

La doctrine en matière de sûreté nucléaire : une amélioration continue intégrant mieux la gestion d'un accident nucléaire

Par Jean-Luc LACHAUME
et Sylvie CADET-MERCIER
Autorité de sûreté nucléaire (ASN)

Depuis les années 1970, la doctrine en matière de sûreté nucléaire a évolué, prenant en compte les leçons des incidents et accidents qui sont survenus dans le monde. À l'origine, la priorité était accordée à la prévention des accidents. Au fil des années, la limitation des conséquences des accidents et la gestion de crise ont été renforcées dans la doctrine de sûreté.

Cette évolution a conduit à un renforcement notable des installations nucléaires : l'analyse d'initiateurs d'accidents plus complexes, résultant notamment de cumuls d'événements, a conduit à la mise en place de dispositions matérielles et organisationnelles complémentaires afin de limiter les conséquences radiologiques. Puis, après l'accident de Tchernobyl, elle a conduit à un renforcement de la protection des populations : la gestion de crise, notamment en ce qui concerne la phase post rejets radioactifs, s'est particulièrement développée afin de mieux gérer sur le long terme les conséquences sanitaires, sociales et environnementales d'un accident.

Les centrales nucléaires se caractérisent par la présence d'une grande quantité de produits radioactifs, dont le confinement constitue un objectif primordial. En matière de sûreté, la conception d'un réacteur nucléaire consiste à définir des dispositions matérielles ou organisationnelles permettant de prévenir les incidents et de limiter les rejets de substances radioactives ou dangereuses, ainsi que leurs impacts sur l'homme et l'environnement, lors des incidents ou des accidents.

Depuis les années 1970, la doctrine en matière de sûreté nucléaire a évolué, prenant en compte les leçons des incidents et accidents qui sont survenus dans le monde. À l'origine, la priorité était accordée à la prévention des accidents. Au fil des années, la limitation des conséquences des accidents et la gestion de crise ont été renforcées dans la doctrine de sûreté.

Historiquement, les analyses de sûreté réalisées lors de la conception des réacteurs ne retenaient que des événements uniques

Lors de la conception, des mesures sont prises pour prévenir les événements indésirables. Toutefois, il est pos-

tulé que de tels événements peuvent survenir ; les événements pouvant affecter une centrale nucléaire peuvent être d'origine interne ou externe :

- un événement interne correspond à une défaillance intrinsèque de matériels de l'installation : par exemple, un dysfonctionnement conduisant à l'ouverture intempestive d'une vanne, à l'arrêt d'une pompe... ou à une rupture d'équipements.

En matière de sûreté, la conception a pour objectif de définir une disposition – ou parade –, pour mettre fin à la situation accidentelle ou pour en limiter les conséquences. Ces parades sont définies en analysant les défaillances de matériels considérées comme plausibles et les scénarios qui en résultent. Dans la plupart des cas, les parades consistent à activer l'arrêt automatique du réacteur ainsi qu'un système de secours apportant de l'eau ou de l'électricité, ce qui permet de revenir à un état maîtrisé de l'installation ;

- un événement externe correspond à un aléa externe à l'installation, qui peut induire des défaillances de matériels dans celle-ci : par exemple, un séisme, une inondation ou des conditions climatiques exceptionnelles (températures extrêmes, par exemple).

En matière de sûreté, la conception a pour objectif de définir des dispositions pour garantir le fonctionnement des équipements importants pour la sûreté lors de la survenue de ces événements et donc de se prémunir d'un risque de défaillance de ces équipements, en dimensionnant par exemple des matériels résistant au séisme ou en assurant un traçage (chauffage) des tuyauteries.

Il n'était pas postulé à l'époque de la conception que les dispositions définies puissent défaillir. Le risque d'accident grave était alors considéré comme hautement improbable, malgré la publication du rapport WASH-1400 (dont l'objectif était d'évaluer les risques pour la population dus à un accident dans une centrale nucléaire) et la survenue dans le monde de plusieurs accidents graves avec des conséquences radiologiques, tel celui de Windscale au Royaume-Uni, en 1957. Il existait cependant en France une organisation nationale de crise prévue par le plan d'organisation des secours (Orsec – plan créé en 1952, mais non spécifique au nucléaire) pour gérer toute situation accidentelle, mais aucun exercice nucléaire destiné à la tester n'était réalisé.

