에너지 백과 사전 Encyklopedia Energii Enciclopedia da Energia Enciclopèdia de la energia
Encyclopédie de l'énergie Enciclopedia de la Energia Bách Khoa toàn thư về năng lượng
دایرہ المعارف انرژی Enciclopedia della Energia موسوعة الطاقة
Encyclopedy of Energy Enzyklopädie für Energie Энциклопедия Энергии
Εγκυκλοπαίδεια της Ενέργειας 能源百科全书 エネルギーの百科事典 Enerji ansiklopedisi

Article : 035

La sûreté nucléaire

TARRIDE Bruno

oct.-15

Niveau de lecture : Assez difficile

Rubrique : Energie nucléaire

Quelles sont les méthodes et les concepts utilisés dans l'industrie nucléaire, aux niveaux conception et exploitation, qui assurent à cette activité industrielle un niveau de sûreté acceptable, principalement dans le cas des réacteurs nucléaires ?

1. *Objectifs généraux de la sûreté nucléaire, notion de risque acceptable*

Les installations nucléaires induisent des risques spécifiques, de nature radio-toxicologique pour l'homme et l'environnement, qu'il convient de traiter par une approche rigoureuse.

1.1. Définition et organisation de la sûreté nucléaire

Si la sécurité nucléaire vise à se prémunir de l'ensemble des risques liés à l'utilisation de l'énergie nucléaire (y compris, par exemple, la lutte contre la malveillance), la sûreté nucléaire limite son champ à la prise en compte du risque de dispersion de produits radioactifs, lié à l'exploitation des installations. Elle peut donc se définir ainsi : la sûreté désigne l'ensemble des dispositions techniques et organisationnelles, prises à tous les stades de la vie d'une installation, pour que son fonctionnement présente des risques jugés acceptables, pour le personnel, le public et l' environnement. Il s'agit donc à la fois:

- d'assurer le fonctionnement normal de l'installation en limitant, autant que possible, la production d'effluents et de déchets radioactifs, ainsi que l'exposition des travailleurs aux rayonnements ionisants ;
- de prévenir les incidents et les accidents ;
- dans l'hypothèse de survenue de telles situations, malgré les mesures prises pour les éviter, de limiter les effets (*mitigation*) de la dispersion incontrôlée de produits radioactifs sur les populations et l' environnement.

En France, la sûreté nucléaire concerne les acteurs principaux suivants (tableau 1) :

- les exploitants, responsables au premier chef de la sûreté de leurs installations ;
- l'autorité de sûreté nucléaire (ASN) qui fixe les objectifs et s'assure de leurs atteintes, avec son appui technique l'Institut de Radioprotection et de Sureté Nucléaire (IRSN) et ses commissions d'experts (groupes permanents),
- les autorités publiques (parlement) auxquelles l'autorité de sûreté rend compte de son action,
- enfin, les représentants de la société civile.

Tableau 1 : Organisation de la sûreté : relations ASN/exploitant

ASN	Exploitant
Définit les objectifs de sûreté	
	Propose des modalités pour les atteindre
S'assure de l'adéquation de ces modalités	
	Met en œuvre les modalités approuvées
S'assure que la mise en œuvre est correcte	

En matière de transparence et de sûreté nucléaire, le besoin s'est ressenti de mettre en place un fondement législatif fort sur ces sujets, ce qui s'est concrétisé par l'adoption de la loi TSN n°2006-686 du 13/06/2006. C'est cette loi qui instaure une autorité de sûreté nucléaire indépendante, alors que précédemment elle était sous tutelle des ministères en charge de l'Industrie, de l'Environnement et de la Santé. En outre, elle traite aussi de l'information du public en matière de sécurité nucléaire,

- en renforçant le droit à l'information,
- localement, en donnant un véritable cadre légal aux CLI (Commissions Locales d'Information),
- en instituant un Haut comité pour la transparence, pour généraliser le débat au niveau national.

Enfin, le titre IV de la loi constitue l'une de ses avancées essentielles, puisqu'il institue le premier régime légal complet des Installations Nucléaires de Base (INB) et des transports de matières radioactives : la loi définit l'ensemble des actes juridiques applicables à ces activités, des autorisations de création au démantèlement, en passant par les contrôles et les éventuelles sanctions pénales.

