

The logo for IRSN, featuring the letters 'IRSN' in a bold, sans-serif font. The 'I', 'R', and 'S' are red, while the 'N' is blue.

INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

LE POINT DE VUE DE L'IRSN SUR LA SURETE ET LA RADIOPROTECTION DU PARC ELECTRONUCLEAIRE FRANÇAIS EN 2008

RAPPORT DSR N° 316

DIRECTION DE LA SURETE DES REACTEURS

SOMMAIRE

INTRODUCTION ET SYNTHÈSE	2
EVALUATION GLOBALE DE LA SÛRETÉ DU PARC EN EXPLOITATION	4
LES TENDANCES DE 2008 SOULIGNÉES PAR L'IRSN	5
ÉVÉNEMENTS ET INCIDENTS	13
DÉLICATE OPÉRATION DE DÉCHARGEMENT DE COMBUSTIBLE À LA CENTRALE DU TRICASTIN	14
INDISPONIBILITÉ PARTIELLE D'UNE FONCTION DE SAUVEGARDE	18
LES ÉVÉNEMENTS CONCERNANT LA RADIOPROTECTION	21
ENVASEMENT DU RU D'EAU ARRIÈRE DE LA STATION DE POMPAGE DE LA CENTRALE DE FESSENHEIM ..	25
ANOMALIES GÉNÉRIQUES CONCERNANT LE PARC.....	29
FISSURATION PAR FATIGUE DES TUBES DE GÉNÉRATEURS DE VAPEUR.....	30
CORROSION DES MATÉRIELS SITUÉS EN BORD DE MER ; LES GROUPES ÉLECTROGÈNES DE SECOURS ..	36
LES RISQUES LIÉS À L'UTILISATION DE L'HYDROGÈNE	40
INTRODUCTION D'UN NOUVEAU MATÉRIAU DE GAINAGE DU COMBUSTIBLE.....	44
TEMPÉRATURE AMBIANTE ÉLEVÉE POUR LES POMPES D'INJECTION DE SÛRETÉ.....	48
DÉGRADATIONS DES SUPPORTS DE CERTAINES CANALISATIONS IMPORTANTES POUR LA SÛRETÉ.....	51
LES ÉVOLUTIONS SIGNIFICATIVES.....	54
L'INCIDENCE DES PÉRIODES DE CANICULE SUR LA SÛRETÉ DES CENTRALES.....	55
LA POLITIQUE DE MAINTENANCE D'EDF	58
LE MANAGEMENT DE LA SÛRETÉ DANS UN CONTEXTE DE COMPÉTITIVITÉ.....	61
MODIFICATIONS DES LOGICIELS DU SYSTÈME DE PROTECTION DU RÉACTEUR.....	65
DÉFINITIONS ET ABRÉVIATIONS	69
CRÉDIT PHOTO	70

Les mots écrits en [bleu et soulignés](#) renvoient à des liens. Ces liens sont actifs sur www.irsn.org.

Les liens qui renvoient au rapport annuel de l'IRSN « Le point de vue de l'IRSN sur la sûreté et la radioprotection du parc électronucléaire français en 2007 » sont activés par le terme « [rapport IRSN](#) » dans le texte.

LES EVOLUTIONS SIGNIFICATIVES

Des avancées dans l'état des connaissances techniques et scientifiques, des faiblesses identifiées ou des leçons tirées du retour d'expérience, un environnement ou une réglementation qui évoluent, des impératifs économiques... autant de raisons qui conduisent à faire évoluer les installations ou leurs modalités d'exploitation. Les réexamens de sûreté, réalisés par les exploitants tous les 10 ans, sont l'un des cadres essentiels pour la mise en œuvre de telles évolutions. En effet, les évolutions ou modifications les plus importantes nécessitent plusieurs années de réflexions et d'études avant leur définition précise et leur mise en place. L'IRSN analyse ces évolutions ou modifications à différents stades. Durant l'année 2008, plusieurs sujets de ce type ont été examinés par l'IRSN ; parmi lesquels ceux exposés dans ce chapitre.

Bien que les centrales nucléaires d'EDF soient conçues pour supporter des températures élevées de l'air et de l'eau, les événements caniculaires de 2003 et 2006 ont montré la nécessité, dans un contexte de réchauffement climatique, de renforcer la protection des centrales à l'égard des risques de canicule. EDF a lancé un plan d'actions à court, moyen et long termes dont l'IRSN analyse les développements depuis 2003.

Réaliser une maintenance efficace pour la sûreté, tout en limitant les coûts, y compris « radiologique » ; cet objectif d'optimisation de la maintenance conduit EDF à définir des évolutions significatives de l'organisation et des méthodes qui la régissent, dont l'incidence sur la sûreté a fait l'objet d'une évaluation par l'IRSN.

Réduire les coûts de production sans compromettre la sûreté des installations est l'objectif affiché d'EDF depuis plusieurs années. Toutefois, l'accroissement des pressions productives est une des manifestations de la recherche de compétitivité. Si ce n'est pas contrebalancé par des mesures managériales et organisationnelles visant le maintien d'un haut niveau de sûreté, cela peut conduire à des dérives propres à favoriser l'occurrence d'un accident. Ce sujet a fait l'objet d'une évaluation spécifique de l'IRSN.

Les changements de gestion de combustible et les évolutions destinées à améliorer la sûreté nécessitent des modifications des logiciels du système de protection du réacteur, dont la fiabilité doit être évaluée. Compte tenu de leur nombre important et de leur complexité, l'IRSN a développé une méthode d'évaluation des logiciels de sûreté critiques (à temps de réponse garanti), en utilisant directement les résultats qu'il a acquis par des recherches et développements propres.

L'incidence des périodes de canicule sur la sûreté des centrales

Les centrales nucléaires d'EDF ont été conçues pour supporter les températures élevées de l'air et de l'eau susceptibles de survenir localement. Toutefois, à la suite des événements caniculaires de 2003 et 2006, il est apparu nécessaire de renforcer la protection de ces centrales à l'égard du risque d'une canicule dans un contexte de réchauffement climatique. EDF a ainsi lancé un plan d'actions à court, moyen et long termes dont l'IRSN analyse les développements depuis 2003. Des étapes importantes dans l'analyse ont été franchies en 2007 et 2008.