Et si les parades définies venaient à défaillir ?

Dans les années 1975, afin d'améliorer la sûreté des réacteurs, l'autorité de sûreté française a demandé aux concepteurs d'étudier également les conséquences d'une défaillance de matériels cumulée à celle de la parade prévue pour en limiter les conséquences. Ces études ont naturellement montré la nécessité de disposer de parades complémentaires (matériels ou procédures post-accidentelles) pour être en mesure de ramener le réacteur à un état sûr.

Ces parades complémentaires ont été mises en œuvre dans les centrales françaises au début des années 1980. Des procédures, dites ultimes, ont aussi été déployées pour limiter les conséquences radiologiques en cas d'accident avec fusion du cœur. Les études sur les accidents graves ont aussi conduit à mettre en place des matériels complémentaires (par exemple, les recombineurs d'hydrogène), notamment pour limiter les risques d'une défaillance de l'enceinte de confinement.

L'accident de Three Mile Island survenu en 1979 aux États-Unis a confirmé qu'il pouvait se produire une succession de défaillances techniques et d'erreurs humaines

L'accident de Three Mile Island qui s'est produit le 28 mars 1979 a débuté par un incident d'exploitation relativement banal : la défaillance de l'alimentation normale en eau des générateurs de vapeur, qui ont pour fonction d'évacuer la puissance du réacteur vers le circuit secondaire. La perte de cette capacité d'évacuation de la chaleur par les générateurs de vapeur a entraîné, en l'espace de quelques secondes, une forte augmentation de la température et de la pression dans le circuit primaire, provoquant l'arrêt automatique du réacteur. Cela correspond au scénario étudié lors de la conception.

Toutefois, deux défaillances complémentaires sont intervenues :

- la première défaillance complémentaire a affecté la vanne de décharge du pressuriseur, qui a pour fonction d'écarter la pression du circuit primaire : après s'être ouverte sous l'effet de l'augmentation de la pression, elle ne s'est pas refermée automatiquement lorsque la pression du circuit primaire a diminué. Par ailleurs, une erreur de conception a conduit à ce que l'opérateur ne dispose pas de cette information : en effet, le voyant en salle de commande indiquait l'ordre donné, mais pas la position réelle de la vanne. Le maintien de la vanne en position ouverte a conduit à une perte de fluide dans le circuit primaire, qui participe au refroidissement du cœur, dans l'enceinte de confinement ;
- la seconde défaillance complémentaire a concerné l'alimentation de secours des générateurs de vapeur : ce système n'a pas démarré, car deux vannes étaient fermées, au lieu d'être ouvertes, suite à une opération de maintenance. Par ailleurs, une erreur liée à la conception des générateurs de vapeur a empêché le refroidissement du cœur en l'absence de débit (thermosiphon). Cela a donc conduit au non refroidissement du circuit primaire par les générateurs de vapeur.

Les opérateurs en salle de commande n'ont pas été en mesure d'apprécier l'état réel de l'installation, notamment du fait de la présence d'alarmes en nombre très important et sans hiérarchisation ; ils ont donc réalisé des actions inappropriées. L'ensemble de ces défaillances a conduit à la perte du refroidissement du cœur, puis à sa fusion partielle (en moins de trois heures). Mais cela n'a pas généré de rejets importants dans l'environnement (la radioactivité est restée confinée majoritairement dans l'enceinte de confinement).

Cet accident a clairement montré qu'une succession de défaillances techniques et d'erreurs humaines est possible et peut conduire à des accidents plus graves que ceux considérés lors de la conception des centrales nucléaires. Après cet accident, les études probabilistes de sûreté (EPS), réalisées sur la base d'une liste aussi réaliste et complète que possible d'événements initiateurs et de situations couvrant des événements complexes et des cumuls d'événements, notamment celles liées à la perte des systèmes redondants ou à l'occurrence d'une agression interne ou externe, se sont fortement développées.

