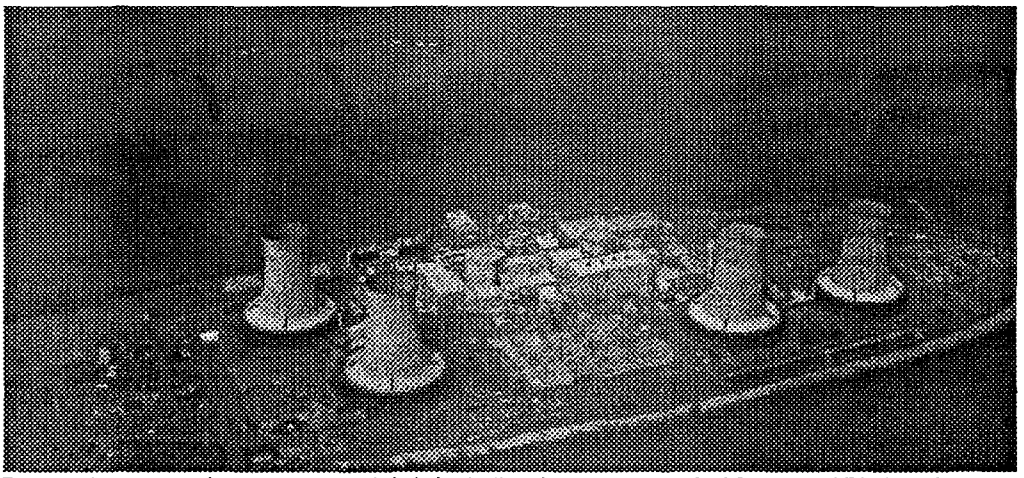
MAÎTRISER LE RISQUE

Les risques d'accident dans les centrales nucléaires ne peuvent être tenus pour nuls. Le problème est d'évaluer leur probabilité. La méthode des études probabilistes de sûreté permet de le faire et, en identifiant les sources de risque potentiel, de les prévenir. Elle ne saurait cependant se substituer aux autres modes de décision.

LAURENT MAGNE
Département Etudes de Sûreté de Fiabilité,
Service Réacteurs Nucléaires et Echangeurs.

Les applications des études probabilistes
Comment insérer les études probabilistes dans un processus de décision ?



De nombreux enseignements ont été tirés de l'accident survenu le 28 mars 1979 dans la centrale de Three Mile Island.

31-15

La sûreté des centrales nucléaires a été une préoccupation majeure des concepteurs. Pour la

garantir, les choix technologiques ont toujours été fondés, dans le passé, sur des études de physique et de technologie industrielle, dites « déterministes ». Les circuits, les systèmes de sauvegarde, les procédures d'exploitation ou de maintenance ont été conçus pour prévenir, avec suffisamment de marge, la plupart des accidents. Pourtant, malgré ces précautions, les risques ne peuvent jamais être considérés comme nuls. Pour les évaluer, on dispose d'un outil d'un genre nouveau : les études probabilistes de sûreté (EPS).

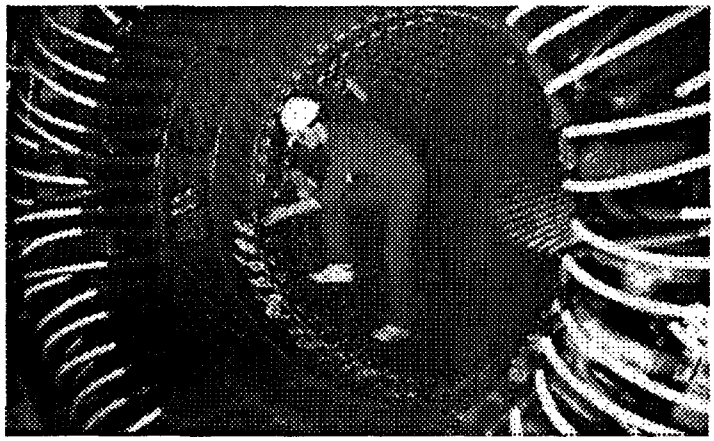
Les EPS des centrales nucléaires ont débuté au milieu des années 1970, aux États-Unis, avec le rapport dit *Rasmussen* (Reactor Safety ; an assessment of accident risks in US commercial nuclear power plants, Wash 1400, nureg 74/014, usnrc, octobre 75). Un des objectifs était d'évaluer la probabilité des accidents en fonction de leur gravité : selon l'auteur du rapport américain les accidents les plus graves devaient avoir une probabilité extrêmement faible.

Au-delà de l'évaluation probabiliste elle-même, la commission réglementaire américaine a considéré que de telles études étaient très intéressantes par la réflexion d'ensemble qu'elles impliquent sur les risques. C'est pourquoi, au début des années 1980, lors d'un vaste programme d'évaluation du risque de toutes les centrales, dénommé *Individual Plant Examination,* la commission a suggéré aux exploitants d'utiliser des évaluations probabilistes. Dans toutes les centrales nucléaires, il s'agissait de mener l'analyse la plus complète possible du risque : les dangers potentiels, les points faibles, etc.

L'objectif d'une EPS est d'identifier et d'évaluer des scénarios accidentels menant à un événement redouté, qu'on assimile au risque (par exemple, l'endommagement du cœur, ou des rejets radioactifs dans l'environnement).

L'identification des scénarios accidentels est une tâche difficile, car le système analysé est d'une complexité à la fois :
- structurelle : une centrale nucléaire est formée d'un nombre considérable de circuits, sous-systèmes ou composants, faisant appel à des technologies variées (neutronique, thermohydraulique, chimique, électrotechnique, etc.) ; - fonctionnelle : un grand nombre de fonctions sont remplies (transfert d'énergie, régulation, protection, sauvegarde, etc.) ;
- organisationnelle : une installation nucléaire met en œuvre des équipes multiples et des tâches diverses (conduite, inspections, maintenance, animation, etc.).

