

Cette démarche, si elle a été couronnée de succès pour l'EPS du palier 1300 MWe (et du palier 900 MWe, appliquée par l'IRSN), va se heurter à des difficultés croissantes dans sa mise à jour notamment pour les données. En effet l'évolution des procédures demande de revoir systématiquement les méthodes. Par ailleurs, l'étude de plus en plus poussée de la conduite accidentelle sur simulateur avec l'apport des techniques psychologiques et ergonomiques montre que l'activité des opérateurs se résume difficilement à l'application des procédures et est en fait extraordinairement complexe, et étroitement dépendante de la situation et de ses particularités. Enfin la focalisation sur l'erreur humaine individuelle apparaît comme une impasse, notamment à cause du haut degré de récupération des erreurs. L'analyse des accidents montre que la conduite en salle de commande résulte plus d'un processus collectif délibéré au niveau de l'équipe que de la somme des erreurs individuelles. Dans le monde anglo-saxon cette même réflexion débouche sur l'étude des « commission errors » (erreurs où l'intention est erronée, par opposition par exemple aux « omission errors » où l'intention est correcte et la réalisation erronée) et un approfondissement des PSF (« performing shaping factors », caractéristiques de la tâche et de l'installation, modulant la probabilité de l'échec). En écho au développement de courants sociologiques ou psychologiques comme la cognition distribuée, il apparaît nécessaire de prendre en compte de façon beaucoup plus systémique les interactions entre opérateurs, procédures et interface.

Ces réflexions aboutiront à la conception par EDF R&D de la méthode MERMOS, tandis que la NRC fera développer la méthode ATHEANA aux Etats-Unis. Aujourd'hui la méthode MERMOS est la méthode de référence d'EDF pour l'analyse de la conduite après la survenue de l'initiateur (conduite post-accidentelle, échecs de type C) : elle a été utilisée pour réaliser l'EPS du palier N4 et pour réactualiser celle du palier 900 MWe. La méthode MERMOS prend en compte globalement la conduite au niveau du système opérateurs / procédures / interfaces. Les erreurs individuelles des opéra-

teurs sont prises en compte comme élément d'un contexte particulier qui favorise un comportement cohérent du système justifié dans une situation légèrement différente, mais inadapté à celle résultant de l'initiateur.

Exemple de l'impact du facteur humain dans le chiffre d'une EPS

Une étude EPS d'EDF donne les chiffres suivants de contribution au risque :

- facteur humain post-accidentel (type C) : 16,8 % ;
- facteur humain pré-accidentel (type A) : 5,7%.

Il n'y a quasiment pas d'évaluation de la contribution des actions de type B dans les EPS d'EDF car les causes techniques et humaines ne sont pas distinguées dans les statistiques à partir desquelles sont élaborées les probabilités des initiateurs.

Les difficultés de l'EPFH

La première grande difficulté de l'EPFH est le recueil de données. La différence entre les proportions précédentes de contribution du facteur humain (FH) dans le risque et les 62% de l'étude de retour d'expérience citée dans le premier paragraphe montre la distance qui sépare l'analyse des « presque accidents » et l'évaluation de la probabilité d'occurrence des accidents. Il est très difficile de disposer de grilles d'analyse cohérentes entre recueil de données et prévision. La prise en compte dans les données EPFH du retour d'expérience d'exploitation est donc plutôt ardue, sans compter que ce retour d'expérience FH est rare, sensible et volatil. En compensation, l'observation de la conduite sur simulateur est systématiquement utilisée, tout spécialement à EDF ; néanmoins, il est toujours besoin d'extrapoler les observations aux situations graves, car le système est efficace et l'on observe très rarement des échecs graves de la conduite simulée. Il est difficile d'utiliser les données provenant d'autres installations nucléaires (autres exploitants, autres pays) sans passer par une modélisation simplificatrice dont on sait les limites.

On reproche également à l'EPFH son manque de répétabilité et un défaut dans

Dossier : Les études probabilistes de sûreté

l'évaluation de l'incertitude des résultats. Ces problèmes semblent peu susceptibles de progresser, car ils sont liés à la complexité de la modélisation du comportement humain. Le premier peut être combattu par le développement de l'expertise et la capitalisation du retour d'expérience qui permet de valider et de compléter les analyses effectuées ; mais le second est difficile à évacuer, même s'il est disproportionné de comparer analyses de fiabilité de matériel et analyses EPFH : les EPS sont traditionnellement centrées sur le matériel, et beaucoup plus de forces sont investies dans cette partie, que l'on sait traiter et où l'on dispose souvent de données nombreuses.

Perspectives

L'EPFH est encore et toujours en plein développement, et de toute façon de plus en plus indispensable aux EPS car les hommes et les organisations changent plus vite que les matériels des installations nucléaires. Le potentiel d'amélioration de la sûreté via cette perspective d'évaluation semble de plus en plus important mais la progression est lente. Les effets indirects sont déjà appréciables : en effet, l'EPFH est au cœur du développement de la culture de sûreté par sa dimension humaine et systémique.

Les exigences de références proposées par WENRA concernant les études probabilistes de sûreté

par **Thomas Maurin**, sous-directeur chargé des réacteurs de puissance - DGSNR

L'association WENRA rassemble les Autorités de sûreté nucléaires d'Europe de l'Ouest (Allemagne, Belgique, Espagne, Finlande, France, Italie, Pays-Bas, Royaume-Uni, Suède, Suisse), auxquelles se sont jointes récemment celles des pays candidats à l'entrée dans l'Union européenne.

Un groupe de travail a été établi par cette association pour étudier les principales différences entre pays des exigences de sûreté, de la conception déterministe ou probabiliste jusqu'aux sujets du management de la sûreté et de la culture de sûreté, pour les réacteurs de puissance actuellement en exploitation.

Les travaux se sont appuyés à la fois sur les exigences nationales des pays participant et sur les standards internationaux de l'Agence internationale de l'énergie atomique, de façon à identifier des exigences de référence sur six thèmes, dont celui des études probabilistes de sûreté.

Un rapport sur les travaux d'harmonisation de la sûreté des réacteurs, décrivant la méthodologie suivie et présentant les exigences de référence, est rendu public sur le site Internet de l'ASN, pour permettre aux parties intéressées de faire leurs commentaires sur cette démarche et ses premiers résultats. Le groupe de travail poursuit par ailleurs ses travaux sur d'autres thèmes liés à la sûreté des réacteurs, de façon à parvenir à un ensemble cohérent d'exigences de référence. Les membres de WENRA comptent développer des plans d'actions nationaux pour 2006 de façon à aligner à terme les pratiques nationales sur les exigences de référence identifiées par le groupe de travail.

Les exigences ou niveaux de référence correspondant aux EPS sont les suivants:

1. Portée et contenu des EPS

1.1 Les EPS doivent être développées pour les niveaux 1 et 2.

1.2 Les EPS doivent inclure tous les modes de fonctionnement, tous les initiateurs et agressions pertinents, y compris l'incendie interne, l'inondation interne, les conditions météorologiques extrêmes et les événements sismiques.

1.3 Les EPS doivent inclure toutes les dépendances pertinentes (dépendances fonctionnelles, dépendances géographiques et autres défauts de mode commun).

1.4 Les EPS doivent contenir des analyses d'incertitude ou de sensibilité.

1.5 Les EPS doivent être fondées sur une modélisation réaliste du comportement de l'installation, prenant en compte la performance humaine dans les limites supposées dans les procédures de conduite normales et accidentelles.

1.6 Les défaillances humaines doivent être analysées, en prenant en compte les facteurs susceptibles d'influencer la performance des opérateurs dans tous les états de l'installation.

2. Qualité des EPS

2.1 Les EPS doivent être réalisées, documentées et tenues à jour suivant le système de gestion de la qualité de l'exploitant.

2.2 Les EPS doivent être réalisées suivant une méthodologie conforme à l'état de l'art.

3. Utilisation des EPS

3.1 Les EPS doivent être utilisées pour le management de la sûreté. Leur rôle dans

Dossier : Les études probabilistes de sûreté

le processus de prise de décision doit être défini.

3.2 Les EPS doivent être utilisées pour identifier le besoin de modifications de l'installation et de ses procédures, afin de réduire le risque créé par l'installation.

3.3 Les EPS doivent être utilisées pour estimer le risque global créé par l'installation, pour démontrer qu'une conception équilibrée a été obtenue, et pour donner l'assurance qu'il n'y a pas d'« effet falaise »⁽¹⁾.

3.4 Les EPS doivent être utilisées pour estimer le caractère adéquat des modifications de l'installation, des changements des spécifications techniques et des procédures et pour estimer la gravité des événements d'exploitation.

3.5 Des résultats des EPS doivent être utilisés comme données pour le développe-

ment et la validation des programmes de formation de l'exploitant en rapport avec la sûreté, y compris la formation sur simulateur des opérateurs de salle de commande.

Dans le cas de la France, les points relevés en écart par rapport aux exigences de référence concernent essentiellement des compléments à apporter à la réglementation, les pratiques ayant été développées sans être intégrées dans des textes à caractère réglementaire. Un travail réglementaire important est donc à mener. Cependant, certaines exigences ne sont pas aujourd'hui mises en œuvre en France et pourront nécessiter des travaux plus ambitieux ; on peut ainsi citer le développement d'études probabilistes couvrant les agressions internes et externes comme le séisme ou l'incendie.

1 Effet falaise : brusque aggravation des conséquences en fonction du franchissement d'un seuil par un paramètre donné.

Comparaison franco-belge des EPS de niveau 1 pour deux types de REP similaires : le palier REP 900 MWe français et le REP Tihange 1 belge

par **Patricia Dupuy**, expert EPS – IRSN (France),
François Corenwinder, chef de projet pour les EPS de niveau 1 sur les REP 900 MWe – IRSN (France)
 et **Dries Gryffroy**, chef de projet pour l'évaluation des EPS – Association Vinçotte nucléaire (Belgique)

Introduction

Dans le cadre de la coopération entre les Autorités de sûreté françaises et belges, une comparaison des EPS (études probabilistes de sûreté) est effectuée depuis plusieurs années. La présente étude comparative concerne deux EPS de niveau 1 pour des événements internes, effectuées pour les états de puissance et pour les états d'arrêt des réacteurs : l'EPS française sur le palier REP 900 MWe et l'EPS belge sur le REP Tihange 1. Ces REP ont tous deux été conçus par Framatome et sont de même génération.

L'EPS sur le palier REP 900 MWe a été réalisée par l'IRSN pour l'Autorité de sûreté nucléaire française et le rapport de synthèse correspondant a été publié en 1990. Le rapport de synthèse de l'EPS réalisée sur Tihange 1 a été publié en 1997 par la société belge architecte-ingénieur (Tractebel Energy Engineering) pour le compte de l'exploitant belge (Electrabel), et a été soumis à AVN (Association Vinçotte nucléaire) pour évaluation par un organisme de réglementation. La comparaison de ces deux EPS a été effectuée par l'IRSN et l'AVN.

L'intérêt, pour les deux parties, de cet exercice de comparaison des EPS est essentiellement lié à leur besoin de revoir en détail les modèles d'EPS et d'améliorer ou d'ajuster les hypothèses qui les sous-tendent lors des mises à jour actuelles ou futures de ces EPS. Pour atteindre ces objectifs, l'exercice

de comparaison des EPS a consisté à identifier et à tenter d'expliquer les principales différences constatées entre les résultats des deux EPS.

Dans ce document, les auteurs ont voulu présenter un tour d'horizon qualitatif des enseignements les plus utiles que l'on peut tirer de cet exercice de comparaison des EPS. Ces enseignements présentent un grand intérêt pour ceux qui élaborent les EPS, comme pour ceux qui les évaluent.

Approche globale

L'approche globale adoptée pour cet exercice consiste en une comparaison directe des résultats des EPS, avec pour objectif premier d'identifier les différences les plus frappantes, et d'essayer de les expliquer en comparant la conception des systèmes, les pratiques d'exploitation, les hypothèses, les modèles et les données.

Cette approche conduisant à une identification directe des différences entre les deux EPS dont l'impact sur les résultats est assez significatif, elle a été préférée à une approche plus complexe fondée sur des évaluations détaillées et systématiques des éléments caractéristiques des EPS (événements initiateurs, séquences accidentelles, modélisation des systèmes, données, pratiques d'exploitation, fiabilité humaine), où l'interprétation des résultats des EPS aurait été repoussée à la fin de l'exercice de comparaison.

Méthodologie

La première étape de l'exercice a consisté à comparer de manière globale les résultats pour les familles d'événements initiateurs lorsque le réacteur fonctionne à pleine puissance. A ce stade, l'exercice s'est limité à une comparaison des définitions et des fréquences des événements initiateurs, ainsi que des fréquences de fusion du cœur correspondantes.

Cette comparaison globale a permis de commencer à identifier et à expliquer certaines différences frappantes, principalement liées à des spécificités relatives à la conception des installations et aux pratiques d'exploitation. Néanmoins, cette comparaison globale s'est révélée trop succincte pour qu'il soit possible d'en tirer des enseignements utiles, démontrant ainsi la nécessité de procéder à une comparaison plus détaillée.

C'est la raison pour laquelle, lors d'une seconde étape, certaines familles d'événements initiateurs et certaines séquences accidentelles à pleine puissance ont été sélectionnées pour faire l'objet d'une comparaison plus approfondie. Cette sélection s'est effectuée essentiellement sur la base des critères suivants :

- une forte contribution à la fréquence de fusion du cœur dans l'une des études ou dans les deux ;
- des problèmes de sûreté et des inquiétudes soulevés dans les analyses de sûreté actuelles ;
- des différences significatives entre les résultats des deux EPS, soit en termes de fréquence de fusion du cœur, soit en termes de contribution au risque global (fréquence de fusion du cœur totale).

Le premier critère de sélection a conduit à retenir les accidents de perte de réfrigérant primaire (APRP) et la perte des alimentations électriques externes pour les soumettre à une comparaison plus approfondie. Au titre du second critère, il a été décidé d'analyser certaines séquences de fusion du cœur à haute pression, telles que celles induites par la perte de l'alimentation normale en eau, ainsi que des séquences avec bipasse de l'enceinte présentant un risque de rejets précoces et

importants, telles que les séquences de fusion du cœur par rupture de tube de générateur de vapeur (RTGV). Le troisième critère a conduit à sélectionner la dilution homogène du bore. Trois autres familles d'événements initiateurs qui satisfaisaient au dernier critère (perte de source froide, perte de tableaux électriques, et transitoire avec échec de l'arrêt automatique du réacteur sans chute de barres) n'ont pas été examinées en détail, car il a été constaté que les divergences de résultats des EPS pouvaient s'expliquer par certaines différences de conception évidentes des installations.

La comparaison détaillée a été poursuivie jusqu'au niveau des principales séquences de fusion du cœur ou des valeurs minimales de coupure, en essayant au passage d'expliquer les différences observées par une comparaison des données, des spécificités de conception du système, des hypothèses fonctionnelles et thermohydrauliques utilisées dans les analyses de séquences accidentelles, de la construction des arbres d'événements, et de la modélisation des actions humaines.

Un exercice de comparaison des EPS effectuées pour les phases d'arrêt du réacteur a été lancé plus récemment. Dans celui-ci, la comparaison globale ne se limite pas aux événements initiateurs et aux fréquences de fusion du cœur correspondantes, mais concerne également la définition des états de fonctionnement de l'installation, les pratiques d'exploitation et les configurations et disponibilités des systèmes dans ces différents états. De plus, une comparaison détaillée des APRP petite brèche en état d'arrêt à froid a été entreprise. Pour cet exercice de comparaison concernant les phases d'arrêt du réacteur, la version mise à jour de l'EPS pour le palier REP 900 MWe est utilisée.

Enseignements à tirer

Après avoir examiné l'ensemble des différences constatées pour les familles d'événements initiateurs sélectionnées, nous avons tenté de classer et de résumer les informations utiles que l'exercice de comparaison des EPS avait permis d'obtenir et d'en tirer des enseignements pour les mises à jour actuelles ou futures des EPS.

Cette partie présente une synthèse des enseignements que l'on peut tirer pour les états de puissance des réacteurs.

a) Cet exercice de comparaison des EPS a permis, en les confrontant, de corroborer les résultats et les hypothèses qui les sous-tendent pour la plupart des principales séquences accidentelles dans les deux EPS, et de vérifier si celles-ci s'appuyaient sur des hypothèses similaires d'un point de vue fonctionnel.

De fait, la comparaison a fait apparaître de nombreuses similitudes entre les deux études, en termes de résultats et de contributions au risque, comme en termes de méthodologie et d'hypothèses qui sous-tendent l'EPS. En réalité, bien que l'exercice de comparaison des EPS ait davantage porté sur l'identification et l'analyse des divergences, il a montré qu'il existe bien plus de similitudes que de différences entre les deux EPS.

Plus précisément, la comparaison détaillée des APRP grosse brèche, RTGV et perte des alimentations électriques externes a montré que les séquences de fusion du cœur obtenues dans les deux études sont liées aux mêmes fonctions vitales de sûreté avec des hypothèses fonctionnelles similaires pour les systèmes impliqués, tandis que les différences de fréquence de fusion du cœur pouvaient souvent s'expliquer par des spécificités des installations (différences de conception ou de données).

