Chapitre 7
Options et considérations de sûreté au stade de la conception

L'atteinte du niveau de sûreté visé à la conception d'une installation comme un réacteur électronucléaire suppose une bonne déclinaison des objectifs généraux, concepts, principes et méthodes introduits dans le chapitre précédent.

Dans les faits et de façon assez schématique, si la conception d'un réacteur électronucléaire vise en premier lieu à déterminer l'ensemble des caractéristiques du « procédé » (voir plus loin la figure 7.1) qui vont permettre une production d'électricité dans les conditions souhaitées, elle suit généralement un processus itératif fondé au départ sur le choix d'options techniques dont bien évidemment certaines sont en rapport avec la sûreté, conforté – et corrigé autant que de besoin – par des vérifications comportant un certain nombre d'études contribuant à ce que l'on appelle désormais « démonstration de sûreté ».

Certaines options techniques ont un lien évident avec le concept de défense en profondeur présenté au chapitre précédent :

– le choix du site d'implantation du réacteur y contribue pour ce qui concerne par exemple les possibilités de refroidissement, la définition des agressions externes à considérer (séismes, inondations, activités humaines au voisinage de l'installation) et la considération des populations susceptibles d'être touchées en cas de rejet accidentel de substances radioactives…) ;

- des caractéristiques neutroniques intrinsèques du cœur du réacteur favorables à la maîtrise de la réactivité participent également à la défense en profondeur ;
- le choix du matériau des gaines des crayons combustibles, qui doit leur procurer une résistance appropriée dans les différentes situations envisagées, participe aux quatre premiers niveaux de la défense en profondeur ;
- la surveillance neutronique du cœur, les systèmes de limitation (puissance…) ainsi que de protection et l'arrêt automatique du réacteur déclenché par ce système contribuent à différents niveaux de la défense en profondeur ;
- les choix en matière d'architecture des systèmes de sauvegarde, par exemple en termes de redondance et de diversification technologique, sont guidés par la fiabilité recherchée des dispositions prévues au troisième niveau de la défense en profondeur…

Les choix techniques associés à des considérations de sûreté au stade de la conception – dont il sera question aux paragraphes 7.1 et 7.2 – peuvent ainsi résulter des objectifs généraux, des concepts, des principes ou des méthodes introduits dans le chapitre précédent et être le reflet de bonnes pratiques industrielles, historiquement éprouvées. En revanche, certains équipements peuvent nécessiter une approche spécifique de sûreté du fait de choix associés à des évolutions technologies importantes : c'est le cas des systèmes de contrôle-commande à base de logiciels programmés, sujet développé au paragraphe 7.3. La notion de classement de sûreté des équipements est développée au paragraphe 7.4. Quelques éléments relatifs à la conception des équipements sous pression nucléaires sont présentés au paragraphe 7.5. Des considérations générales sur la prise en compte des agressions dans la conception des installations font l'objet du paragraphe 7.6. Enfin, certains choix techniques peuvent être associés à des considérations qui ne correspondent pas à la mission première de l'installation : c'est ainsi que le caractère très particulier des risques liés aux installations nucléaires conduit à retenir des choix de conception visant à faciliter leur démantèlement, sujet abordé au paragraphe 7.7.

On peut ajouter ici que la radioprotection des travailleurs en exploitation (sujet abordé au chapitre 31) ou la préparation à la gestion de situations d'urgence (chapitre 38) ont également une influence sur les choix de conception d'une installation nucléaire.

Le guide ASN n° 22 énonce ainsi des recommandations générales ou spécifiques relatives à la conception d'un réacteur électronucléaire, qui couvrent un domaine plus large que celui du présent chapitre[288].

288. Ces recommandations générales et spécifiques font l'objet des parties IV à VII du guide ASN n° 22.

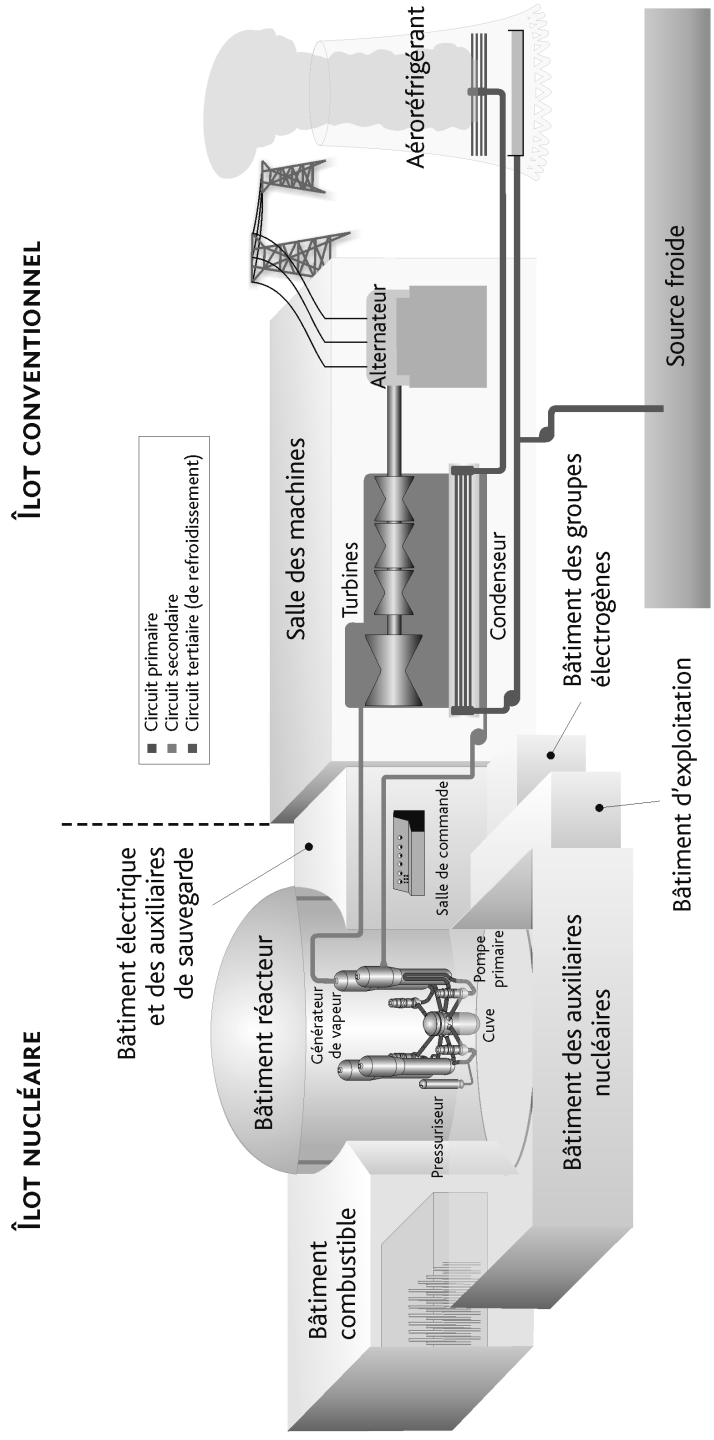

Figure 7.1. Présentation générale d'un réacteur à eau sous pression à quatre boucles (1 300 MWe ou 1 450 MWe) et de ses principaux circuits. Georges Goué/Médiathèque IRSN.

L'étude des conditions de fonctionnement, correspondant à des défaillances internes propres à l'installation, ainsi que celle des agressions font l'objet de chapitres ultérieurs ; il s'agit d'éléments qui vont servir :

– d'une part à la conception et au dimensionnement proprement dit des structures, systèmes et composants importants pour la sûreté de l'installation,

– d'autre part à la démonstration de sûreté, fondée sur la conception et le dimensionnement retenus.

7.1. Différents types de dispositions de conception associées à des considérations de sûreté

De façon générale, les concepteurs cherchent à limiter les possibilités de dysfonctionnement des équipements. Cela repose en particulier sur :

– une fiabilité appropriée des équipements pour les fonctions ou les missions qui leurs sont assignées,

– une conception tolérante aux écarts comportant des dispositions permettant le retour à l'état de référence,

– une conception pardonnante à l'égard des erreurs humaines.

Pour expliciter cela et afin d'y parvenir, différents types de dispositions sont adoptées aux stades de la conception, puis de la réalisation et de l'exploitation. Elles sont très variées et dépendent de l'importance pour la sûreté des équipements ou systèmes auxquels ils appartiennent, en relation avec la démonstration de sûreté. Pour ce qui concerne les équipements, il s'agit de dispositions relatives :

– à la conception générale, telle que l'adoption autant que possible du principe de « panne sûre »[289] – cela signifie que, en cas de défaillance de l'un des composants d'un équipement, celui-ci demeure ou se met dans une configuration favorable au plan de la sûreté ;

– au choix des matériaux et au dimensionnement ; à ce titre, les équipements peuvent être par exemple conçus pour rester structurellement intègres dans différentes conditions de fonctionnement ou situations d'agression interne ou externe ;

– à leurs modalités de fabrication ;

– à leur qualification pour les différentes conditions de fonctionnement et d'ambiance dans lesquelles ils seront ou seraient amenés à fonctionner ;

289. Ce principe est notamment cité dans le document *Specific Safety Requirements* No. SSR-2/1 (Rev. 1, 2016) de l'AIEA (*Requirement 26*).

– aux modalités des contrôles à réaliser au cours de leur fabrication, ainsi qu'aux modalités des essais lors des phases du démarrage de l'installation, puis de façon périodique en exploitation ;

– aux modalités des contrôles (périodiques ou non) dans le cadre du suivi en service – il est important de concevoir des équipements qui soient autant que possible « inspectables », voire par plusieurs méthodes ;

– aux possibilités de détecter des dysfonctionnements par une instrumentation spécifique...