Une telle analyse globale présente l'avantage de confronter des acteurs aux compétences diverses, qui ne se rencontrent pas fréquemment : des concepteurs, des responsables de procédures d'exploitation, des exploitants, des spécialistes du facteur humain, etc. Toutes ces connaissances sont synthétisées en modèles mathématiques, par des « fiabilistes », spécialistes des études probabilistes.



La prise en compte du facteur humain est essentielle dans le cadre des études probabilistes. En haut, salle de commande de la centrale de Chooz et, en bas, maintenance d'un alternateur.

En France, EDF et le CEA ont engagé de telles analyses au milieu des années 1980. Les premières ont été terminées en 1990. Elles ont d'abord permis de confirmer des hypothèses déjà connues sur les risques des centrales nucléaires. Ainsi, par exemple, le risque issu de « petites fuites d'eau » sur le circuit primaire est paradoxalement plus élevé que le risque issu de « grosses fuites ». Cela est dû au fait que les systèmes sont dimensionnés pour faire face à des fuites d'eau importantes : dans ce cas, un système de sauvegarde automatique prend le relais des opérateurs pour gérer la situation accidentelle. En revanche, dans le cas d'une petite fuite d'eau, le diagnostic n'est pas toujours clair. L'opérateur peut avoir tendance à croire que le déclenchement du système de sauvegarde est intempestif, et décider de le mettre hors circuit pour « garder la main ».

Une telle idée, confirmée par l'étude française, était déjà assez répandue depuis l'accident de Three Mile Island, survenu le 28 mars 1979. L'accident avait causé des dégâts matériels importants, mais n'a eu aucune autre conséquence grave, ni humaine ni radiologique. De nombreux enseignements ont été tirés de cet accident, si bien que la sûreté de ce type de centrales nucléaires a beaucoup progressé depuis le début des années 1980. Les études ont ensuite permis de souligner des aspects moins connus à l'époque. Ainsi, par exemple, à la différence d'un train ou d'un avion, une centrale nucléaire à l'arrêt présente toujours un risque, au moins aussi important, sinon plus, qu'une centrale nucléaire en pleine puissance. En effet, même quand la réaction nucléaire est bloquée, il faut continuer à refroidir le cœur.

Enfin, ces études exhaustives ont permis d'identifier quelques rares scénarios de pannes, inconnus jusqu'alors.

Cette analyse de risque aboutit à la constitution de modèles mathématiques complexes[1] (voir « Comment réalise-t-on une étude probabiliste de sûreté ? »). Parce qu'on ne peut pas appréhender tout le volume des informations, ou parce qu'on ne sait pas évaluer certains aspects, une simplification s'impose : il est nécessaire de considérer des situations ressemblantes comme équivalentes, de prendre des défaillances partielles pour des défaillances totales, de passer sous silence certains détails.

Les situations les plus délicates sont celles où intervient l'homme. Elles sont bien sûr nombreuses, car il fait partie intégrante du système. Mais les descriptions de l'homme, dans ces études, sont assez pauvres. On ne s'intéresse, au long d'un scénario, qu'à une ou deux décisions prises par les opérateurs. De nombreux aspects, notamment organisationnels, sont traités de façon trop simple. Ensuite, la quantification probabiliste des comportements est

fondée sur des données rudimentaires, même si de gros efforts d'observation des opérateurs ont été effectués par l'intermédiaire d'essais sur simulateurs de taille réelle, qui reproduisent des conditions très proches de la réalité.

Ces études, si elles apportent un éclairage intéressant sur quelques actions clés des hommes en situation accidentelle, ne suffisent pas à faire le tour de l'évaluation de la sûreté. D'autres analyses (qualitatives, ergonomiques, psychosociologiques) doivent être menées, bien au-delà de la seule évaluation probabiliste.

L'exemple du facteur humain souligne que les connaissances mises en œuvre dans les EPS reposent inévitablement sur des hypothèses, extrapolations et approximations. Elles sont donc entachées d'incertitudes. Comment alors valider ces modèles ? On ne dispose pas de vérification expérimentale. Les événements redoutés dont on évalue la probabilité sont heureusement trop rares pour disposer d'une observation statistique. La seule méthode possible est la « revue critique » : le modèle construit par une équipe est confié à d'autres spécialistes qui émettront critiques et recommandations.

En France, EDF a construit les modèles des centrales nucléaires de 1300 MW, et le CEA ceux des centrales de 900 MW. Entre 1991 et 1994, les deux organismes se sont livrés à un long travail de comparaison des hypothèses, des choix et des données.

COMMENT RÉALISE-T-ON UNE ÉTUDE PROBABILISTE DE SÛRETÉ ?

Une EPS revêt la forme suivante :
- le risque est assimilé à un événement redouté, dont on définit précisément les caractéristiques. Par exemple, le début d'endommagement du coeur, caractérisé par une température élevée des éléments combustibles (1 204 °C) ;
- l'événement redouté ne peut être atteint que par des scénarios accidentels, c'est-à-dire la conjonction d'autres événements moins graves : des accidents dits « initiateurs », des actions humaines, des pannes de sous-systèmes ;
- chacun de ces événements est lui-même décomposé jusqu'aux « sous-événements » les plus élémentaires : défaillances de matériels, diagnostics erronés, etc.;
- à chaque sous-événement élémentaire est associée une probabilité, qui peut être quantifiée à partir, par exemple, se statistiques sur les défaillances des composants voir « Les facteurs d'importance des matériels »). La connaissance de l'ensemble de ces probabilités permet d'évaluer la probabilité du risque.