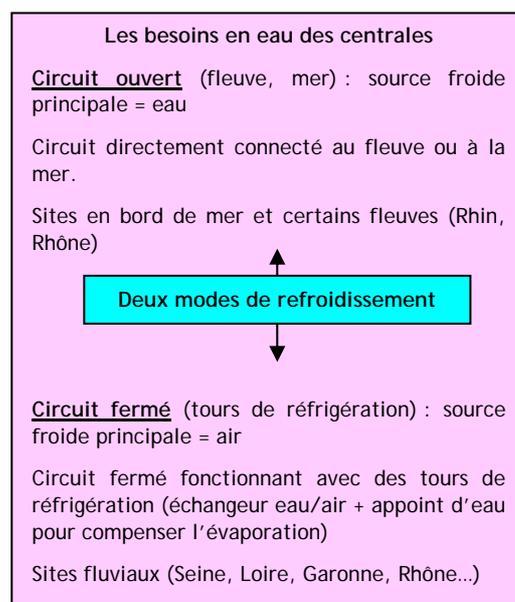
Les besoins en refroidissement des centrales nucléaires

Les centrales nucléaires ont besoin d'une source de refroidissement pour pouvoir produire de l'électricité tout en garantissant la sûreté. Cette source de refroidissement est constituée, selon les sites et les équipements de la centrale, par l'air ou par l'eau de la mer ou d'une rivière (source froide). Le refroidissement doit, pour l'air, assurer le bon fonctionnement des matériels quelle que soit la température de l'air extérieur, pour l'eau assurer la performance des systèmes utilisant la source froide pour refroidir différents équipements. Aussi, des températures élevées de l'eau ou de l'air sont susceptibles d'affecter le fonctionnement et la sûreté des centrales nucléaires.

L'impact de l'épisode caniculaire de 2003 sur les sources de refroidissement des centrales

Les centrales nucléaires ont été conçues pour supporter des températures élevées - dites « températures de dimensionnement » - de l'air et de l'eau, définies pour la plupart dans les années 1970. En outre, le fonctionnement des réacteurs nucléaires s'inscrit dans les limites de températures de l'eau, et de l'air dans les locaux, prescrites dans les règles générales d'exploitation (RGE) et les arrêtés d'autorisation de rejets d'effluents et de prélèvements d'eau, qui imposent des dispositions particulières d'exploitation en cas de dépassement.

La canicule de l'été 2003 a constitué un événement climatique majeur, par son ampleur géographique, sa durée et les niveaux de température observés. Au cours de cet épisode caniculaire, les températures de dimensionnement retenues à la conception des centrales ont parfois été dépassées, contraignant EDF à réduire la production de certains réacteurs pour respecter les règles générales d'exploitation et les arrêtés d'autorisation de rejets.



Lancement par EDF d'un plan d'actions « grands chauds » et son analyse par l'IRSN

Après l'été 2003, afin de garantir le bon fonctionnement des réacteurs en cas de températures élevées de l'air ou de l'eau, dans le respect des principes de sûreté, EDF a lancé un vaste plan d'actions.

A court terme, des modifications temporaires des RGE ont été proposées annuellement par les centrales et analysées par l'IRSN en prévision des étés 2004 à 2008. Elles portent, d'une part sur les conditions de fonctionnement des systèmes de ventilation, d'autre part sur la surveillance des matériels de la source froide. En complément, EDF a élaboré des règles particulières d'exploitation en période de canicule en renforçant la surveillance des matériels sensibles à la chaleur et en prescrivant des règles de conduite et, si nécessaire, la mise en place de moyens mobiles temporaires de refroidissement.

Pour le plus long terme, EDF a en avril 2006, transmis à l'ASN une démarche de protection des centrales nucléaires contre les risques associés à une canicule. Il s'agit d'un dossier « grands chauds » et de notes d'études destinées entre autres à préciser les méthodes à suivre pour réévaluer les températures maximales de l'air et de l'eau auxquelles les installations devront faire face. Dans ce dossier, EDF affiche l'objectif de construire un référentiel valable pour les trente prochaines années. Pour cela, EDF vise à déterminer des températures « extrêmes » de l'air et de la source froide, en tenant compte des effets du réchauffement climatique au cours de cette période. Ces températures seront ensuite utilisées pour les études de vérification de la tenue et des performances des différents systèmes et des équipements associés.

En 2006 et 2007, l'IRSN a examiné la démarche décrite dans le dossier « grands chauds » pour les réacteurs de 900 MWe qui se sont avérés les plus sensibles aux températures élevées. Après examen, l'IRSN a estimé que la démarche proposée par EDF est globalement satisfaisante. Toutefois, l'analyse du dossier « grands chauds » devait être poursuivie par l'analyse des notes d'études.

Aussi, dans le courant de 2008, une analyse complémentaire a été menée par l'IRSN, d'une part sur la détermination des températures de l'air et de l'eau à retenir pour les différentes centrales du parc nucléaire d'EDF, d'autre part sur les situations de fonctionnement enveloppes retenues par EDF pour mener les études relatives aux centrales du palier 900 MWe.

Après examen, l'IRSN considère que l'application de la démarche retenue conduira à une amélioration de la sûreté des réacteurs lors de températures élevées. L'IRSN a cependant souligné certaines insuffisances du dossier EDF, portant sur l'exhaustivité des situations accidentelles à considérer aux températures élevées et sur la détermination des températures retenues pour mener les études de vérification thermique. Sur ce point, l'IRSN a souligné que les températures « extrêmes » de l'air et de l'eau, déterminée selon la démarche prévue, devront être révisées en cohérence avec les évolutions des connaissances scientifiques, des méthodes et des données disponibles. A ce titre, une veille climatique est mise en œuvre par EDF.

Des actions d'amélioration réalisées et à venir

La mise en œuvre du dossier « grands chauds » implique de réaliser des modifications matérielles et documentaires dans les centrales. D'ores et déjà, les études d'EDF ont conduit à réaliser ou à prévoir la réalisation de modifications telles que par exemple :

- le remplacement des groupes de réfrigération pour augmenter leurs performances,
- l'ajout de climatiseurs,
- l'augmentation des performances des échangeurs thermiques importants pour la sûreté,
- des modifications de certains matériels pour garantir leur tenue à des températures supérieures à celles retenues lors de la conception initiale des centrales.

