctions majeures de CAFTA (Source: CAFTA user's manual)

Éditeur d'arbre de défaillance:

L'éditeur reconnaît la structure des modèles d'arbres de défaillances, la signification des types de portes, la différence entre les événements de base et les portes ainsi que les liens entre les événements de base et les portes et entre les portes. Ces capacités permettent à l'éditeur de vérifier le modèle au fur et à mesure qu'il est construit. En plus l'éditeur d'arbre de défaillance supporte plusieurs fonctions spécialisées d'édition (ex.: porte VRAI ou FAUX). L'éditeur procure aussi un lien avec la base de données, permettant à l'utilisateur d'introduire les données descriptives et de fiabilité pendant qu'il construit le modèle.

Base de données de fiabilité:

CAFTA pour Windows est composé de trois bases de données:

- BE: Basic event database-base de données des événements de base
  Contient les noms (code) des événements de base, leur description, probabilités et autres informations.

- TC: Failure rate database-base de données des taux de défaillance
  Contient les taux de défaillance ou les probabilités de défaillance sur demande pour chaque type d'événement.

- GT: Gate description data- description des données des portes
  Contient les informations sur les portes, incluant les descriptions et références. Cette base de données ne contient aucune donnée de fiabilité, seulement des informations décrivant le modèle d'arbre de défaillance.

Générateur de coupes:

L'arbre de défaillance peut être réduit à la forme de coupes en utilisant le générateur de coupes: CQUANT. CAFTA pour Windows permet aussi de tronquer ou enlever des coupes ayant de faibles probabilités d'occurrence.

Éditeur de coupes:

L'éditeur de coupes supporte la révision des résultats des coupes et procure une analyse qualitative pour l'analyste. L'éditeur peut être utilisé pour classer les événements en ordre d'importance et pour les études de sensibilité.

K.2 GTPROB

Cet outil d'arbre de défaillance calcule les probabilités des portes sans générer de coupes. Cela est très utile pour les applications requérant un haut degré de précision ou pour les modèles utilisant de grandes probabilités.

K.3 UNCERT

Un outil d'arbre de défaillance calculant les distributions d'incertitude pour les probabilités de défaillances d'un système.

K.4 ETA

Un outil permettant de développer des arbres d'événements pour l'analyse des séquences d'accident.

K.5 PRAQUANT

Un outil permettant de quantifier les séquences d'accident afin d'évaluer la contribution de chacune des séquences à la fréquence globale de dégradation du coeur.

K.6 RMQS

Un outil interactif combinant les arbres de défaillances et d'événements en un modèle permettant ainsi des évaluations rapides et faciles de la centrale. Les mesures de risque peuvent donc être réévaluées aussi souvent que désiré.

K.7 GSEAO

Un outil développé par STAR Inc. pour Gentilly-2 pour concevoir des séquences d'événements. Il facilite la gestion graphique des séquences d'événements au moyen de fonctions de génération, d'édition, d'exportation et d'impression. Le logiciel supporte les figures multiples, les échelles de temps, les liens multiples, les références d'entrées et de sorties, les jonctions et/ou, les différents événements, les textes descriptifs et les notes explicatives. Malheureusement, ce logiciel n'effectue aucun calcul.