Une EPS est finaliment composée d'un ensemble de modèles assez complexes représentant les scénarios accidentels et les études locales plus détaillées. L'EPS « 1300 » d'EDF en comprend environ 500.
Le tout est bien sûr informatisé, pour gérer les connaissances et les données, pour effectuer les calculs, et pour exploiter les résultats.

Les applications des études probabilistes

Malgré leurs limites, les études probabilistes présentent l'avantage d'être des modèles globaux du risque des centrales. On peut donc utiliser ces modèles pour orienter des décisions d'exploitation, de maintenance ou de conception.

Par exemple, EDF a lancé, depuis 1994, un important programme d'optimisation de la maintenance, visant à améliorer la sûreté des centrales, leur disponibilité et leurs coûts d'exploitation. Concernant la sûreté, les EPS ont été retenues comme un des moyens d'optimisation. Elles sont utilisées pour fournir des évaluations relatives de l'importance, vis-à-vis des risques, de certains matériels (voir « Les facteurs d'importance des matériels »). La liste de ceux qui sont jugés « critiques » fait l'objet d'un programme de maintenance préventive. Lors d'une étape ultérieure, la prescription de leurs tâches de maintenance est améliorée.

Les EPS sont particulièrement utiles pour détecter des points sensibles. Mais elles ne suffisent pas à tous les détecter. Un matériel peut être
« critique » au sens des EPS, mais aussi au sens de la sûreté
« déterministe » (car lié à des dispositions réglementaires), ou au sens de la disponibilité des centrales, ou bien encore des coûts d'exploitation. C'est pourquoi les analyses probabilistes de sûreté sont complétées par d'autres études.

Aux États-Unis aussi, les applications des EPS se développent dans un grand nombre de directions. Elles apparaissent comme un bon outil pour répartir efficacement les ressources disponibles tout en conservant un très haut niveau de sûreté.

Le développement foisonnant de ces applications pose avec une acuité accrue les problèmes liés à la complexité des systèmes, les lacunes des modèles et la difficulté de leur validation. Les efforts de la recherche doivent porter dans toutes ces directions, car les études probabilistes sont sollicitées pour faire partie intégrante des processus de décision.

Maîtriser la complexité :

Il faut apprendre à simplifier et à fournir des résultats pertinents, même lorsque les connaissances sont imparfaites.

Première idée : mettre de l'ordre dans les modèles, par des méthodes systématiques, des guides de réalisation, par une rigueur accrue de modélisation. Deuxième idée : parvenir à séparer, lors de la modélisation, les aspects les mieux maîtrisés de ceux qui restent entachés de fortes incertitudes, et exigent encore de grands développements. D'un côté, des modèles de référence, robustes et validés. De l'autre côté, des modèles ciblés, probabilistes ou non, pour approfondir les points les plus délicats ou les moins décrits, afin de faire évoluer ces modèles de référence.

Repousser les limites :

Il faut chercher à combler les principales lacunes des EPS :
- l'évaluation du facteur humain. Sa modélisation probabiliste est insuffisante. Elle doit être plus représentative, afin de prendre en compte à la fois les aspects individuels et collectifs, l'activité des individus et l'organisation du travail ;
- les données d'entrée. Les EPS dépendent fortement de leur qualité. Etablir un recueil d'informations statistiques sur les défaillances des matériels est loin d'être immédiat. Cela suppose une organisation très lourde ainsi qu'une définition claire de ce qu'on appelle une défaillance. Par exemple, une légère défaillance, en situation normale, donnera lieu à une

réparation, alors que le matériel pourrait continuer à fonctionner en situation accidentelle. Les opérateurs qui recueillent les informations à la source ont donc besoin de critères précis. C'est déjà délicat pour les matériels isolés, c'est encore plus difficile si l'on souhaite des informations sur les dépendances qu'entretiennent certains composants entre eux (voir « Les modes communs de défaillance ») ;
- certains sous-systèmes des centrales nucléaires sont particulièrement complexes. C'est notamment le cas des systèmes de contrôle-commande, qui comportent des logiciels. Certains scénarios sont aussi très compliqués, du fait des nombreuses interdépendances (temporelles, fonctionnelles) dont ils rendent compte. De gros progrès restent à accomplir dans la modélisation et l'évaluation probabiliste du comportement de ces systèmes ;
- enfin, comment évaluer l'incertitude des résultats ? L'incertitude est liée aux données d'entrée. Mais elle tient aussi aux phénomènes physiques mis en jeu en situation accidentelle (aucune expérimentation en vraie grandeur n'est possible) ou au facteur humain.

Mieux valider les modèles :

La pratique de la revue critique par d'autres spécialistes des EPS pourrait être étendue à d'autres scientifiques (physiciens ou ingénieurs du monde « déterministe »), car la confrontation de différents points de vue est souvent féconde.

La validation des modèles n'est possible que si le lecteur dispose, clairement et simplement, de toutes les hypothèses retenues en amont d'un résultat. Mais si la documentation explicative est trop volumineuse (une EPS peut représenter jusqu'à 15000 pages de documentation), elle ne sert plus à rien. Trop d'information nuit. Il faut sans doute creuser des idées du côté des outils informatiques (mode d'emploi informatisé, documentation structurée,...).

Comment insérer les études probabilistes dans un processus de décision ?

Au-delà de ces efforts des chercheurs, se pose à l'ensemble de la communauté nucléaire la question de la place des EPS dans les décisions concernant la sûreté. Dans les processus de décision (pour l'exploitation, la maintenance ou la conception), les décideurs ne sont pas spécialistes des EPS. Comment insérer ces études dans les processus de décision ? Les statisticiens économistes se posent la même question lorsqu'ils préparent des dossiers pour un gestionnaire.