En outre, les événements initiateurs examinés dans les deux études sont globalement identiques, même s'ils sont parfois regroupés dans des familles différentes. Les rares exceptions concernent des événements initiateurs qui n'entraînent pas l'arrêt d'urgence du réacteur ou la mise en route du circuit de refroidissement de secours du cœur et qui n'ont pas été pris en compte dans l'EPS belge, de même que certains événements initiateurs caractérisant la perte de systèmes supports dont la conception diffère (perte de source froide, perte des tableaux électriques).

La constatation de ces nombreuses similitudes a finalement permis de renforcer la confiance dans les modèles et les résultats des EPS.

b) Même si les installations sont globalement similaires, l'exercice de comparaison des EPS a fait apparaître certaines dissimilarités inattendues en termes de conception des systèmes. Ce point peut être illustré par les exemples suivants :

- les lignes d'injection du système d'injection de sécurité basse pression (ISBP) du circuit primaire (CP), dans le réacteur Tihange 1, possèdent une partie commune avec une vanne motorisée qui ne reçoit aucun signal d'actionnement automatique : la possibilité que la vanne se retrouve en position fermée, à la suite d'une erreur humaine pendant un essai ou une opération de maintenance, a un impact important sur les résultats des APRP dans l'EPS belge ;
- les différences de conception du circuit d'aspersion de l'enceinte (EAS), à savoir essentiellement une redondance plus élevée dans Tihange 1 et un déclenchement différent de la phase de recirculation (automatique dans les installations françaises, manuel à Tihange 1), se ressentent clairement sur les résultats des APRP dans les deux EPS ;
- les différences relatives à la capacité de la bache du circuit d'eau alimentaire de secours des générateurs de vapeur (ASG) et aux actions de conduite requises pour réalimenter la bache ASG expliquent certaines divergences importantes entre les résultats obtenus pour la perte des alimentations électriques externes et pour la perte de l'alimentation normale en eau ;
- les différences de conception du circuit de réfrigération intermédiaire et du circuit d'eau brute secourue justifient le fait que la définition et la modélisation des événements initiateurs « perte de source froide » soient différentes.

A cet égard, l'exercice de comparaison des EPS offre une bonne occasion de comparer les différentes options de conception et d'évaluer leur impact sur les résultats des EPS. Il met également en lumière la nécessité de disposer de modèles d'EPS suffisamment détaillés, adaptés aux différents types d'installations.

c) Pour la quasi-totalité des familles d'événements initiateurs examinées, l'exercice de comparaison des EPS a permis de détecter d'importantes différences en termes d'expérience d'exploitation et de données de fiabilité. Les exemples suivants sont caractéristiques :

- en ce qui concerne le retour d'expérience en exploitation, il est utile de mentionner un événement survenu dans une installation qui incite à considérer, dans l'EPS française, un refus à l'ouverture de cause commune de toutes les vannes de décharge du pressuriseur dû à une erreur de maintenance ;
- les différences en termes d'origine des données entraînent des différences en termes de données de fiabilité pour plusieurs composants importants des systèmes et des valeurs différentes du temps de récupération du réseau en cas de perte des alimentations électriques externes, qui ont toutes un impact considérable sur les résultats des EPS ;
- les différences d'opinion des experts entraînent des différences en termes de fréquence des APRP grosse brèche (d'un ordre de grandeur) et en termes de défaillances de cause commune pour les pompes du circuit ASG (qu'on peut regrouper par type de pompe ou par cause de défaillance).

L'impact des deux premiers exemples sur les résultats des EPS démontre l'importance de données spécifiques des installations. Le troisième exemple met en lumière certaines hypothèses ou données pour lesquelles une harmonisation serait souhaitable.

d) L'exercice de comparaison des EPS a fait apparaître certaines différences dans les hypothèses fonctionnelles ou thermohydrauliques, qui se reflètent dans les critères de succès utilisés dans les arbres d'événements.

Il convient de noter que ces différences ont généralement un impact assez faible sur les séquences accidentelles, les hypothèses principales étant globalement identiques dans les deux EPS. Néanmoins, une tentative a été faite pour identifier clairement les hypothèses de base qui diffèrent et pour

déterminer l'intérêt d'une meilleure validation ou de calculs supplémentaires étayant ces hypothèses. Cela pourrait s'avérer très utile pour améliorer la qualité des modèles d'EPS en vue des diverses applications des EPS (par exemple, l'analyse des événements précurseurs).

Quelques exemples caractéristiques sont : l'actionnement des soupapes de protection du circuit secondaire en cas de perte des alimentations électriques externes, quelques critères de succès dans les séquences RTGV (par exemple, pour le système d'injection de sécurité haute pression et le circuit de refroidissement du réacteur à l'arrêt), et l'importance des systèmes supports tels que les systèmes de ventilation dédiés.

e) L'exercice de comparaison des EPS a permis d'identifier certaines différences concernant les choix de modélisation, même si, dans l'ensemble, les modèles étaient assez similaires.

L'analyse détaillée a permis d'évaluer l'impact de chacune des hypothèses de modélisation qui paraissaient différer d'une EPS à l'autre. Elle a permis d'identifier :

- les modèles ou hypothèses qui pouvaient être améliorés dans l'une des études, en tenant compte de ceux utilisés dans l'autre (par exemple, l'amélioration de la modélisation des actions de récupération effectuées par l'équipe de crise dans l'EPS française, la prise en compte dans l'EPS belge de certains événements initiateurs ou états du réacteur qui avaient été négligés, etc.) ;
- les modèles pour lesquels une meilleure harmonisation est souhaitable (par exemple, le type des initiateurs conduisant à la perte des alimentations électriques externes et leur fréquence, la courbe probabiliste du débit de fuite en cas d'APRP par défaillance des joints des pompes primaires, etc.) ;
- les hypothèses de modélisation spécifiques de l'une des études ayant un impact important sur les résultats, qui pourraient également être applicables à l'autre étude (par exemple, l'extension de la durée d'une séquence accidentelle au-delà de 24h, et différents scénarios de rétablissement du courant

alternatif avant fusion du cœur en cas de perte totale des alimentations électriques, hypothèses qui sont toutes deux prises en compte dans l'EPS française).

f) L'exercice de comparaison des EPS a permis de comparer la structure et la complexité des modèles d'EPS.

Cette comparaison a permis aux deux groupes EPS de l'IRSN et de l'AVN d'explorer d'autres méthodes pour définir ou regrouper les événements initiateurs ou pour construire les arbres d'événements. En particulier, certains accidents plus complexes, tels que la perte totale des alimentations électriques et la perte simultanée de l'alimentation normale et de l'alimentation de secours en eau, sont modélisés comme des événements initiateurs séparés avec leurs propres fréquences et leurs propres arbres d'événements dans l'EPS française, tandis que dans l'EPS du réacteur Tihange 1 ces scénarios sont incorporés dans les séquences accidentelles de leurs événements initiateurs d'origine (respectivement, la perte des alimentations électriques externes et la perte de l'alimentation normale en eau).

Un autre exemple, qui a été clairement observé dans les arbres d'événements des RTGV, concerne le choix de construire des classes d'événements soit comme des missions de système uniques dans l'EPS française, soit relativement à des fonctions de sûreté combinant plusieurs options avec différentes missions de système dans l'EPS belge.

De façon générale, il a été conclu que la structure du modèle d'EPS devait être compréhensible pour les autres experts EPS (par exemple, en vue des diverses applications des EPS), mais qu'elle devait éviter une simplification excessive des séquences accidentelles.

g) L'exercice de comparaison des EPS a permis de soumettre les modèles d'EPS à l'examen de spécialistes du domaine, et d'y identifier certains défauts mineurs. Quelques exemples caractéristiques concernent :

- l'association inappropriée d'arbres d'événements pour des séquences

d'APRP induites après une perte des alimentations électriques externes ;

- la modélisation des actions humaines, dans le cas d'une perte totale de l'alimentation en eau, qui ne tient pas compte des procédures de conduite accidentelle spécifiques ;

- certaines séquences accidentelles qui ont été oubliées ou négligées sans justification.

Conclusions

L'exercice de comparaison des EPS a fait apparaître de nombreuses similitudes entre l'EPS française du palier REP 900 MWe et l'EPS belge du REP Tihange 1, non seulement en ce qui concerne les séquences accidentelles principales, mais également pour ce qui est des hypothèses sous-jacentes, de la modélisation et des données. Il est également apparu que les différences constatées pour les séquences accidentelles et leurs valeurs minimales de coupure s'expliquent souvent par des spécificités des installations liées à la conception des systèmes, aux procédures d'exploitation, à l'expérience d'exploitation, etc. C'est pour cette raison que la présente comparaison se révèle très utile pour corroborer les résultats des deux EPS.

Un tel exercice d'évaluation comparative « *a posteriori* » constitue également un pas vers l'harmonisation des EPS, en marge de l'élaboration de directives ou de normes EPS « *a priori* ». En effet, bien que de nombreuses dissimilarités entre les résultats des EPS s'expliquent par des divergences dans la conception et dans les pratiques d'exploitation, le présent exercice de comparaison des EPS a également mis en lumière plusieurs différences en termes de méthodes, de modèles et de données qui ont un impact important sur les résultats des EPS. Les événements initiateurs et leurs fréquences, les données de fiabilité des circuits de sauvegarde, certains choix de modélisation, et certaines hypothèses fonctionnelles ou thermohydrauliques liées aux critères de succès constituent quelques exemples caractéristiques. Il s'agit d'aspects pour lesquels des améliorations du modèle d'EPS seraient souhaitables.

Dossier : Les études probabilistes de sûreté

En pratique, l'IRSN, qui effectue ses propres EPS, tient compte, dans la mesure du possible, des principaux enseignements tirés de la présente comparaison pour la version en cours de mise à jour de l'EPS du palier REP 900 MWe.

Du point de vue d'AVN, cet exercice de comparaison des EPS a fourni des éléments techniques et des arguments pour discuter avec la société belge architecte-ingénieur et l'exploitant belge, dans le cadre de l'évaluation des EPS.

Plus généralement, les Français et les Belges s'accordent à penser qu'un échange de vues fructueux entre experts EPS de différents organismes, qu'ils soient en charge du développement ou de l'évaluation,

peut permettre un enrichissement mutuel des modèles d'EPS et déboucher sur une confiance accrue des autorités réglementaires dans la qualité des modèles d'EPS, en particulier lorsque ceux-ci sont utilisés dans le cadre des applications des EPS (par exemple, pour l'analyse des événements précurseurs) et pour la prise de décision fondée sur une analyse probabiliste des risques.

L'exercice de comparaison des EPS se poursuit actuellement pour les états de pleine puissance et d'arrêt des réacteurs. En outre, cette comparaison a également été élargie à d'autres REP de même conception Framatome, notamment la centrale de Koeberg, avec la participation de l'Autorité de sûreté sud-africaine NNR.

Un outil de gestion et de réglementation de la sûreté : l'EPS

par **Jorma Sandberg**, conseillère principale
et **Reino Virolainen**, directeur du service d'évaluation
des risques – STUK (Helsinki, Finlande)

Vingt ans d'études probabilistes de sûreté en Finlande

En Finlande, l'Autorité de sûreté et de radioprotection (STUK) a introduit et généralisé l'étude probabiliste de sûreté (EPS) en matière de réglementation de la sûreté nucléaire. L'EPS est également un outil de gestion de la sûreté couramment utilisé par les exploitants (centrales électriques).

C'est au début des années 70 que les autorités et les exploitants finlandais ont reconnu les possibilités offertes par les méthodes probabilistes. A partir de 1984, le STUK a formellement exigé des exploitants finlandais qu'ils effectuent des EPS. Les conclusions de ces premières études probabilistes de sûreté lui ont été présentées en 1989.

Le STUK a également demandé que les EPS soient considérées comme des projets internes et qu'elles soient donc réalisées par le personnel de l'exploitant, les consultants externes ne devant être sollicités que pour des tâches spécifiques. L'objectif était de créer un modèle d'EPS vivante facile d'utilisation et constamment actualisé, partant du principe que, si le personnel de la centrale participait aux études probabilistes de sûreté, les conclusions de celles-ci seraient d'autant mieux exploitées. De ces décisions a découlé l'utilisation actuelle de l'EPS dans l'approche éclairée par le risque adoptée par le STUK en matière de réglementation, et par les exploitants en matière de gestion de la sûreté. Par le terme d'approche réglementaire éclairée par le risque, nous désignons un processus de décision réglementaire dans lequel sont pris en compte et se complètent les conclu-

sions des EPS, les critères déterministes et les appréciations techniques. Les méthodes éclairées par le risque visent avant tout à assurer la gestion ciblée, la plus efficace possible, des moyens disponibles pour améliorer la sûreté nucléaire.

Champ d'application des études probabilistes de sûreté

La Finlande recense quatre tranches nucléaires : la société d'énergie TVO possède sur le site d'Olkiluoto deux tranches de conception suédoise, qui fonctionnent grâce à des réacteurs à eau bouillante de 840 MWe fournis par Asea-Atom ; la société Fortum (anciennement IVO) possède sur le site de Loviisa les deux autres tranches, de type russe modifié, qui fonctionnent grâce à des réacteurs à eau sous pression VVER 440 de 500 MWe. Ces quatre tranches ont été mises en service entre 1977 et 1982.

Des modèles d'EPS vivante de niveau 1 et de niveau 2 ont été mis au point par les centrales d'Olkiluoto et de Loviisa. Le niveau 1 inclut le calcul de la fréquence de fusion du cœur du réacteur, probabilité annuelle, et le niveau 2 l'évaluation du volume et de la fréquence des rejets de produits radioactifs dans l'environnement. A l'heure actuelle, les études de niveau 1 en fonctionnement à pleine puissance couvrent les initiateurs internes, les agressions internes (incendies, inondations) et les agressions externes, telles que les conditions météorologiques extrêmes et les événements sismiques. En état d'arrêt ou de fonctionnement à puissance réduite, les EPS de niveau 1 couvrent les initiateurs internes et certaines des agressions



Figure 1 : Centrale d'Olkiluoto

internes et externes ; en état de fonctionnement à pleine puissance, les EPS de niveau 2 couvrent les initiateurs internes et certaines agressions internes.

Le modèle EPS d'Olkiluoto a été mis en œuvre dans le programme SPSA, développé par le STUK. Les centrales de Loviisa ont principalement utilisé le logiciel CAFTA pour leur modèle EPS. Depuis peu, il a été décidé d'adopter le logiciel Risk Spectrum.

Le STUK et les exploitants ont conclu un accord spécial pour que le modèle d'EPS vivante constitue une plateforme d'informations commune. Aux termes de cet accord, le STUK et les exploitants utilisent un même modèle EPS actualisé pour résoudre leurs problèmes de sûreté, ce qui facilite la communication des deux parties dans ce domaine. L'utilisation de ce modèle commun est subordonnée à l'examen rigoureux des modèles EPS par le STUK.

Prescriptions réglementaires

Les lignes directrices relatives à l'application du modèle d'EPS vivante en Finlande sont présentées dans le guide réglementaire YVL 2.8, qui a été publié pour la première fois par le STUK en 1987. Ce guide a été révisé en 2003 afin de tenir compte des avancées réalisées en matière d'EPS. L'EPS

vivante couvre toute la durée de vie de la centrale : elle est formellement intégrée au processus réglementaire des centrales électriques nucléaires dès le début de la phase de conception. Elle est ensuite utilisée durant les phases de construction et d'exploitation, pendant toute la durée de vie de la centrale. (Pour une description générale de l'utilisation de l'EPS vivante dans la réglementation, se reporter à la figure 2).

Conformément aux prescriptions du guide réglementaire YVL 2.8, l'exploitant est tenu de considérer les conclusions de l'EPS dans ses prises de décision, en matière de sûreté dans des centrales en service, sur des sujets tel que :

- la réalisation de modifications et de mises en conformité de la centrale ;
- l'examen et l'amélioration du cahier des spécifications techniques en vue de son amélioration ;
- l'évaluation du classement de sûreté des systèmes et des composants ;
- la planification du programme d'essais périodiques ;
- la planification du programme d'inspection en service ;
- la planification du programme de maintenance en exploitation ;

Dossier : Les études probabilistes de sûreté

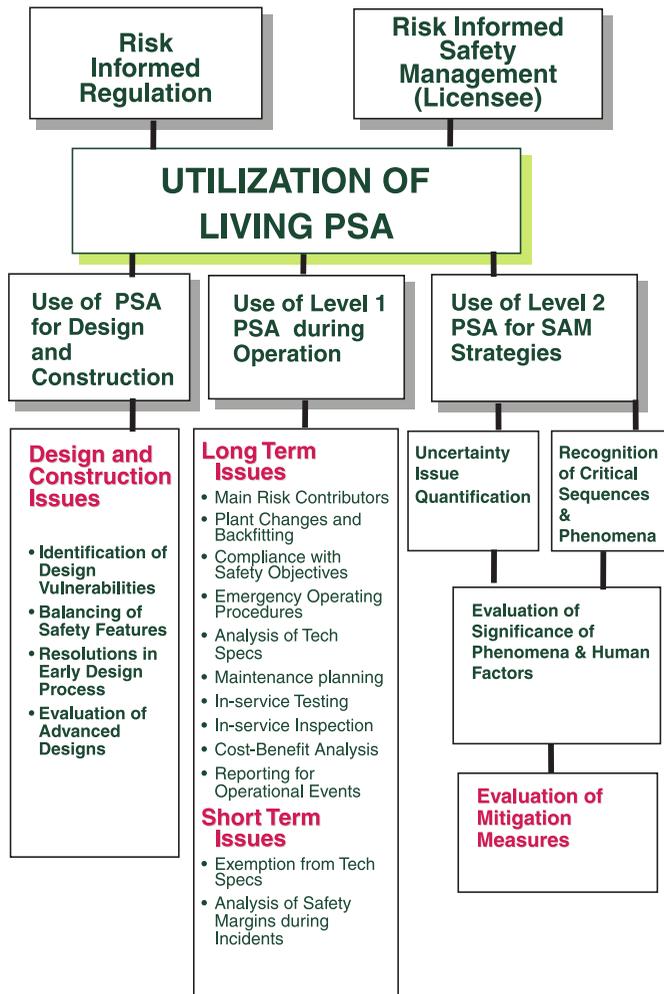


Figure 2 : Utilisation de l'EPS vivante pour une réglementation et une gestion de la sûreté éclairées par le risque

- le recensement des incidents d'exploitation ;
- les procédures de conduite incidentelle et de conduite accidentelle ;
- la formation du personnel ;
- l'évaluation des programmes d'assurance qualité.