Des dispositions de conception concernent par ailleurs l'architecture des systèmes, de façon à obtenir une fiabilité appropriée, permettant une démonstration de sûreté cohérente avec les objectifs de sûreté visés ; il s'agit en particulier de réduire les risques de défaillances par cause commune (ou de mode commun) entre systèmes ou équipements assurant une fonction similaire. À titre d'exemple, les systèmes peuvent être conçus en retenant des dispositions telles que :

– le secours, par des sources électriques dédiées, de l'alimentation électrique de l'ensemble des équipements actifs[290] d'un système ; une telle disposition vise à assurer le fonctionnement du système malgré la défaillance du réseau électrique externe assurant l'alimentation électrique normale des équipements ;

– l'application du « critère de défaillance unique » à certains systèmes ; cette disposition sera plus amplement détaillée au paragraphe 7.2 ;

– la diversification technologique des équipements permettant d'assurer une fonction donnée ; cette diversification vise à limiter les risques de défaillances de mode commun (elle ne doit toutefois pas être appliquée par principe si elle conduit à des fiabilités réduites des technologies mises en œuvre) ;

– la séparation géographique ou physique des voies redondantes, afin de limiter les risques de défaillances de mode commun en cas d'agression (inondation interne, incendie...) ;

– une conception appropriée des systèmes « supports » aux systèmes de sûreté, en vue d'éviter des défaillances de mode commun sur des voies redondantes de ces systèmes (par exemple systèmes de conditionnement thermique, systèmes d'alimentation en fluides – carburant, électricité, air comprimé...).

Des exigences[291] proportionnées à ce qui est attendu des équipements et des systèmes sont retenues par les concepteurs ; elles constituent une base pour la démonstration de sûreté dans les différentes conditions de fonctionnement et situations d'agressions considérées.

290. Pompes, vannes... Cette notion est précisée au paragraphe 7.2.
291. Notion d'« exigences définies » dans la règlementation française (depuis l'« arrêté qualité » de 1984).

Les dispositions retenues doivent bien entendu tenir compte des aspects organisationnels et humains. La maîtrise de la qualité de toutes les activités intervenant dans la conception, l'approvisionnement, la fabrication, le montage, les essais et les contrôles, ainsi que dans la préparation à l'exploitation, revêt une importance particulière, mais elle ne constitue qu'une part de la prise en compte des aspects organisationnels et humains au stade de la conception, sujet qui est plus largement développé au chapitre 16.

7.2. Le critère de défaillance unique

Les systèmes qui vont contribuer à la prévention des incidents et des accidents ainsi qu'à la limitation de leurs conséquences doivent être d'une fiabilité appropriée. Une étude de fiabilité précise est difficile à mener au moment des premiers choix en matière de systèmes. Une approche systématique a été retenue au stade de la conception, consistant en l'application d'un « critère de défaillance unique » pour ces systèmes[292] ; ce critère peut être résumé comme suit : la fonction d'un système doit pouvoir être remplie même en cas de défaillance d'un quelconque de ses composants[293].

Son application est simple : il est postulé que, au moment de la sollicitation du système, l'un quelconque de ses composants est défaillant. Il faut, bien sûr, rechercher à cette fin le composant dont le mauvais fonctionnement a les conséquences les plus défavorables dans les conditions considérées.

On distingue toutefois les composants « actifs » qui nécessitent un mouvement (pompes, vannes…) pour remplir leurs missions dans les situations considérées, à l'opposé des composants « passifs » (capacités ou récipients, tuyaux, échangeurs de chaleur…).

Une « défaillance active » est le refus de fonctionnement d'un composant actif sollicité[294].

Une « défaillance passive » est généralement une fuite, d'ampleur limitée si elle peut être localisée et arrêtée ; dans le cas contraire, il faut considérer que tout le fluide pouvant s'échapper par la brèche est perdu. Une défaillance passive peut être également un blocage s'opposant à l'écoulement d'un fluide.

Compte tenu de cette distinction, le critère de défaillance unique s'applique de la façon suivante[295] :

---

292. Une autre voie d'amélioration de la fiabilité au-delà de l'application du critère de défaillance unique consiste à apporter une diversification, la multiplication d'équipements identiques ne pouvant pas améliorer significativement la fiabilité compte tenu des possibilités des défaillances de mode commun mentionnées plus loin.
293. Règle fondamentale de sûreté I.3.a.
294. Cela n'exclut pas la nécessité d'examiner les possibilités de fonctionnements intempestifs d'équipements actifs.
295. Il convient de bien distinguer le critère de conception explicité dans la RFS I.3.c et l'aggravant unique retenu dans les études de sûreté, qui sera vu au chapitre 8.

– les systèmes de protection et de sauvegarde doivent pouvoir assurer pleinement leur fonction malgré une défaillance active quelconque ;

– les systèmes précités qui doivent assurer une mission de longue durée doivent pouvoir assurer leur fonction même s'il survient une défaillance passive après 24 heures ; en outre, pour ces systèmes, il convient de s'assurer qu'une défaillance passive qui surviendrait avant 24 heures ne conduirait pas à un accroissement très notable des conséquences de l'accident (« effet falaise »[296]).

La façon d'appliquer de manière pratique ce critère a donné lieu à de nombreuses discussions, en particulier sur deux questions complémentaires :

– comment tenir compte des indisponibilités de matériels ou de systèmes connues avant l'occurrence de la situation considérée ou pour maintenance ?

– faut-il tenir compte des erreurs humaines et comment ?

Certains constructeurs ont fait le choix de systèmes présentant une triple ou une quadruple redondance – chacun des trains (voies ou files) étant capable d'assurer tout ou partie de la fonction. On parle alors de systèmes à 3 ou 4 trains. Ce sujet peut aussi faire l'objet d'exigences règlementaires.

Suivant en cela le bailleur de la licence, l'exploitant et le constructeur français ont, pour les tranches de 900 MWe et après étude d'une large gamme de solutions possibles, conçu une architecture des systèmes de sauvegarde comportant deux voies électriques (voie A et voie B), capables d'assurer leur fonction en cas de défaillance d'un composant. Cette disposition, retenue ensuite jusques et y compris pour les tranches de 1 450 MWe, permet de limiter le nombre de matériels et donc les investissements. Elle impose par contre une très grande vigilance quant à la disponibilité des deux trains ; cela se traduit en particulier par des contraintes sévères sur les durées maximales admises d'indisponibilité fortuite des matériels et des limitations strictes pour la mise en indisponibilité volontaire d'une voie, pour entretien par exemple, pendant les périodes de fonctionnement où le système considéré est nécessaire à la sûreté.

Dans le cas du réacteur EPR Flamanville 3, les fonctions de sauvegarde du réacteur sont assurées par plusieurs trains physiquement indépendants. Le choix pour le système d'injection de sécurité (RIS) a été notamment d'adopter quatre trains redondants, chacun de ces trains – raccordé à l'une des quatre voies électriques – étant capable d'assurer seul la fonction de sûreté attendue du système ; le raisonnement est qu'un train n'est pas à même d'injecter de l'eau dans le réacteur du fait de l'accident (accident de perte de réfrigérant primaire), qu'un deuxième train est indisponible en application du critère de défaillance unique et qu'un troisième est indisponible du fait d'une maintenance préventive en cours[297].

L'application en base du critère de défaillance unique permet d'avoir une bonne confiance dans la capacité des systèmes auxquels il est appliqué à réaliser

296. Définition précisée dans le focus du chapitre 8.
297. Le cas des autres systèmes de sauvegarde de l'EPR est précisé au chapitre 18.

les fonctions qui leur sont assignées. Toutefois, pour pouvoir rendre suffisamment improbables les défaillances simultanées de deux voies redondantes (défaillances de cause commune[298], de mode commun ou « modes communs »), il faut remplir une double condition :

– éviter qu'une même agression puisse affecter les matériels des deux voies,

– limiter, autant que faire se peut, les défaillances simultanées de plusieurs matériels identiques.

La première condition conduit à retenir des règles d'implantation et d'installation très strictes. Les matériels des différentes voies des systèmes redondants peuvent ainsi être disposés dans des locaux différents, complètement séparés. C'est la séparation géographique qui amène, par exemple, à implanter les deux groupes électrogènes à moteur diesel d'une tranche dans deux locaux distants l'un de l'autre (cette distance est telle que même la chute d'un avion sur l'installation ne pourrait pas affecter directement, de façon simultanée, les deux locaux. La figure 7.2 donne un exemple correspondant à l'implantation de matériels des systèmes de sauvegarde RIS et EAS d'un réacteur de 1 300 MWe du palier P4.

Toutefois, une séparation géographique complète n'est pas toujours possible. Des séparations physiques par des écrans ou des murs appropriés peuvent alors être mises en place. Des problèmes de ce type se posent notamment pour les matériels électriques ou du contrôle-commande, par exemple en salle de commande.

Concernant la seconde condition, les défaillances possibles de mode commun sont beaucoup plus difficiles à identifier et à prendre en compte. Il peut en effet s'agir d'erreurs de conception, de fabrication ou d'entretien qui risquent d'affecter simultanément plusieurs matériels. Ce sont donc des défauts relevant de la qualité générale de l'installation ou de son exploitation.

Il convient de noter que les études de fiabilité des matériels font apparaître que le gain de fiabilité apporté par une redondance supplémentaire est de plus en plus faible au fur et à mesure que le nombre de voies augmente.

La prévention des modes communs de défaillances ne doit pas « oublier » une composante dont l'importance n'a été perçue que progressivement. Il s'agit de l'influence des facteurs organisationnels et humains et des défaillances liées aux activités de maintenance ou de conduite. C'est l'accident de Three Mile Island survenu aux États-Unis en 1979 qui fera prendre conscience de l'importance qu'il convient d'accorder aux facteurs humains dès la conception. Il faudra quelques années encore pour que soient détectés, déclarés et analysés des exemples d'erreurs d'intervention ou de maintenance ayant mis en cause la disponibilité ou le bon fonctionnement de plusieurs, voire de la totalité, des matériels assurant une fonction de sûreté.

298. On appelle ainsi des défaillances dépendantes, ayant pour origine la même cause directe (cause commune) ou la même cause indirecte.