Un transfert de connaissance doit être organisé, et une organisation mise en place, en définissant notamment qui sont les utilisateurs des EPS.

D'abord, on trouve les ingénieurs d'études ou les chercheurs, garants de la connaissance contenue dans les EPS, qui produisent les modèles de référence, ou qui approfondissent les points délicats.

Ensuite, on trouve les personnes qui font fonctionner les modèles pour produire les résultats et aider aux décisions. Ils doivent être suffisamment expérimentés pour exploiter les EPS à bon escient, et pour communiquer les résultats.

Enfin, les destinataires des résultats, qui seront amenés à prendre les décisions. Ils doivent être sensibilisés aux études probabilistes, en connaître les hypothèses clés, pour recevoir les résultats sans erreur d'interprétation.

Ce qui domine, dans le processus ainsi décrit, c'est la communication, le dialogue, le transfert d'informations, le jugement, la délibération. Beaucoup d'efforts doivent être faits dans ce sens, notamment par les chercheurs.

Grâce au volume et à la qualité des connaissances manipulées dans les EPS, ces modèles sont des outils puissants d'interrogation et de détection des points sensibles. De ce fait, ils peuvent être un bon moyen d'aide à la diffusion d'une culture de sûreté indispensable à l'exploitation des centrales nucléaires. Mais il n'est en général pas possible de déduire de leurs seuls enseignements les modifications ou les solutions à apporter. Par exemple, imaginons que, dans un scénario accidentel, l'action humaine soit identifiée comme un facteur « sensible ». Faut-il en tirer la conclusion systématique que la bonne modification tient à l'automatisation de l'action ? Certes, le scénario considéré verrait sa probabilité réduite. Cependant, on est en général incapable de mesurer en retour les effets de cette modification sur l'ensemble de l'installation. Génère-t-elle d'autres scénarios ? Quelle influence a-t-elle sur les autres actions des opérateurs ? Ces questions ne relèvent plus de l'approche probabiliste. Attention donc à un usage des études probabilistes à mauvais escient. Ce sont des outils irremplaçables d'évaluation du risque, par la qualité de leur analyse, la perception des interactions des systèmes entre eux, et par leur recherche d'exhaustivité. Mais leur « rationalité quantitative » a ses limites. Si les EPS tendent à gagner en importance dans les processus de décision, elles ne doivent pas se substituer à l'ingénierie traditionnelle ni à d'autres outils de décision, mais seulement les compléter.

LES FACTEURS D'IMPORTANCE DES MATERIELS

Les EPS peuvent être utilisées pour évaluer l'importance de certains sous-événements élémentaires relativement à un événement redouté. Pour cela, il existe de nombreux indicateurs, appelés « facteurs d'importance », que l'on calcule en fonction de l'impact d'une variation de la probabilité d'une action élémentaire sur l'événement redouté.
Dans la pratique, on considère généralement le facteur d'augmentation de risque, ou FAR, qui mesure l'acroissement relatif du risque si la défaillance s'est produite, et le facteur de diminution de risque, ou FDR, qui mesure la diminution relative du risque si la défaillance ne se produit jamais.
Ces deux indicateurs diffèrent quant à leur valeur, quant aux hiérarchies auxquelles ils aboutissent, et quant aux interprétations possibles. Prenons l'exemple d'un moteur qui n'aurait que deux scénérios possibles de panne : la rupture de l'arbre, et la conjonction d'une fuite d'huile et d'un défaut de détection (panne du voyant lumineux).
Considérons que l'arbre est très fiable. Il y a peu de chance de le voir casser. Par contre, une fuite d'huile combinée à une panne de voyant est plus fréquente.
Nous pouvons tirer les conclusions suivantes : l'huile contribue fortement au risque. La maintenance devrait être orientée, autant que possible, vers une fiabilisation de ce point. En revanche, l'arbre contribue peu au risque. La maintenance devrait être orienté vers des inspections afin d'éviter une rupture.

	FAR	FDR	Commentaires
Arbre	**fort**	**faible**	Si l'arbre est cassé, il n'y a plus aucune ligne de défense : le

Arbre	**fort**	**faible**	FAR est donc très fort. Mais l'arbre est déjà très fiable. On ne peut donc espérer aucune diminution sensible de risque : le FDR est très faible.
Huile	**faible**	**fort**	S'il y a une fuite d'huile, il reste une ligne de défense (le voyant lumineux). Le FAR est relativement peu élevé. Les éléments qui pèsent le plus sur les risques sont l'huile et le voyant. C'est là qu'on peut espérer le plus de diminution de risque. Le FDR est donc très fort.

Dans les études des matériels des centrales nucléaires, on se heurte à trois difficultés particulières :
- pour déterminer si un composant est critique au sens des EPS, il faut des seuils. Leur choix est délicat. On tente de trouver, dans la réglementation ou dans d'autres études, des éléments permettant de les fixer en cohérence avec d'autres choix déjà faits. Sinon, ils doivent être fixés arbitrairement, après une délibération entre les parties concernées ;
- les calculs d'estimation des facteurs d'importance sont beaucoup plus détaillés que les évaluations globales effectuées avec les EPS. De ce point de vue, beaucoup d'événements sont insuffisamment modélisés. Chaque calcul doit donc être accompagné d'une étude complémentaire importante, afin d'assurer la validité nécessaire des résultats ;
- comment utiliser les résultats en maintenance ? Même dans l'exemple simple du moteur, les mots fiabilisation ou inspection ne sont pas très concrets. Si un matériel est critique, ce n'est pas une raison pour le démonter souvent. Une maintenance trop fréquente peut le fragiliser, ou le rendre trop longtemps indisponible, ce qui nuirait à la sûreté de l'ensemble. Les facteurs d'importance ne sont que des éléments d'information parmi d'autres pour prendre des décisions.