L'objectif visé par EDF est la mise en place de l'ensemble des modifications sur un premier réacteur de 900 MWe à l'horizon de 2011. Dans l'attente de l'implantation de cet ensemble de modifications « grands chauds », des dispositions transitoires ainsi que certaines modifications sont mises en œuvre à plus court terme. Ces actions permettent d'améliorer la protection des réacteurs du parc en exploitation à l'égard des risques d'une canicule analogue à celle observée en 2003.

A long terme, les modifications associées au nouveau dossier « grands chauds » seront mises en place sur l'ensemble du parc électronucléaire français, pour renforcer la protection des réacteurs du parc en exploitation à l'égard du risque de températures extrêmes, en tenant compte de l'évolution climatique, envisageable à l'horizon 2030.



Groupe de réfrigération



Echangeur thermique eau/eau

LA POLITIQUE DE MAINTENANCE D'EDF

A la demande de l'ASN, L'IRSN a procédé à un examen approfondi de la politique de maintenance d'EDF et de sa mise en œuvre par les centrales afin d'évaluer l'incidence, sur la sûreté des réacteurs, des évolutions d'organisation et de méthodes mises en œuvre par EDF pour optimiser la maintenance. Les conclusions de cet examen ont été présentées au groupe permanent d'experts pour les réacteurs nucléaires lors d'une réunion tenue en mars 2008.

L'IRSN a organisé son évaluation selon deux axes. Le premier axe, essentiellement technique, concernait les méthodes de maintenance, le processus de capitalisation du retour d'expérience et l'analyse du retour d'expérience concernant certains matériels importants pour la sûreté. Le deuxième axe, relatif aux aspects organisationnels et humains, a traité des processus de gestion des compétences, de préparation et de surveillance des opérations de maintenance.

Des méthodes de maintenance qui privilégient la surveillance

L'Optimisation de la Maintenance par la Fiabilité (OMF) est une méthode fondée sur une analyse fonctionnelle qui permet de faire des choix concernant la maintenance des matériels en fonction de la gravité de leurs modes de défaillance pour la sûreté et la disponibilité des réacteurs en exploitation et en fonction du retour d'expérience.

La maintenance conditionnelle permet de limiter les opérations lourdes de maintenance intrusives en les subordonnant à une évolution anormale des valeurs de certains paramètres de fonctionnement ou au constat d'une dégradation.

La maintenance par matériels témoins permet de limiter les opérations lourdes de maintenance intrusives à certains matériels d'une même famille technologique dont l'état de santé est réputé représentatif de celui de la famille.

EDF a développé plusieurs méthodes de maintenance (OMF, maintenance conditionnelle, maintenance par matériels témoins) en vue d'optimiser les activités correspondantes. Il s'agit pour EDF de faire une maintenance efficace au plan de la sûreté en limitant les interventions de maintenance coûteuses, y compris en termes radiologiques.

L'IRSN a examiné ces méthodes afin de déterminer si les évolutions de maintenance qui pourraient en découler ne risquent pas de conduire à une dégradation de la sûreté des installations.

Au terme de son analyse, l'IRSN estime que les méthodes précitées, qui privilégient la surveillance des matériels aux opérations de maintenance intrusives

présentent de l'intérêt. Il estime en particulier que l'application de ces méthodes devraient permettre, dans certains cas de limiter les dégradations de matériels qui pourraient résulter des démontages et de limiter les doses de rayonnement reçues par les intervenants lors de ces opérations. Par contre, ces méthodes induisent un risque nouveau qui est celui de ne pas détecter des défauts non prévisibles qui auraient pu être découverts par des examens plus approfondis lors des démontages de matériels. Dans ces conditions, pour les matériels importants pour la sûreté faisant l'objet d'une telle maintenance, l'IRSN estime donc indispensable le maintien de visites complètes, à une périodicité adaptée ; EDF en a accepté ce principe.

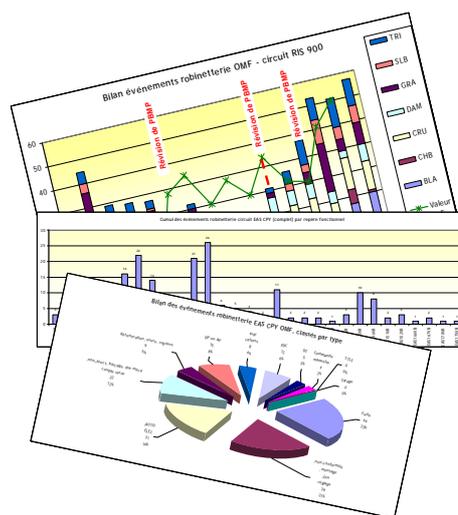
Un processus de capitalisation du retour d'expérience à compléter

Les effets d'une évolution des pratiques de maintenance sur la fiabilité des équipements ne sont pas immédiats. Ils n'apparaissent généralement que quelques années plus tard, d'où la nécessité d'effectuer une analyse fine du comportement des matériels sur la durée. Bien qu'EDF utilise des outils visant à capitaliser le retour d'expérience, l'IRSN n'est pas en mesure de confirmer que leur efficacité est suffisante pour détecter des signaux faibles précurseurs de défaillances. En effet, tant au plan local qu'au plan national, EDF n'a pas mis en place d'outil spécifique permettant d'évaluer l'adéquation des opérations de maintenance réalisées. Les indicateurs généralement utilisés (nombre d'évènements ou nombre d'indisponibilités de matériels importants pour la sûreté...) n'apportent pas suffisamment d'informations pour pouvoir être exploités en termes de maintenance. L'IRSN a donc estimé indispensable qu'EDF complète son processus actuel par un ensemble d'indicateurs permettant d'évaluer périodiquement l'efficacité de la maintenance.

Des programmes de maintenance qui peuvent être améliorés

L'IRSN a spécifiquement analysé le retour d'expérience pour un ensemble d'échantillons de matériels faisant l'objet de différentes méthodes de maintenance (OMF ou non, maintenance conditionnelle, maintenance par matériels témoins). L'IRSN a examiné plus de 20 000 évènements parmi ceux enregistrés dans la base de données du Système EDF d'Analyse Par l'Historisation pour le Retour d'expérience (SAPHIR). Les questions résultant des observations et des analyses de l'IRSN ont conduit EDF à améliorer dans certains cas les programmes de maintenance, par exemple en augmentant la fréquence de certaines visites périodiques.