1.2. Notion de risque acceptable

La notion de risque acceptable ne se réfère pas à des critères définis et absolus. Elle résulte de choix économiques, sociétaux ou politiques et est donc susceptible d'évoluer dans le temps et d'un pays à l'autre. Si les experts ont un rôle de proposition, la décision finale relève d'une appréciation politique qui intègre ces différentes dimensions.

L'importance du risque associé à un réacteur nucléaire résulte de nombreux facteurs spécifiques :

- en premier lieu, un inventaire important de matières radioactives s'accumulant dans le cœur (produits de fission et actinides), et dans une moindre mesure dans le fluide caloporteur (produits d'activation), et susceptible d'être disséminé dans l'environnement en cas d'accidents ;
- un process reposant sur une réaction en chaine qui peut potentiellement s'emballer ;
- une densité de puissance thermique pouvant être considérable dans le cœur des réacteurs « de puissance » ;
- une énergie thermique du combustible ne s'annulant pas, même après l'arrêt de la réaction en chaine ; la puissance résiduelle est alors décroissante dans le temps, car liée à la désintégration

radioactive des produits de fissions et actinides, émetteurs de rayonnements freinés dans la matière ;

- enfin, en dépit des mesures prises pour maîtriser ces risques, le retour d'expérience d'exploitation a montré que des accidents beaucoup plus graves que ceux qui étaient redoutés à la conception pouvaient se produire (Three Mile Island, Tchernobyl, Fukushima) ; leur analyse a montré qu'il convenait d'introduire une approche évolutive pour mieux prendre en compte les dimensions complexes (combinatoire de défaillances possibles, nombreuses interactions et contre-réactions) et sociotechniques (facteurs organisationnels et humains) du système réacteur [notice 023].

L'appréciation des risques liés à l'exploitation d'une installation nucléaire conduit à distinguer, comme pour tout dispositif industriel, les risques potentiels, ceux qui seraient à craindre en l'absence de toute mesure de protection, et les risques résiduels, qui subsistent, en dépit des dispositions prises pour gérer les accidents (prévention/*mitigation*).

On porte sur le risque accidentel une double appréciation en termes de probabilité d'occurrence, et en termes de gravité, selon l'ampleur de ses conséquences. Au début des années 1970, Farmer a proposé, sur un diagramme probabilités-conséquences, une limite entre domaine acceptable et inacceptable, les conséquences étant exprimées en termes de rejets radioactifs (figure 1).

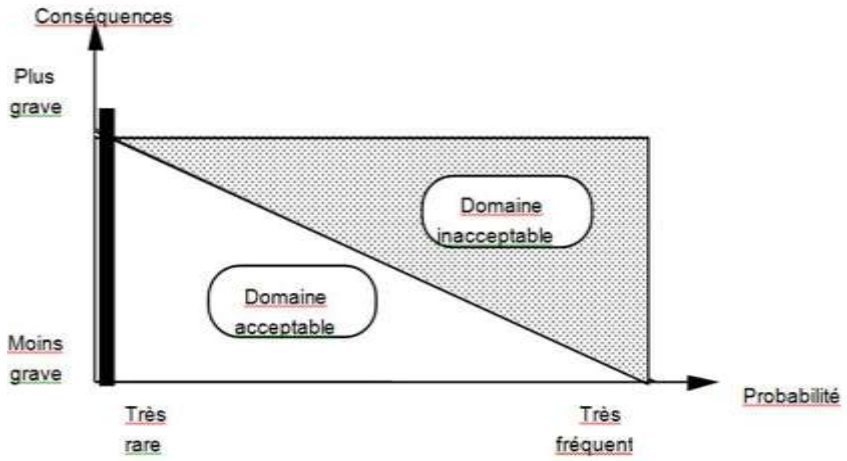

Fig. 1: Notion de risque acceptable, selon Farmer

Le principe général de la démarche d'acceptabilité de Farmer est alors le suivant : plus l'accident est probable, plus ses conséquences doivent être limitées par des contre-mesures. Le concepteur d'un réacteur nucléaire cherchera à approfondir cette démarche, en précisant des couples de plages de probabilités et de conséquences radiologiques considérées comme acceptables. De façon à rester dans le domaine acceptable du diagramme, les spécialistes de la sûreté ont édifié un ensemble de principes et méthodes applicables à toutes les phases de la vie de l'installation. Ceux-ci sont décrits ci-dessous.