LES MODES COMMUNS DE DEFAILLANCE

On dit qu'une défaillance est « de mode commun » quand elle affecte simultanément ou en cascade plusieurs matériels.

Prenons l'exemple de deux pompes placées en redondance dans un circuit hydraulique, de sorte qu'une seule suffit à assurer le mouvement du fluide. Certaines pannes, comme la perte généralisée de l'alimentation électrique, peuvent affecter simultanément les deux pompes. C'est une défaillance de cause commune, facilement identifiable.

Mais les deux pompes peuvent aussi tomber en panne ensemble pour des raisons moins évidentes : un environnement corrosif, un incendie, etc. Par ailleurs, si elles sont de la même marque, des défauts de série ont pu apparaître à la fabrication. Enfin, la maintenance, la mise en service ou l'entretien sont sources d'interventions similaires sur chacune des pompes. Une erreur systématique est toujours possible.

Il existe donc de nombreuses causes potentielles de défaillances simultanées, sans que l'on sache les recenser de façon exhaustive ni les évaluer précisément. Ces modes communs posent deux difficultés aux fiabilistes :

- un manque d'informations statistiques. Les événements affectant plusieurs matériels simultanément sont très rares. Ensuite, il faut savoir déceler, parmi les défaillances observées, celles qui « auraient pu » apparaître sur des composants voisins. Enfin, la notion de simultanéité est difficilement utilisable dans la pratique : certaines défaillances de cause commune peuvent être très espacées dans le temps ;

- lors de la modélisation du risque, le fiabiliste doit choisir, parmi tous les composants, ceux qui sont susceptibles de présenter une dépendance significative. Comme les données d'exploitation ne fournissent pas d'indications suffisantes, ce choix comporte une forte part d'arbitraire. Lors d'une étude passée, il s'est porté sur « tous les composants identiques et redondants au sein d'un même sous-système ». On aurait aussi bien pu y inclure « des composants proches (non seulement identiques), et au sein de sous-systèmes différents ».

Les enseignements que l'on peut tirer de ces modes communs ne sont pas plus évidents. Reprenons l'exemple des deux pompes. Après avoir décelé et quantifié une dépendance, le fiabiliste pourra la souligner comme un point faible de l'installation. Mais quelles solutions préconiser ? Faut-il améliorer la maintenance, protéger les pompes des agressions, ou diversifier leur conception? Seule une étude détaillée du problème (et non une étude probabiliste) pourra éventuellement répondre. Enfin, si une solution est proposée, les outils fiabilistes sont beaucoup trop limités pour en évaluer l'impact.

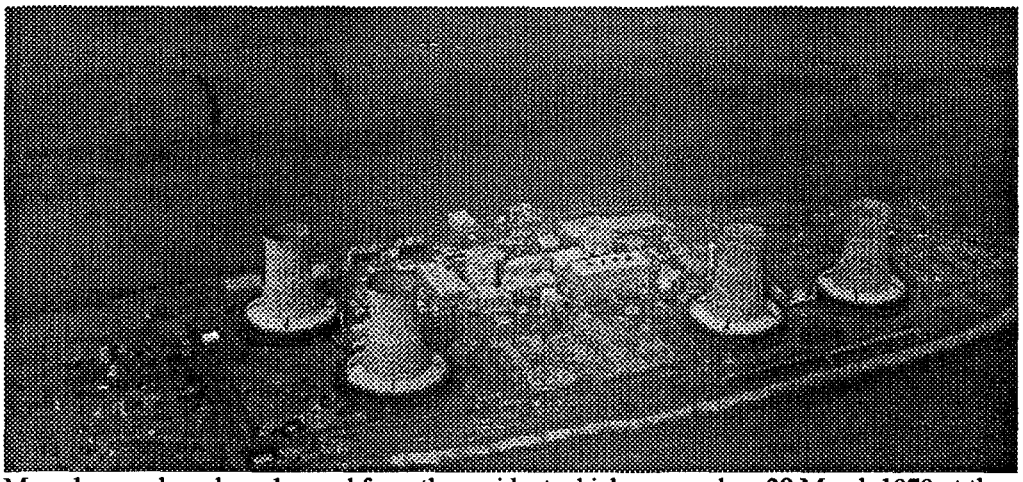
précédent sommaire suivant

RISK MANAGEMENT

There is always a risk of an accident occurring at a nuclear powerplant, however small. The problem lies in estimating the probability of it occuring. The method of probabilistic safety assessment provides this estimate, and by identifying the sources of potential risk, makes it possible to prevent them from occurring. It is not, however, a substitute for other decision-making processes.

LAURENT MAGNE
Safety and Reliability Branch, Nuclear Reactors and Heat Exchangers Department.

Applications of probability studies
How can probabilistic studies be introduced into the decision-making process?



Many lessons have been learned from the accident which occurred on 28 March 1979 at the Three-Mile Island powerplant.

Safety in nuclear powerplants is a major preoccupation of designers. In the past, technological choices to ensure safety have been based on what are known as 'determinist' studies in physics and industrial technology. Circuits, safety systems, operation and maintenance procedures, etc. are all designed to prevent, within an acceptable margin, the majority of accidents. Despite these precautions, however, risk can never be regarded as zero. But now there is a new tool available: probabilistic safety assessment (PSA).

Application of PSA in nuclear powerplants began in the mid-seventies in the USA, as reported by Rasmussen (Reactor Safety; an assessment of accident risks in US commercial nuclear power plants, Wash 1400, nureg 74/014, usnrc, Oct. 1975). One of its objectives was to evaluate the probability of accidents as a function of their seriousness: according to the author of the American report, the most serious accidents should have the lowest probability.