En complément des évolutions des méthodes, la nouvelle politique de maintenance d'EDF nécessite des modifications de l'organisation du travail. Ceci a conduit l'IRSN à examiner le maintien des compétences de maintenance ainsi que les modalités de contrôle et de surveillance de la qualité des opérations correspondantes.



Un dispositif de gestion des compétences globalement robuste

EDF a fait évoluer sa politique industrielle d'achat (en termes de matériels et de prestations) afin de bénéficier d'un « effet de volume » et de contribuer au maintien des compétences des prestataires. Cette politique conduit à de nouvelles relations entre EDF et ses prestataires et à une transformation des métiers de la maintenance. Pour accompagner ces changements, EDF comme ses sous-traitants ont dû faire évoluer la gestion de leurs compétences. En 2008, l'IRSN a examiné le dispositif de gestion des compétences en cours de déploiement dans les services de maintenance des centrales d'EDF. Ce dispositif comprend un ensemble d'outils comme « les prospectives métiers » et « les cartographies de compétences ». Les dispositions prises par EDF apparaissent globalement robustes ; elles permettent à chaque centrale d'identifier, par domaine d'activité, les compétences disponibles mais également de prévoir des plans de professionnalisation et de recrutement. EDF développe également des démarches permettant l'évaluation des compétences des entreprises prestataires en préalable aux passations de marché et à l'issue des prestations. Parallèlement, EDF met en place des partenariats avec les entreprises prestataires afin de mieux structurer les parcours de formation de leur personnel. L'IRSN estime que

dans leur principe ces initiatives sont positives, mais qu'une évaluation de leurs effets sur les systèmes de gestion des compétences mis en place par les entreprises prestataires doit être menée sur le terrain. Les inspections conduites par l'ASN dans ces entreprises permettront d'apprécier la situation à moyen terme de l'externalisation des activités de maintenance.

Les métiers de la préparation en pleine évolution



Intervention de maintenance sur un groupe électrogène à moteur diesel

Dans le contexte du recours à la sous-traitance, la préparation des interventions de maintenance est un élément clé de la sûreté, et notamment lors des arrêts pour maintenance des réacteurs. La préparation permet également d'établir les bases du programme de surveillance à mettre en œuvre en phase de réalisation. Or, les évolutions de la politique de maintenance d'EDF s'accompagnent d'une mutation des métiers de la préparation qui se traduit entre autres par un élargissement des compétences mises en œuvre. Ainsi, au-delà des tâches techniques traditionnelles, les préparateurs assurent désormais aussi des missions relevant de la gestion de projet (coordination de travaux, négociation avec les prestataires etc.). Pour l'IRSN, EDF doit veiller à ce que, malgré les contraintes nouvelles auxquelles sont soumises les activités des préparateurs, ceux-ci puissent exercer sereinement les tâches nécessitant réflexion et allier un travail de fond aux sollicitations en temps réel dont ils font l'objet.

Des ressources à la hauteur des ambitions en matière de surveillance ?

La surveillance des opérations de maintenance sous-traitées, dont la majeure partie est réalisée sur le terrain, contribue à prévenir et détecter des écarts des prestataires. Toutefois, l'examen réalisé en 2008 par l'IRSN dans plusieurs centrales, a montré qu'EDF éprouve certaines difficultés à justifier que les effectifs affectés à la surveillance sont suffisants pour réaliser les actions prévues. EDF a ainsi été amené à préciser l'organisation mise en place pour assurer la compatibilité entre les ressources affectées à la surveillance et le contenu technique des programmes de surveillance.

Le management de la sûreté dans un contexte de compétitivité

Au cours des dernières années, le marché de l'électricité s'est progressivement ouvert à la concurrence. En prenant le statut de « société anonyme » et en devenant un acteur industriel dans un marché concurrentiel, EDF se trouve désormais davantage confronté à la question de sa compétitivité. Optimiser les coûts de production sans compromettre la sûreté des installations est un objectif affiché d'EDF.

La recherche de la compétitivité rend nécessaire le renforcement du management de la sûreté

Manager la sûreté c'est mettre en place et faire vivre dans le temps les dispositions techniques, organisationnelles et humaines qui permettent une maîtrise satisfaisante des risques.

L'accroissement des pressions liées à la production est une des manifestations associées à la recherche de la recherche de compétitivité. S'il n'est pas contrebalancé par des dispositions managériales et organisationnelles dédiées au maintien d'un haut niveau de sûreté, il peut conduire à des dérives propres à favoriser l'occurrence d'un accident. La pression liée à la production a été un des facteurs à l'origine de L'accident de criticité de l'usine de Tokai Mura (Japon - 1999), de la collision ferroviaire de Paddington (Grande Bretagne - 1999), de la corrosion du couvercle de cuve à la centrale nucléaire de Davis Besse (États-Unis - 2002) ou de l'explosion en vol de la navette Columbia (États-Unis - 2003)

Toutefois, l'évocation de ces accidents ne doit pas laisser penser qu'il existe une relation systématique et déterministe entre la recherche de la compétitivité et une « catastrophe ». Si la recherche de la compétitivité complique de manière certaine et évidente le management de la sûreté, elle ne le rend pourtant pas impossible.

Le système de management de la sûreté et les leviers de compétitivité mis en œuvre par EDF

EDF a fait évoluer progressivement son système de management de la sûreté du parc nucléaire. Initialement tourné vers des dispositions relevant des démarches « d'assurance de la qualité », EDF a ensuite développé des « outils organisationnels » destinés à l'identification et à la gestion des risques, puis a complété son dispositif en mettant en œuvre les principes du « management par la qualité ». Renforçant les liens entre management de la sûreté et facteurs humains, EDF déploie depuis fin 2006 sur l'ensemble de ses sites des pratiques de « performance humaine » dont les effets sont, en 2008, encore difficilement appréciables. Ces pratiques comprennent deux volets centrés respectivement sur les intervenants de premier niveau et sur leurs managers ; elles visent :

- la fiabilisation des interventions par la mise en œuvre de pratiques « standards » telles que le *pré-job briefing*, la *minute d'arrêt*, le recours à un contrôle spécifique (*autocontrôle ou contrôle croisé*), la *communication sécurisée*, le *débriefing*,

- L'amélioration de la connaissance des conditions réelles d'intervention par un renforcement de la présence des managers sur le terrain.