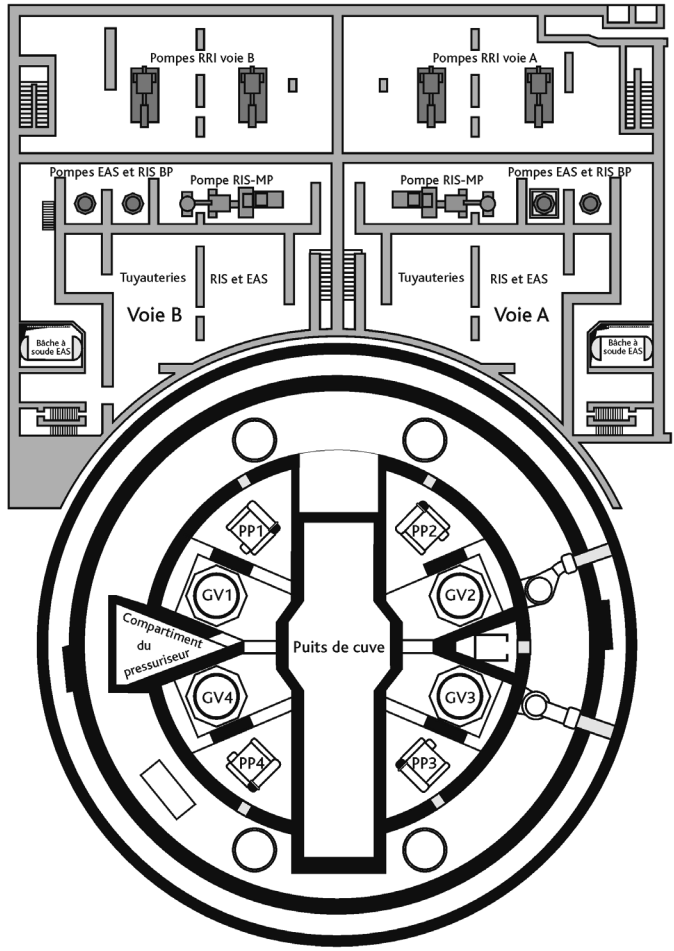

Figure 7.2. Implantation des matériels de sauvegarde des circuits RIS et EAS dans un réacteur de 1 300 MWe de type P4. IRSN.

Les exemples qui suivent font partie des plus significatifs mais ne suffisent évidemment pas pour déterminer des valeurs des probabilités de défaillances de mode commun.

Le premier exemple concerne une tranche de la centrale nucléaire de Philippsburg en Allemagne (région de Karlsruhe). Compte tenu des niveaux de redondance affectés aux différents systèmes importants pour la sûreté, elle disposait de huit groupes électrogènes à moteur diesel. C'est au cours d'une vérification de routine du réglage d'un seuil de ces groupes électrogènes qu'une équipe d'intervention qui ne connaissait pas bien les équipements et utilisait une procédure un peu ambiguë a laissé, en 1987, les huit groupes électrogènes dans un état qui empêchait leur démarrage automatique. Une ronde effectuée 15 heures plus tard a permis de détecter cette erreur et de la corriger.

En France, plusieurs anomalies du même type sont survenues en 1989 dans les réacteurs comme le maintien de pièces inadaptées dans les trois soupapes d'un pressuriseur ou l'isolement de quatre capteurs de niveau d'eau sur cinq d'un autre pressuriseur. On reviendra plus amplement sur ce sujet au paragraphe 22.2.1.

7.3. La spécificité des systèmes programmés (à base de logiciels de contrôle-commande)

Les systèmes de contrôle-commande jouent (parmi d'autres) un rôle très important dans la sûreté des réacteurs nucléaires. Cette importance se traduit notamment par une activité particulièrement soutenue des groupes de travail internationaux et des organismes de normalisation dans ce domaine.

Les systèmes de contrôle-commande des réacteurs électronucléaires participent à des fonctions de surveillance, de régulation, de limitation et de protection de l'installation. On considère généralement qu'ils comportent trois sous-ensembles :

– des interfaces avec le « procédé » : il s'agit de capteurs et d'actionneurs déclenchant des actions, soit « tout ou rien », soit « continues » ;

– des automates chargés de traiter les mesures et les ordres des opérateurs, d'envoyer des ordres aux actionneurs et d'élaborer les informations nécessaires à l'exploitation ;

– des interfaces avec les opérateurs (moyens de conduite) et avec les équipes de maintenance.

Les systèmes de contrôle-commande permettent de réaliser des fonctions, parmi lesquelles on peut par exemple distinguer :

– les fonctions de « protection » proprement dites du réacteur ; il s'agit par exemple de l'arrêt automatique du réacteur ou de la mise en service de systèmes de sauvegarde ;

– les fonctions nécessaires à l'atteinte de l'état sûr[299] à la suite d'une situation incidentelle ou accidentelle ;

– des fonctions automatiques et manuelles utilisées en fonctionnement normal.

Les systèmes de contrôle-commande sont organisés selon une architecture visant à satisfaire des exigences fonctionnelles (par exemple, certains systèmes doivent communiquer avec d'autres) et des exigences de sûreté (par exemple, l'indépendance entre certains systèmes).

Le développement des technologies numériques offre des capacités croissantes de calcul et d'interconnexions, qui permettent de mettre en œuvre des systèmes de contrôle-commande performants ; dans le cas des réacteurs à eau sous pression,

299. Définition précisée dans le focus du chapitre 8.

on peut citer la réalisation de fonctions « avancées » comme le calcul du rapport de flux thermique critique (RFTC) dans le cœur (notion présentée au paragraphe 5.6), la détection en temps réel de défaillances de matériels, ou encore la mise à la disposition des opérateurs d'interfaces plus élaborées.

Ce type de technologies a été introduit progressivement à partir des réacteurs de 1 300 MWe (paliers P4 et P'4), puis de 1 450 MWe (palier N4). Ces technologies soulèvent toutefois des difficultés spécifiques en termes de démonstration de sûreté, ce qui a conduit les parties intéressées (Siemens, Framatome, Électricité de France et l'IRSN) à développer une approche particulière. Cette approche a évolué au cours du temps en tenant compte des évolutions technologiques, telles que les communications par réseaux, ainsi que des progrès scientifiques et techniques, comme les méthodes de vérification « formelles » fondées sur des approches mathématiques. Elle est cohérente avec le consensus international exprimé dans les textes de l'AIEA et de la Commission électrotechnique internationale (CEI), et similaire à celles adoptées dans d'autres secteurs industriels où le contrôle-commande exécute des fonctions importantes pour la sûreté, comme l'avionique, le spatial ou le ferroviaire.

En 2000, l'autorité de sûreté a diffusé la règle fondamentale de sûreté (RFS) II.4.1.a, intitulée « Logiciels des systèmes électriques classés de sûreté », préparée alors avec l'IPSN et les industriels ; elle a pour objet de *« préciser les principes et les exigences à respecter pour la conception, la réalisation, la mise en œuvre et l'exploitation des logiciels des systèmes programmés classés de sûreté »*. Plus récemment, en janvier 2018, l'IRSN a rendu public sur son site internet une « démarche de sûreté »[300] intitulée « Principes relatifs à la démarche de conception du contrôle-commande numérique ». Cette démarche, qui s'inscrit dans la continuité de la RFS II.4.1.a, apporte des précisions sur les principes et les exigences de la RFS, en tenant compte de l'expérience acquise lors des évaluations menées pour le parc électronucléaire français, notamment de celles relatives aux systèmes spécifiques de contrôle-commande du réacteur EPR, nourries des échanges avec les experts du secteur nucléaire, et reflète la pratique française.

Les fonctions associées aux systèmes programmés peuvent connaître des défaillances du fait d'une logique inadéquate dans certains cas ; il s'agit donc de sources de défaillance des systèmes autres que les pannes aléatoires des matériels, ce qui suscite des interrogations quant à leurs conséquences.

Si les pannes matérielles pouvant affecter les systèmes de sûreté sont prises en compte par la mise en œuvre d'architectures redondantes et par la réalisation d'essais périodiques adaptés et par de la maintenance préventive, les défauts pouvant affecter les logiciels ne sont pas de même nature et ne peuvent pas être prévenus ou étudiés avec les mêmes moyens.

L'approche classique de développement des logiciels, utilisée par exemple en informatique bureautique, ne permet pas de maîtriser suffisamment leur conception et conduit à la réalisation de produits non vérifiables et affectés de nombreux défauts.

300. À considérer comme un référentiel d'expertise pour l'IRSN.

De plus, les tentatives faites pour maîtriser la fiabilité de logiciels sans viser en priorité à éliminer les défauts de leurs logiques se sont révélées inadéquates : par exemple, la mise en parallèle de plusieurs versions dans l'espoir de masquer les défauts de chacune par un vote majoritaire, est peu praticable dans les faits et des expérimentations ont montré son inefficacité ; les analyses probabilistes visant à estimer des taux de défaillance ne sont pas applicables à l'évaluation de logiciels et les analyses de « propagation » de défaillances utilisées avec succès pour les matériels ne sont pas non plus applicables aux logiciels.

C'est pourquoi, comme cela a été indiqué ci-dessus, une démarche spécifique a été retenue pour la conception de systèmes de contrôle-commande programmés de réacteurs nucléaires, considérée comme permettant d'apporter les justifications appropriées de leur validité. Elle est fondée sur une maîtrise des différentes étapes du processus industriel que sont la spécification des exigences de conception, la conception, la réalisation et l'intégration (assemblage des différents composants du système), qui comportent chacune des vérifications ; une étape finale de validation indépendante constitue une précaution supplémentaire.

Cette démarche est complétée par une diversification fonctionnelle qui permet de pallier un hypothétique défaut de conception ou de réalisation de certaines fonctions, au moyen d'autres fonctions utilisant des signaux physiques ou des traitements différents. De plus, une hypothétique défaillance technologique d'une famille de calculateurs est palliée par un moyen fondé sur des mécanismes et des composants logiciels et matériels différents.

7.4. Classement de sûreté des équipements

7.4.1. Importance des équipements pour la sûreté et classement de sûreté

L'atteinte et le maintien d'un niveau de sûreté approprié nécessite que soit mise en œuvre une démarche garantissant que les équipements[301] font l'objet d'exigences adaptées en termes de conception, de fabrication, de qualification, d'exploitation et de suivi en service, proportionnées à leur importance pour la sûreté. C'est le rôle du classement de sûreté.

Les équipements peuvent être classés au titre de la prévention des incidents et accidents, de la limitation de leurs conséquences ou de la protection contre les agressions, ainsi qu'en fonction de leur typologie (mécaniques, électriques…).

301. Cette notion utilisée dans ce paragraphe vise des matériels (structures, composants) ou des systèmes composés de matériels (ce que recouvre le terme SSC en anglais) considérés comme des « éléments importants pour la sûreté » selon la terminologie de l'« arrêté qualité » du 10 août 1984. Le guide ASN n° 22 élargit la notion de classement aux éléments importants pour la protection (EIP), notion de la loi TSN (voir le paragraphe 2.2).