In addition to the probabilistic evaluation itself, the US regulatory commission considered that such studies were extremely interesting in terms of the overall considerations of risk which they implied. For this reason, at the end of the eighties, in the Individual Plant Examination, a vast programme of risk evaluation in all powerplants, the commission recommended that operators use probabilistic evaluation. In all nuclear powerplants, it meant carrying out the most thorough analysis possible, covering potential dangers, weak points, etc.

The objective of a PSA is to identify and to evaluate accident scenarios related to an unacceptable event with which risk is associated (e.g. core damage, radioactive leakage to the environment, etc.).

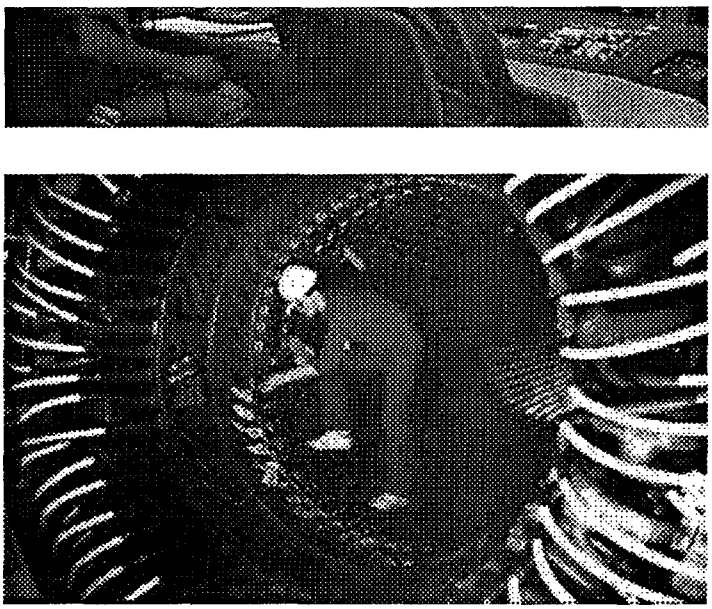
The identification of accident scenarios is a difficult task, because the system analysed has an innate complexity which is simultaneously:

- structural: a nuclear powerplant is made up of a considerable number of circuits, sub-systems, or components, in which various technologies are involved (nuclear, thermohydraulic, chemical, electrotechnical, etc.);

- functional: a large number of functions are involved (energy transfer, control, protection, safety, etc.);

- organisational: a nuclear facility requires many teams involved in various tasks (operation, inspection, maintenance, co-ordination, etc.).

A global analysis such as this has the advantage of bringing together experts from various backgrounds who rarely have an opportunity to meet: designers, line managers, operators, ergonomists, and so on. All these skills are synthesised in mathematical models by risk engineers, specialists in probability studies.



Taking the human factor into account is essential in probability studies.
Top: the control room at the Chooz plant.
Bottom: alternator maintenance.

In France, EDF and the CEA have been engaged in these analyses from the mid-eighties.The first ones were concluded in 1990. First of all they confirmed previously-formulated hypotheses regarding risks in nuclear powerplants. Thus, for instance, the risk involved in 'small leakages of water' from the primary circuit is paradoxically greater than that associated with 'large leakages'. This is due to the fact that the systems are designed to deal with significant leakages: in such cases, an automatic safety system takes over from the operators to deal with the accident situation. In contrast, when there is only a minor water leak, the diagnosis is not always clear. The operator can have a tendency to think that the safety system tripping has been faulty and override it.

This sort of thinking, confirmed by the French study, has been widespread since the accident at Three Mile Island on 28th March 1979. This accident caused important material damage, but had no other serious human or radiological consequences. Numerous lessons have been learned from this accident, and the safety of this type of nuclear powerplant has improved significantly since the beginning of the eighties. The studies also underlined the aspects least known at the time. Thus, for instance, there is a fundamental difference between the case of a train or an aircraft, in that even when shut down, a nuclear plant presents a constant risk which is just as great as that of a fully-operational plant, perhaps even more so. Even when the nuclear reaction is inhibited, it is still necessary to provide cooling for the core.

These exhaustive studies have in fact brought to light several rare breakdown scenarios which had hitherto not been recognised.

This risk analysis involves the creation of complex mathematical models(1) ('How is a probability safety assessment carried out ?'). Because it is not always possible to handle the large volume of information, or because certain aspects cannot be evaluated, a degree of simplification is imposed: it becomes necessary to consider situations recognised as equivalent, to take partial failures as total failures, or to neglect certain details. The most delicate situations are those involving human beings. They are certainly numerous, for humans are an integral part of the system, but in these studies descriptions of human activities are quite scarce. Throughout the scenario, interest was shown in only one or two decisions taken by operators, and many aspects, notably organisational aspects, are given an over-simplified

treatment. Finally, the probabilistic quantification of behaviour is based upon rudimentary data, even if the substantial efforts of observation by operators have been carried out via full-scale simulator tests which reproduce conditions very close to reality.

Although these studies may shed light on some key human activities in an accident situation, they are not sufficient for a complete safety evaluation. Other analyses (qualitative, ergonomic, psycho-sociological) must be carried out, even beyond the single probabilistic evaluation. The example of the human factor underlines the fact that the knowledge deployed in a PSA inevitably rests upon hypothesis, extrapolation, and approximation. As a result, they are full of uncertainties. How then are such models to be validated? It is not possible to verify them experimentally. The events involved in evaluating the probability are (fortunately!) too rare to provide statistical confirmation. The only possible method is the 'critical review' : the model drawn up by a team is given to other specialists who provide criticisms and recommendations.

