

Préface de Philippe Le Poac

C'est au président de l'IMdR (Institut pour la Maîtrise des Risques) que les auteurs ont demandé cette préface, mais c'est peut-être aussi à celui qui a passé quarante ans de sa vie professionnelle au CEA, le Commissariat à l'Énergie Atomique, créé par une ordonnance du Général de Gaulle le 18 octobre 1945, et devenu Commissariat à l'Énergie Atomique et aux Énergies Alternatives en 2010.

On me pardonnera donc si cette préface est émaillée de quelques souvenirs personnels.

La sûreté de fonctionnement est dans l'ADN historique de l'IMdR. Et la sûreté de fonctionnement intègre la fiabilité, la maintenabilité, la disponibilité et la sécurité.

Le premier chapitre rappelle l'histoire de la notion et du mot fiabilité. Il est des domaines où la fiabilité est indépendante de la sécurité. On peut même penser à des cas où un système en panne étant devenu immobilisé devient totalement sûr. Une caractéristique essentielle du domaine nucléaire est que la fiabilité est inséparable de la sécurité.

Je suis obligé de parler vocabulaire. Pendant toute ma vie professionnelle, comme tous les professionnels du nucléaire, j'ai utilisé ces mots « sûreté nucléaire », traduction historique des mots anglais *nuclear safety*.

La loi 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire, dite loi TSN, a créé officiellement l'ASN, l'Autorité de Sûreté Nucléaire et définit la sûreté nucléaire comme l'ensemble des dispositions techniques et des mesures d'organisation relatives à la conception, à la construction, au fonctionnement, à l'arrêt et au démantèlement des installations nucléaires de base, ainsi qu'au transport des substances radioactives, prises en vue de prévenir les accidents ou d'en limiter les effets.

Devenu président de l'IMdR et me confrontant avec les autres milieux industriels, je me suis avisé que le mot anglais *safety* signifie sécurité. En dehors du domaine nucléaire, il est admis que la sécurité (*safety*) concerne la protection des personnes, des biens et de l'environnement contre les risques que pourrait créer un système. Et la sûreté (*security*) concerne la lutte contre la malveillance qui pourrait menacer le système. Les auteurs, conscients de cette difficulté de langage, utilisent d'ailleurs à plusieurs reprises les mots joints sécurité/sûreté.

Le chapitre 3 présente les principes du calcul de fiabilité dans les EPS (Évaluations Probabilistes de Sûreté) (en anglais : PSA, *Probabilistic Safety Assessment*) de niveau 1 dont l'objectif principal est de calculer le risque de fusion du cœur. Ces EPS s'appuient sur deux types de modèles : les arbres de défaillances et les arbres d'événements.

Le point de départ d'un arbre d'événements est ce qu'on appelle un événement initiateur. Cela peut être une défaillance simple, comme la rupture d'une tuyauterie, ou la résultante d'un arbre de défaillances. Il en est de même pour les événements correspondant aux embranchements des arbres d'événements.

La représentation graphique d'un arbre de défaillances et d'un arbre d'événements évoque un « nœud papillon » couramment utilisé en dehors du domaine nucléaire dans les études de danger imposées par la directive européenne Seveso pour des installations chimiques, gazières ou pétrolières.

Pour construire des arbres d'événements, le domaine du nucléaire fait un usage intensif de la modélisation physique et de la simulation numérique qui a fait des progrès considérables grâce à l'augmentation gigantesque des capacités de calcul informatique.

Ainsi, le code déterministe de thermohydraulique Cathare, développé en collaboration par le CEA, EDF, Areva et l'IRSN, permet, couplé avec un code de neutronique, de calculer avec précision l'évolution de la température et de la pression dans le circuit primaire en situations normales ou accidentelles.

La fiabilité nécessite des données.

Le chapitre 2 traite des données d'entrée : retour d'expérience et expertise. Le retour d'expérience (REX) comprend le retour d'expérience « événementiel » et le retour d'expérience « matériel ».

Il existe des composants actifs qui ne sont pas réparables mais qui peuvent être changés lors de la maintenance corrective ou préventive. Il y a aussi des composants actifs qui sont réparables. Pour ces composants, on dispose de données statistiques qui permettront d'évaluer leur fiabilité.