En complément, différents projets ont été lancés par EDF au cours des 10 dernières années en vue de renforcer certains axes du management de la sûreté ; notamment des projets relatifs à la gestion des compétences, au suivi des prestataires, à la maîtrise des risques d'incendie ou à la diminution du nombre d'arrêts automatiques intempestifs des réacteurs.

Parallèlement des mesures destinées à augmenter la compétitivité ont été mises en place par EDF. Les principales concernent l'optimisation des programmes de maintenance et la réduction des opérations de maintenance, la réduction des durées des arrêts périodiques des réacteurs, l'allongement des cycles permettant la diminution de la fréquence de rechargement du combustible, la rationalisation des politiques d'achat de prestations et des pratiques de contractualisation, les démarches d'optimisation des coûts et des effectifs.

A la demande de l'ASN, l'IRSN a évalué le système de management de la sûreté d'EDF entre octobre 2006 et octobre 2007. Cette évaluation a essentiellement reposé sur des entretiens avec des salariés d'EDF et des observations de situations de travail (près de 150 entretiens et environ 70 demi-journées d'observation dans les entités nationales ainsi que dans 10 centrales).

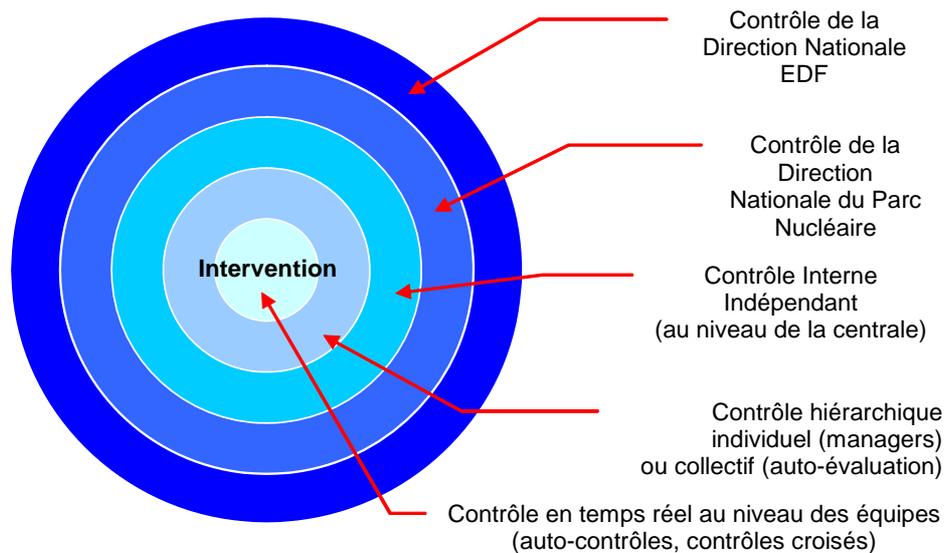
Le 24 avril 2008, l'IRSN a présenté ses conclusions au groupe permanent d'experts pour les réacteurs nucléaires. L'évaluation réalisée par l'IRSN a permis de mettre en évidence plusieurs points forts du management de la sûreté mis en place par EDF, mais aussi plusieurs points qui nécessitent vigilance.

Les atouts du système de management de la sûreté d'EDF

Le premier constat fait par l'IRSN est la réelle dynamique développée par EDF autour des questions de sûreté, tant au niveau national qu'au sein des centrales nucléaires. La sûreté est encadrée, pilotée, contrôlée, mesurée, placée au cœur des performances du parc, et ce dans différentes instances, à différents niveaux hiérarchiques et au plus près du terrain, par des dispositifs formels ou informels. La dynamique managériale créatrice de ce « mouvement autour de la sûreté » contribue à l'entretien et au développement de la « *culture de sûreté* ».

Un autre point fort réside dans l'engagement personnel et collectif du personnel EDF sur les questions touchant à la sûreté. Au-delà des dispositifs techniques ou organisationnels mis en place comme lignes de défense, la maîtrise de la sûreté du parc nucléaire français passe *in fine* par les hommes et les femmes, salariés d'EDF ou prestataires, qui interviennent quotidiennement dans les installations. Malgré l'expression de difficultés, de préoccupations, voire d'inquiétudes ou de lassitude, aucun des propos recueillis par l'IRSN au cours de son évaluation ne révèle de l'indifférence à l'égard des questions de sûreté. Tous se sentent au moins concernés par la sûreté, la plupart sont impliqués à des degrés divers dans son management.

Par ailleurs, le système de contrôle est un maillon important du management de la sûreté. La structure « multicouches » du système de contrôle développé par EDF permet à ce système de jouer son rôle dans la détection des fragilités organisationnelles de l'exploitation des installations.



Le système de contrôles multicouches mis en place par EDF

L'analyse réalisée par l'IRSN montre également les capacités d'EDF à s'organiser en « mode projet ». Ainsi, s'agissant de la gestion des arrêts des réacteurs pour les opérations de maintenance et de rechargement de combustible ou de l'organisation de l'appui technique national pour résoudre des problèmes techniques, le fonctionnement en « mode projet » agit comme un outil de « décloisonnement » d'une grande efficacité et permet de planifier et d'optimiser le travail dans les installations.

Enfin, la multiplicité des regards, amenant une diversité de points de vue dans les processus de décision, est un facteur de performance des organisations de haute fiabilité. Les observations de l'IRSN mettent en évidence des situations dans lesquelles la multiplicité des regards est institutionnalisée et planifiée (réunions formelles rythmant l'arrêt de tranche, par exemple) ou s'organise en temps réel en tant que de besoin. Cette caractéristique du fonctionnement des organisations d'EDF favorise la prise de recul permettant aux individus de s'abstraire des pressions du terrain dans lesquelles ils sont la plupart du temps plongés.

Des sujets nécessitent de la vigilance dans les années à venir

L'évaluation de l'IRSN a également mis en évidence certaines vulnérabilités qui devront faire l'objet d'une attention particulière dans les années à venir.