L'affectation des équipements à un nombre réduit de classes de sûreté permet de simplifier la conception en attribuant des exigences communes à tous les équipements relevant d'une même classe.

La liste des classes de sûreté retenue par Électricité de France est présentée ci-après pour les réacteurs de 900 MWe, 1 300 MWe et 1 450 MWe – le cas du réacteur EPR Flamanville 3 est abordé plus loin –, puis des éléments d'explication sont apportés sur les caractéristiques des différentes classes, notamment sur les classes utilisant l'appellation « non classé », sémantiquement équivoque, mais historiquement logique :

– les équipements mécaniques sous pression relèvent des classes 1 à 3 et « non classé » ;
– les équipements mécaniques sans pression relèvent d'une classe « lié à la sûreté » (LS, appellation spécifique aux réacteurs des paliers 1 300 MWe et 1 450 MWe) et d'une classe « non classé » ;
– les équipements électriques relèvent des classes 1E, D (spécifique aux réacteurs de 1 300 MWe), 2E (spécifique au palier N4) et « non classé ».

Enfin, à l'ensemble de ces classes s'ajoute la classe IPS-NC d'équipements « importants pour la sûreté – non classés ». Dans l'appellation IPS-NC, « non classé » signifie que les équipements qui en relèvent n'étaient pas classés à la conception initiale des réacteurs déjà construits, alors que ces équipements sont importants pour la sûreté ; la classe IPS-NC est une classe de sûreté à part entière et des exigences lui sont associées (assurance de la qualité et essais périodiques).

Les ouvrages de génie civil font également l'objet d'un classement en rapport avec leur importance pour la sûreté.

▶ Classes de sûreté initialement retenues pour les réacteurs de 900 MWe et 1 300 MWe

À la conception initiale des réacteurs de 900 MWe et de 1 300 MWe, seules les classes 1 à 3 et 1E ont été retenues par Électricité de France ; elles ont été complétées, mais elles sont toujours en vigueur. En effet, à cette époque, l'intérêt se portait surtout sur la conception des systèmes de protection et de sauvegarde et notamment sur les premières phases des accidents au cours desquelles ces systèmes sont mis en œuvre de façon automatique.

La classe 1, la plus contraignante en termes d'exigences, s'applique aux équipements mécaniques soumis à la pression dont la défaillance entraînerait un accident de perte de réfrigérant primaire (APRP) correspondant à une condition de fonctionnement de catégorie 3 ou 4, selon la taille de la brèche (voir les chapitres 8 et 9).

La classe 2 s'applique aux équipements mécaniques soumis à la pression des circuits véhiculant du fluide primaire mais ne relevant pas de la classe de sûreté 1, ainsi qu'aux matériels des systèmes nécessaires pour confiner la radioactivité en cas d'APRP

(ce qui inclut les matériels mécaniques des systèmes de sauvegarde, tels que les systèmes d'injection de sûreté et d'aspersion d'eau dans l'enceinte de confinement), aux traversées de l'enceinte de confinement et à des équipements contenant du fluide radioactif (tels que certains équipements du système de contrôle chimique et volumétrique du fluide primaire [RCV]).

La classe 3 s'applique aux équipements mécaniques soumis à la pression, importants pour la sûreté mais ne relevant pas des classes de sûreté 1 et 2. Elle s'applique ainsi aux équipements dont la défaillance n'a pas de conséquences radiologiques directes, ainsi qu'aux équipements dont la défaillance pourrait conduire à un relâchement de gaz radioactifs entreposés pour décroissance. En particulier, les équipements mécaniques des systèmes supports aux systèmes de sauvegarde relèvent de la classe 3.

La classe 1E correspond aux équipements électriques assurant :

- l'arrêt automatique du réacteur,
- le refroidissement de secours du cœur,
- l'évacuation de la chaleur résiduelle du réacteur,
- l'évacuation de la chaleur du bâtiment du réacteur,
- l'isolement de l'enceinte de confinement,
- la prévention de rejets importants de substances radioactives dans l'environnement.

Les ouvrages de génie civil sont classés de sûreté s'ils :

- assurent une fonction de sûreté,
- supportent, protégent ou abritent des équipements mécaniques ou électriques classés de sûreté,
- assurent la protection biologique contre les rayonnements ionisants ou un confinement de substances radioactives liquides ou gazeuses.

▶ Classes de sûreté complémentaires pour les réacteurs de 900 MWe, de 1 300 MWe et de 1 450 MWe

Comme cela a été indiqué plus haut, les classes de sûreté retenues lors de la conception des réacteurs de 900 MWe et de 1 300 MWe visaient principalement les équipements dont la défaillance pouvait être à l'origine d'un accident et les équipements des systèmes intervenant dans la phase de fonctionnement automatique des réacteurs à la suite d'un accident. Plusieurs études ont mis en évidence que cette approche était trop restrictive et que la démonstration de sûreté reposait en fait sur un nombre plus important d'équipements qui méritaient de se voir attribuer un classement de sûreté.

À titre d'exemple, en cas d'accident de rupture d'un tube de générateur de vapeur, la phase pendant laquelle l'équipe de conduite est appelée à intervenir manuellement

est essentielle pour limiter les conséquences radiologiques. Les systèmes utilisés à cette fin ne sont pas les systèmes de sauvegarde classés de sûreté au titre des pratiques évoquées ci-dessus, mais des équipements mis en œuvre manuellement par des opérateurs, non classés selon ces pratiques, à savoir les organes de décharge dans l'atmosphère du circuit secondaire, qui permettent de refroidir le circuit primaire jusqu'à un état sûr, et le système d'aspersion d'eau dans le pressuriseur dont l'action est indispensable pour réduire la pression dans le circuit primaire et limiter ainsi les relâchements de substances radioactives.

Aussi, dans les années 1980, le classement de sûreté a été complété pour les équipements électriques par l'introduction, pour les réacteurs de 1 450 MWe, de la classe 2E et, rétrospectivement pour les réacteurs de 1 300 MWe, de la classe D, qui concernent les équipements utilisés lors de la phase d'intervention humaine[302] en vue d'assurer le retour et le maintien du réacteur dans un état sûr à la suite d'une situation accidentelle. De la même façon, les équipements mécaniques non soumis à la pression utilisés dans la démonstration de sûreté, qui n'étaient pas classés de sûreté, se sont vus attribuer la classe « lié à la sûreté » (LS).

Enfin, pour les réacteurs déjà construits à cette époque (réacteurs de 900 MWe et de 1 300 MWe de type P4), une classe IPS-NC (important pour la sûreté – « non classé ») a été introduite pour les équipements mécaniques ou électriques nécessaires au retour et au maintien du réacteur dans un état sûr dans les conditions de fonctionnement de dimensionnement et dans les situations du « domaine complémentaire » – voir les chapitres 8 et 13). Ce classement a ensuite été étendu, pour tous les types de réacteurs, à des dispositions nécessaires pour la protection contre les agressions internes ou externes (incendie, inondation, explosion…), ainsi qu'à des équipements non indispensables mais permettant de faciliter ou d'améliorer la conduite accidentelle.

▶ Classes de sûreté du réacteur EPR (Flamanville 3)

Le classement de sûreté des matériels et des systèmes du réacteur EPR reflète :

– l'importance de la fonction de sûreté qu'ils réalisent : c'est l'objet du classement « fonctionnel » ;

– leur importance en tant que barrière de confinement, en fonction des rejets pouvant résulter de leur défaillance, à l'intérieur de l'installation et dans l'environnement : c'est l'objet du classement « mécanique ».

La définition du classement fonctionnel fait intervenir trois états physiques du réacteur :

– l'état contrôlé : le cœur est sous-critique, l'évacuation de la puissance est assurée à court terme par exemple par les générateurs de vapeur, l'inventaire en eau dans le cœur est stable, les rejets radioactifs restent tolérables ;

302. Phase dite C, après la phase automatique dite B (voir le paragraphe 8.4).

– l'état d'arrêt sûr : le cœur est sous-critique, la chaleur résiduelle est évacuée durablement, les rejets radioactifs restent tolérables ;

– l'état final : le cœur est sous-critique, la puissance résiduelle est évacuée par les systèmes primaire ou secondaire, les rejets radioactifs restent tolérables.

Sont classées F1A toutes les fonctions de sûreté (et les matériels et systèmes assurant ces fonctions) nécessaires pour atteindre l'état contrôlé du réacteur dans les conditions de fonctionnement de référence PCC-2 à PCC-4 (désignation pour le réacteur EPR des conditions de fonctionnement de référence de catégories 2 à 4 – les désignations adoptées pour le réacteur EPR sont précisées aux paragraphes 8.1 et 13.5).

Sont classées F1B toutes les fonctions de sûreté nécessaires, au-delà de l'atteinte de l'état contrôlé, pour atteindre l'état sûr et pour le maintenir dans les conditions de fonctionnement de référence PCC-2 à PCC-4.

Sont classées F2 notamment :

– les fonctions de sûreté nécessaires pour atteindre et maintenir l'état final pour les conditions de fonctionnement RRC-A,

– les fonctions nécessaires pour prévenir les rejets importants et pour atteindre et maintenir un état maîtrisé en cas d'accident avec fusion du cœur postulé (RRC-B),

– les fonctions conçues pour maîtriser les agressions externes ou internes.

Le classement mécanique concerne tous les équipements ou portions de circuits :

– dont la défaillance peut conduire, dans les conditions de fonctionnement de référence PCC-1 à PCC-4 et RRC, à un rejet d'activité significativement supérieur à la contamination du milieu environnant,

– ou qui participent à une fonction de sûreté F1A ou F1B.

Les classes mécaniques sont :

– M1 pour le circuit primaire principal,

– M2 pour les équipements ou portions de circuits dont le fonctionnement est prévu dans des situations où ils sont susceptibles de véhiculer du fluide primaire alors que l'intégrité des gaines du combustible n'est pas garantie (par exemple l'injection de sécurité),

– M3 pour les autres équipements ou portions de circuits mécaniques classés (par exemple les systèmes supports des systèmes de sauvegarde).

7.4.2. Exigences génériques associées aux différentes classes de sûreté

Des exigences génériques sont associées aux différentes classes de sûreté. Les différences entre classes sont illustrées ci-après pour les classes retenues pour les réacteurs

de 900 MWe, de 1 300 MWe et de 1 450 MWe. Une démarche similaire a été appliquée pour le réacteur EPR Flamanville 3. Les exigences en matière de qualification ne sont pas mentionnées ici car elles sont développées au paragraphe 7.4.3.