Dans le cas d'une nouvelle tranche, l'obtention de l'autorisation de création est subordonnée à la réalisation d'une EPS sommaire de niveaux 1 et 2 et celle de l'autorisation de mise en service à une EPS exhaustive de niveaux 1 et 2.

Modifications de la centrale justifiées par l'EPS

L'EPS joue un rôle déterminant dans l'évaluation des propositions de modification des centrales. L'exploitant est tenu de pré-

senter au STUK une évaluation de l'impact sur la sûreté de chaque modification proposée, quelle que soit la classe de sûreté des systèmes faisant l'objet de la modification. De nombreuses modifications ont d'ores et déjà été réalisées sur la base des conclusions d'EPS de niveau 1, la priorité maximale étant donnée à celles ayant les conséquences les plus importantes sur les risques.

Par exemple, les modifications apportées à la centrale de Loviisa au cours des dernières années ont permis de diviser par dix la fréquence estimée de fusion du cœur du réacteur. Les modifications apportées à la centrale concernent les systèmes de refroidissement du réacteur à l'arrêt, de réfrigération intermédiaire, de sécurité contre l'incendie, et la prévention du blocage de la prise d'eau de mer par des algues ou de la glace.

Outre des modifications matérielles, un nouveau manuel des procédures de conduite accidentelle a été élaboré afin de fournir aux exploitants des lignes directrices devant leur permettre de mieux gérer certaines séquences accidentelles, dont l'importance en termes de risques est indiquée par l'EPS. De nouveaux enseignements, mis en évidence par l'EPS, ont également été intégrés aux programmes de formation des exploitants.

Incidents d'exploitation

Dans le domaine des incidents d'exploitation, l'EPS est couramment utilisée pour évaluer l'importance au plan de la sûreté des défaillances de composants et des incidents. Le suivi des risques est désormais une pratique courante au STUK. Depuis 1995, l'Autorité de sûreté et de radioprotection finlandaise effectuée, chaque année, une étude de suivi des risques systématique dans chacune des tranches nucléaires du pays.

Au vu des conclusions de ces études de suivi, le STUK a fixé un objectif concernant la disponibilité des équipements dans les centrales nucléaires finlandaises en se fondant sur les risques internes. Ainsi, l'indisponibilité des équipements (défaillances de composants, maintenance préventive, dérogations aux spécifications techniques)

devrait compter pour moins de 5% dans la probabilité annuelle de fusion du cœur estimée. Cet objectif appuie la stratégie du STUK visant à réduire le nombre et l'importance des équipements indisponibles dans les centrales nucléaires. La nécessité d'analyser des incidents plus graves (les véritables événements initiateurs) est évaluée au cas par cas, en se référant, par exemple, à l'échelle INES et aux études des incidents.

Évaluation des spécifications techniques d'exploitation

Les exigences et les limitations techniques relatives aux systèmes des centrales nucléaires sont énoncées dans les spécifications techniques d'exploitation. Une grande partie de ces spécifications concerne la limitation des temps d'indisponibilité autorisés pour réparation en cas de défaillance de systèmes ou de composants.

Les conclusions des EPS apportent des arguments en faveur de l'assouplissement des spécifications techniques dans certains cas précis. Lorsqu'un exploitant demande une dérogation temporaire aux spécifications techniques d'exploitation, il est tenu d'en évaluer la portée en termes de sûreté par une EPS. Cependant, pour que la dérogation soit accordée, le léger dépassement du temps d'indisponibilité autorisé ne doit entraîner qu'une faible augmentation de la probabilité de fusion du cœur du réacteur par rapport au fonctionnement normal. La procédure de délivrance de dérogations recourt à des analyses déterministes et probabilistes comme méthodes complémentaires.

La pertinence des temps d'indisponibilité autorisés prévus dans les spécifications techniques d'exploitation a été revue à la lumière des EPS. Certaines incohérences ont ainsi été identifiées entre différents systèmes de sûreté dans la définition des temps d'indisponibilité autorisés par rapport à leurs conséquences sur les risques. Après analyse, il a, par exemple, été démontré qu'une défaillance sur un sous-système doublement redondant du circuit d'eau brute comporte plus de risque qu'une défaillance sur un sous-système quadruplement redondant du circuit d'alimentation de secours des générateurs de

vapeur. De plus, il a été relevé certaines asymétries entre plusieurs combinaisons de défaillances similaires de sous-systèmes. Par exemple, à la centrale d'Olkiluoto, les combinaisons de doubles défaillances des voies A et B dans le circuit d'eau brute ne sont pas identiques à celles des voies A et C. Cette asymétrie peut s'expliquer par la plus grande sensibilité aux initiateurs de cause commune, tels que les incendies et les inondations, des voies A et C, comparée à celles des voies A et B, en raison de différences de séparation physique.

L'analyse des risques a également remis en cause l'idée conventionnelle selon laquelle, dans tous les cas de défaillance, l'arrêt de la centrale constitue la solution la plus sûre. Si des dégradations se produisent dans les circuits utilisés pour l'évacuation de la chaleur résiduelle, il peut être plus sûr de poursuivre l'exploitation que de procéder à l'arrêt immédiat de la centrale, même si l'arrêt est préconisé dans les spécifications techniques d'exploitation en vigueur. Au vu des études de risques, un exploitant a ainsi demandé que certaines modifications soient apportées aux spécifications techniques d'exploitation pour certaines configurations de centrales (incluant une indisponibilité de voies spécifiques des circuits de sûreté).

Au vu des résultats de l'EPS concernant les états d'arrêt de la centrale d'Olkiluoto en phase d'EPS, le STUK s'est empressé de demander la modification des spécifications techniques d'exploitation relatives à ces états. Selon les nouvelles prescriptions demandées, le sas de l'enceinte de confinement doit être fermé pendant la maintenance des pompes primaires principales. Des erreurs de maintenance pourraient provoquer une fuite importante dans la partie inférieure de la cuve du réacteur via le point de raccordement de celle-ci avec la pompe. Si une fuite de ce genre se produisait et que le sas inférieur était ouvert, l'eau s'échapperait de l'enceinte de confinement et empêcherait alors toute action de refroidissement, provoquant une fusion rapide du cœur. Ce problème est typique des réacteurs à eau bouillante modernes fonctionnant avec des pompes primaires principales internes. La probabilité qu'une erreur de maintenance entraîne une fuite

importante est extrêmement faible ; cependant, si le phénomène survenait, il n'y aurait quasiment aucune possibilité de le contrer. De plus, l'ouverture de la cuve du réacteur et de l'enceinte de confinement aggraverait les conséquences radiologiques.

Analyse de la maintenance préventive

Le STUK autorise la maintenance préventive durant le fonctionnement en puissance à condition que les critères déterministes de sûreté soient remplis (par exemple : critère de défaillance unique) et que la contribution aux risques soit faible. La maintenance en exploitation permettrait de réduire les risques liés à l'arrêt du réacteur et d'augmenter la fiabilité des composants qui en font l'objet. Cependant, la majorité des procédures de maintenance sont effectuées pendant la révision annuelle.

Les EPS permettent de réduire les risques résultant de la maintenance préventive en exploitation. La centrale REB d'Olkiluoto, avec ses quatre voies de sûreté redondantes A, B, C et D en parallèle, fournit un exemple d'optimisation de la maintenance préventive en exploitation. La capacité de ces systèmes de sûreté est de $4 \times 50\%$. Sur le site d'Olkiluoto, la mise hors service successive de l'un des quatre sous-systèmes redondants est autorisée.

Selon la première EPS d'Olkiluoto, en 1989, la contribution au risque de la maintenance préventive en exploitation représentait environ 5% de la fréquence globale de fusion du cœur. Lorsque le programme de maintenance a été optimisé à l'aide des EPS, celle-ci a pu être ramenée à moins de 1% de la fréquence globale de fusion du cœur.

Analyse des inspections et des contrôles en service

La surveillance des tuyauteries d'une centrale nucléaire, notamment des joints soudés, exige des contrôles non destructifs, tels que les ultrasons ou les courants de Foucault. Ces contrôles sont très consommateurs de temps et d'argent, et exposent, en outre, les personnes qui en sont char-

gées à de fortes doses d'irradiation. Aussi les objectifs de ces inspections doivent-ils être définis avec précision. Les exigences en matière d'inspection en service font l'objet de normes, telles celles de l'ASME, mais des méthodes probabilistes peuvent être utilisées pour une sélection plus efficace des joints soudés devant être inspectés.

Des projets pilotes en matière d'inspection en service des tuyauteries d'une centrale REP (Loviisa) et d'une REB (Olkiluoto) ont été menés à bien par le STUK, en collaboration avec les exploitants. La procédure éclairée par le risque du STUK associe les données spécifiques de la centrale fournies par l'EPS et les considérations conventionnelles pour justifier la planification du programme détaillé d'inspection en service des systèmes.

La procédure comprend plusieurs étapes : sélection des systèmes, évaluation des mécanismes de dégradation des tuyauteries, évaluation des conséquences des ruptures de tuyauteries et catégorisation des tronçons de tuyauteries.

Le classement des tronçons de tuyauteries en différentes catégories de dégradation se fonde principalement sur l'appréciation qualitative du mécanisme de dégradation auquel ils sont exposés. Jusqu'à présent, peu de méthodes probabilistes de mécanique de la rupture ont été présentées pour calculer les probabilités de rupture des canalisations. Le recours à l'avis et à l'expérience d'un expert en matière de défaillance de canalisation constitue donc une alternative pour déterminer dans quelle catégorie de dégradation chaque segment doit être classé.

Le classement des tronçons de tuyauteries en différentes catégories de conséquences se fonde sur la probabilité conditionnelle de fusion du cœur définie par les EPS. Les tronçons de tuyauteries sont divisés en différentes catégories : tronçons à risque élevé, moyen et faible, puis le groupe d'experts combine les informations conventionnelles et probabilistes. Au sein de ce groupe, figurent des experts de différents domaines : conception, exploitation, maintenance, ingénierie des structures et du matériel, étude probabiliste de sûreté et inspection en service.

Dossier : Les études probabilistes de sûreté

L'étude pilote sur les inspections en service a joué un rôle majeur dans l'évolution des méthodes probabilistes d'évaluation des risques, en fournissant des lignes directrices pour leur développement et en permettant la définition d'une nouvelle stratégie de contrôle pour les systèmes concernés. La pertinence de la méthode et des orientations données en matière d'EPS sera évaluée à la lumière des résultats de ce projet pilote. Sa mise en place devrait aboutir à une sûreté accrue et à une utilisation plus efficace des moyens réglementaires et, dans le cas d'une véritable optimisation de la méthode, à une réduction du fardeau réglementaire inutile et des coûts supportés par l'exploitant.

L'EPS peut également être utilisée pour optimiser les contrôles en service des systèmes de centrales nucléaires. Par exemple, au vu des conclusions des EPS, des modifications ont été apportées à certaines procédures de contrôle des générateurs diesels de la centrale d'Olkiluoto, afin de réduire les effets négatifs des contrôles sur le vieillissement des équipements.

Conclusion

L'EPS s'est imposée comme un précieux outil d'aide à la décision dans le développement des systèmes et des procédures d'exploitation des centrales nucléaires. Les possibilités et les limitations de l'analyse de risques sont bien établies. Certaines applications sont déjà d'utilisation courante ; d'autres ont encore besoin d'être développées. L'Autorité finlandaise de sûreté et de radioprotection (STUK) a pour objectif de parvenir à un usage extensif des méthodes éclairées par le risque, où les approches déterministe et probabiliste se complètent de manière équilibrée.

En 2002, le Parlement finlandais a donné son aval pour que la société d'énergie TVO construise une nouvelle tranche nucléaire à Olkiluoto ou Loviisa. TVO a reçu des offres pour un réacteur d'une gamme de puissance de 1000 à 1600 MW. Une autorisation de création devrait être demandée fin 2003. Les EPS et l'intégration de la prise en compte des risques devraient être utilisées dès le début de la procédure d'autorisation de cette nouvelle tranche.

Enjeux et perspectives dans un environnement éclairé par le risque

par **Jeffrey S. Merrifield**, membre de la Commission américaine de réglementation de l'énergie nucléaire (U.S. Nuclear Regulatory Commission) – NRC

Introduction

La prise en compte des risques dans nos processus réglementaires continue de se développer et joue un rôle croissant dans l'approche adoptée au sein de la Commission américaine de réglementation de l'énergie nucléaire (NRC - *U.S. Nuclear Regulatory Commission*). Au cours de ces dernières années, nous avons consacré à cette tâche une part importante de notre temps et de nos moyens, afin de mieux adapter notre travail et notre cadre réglementaire aux aspects qui sont les plus significatifs pour la sûreté. En éclairant notre réglementation par des analyses de risque et en intégrant la prise en compte des risques à nos processus de décision, nous avons amélioré la sûreté en permettant à la NRC et aux exploitants de concentrer leur attention et leurs moyens sur les problèmes de conception et d'exploitation les plus importants pour la sûreté. Cependant, nous devons nous montrer attentifs à la manière dont sont perçues nos initiatives probabilistes. Pour l'opinion publique, elles répondent à une volonté de réduire le fardeau réglementaire, au risque de faire passer la sécurité au second plan. Bien qu'il y ait sans doute matière à alléger le fardeau réglementaire, notre premier objectif reste celui de la sûreté. Nous devons donc relever un défi de taille : comment présenter à nos partenaires extérieurs de façon précise et responsable les initiatives que nous prenons pour prendre en compte de façon précise et responsable les risques dans nos actions ?

A ce sujet, je souhaiterais m'arrêter sur trois points :

1) les récentes avancées de la NRC dans certains domaines fondamentaux de la prise en compte des risques ;

2) mes remarques concernant l'intégration de la prise en compte des risques dans l'exploitation quotidienne d'une centrale nucléaire ;

3) mon point de vue sur le rôle que la NRC et l'industrie nucléaire devraient jouer dans la diffusion des initiatives prises dans ce domaine.

Avancées

Lorsque la NRC s'est attelée à l'élaboration du nouveau programme de surveillance des réacteurs à la fin des années 90, l'industrie nucléaire faisait preuve d'une efficacité accrue dans le domaine de la sûreté, mais la méthode d'évaluation des performances des exploitants, fondée essentiellement sur leur respect de la réglementation, se révélait obsolète. Nous avons pris conscience du fait que la procédure qui nous avait été utile pendant de si nombreuses années était désormais dépassée : elle était très subjective et dépendait trop de l'appréciation de nos inspecteurs. Dans de nombreux cas, ceux-ci consacraient trop de temps (le leur et celui des exploitants) à des questions ne revêtant pas d'importance en termes de risque, et trop peu à d'autres constituant, en revanche, un risque important pour la sûreté. Certains inspecteurs ont ainsi conduit des programmes d'actions correctives, dans lesquels le respect de la réglementation prenait le pas sur la sûreté, ce qui, il faut bien l'avouer, n'était pas toujours dans le meilleur intérêt de la population.

Quelque chose manquait : un processus plus objectif, plus respectueux des délais et plus prévisible de suivi des performances des exploitants, intégrant la prise en compte des risques. Le nouveau programme de surveillance des réacteurs, mis en

place par la NRC en 2000, a constitué un progrès majeur dans notre capacité à identifier les problèmes de performances et à garantir que les exploitants prenaient les mesures appropriées avant que les performances de la centrale ne soient affectées. La principale originalité de ce processus résidait dans le recentrage des moyens d'inspection sur les questions qui présentaient le plus d'importance en matière de sûreté. J'estime que la prise en compte et l'analyse des données des indicateurs de performance conjuguées aux résultats des inspections et des évaluations éclairées par le risque constituent une avancée importante dans la mise en œuvre du programme, et ont amélioré la fonction de surveillance que nous exerçons.