L'accident de Three Mile Island a aussi montré que les opérateurs, les responsables de la centrale et les autorités en charge de la protection des populations n'étaient pas suffisamment préparés pour gérer un accident avec fusion du cœur.

En France, à la suite de cet accident, il a été décidé de fixer les périmètres des plans particuliers d'intervention (PPI) autour des centrales nucléaires à 5 kilomètres pour l'évacuation des populations et à 10 kilomètres pour leur mise à l'abri. Ces distances ont été définies par l'Institut de protection et de sûreté nucléaire (IPSN, devenu aujourd'hui, l'Institut de radioprotection et de sûreté nucléaire (IRSN)) afin de prendre en compte les conséquences à court



Exercice de sécurité civile à la centrale nucléaire EDF de Saint Alban/Saint Maurice, janvier 2012.

« Pour tester les plans d'urgence interne (PUI) de chaque centrale nucléaire, le Service central de sûreté des installations nucléaires (SCSIN, aujourd'hui l'ASN) décida d'organiser des exercices de crise. Le premier exercice de crise préparé par l'IPSN eut lieu à Fessenheim en 1980. Le centre de crise de l'IPSN fut créé en 1982, et celui du SCSIN en 1984. »

terme d'un accident entraînant une fusion du cœur du réacteur, puis une défaillance après vingt-quatre heures de l'enceinte de confinement conduisant à un rejet filtré de produits radioactifs.

De plus, il a également été décidé, toujours à la suite de cet accident, de mettre en place des plans d'urgence interne (PUI) pour chaque centrale nucléaire. Pour tester ces plans, le Service central de sûreté des installations nucléaires (SCSIN, aujourd'hui l'ASN) décida d'organiser des exercices de crise. Le premier exercice de crise préparé par l'IPSN eut lieu à Fessenheim en 1980. Le centre de crise de l'IPSN fut créé en 1982, et celui du SCSIN en 1984.

En France, plusieurs défaillances sont induites en 1987 par un unique événement, un froid intense

Le 12 janvier 1987, une vague de froid s'étend sur l'ensemble du pays, ce qui conduit à une forte consommation électrique. Ces conditions de température conduisent à l'arrêt de trois groupes de production de la centrale thermique de Cordemais (Loire-Atlantique), ce qui entraîne une chute importante de la tension enregistrée sur le réseau 400 kVolts de la région Ouest et, en conséquence,

l'arrêt automatique de plusieurs réacteurs nucléaires dans cette même région.

Sur le réacteur de Chinon B3, à la suite de l'arrêt automatique du réacteur, deux défaillances principales liées au froid sont survenues :

- la perte du traçage des dispositifs d'assistance des soupapes de protection des générateurs de vapeur, ce qui a conduit à l'inétanchéité de deux soupapes,
- le gel de deux chaînes de mesure du niveau d'eau dans le réservoir alimentant le système d'injection de sécurité, ce qui aurait pu affecter le fonctionnement de ce système en cas de besoin.

Le retour d'expérience de cet événement montre que le cumul plausible de plusieurs défaillances pouvant résulter d'un unique événement (dans ce cas, le froid) doit aussi faire l'objet d'une attention particulière. Le cumul d'une perte du réseau électrique avec une situation de grand froid doit donc être considéré comme plausible, et, à ce titre, doit être considéré dans les analyses de sûreté, puisque c'est précisément pendant les périodes les plus froides que le réseau est le plus sollicité, et devient de ce fait plus sensible à une perturbation, telle que l'arrêt fortuit d'un réacteur nucléaire.

Par ailleurs, cet événement rappelle qu'il convient lors de la conception de prévenir les situations où un événement pourrait causer simultanément un défaut nécessitant l'intervention d'un système de sauvegarde et un défaut rendant impossible son fonctionnement.