▶ Exigences de conception, de fabrication et de suivi en exploitation

Les équipements classés 1, 2, 3, LS, 1E, 2E, D et les ouvrages de génie civil classés font l'objet des exigences suivantes :

- application d'un code de conception et de construction qui définit notamment les méthodes de calcul, d'approvisionnement, de construction, d'implantation,
- mise en œuvre de procédures d'assurance de la qualité (exigences de l'« arrêté INB » de 2012, après celles de l'« arrêté qualité » de 1984),
- réalisation d'essais périodiques en exploitation (suivi périodique en exploitation pour les ouvrages de génie civil),
- « tenue » aux sollicitations sismiques.

De plus, pour les équipements électriques des classes 1E et 2E, la redondance et le secours de leurs alimentations électriques sont requis. En revanche, pour les équipements électriques de la classe D des réacteurs de 1 300 MWe, la redondance et le secours de leurs alimentations électriques n'ont pas été requis, bien qu'ils fussent le plus souvent réalisés.

Les codes de conception et de construction appliqués aux équipements classés étaient initialement des codes américains (ASME notamment) ; ils ont été progressivement remplacés par les codes français suivants :

- le recueil des règles de conception et de construction des matériels[303] mécaniques des îlots nucléaires REP (RCC-M) au lieu du code ASME III, dont la version révisée de 1986 a fait l'objet d'une acceptation[304] de l'autorité de sûreté en 1986 ; ce recueil a été utilisé à partir des réacteurs de 1 300 MWe de la centrale nucléaire de Cattenom, pour les classes 1 à 3, avec un niveau d'exigences décroissantes (notamment en matière de contrôles de fabrication) de 1 à 3 ;
- le recueil des règles de conception et de construction des matériels électriques des îlots nucléaires REP (RCC-E) au lieu des normes de l'IEEE[305], dont la version révisée de 1984 a fait l'objet d'une acceptation de l'autorité de sûreté également en 1986, pour les classes 1E et 2E.

303. Les codes de conception et de construction utilisent le terme « matériel » et non celui d'« équipement ».
304. Acceptation assortie de conditions d'utilisation. Cette acceptation a fait l'objet de RFS qui sont citées dans l'annexe du chapitre 2.
305. Institute of Electrical and Electronics Engineers (Institut des ingénieurs électriciens et électroniciens, association professionnelle).

Quelques indications sont fournies sur le RCC-M dans le focus à la fin du présent chapitre.

Les structures de génie civil ont, pour les premières tranches du parc électronucléaire français, été réalisées selon des « cahiers de prescriptions spéciales » regroupant des règles et pratiques françaises (règles du ministère en charge des travaux publics et des transports) et, pour les parties métalliques, du code ASME III. La version révisée de 1981 du recueil d'exigences RCC-G (règles de conception et de construction pour le génie civil des îlots nucléaires REP) a fait l'objet d'une acceptation de l'autorité de sûreté. À partir de 2006, pour le réacteur EPR Flamanville 3 (et pour les réexamens périodiques des réacteurs du parc électronucléaire), c'est le recueil des règles de conception et de construction pour le génie civil RCC-CW[306], intégrant les Eurocodes[307], qui est utilisé.

Il convient aussi de citer le RCC-C, recueil des règles de conception et de construction spécifique pour les assemblages combustibles des centrales nucléaires REP, utilisé depuis la fin des années 1980, et le RCC-I, recueil des règles de conception et de construction applicables à la protection contre l'incendie des tranches REP, utilisé depuis le début des années 1980.

Pour le réacteur EPR, les exigences associées aux équipements électriques classés fonctionnellement F1A et F1B sont identiques à celles qui ont été appliquées aux équipements classés respectivement 1E et 2E des réacteurs précédents : celles qui sont associées aux équipements mécaniques sous pression classés M1, M2 et M3 sont identiques à celles des équipements classés respectivement 1, 2 et 3 des réacteurs précédents. Il est à noter toutefois que l'utilisation des codes américains ASME et IEEE et des règles établies par le comité de sûreté nucléaire allemand KTA sont autorisées dans certaines conditions.

▶ Exigences fonctionnelles

Les exigences fonctionnelles sont relatives à la fonction de sûreté réalisée par les équipements.

Aux équipements électriques n'est assigné qu'un seul type d'exigence fonctionnelle, celui d'assurer la réalisation de la fonction qu'ils doivent remplir (« fonctionnalité »).

Pour les équipements mécaniques, comme cela a été introduit au paragraphe 7.2, sont distingués les équipements (vannes, pompes, clapets…) comportant des mécanismes ou des parties mobiles qui doivent accomplir un mouvement pour assurer leur fonction de sûreté (équipements « actifs ») et les autres équipements (récipients ou capacités, tuyauteries, échangeurs…), qui sont « passifs ». Trois types d'exigences fonctionnelles sont définis :

306. CW pour *Civil Works*, ou aussi ETC-C (*EPR Technical Code for Civil works)*.
307. Les Eurocodes sont les normes européennes de dimensionnement et de justification des structures de bâtiment et de génie civil consultables à l'adresse http://eurocodes.fr/.

1. L'« intégrité »[308] pour une « barrière de pression », qui s'applique à l'enveloppe sous pression des équipements mécaniques passifs ; elle vise à garantir que ces équipements assurent le confinement du fluide véhiculé.
2. La « capacité fonctionnelle », qui s'applique aux équipements passifs traversés par un fluide ; elle limite les déformations acceptables de ces équipements de telle sorte qu'il n'y ait pas de réduction du débit du fluide qui empêcherait l'accomplissement de la fonction de sûreté concernée.
3. L'« opérabilité », qui s'applique aux équipements mécaniques actifs ; elle consiste à assurer le bon fonctionnement des mécanismes ou parties mobiles dont le mouvement est nécessaire à l'accomplissement de la fonction de sûreté de ces équipements (vannes, clapets, soupapes…).

Les exigences fonctionnelles interviennent dans le choix des règles et critères des codes de conception et de construction des matériels mécaniques à retenir pour la conception (y compris le dimensionnement) des matériels concernés. Les codes précisent les méthodes de calcul applicables aux matériels (classés en niveaux – voir le focus à la fin du présent chapitre) pour s'assurer de leur résistance à l'égard d'un certain nombre de types d'endommagement ; le RCC-M prévoit, pour chaque niveau, quatre niveaux de critères, de sévérité décroissante, désignés par les lettres A, B, C et D, auxquels sont associées des règles et des limites (critères) spécifiques.

▶ Exigence de tenue aux sollicitations sismiques

En parallèle du classement de sûreté, un classement sismique est défini. Il s'applique aux équipements dont le fonctionnement ou l'intégrité doit être maintenu lorsqu'ils sont soumis aux chargements résultant d'un séisme. Quel que soit le palier de réacteurs, des chargements sismiques ont été considérés à la conception pour le dimensionnement des équipements classés, ce qui a conduit au classement sismique des équipements mécaniques classés 1, 2, 3 et LS et des équipements électriques classés 1E, 2E et D. Le classement sismique des matériels importants pour la sûreté non classés (IPS-NC) de sûreté est défini au cas par cas, en fonction de leur rôle dans les situations pouvant être induites par un séisme.

Pour le réacteur EPR, les équipements classés fonctionnellement F1A et F1B ou ayant un classement mécanique M1 ou M2 sont classés « sismiques ». Le classement sismique des matériels F2 et M3 est défini au cas par cas, en fonction de leur rôle dans les situations pouvant être induites par un séisme.

308. Ce terme est notamment utilisé dans la règlementation française. L'intégrité d'une barrière y est définie ainsi : *« Absence d'altération irréversible d'une barrière remettant en cause l'efficacité prévue dans la démonstration de sûreté nucléaire »* (guide ASN n° 22, annexe 1). Selon cette définition, une inétanchéité peut être considérée comme une perte d'intégrité.

Les équipements classés « sismiques » doivent satisfaire leurs exigences fonctionnelles lorsqu'ils sont soumis aux chargements résultant d'un séisme majoré de sécurité (SMS) ou d'un séisme de dimensionnement (SDD)[309].

7.4.3. Qualification des équipements aux conditions accidentelles

La qualification est la démonstration qu'un équipement important pour la sûreté est apte à assurer ses fonctions dans les conditions (température, pression, humidité, irradiation, séisme…) auxquelles il est susceptible d'être soumis.

Le processus de qualification des équipements débute dès la conception du réacteur par l'identification des exigences qui leur sont attribuées et se poursuit par la définition et la réalisation d'un programme de qualification permettant d'apporter les justifications appropriées quant au respect de ces exigences ; il est visé que ce processus soit, autant que possible, achevé à la mise en service du réacteur.

Les sollicitations prises en compte lors du processus de qualification sont :

– l'ambiance dégradée dans laquelle l'équipement doit fonctionner, en termes de pression, de température, d'humidité et d'irradiation ;

– les sollicitations sismiques, pour les équipements classés sismiques ;

– des conditions particulières : il s'agit par exemple de l'aptitude, pour une vanne ou un clapet situé sur une tuyauterie de haute énergie (THE), à isoler une brèche de cette tuyauterie, de l'aptitude à véhiculer du fluide radioactif chargé de débris (pour les équipements des circuits véhiculant du fluide primaire en recirculation à partir des puisards du bâtiment du réacteur)…

La qualification aux conditions accidentelles concerne les équipements électriques et les équipements mécaniques actifs ayant une exigence d'« opérabilité ». Pour les équipements mécaniques passifs, l'application de critères de conception appropriés est réputée garantir le respect de leurs exigences fonctionnelles (intégrité, capacité fonctionnelle), sans démonstration supplémentaire. Toutefois, les équipements appartenant à la troisième barrière de confinement et à son « extension » (voir le paragraphe 6.3) font l'objet d'une exigence d'étanchéité qui peut nécessiter la qualification de composants passifs, quand ceux-ci peuvent être dégradés dans les conditions accidentelles retenues (cas des joints en matériaux élastomères).