Afin d'aider nos inspecteurs, nous avons conçu un processus de présélection éclairée par le risque, dont les grandes lignes sont exposées dans les registres d'inspection de chaque centrale nucléaire. Ce processus de présélection intègre des informations sur les risques spécifiques de la centrale qui aident nos inspecteurs à évaluer la portée des différents résultats obtenus au regard de la sûreté nucléaire. A l'heure actuelle, la présélection est un processus lourd, dont les résultats sont souvent tardifs. Nous continuons néanmoins d'améliorer la version initiale des registres en menant à bien un processus d'étalonnage pour chacune des centrales nucléaires en service. En outre, nous allons accélérer et étalonner nos modèles d'analyse des risques types, qui sont un instrument plus précis pour procéder à des évaluations indépendantes des incidents et des changements proposés au sein de la centrale. Ces améliorations permettront de pallier les incohérences du programme actuel et de supprimer ainsi l'instabilité et l'imprévisibilité réglementaires.

La Commission a également pu se réjouir d'une autre grande avancée en 2001 en autorisant, après instruction, la centrale nucléaire *South Texas Project* à déroger à certaines exigences réglementaires concernant le traitement particulier de structures, systèmes ou composants.

Ces exigences incluent notamment une inspection spécifique, ainsi que des programmes de contrôle et d'assurance qualité qui visent à garantir la qualité et la fiabilité des structures, des systèmes et des composants liés à la sûreté ou importants à cet égard. L'exploitant de la centrale *South Texas* s'est livré à un processus d'examen rigoureux destiné à déterminer quels étaient les structures, systèmes et composants de moindre importance en matière de sûreté, puis il a soumis des demandes d'exemption de certaines exigences réglementaires. Le processus d'examen a consisté en une catégorisation des structures, systèmes et composants, et en leur traitement différencié, conformément à leur catégorisation. Pour mener à bien cette catégorisation, nos employés et ceux du *South Texas Project* se sont principalement appuyés sur une étude probabiliste exhaustive de la sûreté, et sur la prise en compte de certains aspects déterministes. Cet examen a confirmé la nécessité d'une catégorisation précise et d'une évaluation probabiliste fiable des risques. En approuvant ces exemptions, la NRC a réalisé une avancée notable et prouvé sa volonté d'adopter une approche réglementaire intégrant la prise en compte des risques.

Je pense que les enseignements tirés des demandes du *South Texas Project* ont fortement contribué à modeler les nouvelles règles relatives à la prise en compte des risques qui ont récemment été proposées. Celles-ci visent à modifier la réglementation de la NRC, afin d'assouplir, dans nos centrales, les exigences de l'application du traitement particulier pour les matériels de sûreté à faible risque⁽¹⁾. Ces nouvelles règles, si elles sont approuvées, adopteront une approche similaire à celle du *South Texas Project* et permettront aux exploitants d'entreprendre la catégorisation de leurs structures, systèmes et composants en tenant compte des risques, et d'adapter les prescriptions de traitement en fonction de leur importance. Selon cette approche, les exploitants seraient autorisés à limiter les exigences de traitement particulier pour les structures, systèmes et composants considérés comme

1. 10 CFR 50.69 Catégorisation et traitement éclairés par le risque des structures, systèmes et composants.

non déterminants au plan de la sûreté, et devraient renforcer les exigences pour les équipements considérés, en revanche, comme particulièrement importants pour la sûreté d'une installation. Cela est, malheureusement, beaucoup plus facile à dire qu'à faire. Le processus de décision a été lent et difficile car la mesure proposée et les orientations qu'elle implique doivent satisfaire à tous les critères d'autorisation et à toutes les conceptions de réacteur, actuelles et futures. Cependant, je suis heureux que la mesure proposée ait fait l'objet d'une consultation publique en mai 2003.

Il convient de souligner que cet effort de réglementation, s'il vise à garantir que le champ d'application des prescriptions de traitement particulier des structures, systèmes et composants prenne en compte les risques, n'a pas pour objectif de permettre la suppression des exigences de fonctionnement, ou d'accepter que des matériels requis par la conception déterministe classique disparaissent de la centrale. En revanche, en modifiant la réglementation actuelle dans le but de permettre l'adoption d'une autre approche du traitement particulier prenant en compte les risques, la nouvelle réglementation devrait permettre aux exploitants et au personnel de la NRC de concentrer leurs moyens sur les structures, les systèmes et les composants qui contribuent de manière significative à la sûreté de la centrale.

Autre grand projet en cours à la NRC en matière de sûreté : notre effort pour éclairer par le risque les spécifications techniques dans notre réglementation. Nous nous sommes d'abord concentrés sur la révision de la réglementation de la NRC relative aux spécifications en matière de contrôle des gaz combustibles⁽²⁾, notamment de l'hydrogène, dans le cas de certains accidents hypothétiques. Le personnel de la commission a proposé une modification de la réglementation en août 2002 qui visait à supprimer les spécifications relatives aux recombineurs et aux circuits

de purge de l'hydrogène, ainsi qu'à assouplir les spécifications relatives aux dispositifs de contrôle de l'hydrogène et de l'oxygène afin d'accorder leur traitement à leur importance en matière de sûreté. Je pense que, après révision, la réglementation permettra d'atteindre l'objectif de faire en sorte que les dispositions relatives aux gaz combustibles soient éclairées par le risque et fondées sur les performances.

Le personnel de la commission travaille également à une approche probabiliste des critères d'acceptation des circuits de refroidissement de secours du cœur⁽³⁾. Il s'agit là de notre plus grand défi à ce jour en matière d'intégration des risques dans la réglementation. Car ce sont sur ces critères que reposent les réglementations de la NRC concernant les circuits de refroidissement de secours du cœur dans les cas d'accidents de perte de réfrigérant primaire. Or, depuis leur établissement, et durant leur application au cours de ces vingt dernières années, ces critères se sont fondés sur des hypothèses conservatives et des données limitées.

Les changements envisagés visent principalement à fournir (1) une alternative aux critères prescriptifs d'acceptation des circuits de refroidissement de secours du cœur, pour les fonder sur les performances, (2) une alternative aux exigences de fiabilité des circuits de refroidissement de secours du cœur pour mieux les adapter à la fréquence de sollicitation de leur fonction de sûreté, (3) une redéfinition du spectre des dimensions des brèches des canalisations.

Cependant, ma philosophie, en ce qui concerne les exigences relatives au circuit de refroidissement de secours du cœur, peut se résumer ainsi : n'effectuer aucun changement qui n'ait été précisément étudié car la population aurait alors l'impression que la mesure proposée n'a pas de fondement technique solide et ne s'appuie pas sur des recherches probantes. Si elle peut constituer pour certains un moyen tentant pour arriver rapidement à réduire

2. 10 CFR 50.44 Normes des systèmes de contrôle des gaz combustibles dans les réacteurs de puissance à refroidissement à eau légère.

3. 10 CFR 50.46 Critères d'acceptation des systèmes de refroidissement de secours du cœur pour les réacteurs nucléaires de puissance à eau légère.

le fardeau réglementaire inutile, une action prématurée, dénuée de tout fondement technique solide, impliquerait que nous connaissions les solutions avant d'achever les essais techniques. De plus, elle mettrait en péril les efforts que nous déployons pour gagner davantage la confiance du public. Cette confiance est stimulée non seulement par l'existence de bases techniques solides, mais aussi par un dialogue ouvert et honnête avec nos partenaires, en ce qui concerne nos initiatives de prise en compte des risques. Parce que nous laissons à notre personnel le temps nécessaire pour résoudre les problèmes techniques, je suis sûr que nous sommes sur la bonne voie pour gagner la confiance du public. Si nous agissions avec précipitation aujourd'hui, nous risquerions d'entamer la confiance de nos partenaires en n'offrant pas au public la possibilité de se prononcer sur la position définitive de nos services.

Intégration de la connaissance des risques dans l'exploitation quotidienne des centrales

A présent, je voudrais évoquer le rôle de la prise en compte des risques dans l'exploitation quotidienne des centrales. Durant mes quatre premières années à la commission, j'ai eu l'occasion de visiter les sites des 103 centrales nucléaires en service aux Etats-Unis. Lors de ces visites, j'ai été surpris par la multitude de façons dont les exploitants prennent en compte les risques dans la gestion et l'exploitation de leurs installations. Certains intègrent l'éclairage probabiliste des risques dans la quasi-totalité des activités quotidiennes de la centrale, y compris dans la planification de la maintenance et le contrôle de la configuration. Ils disposent d'EPS temps réel qui fournissent un état des risques aux opérateurs et aux analystes de contrôle du travail, et ils communiquent à l'ensemble des employés par voie d'affichage dans toute la centrale les informations relatives aux risques de leur environnement actuel. Ils ont également intégré la prise en compte des risques dans les durées d'indisponibilité des matériels et les intervalles entre les

contrôles périodiques. Cependant, dans d'autres centrales, la prise en compte des risques n'en est encore qu'à ses débuts et il est évident que leurs exploitants n'ont pas l'intention de l'utiliser au-delà de ce qui est nécessaire pour satisfaire leurs obligations réglementaires.

Au fil des discussions et des observations, j'ai constaté avec plaisir que la plupart des directeurs de centrale considéraient l'intégration des risques comme un vecteur d'amélioration de la sûreté et un outil de gestion fondamental. Beaucoup d'entre eux m'ont affirmé que la prise en compte des risques faisait désormais partie intégrante de leur culture et qu'elle avait changé leur mode de travail. Pour ces directeurs, toutes les conséquences en matière de sûreté entraînées par des propositions de modifications de la centrale sont évaluées de manière intégrée, dans le cadre d'une approche globale de gestion des risques. Ils s'appuient sur l'analyse des risques pour améliorer la prise de décision au plan de l'exploitation et de l'ingénierie, en identifiant et en mettant à profit les occasions de réduire les risques. Ils utilisent des EPS temps réel pour déterminer les périodes d'indisponibilité des systèmes ou des composants résultant d'une maintenance préventive ou de contrôles périodiques. Dans ces cas, les analyses de risques complètent les approches d'ingénierie conventionnelles dans le processus de décision. Le risque ne détermine pas à lui seul la décision, mais il revêt une importance de plus en plus grande dans celle-ci. Pour ces directeurs de centrale, l'utilisation accrue de l'analyse de risques ne permet pas seulement une exploitation plus sûre des centrales, elle est aussi économiquement rationnelle.

Dans d'autres centrales, il n'est pas certain que la prise en compte des risques aille au-delà de l'obligation de satisfaire aux exigences réglementaires, comme celles qui concernent la maintenance⁽⁴⁾ ou le programme de surveillance des réacteurs. Je le regrette. Comme l'expérience l'a déjà montré, c'est là manquer une occasion d'améliorer la sûreté des centrales, mais aussi d'en tirer des avantages économiques.

4. 10 CFR 50.65 Exigences en matière de contrôle de l'efficacité de la maintenance dans les centrales nucléaires.

Il est essentiel que les exploitants conçoivent et adoptent de meilleures pratiques d'utilisation des méthodes éclairées par le risque afin d'évaluer l'importance et le caractère prioritaire des éléments de leur travail quotidien. Les exploitants doivent mettre au point les outils appropriés pour mesurer les implications de leurs actions en termes de risques. Pourtant, du fait que la prise en compte des risques et les conclusions des études probabilistes de sûreté (EPS) jouent un rôle croissant dans la gestion des centrales, le besoin d'une EPS encore plus fiable se fait sentir. Cela aura un coût : la portée, le degré de précision et la qualité des EPS doivent être à la hauteur des objectifs visés. A l'issue des consultations que j'ai organisées avec les principaux acteurs du secteur, il apparaît clairement que les bénéfices futurs dépassent de beaucoup les coûts prévus.

Communication

La communication constitue actuellement un important défi à relever pour la NRC. Si nous avons réalisé des progrès dans ce domaine, notamment avec le programme de surveillance des réacteurs et la diffusion d'informations à nos partenaires extérieurs via notre site Internet, il nous reste encore fort à faire. Dans son ensemble, l'industrie nucléaire reste réactive plutôt que proactive dans sa manière de communiquer, ce qui limite notre aptitude à transmettre efficacement des informations au public sur le risque et ses implications.

Nous pouvons avoir la connaissance des risques la plus avancée, le savoir-faire le plus affiné, disposer des meilleurs spécialistes du domaine, si nous n'avons pas un plan de communication efficace, nous échouons. Ce n'est qu'en apprenant à communiquer efficacement avec le public et leurs partenaires sur le risque et ses conséquences que la NRC et l'industrie nucléaire parviendront à concevoir une réglementation éclairée par le risque et à utiliser la prise en compte des risques pour alléger le fardeau réglementaire inutile. Pour la plupart de nos partenaires, et même de nos employés, le risque reste une inconnue, un mystère. Comme souvent pour le public, lorsqu'il s'agit de science et de technique, l'incertitude entraîne l'appréhension, et l'appréhension la peur.

D'autres partenaires, y compris certains groupes de pression et quelques membres du Congrès, accueillent avec scepticisme les efforts que nous déployons aux fins d'une approche réglementaire éclairée par le risque. Pour eux, les initiatives que nous prenons en matière de risque ne sont qu'une nouvelle astuce de l'industrie nucléaire et de la NRC pour assouplir les exigences réglementaires. Rien ne saurait être plus loin de la vérité.

Il est impératif que la NRC et l'industrie nucléaire abordent la question du risque d'une façon qui la rende plus compréhensible pour nos partenaires et permette de gagner leur confiance. Nous devons démontrer qu'une approche éclairée par le risque de la réglementation ne signifie en aucune manière un engagement moindre en matière de sûreté. En réalité, une telle approche conduit à un engagement encore plus grand car elle permet à la NRC et aux exploitants de concentrer leurs moyens sur les points les plus importants en termes de risque. D'un point de vue cumulatif, des problèmes de communication mineurs peuvent aboutir à une baisse de la confiance du public. Si nous voulons tirer profit de notre meilleure expertise en matière de risques, nous ne pouvons nous permettre de délaissier la communication.

Conclusion

Théodore Roosevelt a, en son temps, déclaré : « Dans tout moment de décision, la meilleure chose que vous puissiez faire est la bonne, la seconde meilleure chose que vous puissiez faire est la mauvaise, et la pire que vous puissiez faire est rien du tout ». Le succès de nos initiatives éclairées par le risque dépend des décisions que nous prenons aujourd'hui pour soutenir les efforts engagés. Au cours de ces dernières années, nous avons étendu notre prise en compte des risques, nous avons allégé le fardeau réglementaire inutile et nous avons rendu nos processus réglementaires plus objectifs, mais il nous reste encore beaucoup à faire. La réglementation pourrait ainsi être renforcée et des moyens être alloués pour qu'elle se concentre sur les matériels et les activités les plus importants en termes de risques, et qu'elle assure un cadre cohérent pour le processus de décision réglementaire.

L'EPS dans la réglementation nucléaire de l'Afrique du Sud

par **T. Hill**, National Nuclear Regulator (Cape Town, Afrique du Sud)



Introduction

L'Autorité de sûreté nucléaire sud-africaine (NNR – *South African National Nuclear Regulator*) définit le cadre réglementaire des activités qui impliquent l'utilisation de produits radioactifs et constituent un risque pour le public ou le personnel d'une centrale. Elle réglemente ainsi la plupart des étapes du cycle du combustible nucléaire, depuis l'extraction jusqu'à la fabrication des assemblages combustibles, et gère également les deux REP de 900 MWe de la centrale de Koeberg, un réacteur de recherche et des centres de stockage définitifs.

Au début des années soixante-dix, des normes fondamentales de sûreté ont été expressément définies par le prédécesseur de NNR pour l'autorisation de création de la centrale de Koeberg. Ces règles, qui incluent des critères de risques, ont, par la suite, été appliquées à la réglementation des installations nucléaires. Dans la mesure où les seuls critères quantitatifs imposés par la NNR sont d'ordre « radiologique », l'approche sud-africaine en matière d'autorisation a donc été définie comme purement « fondée sur le risque ». Comme cela est exposé ci-après, ce point n'est pas tout à fait exact et doit être reconsidéré.

Une EPS de niveau 3 a été réalisée sur les deux réacteurs à eau sous pression (REP) de 900 MWe de Koeberg à la fin des années soixante dix. Cette étude a porté sur les risques encourus en phase de puissance ou d'arrêt, ainsi que sur les accidents non liés au réacteur concernant, par exemple, l'entreposage du combustible usé, la manutention du combustible ou les activités de traitement des déchets.

L'EPS de la centrale de Koeberg a été revue en 1991 après l'informatisation du niveau 1 grâce à des logiciels mis au point par la société exploitante Eskom. Des examens par des pairs ont été effectués entre 1994 et 1996.

Le réexamen de sûreté de Koeberg mené entre 1996 et 1998 s'est accompagné d'un examen approfondi, visant notamment à étalonner l'EPS de Koeberg sur le modèle français de l'EPS-900 (EPS de niveau 1) et sur l'évaluation indépendante (IPE – *Independent Plant Evaluation*) de la centrale de North Anna (EPS de niveau 2).