La première de ces vulnérabilités est la complexité des règles auxquelles sont subordonnées les activités des intervenants dans les installations. La question des règles et des prescriptions techniques ou organisationnelles est apparue de manière récurrente, et souvent ressentie comme facteur de difficultés, lors des différentes observations réalisées par l'IRSN dans les centrales EDF. Les règles ont été conçues pour encadrer et faciliter l'exploitation d'un système technique complexe, mais leur sens est parfois perdu et elles sont actuellement sujettes à des interprétations ou à des dérives bureaucratiques lors de leur utilisation. Elles sont difficilement maîtrisables dans leur ensemble et consommatrices de ressources pour leur mise à jour. La multiplication des contraintes et la recherche de performance toujours accrues conduisent à préciser de plus en plus finement les limites de ce qui est autorisé et de ce qui est interdit. L'ensemble des règles applicables au sein d'une centrale nucléaire constitue un système tentaculaire qui assure de plus en plus difficilement sa fonction première de ligne de défense.

La dynamique managériale mentionné plus haut a cependant pour conséquence négative de multiplier les démarches, les dispositifs, les actions et les projets ; et d'induire un effet d'accumulation pour les salariés. Bien que difficile à caractériser, cet effet d'empilement cristallise nombre de frustrations sur le terrain (« *je n'ai plus le temps de faire mon métier...* »). De plus, le déploiement de ces démarches n'est que trop rarement précédé d'une analyse préalable des conséquences induites alors que certaines d'entre elles ont un impact non négligeable sur l'organisation en place (gestion des pièces de rechange, démarches d'optimisation des coûts et des effectifs). Leur accompagnement n'est pas toujours optimal et la charge de travail liée à leur mise en place n'est pas toujours anticipée. Les causes des difficultés rencontrées au cours de cette mise en place ne sont pas suffisamment prises en compte.

Aussi, le retour d'expérience (REX) « organisationnel » (traitement des dysfonctionnements ou écarts organisationnels) apparaît problématique. C'est le cas notamment lors des arrêts périodiques des réacteurs pendant lesquels la constitution du REX organisationnel « au fil de l'eau » semble mal s'accommoder de la multiplicité des activités. Certains dispositifs dédiés à l'analyse *a posteriori* de décisions délicates ont du mal à produire les résultats escomptés. Par ailleurs, le personnel des centrales a parfois fait état de difficultés pour tenir compte des enseignements du retour d'expérience, compte tenu du fait que les destinataires de ces enseignements ne sont pas toujours bien identifiés.

Concernant le contrôle hiérarchique et le contrôle exercé par « la filière indépendante de sûreté » au sein des centrales nucléaires, il existe aussi des difficultés de positionnement des acteurs qui semblent bien identifiées et prises en compte par EDF. Par ailleurs, l'analyse de l'IRSN caractérise clairement des possibilités de défaillances des contrôles internes. La légitimité d'action des services sûreté/qualité associée aux orientations fixées par la direction de la centrale, la capacité collective d'auto-interrogation et de traitement des alertes, la compétence des intervenants en matière d'analyse de sûreté, apparaissent comme des points de vulnérabilité. Les actions engagées au niveau national sur ces sujets témoignent de la prise de conscience de ces fragilités. L'efficacité de ces actions, trop récentes pour avoir été analysées, fera l'objet d'une attention particulière de l'IRSN dans les années à venir.

Un besoin de « respiration »

L'amélioration continue recherchée ne doit pas induire un « mouvement perpétuel ». Celui-ci peut en effet être déstabilisant pour les acteurs du terrain qui sont loin des décisions à l'origine de ce mouvement et qui ont peu d'éléments pour en comprendre les tenants et les aboutissants. Pour l'IRSN, le renforcement de la robustesse du système de management de la sûreté d'EDF nécessite l'introduction de « temps de respiration » ; ceux-ci devraient être mis à profit pour renforcer les lignes de défense organisationnelles qui auraient été affaiblies et clarifier la manière dont les exigences de sûreté et de compétitivité doivent être conjointement gérées. La force du système de management de la sûreté d'EDF est qu'il est porté, sur le terrain, par des hommes et des femmes qui sont capables de comprendre, d'innover, voire de s'opposer à certaines décisions. Pour l'IRSN, cette force doit être entretenue.

Modifications des logiciels du système de protection du réacteur

Les changements de gestion du combustible et les évolutions destinées à améliorer la sûreté nécessitent des modifications des logiciels du système de protection du réacteur. Comme toute modification d'un matériel ou d'un logiciel participant à une fonction de sûreté, ces modifications font l'objet d'une autorisation par l'Autorité de Sûreté Nucléaire. Compte tenu du nombre important de celles-ci et de leur complexité, l'IRSN a développé une méthode d'évaluation des logiciels de sûreté critiques « temps réels » (à temps de réponse garanti), utilisant directement les résultats qu'il a acquis par ses propres recherches et développements.

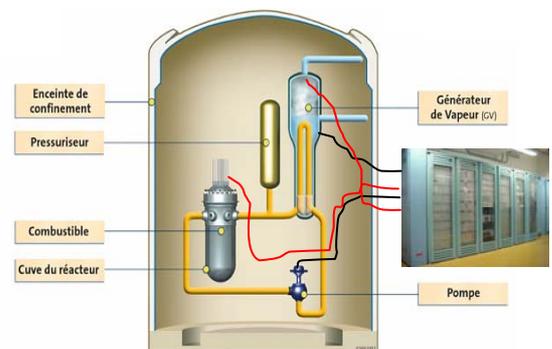
Rôle du système de protection du réacteur

En cas de détection d'un évènement anormal, tel qu'une augmentation excessive de la température du réacteur, les systèmes de protection et de sauvegarde activent des dispositifs de pilotage automatique afin de maintenir l'installation dans un état sûr en évitant aux opérateurs de devoir agir sans temps de réflexion.

Pour les réacteurs français à eau sous pression de 1300 MWe et de 1450 MWe, les fonctions de protection et de sauvegarde sont assurées par le Système de Protection Intégré Numérique (SPIN). Ce dispositif comporte 3 étages (voir le schéma ci-contre)

Le SPIN des réacteurs de 1300 MWe contient des logiciels dans les étages 2 et 3 et celui du 1450 MWe dans les 3 étages.