Les revêtements et les peintures (notamment de parois en béton) à l'intérieur du bâtiment du réacteur ont également une exigence de qualification à des conditions d'ambiance dégradées (pression, température, humidité…), afin de garantir qu'ils ne risquent pas de produire en conditions accidentelles des débris susceptibles d'entraver

309. Ces notions sont précisées au paragraphe 12.3. Le SDD peut être, comme cela est le cas pour le parc électronucléaire français, une enveloppe des séismes majorés de sécurité (SMS) des sites d'implantation des réacteurs ; il en est de même pour le demi-séisme de dimensionnement (DSD) par rapport au séisme maximal historiquement vraisemblable (SMHV).

la recirculation d'eau par les puisards et les systèmes d'injection de secours d'eau dans le circuit primaire (RIS) ainsi que d'aspersion d'eau dans l'enceinte de confinement (EAS) – ce sujet est abordé notamment au chapitre 9.

En complément des conditions accidentelles, la qualification tient compte du vieillissement des équipements et des revêtements (vieillissement dû à la température, à l'irradiation et aux sollicitations mécaniques subies tout au long de la vie de l'installation [vibrations…]).

Jusqu'en 2006, les équipements à qualifier se voyaient appliquer l'un des trois « profils de qualification » standardisés suivants :

– le profil dit K1 pour les équipements implantés dans le bâtiment du réacteur nécessaires dans des conditions accidentelles entraînant une ambiance dégradée dans le bâtiment. Ce profil (voir la figure 7.3 plus loin) est enveloppe des conditions d'ambiance accidentelle les plus pénalisantes retenues (hors accident avec fusion du cœur), à savoir celles qui pouvaient résulter d'un accident de perte de réfrigérant primaire ou de rupture d'une tuyauterie de vapeur ;

– le profil dit K2 pour les équipements implantés dans le bâtiment du réacteur qui doivent être aptes à remplir leurs fonctions dans les conditions d'ambiance normales ;

– le profil dit K3 pour les équipements implantés en dehors du bâtiment du réacteur ; toutefois, les équipements nécessaires dans des conditions accidentelles entraînant une ambiance dégradée dans les locaux où ils sont implantés (par exemple ceux qui sont implantés dans les casemates abritant les lignes de vapeur) ainsi que les équipements pouvant être amenés à véhiculer du fluide radioactif chargé de débris (matériels des systèmes RIS et EAS) subissaient en outre une qualification à ces conditions particulières (profil dit K3AD).

À partir de 2006, différentes familles d'ambiance (au nombre de six) ont été définies par Électricité de France et prises en compte pour la qualification des équipements du bâtiment du réacteur, permettant de mieux adapter leur qualification aux doses d'irradiation en situation accidentelle et aux durées pendant lesquelles leur fonctionnement devait être assuré en ambiance dégradée. La définition des familles d'ambiance repose sur deux paramètres :

– le type d'ambiance accidentelle à laquelle l'équipement peut être soumis pendant son fonctionnement,

– la durée de la phase accidentelle pendant laquelle il doit être apte à remplir sa fonction.

Des familles d'ambiance avaient déjà été définies auparavant (dans les années 1990) pour les équipements implantés en dehors du bâtiment du réacteur, en fonction des mêmes paramètres.

La prise en compte des familles d'ambiance a notamment permis de prononcer la qualification aux conditions accidentelles d'équipements déjà en place mais qui

faisaient l'objet d'écarts, par exemple les moteurs des pompes du système RRA, pour lesquels les doses d'irradiation accidentelle correspondent à la famille 4, alors que la dose maximale retenue pour les matériels utilisés lors d'un accident de perte de réfrigérant primaire de type « grosse brèche » est celle de la famille 6, qui correspond au profil de qualification K1[310].

Pour le réacteur EPR Flamanville 3, les familles d'ambiance ont été définies et appliquées dès la conception.

La qualification d'un équipement peut être obtenue soit par des essais, soit par des analyses (études), soit en combinant ces deux méthodes.

La qualification par essais consiste à soumettre un équipement « modèle » à des chargements représentatifs des conditions de fonctionnement normal et accidentel auxquelles il doit pouvoir faire face ; le programme des essais est décomposé en séquences d'essais successifs, qui visent à représenter les sollicitations susceptibles d'être subies par l'équipement. Cette méthode est celle qui est utilisée le plus souvent pour les équipements électriques.

À titre d'exemple, les équipements implantés dans le bâtiment du réacteur dont le fonctionnement est prévu dans le cas d'un accident de perte de réfrigérant primaire de type « grosse brèche » (voir le chapitre 9) ou de rupture d'une tuyauterie de vapeur subissent, lorsqu'ils sont qualifiés par des essais, la séquence d'essais normalisée suivante (correspondant au profil de qualification K1 du RCC-E) :

– au début de la procédure de qualification, des essais de référence, qui consistent à mesurer les caractéristiques fonctionnelles et électriques de l'équipement dans ses conditions normales de fonctionnement ;

– des essais aux limites d'emploi fonctionnelles de l'équipement, qui visent à caractériser le comportement de l'équipement dans les conditions limites de température, d'humidité, de perturbations électriques du fonctionnement normal ;

– des essais d'appréciation des évolutions possibles du comportement de l'équipement dans le temps, qui visent à simuler son vieillissement par des essais de vieillissement thermique (cas des équipements électriques), de sollicitations répétées (cycles d'ouverture et de fermeture pour les vannes, de démarrage et d'arrêt pour les moteurs, par exemple), de vibrations, d'irradiation (ce dernier essai peut être regroupé avec l'essai d'irradiation accidentelle) ;

310. La famille d'ambiance du circuit RRA est la famille 4 (ambiance thermodynamique dégradée et ambiance faible en irradiation, à long terme), car il est, dans la démonstration de sûreté, « valorisé » seulement pour l'étude des accidents de rupture de tuyauterie de vapeur (RTV) et des accidents de perte de réfrigérant primaire (APRP) de type « petite brèche ». Dans ces accidents, l'irradiation est faible (on considère 10 % de rupture de gaines pour un APRP « petite brèche », alors que l'on considère 100 % de rupture de gaines pour un APRP « grosse brèche » auquel correspond la dose d'irradiation accidentelle du profil K1). Ainsi, en prenant la dose correspondant à la famille 4, la dose de qualification a pu être réduite – sachant que les moteurs des pompes du circuit RRA ne peuvent pas être qualifiés à la dose K1.

– des essais de tenue aux séismes : l'équipement subit cinq fois les sollicitations correspondant au demi-séisme de dimensionnement (DSD) et au moins une fois celles correspondant au séisme de dimensionnement (SDD) ;

– des essais d'irradiation accidentelle ;

– des essais thermodynamiques effectués en soumettant l'équipement au profil K1.

Pour les équipements implantés dans le bâtiment du réacteur pour lesquels le profil de qualification K2 est retenu, les deux derniers essais ne sont pas effectués.

Pour les équipements implantés à l'extérieur du bâtiment du réacteur, pour lesquels le profil de qualification K3 est retenu, les essais d'irradiation et les essais thermodynamiques ne sont pas effectués, sauf pour les équipements relevant du profil K3AD qui sont qualifiés à l'ambiance thermodynamique (cas de ceux qui sont situés dans les casemates abritant les lignes de vapeur) ou à l'irradiation accidentelle (cas des équipements des systèmes RIS et EAS situés sur les lignes de recirculation d'eau à partir des puisards).

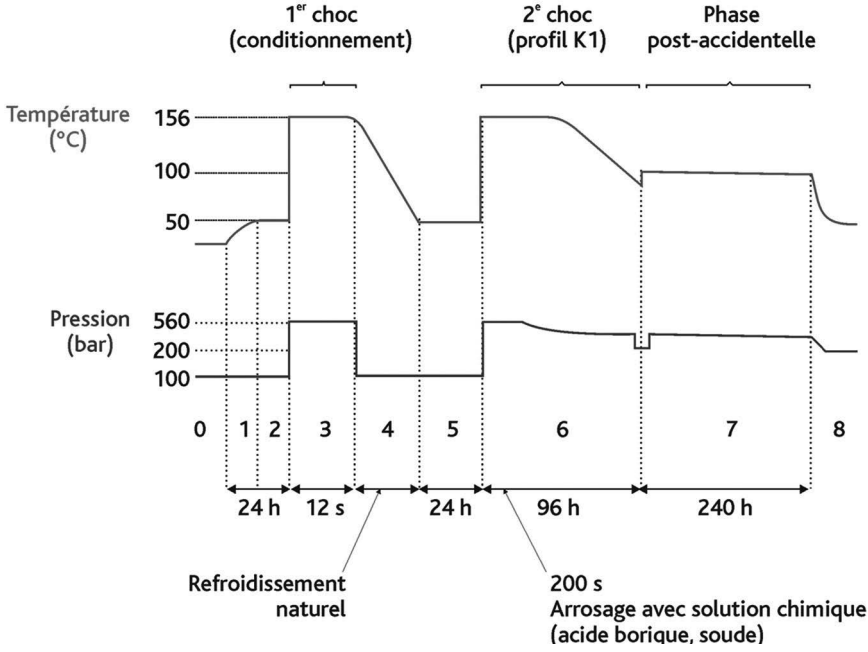

Figure 7.3. Exemple de profil de qualification K1. Marc Bouscasse/IRSN.

La qualification par analyses peut être réalisée :

– soit par analogie, sur la base de règles préétablies (technologie et dimensions similaires…), avec un équipement déjà qualifié par essais ; cette méthode est utilisée en particulier pour la robinetterie et les pompes ;

– soit par calcul avec un modèle de simulation représentatif de l'équipement et des méthodes ou codes de calcul qualifiés ; cette méthode est utilisée en particulier pour la qualification sismique de la robinetterie, des pompes et des gros équipements ;

– soit par l'expérience d'exploitation, quand les conditions correspondantes ont été au moins aussi sévères que celles auxquelles l'équipement doit pouvoir « résister ».