A partir de 1984 environ, des EPS ont été réalisées pour d'autres installations nucléaires du pays, dont un réacteur de recherche, des sites de fabrication du combustible et d'autres types d'installations. L'EPS menée sur le réacteur de recherche a

fait l'objet d'un réexamen de sûreté à partir de 1997-1998 et une nouvelle EPS de référence a été développée.

Des évaluations des risques pour le public ont, par ailleurs, été effectuées sur les sites d'extraction et de traitement des minerais. Bien que ces études aient été concentrées essentiellement sur l'impact environnemental, des facteurs de risques ont été pris en compte.

L'EPS joue, par conséquent, un rôle déterminant dans le cadre réglementaire de l'industrie nucléaire sud-africaine depuis plusieurs décennies, en couvrant une large gamme d'activités dans ce secteur et en se révélant fondamentale dans le processus de prise de décision réglementaire.

EXIGENCES REGLEMENTAIRES

Les normes fondamentales de sûreté édictées par la NNR incluent des limites de dose pour le public et le personnel de la centrale dans des conditions d'exploitation normale, des critères de risques en termes de risque individuel et de risque pour la population (tableau 1), adaptés pour le cas d'accidents plus graves, la défense en profondeur et l'application du principe ALARA. D'une manière générale, les exigences en matière d'autorisation requièrent que la conception et les règles d'exploitation de la centrale respectent les normes et les pratiques reconnues au plan international en matière de sûreté, et qu'une évaluation quantitative des risques soit effectuée pour en attester. Les exigences de la NNR en matière d'évaluation des risques sont énoncées dans le « texte d'autorisation » (ou directive) LD-1091.

Les exigences énoncées dans la directive LD-1091 concernent les points suivants :

1. le développement et la mise à jour d'une EPS de référence pour la centrale et la mise en évidence du respect des critères de risques définis par la NNR ;
2. les exigences relatives à la base de données des EPS, s'agissant de l'utilisation des données génériques et spécifiques de la centrale, obtenues grâce aux programmes de maintenance et de contrôle, ainsi que celles concernant l'analyse des causes pro-

fondes des événements et la formation des exploitants ;

3. le domaine de couverture de l'EPS :

- l'ensemble des activités effectuées sur le site, y compris la manutention, l'entreposage et l'utilisation des produits radioactifs,
- la base de données de fiabilité,
- l'étude des événements initiateurs,
- l'analyse de la fiabilité des matériels,
- la quantification des séquences incidentelles au niveau de la centrale,
- l'évaluation du terme source,
- l'étude d'impact sur l'environnement (EPS de niveau 3),
- le risque pour les opérateurs ;

4. le développement et l'utilisation d'un système de gestion des risques afin de tenir compte de leur évolution ;

5. La procédure d'assurance qualité.

LA PRISE DE DECISION EN MATIERE DE SURETE

L'exploitant est tenu de se conformer aux exigences déterministes correspondant à la conception et aux règles générales d'exploitation de la centrale, conformément aux pratiques reconnues au plan international. Les exigences en matière de conception s'appliquent à différentes conditions d'exploitation de la centrale, comprenant les conditions normales d'exploitation et les « accidents crédibles ». S'agissant des réacteurs de puissance, ces accidents sont définis comme des événements d'une fréquence annuelle supérieure à 10^{-6} , généralement déterminée selon des conservatismes.

De plus, l'EPS de référence de la centrale doit servir à attester le respect des critères quantitatifs de risques et de doses suivants :

- conditions normales d'exploitation : tableau 1 ;
- conditions accidentelles : tableau 1, en incluant la prévention des accidents de plus grande ampleur (figure 1) et les exigences qualitatives définies ci-après.

Dossier : Les études probabilistes de sûreté

	ACCIDENTS	EXPLOITATION NORMALE
TYPE D'ÉVALUATION	PROBABILISTE	DETERMINISTE
POPULATION		
RISQUE MOYEN :	10^{-8} accidents mortels par personne par an (par site)	Contrôlé par application du principe ALARA
RISQUE INDIVIDUEL :	5×10^{-6} accidents mortels par an	Dose effective de 250 Sv/an reçue par un membre du groupe critique
PERSONNEL DE LA CENTRALE		
RISQUE MOYEN :	10^{-5} accidents mortels par an	Contrôlé par application du principe ALARA
RISQUE INDIVIDUEL :	5×10^{-5} accidents mortels	20 Sv/an

Tableau 1 : critères de risques

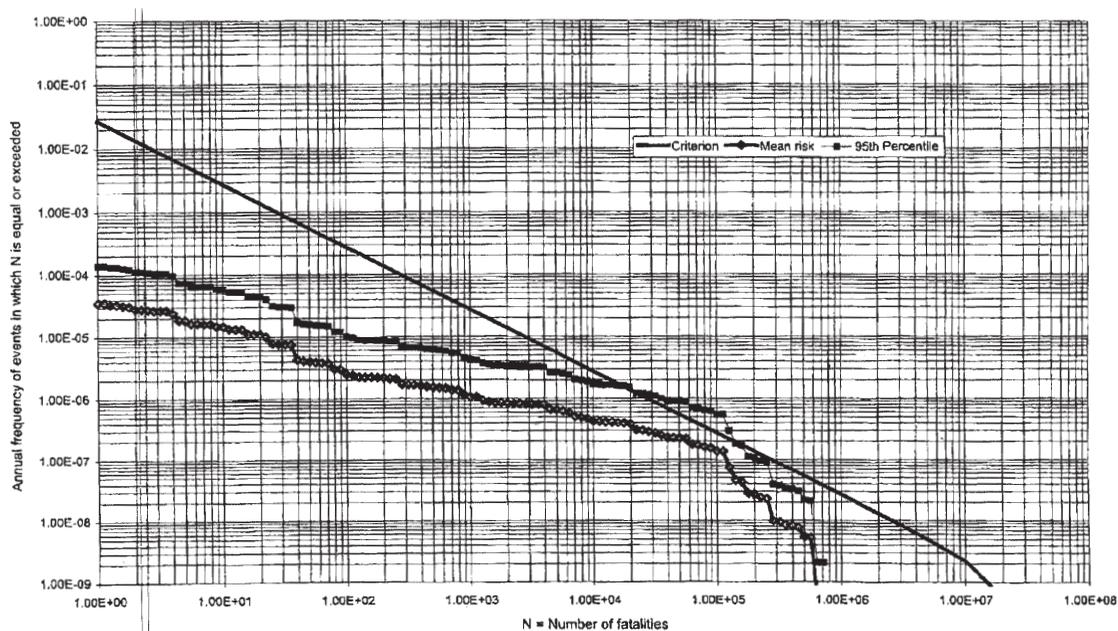


Figure 1 : Critères de risques et conséquences pour l'installation nucléaire,

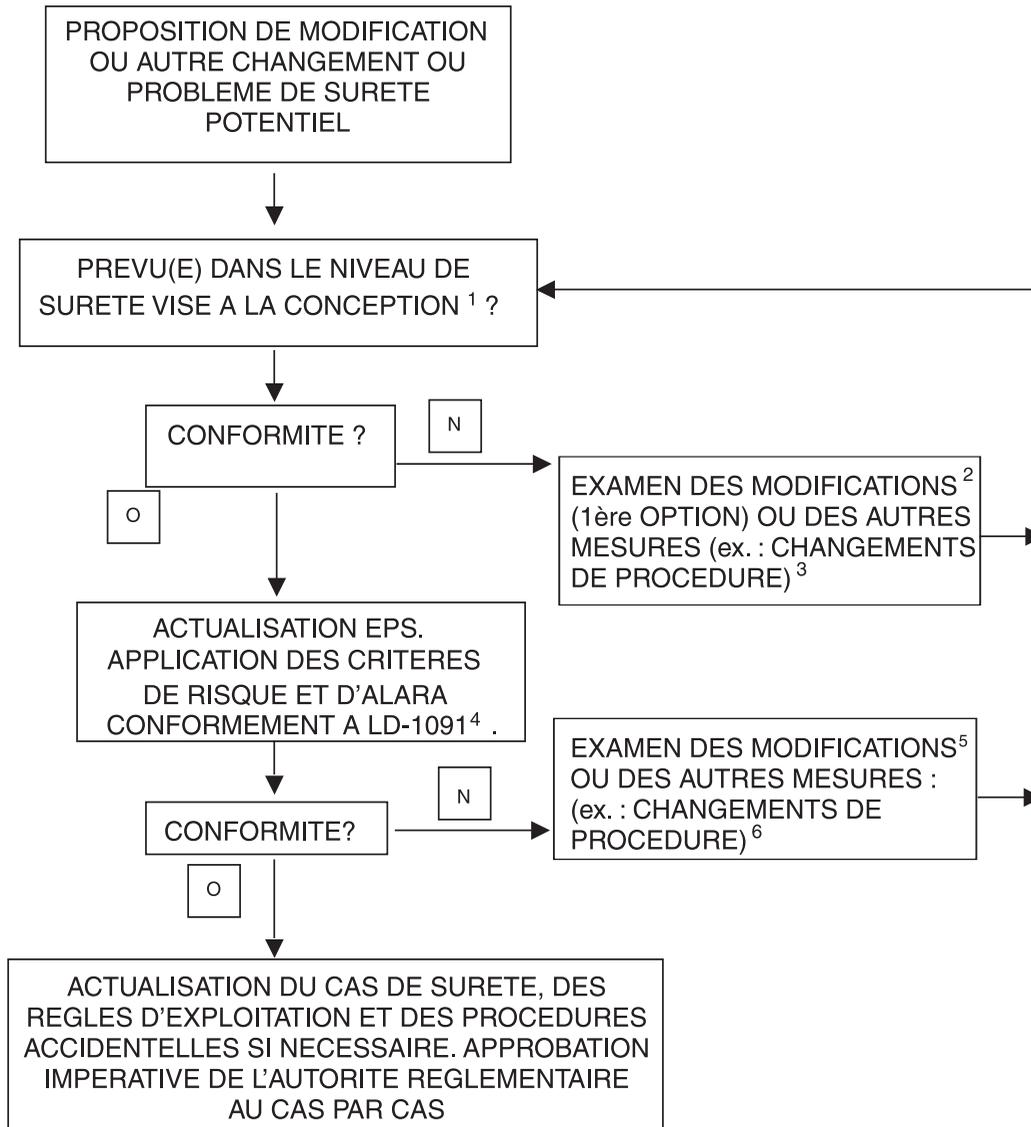
L'EPS doit couvrir les conditions normales d'exploitation prises en compte, ou non, dans le dimensionnement, ainsi que les accidents graves.

Le rôle de l'analyse déterministe et probabiliste dans le processus de décision est décrit à la figure 2.

Bien que les exigences officielles de la NNR en matière de conformité concernent les risques pour le public et le personnel de la centrale, c'est-à-dire les résultats des EPS

de niveau 3, les résultats des EPS de niveaux 1 et 2 sont pris en compte dans le processus de prise de décision pour différents types de demandes présentées par l'exploitant. Par exemple, les résultats des EPS de niveau 1 suffisent pour la plupart des évaluations relatives aux modifications et au programme de maintenance. Les résultats des EPS de niveaux 2 et 3 sont utilisés dans le cadre des modifications liées aux cas d'accidents graves (ex. : noyage du puits de cuve, guide de gestion des acci-

Dossier : Les études probabilistes de sûreté



Notes

- (1) Fréquences et conséquences des accidents prévues par les conditions de la centrale (c'est-à-dire conformément à l'ANS N-18.2), exigences en matière de défense en profondeur (ex. : critère de défaillance unique), classement des équipements conformément au dimensionnement. Réalisation d'une **analyse conservative**.
- (2) Toute modification doit satisfaire aux critères déterminés fixés par le dimensionnement. Dans des situations exceptionnelles, un « cas spécifique » peut être défini pour des mesures alternatives, concernant notamment les procédures d'exploitation, une surveillance accrue, etc. L'approbation de l'autorité réglementaire est impérative.
- (3) Procédures considérées comme liées à la sûreté (critique).
- (4) **Analyse fondée sur les meilleures estimations.** Les incertitudes doivent être prises en considération dans la validation des valeurs moyennes. Les données génériques et/ou spécifiques de la centrale doivent être vérifiées.
- (5) Les décisions de modifications (y compris de classement des équipements) pour parer aux accidents non prévus dans le dimensionnement tiennent compte du rapport risques-avantages.
- (6) Le classement des procédures (ex. : procédures de sûreté, lignes directrices) relatives aux accidents graves ou non prévus dans le dimensionnement tient compte du rapport risques-avantages.

Figure 2 : Rôle de l'évaluation déterministe et probabiliste dans le processus de contrôle des modifications applicable aux réacteurs de puissance

dents graves, etc.) et des bases techniques des plans d'urgence.

Selon l'approche de la NNR, si la quantification de la sûreté est théoriquement possible grâce à une évaluation des risques,

dans la pratique, elle ne peut être réalisée qu'avec un succès limité. Les problèmes posés sont les suivants :

- accès à des données crédibles et réalistes (intégrant les incertitudes) tenant compte du retour d'expérience ;

- conformité aux normes et codes techniques et aux règles générales d'exploitation de la centrale (ex. : programme de maintenance) dans la mesure où l'impact des modifications (ou dérogations) peut être évalué en termes quantitatifs ;
- intégration de considérations qualitatives dans un processus quantitatif et, dans certains cas, impossibilité d'effectuer une évaluation quantitative.

En conclusion, l'applicabilité de données génériques à une centrale spécifique est subordonnée au respect des normes et pratiques des centrales dont sont issues ces données. Cependant, en termes de risques, l'analyse des changements apportés (ou des dérogations) à ces normes et pratiques n'est généralement pas crédible sans retour d'expérience préalable (ou sans l'avis d'un expert approprié), à moins que le risque présenté par les composants concernés ne soit si faible que l'impact puisse être considéré comme négligeable.

La sûreté des réacteurs nucléaires est bien trop complexe pour permettre une quantification tous azimuts. Cependant, l'EPS offre un vaste cadre pour l'évaluation de la sûreté et, utilisée correctement, peut constituer un moyen efficace d'identification des faiblesses de conception et d'exploitation. L'avantage des EPS dépasse la production de résultats d'ordre quantitatif, en permettant aux décisions fondées sur la connaissance des risques de reposer également sur des critères qualitatifs.

PROCESSUS D'AUTORISATION

Une fois le dossier de sûreté (qui inclut l'EPS) examiné et approuvé par la NNR, des conditions d'autorisation, autres que celles liées à la conception, sont définies. Il s'agit alors d'identifier toutes les dispositions nécessaires en matière d'analyse des risques pour garantir des niveaux de risques acceptables.

Les conditions d'autorisation englobent généralement les aspects suivants :

- aspects liés à la sûreté dans les documents de présentation et de conception de la centrale ;
- procédures de contrôle des modifications ;

- établissement des spécifications techniques d'exploitation et respect de celles-ci ;
- procédures accidentelles et incidentelles ;
- programme d'inspection en service ;
- programme de maintenance ;
- programme de radioprotection en exploitation ;
- programme de traitement des déchets ;
- plan d'urgence ;
- programme de déclaration d'événements ;
- réalisation d'une analyse des risques solide et mise à jour ;
- programme de gestion de la qualité.

Toute modification apportée à une condition d'autorisation établie, ou toute adjonction à une centrale existante, considérée comme importante pour la sûreté ou exigeant une modification de l'autorisation délivrée pour la centrale, est subordonnée à la présentation d'une demande de modification de l'autorisation s'appuyant sur une analyse de sûreté, incluant, le cas échéant, une analyse des risques. Cette analyse est soumise à l'autorité réglementaire à l'appui de toute demande d'autorisation de création d'une nouvelle centrale ou de toute demande de modification importante, en termes de risques, d'une installation existante.

Le guide d'autorisation de la NNR LG-1046 fournit des lignes directrices destinées à l'évaluation des sites de réacteurs de puissance. Le guide d'autorisation LG-1037 concerne spécifiquement l'évaluation des réacteurs modulaires à lit de boulets.

Des exigences de sûreté paraissant inutilement restrictives peuvent donc, en principe, être modifiées après présentation et approbation par la NNR d'une évaluation de sûreté.

Règles générales d'exploitation

Les règles générales d'exploitation (RGE) s'appliquent aux points couverts par les conditions d'autorisation.

Conformément aux conditions d'autorisation et aux guides émis par la NNR, toute modification des RGE ayant une incidence

sur le dossier de sûreté (qui inclut l'EPS) nécessite un examen de sûreté préalable.

L'exploitant a ainsi eu fréquemment recours à l'EPS pour appuyer des demandes d'assouplissement des spécifications techniques concernant les durées d'indisponibilité admissibles. Ces demandes sont examinées par la NNR en fonction des risques et de la défense en profondeur.

Une procédure de gestion des arrêts programmés a été mise en place.

S'agissant des risques pour le personnel d'une centrale, des verrouillages de sécurité ont été installés sur les équipements de manutention du combustible pour répondre aux problèmes liés aux activités de manutention dans le bâtiment du réacteur.