1.3. L'approche de sûreté déterministe : les grands principes de sûreté

L'approche de sûreté qualifiée de "déterministe " est issue de la pratique initiale nord-américaine.

Elle consiste à imaginer un certain nombre d'événements initiateurs et scénarii induits, pouvant conduire à des conséquences pour l'homme ou l'environnement. Pour chacune de ces situations, on cherchera à définir les parades matérielles (conception) et organisationnelles (exploitation) qu'il convient de mettre en œuvre pour que les conséquences demeurent acceptables.

1.3.1. Fonctions de sûreté et barrières de confinement

La démonstration de sûreté repose sur le respect de fonctions de sûreté. Plus précisément, en cas de situation accidentelle susceptible de mettre transitoirement en défaut une ou plusieurs de ces fonctions, il conviendra de se ramener rapidement à un état sûr, caractérisé par leur respect.

En regard de la nature du risque spécifiée plus haut, les trois fonctions de sûreté à respecter, pour un réacteur nucléaire, sont :

- la maitrise de la réaction en chaîne,
- le maintien du refroidissement du combustible en toutes circonstances (donc y compris à l'arrêt) en garantissant l'extraction, le transport et l'évacuation de la puissance thermique vers une source froide ;
- le confinement des produits radioactifs accumulés.

Pour garantir cette dernière fonction de confinement, on interpose une succession de barrières physiques entre les substances radioactives et l'environnement. C'est le concept des barrières de confinement. Sur un réacteur nucléaire, trois barrières indépendantes séparent généralement le combustible de l'environnement (figure 2) :

- la première est la gaine entourant le combustible,
- la seconde est généralement constituée de l'enveloppe contenant le cœur et l'eau de refroidissement du réacteur,
- la troisième est généralement constituée d'une enceinte en béton ou en acier entourant le réacteur, l'enceinte de confinement.

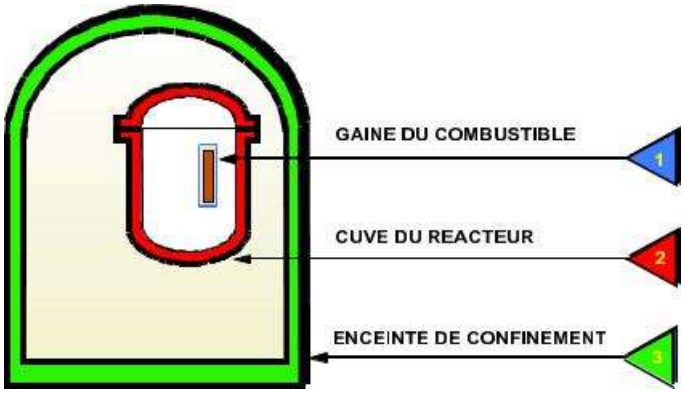

Fig. 2: Les trois barrières de confinement

Malgré le soin apporté à la conception et à la réalisation de ces barrières, leur étanchéité n'est pas parfaite et surtout elle se dégrade dans le temps. Aussi, l'étanchéité de ces barrières fait l'objet de contrôles périodiques. La première barrière est particulièrement exposée et son étanchéité est surveillée en mesurant l'activité du fluide caloporteur contenue dans le circuit primaire de refroidissement. De plus, ces trois barrières doivent rester indépendantes, même en situation dégradée, et ne pas être contournées (par exemple via des traversées).

De façon à assurer trois barrières fortes pour tous les risques identifiés, on définit un ensemble de dispositions matérielles et organisationnelles selon une logique de lignes de défense successives s'opposant au développement d'une situation accidentelle. C'est le principe de la défense en profondeur.

1.3.2. Concept de défense en profondeur

Ce concept repose sur le principe suivant : malgré les mesures prises pour établir une ligne de défense forte, on envisage sa défaillance et on conçoit alors une nouvelle ligne aval pour faire face à la situation. Cette démarche, élaborée initialement pour le dimensionnement et la conception des installations, est désormais appliquée en phase d'exploitation. Elle comportait initialement trois niveaux qui ont ensuite été portés à cinq (Figure 3).

- Niveau 1 : prévention pour rester dans le domaine de fonctionnement optimal.