Un cas particulier concerne des composants actifs en attente : ils ne fonctionnent pas habituellement mais doivent pouvoir être opérationnels pour assurer des fonctions de sûreté en cas de besoin. Ces composants doivent être testés et leurs défaillances lors des essais alimentent les données nécessaires à l'évaluation de la fiabilité.

Le chapitre 5 présente les principales modélisations probabiliste et statistique utilisées pour la fiabilité des matériels industriels en soulignant la diversité des approches dues à la nature des équipements, l'impact de la maintenance, la qualité du retour d'expérience et la complexité du monde réel.

L'effet de la maintenance pour les matériels réparables est modélisé, que la maintenance soit corrective, c'est-à-dire exécutée après détection d'une panne et destinée à remettre le matériel réparable dans un état dans lequel il peut accomplir la fonction requise ou que la maintenance soit préventive, c'est-à-dire exécutée à des intervalles prédéterminés ou selon des critères prescrits et destinée à réduire la probabilité de défaillance du matériel.

Il est rappelé que toutes les approches fréquentielles reposent exclusivement sur les données de REX disponibles : la qualité du résultat de l'étude de fiabilité dépend de la qualité des données.

Le recueil de données HUMS (*Health and Usage Monitoring Systems*) de surveillance se fait à l'aide de capteurs toujours plus nombreux avec un échantillonnage dans le temps de plus en plus serré. La masse de données devient telle que les auteurs de cet ouvrage parlent de passage du trop peu au trop-plein et consacrent un chapitre particulier (le chapitre 7) aux méthodes développées pour faire face à l'impact du Big Data sur la fiabilité. De nombreuses questions se posent : il s'agit de collecter les données pertinentes, prétraiter et valider des données massives. Si les techniques de Machine Learning peuvent aider, il n'est pas question de se fier aveuglément à des modèles boîtes noires. Des facteurs influents, insoupçonnés initialement, peuvent être mis en évidence. Mais on n'aura confiance dans les algorithmes du Big Data que si leurs résultats sont explicables et expliqués. Et les auteurs insistent sur le besoin d'un recours aux modèles physiques et aux analyses des facteurs organisationnel et humain.

Lorsque les données sont insuffisantes, des méthodes bayésiennes sont nécessaires en les combinant avec des avis d'experts.

Il est des cas où le REX ne présente aucune défaillance. C'est le cas lorsque l'on étudie un matériel très fiable ou largement dimensionné à la conception.

C'est aussi le cas d'un composant passif non remplaçable comme la cuve d'un réacteur.

L'analyse de fiabilité des structures s'impose alors. C'est l'objet du chapitre 4.

Il y a défaillance d'une structure lorsqu'une sollicitation notée S excède une résistance notée R . La méthode contrainte-résistance permet la comparaison avec un code numérique de mécanique des structures. La sollicitation et la résistance s'expriment par des variables qui sont considérées aléatoires. La probabilité de défaillance est alors déterminée en propageant les incertitudes dans le code de simulation physico-mathématique. Le nombre de calculs par la méthode Monte-Carlo devient prohibitif pour des événements rares et d'autres méthodes sont présentées.

Des essais mécaniques permettent de déterminer les variables de résistance d'un matériau.

Une partie importante de la sûreté nucléaire repose sur l'intégrité de la cuve. La tenue mécanique de cette structure métallique épaisse a donné lieu à des travaux importants sur la mécanique de la rupture, la science de la propagation d'une fissure. L'approche probabiliste du risque de rupture brutale de la cuve consiste à propager les incertitudes dans le modèle de mécanique de la rupture pour divers transitoires thermohydrauliques. La ténacité du matériau, mesure de sa résistance à la propagation d'une fissure, est la première variable considérée comme aléatoire. Les études réalisées par le CEA, EDF et Areva ont conclu qu'une représentation probabiliste de la ténacité peut être donnée par une loi de Weibull à trois paramètres.