Une fois la qualification d'un équipement modèle prononcée, il est essentiel d'éviter que la fabrication, le montage, la maintenance ou l'exploitation des équipements dans les installations ne viennent la remettre en cause au cours du temps. Cela est assuré par un ensemble de dispositions regroupées sous l'expression « pérennité de la qualification », avec :

– la création et le maintien par le fournisseur d'un dossier de référence (DDR), qui décrit les éléments de fabrication permettant d'assurer la conformité des matériels fabriqués au modèle qualifié et d'en maîtriser les évolutions éventuelles ;

– l'élaboration, dès que la qualification d'un équipement modèle a été prononcée, d'une fiche de pérennité de la qualification précisant les prescriptions de montage et de maintenance à respecter (à titre d'exemples : types de graisses et de joints à utiliser pour satisfaire la qualification aux conditions d'ambiance, couples de serrage et freinage de la visserie pour satisfaire la qualification sismique…) ; ces prescriptions sont notamment prises en compte lors de la préparation des interventions sur les équipements ; le recueil des prescriptions de maintien de la qualification (RPMQ) est l'outil permettant aux centrales de maintenir la qualification dans le temps ;

– la maîtrise de l'approvisionnement et des conditions d'entreposage des pièces de rechange.

En règle générale, un équipement est qualifié pour une certaine « durée de vie ». Une extension de sa qualification peut néanmoins se révéler nécessaire ou souhaitable :

– soit pour augmenter sa « durée de vie » ;

– soit parce que la « durée de vie » qualifiée est revue à la baisse :

  • du fait de conditions d'environnement en fonctionnement normal (température, irradiation…) plus défavorables que prévu,

  • du fait d'évolutions des connaissances (retour d'expérience, connaissances nouvelles) mettant en évidence des mécanismes de vieillissement plus rapides que prévu, voire non connus précédemment.

Cette extension peut être réalisée par un ensemble de méthodes regroupées sous l'expression « réévaluation et extension de la durée de vie qualifiée »[311]. À titre d'exemple, des prélèvements et des essais de qualification ont été effectués sur des

311. L'expression « qualification progressive » est aussi utilisée.

câbles électriques et des peintures du bâtiment du réacteur dans le cadre du projet d'Électricité de France d'extension de la « durée de fonctionnement » des réacteurs (projet « DDF »). Il peut être également prévu de remplacer certains composants sensibles au vieillissement par de nouveaux composants neufs identiques.

Il convient de souligner ici le mode de qualification spécifique adopté pour le composant essentiel que constitue la cuve du réacteur, soumise notamment à une irradiation neutronique en provenance du cœur du réacteur. Des éprouvettes constituées du même matériau que celui de la cuve sont irradiées dans des zones proches du cœur et font l'objet d'essais mécaniques à différents moments de la vie de l'installation dans le but d'anticiper le comportement du matériau de la cuve (notamment en termes de seuil de transition de comportement mécanique ductile-fragile).

La qualification d'équipements aux conditions des accidents avec fusion du cœur est illustrée au chapitre 17 (pour les recombineurs d'hydrogène, le filtre à sable du système d'éventage-filtration de l'enceinte de confinement et le récupérateur de matériaux fondus du réacteur EPR).

7.5. Quelques éléments relatifs à la conception des équipements sous pression nucléaires[312]

L'histoire de la règlementation relative aux appareils à pression et plus spécifiquement de celle qui s'applique aux appareils utilisés dans les réacteurs nucléaires, dorénavant désignés d'équipements sous pression nucléaires (ESPN), est succinctement brossée dans le focus du chapitre 2. Quelques précisions plus techniques sont apportées ci-après concernant la conception de ces équipements[313].

De façon très schématique, les dispositions à retenir pour la conception d'un équipement sous pression visent la sécurité des personnes, en évitant notamment une rupture brutale de l'équipement en exploitation. En plus des dispositions techniques de nature à prévenir ce type d'accident, des « accessoires » de sécurité (tels que des soupapes…) sont installés sur les équipements, de façon à permettre une décompression suffisamment rapide avant qu'une augmentation de la pression ne soit de nature à provoquer la rupture de l'équipement.

Comme cela a été indiqué au chapitre 2, la règlementation relative aux ESPN[314] permet la mise en œuvre d'une approche unifiée et proportionnée aux risques pour tous les équipements sous pression nucléaires ; cette approche tient compte, selon l'équipement :

312. Éléments établis en collaboration avec Simon Liu de l'ASN/DEP et Remy Catteau de l'ASN/DCN.
313. Le lecteur pourra également consulter sur ce sujet les articles BN3280V1 et BN3282V1 des Techniques de l'ingénieur, rédigés par Jean-Marie Grandemange (†), intitulés « Conception des enceintes sous pression », parties 1 et 2, de janvier 2008.
314. Arrêté du 30 décembre 2015 « relatif aux équipements sous pression nucléaires », arrêté du 3 septembre 2018 « modifiant certaines dispositions applicables aux équipements sous pression nucléaires et à certains accessoires de sécurité destinés à leur protection ».

– de la pression et du volume ; ces éléments et le(s) type(s) de fluide(s) contenu(s) dans l'équipement déterminent la « catégorie » de l'équipement ; les cinq catégories définies à l'article R.557-9-3 du code de l'environnement sont notées (par ordre croissant des risques) 0, I, II, III, IV ;

– de l'inventaire radiologique contenu ou susceptible d'être contenu dans l'équipement en exploitation ;

– de la prise en compte ou non de sa défaillance dans les justifications de sûreté du réacteur.

Trois « niveaux » d'exigences sont définis, notés N1, N2 et N3 (par ordre décroissant), le niveau N1 le plus élevé visant *« les équipements pour lesquels le rapport de sûreté ne prévoit pas de mesures permettant de ramener l'installation dans un état sûr, ainsi que les équipements sous pression nucléaires constituant le circuit primaire principal et le circuit secondaire principal des chaudières nucléaires à eau… »*.

Sont classés N2 les équipements sous pression nucléaires qui ne sont pas classés N1 et dont la défaillance peut conduire à un rejet d'activité supérieur à 370 GBq, calculé en faisant la somme des activités des éléments présents (pondérées d'un facteur 1/1 000 pour certains comme le tritium, l'azote 13, l'azote 16…).

Sont classés N3 les autres équipements sous pression nucléaires.

La règlementation relative aux ESPN prévoit que, pour les réacteurs électronucléaires, un niveau N2 ou N3 soit attribué aux équipements déjà en exploitation et respectivement classés de sûreté 2 ou 3 – à l'exclusion évidemment du circuit primaire principal et du circuit secondaire principal (qui sont du niveau N1).

La règlementation relative aux ESPN définit ensuite un certain nombre d'exigences essentielles de sécurité[315] pour les équipements N1, N2 et N3, qui ont été classés dans les catégories I à IV – les équipements relevant de la catégorie 0, qui présentent des risques moindres, sont soumis aux règles de l'art ou aux guides professionnels. Les exigences essentielles de sécurité portent notamment sur :

– la conception de l'équipement,

– sa fabrication,

– la qualification technique des opérations d'élaboration de matériaux et de fabrication,

– les assemblages permanents (soudures…) et les opérations de soudage,

– les essais non destructifs ayant pour but de détecter des défauts de fabrication,

– la traçabilité des matériaux,

– les essais hydrostatiques ou les essais de résistance effectués avec un fluide autre que l'eau,

315. Cette notion, issue de la directive européenne 97/23/CE, a été précisée dans le focus du chapitre 2.

– les instructions de service (notices d'instructions), qui précisent les caractéristiques particulières de conception déterminantes pour la « durée de vie » de l'équipement,

– les exigences applicables aux matériaux et à leurs caractéristiques mécaniques.

Pour ce qui concerne le suivi en service, l'arrêté du 10 novembre 1999 (« arrêté exploitation ») demeure applicable pour le circuit primaire principal et pour le circuit secondaire principal des réacteurs à eau sous pression[316].

En matière de conception, la règlementation relative aux ESPN stipule que l'équipement doit être conçu de manière à minimiser les risques de perte d'intégrité *« en tenant compte des altérations des matériaux envisageables* […], *du vieillissement dû à l'irradiation »*. Pour les équipements de niveau N1, ces risques sont ceux qui sont liés :

– *« à la fatigue thermique oligocyclique ou à grand nombre de cycles,*

– *aux comportements thermiques différents de matériaux soudés ensemble,*

– *à la fatigue vibratoire,*

– *aux pics locaux de pression,*

– *au fluage,*

– *aux concentrations de contraintes,*

– *aux phénomènes de corrosion,*

– *aux phénomènes thermohydrauliques locaux nocifs,*

– *à la vidange de l'équipement en cas de rupture de tuyauterie. »*

Pour chaque équipement des réacteurs du parc électronucléaire relevant de la règlementation des appareils à pression, les justifications appropriées sont apportées par Électricité de France dans le cadre de différents dossiers, appelés dossiers de référence règlementaires (DRR) ; ils traitent notamment des matériaux utilisés, de la qualité de fabrication de l'équipement, de sa protection contre les surpressions, des « situations » retenues pour son dimensionnement (ce sujet est développé au paragraphe 8.6), de l'analyse du risque de rupture brutale…

Concernant les matériaux utilisés pour les équipements sous pression nucléaires, il a été explicitement stipulé dès l'arrêté de 1974 que *« les matériaux doivent être choisis de façon à éviter tout risque de rupture brutale en exploitation »* ; un certain nombre de critères concernant les caractéristiques mécaniques des matériaux y ont été prescrits dans ce sens (résistance à la traction, allongement à la rupture, résilience). Des critères

316. Avec quelques modifications apportées par un arrêté en date du 3 septembre 2018 (voir le focus du chapitre 2). Pour les autres ESPN, ce sont les annexes V et VI de l'« arrêté ESPN » qui s'appliquent.

analogues sont spécifiés dans la règlementation relative aux ESPN pour les équipements de niveaux N1 et N2.

Il a été indiqué plus haut que des accessoires de sécurité sont installés sur les équipements relevant de la règlementation des appareils à pression de façon à les décomprimer si nécessaire et éviter leur rupture. À cet égard, les risques de surpression, dans tous les états d'un réacteur à eau sous pression (notamment à froid), dans les circuits primaire et secondaire ainsi que dans certains des circuits qui leur sont connectés, sont tout particulièrement à examiner pour les différentes situations envisageables[317], en vue de définir ou de valider l'ensemble des dispositions de conception et d'exploitation permettant de maîtriser ces risques. Concernant le circuit secondaire, le caractère adéquat de la protection fondée sur l'association de lignes de décharge de vapeur et de soupapes doit être vérifié en considérant aussi l'évacuation de la puissance résiduelle du réacteur, la limitation des rejets radioactifs dans l'environnement et la prévention d'un refroidissement excessif du cœur du réacteur (risque d'apport de réactivité dans le cœur).