Il s'agit de doter l' installation d'une excellente résistance intrinsèque, afin de réduire les risques de défaillance. En particulier à la conception, les matériaux, équipements, systèmes, structures de l'installation doivent être choisis et dimensionnés, avec des marges suffisantes, afin de remplir le rôle qui leur est assigné en cas de sollicitation dans toutes les conditions de fonctionnement prévues. En exploitation, l'application rigoureuse des spécifications techniques des règles générales d'exploitation permet d'assurer un fonctionnement nominal.

- Niveau 2 : surveiller et, en cas d'incident, ramener dans les limites du fonctionnement autorisé (protection).

On cherche à maintenir l'installation dans le domaine autorisé, et, en cas de sortie, d'arrêter l'évolution anormale et s'y ramener. On peut citer comme moyens associés à ce niveau :

. les programmes de surveillance (contrôles et essais périodiques) permettant de détecter des dérives sur les performances des matériels importants pour la sûreté ;

. les systèmes de régulations et les informations en salle de commande, pour permettre au personnel de conduite de surveiller et corriger, dans des délais appropriés, les dérives du procédé ;

. des systèmes automatiques de protection, comme par exemple l'arrêt d'urgence du réacteur, capables d'interrompre rapidement une évolution anormale des paramètres physiques.

- Niveau 3 : en cas d'accident, maîtriser la situation en restant dans les limites de conception, puis ramener en état sûr l'installation (sauvegarde).

Malgré les mesures prises au titre des deux niveaux précédents, on postule la survenue de situations accidentelles. Il convient alors de mettre en place des dispositions techniques et organisationnelles pour y faire face et ainsi limiter ses effets à des niveaux acceptables. On définit ainsi :

. des systèmes de sauvegarde n'ayant aucun rôle dans le fonctionnement normal de l'installation, mais dont la mise en service est automatique en cas d'accidents ; ces systèmes ont pour mission de ramener et maintenir l'installation en état sûr, en préservant le combustible d'un

dénoyage prolongé, en garantissant la disponibilité d'une source froide, du confinement… Ils sont conçus, et régulièrement testés, pour garantir l'efficacité de leur mission ;

- des procédures de conduite post-accidentelle pour éventuellement compléter, à terme, l'action des automatismes par une intervention humaine adaptée.

Fig. 3: Les cinq niveaux de la défense en profondeur

L'accident de Three Mile Island (Etats-Unis, 1979) a cependant amené la communauté internationale à compléter le concept de défense en profondeur. En effet, lors de cet accident, une situation de cumuls de défaillances a conduit à une dégradation du combustible plus sévère que celle envisagée à la conception. Aussi, deux lignes supplémentaires ont été introduites :

- Niveau 4 : prévenir la dégradation des scénarios accidentels (cumuls) et limiter les rejets en cas d'accident grave (dégradation du combustible).

Ce niveau prévoit des dispositions matérielles et organisationnelles complémentaires à celles déjà prises, de façon d'une part à s'assurer de l'absence de conséquences à seuil (effet « falaise ») en cas d'accident complexe et évolutif, d'autre part à garantir le confinement par l'enceinte, en cas de dégradation du combustible. Il vise alors à limiter et retarder d'éventuels rejets radioactifs, pour les rendre compatibles avec des mesures de protection des populations à l'extérieur du site.

C'est à ce niveau que l'on trouve le Plan d'Urgence Interne (PUI) de l'installation.

- Niveau 5 : limiter les conséquences pour les populations en cas de rejets importants (gestion de crise).

En cas d'échec des quatre premiers niveaux relevant de l'installation, des mesures de protection des populations doivent être décidées (confinement, distribution d'iode stable, voire évacuation).

En France, c'est au préfet, représentant local du pouvoir exécutif, de gérer la crise. Pour ce faire, il s'appuie sur :

- des moyens préalablement définis dans un plan particulier d'intervention (PPI) ;
- sur les recommandations de l'autorité de sûreté appuyées par l'organisation nationale de crise.

C'est pourquoi des exercices de crise sont périodiquement programmés, de façon à tester les moyens techniques, entraîner les équipes locales et nationales et s'assurer de l' efficacité de l'organisation du dispositif.

2. Sûreté à la conception, études du rapport de sûreté et dimensionnement des systèmes importants pour la sûreté (IPS)

C'est dès leur conception que les installations nucléaires doivent répondre aux impératifs de sûreté qu'imposent les risques spécifiques de la filière. Les études des situations de fonctionnement et d'agression ainsi que le rapport de sûreté y concourent.