L'accident de Tchernobyl survenu en Union soviétique, en 1986, pose question en matière de gestion post-accidentelle, de culture de sûreté et de transparence en matière nucléaire

Peu d'enseignements ont été tirés de l'accident de Tchernobyl en matière de sûreté nucléaire des installations françaises. Il n'en est pas de même dans le domaine de la gestion d'un accident nucléaire.

Tout d'abord, au plan international est apparue la nécessité d'avoir une approche coordonnée entre États en cas d'accident. Ainsi, les Conventions internationales sur la notification rapide d'un accident nucléaire et sur l'assistance ont été établies dès l'automne 1986.

En France, est apparu le besoin de renforcer la transparence en matière nucléaire. C'est ainsi qu'a été définie une échelle française de gravité permettant de classer les incidents et accidents. Cette échelle a ensuite été adaptée au plan international (échelle INES).

Par ailleurs, le retour d'expérience d'exercices plus réalistes comportant notamment des actions de sécurité civile conduits après 1986 avait montré que la distribution de comprimés d'iode stable à la population était difficile à réaliser en situation d'urgence. Ainsi, il fut décidé en 1997 de pré-distribuer les comprimés aux populations résidant dans les zones concernées par les PPI.

Enfin, le retour d'expérience de l'accident de Tchernobyl a montré que la gestion d'un accident nucléaire ne se résumait pas à la seule phase de rejets radioactifs, mais qu'il fallait aussi s'intéresser aux conséquences sanitaires, sociales et environnementales de l'accident sur le long terme. C'est pourquoi, l'ASN a commencé dès la fin des années 1990 à s'intéresser à la problématique post-accidentelle, ce qui l'a amenée à créer en 2006 un Comité directeur pour la gestion post-accidentelle (CODIRPA).

L'accident de Fukushima survenu au Japon, en 2011, montre qu'un événement extrême peut conduire à un cumul de défaillances, à la fusion du cœur et à la perte de confinement de plusieurs réacteurs sur un même site

Le vendredi 11 mars 2011, un séisme de magnitude 8,9 se produit à 80 kilomètres à l'est de l'île de Honshu au Japon, entraînant la perte de l'alimentation électrique de la centrale de Fukushima Daiichi, l'arrêt automatique des réacteurs et le démarrage de l'alimentation électrique interne de secours (groupes électrogènes de secours à moteur diesel).

Cinquante-cinq minutes plus tard, une vague de 14 mètres atteint la côte : elle endommage les prises d'eau de mer et provoque la perte des générateurs diesel de secours des réacteurs 1 à 4. Dès lors, les réacteurs ne sont plus refroidis. De plus, les opérateurs ne disposent pas en salle de commande d'indications fiables sur l'état des réacteurs.

Malgré les efforts déployés par les opérateurs de la centrale nucléaire de Fukushima Daiichi pour rétablir le refroidissement, les cœurs des réacteurs 1 à 3 sont entrés en fusion et les trois cuves de confinement se sont rompues. De l'hydrogène a été libéré à partir des cuves sous pression des réacteurs, ce qui a entraîné, à l'intérieur des bâtiments des réacteurs des tranches 1, 3 et 4, des explosions qui ont endommagé les structures et les équipements et blessé des membres du personnel. Les décompressions successives et les explosions ont entraîné des rejets importants de produits de fission radioactifs, comme l'iode 131 et le césium 137. Les autorités japonaises ont décidé, quelques heures après le début de l'accident, d'évacuer 80 000 personnes dans un rayon de 20 kilomètres et de mettre à l'abri la population vivant dans une zone correspondant à un rayon de 20 à 30 kilomètres.

L'accident de Fukushima a été provoqué par une agression naturelle extrême, qui a provoqué la défaillance de plusieurs systèmes de sûreté, une situation non prévue lors de la conception.

Cet accident a conduit l'Europe à réaliser des *stress-tests*, consistant à évaluer la résistance des installations pour des scénarios plus sévères que ceux retenus dans les études de sûreté, en particulier le comportement de l'installation en situation d'agression extrême ou de cumul de la perte totale des alimentations électriques et des sources de refroidissement, des situations hautement improbables.