La logique d'un système de protection est en fait constituée de nombreux logiciels implantés sur des cartes électroniques ayant chacune un rôle bien défini. Certains surveillent les paramètres du réacteur, comme par exemple la température, la pression ou le niveau de flux neutronique, d'autres réalisent des échanges de données sur les réseaux reliant les cartes entre elles. Le système de protection des réacteurs de 1300 MWe comporte une quarantaine de cartes et celui des réacteurs plus récents de 1450 MWe, environ une centaine.



Les 3 étages du Système de Protection Intégré Numérique équipent les réacteurs de 1300 MWe (SPIN 1300) et les réacteurs 1450 MWe (SPIN N4). Plusieurs centaines de capteurs et d'actionneurs sont reliés au SPIN.

- Le premier étage collecte les informations fournies par les capteurs de mesure (pression, température...); il est alimenté par des fils noirs sur le schéma
- Le deuxième calcule et compare les résultats aux limites de fonctionnement prévues
- Le troisième gère les résultats de ces comparaisons et décide s'il y a lieu d'arrêter le réacteur et/ou d'activer des systèmes de sauvegarde; il transmet les ordres par des fils rouges sur le schéma

EDF modifie les logiciels de ses systèmes de protection

En 2008, l'IRSN a terminé l'analyse de sûreté concernant quatre modifications qui seront implantées par EDF dans les prochaines années. Ces modifications portent sur les logiciels des systèmes de protection des réacteurs de 1300 MWe et de 1450 MWe ainsi que sur le logiciel d'un système chargé de surveiller la marge par rapport au risque d'ébullition dans la cuve des réacteurs de 900 MWe et de 1450 MWe en situation post-accidentelle.

1/ Modification d'une documentation volumineuse

La documentation du logiciel d'un système de protection comporte plusieurs centaines de documents relatifs à :

- la spécification (que veut-on faire ?),
- la conception (comment le faire ?),
- les tests (est-ce que cela marche ?).

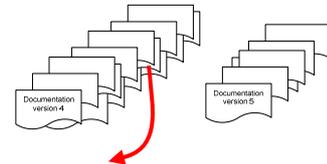
Pour le cas de la modification du SPIN 1300, l'IRSN a examiné environ 70 documents soit 4 000 pages spécifiques au logiciel.

2/ Modification de nombreux fichiers informatiques

Le logiciel proprement dit est constitué de fichiers contenant les programmes sources écrits dans un langage informatique. Parmi le millier de fichiers du logiciel du système de protection des réacteurs de 1300 MWe, 300 ont été modifiés par l'exploitant et ces modifications ont été analysées par l'IRSN. Les fichiers sont plus nombreux pour les réacteurs 1450 MWe.

3/ Modification des tests

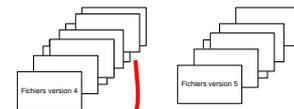
Si quelques tests peuvent être suffisants pour vérifier la qualité d'une modification mineure, une campagne de plusieurs centaines de tests, nécessairement réalisée par le concepteur, est souvent nécessaire dans le cas d'une évolution significative du logiciel. Cette campagne de tests est un élément important de l'analyse de sûreté et se décline suivant « une stratégie de test ». Les tests couvrent tous les niveaux du développement, des tests unitaires de chaque fonction aux essais de l'installation complète. Ces derniers doivent vérifier que les modifications sont bien réalisées et que les parties non modifiées fonctionnent toujours correctement.



2.2.3.3. Modification du logiciel de l'UF5

- Prise en compte du traitement d'une nouvelle carte 32 E.TOR ;
- Prise en compte des nouvelles entrées TOR : Signal TBPP (et son complément) sur la carte 32 E.TOR ajoutée ;
- Ajout d'un filtre Avance/Retard (avec constante T1 et T2) sur la mesure de Pression Enceinte en amont du seuil MAX2 ;

Extrait de la spécification du logiciel dénommé UF5 des réacteurs de 1300 MWe: la mesure de la pression dans l'enceinte est désormais filtrée



```

01 * COMPARAISON DE LA PRESSION LUE SUR LE TABLE TORO AVEC LA VALEUR DU SEUIL MAJ
02 * SUR LA SON LA MEMOIRE PARAMETRE ET ECRITURE DU RESULTAT DE LA COMPARAISON EN
03 * MP4
04 *
05 ***** VERIFIN SEUIL_PEN *****
06 *
07 * LA FONCTION DE FILTRAGE DE LA PRESSION ENCEINTE EST REALISEE DANS LE MODULE FONCT
08 * ELLE INCLUT PAR CONCEPTION L'ECRITURE DE LA VALEUR FILTREE DANS LA TABLE TABR2 ET LA MP4
09 *
10 * COMPARAISON DE LA PRESSION ENCEINTE APRES FILTRAGE LOG DANS LA TABLE TABR2
11 * AVEC LA VALEUR DU SEUIL MAJ2 SE LU SUR LA MEMOIRE PARAMETRE
12 * ET ECRITURE DU RESULTAT DE LA COMPARAISON EN MP42
13 *
14 ***** VERIFIN SEUIL_PEN2 *****
15 *
16 ***** FIN MODIF L.16 *****

```

Extrait du fichier PENC5.SPN chargé de traiter la pression dansenceinte: l'ancienne mesure de la pression de l'enceinte PEN (lignes en rouge) est remplacée par PENS filtrée (lignes en jaune)

Test: UF5_GEN_FILT_NUM « Résolution et implémentation du filtre numérique »		
Environnement de test: ENV_TV1_NUM_02 : TESTEUR + LOG_REPRO + OBS_INT + TRC_EXE		
Référence IAF_UF51_54.2.512		
N°	Procédure de test	Résultat attendu
<i> Filtrage des données analogiques</i>		
3	Ouvrir le fichier UF5_GEN_FILT_NUM.log	Vérifier que le compte-rendu est correct (toutes les étapes du test définies ont été exécutées sans erreur)
4	Ouvrir le fichier UF5_GEN_FILT_NUM_1C.TRC	Les valeurs lues aux adresses des données filtrées sont conformes à celles attendues PENS = (0x013F 0x013E) (Poids Fort faible)

Extrait des tests réalisés sur le logiciel UF5: vérification de la nouvelle mesure de pression filtrée dans l'enceinte PENS

Implantation d'un composant mémoire modifié.