2.1. Etudes des situations de fonctionnement

Conformément à ce qui précède, la démarche de sûreté repose sur l'étude de situations de fonctionnement auxquelles peut être confrontée l'installation, depuis le fonctionnement normal jusqu'aux accidents postulés, avec la justification de l'adéquation des parades mises en œuvre, en application des principes de Farmer et de la défense en profondeur. Cela conduit à définir différentes catégories de situations de dimensionnement selon leur probabilité d'occurrence. A chaque catégorie est associée à un niveau de défense et des conséquences admissibles (tableau 2).

Tableau 2 : Catégories des situations de fonctionnement de dimensionnement « de base»

Catégorie	Occurrence associée	Ligne de défense et parades associées	Conséquences admissibles (Farmer)
Catégorie 1	Quotidienne (fonctionnement normal)	Niveau 1 : - spécifications techniques des RGE,	Autorisation de rejets de l'installation (sur l'année)
Catégorie 2	Transitoires ou incidents mineurs mais fréquents	Niveau 2 : - surveillance, protections - procédures incidentelles	Autorisation de rejets de l'installation (pour l'évènement)
Catégorie 3	Incidents peu fréquents, supposés survenir 1 fois dans la vie de l'installation	Niveau 3 : - système de sauvegarde, enceinte - procédures accidentelles	Rejets de l'ordre de la radioactivité naturelle
Catégorie 4	Accidents non attendus dans la vie de l'installation, mais dimensionnants		Rejets ne nécessitant aucune contre-mesure de protection du public (immédiate/différée)

Le principe de la démarche déterministe peut être défini ainsi :

- un événement initiateur est identifié, car susceptible d'affecter une fonction de sûreté ;
- il est classé suivant sa probabilité d'occurrence, ce qui fixe la limite de ses conséquences admissibles ;
- il est alors étudié à partir d'un scénario « enveloppe » de tous les scenarii possibles, c'est-à-dire majorant du point de vue de ses conséquences ; le caractère enveloppe est garantie par l'application de règles d'études conservatives qui peuvent être, par exemple, des conditions initiales respectant les règles générales d'exploitation et prises dans le sens pénalisant (avec incertitudes), le cumul d'un événement aggravant ou l' action d'un opérateur retardée ;
- les études sont réalisées avec des outils de modélisation et de calcul qualifiés ;
- en lien avec l'intégrité des barrières, des critères « de sûreté » à respecter sont généralement introduits ; ils permettent de découpler les problèmes, tout en garantissant le respect des conséquences admissibles de la catégorie ;
- de façon à vérifier le respect des critères de sûreté et l'atteinte d'un état sûr, il est alors mis en place des parades adaptées ; dans le cas des systèmes importants pour la sûreté, ceux-ci sont conçus de façon à garantir robustesse et marges de dimensionnement.

La liste des situations de fonctionnement de dimensionnement « de base» n'est pas figée et est régulièrement revue sur la base du retour d'expérience d'exploitation. De façon à définir un quatrième niveau de défense, elle est désormais complétée par une liste de situations « complémentaires ou d'accidents graves hypothétiques». Ces situations permettent de définir, de façon réaliste, des dispositions matérielles et organisationnelles « complémentaires » de façon à ce qu'aucune contre-mesure immédiate de protection des populations ne soit nécessaire pour ces situations.

2.2. Etude des agressions

Les agressions constituent des conditions hostiles pouvant conduire à la défaillance d'équipements et/ou à un transitoire pour l'installation. On distingue, dans la démonstration de sûreté, deux types d'agressions (listes non exhaustives) :

- celles d'origine interne : les explosions, les incendies, les inondations internes, les émissions de projectiles, les défaillances d'équipements sous pression, les collisions et chutes de charges ;
- celles d'origine externe : le séisme, les conditions météorologiques ou climatiques extrêmes, les risques induits par les activités industrielles et de transport, dont les explosions et les chutes d'avions, ou toute agression ou cumul identifié par l'exploitant ou l'Autorité de sûreté.

Pour les deux types, la priorité est donnée à la prévention, c'est-à-dire la réduction de leur occurrence. Au titre de la défense en profondeur, sont également introduits des dispositions :

- de surveillance des effets induits, en termes d'intégrité et d'opérabilité des équipements,
- de limitation des conséquences des transitoires engendrés.