In France, models of 1,300 MW nuclear powerplants have been constructed by EDF, and 900 MW stations by the CEA. Between 1991 and 94, these organisations undertook a lengthy process of comparison of hypotheses, choices, and data.

HOW IS A PROBABILISTIC SAFETY ASSESSMENT CARRIED OUT?

The operational method of a PSA is as follows:

- the risk is associated with an 'unacceptable event', the characteristics of which are precisely defined. For example, the onset of core damage, characterised by elevated temperatures of combustible components (1,204°C)

- the 'unacceptable event' can only occur via many accident scenarios, i.e. conjunctions of other, less serious 'intermediate events'.The first one is known as 'the initiator'. This can be followed by human error, sub-system failures, etc.

- each of these 'intermediate events' can itself be broken down into the most elementary sub-events known as 'basic events': equipment failure, diagnostic error, etc.

- each 'basic event' has a probability of occurrence which can be quantified by, for example, component failure statistics (see 'Risk importance of equipment'). Overall knowledge of these probabilities allows the risk probability to be evaluated.

Ultimately, a PSA is composed of a totality of complex models representing the accident scenarios and the most detailed local studies. The '1300' PSA carried out by EDF covers about 500.

The total PSA then has to be fully computerised to manage the data and knowledge involved, to perform calculations, and to exploit the results.

Applications of probability studies

Despite their limitations, probability studies have the advantage of being global models of risk in powerplants. They can therefore be used to guide decision-making regarding operation, maintenance, and design.

For example, in 1994, EDF launched an important programme of maintenance optimisation, intended to improve powerplant safety, availability, and operational cost. With regard to safety, PSA has been retained as one of the means of optimisation. It is used to supply evaluations relative to the importance, in terms of risk, of certain equipment (see 'Risk importance of equipment'). The list of those adjudged to be "critical" forms the basis of a programme of preventive maintenance. In a later stage, the definition of their maintenance tasks is improved.

The PSA is particularly useful for detecting sensitive areas, though it is not sufficient to detect all of them. Equipment can be critical in terms of the PSA, but it can also be critical in terms of deterministic safety (because it is linked to regulatory conditions), or in terms of powerplant availability , or even of operational costs. This is why probabilistic safety analyses have to be complemented by other studies.

In the USA, applications of PSA have also developed in a number of different directions. PSA applications seem to be a useful tool for the efficient allocation of available resources, while at the same time ensuring a high level of safety.

The widespread development of these applications places strong emphasis on problems associated with system complexity, on the limitations of models, and on the difficulty of their validation. Research efforts must be aimed in all these directions, because probabilistic studies are being called upon to take an integral part in the decision-making process.

Managing complexity:

It is necessary to simplify and to supply relevant results, even when knowledge is imperfect. Initial concept: setting the models in order by systematic methods, design guides, more rigourous modeling. Secondary concept: striving to separate during modelling those factors which are most easily manageable from those which involve the highest levels of uncertainty, and thus still require further levels of development. On the one hand, there are robust and valid reference models. On the other, there are target models, probabilistic or otherwise, for more in-depth investigation of the most sensitive and least understood points, so that these reference models can evolve.

Rolling back limits:

It is necessary to try to fill in the principal gaps in the PSAs:

- evaluation of the human factor. Probabilistic models of this are inadequate. They need to be more representative, so as to be able to take into account simultaneously both individual and collective aspects, activities of individuals and the organisation of work;

- input data. PSAs depend very much on input data quality, but establishing a collection of statistical information on equipment failures is not something that can be done instantly. That presupposes a high degree of organisation as well as a clear definition of what is meant by a failure. For example, under normal circumstances a small failure will lead to a repair whereas the equipment could continue to operate in an accident situation. Operators who collect data

at source therefore need precise criteria. This is difficult enough for equipment in isolation, but it is many times more difficult if information on the interdependence of certain components is required (see 'Common cause failures');

- certain sub-systems in nuclear powerplants are particularly complex. This is especially the case with control and command systems incorporating softwares. Some scenarios are also very complex because of the numerous levels of interdependence (temporal or functional) which have to be taken into account. Overall progress depends upon being able to incorporate a probabilistic evaluation of the behaviour of these systems into the model;

- evaluating the confidence level of the results. This depends not only on the uncertainties of the input data, but also on the physical phenomena introduced by the accident situation (for which no full-scale tests are available), or on the human factor.

Better validation of models:

The practice of the critical review of the PSAs by other specialists could be extended to include scientists in other disciplines, notably physicists or engineers from the 'deterministic' world, because confrontation between different viewpoints can be very profitable.

Validation of models is possible only if the reader has available in clear and simple terms all the hypotheses formulated ahead of a result. But if the explanatory documentation is too voluminous (and a PSA can run to 15,000 pages), it will never get started. Too much information is as bad as too little. It will certainly be necessary to look at computer-based tools (computerized instructions for use, structured documentation, etc.).

How can probabilistic studies be introduced into the decision-making process?

Over and above these research efforts, there exists among the nuclear power community the question of the place of PSA in decisions concerning safety. In the decision-making process (for operation, maintenance, or design), the persons making the decisions will not be PSA specialists. How then are these studies to be introduced into the decision-making process? Economic statisticians ask the same question when preparing management documentation.

Knowledge transfer must be organised, and an organisation set up, particularly in order to define who are the users of PSA.

First of all, it is necessary to find design and research engineers who will be the guarantors of the knowledge contained in the PSA, and who will produce the reference models, and investigate sensitive areas in depth.

The next requirement is for people to operate the models to produce results and assist decision-making. They must be sufficiently experienced to exploit the PSA correctly, and to communicate the results.

Finally, those for whom the results are intended, the decision makers, must be involved. They must be aware of probability studies, and know the key hypotheses, so as to be able to interpret the results accurately.