Par ailleurs, il a aussi conduit à s'interroger sur le caractère approprié des parades envisagées en cas d'événement affectant tous les réacteurs d'un site : certains matériels (pompes, dispositifs de dépressurisation et de filtration, moyens de secours mobiles) sont en effet communs à plusieurs réacteurs.

À la suite de cet accident, la France a défini pour ses installations un « noyau dur », qui est constitué de matériels robustes, disponibles en toutes circonstances, capables de résister à des séismes ou à des inondations plus importants que ceux retenus lors de la conception ; des matériels permettant de prévenir un accident grave ou d'en maîtriser les conséquences, ou nécessaires à la gestion des situations de crise (moyens de gestion). La force d'action rapide nucléaire (FARN), créée par EDF, contribue à l'atteinte de ces objectifs.

L'accident de Fukushima a également contribué au renforcement de la préparation à la gestion d'un accident nucléaire. Ainsi, les associations regroupant les autorités de sûreté et de radioprotection européennes (WENRA et HERCA) ont adopté en 2014 une approche visant à améliorer la gestion des situations d'urgence et leur coordination transfrontalière. L'approche HERCA/WENRA vise

à promouvoir, en cas d'accident, la transmission rapide d'informations entre les pays concernés et la cohérence des recommandations émises par les autorités de radio-protection et de sûreté pour assurer la protection des populations.

En France, sous la direction du Secrétariat général de la Défense et de la sécurité nationale (SGDSN), un plan national de réponse à un accident nucléaire ou radiologique majeur a été élaboré. Sur la base du retour d'expérience de l'accident de Fukushima et de l'approche HERCA/WENRA, les pouvoirs publics ont également décidé d'étendre à 20 kilomètres les rayons des PPI et la distribution des comprimés d'iode stable aux populations.

Enfin, le CODIRPA a publié en 2012 de premiers éléments de doctrine destinés à améliorer la préparation à la gestion post-accidentelle, lesquels ont été complétés en 2019 pour mieux tenir compte du retour d'expérience de l'accident de Fukushima Daiichi. En effet, cet accident a montré qu'il fallait envisager des rejets radioactifs pendant plusieurs jours, alors que la doctrine de 2012 ne prenait en compte qu'un accident d'ampleur modérée s'accompagnant de rejets sur une courte durée.

Conclusion

La sûreté des réacteurs reposait à leur conception, dans les années 1970, essentiellement sur la prévention des accidents. Après l'accident de Three Mile Island notamment, la doctrine en matière de sûreté a notablement évolué : des moyens complémentaires ont été mis en place pour

prévenir l'accident grave (fusion du cœur) ; des moyens additionnels ont aussi été mis en place pour faire face aux cumuls d'événements. Enfin, le renforcement de la gestion des accidents graves, en termes de moyens participant à la limitation des conséquences et à la protection des populations, a été engagé. Il faut souligner que l'EPR a bénéficié dès sa conception de ces améliorations.

La gestion de crise, notamment en ce qui concerne la phase post rejets radioactifs, s'est particulièrement développée après l'accident de Tchernobyl afin de gérer les conséquences sanitaires, sociales et environnementales d'un accident sur le long terme. Les travaux pilotés par l'ASN ont conduit à la publication des premiers éléments de la doctrine nationale relative à la gestion post-accidentelle dans des territoires contaminés par des rejets en provenance d'une installation accidentée.

Enfin, l'accident de Fukushima Daiichi, qui a conduit à l'évacuation de la population d'une zone importante autour de la centrale, pose de nouvelles questions sur la gestion de crise, notamment : au nom du principe de précaution, faut-il évacuer (prévenir des cancers potentiels) des populations au risque d'engendrer des décès ? L'accident récent de Lubrizol, pour lequel aucune évacuation n'a eu lieu pour des raisons sanitaires, a mis en évidence que la confiance de la population dans les mesures prises par les pouvoirs publics était déterminante en matière de gestion de crise. Les années à venir seront assurément très riches en réflexions et débats sur ce qu'est une bonne gestion de crise.