7.6. Quelques considérations générales sur la prise en compte des agressions dans la conception des installations

Certains phénomènes ou certains événements peuvent être à l'origine de conditions de nature à entraîner de manière directe ou indirecte des dommages à des équipements d'un réacteur électronucléaire avec des conséquences sur la sûreté. On les désigne sous le terme « agressions ». Selon leur origine[318], on distingue :

– les agressions internes quand la source de l'agression se trouve à l'intérieur de l'installation ; il s'agit par exemple d'un incendie qui se déclare dans un local, d'une inondation résultant de la rupture d'un réservoir, de l'impact d'un tronçon de tuyauterie sur un matériel en cas de rupture de cette tuyauterie (phénomène communément appelé fouettement de tuyauterie), de l'impact sur un matériel d'une charge qui chute (par exemple au cours d'une manutention)… ;

– les agressions externes d'origine naturelle : c'est le cas des séismes, des crues de cours d'eau, des ruptures de digues, voire de barrages, en amont de l'installation, de températures élevées, voire très élevées (canicule), de vents forts… ;

317. Dans les « directives techniques pour la conception et la construction de la prochaine génération de réacteurs nucléaires à eau sous pression » et dans le guide ASN n° 22, les situations envisageables sont les conditions de fonctionnement de référence (voir le paragraphe 6.5 et le chapitre 8) ainsi que les incidents de deuxième catégorie cumulés à une défaillance supposée de l'arrêt automatique du réacteur (l'arrêt automatique du réacteur a un effet bénéfique car il conduit à une baisse des pressions dans les circuits).

318. Les actes de malveillance constituent aussi des agressions ; ils ne sont pas abordés dans le présent ouvrage. Le lecteur pourra consulter, par exemple, l'ouvrage intitulé « Approche comparative entre sûreté et sécurité nucléaires », J. Jalouneix *et al.*, Collection documents de référence, IRSN/EDP Sciences, avril 2009, ainsi que l'article BN3940 V2 du 10 juillet 2017 des Techniques de l'ingénieur, par Jean Jalouneix, intitulé « Protection et contrôle des matières nucléaires ».

– les agressions externes associées à des activités humaines extérieures à l'installation, comme une chute d'avion ou une explosion accidentelle de gaz à proximité de l'installation.

À l'instar des événements internes à l'installation retenus dans le domaine de conception de base, des dispositions sont prises pour prévenir l'occurrence des agressions internes, mais leur survenue est toutefois postulée et d'autres dispositions sont prises pour en limiter les conséquences. En revanche, à l'égard des agressions externes, au-delà du choix du site – qui revêt une importance particulière –, les dispositions de conception ou d'exploitation visent la limitation des conséquences.

La disponibilité des équipements d'un réacteur électronucléaire nécessaires pour accomplir les fonctions de sûreté ne doit pas être compromise (du fait d'éventuels endommagements) lorsque survient une agression, compte tenu des règles d'étude associées, des effets directs ou indirects de cette agression (voir à ce sujet le guide ASN n° 22), tout particulièrement les trois fonctions fondamentales de sûreté que sont :

– la maîtrise de la réactivité (incluant bien évidemment l'arrêt du réacteur[319]),

– l'évacuation de la puissance (résiduelle si le réacteur est mis à l'arrêt),

– le confinement des produits radioactifs.

En d'autres termes, un « état sûr »[320] du réacteur doit pouvoir être rejoint si nécessaire et maintenu après une agression, dans lequel les fonctions précitées seront assurées durablement.

À cette fin, les équipements jouant un rôle dans les fonctions de sûreté sont, en tant que de besoin, protégés contre les effets de l'agression :

– soit par des dispositions qui empêchent les effets de l'agression de les atteindre ; c'est par exemple le cas des équipements protégés par des « filets de protection » contre d'éventuels projectiles en cas de vents violents, ou des équipements protégés par des structures pouvant résister à d'éventuelles chutes de charges… ;

– soit par une conception leur permettant de rester opérationnels en cas de survenue de l'agression ; c'est par exemple le cas des équipements qui sont conçus et dimensionnés pour résister aux séismes retenus dans les bases de conception du réacteur, voire à un séisme extrême[321].

319. De façon générale, l'exploitant d'une centrale doit être en mesure d'apprécier rapidement les risques en cas de survenue d'une agression externe afin de maintenir le ou les réacteurs du site concerné dans l'état de repli considéré comme le plus sûr ou en poursuivre l'exploitation (RFS I.3.b).

320. La définition de cette notion est donnée dans le focus du chapitre 8.

321. Cette notion a été retenue dans le cadre du retour d'expérience de l'accident de la centrale nucléaire de Fukushima Daiichi (voir le chapitre 6 précédent).

De façon générale, dans la démonstration de sûreté, l'analyse des risques liés aux agressions comprend deux phases :

– la détermination des caractéristiques des agressions[322] susceptibles d'affecter l'installation : pour un certain nombre d'agressions, un niveau de référence est défini pour la conception de l'installation ;

– la démonstration d'une protection appropriée à l'égard de chaque agression retenue.

Pour certaines agressions (rupture de tuyauterie, projectile interne…), une séparation géographique des équipements importants pour la sûreté peut être un moyen de protection de nature à éviter que des voies redondantes puissent être affectées par une même agression. Pour d'autres agressions, particulièrement les agressions externes d'origine naturelle, des études particulières sont souvent nécessaires car les effets de ces agressions peuvent affecter simultanément des voies redondantes, voire la totalité des installations d'un site.

Quelques autres éléments concernant l'étude des agressions, internes et externes, sont développés au paragraphe 11.1.

7.7. L'anticipation du démantèlement au stade de la conception

Il est important que les opérations de démantèlement d'une installation nucléaire fassent l'objet d'une réflexion dès le stade de sa conception, pour éviter que, le moment venu, apparaissent des difficultés de nature à compliquer et à retarder fortement ces opérations.

À cet égard, le guide ASN n° 22, relatif à la conception des réacteurs à eau sous pression, contient des recommandations pour la prise en compte du démantèlement au stade de la conception d'un tel réacteur : *« L'arrêt définitif, le démantèlement et l'état physique de l'installation visé après le démantèlement doivent être pris en compte à la conception afin d'en faciliter le déroulement avec notamment l'objectif de :*

– *permettre le démantèlement dans un délai aussi court que possible,*

– *permettre un assainissement complet de l'installation, c'est-à-dire le retour à l'état initial avant activation ou contamination des structures. »*

Il est aussi indiqué dans ce guide que, lors de la conception, les choix techniques établis en considérant notamment le retour d'expérience en matière de démantèlement, doivent notamment porter sur :

– *« la conception des équipements, l'agencement du bâti et des voies d'accès. Les équipements susceptibles de contenir des substances radioactives en fonction-*

322. Dans le cas des agressions externes, le terme « aléa » est souvent utilisé pour désigner ces caractéristiques.

nement normal et lors d'incidents doivent être conçus de façon à favoriser, dans la mesure du possible, leur inspection, leur caractérisation radiologique, leur assainissement, leur démontage et leur transport. Lorsque cela est pertinent, des protections radiologiques, facilement amovibles lors des opérations de démantèlement, doivent être mises en œuvre de façon à réduire l'activation des matériels et des équipements. Le bâti doit être agencé en tenant compte des futures opérations de démantèlement, en particulier pour ce qui concerne les composants dont la manutention est complexe. Une réflexion doit également être menée pour les équipements susceptibles de contenir des substances radioactives lors d'accidents ;

– *les matériaux : ils doivent être choisis en tenant compte de leur composition chimique et des phénomènes auxquels ils sont susceptibles d'être soumis afin de limiter les risques liés aux opérations de démantèlement et de faciliter la gestion ultérieure des déchets produits lors de ces opérations. »*

#FOCUS

Le RCC-M

Pour les matériels mécaniques (c'est-à-dire les récipients comme la cuve du réacteur, le pressuriseur, les tuyauteries, les organes de robinetterie…), le code de conception et de construction ASME a été initialement utilisé pour les réacteurs du palier 900 MWe, « introduit » de fait dans le cadre de la licence Westinghouse. Mais, ultérieurement, l'ingénierie française s'est dotée d'un code de nature équivalente, le RCC-M – recueil des règles de conception et de construction pour les matériels mécaniques.

Ce code (comme le code ASME) propose des règles qui traduisent le meilleur état de l'art concernant divers aspects, parmi lesquels :

– le choix des matériaux,
– les types d'assemblages soudés,
– le dimensionnement (vérification de règles et critères mécaniques),
– les contrôles de fabrication…

Trois jeux de règles sont proposés, associés à trois « niveaux » des matériels :

– les matériels de niveau 1, pour lesquels est proposé le jeu de règles les plus sévères,
– les matériels de niveau 2,
– les matériels de niveau 3, pour lesquels est proposé le jeu de règles les moins sévères (autorisant notamment des contrôles partiels de fabrication).

Les matériels classés de sûreté 1, 2 et 3 sont alors soumis respectivement aux jeux de règles des niveaux 1, 2 et 3, sachant que des surclassements peuvent être adoptés au cas par cas.

Pour le dimensionnement (ou la vérification du dimensionnement), les règles et critères visent à se prémunir des divers modes d'endommagement redoutés à l'égard de chargements de différentes natures : par exemple des chargements thermomécaniques maintenus pendant un temps suffisant pour générer un risque d'endommagement par fluage, des chargements de brève durée pouvant conduire à un risque de déformation excessive instantanée, des chargements répétés créant un risque d'endommagement par fatigue.

Les limites préconisées – de catégories A, B, C et D par ordre décroissant de sévérité – ne sont pas les mêmes non seulement selon le « niveau » affecté à un matériel – donc sa classe de sûreté – et selon la catégorie de la situation de dimensionnement considérée, mais aussi selon l'exigence associée, fonction du rôle joué par le matériel. Les matériels « non statiques » peuvent être soumis à des règles et critères plus drastiques que les matériels « statiques ».

Pour l'application des codes tels que le RCC-M, les chargements thermomécaniques et leurs évolutions temporelles sont déterminés par les études des événements postulés dans l'analyse déterministe de la sûreté. Ces chargements font généralement l'objet de regroupements et de cumuls conservatifs (n'ayant souvent aucun caractère de vraisemblance) avant l'étape de vérification du respect des règles et critères mécaniques.