2.3. Le rapport de sûreté

L'exploitant soumet à l'Autorité de Sûreté Nucléaire une demande d'autorisation de création et un dossier appelé « rapport de sûreté ». C'est sur la base des différentes versions de ce document que l'autorité de sûreté délivre une autorisation de démarrage (phase d'essais), puis de mise en service de l'installation.

Dans ce rapport, l'exploitant décrit l'installation, son intégration dans son environnement, ainsi que les activités qui seront menées (volumes I et II). Le volume III du rapport constitue la partie démonstrative : il présente la synthèse des études d'incidents et d'accidents d'origine interne ou liée à une agression externe et justifie que les objectifs de sûreté sont atteints grâce à l'adéquation des parades. Le rapport de sûreté est donc en lien d'une part avec les dossiers de conception des systèmes importants pour la sûreté, d'autre part avec les règles générales d'exploitation, comme cela est développé ci-dessous.

2.4. Principes de conception des systèmes importants pour la sûreté (IPS)

Les systèmes de protection et de sauvegarde, couvrant les premiers niveaux de la défense en profondeur, sont qualifiés « importants pour la sûreté » (IPS). Ils interviennent automatiquement, dès le début de l'accident, pour ramener le réacteur en état sûr ou dans un état maîtrisable par les opérateurs. Leur bonne conception repose sur l'étude des situations de fonctionnement de dimensionnement et quelques grands principes.

2.4.1. Critère de défaillance unique, redondance et prévention des défaillances de mode commun

Pour les systèmes IPS, qui doivent opérer dans les situations incidentelles et accidentelles, la règle du critère de défaillance unique (CDU) doit être appliquée. Elle signifie « qu'un système IPS doit assurer sa mission malgré la défaillance active d'un de ses composants. S'il assure une mission au-delà de 24 heures, il doit assurer sa mission après ce délai, même si survient une défaillance mécanique active ou passive ». On peut donner comme exemple de défaillances :

- actives : refus de démarrage d'une pompe, de manœuvre d'une vanne,
- passives : fuite d'une tuyauterie, d'un équipement appartenant à un système IPS.

Cette importante règle amène à concevoir des systèmes redondants**,** à savoir équipés d'au moins deux voies, chaque voie étant capable, à elle seule, d'assurer la fonction. Dans la pratique, la redondance prévue peut être supérieure à 2, de façon à permettre la réalisation d'essais périodiques ou de la maintenance en fonctionnement.

L'utilisation du critère de défaillance unique n'est cependant pas suffisante pour garantir un haut niveau de fiabilité des systèmes IPS, car il convient de considérer la possibilité de défaillances de mode commun, une cause unique (agression ou erreur humaine) affectant simultanément les différentes voies d'un même système et conduisant à la perte de sa fonction de sûreté.Les méthodes habituellement utilisées pour se prémunir contre les modes communs sont : la diversification fonctionnelle des équipements, ainsi que celle des systèmes supports, et la séparation physique des voies redondantes.

2.4.2. Classement de sûreté

Le classement de sûreté permet de définir les exigences relatives à la conception, la réalisation, l'exploitation et la maintenance des moyens IPS. Les caractéristiques d'un matériel classé de sûreté sont alors :

- redondance et indépendance, secours électrique,
- classement sismique,
- qualification aux conditions d'ambiance accidentelle,
- étudié avec des règles conservatives, intégrant marges et incertitudes,
- soumission à un code de conception et de construction,
- impositions en matière d'assurance de la qualité,
- exigences d'exploitation (essais périodiques).

Pour les équipements et ouvrages de génie civil IPS, le classement sismique permet de préciser les exigences d'intégrité, de capacité fonctionnelle ou d'opérabilité pendant et après un séisme. Les exigences de qualification sont destinées à s'assurer de la capacité des moyens IPS à accomplir leur mission, en toute circonstance. Elles sont basées sur la définition de sollicitations enveloppes, incluant les conditions d'ambiance dégradée et autres agressions susceptibles d'être rencontrées.

La conception doit tenir compte de la dépendance de ces systèmes IPS aux systèmes supports, type source froide, ventilations ou alimentations électriques. Par exemple, la perte de tension externe impose de prévoir des groupes alternateurs entrainés par moteur diesel, pour secourir les tableaux électriques alimentant les matériels IPS.