J'ouvre une parenthèse personnelle. Jeune ingénieur tout juste sorti de l'école, j'ai découvert la mécanique linéaire élastique de la rupture (LEFM, *Linear Elastic Fracture Mechanics*) et la norme ASTM E399 (*Standard Test Method for Linear-Elastic Plane-Strain Fracture Toughness of Metallic Materials*) de détermination du K_{IC} , le facteur d'intensité de contrainte critique, mesure de la ténacité d'un matériau. J'ai fait partie des chercheurs français qui ont développé en France au milieu des années 1970 la mécanique élastoplastique de la rupture (EPFM, *Elasto Plastic Fracture Mechanics*) pour étendre la mécanique linéaire élastique de la rupture et prendre en compte la plasticité de l'acier de cuve. Et j'ai effectué, avec d'autres, les premiers travaux sur l'intégrale J . Beaucoup plus tard, j'ai eu l'honneur de diriger le département des matériaux pour le nucléaire sur le centre CEA de Saclay. Les travaux sur l'intégrale J avaient débouché entre-temps sur la norme ASTM E813 (*Test Method for J_{IC} , a Measure of Fracture Toughness*).

La fiabilité et la sécurité/sûreté ne s'évaluent pas seulement au moment de la conception et de la réalisation. Elles s'évaluent périodiquement. L'extension de la durée de vie des centrales nucléaires impose d'étudier le vieillissement des matériaux et plus particulièrement les effets de l'irradiation. En effet, celle-ci se traduisant par une baisse

de la ténacité ou, autrement dit, l'augmentation de la fragilité, il faut étudier l'évolution de cette caractéristique au cours du temps au fur et à mesure que les effets d'irradiation se cumulent.

Pour cela, il faut irradier des échantillons dans un réacteur expérimental ou dans un réacteur de production d'électricité. Il faut ensuite mesurer les propriétés des échantillons irradiés dans des « labos chauds », c'est-à-dire des laboratoires équipés de cellules blindées, capables d'accueillir en toute sécurité des matériaux fortement radioactifs, et de télémanipulateurs permettant de procéder aux expérimentations.

Mais la fiabilité et la sécurité/sûreté de systèmes sociotechniques complexes n'est pas que l'affaire des sciences de l'ingénieur. Les sciences humaines et sociales sont mises à contribution. L'accident de Three Mile Island en 1979, intervenu suite à des actions inappropriées des opérateurs, a montré l'importance du facteur humain.

Le chapitre 6 traite des dimensions humaines et organisationnelles de la fiabilité et de la sûreté nucléaire.

La dimension organisationnelle s'est ajoutée car il n'y a pas que l'erreur humaine individuelle, toujours possible, qui doit être prise en compte. L'ensemble de l'organisme doit être examiné car la fiabilité et la sécurité/sûreté dépendent aussi du management qui prend des décisions, rend des arbitrages, alloue des ressources, gère les compétences, organise le retour d'expérience, développe des valeurs et une culture.

La loi TSN, citée précédemment, dit que la sécurité nucléaire comprend la sûreté nucléaire, la radioprotection, la prévention et la lutte contre les actes de malveillance, ainsi que les actions de sécurité civile en cas d'accident.

La sécurité nucléaire comprend donc la sûreté nucléaire, mais y ajoute d'autres considérations comme la lutte contre les actes de malveillance.

Un humain, ami du système, peut commettre une erreur involontaire mais il peut aussi y avoir d'autres humains, ennemis du système, qui peuvent chercher à nuire volontairement au système. La fiabilité et la sécurité/sûreté dépendent aussi des lignes de défense, techniques et organisationnelles, qui auront été prévues contre des attaques malveillantes, physiques ou informatiques.

Le présent ouvrage fait le point sur les études de fiabilité menées dans le domaine de la production nucléaire d'électricité mais certaines démarches et méthodes pourront être appliquées à d'autres secteurs industriels. La société qui a toujours été exigeante avec le nucléaire compte tenu des risques encourus le devient de plus en plus pour

d'autres activités économiques. L'expérience acquise dans le domaine nucléaire pourra utilement inspirer les personnes en charge de la fiabilité, de la sûreté de fonctionnement et de la sécurité de systèmes sociotechniques complexes.