S'agissant de l'installation de râteliers de stockage du combustible usé dans la centrale de Koeberg, il est apparu nécessaire de répondre à des exigences supplémentaires (modifications et changements de procédures). A cet égard, et en ce qui concerne les autres types d'installations évaluées mentionnées ci-dessous, l'EPS s'est révélée un outil performant d'évaluation des faiblesses de conception principalement dues au facteur humain. Cependant, un soin particulier doit être apporté au calcul et à la combinaison des probabilités d'erreurs humaines, car le risque persiste de procéder à des analyses irréalistes, et d'aboutir ainsi à des conclusions erronées et à la perte des apports éventuels des EPS.

TYPES D'INSTALLATIONS EVALUEES

Des EPS ont été réalisées dans le cadre de demandes d'autorisation pour les installations suivantes :

1. les deux REP de 900 MWe de Koeberg ;
2. le réacteur de recherche Safari de 120 MW ;
3. l'usine de fabrication d'hexafluorure d'uranium (UF6) ;
4. les usines d'enrichissement et de traitement de l'uranium ;
5. les usines de fabrication du combustible ;

6. l'ensemble des cellules chaudes (production d'isotopes pour usage médical) ;
7. différents sites de stockage des déchets ;
8. les ateliers de décontamination et les installations de stockage associées ;
9. l'installation d'enrichissement par laser ;
10. l'installation d'ionisation des aliments ;
11. des laboratoires et diverses installations contaminées.

IMPACT DE L'EPS SUR LE PROCESSUS REGLEMENTAIRE

Renforcement de la réglementation

L'obligation pour l'exploitant de mettre à jour l'EPS de référence de la centrale, et d'identifier ainsi les problèmes de sûreté, constitue une avancée considérable dans la réglementation nucléaire, notamment en ce qui concerne :

1. l'identification des faiblesses de conception ;
2. l'analyse du retour d'expérience (au niveau national et international) ;
3. l'analyse des modifications ;
4. l'évaluation des programmes de sûreté en exploitation ;
5. la conduite d'examen périodiques.

Si la conception et les règles d'exploitation d'une centrale peuvent reposer sur des conceptions déterministes, l'approche quantitative vient généralement les appuyer et constitue un outil d'évaluation globale de la sûreté de la centrale. Soumis à l'obligation de réaliser et de mettre à jour une analyse des risques approfondie, l'exploitant se voit investi d'une plus grande responsabilité en matière d'identification et de gestion des problèmes de sûreté. Les mesures adoptées en vue de l'observation des critères de risques ou de la réduction des risques donnent généralement lieu à de nombreuses exigences d'autorisation supplémentaires allant au-delà des contraintes imposées par le dimensionnement, s'agissant des modifications des programmes de sûreté en exploitation décrits ci-après.

Retour d'expérience

Programme de maintenance

Le programme initial de maintenance à intervalles fixes mis au point pour une centrale a été enrichi de techniques probabilistes afin de l'optimiser dans les points suivants :

- hiérarchisation des composants en fonction de leur importance ;
- surveillance de la fiabilité ;
- contrôle fondé sur l'état de la centrale ;
- maintenance axée sur la fiabilité.

Le retour d'expérience des activités de maintenance constitue une source d'information importante sur la fiabilité des équipements de sûreté. Les données issues de la maintenance et du contrôle de certains équipements sont comparées aux données génériques afin d'affiner les données spécifiques de la centrale. L'EPS fournit un cadre logique pour ces analyses.

Déclaration et analyse des événements/incidents

L'établissement d'un système d'identification, de déclaration et d'analyse des événements est l'une des conditions à satisfaire pour l'obtention de l'autorisation. Les données sont analysées et comparées aux données internationales. La base de données des EPS est actualisée si nécessaire. Des mesures sont prises en réaction à toute évolution jugée inacceptable.

Retour d'expérience international

Conformément aux exigences d'autorisation, le retour d'expérience international a amené de nombreuses modifications ou améliorations des procédures. L'EPS a contribué à l'identification et à l'analyse des problèmes de sûreté, ainsi qu'à la formulation de propositions d'amélioration.

Modifications

L'EPS a fréquemment été utilisée pour appuyer des décisions relatives à l'acceptabilité des modifications proposées par l'exploitant et aux échéanciers proposés pour résoudre les problèmes de sûreté.

Dans l'évaluation des nouvelles conceptions de combustibles, par exemple, l'augmentation des termes sources possibles en

cas d'accidents graves, en raison de taux d'enrichissement et de combustion plus élevés, a été prise en considération. L'augmentation des risques a conduit à accroître la pression exercée sur l'exploitant pour inciter ce dernier à s'attaquer aux problèmes de sûreté majeurs.

De nombreuses modifications importantes ont été adoptées sur la base des risques à l'arrêt.

Les modifications qui ont abouti à une extension sensible des travaux menés dans le cadre des EPS sont notamment :

- l'utilisation de quatre conteneurs de stockage à sec pour les combustibles usés ;
- le remplacement des râteliers de stockage situés dans la piscine de refroidissement (râteliers de stockage compacts) ;
- l'instauration de procédures accidentelles de type approche par états ;
- l'instauration de guide de gestion des accidents graves.

Réexamens de la conception

En 1979, la société Eskom a présenté à l'Autorité de sûreté les résultats d'une EPS des termes sources, incluant les accidents de réacteurs en états de puissance et d'arrêt, ainsi que les accidents liés au stockage des éléments dans la piscine de refroidissement, à la manutention du combustible et au traitement des déchets, en vue de l'approbation de la conception et de la mise en service de la centrale de Koeberg.

La conception initiale de la centrale ne respectait pas les critères de risques du fait de l'inadéquation de l'alimentation externe du site et de la source froide d'ultime secours. Pour y remédier, Eskom a équipé la centrale d'une alimentation électrique spécifique, indépendante du réseau national, et a défini de nouvelles procédures pour utiliser des sources de refroidissement complémentaires dans l'éventualité d'une perte de la source froide.

Réexamens périodiques

L'EPS a été utilisée dans le cadre du réexamen de sûreté de la centrale de Koeberg réalisé par l'exploitant Eskom. Des différences entre la centrale de Koeberg et les centrales françaises CP1 ont été évaluées

Dossier : Les études probabilistes de sûreté

en fonction des risques et de la défense en profondeur. Un processus qualitatif d'analyse des risques a été mis au point pour le criblage et la hiérarchisation des résultats.

Parallèlement au réexamen périodique de Koeberg, il a été procédé à une révision de l'EPS aux fins suivantes :

1. étalonner l'EPS de la centrale de Koeberg (EPS de niveaux 1 et 2) par rapport à l'EPS-900 (EPS de niveau 1 effectuée par l'IPSN sur les centrales EDF de 900 MWe) et à l'évaluation indépendante de la centrale de North Anna (EPS de niveau 2 essentiellement),
2. vérifier que l'EPS est cohérente avec le rapport de sûreté et les RGE. Ce point a été intégré au projet de particularisation de l'EPS (*PRA Customisation Project*) désormais achevé.

A la suite du réexamen de sûreté, la NNR et la DSIN (devenue DGSNR)^o ont poursuivi leur coopération en vue de partager les résultats des EPS, leurs connaissances, ainsi que leurs données.

Bases des plans d'urgence

Sous la pression de l'expansion urbaine, les centrales nucléaires ont dû reconsidérer les bases techniques des plans d'urgence. Dans le cas de la centrale de Koeberg, bien que l'EPS ne prenne pas en compte l'existence d'un plan d'urgence, les résultats de cette étude, conjugués à la modélisation de l'évacuation, ont contribué à l'élaboration de nouvelles bases techniques pour les rayons des zones du plan d'urgence, et à la fixation des délais d'évacuation pour ces zones. Cette opération a nécessité de se reporter à une courbe cumulée du terme source en fonction de la fréquence de dépassement pour définir un accident de référence.

Cohérence et transparence

Les exigences de la NNR en matière d'évaluation des risques ne sont pas seulement nécessaires pour pallier l'insuffisance des réglementations déterministes conventionnelles à remédier aux problèmes de sûreté, mais également pour garder clairement à l'esprit l'objectif premier de la réglementation nucléaire, à savoir la pro-

tection du public et du personnel des centrales. A cet égard, l'EPS offre un cadre général de débat pour les questions relatives à la sûreté et contribue à améliorer la transparence et la cohérence du processus de décision.

Simplification

Outre des exigences en matière d'analyse des risques, les autorisations actuelles de la centrale de Koeberg et d'autres installations incluent de nombreuses conditions spécifiques. Les exigences relatives à la modification de ces conditions imposent un lourd fardeau administratif à l'Autorité de sûreté, ainsi qu'à l'exploitant.

Un grand nombre d'exigences impératives figurant dans l'actuelle autorisation de la centrale de Koeberg seront bientôt remplacées par diverses exigences « axées sur les processus », incluant notamment des processus de criblage et d'évaluation de la sûreté. L'EPS sera ensuite utilisée dans le cadre de ces processus.

Fardeau réglementaire

Evaluations techniques

Plus d'un millier de demandes d'autorisation de modifications ont été soumises à la NNR pour la seule centrale de Koeberg. A chacune de ces demandes est jointe une étude, ou tout au moins une évaluation des risques. L'appréciation de la NNR pour chacune de ces demandes est enregistrée aux fins de référence ultérieure.

Le recours à l'EPS impose, certes, une charge de travail supplémentaire considérable, mais celle-ci est largement compensée par l'avantage de disposer d'un cadre de décision objectif. La nouvelle approche adoptée en matière d'autorisation devrait permettre d'alléger quelque peu le fardeau réglementaire.

Inspections

Des indicateurs et des objectifs de sûreté ont été définis à l'appui du programme d'assurance de la conformité de la centrale de Koeberg.

Les inspecteurs s'appuient sur un système de hiérarchisation des problèmes de sûreté et d'examen des indicateurs, fondé sur une

évaluation qualitative et/ou quantitative des exigences fondamentales de sûreté, dans le but de réduire la subjectivité au minimum. De ce fait, ce système implique le recours à l'EPS.

Les indicateurs et les objectifs de sûreté ont été associés à un programme d'assurance de la conformité. Des modifications ont ainsi dû être apportées au programme de base de la centrale de Koeberg pour intégrer les indicateurs et les objectifs de sûreté. Le système d'indicateurs de sûreté est ensuite employé pour axer les inspections et les audits sur les domaines suscitant une inquiétude particulière.

CONCLUSIONS

A en juger par notre expérience, les principaux apports de l'EPS dans le processus réglementaire sont les suivants :

- un cadre d'information, en principe exhaustif, sur la sûreté nucléaire permettant une appréciation quantitative de la sûreté ;
- une approche rationnelle et structurée dans la résolution de problèmes complexes et variés, pour lesquels les autres méthodes se révèlent inadaptées ;
- une attention fixée sur l'objectif premier de la réglementation nucléaire, à savoir la protection du public et du personnel, et, en conséquence, la transparence du processus réglementaire ;

- l'amélioration du processus d'autorisation par l'instauration d'un processus d'identification des nouveaux problèmes de sûreté qui puisse être utilisé par l'autorité réglementaire et par l'exploitant ;

- un cadre de hiérarchisation des activités réglementaires et, de ce fait, l'allègement de la charge de l'Autorité de sûreté sans compromettre la sûreté.

L'élaboration et la conduite d'EPS est indispensable pour éliminer toute erreur des résultats et éviter une mobilisation inutile de moyens.

L'EPS ne doit pas être rejetée sous prétexte des grandes incertitudes qu'elle comporte car celles-ci sont inhérentes à tout processus de décision. Le processus de décision doit tenir compte des incertitudes : les décisions ne reposant que sur des estimations ponctuelles peuvent se révéler trompeuses.

Les connaissances et l'expérience en matière de sûreté nucléaire n'étant qu'indirectement utilisées dans l'EPS (à travers la fixation des données de fiabilité/fragilité, par exemple), l'avis d'expert reste un complément indispensable. Comme il n'est pas toujours possible ou pratique de quantifier tous les problèmes de sûreté de manière satisfaisante, ou même d'être sûr que tous les événements ont été recensés, l'EPS n'est pas considérée comme le parfait substitut au processus de décision fondé sur la défense en profondeur et les critères qualitatifs. On ne doit pas se fier absolument aux seuls résultats chiffrés des EPS.

La politique du MEDD en matière de prévention des risques industriels majeurs dans les installations classées : que peuvent apporter les études probabilistes de sûreté dans le domaine des installations Seveso ?

par **Bruno Cahen** – Direction de la prévention des pollutions et des risques (DPPR) – Ministère de l'écologie et du développement durable

Les référentiels de prévention des risques industriels majeurs et de sûreté de fonctionnement sont de plus en plus européens, voire internationaux. Pour les installations classées les plus dangereuses, les grands principes en sont précisés dans la directive dite Seveso II du 30 décembre 1996, qui renforce la première du nom, publiée en 1982. En France, on dénombre environ 1200 installations Seveso. Même si les outils et les pratiques diffèrent, le principe de la prévention des risques par une défense en profondeur améliorée de manière continue par le retour d'expérience et la diffusion large des bonnes pratiques est approuvé par l'ensemble des opérateurs industriels et des autorités de contrôle. En application de ce principe, les installations nouvelles doivent être conçues, construites et exploitées selon l'état de l'art du moment. Pour les installations existantes, une obligation d'amélioration continue de la sécurité incombe aux exploitants.

Les exploitants Seveso doivent apporter à l'inspection des installations classées la démonstration de la prévention des risques liés à des procédés ou des substances dangereuses, dans toutes les

phases de conception, de démarrage, d'exploitation, de maintenance ou travaux jusqu'au démantèlement des installations. En France, cette démonstration doit être apportée à travers une étude de dangers, liée au référentiel d'exploitation de l'industriel, dit « système de gestion de la sécurité ». Le terme d'étude de dangers, qui peut sembler inapproprié, est historique.

L'article 4 de la loi n°2003-699 du 30 juillet 2003 introduit au niveau législatif les principes de l'étude de dangers, définis d'une manière générale par le décret n°77-1133 du 21 septembre 1977 et de manière plus approfondie pour les seules installations Seveso par l'arrêté ministériel du 10 mai 2000 : l'étude de dangers⁽¹⁾ doit justifier les mesures de prévention mises en place afin de réduire la probabilité d'occurrence et la gravité potentielle de leurs effets sur les intérêts visés à l'article L.511-1 du code de l'environnement. Ces mesures techniques ou organisationnelles doivent assurer la sûreté de fonctionnement des installations, y compris en phase transitoire ou en marche dégradée. Elles doivent par conséquent être fiables, le cas échéant redondantes et indépendantes.

1. A ce propos on pourra consulter le guide intitulé « principes généraux des études de dangers - version 1 » élaboré par des représentants des principaux exploitants d'installations Seveso à hauts risques, des représentants de l'administration et des organismes experts en risques industriels et diffusé par la Direction de la prévention des pollutions et des risques le 25 juin 2003, qui complète le guide précédent diffusé en 1995.

La profondeur d'analyse doit être adaptée à la nature des installations et à la sensibilité de leur environnement, selon le principe de proportionnalité défini au quatrième alinéa du 5° de l'article 3 du décret n°77-1133 du 21 septembre 1977 modifié.

L'étude de dangers peut utilement conforter sa démonstration par des éléments de comparaison avec l'état de l'art en matière de conception et d'exploitation d'installations semblables au niveau européen ou mondial.

La défense en profondeur renvoie à la définition et à l'évaluation de barrières de sécurité fiables et indépendantes et donc à l'évaluation de probabilités de défaillance, ou encore de probabilité d'occurrence d'un scénario accidentel pouvant conduire à une atteinte à la santé ou la sécurité des personnes ou de l'environnement hors du site. Ces questions d'analyse de risques, liées à la justification des lignes de défense nécessaires et suffisantes, sont particulièrement complexes pour les installations classées en raison de la disparité des installations et de son corollaire, le manque de données de fiabilité. En effet, contrairement aux réacteurs de puissance, les installations Seveso sont de nature, de taille et de conception très variables. Entre un stockage d'engrais en vrac, une sphère de GPL et une usine de chimie fine multiproduit, il est difficile de trouver un standard commun pour les équipements ou les procédures d'exploitation. Cette disparité se double d'une multiplicité d'opérateurs industriels, de taille et de pratiques hétéroclites.

Si autorités, experts et exploitants s'accordent sur les principes, la question des données de fiabilité et de la justification des barrières de sécurité fait l'objet d'intenses débats entre les autorités de contrôle, les experts et les syndicats professionnels au niveau européen. Les enjeux économiques et sociaux sous-jacents au choix de scénarios servant à définir les zones de maîtrise

de l'urbanisation autour des installations ne contribuent pas à apaiser le débat. Afin de définir des méthodes et outils communs européens, les Etats membres ont lancé plusieurs programmes de recherche et développement⁽²⁾. La constitution d'une base de données européennes sur les probabilités et effets de scénarios accidentels courants, les mesures de prévention et l'évaluation de la fiabilité, décidée en septembre 2002, est en cours. Il s'agit d'un exercice difficile, long et à l'issue incertaine.