L'étude des situations de fonctionnement, conduites avec des hypothèses conservatives, confèrent finalement aux moyens conçus des marges de dimensionnement importantes. Elles permettent également de fixer les exigences fonctionnelles minimales associées (débit requis, volume d'eau dans une bâche…)

A noter que l'approche déterministe peut être croisée, pour les installations à fort enjeux de sûreté, par la réalisation d'études probabilistes de sûreté (EPS). Dans cette approche probabiliste, on définit une situation redoutée (exemple la fusion du cœur), puis, à partir d'une liste d'événements initiateurs, on construit des arbres d'événements en examinant la réussite ou l'échec de l'action des automatismes ou de celle des opérateurs pour tenter de ramener le réacteur vers un état sûr, chaque évènement élémentaire étant associé à une probabilité. Les EPS permettent ainsi une appréciation du niveau global de la sûreté, mais surtout de mettre en évidence les points forts et points faibles de l'installation.

3. Sûreté à l'exploitation et règles générales d'exploitation (RGE)

L'exploitation d'une installation nucléaire couvre la période comprise entre son démarrage et sa mise à l'arrêt définitif. Pendant cette période, l'exploitant est le responsable de la sûreté de son installation et doit en rendre compte à l'autorité de sûreté nucléaire. Il doit maintenir le niveau de sûreté déterminé par la conception mais il doit aussi l'améliorer autant que possible, par des modifications matérielles et organisationnelles. Celles-ci sont généralement issues des réexamens périodiques de sûreté.

En cohérence avec le rapport de sûreté, les règles générales d'exploitation (RGE), rédigées par l'exploitant, définissent les principes et règles pour exploiter l'installation en conditions sûres. Comme leur nom l'indique, elles ont un caractère réglementaire, car soumises à l'autorité de sûreté à l'appui de la demande de mise en service de l'installation. Au cours du fonctionnement, l'exploitant doit être en mesure de démontrer, en permanence, le respect de ces règles qu'il s'est lui-même fixé. De même que des modifications peuvent être apportées à l'installation, des modifications des pratiques peuvent être envisagées au cours de la vie de l'installation. Elles doivent alors se traduire par des modifications des RGE et être à nouveau soumises, pour approbation, à l'autorité de sûreté.

Les différents chapitres des RGE recouvrent essentiellement les 4 premiers niveaux de la défense en profondeur en exploitation : à savoir prévention, surveillance, maîtrise des incidents et accidents postulés et gestion des accidents graves sur le site. Ce document comporte trois composantes essentielles.

3.1. Définition du domaine de fonctionnement et de ses limites

Au titre du premier niveau de la défense en profondeur, la sûreté en exploitation est assurée par le respect de spécifications techniques, définissant les limites du fonctionnement autorisé, de sorte que l'on puisse garantir d'être couvert pas la démonstration du rapport de sûreté. Ces spécifications visent trois objectifs principaux :

- définir les limites des paramètres physiques, les réglages des seuils de protection et les configurations des systèmes pour les différents états d'exploitation de l'installation ;
- préciser, la liste des systèmes IPS, inutiles au fonctionnement normal, mais devant être requis pour garantir le caractère opérationnel des parades prévues pour faire face aux situations accidentelles ;
- définir les actions de repli à mettre en œuvre en cas de fonctionnement dégradé (exemple : indisponibilité d'un système IPS), ainsi que le délai maximal autorisé pour leur mise en œuvre.

A noter que la maintenance préventive (conditionnelle et périodique) fait également partie de la première ligne de défense en profondeur.

3.2. Contrôles et essais périodiques

Les contrôles et essais périodiques contribuent au deuxième niveau de défense en profondeur au niveau de la surveillance. Leur but est de garantir, en exploitation, le respect des hypothèses retenues pour les études du rapport de sûreté, en particulier par l'assurance de la non-dérive des performances des matériels et systèmes IPS, autrement dit leur capacité à remplir la mission pour laquelle ils ont été conçus. Le chapitre associé des RGE donne les principes de réalisation des essais périodiques. Pour chaque essai, il précise la périodicité, le mode opératoire, les critères de validité, la conduite à tenir en cas d'invalidité de l'essai, les conditions de remise en service...