Philippe LE POAC
Président de l'IMdR

Préface d'Antoine Grall

Dans une société attentive aux risques pour les personnes et l'environnement et face à des systèmes de production de plus en plus sophistiqués et soumis à des objectifs d'optimisation et de maîtrise des coûts, la sûreté de fonctionnement prend une place croissante. De nombreux événements non souhaités peuvent, lorsqu'ils sont considérés individuellement, être évalués comme très improbables et sans conséquence forte. Néanmoins, au sein de systèmes complexes, les effets de cumuls et d'interactions peuvent être très importants. Une démarche de sûreté de fonctionnement n'a pas pour ambition de supprimer tout risque, mais de le contrôler. Il s'agit de déterminer et caractériser une conception et un mode de fonctionnement permettant un bon équilibre entre différents critères liés au fonctionnement du système et à son interaction avec l'environnement. La caractérisation précise du « bon » équilibre peut être très variable d'un domaine d'application à l'autre en fonction de l'importance donnée aux aspects économiques, fiabilistes, environnementaux, etc.

L'ouvrage qui nous est proposé s'intéresse spécifiquement aux systèmes de production d'énergie électrique et au domaine du nucléaire. « Fiabilité » et « énergie nucléaire » sont des termes qui cohabitent naturellement. Personne ne peut nier la part importante des progrès qu'ont connus les méthodes et études de sûreté de fonctionnement dans le cadre de travaux menés dans le secteur de la production nucléaire d'électricité. Cet ouvrage coordonné par André Lannoy rassemble exclusivement des contributions d'auteurs ayant des compétences reconnues en fiabilité et une forte expérience dans le domaine du nucléaire. Il montre le large spectre et la complexité des problématiques abordées.

Doit-on considérer qu'il existe une fiabilité spécifique au nucléaire ? Autrement dit, est-il pertinent de se plonger dans la lecture des différents chapitres si l'on est intéressé par la fiabilité en association avec d'autres domaines d'application ? La réponse est à mon sens résolument affirmative. Indépendamment de l'objet étudié, tout

ingénieur en sûreté de fonctionnement dispose du même ensemble de techniques et méthodes auxquelles il peut faire appel. Son travail demande de les exploiter au mieux à partir d'une compréhension fine des mécanismes dysfonctionnels en jeu. Un site de production d'énergie nucléaire représente un système complexe, au sein duquel se côtoient des problématiques diverses, transverses à de nombreux domaines, liées par exemple à l'analyse de composants passifs (structures), de systèmes dynamiques (composants actifs et contrôle-commande), de performance humaine, etc. Il existe dans le domaine de la sûreté nucléaire une exigence d'amélioration continue qui amène à des réexamens périodiques et à une prise en compte de l'évolution des connaissances. Les points d'insistance, les procédures et le cadre réglementaire peuvent être spécifiques mais le fiabiliste amateur aussi bien que confirmé pourra tirer un bénéfice important du partage d'expertise proposé par les auteurs des différents chapitres.

De nombreux aspects sont abordés au fil des pages et les grilles de lecture peuvent être diverses. Les données sont présentes à toutes les étapes des études de fiabilité. Qu'elles proviennent d'essais accélérés, d'expertises de retours d'expérience ou d'instruments de captation en temps réel, leur exploitation est primordiale. Trois chapitres leur sont plus particulièrement associés. Le chapitre 2 apporte un point de vue général sur le retour d'expérience et les concepts associés, en mettant en avant les retours d'expérience événementiel et matériel. Le chapitre 5 donne au lecteur une vision globale des principaux cadres de modélisation stochastique basés sur les données et exploités en fiabilité. Ils ont pour objet de décrire le comportement de sous-systèmes ou composants spécifiques et sont en pratique choisis, ajustés et validés par confrontation avec les données observées. Enfin, le chapitre 7 est orienté vers une problématique d'actualité qui est celle de la disponibilité de masses de données de surveillance. Cette nouvelle configuration est rendue possible en particulier grâce aux dispositifs de surveillance modernes. Elle constitue un défi particulier pour le domaine de la fiabilité qui est historiquement confronté à une faible quantité de données.