En France, afin d'évaluer la faisabilité et le coût d'études probabilistes sur des installations Seveso, la Direction de la prévention des pollutions et des risques du MEDD fait réaliser une étude probabiliste de sûreté de niveau 1, en choisissant une installation très simple, relativement standard au niveau mondial (stockage de GPL, dont il existe plusieurs centaines de milliers d'exemplaires dans le monde). L'étude exploite les bases de données mondiales disponibles. Cette étude n'est pas achevée, mais les premières conclusions confirment l'insuffisance des données disponibles. Les résultats obtenus à ce jour, en termes de probabilité d'occurrence d'un BLEVE⁽³⁾ du réservoir, ou en termes de probabilité de défaillance des principales barrières de prévention de cet accident, sont difficiles à interpréter.

Une question centrale n'y trouve pas de réponse : quelle technologie pour les futurs réservoirs de stockage de GPL ? Seront-ils plus fiables, à court et à long terme, s'ils sont enterrés ou à l'air libre, et dans quelles conditions ?

Au vu de cette expérience, la réalisation d'une EPS de niveau 1 sur l'ensemble des installations dans un complexe chimique moyen n'est sans doute pas envisageable à ce jour, car la plupart des installations de chimie fine sont non standard, existant en quelques exemplaires au niveau européen ou mondial.

2. Le site Internet de la Commission européenne présente ces projets. On notera les projets ARAMIS, ACUTEX SHAPE-RISK, qui visent à définir des méthodes et outils européens, essentiellement pour l'analyse de risque, mais également pour la définition et la justification du choix des mesures de prévention et de protection contre les incidents et accidents industriels.

3. BLEVE : explosion d'un réservoir contenant un gaz liquéfié brusquement porté à ébullition par dépressurisation.

Dossier : Les études probabilistes de sûreté

A défaut d'étude probabiliste, la prévention des risques industriels en France peut progresser à court et moyen terme par une mise en pratique harmonisée de l'état de l'art et par la prise en compte combinée des facteurs humains, organisationnels et techniques de prévention.

1/ Pour les installations nouvelles, mettre en application l'état de l'art, ce qui suppose que l'industriel présente des éléments de comparaison de son projet avec les installations les plus performantes ou les plus récentes au niveau mondial.

2/ Pour les installations existantes, maintenir la vigilance sur un parc vieillissant : en s'appuyant sur des méthodes d'analyse de risque actuellement utilisées par les entreprises, sur le retour d'expérience, sur des éléments de comparaison entre sites similaires, il est possible de diffuser les meilleures pratiques internationales (systèmes et matériels, organisation, formation, maintenance, identification et correction des écarts). L'implication du plus haut niveau de la direction des entreprises est nécessaire. Les fédérations professionnelles, les sociétés d'assurances, les organismes de recherche et d'expertise peuvent jouer un rôle majeur de diffusion internationale. Les pouvoirs publics peuvent également impulser ces actions.

En termes de méthodologie d'analyse de risques, pour les études de dangers la combinaison des acquis des approches déterministes et probabilistes devrait permettre de justifier plus finement le caractère nécessaire et suffisant des mesures de prévention mises en place : barrières de sécurité définies en fonction d'accidents identifiés, et évaluation de leur fiabilité (cf. autres domaines : aéronautique, ferroviaire, nucléaire...). Le système de prévention doit également être robuste face aux dérives et à l'imprévu : l'écart, c'est la normalité ; en matière de fonctionnement, de procédures, les automatismes et les personnes doivent en permanence détecter des écarts et engager des actions correctives ; la sûreté, ou le risque, découle de ces chaînes d'écarts / détection / correction.

Le MEDD a engagé depuis 2002, avec les représentants des principales fédérations, une mise en commun des méthodes et pratiques d'analyse de risque, pour déboucher en 2003 sur des principes méthodologiques communs. Des outils ou guides d'application pourront être développés, par type d'installation ou par secteur d'activité. Ces travaux ont démarré pour le chlore, le GPL et seront bientôt engagés pour le stockage de produits pétroliers liquides.

Pour une approche probabiliste dans les études de dangers des sites pétrochimiques.

L'expérience du groupe Shell

par **Bruno Chevalier**, chargé de mission
« risques industriels » - Shell

Un facteur de réussite : le système de management HSE⁽¹⁾ (ou HSE-MS)

La dramatique catastrophe de la plateforme Shell « Piper Alpha » en Mer du Nord, voici une quinzaine d'années, rappelle que, malgré les précautions prises dans nos activités depuis que le pétrole est exploité à l'échelle industrielle, nous n'étions toujours pas à l'abri d'un accident grave et qu'il fallait donc inscrire le « management » des problèmes HSE comme la **priorité N° 1 de tous les dirigeants de Shell**.

En 1994 le groupe Shell a donc publié un guide fixant les principes d'établissement et de déclinaison d'un tel système de « management », les responsables d'activité ayant jusqu'au 31/12/1999 pour le mettre en place. Corrélativement, en 1997, le groupe publiait une nouvelle révision de sa politique HSE qui précisait : HSE doit être gérée avec une priorité majeure au même titre que les autres aspects du « business ».

Cela faisait du patron de chaque installation industrielle le premier responsable en matière d'HSE ; l'intégration d'HSE dans ses préoccupations quotidiennes rendait « obsolètes » les organisations où l'on voyait encore des « responsables » HSE ; elles furent remplacées par des petites cellules de conseil, la responsabilité incombant en totalité à la ligne hiérarchique opérationnelle.

Ce système de management (*cf. graphique 1*) définit en détail l'approche HSE qui doit être conduite par le directeur du site : elle insiste sur son engagement personnel, son appropriation de la politique HSE du groupe, la définition d'objectifs détaillés dans les trois domaines H, S et E, l'identification des règles / procédures à suivre et la définition des moyens à la disposition de la hiérarchie ; l'analyse des risques et de leurs conséquences est au cœur du dispositif ; bien sûr, reporting des performances, audits internes et externes, revue de direction et actions correctives complètent une approche qui s'apparente étroitement au concept de qualité totale.

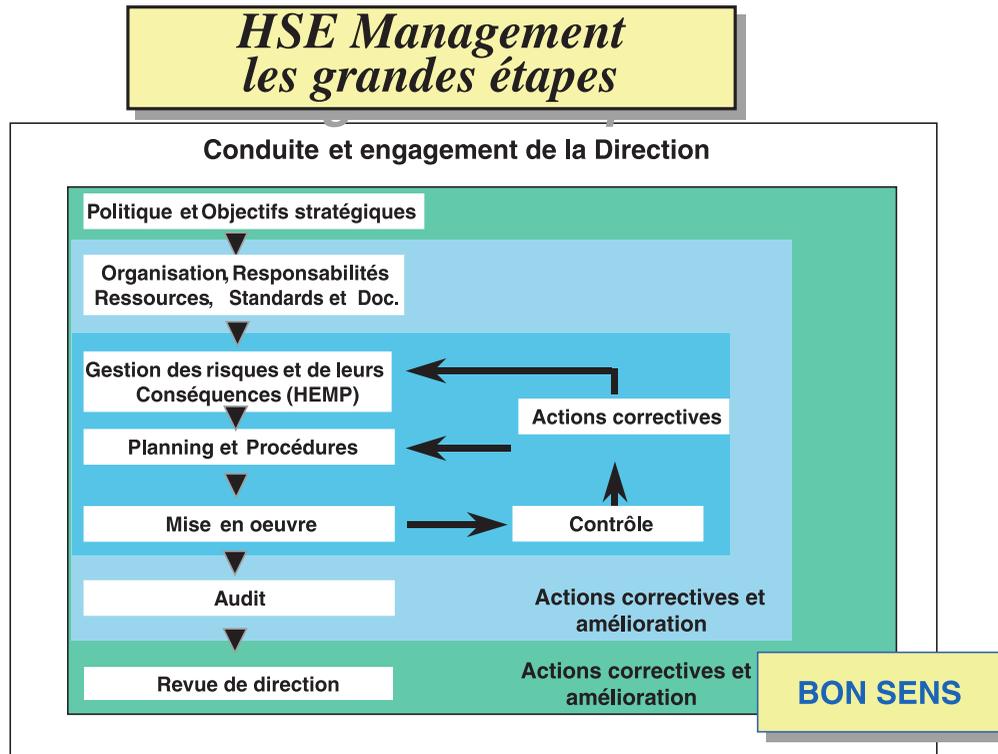
La gestion des risques et de leurs conséquences (HEMP⁽²⁾)

Cette démarche constitue une approche systématique de la maîtrise des risques (et de leurs conséquences) dans le but de répondre à la politique HSE de Shell : pas d'atteinte à l'intégrité des personnes ni à l'environnement, respect strict de la législation du pays et amélioration continue des performances .

Identification des dangers

L'ensemble des activités et services critiques du point de vue d'HSE sont recensés de façon **exhaustive** dans les sites industriels dits « Seveso » (engineering, entretien, modifications, opérations) mais aussi

1. Hygiène (industrielle), sécurité et environnement.
2. Hazards and Effects Management Process.



Graphique 1 : HSE Management : les grandes étapes

pour les activités commerciales, le transport routier, les activités tertiaires (problème de santé - alcool / drogues), etc.

Les sources de danger sont identifiées :

- produits explosifs, toxiques ou inflammables ;
- situations dangereuses (réacteur à haute pression / haute température, entretien d'équipements en milieu confiné, conduite d'un véhicule transportant des matières dangereuses...).

Caractérisation des scénarios

Pour chaque source de danger, l'événement redouté qui conduirait à la matérialisation du danger est déterminé (perte de confinement, renversement d'un camion-citerne...) ainsi que les menaces qui y conduiraient (corrosion sur un équipement, non-respect de procédure...) et les conséquences qui en découleraient (explosion d'un nuage de gaz, pollution de la nappe phréatique...).

Sont également rappelées les mesures préventives résultant de la législation, les

règles de construction propres à Shell, ou les procédures existant sur le site ainsi que les mesures de protection déjà en vigueur sur l'installation (détecteur d'hydrocarbures, moyens de lutte contre l'incendie, organisation POI⁽³⁾ et gestion de crise...).

Classement des scénarios : la matrice d'évaluation de risques

Shell a défini une matrice d'évaluation des risques qui permet de classer l'ensemble des scénarios identifiés en fonction de leurs impacts concernant les personnes, les installations, l'atteinte à l'environnement et à la réputation de la société Shell (cf. graphique 2).

Pour chacun de ces quatre items, des critères de fréquence d'occurrence et de gravité sont donnés ; ceux-ci s'appuient sur une **accidentologie** aussi complète que possible incluant :

- les incidents répertoriés dans l'industrie pétrochimique au niveau mondial (cf. Concawe ...)
- les bases de données nationales (cf. Barpi)

³ Plan d'organisation interne.

Dossier : Les études probabilistes de sûreté

Gravité	CONSEQUENCES				PROBABILITE				
	Personnes	Biens	Environnement	Réputation	A	B	C	D	E
					Pas connu dans votre industrie	S'est produit dans votre industrie	Arrivé dans votre compagnie	Arrivé plusieurs fois par an dans votre compagnie	Arrivé plusieurs fois par an sur votre site
0	Pas de blessé	Pas de dommage	Pas d'effet (ni environnement ni coût)	Pas d'impact					
1	Blessures légères (Soin infirmerie ou ASA)	Dommages légers. Pas d'arrêt de production (coût < 10.000 €)	Faibles effets (interne au site et coût négligeable)	Impact faible					
2	Blessures mineures (AAA)	Dommages mineurs. Bref arrêt de production (coût < 100.000 €)	Effets mineurs	Impact limité					
3	Blessures graves (Arrêt de travail prolongé)	Dommages localisés. Arrêt partiel d'unité (peut redémarrer et coût < 1 M €)	effets localisés	Impact important					
4	Un à trois décès	Dommages importants (pertes partielles d'opération 2 semaines d'arrêt coût < 10 M €)	Effets importants	Impact national					
5	Plusieurs décès	Dommages énormes (perte partielle ou totale d'opération et coût > 10M €)	Effets énormes	Impact international					

Graphique 2 : Matrice d'évaluation des risques

- les bases de données du groupe Shell résultant de l'expérience de dizaines de sites industriels (MF-9 et 10, Safety Newsletter, HSE Forum) ;
- l'histoire passée des accidents survenus sur le site étudié, les archives, les analyses Tripod ;
- etc.

Compte tenu de ces informations, chaque scénario défini ci-dessus est coté au regard des quatre items (le plus pénalisant en termes de gravité / probabilité est retenu) puis positionné dans la matrice. Celle-ci comporte trois zones :

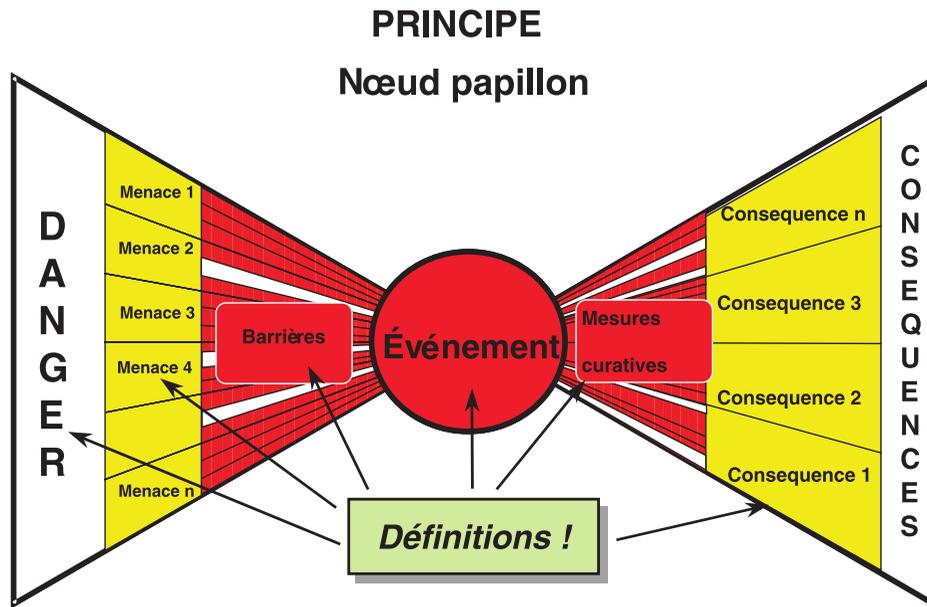
- verte (scénario mineur facilement contrôlé par les moyens déjà en place) ;
- rouge (scénario aux conséquences inacceptables - doit être étudié en détail et donner lieu à des mesures complémentaires) ;
- orange (scénario devant faire l'objet d'une étude particulière). Cette zone, considérée comme ALARP (as low as reasonably practicable), doit être évitée ; l'étude à mener recherche les mesures faciles à mettre en œuvre et d'un coût raisonnable qui permettent de ramener le scénario considéré dans la zone verte.

Scénarios critiques et « nœud papillon »

Les scénarios, en zone rouge ou orange, qui pourraient avoir des conséquences catastrophiques, sont visualisés selon la technique Shell dite du nœud papillon (cf. graphique 3).

A partir de la source de danger significatif et de l'événement redouté qui traduit sa matérialisation, sont représentées les différentes causes (ou menaces) qui conduisent à l'événement ainsi que les conséquences qui en résultent.

Pour chacun de ces processus (causes et conséquences), seront définies les mesures (« barrières ») supplémentaires qui permettent soit de contrôler (ou supprimer) les causes, soit d'atténuer les conséquences pour amener les effets résiduels de celles-ci à un niveau acceptable. Elles s'ajoutent aux mesures initiales déjà prises ; ce peuvent être des équipements de contrôle (instrumentation) ajoutés au procédé (prévention), des dispositifs d'atténuation des conséquences (détecteur, moyens fixes de lutte contre le feu, plan anti-pollution...), des procédures qui permettent de s'assurer de l'intégrité des équipements (boucle de corrosion, campagne de mesures d'épaisseur, inspection...) ou des consignes de tra-



Graphique 3

vail strictes (test, permis de travail « avec feu » en zone dangereuse...).

L'ensemble de ces mesures doit faire l'objet d'une gestion précise incluant la documentation et la traçabilité de la mesure, le contrôle permanent de son efficacité, la hiérarchisation des différentes mesures placées sur une même cause et bien sûr l'attribution à un « propriétaire » en charge de ces actions. Cela fait partie intégrante du HSE-MS !

Enfin chaque événement redouté est analysé quant à ses conséquences et aux phénomènes physiques ou chimiques qu'il peut engendrer : BLEVE⁽⁴⁾, UVCE, flash fire, nuage toxique, pollution de nappe phréatique... Ces phénomènes sont modélisés (Shell utilise des modèles tels que FRED, développés en interne) et quantifiés (calcul du débit de fuite, masse / volume du nuage de gaz, dispersion / dilution des gaz, calcul des effets thermiques, toxiques et des surpressions en fonction de la distance, etc.).

Deux approches dans le groupe Shell

La détermination des barrières ci-dessus résulte d'une approche qualitative ou quantitative. Les deux techniques sont appliquées par Shell.

Quantitative Risk Assessment (QRA)

- Evaluation de la probabilité du scénario

Pour chaque scénario critique est établi un **arbre des causes** aussi exhaustif que possible, intégrant toutes les causes pouvant conduire à l'événement redouté et leur probabilité d'occurrence compte tenu des mesures prises (barrières de prévention) : défaillances d'équipement, non-respect de procédure ou comportement inadapté. Ces probabilités d'occurrence par heure, par an ou par opération, sont extraites des bases de données de l'industrie pétrochimique ou d'autres branches d'activité comparables et résultent de l'expérience acquise sur de nombreuses raffineries, usines chimiques, dépôts pétroliers, etc.