3.3. Conduite en cas d'incidents, accidents ou agressions

Au titre des troisième et quatrième niveaux de défense en profondeur, la maîtrise des situations incidentelles et accidentelles est assurée par l'application de procédures de conduite par les opérateurs. Celles-ci sont établies sur la base d'études de simulation de séquences accidentelles.

Suite à l'accident de Three Miles Island, une évolution majeure de la philosophie de la conduite post-accidentelle a été introduite. L'industrie nucléaire a pris alors conscience de l'impossibilité d'associer des stratégies de conduite à l'infinité de combinaisons de défaillances possibles, d'où le développement d'une approche « par état » (APE) reposant sur un diagnostic d'état physique de l'installation, puis l'orientation vers une stratégie adaptée d'une part à cet état, d'autre part à la liste des moyens disponibles. La démarche étant itérative, elle permet de s'adapter à une situation évolutive et rassure l'opérateur, toute erreur pouvant être rattrapée (figure 4).

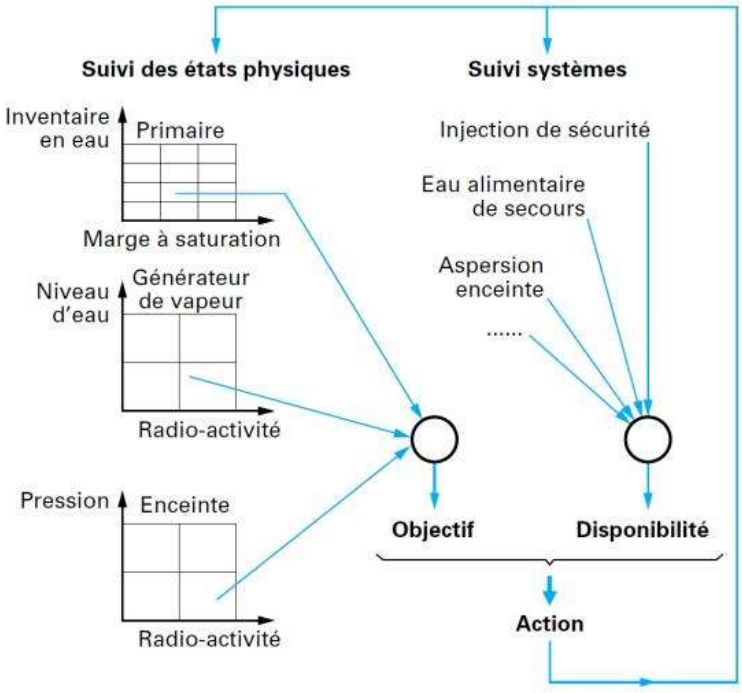

Fig. 4: Principe de l'APE pour un REP - source : Techniques de l'ingénieur

Le chapitre des RGE associé à ce thème, présente les règles de conduite, précisant les critères d'entrée en procédures incidentelle/accidentelle, les stratégies de conduite proposées pour ramener le réacteur en état sûr, les moyens de surveillance de la réussite de cette stratégie, les critères de sortie des procédures ou, en cas de dégradation du combustible, de mise en œuvre du plan d'urgence interne. Il est désormais complété par la conduite en cas d'agression interne ou externe, suivant la même logique.

4. En conclusion : une sûreté évolutive

Les exigences de la sûreté ne sont pas figées. Malgré la rigueur de l'approche présentée, visant l'exhaustivité de l'analyse des risques et plaçant des parades en regard, il convient de se préparer à faire face à des situations mal anticipées à la conception. C'est pourquoi, l'approche française de la sûreté affiche une logique d'amélioration continue. Dans le cadre de réexamens périodiques, il est prévu le renforcement du référentiel d'exigences de sûreté en intégrant, outre l'amélioration des connaissances scientifiques et l'évolution des standards internationaux, les leçons de l'expérience, et tout particulièrement celles des grands accidents nucléaires [notice 023].

Les deux dernières lignes de défense en profondeur et la conduite post-accidentelle « par état » résultent des enseignements de Three Mile Island. Pour ce qui concerne la catastrophe de Fukushima, on peut citer l'introduction d'un noyau dur de dispositions, nombre limité d'équipements résistant à des agressions extrêmes (au-delà du dimensionnent initial) et permettant de garantir qu'aucun « effet falaise » ne pourrait conduire à affaiblir les derniers niveaux de la défense en profondeur.