The factors dominating the process just described are communication, dialogue, information transfer, judgement, and deliberation. Great efforts must be aimed in these directions, especially by researchers.

Because of the volume and the quality of the information handled in the PSA, these models are powerful tools for detection and investigation of sensitive areas. This makes them very useful in the diffusion of an indispensable culture of safety in the operation of nuclear powerplants. But, in general, it is not possible to infer from these lessons alone the modifications or solutions which have to be applied. For instance, if in a particular accident scenario, a human action is identified as a 'sensitive factor'. Can it therefore be systematically concluded that a good modification would be to automate that action? Certainly, the scenario under consideration might well be contained, but on the other hand it is not possible to assess the effects of this modification on the whole facility. Would it generate further accident scenarios? What effect would it have on other operator actions? These questions are no longer a matter for the probabilistic approach. Therefore we must guard against misuse of probabilistic studies. They are irreplaceable tools for the evaluation of risk, by the quality of their analysis, their perception of system interaction, and the exhaustive nature of their research. But what might be called their 'quantitative rationality' has its limits. If PSA tends to gain in importance in the decision-making process, it must be as an adjunct rather than as a substitute for traditional engineering or other decision-making tools.

RISK IMPORTANCE OF EQUIPMENT

Probability safety assessment can be used to evaluate the importance of certain elementary sub-events relative to an unacceptable event. Numerous indicators, known as factors of importance, exist which are calculated as a function of a variation of the probability of an elementary action upon a major event.
In practice, the two factors considered are Risk Achievement Worth (RAW), which measures the relative increase in risk if the failure occurs, and the Risk Reduction Worth (RRW), which measures the relative decrease in risk if the failure never occurs. These two indicators differ not only in their values, but also in the hierarchies within which they occur, and in their possible interpretations. As a simple example, consider an engine which has only two possible breakdown scenarios: fracture of a shaft, or an oil leak in combination with lack of detection (warning light failure). It can be assumed that the shaft is very reliable and that there is little chance of fracture occurring, whereas oil leaks and warning-light failure are much more frequent. The following conclusions can therefore be reached. Oil is a high risk contributor, so that maintenance must be directed as firmly as possible towards increased reliability in this area. In contrast, the risk associated with the shaft is small, and maintenance need only be directed towards inspections aimed at avoiding fracture.

	RAW	RRW	Comment
Shaft	**high**	**low**	If the shaft fractures, there is no second line of defence: the RAW is therefore very high. But the shaft is also very reliable, so that no reduction in risk can be foreseen, and the RRW is therefore very low.
Oil	**low**	**high**	If there is an oil leak, the warning light provides a line of

defence, so that the RAW remains fairly low. The events which have the greatest effect on risk are the oil and the warning lamp, so that it is there that the main chance of reducing risk lies. The RRW is therefore very high.

In studying equipment for nuclear powerplants, three main areas of difficulty are encountered:
- thresholds are necessary in determining whether a component is critical in the PSA sense, and their selection is sensitive. It is preferable if, from the regulations or in other studies, elements enabling these thresholds to be set in relation to choices already made can be determined. Otherwise, they have to be set arbitrarily after consultation between the parties concerned;
- calculations to estimate factors of importance are much more detailed than the global evaluations carried out with the PSA. From this point of view, many events are not sufficiently well modelled. Each calculation must therefore be accompanied by an important complementary study in order to ensure the necessary validation of results;
- there is then the problem of how to apply the results in terms of maintenance. Even in the simple example of the engine, the words
'reliability' and 'inspection' need further definition. The fact that a piece of equipment is critical is not necessarily a reason for frequent disassembly. In fact, too-frequent maintenance can itself cause embrittlement problems, or keep the component unavailable for too long, all of which can adversely affect overall safety. The factors of importance are only elements of information among others in decision-making.

COMMON CAUSE FAILURES

A failure is defined as in 'common cause failure' when it affects several pieces of equipment simultaneously or consecutively.

Take as an example two pumps located in a hydraulic circuit redundantly, so that only one is actually needed to ensure the flow of fluid. Certain breakdowns, such as a general failure of the electrical supply system, can affect the two pumps simultaneously. This is an easily identifiable common cause failure.

But the pumps could also suffer total breakdown for less obvious reasons: a corrosive environment, a fire, or similar. Also, if they are the same make, it is possible that design or manufacturing faults could affect both at the same time. Likewise, maintenance, commissioning, or servicing are all sources of similar intervention on both pumps, and a systematic error is always possible.

There are then many potential causes of simultaneous failures which it is not possible to list exhaustively or evaluate precisely. These common causes present two main difficulties for reliability
engineers:

- a lack of statistical information. Events affecting several pieces of equipment simultaneously are very infrequent. Again, there is a need to detect, from among the various failures observed, those which 'would have been able' to affect neighboring

components. Finally, the concept of simultaneity is difficult to use in practice: some common cause failures can occur at widely spaced intervals;

- during risk modeling, the reliability engineer must choose from among the components those which are liable to have a significant degree of dependence. Since operational data do not supply sufficient indication, this choice must be to a large extent arbitrary. In one previous study, this was defined as 'all identical and redundant components within the same sub-system'. It might just as well have included 'neighbouring components (not only identical) and in different sub-systems'.

The lessons that can be learned from these common causes are not at all evident. Going back to the example of the two pumps, the reliability engineer, having selected and quantified a dependence, could then specify it as a weak point of the facility. But what solutions could be recommended? Is it better to improve maintenance, protect the pumps from aggressive materials, or diversify their design? Only a detailed study of the problem (and not a probabilistic study) could provide the answer. So, even if a solution is proposed, the reliability tools available are far too limited to evaluate its impact.

previous table of contents next