La combinaison de ces probabilités permet d'obtenir la fourchette de probabilité d'occurrence du scénario critique étudié compte tenu de l'incertitude attachée à chaque probabilité « élémentaire ».

On construira de même un **arbre des événements** (et des conséquences) qui, à partir de l'événement redouté, liste les effets corrélatifs et les mesures (barrières de protection) prévues et mises en place pour atténuer (supprimer) ceux-ci.

4 Explosion d'un réservoir contenant un gaz liquéfié brusquement porté à ébullition par dépressurisation.

Dossier : Les études probabilistes de sûreté

- Estimation de la gravité

Celle-ci repose sur la quantification des atteintes aux personnes dans le périmètre de l'installation étudiée en termes de blessures à caractère irréversible ou létal résultant des effets résiduels. Un recensement des populations exposées à proximité du site est effectué ; les calculs d'effets de l'événement redouté en fonction de la distance permettent de déterminer les populations affectées par celui-ci.

La superposition de l'ensemble des scénarios critiques d'un site donné permet de déterminer :

- les courbes F / N donnant probabilité d'occurrence des scénarios versus populations affectées (effets létaux) ; le « zoning » autour du site avec les secteurs de probabilité décroissante d'occurrence des scénarios critiques.

Un exemple d'application pour un dépôt de GPL en France illustre cette approche (cf. graphiques 3, 4 et 5).

- Acceptabilité du risque résiduel

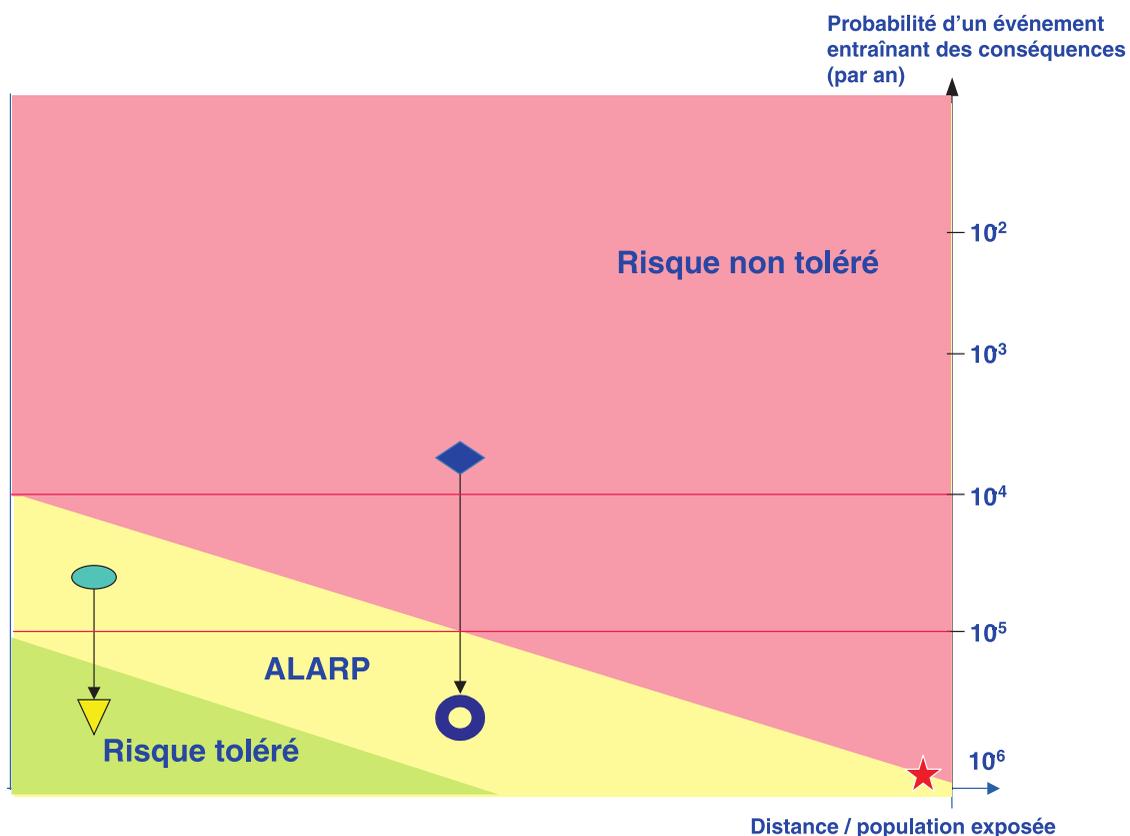
Les éléments calculés ci-dessus (probabilité, gravité, population affectée) doivent être en adéquation avec le niveau d'acceptabilité du risque individuel et sociétal toléré par le gouvernement du pays, ce qui suppose que des critères d'acceptabilité du risque aient été fixés au préalable par l'administration. C'est le cas pour nos installations (raffineries, dépôts...) au Bénélux et en Grande-Bretagne. Si le risque résiduel excède ces limites, l'industriel doit rajouter des **mesures (barrières) complémentaires** jusqu'à arriver dans la zone acceptable.

- Choix des barrières

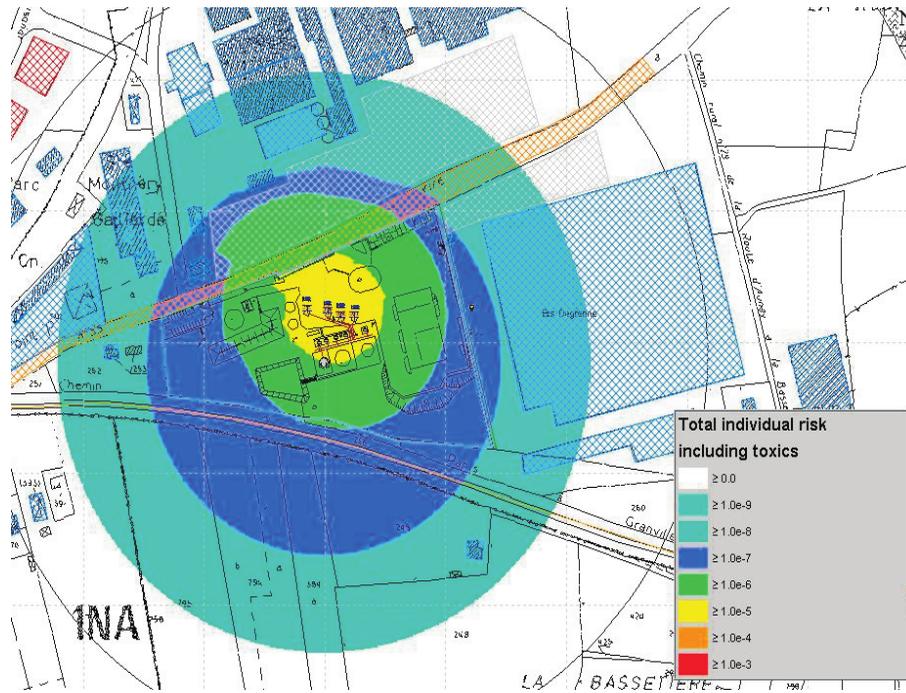
Il doit répondre à quatre critères :

- efficacité : la barrière supplémentaire ajoutée aux installations doit permettre de réduire de façon significative la probabilité d'occurrence de l'événement ou la gravité de ses effets ;

Évaluation des risques - Gravité des effets létaux



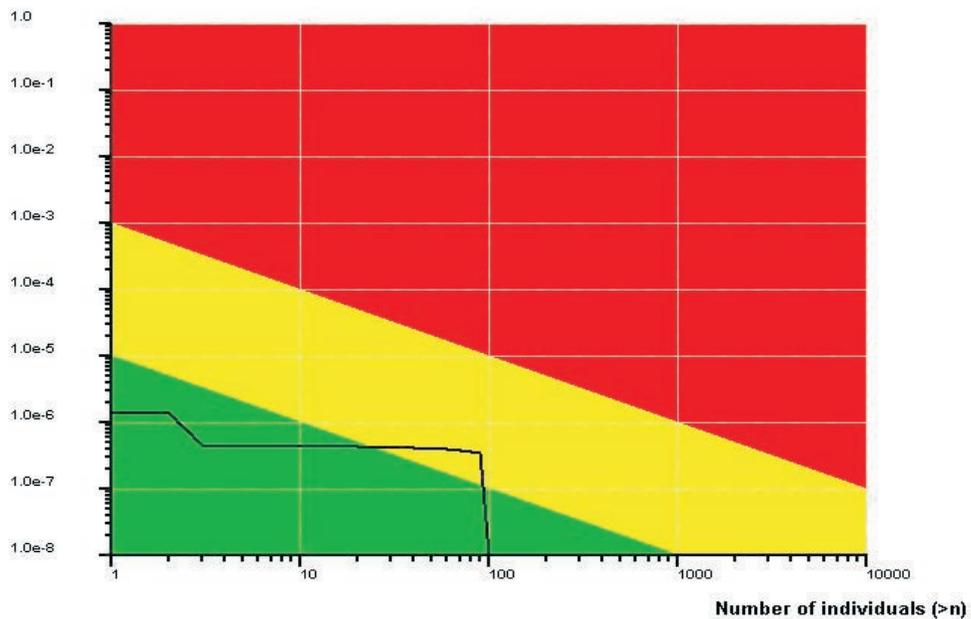
Graphique 4



Graphique 5

Simulation Fn plot

Frequency (f)



Graphique 6 : proposition des industries pétrolières et chimiques

- pérennité : celle-ci doit résister à l'événement redouté et ne pas être mise hors d'usage à cette occasion ;
- fiabilité : un taux de défaillance aussi faible que possible contribue à accroître la fiabilité de l'ensemble des mesures de prévention / protection ;

- coût : le coût de chacune des barrières envisageables est un critère de choix en sus des éléments ci-dessus.

Un exemple permet d'illustrer cette approche : **BLEVE d'une sphère de GPL**. La méthode ci-dessus appliquée à une sphère de GPL construite et exploitée selon

les règles Shell (DEP, IPF, procédures d'exploitation de HSE-MS) et respectant la réglementation française a permis de bâtir l'arbre des causes pouvant conduire au phénomène de BLEVE et de quantifier la probabilité d'occurrence de cet événement en cas de défaillance des barrières incorporées.

Le cas de base conduit à une fourchette de probabilité de **2 à 2, 6x10⁻⁷**, le chemin critique étant la perte de confinement totale du produit stocké.

L'adjonction d'une barrière supplémentaire (enceinte en béton autour de la sphère - gain de fiabilité de **10⁻¹**) améliore sensiblement la fiabilité de l'ensemble (probabilité de **4,2 à 9,5x10⁻⁸**), le chemin critique se déplaçant vers les dispositifs d'arrosage et la résistance de la paroi à la déchirure.

L'ajout d'une deuxième barrière (fiabilisation de la pomperie incendie - gain de **10⁻¹**) améliore assez peu la fiabilité de l'ensemble : **3,2 à 3,9x10⁻⁸**, et ramène le chemin critique à celui du cas de base.

En revanche, installer comme deuxième barrière un ignifuge efficace des parois (cf Gasafe) permet de descendre à des probabilités de l'ordre de **2x10⁻¹¹ mais à un coût élevé (~1M\$)**.

Inversement la perte, dans le cas de base, de deux barrières instrumentales (niveau Larco et niveau alarme « très très haut ») détériore peu la probabilité, à **7x10⁻⁷**, le chemin critique s'appuyant sur l'arrosage, l'intervention de l'opérateur et les instruments restants.

- Remarque : application pour Shell en France

La nouvelle loi sur les risques technologiques et la circulaire du 25 juin 2003 sur les principes de réalisation d'une étude de dangers nous amènera à suivre dans les grandes lignes cette même démarche, l'exploitant se fixant ses propres critères d'acceptabilité du risque résiduel en concertation avec les collectivités locales et le préfet à défaut de règles nationales (cf. graphique 6).

Une bibliographie assez étendue a déjà permis de rassembler six bases de données donnant les taux de défaillance des équipements : LOPA (USA), TNO(Hollande),

OREDA (Scandinavie), AEGPL (France), EDF - nucléaire, raffineries Shell. Malgré le manque d'expérience en France, elle facilitera la transition du déterminisme vers une approche probabiliste de nos études de dangers, en ligne avec de nombreux pays européens.

Approche « qualitative » (raffineries Shell en Australie)

- Principe

Cette approche repose sur un principe **SFAP** (« So Far As Practicable ») imposé par le gouvernement australien. Il fixe à **10⁻³ / an** la limite de probabilité d'occurrence du **risque individuel intolérable** et exige de l'exploitant qu'il réduise les risques « aussi loin que cela est faisable » compte tenu de :

- l'importance des dangers en cause ;
- l'état des connaissances et des moyens pour y remédier ;
- la disponibilité et l'adéquation de ces moyens aux risques ;
- le coût d'atténuation ou d'élimination de ces dangers ou de ces risques.

L'exploitant doit s'assurer qu'il y a suffisamment de mesures de contrôle indépendantes pour prévenir ou atténuer les incidents majeurs.

- Détermination des « mesures de contrôle » (« barrières »)

Les incidents majeurs ou scénarios critiques sont déterminés selon la méthode exposée ci-dessus. Les mesures de réduction du risque (barrières) mises en œuvre sont établies à partir des standards de Shell et de l'industrie pétrolière, de l'expérience technique et opérationnelle acquise sur le site, de nouveaux matériels ayant fait leur preuve, ou par la rédaction de nouvelles procédures d'exploitation.

L'ensemble des mesures de contrôle est identifié et analysé quant à leur robustesse, compte tenu de la qualité de celles-ci, de leur indépendance et de leur nombre. Quatre critères permettent d'évaluer la robustesse des barrières :

- efficacité : capacité à réduire l'occurrence ou la gravité de l'événement ;
- fiabilité : garantie de la réponse en cas de sollicitation ;

Dossier : Les études probabilistes de sûreté

- disponibilité maximale déduction faite des temps d'arrêt, réparation, test ;
- pérennité : assurance que le système (barrière) n'est pas détruit avant d'avoir rempli sa mission lorsque l'événement se produit.

Chaque critère est affecté d'une cotation (%) exprimée en termes d'inefficacité, la somme de ces 4 cotations caractérisant la robustesse de la barrière selon le barème suivant :

Niveau d'inefficacité	Rating
< 5%	+++
5 < <20%	++
20 < <35%	+
>35%	-

Ces cotations sont attribuées de façon qualitative par concertation à l'intérieur d'un panel d'experts du site comprenant chefs d'unités, ingénieur de maintenance, responsables d'instrumentation et d'inspections, technologues... et reposent sur leur expérience, les statistiques de l'usine, son accidentologie propre, etc. Une barrière constituée uniquement de procédures est cotée ++.

- Adéquation des barrières

- Barrières de prévention d'un scénario critique

Il est exigé d'avoir au minimum **trois barrières indépendantes** pour chaque cause ; deux d'entre elles doivent être au moins cotées ++, la troisième au moins +.

- Barrières de protection / d'atténuation des conséquences du scénario critique

Il faut au minimum **deux barrières indépendantes** pour chaque conséquence ; l'une d'entre elles doit être au moins cotée ++.

Chacune de ces barrières fait l'objet d'une gestion précise : tenue à jour de la documentation de celle-ci, contrôle de la permanence et de la validité des cotations (tests...), vérification de l'indépendance

des barrières entre elles, vérification pour chaque scénario critique que toutes les menaces pouvant conduire à l'événement redouté ont été « traitées » ainsi que leurs conséquences potentielles.

Remarque importante : l'approche qualitative décrite est surtout appliquée pour définir, au niveau des installations, les mesures complémentaires nécessaires pour répondre aux exigences de Shell. L'étude quantitative, QRA, est faite en complément pour :

- permettre à l'administration de vérifier que le principe imposé, SFAP (seuil d'intolérabilité à 10^{-3}), est bien respecté ;
- lui donner les éléments nécessaires à la maîtrise de l'urbanisation autour du site.

Note : la démarche suivie par Shell Australie a son équivalent en Europe dans la notion de Safety Integrity Level (**SIL a1/a2, 1, 2 ou 3 par ordre d'exigence croissante**) définie par la norme IEC 61511 ; le nombre de barrières indépendantes à installer est fonction de la criticité du scénario et du taux de défaillance de chaque barrière.

Conclusion

L'approche développée par Shell pour s'assurer que les risques liés à ses installations sont maîtrisés et les conséquences résiduelles ramenées à un niveau acceptable suppose une gestion stricte des barrières mises en place. C'est l'objet même de l'HSE-MS. Mais elle doit être complétée par une organisation qui permet d'anticiper et de gérer la crise ou l'accident si malgré tout il se produit, dotée de moyens (lutte contre le feu, équipe d'intervention, POI...), rodée à la mise en œuvre de ceux-ci pour que notre politique Shell « pas d'atteinte aux personnes et aux biens » ne soit pas un vain mot, sachant que le risque zéro n'existe pas !