Les données de surveillance et de retour d'expérience ne constituent bien évidemment pas la seule source d'information disponible sur l'état et le comportement d'un système ou d'un composant. En ce qui concerne en particulier les composants passifs, des modèles de comportement physiques ou mécaniques sont disponibles. Les analyses de fiabilité des structures représentent un exemple particulièrement intéressant d'association entre ces modèles de comportement déterministes et les incertitudes sur les variables. Le cadre méthodologique est présenté dans le chapitre 4 et mis en application sur des exemples.

Un système de production d'énergie électrique basé sur l'énergie nucléaire est un système complexe et deux chapitres s'intéressent à deux aspects particuliers de cette complexité. Le premier aspect traite des Évaluations Probabilistes de Sûreté. Ces

études englobent des modèles de très grande taille associant arbres de défaillance et arbres d'événements. Étant donné le grand nombre de composants en interaction, la problématique combinatoire est très présente. Dans ce contexte, il est particulièrement intéressant de comprendre comment se fait la mise en pratique. Des approches plus récentes sont également présentées. Le second aspect de la complexité évoquée est porté par les dimensions humaines et organisationnelles qui nécessitent une vision globale et systémique. Elles mobilisent particulièrement des compétences du champ des sciences humaines et sociales et montrent combien la fiabilité a vocation à être un champ d'interdisciplinarité. La problématique de fiabilisation des activités humaines est discutée sous différents aspects.

Pour conclure, je voudrais insister sur l'intérêt de cet ouvrage pour toute personne intéressée par le domaine de la fiabilité. En tant qu'enseignant à de futurs ingénieurs, je ne pourrais que recommander sa lecture aux étudiants. Cette lecture peut permettre aussi bien d'acquérir une vision large sur de nombreux aspects de la fiabilité que de compléter très avantageusement les initiations essentiellement théoriques que l'on peut suivre dans un cadre académique. À travers des présentations claires et précises, l'ouvrage porte la dimension de l'applicabilité sur des systèmes réels de méthodes qui sont souvent présentées avec des exemples simples illustratifs.

En tant que chercheur qui se soucie de l'applicabilité de ses travaux, il me semble intéressant d'être attentif aux points de vue développés et aux pistes de R&D évoquées par les différents auteurs. Elles sont liées à des verrous méthodologiques qu'il faudra réussir à lever et donnent des indications précises quant aux hypothèses présentes dans les cadres théoriques existants qui sont les plus contraignantes.

Antoine GRALL
Professeur des universités, Université de technologie de Troyes,
directeur adjoint de l'école doctorale Sciences pour l'ingénieur

Avant-propos

Les auteurs de cet ouvrage collectif veulent rendre hommage à Henri Procaccia, ancien ingénieur chercheur expert, ancien chef de groupe et ancien chef adjoint de département à EDF R&D, cofondateur, membre d'honneur et membre du comité directeur de l'association ESReDA (European Safety, Reliability & Data Association), membre de l'association IMdR (Institut pour la Maîtrise des Risques), pour son rôle de précurseur dans le domaine de la fiabilité dans le nucléaire.

Henri Procaccia compte parmi les acteurs actifs de la fiabilité et on lui doit de nombreux travaux traitant cette matière de manière approfondie. Dès le début des années 1970, bien avant le couplage du premier réacteur à eau sous pression (de technologie américaine) en France à Fessenheim, Henri Procaccia travaille sur la fiabilité des systèmes et sur la structuration du retour d'expérience, pour les réacteurs à eau sous pression et pour les réacteurs à neutrons rapides.

Dans les années 1980, le faible nombre de données de retour d'expérience issues de centrales encore jeunes l'a fait adhérer à la démarche bayésienne dont il fait la promotion par l'enseignement et l'application. Il est à l'origine du premier recueil de données de fiabilité, le SRDF (Système de Recueil de Données de Fiabilité). À la fin des années 1980, sur la base de ses compétences dans les essais physiques, il convainc EDF de se lancer dans l'analyse de la fiabilité des structures et dans la surveillance en fatigue.

Dans les années 1990, son champ d'investigation concerne surtout l'optimisation de la maintenance et l'aide à la décision. Dans tous ces thèmes, la fiabilité apparaît comme un paramètre essentiel. Les auteurs savent gré à Henri Procaccia d'avoir ainsi favorisé le développement des méthodes de fiabilité, leur application et leur utilisation. Il était également animé d'une profonde humanité.