Les programmes sources comportent de nombreuses lignes de programme, de 40 000 pour les premières installations informatisées à 400 000 pour les dernières. Ces programmes sources sont transformés pour pouvoir être lus par le calculateur (programmes exécutables) ; pour cela, ils sont écrits sous la forme d'une succession de 1 et de 0 et stockés dans des mémoires. La modification du logiciel dans l'installation correspond au remplacement de mémoires. En 2009, 80 % des logiciels du système de protection des réacteurs de 1300 MWe seront modifiés.

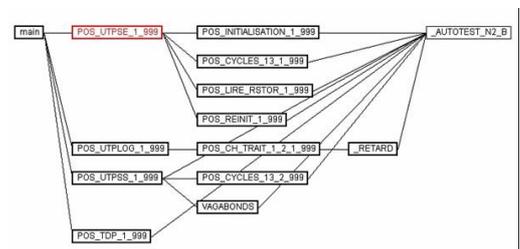
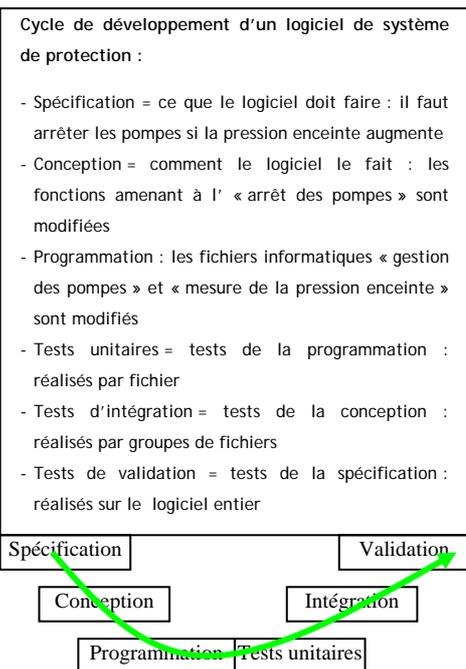
Démarche d'analyse de l'IRSN

Le développement de logiciels (dits critiques) dans le nucléaire doit respecter entre autres les exigences de la Règle Fondamentale de Sécurité (RFS) relative aux logiciels ainsi que les normes internationales de la Commission Électrotechnique Internationale (CEI). L'IRSN participe aux travaux qui conduisent à l'établissement de telles règles et normes.

L'évaluation d'un logiciel par l'IRSN comporte l'examen de documents, en commençant par le Plan Qualité et l'analyse d'impact qui permettent de suivre le processus de développement, puis l'examen du programme source et de programmes exécutables (fichiers informatiques) et, enfin la réalisation de tests. L'IRSN met en œuvre une démarche fondée sur un ensemble de moyens et de méthodes lui permettant de réaliser une revue de ces trois aspects, en sélectionnant les sujets pour lesquels les modifications ont des conséquences significatives pour la sûreté (analyse dite par « échantillonnage »).

1 : L'IRSN examine d'abord l'ensemble des documents pour comprendre comment fonctionne l'organisation mise en place pour réaliser la modification. Il en examine la complétude (c'est-à-dire sa capacité de couvrir tous les aspects et toutes les phases de la modification), la cohérence et évalue les méthodes employées (par exemple : l'indépendance des équipes de développement et de vérification). L'IRSN s'assure que la documentation décrit sans ambiguïté ce que devra faire le logiciel (analyse des spécifications) et comment il le fera (analyse de la conception). L'IRSN examine comment les documents de chaque étape (voir le schéma ci-contre) sont impactés, chaque point de modification doit se décliner de la spécification aux tests de validation.

Implantation d'un composant mémoire



Extrait du graphe d'appel des fonctions du SPIN N4 obtenu au moyen de l'outil QAC

La fonction modifiée (en rouge) appelle 4 fonctions qui doivent toujours fonctionner correctement après la modification.

L'analyse statique réalisée ici exploite le contenu des fichiers

2 : L'IRSN examine les programmes sources. Il s'agit ici de vérifier la bonne « fabrication » du logiciel : application de règles de programmation jugées pertinentes, utilisation adéquate des données traitées, pertinence des commentaires traçant les modifications dans les fichiers. L'IRSN vérifie que la programmation est cohérente avec les documents de spécification et de conception (noms des données et des fonctions, calculs...). A cet effet, l'IRSN utilise des outils informatiques qu'il a développés en collaboration avec des services spécialisés du Commissariat à l'Energie Atomique.

3 : Le dernier examen de l'IRSN porte sur les tests et leur « couverture » (testent-ils toutes les modifications ?). Le fonctionnement du logiciel est-il bien celui attendu ? L'IRSN vérifie que les informations générées par le logiciel présentent un état déterminé y compris pour tout évènement susceptible de survenir (panne, valeur de mesure aberrante ou dégradée ...). L'IRSN examine également le rôle et la qualité des outils matériels et informatiques utilisés par les équipes de développement et de test.

Définitions et abréviations

ASN : Autorité de sûreté nucléaire.

BAN : Bâtiment des auxiliaires nucléaires

Becquerel : (Bq) Unité de mesure, légale et internationale, utilisée pour la radioactivité. Un Becquerel est égal à une désintégration par seconde.

Bore : Le bore est un élément chimique de symbole B et de numéro atomique 5. Il a la propriété d'absorber les neutrons, ce qui permet la maîtrise de la réaction en chaîne.

ASG : Système de secours de l'alimentation en eau des générateurs de vapeur. Ce système a pour rôle l'alimentation en eau des générateurs de vapeur (GV) toutes les fois où elle est impossible à réaliser par le poste d'eau. C'est un circuit de sauvegarde qui, lors d'accidents ou d'incidents entraînant l'indisponibilité de l'alimentation normale des GV (ARE), assure l'alimentation en eau de ceux-ci, permettant ainsi l'évacuation de la puissance résiduelle.

différence axiale de puissance : Différence entre la puissance dans le haut du cœur et la puissance dans le bas du cœur rapportée à la puissance moyenne du cœur

DVH : Système de ventilation du local des pompes d'injection de sécurité à haute pression

DVN : Système de ventilation du bâtiment des auxiliaires nucléaires

EAS : Système (de sauvegarde) d'aspersion dans le bâtiment abritant le réacteur.

[INES](#) : International Nuclear Event Scale, échelle internationale des événements nucléaires à but médiatique.

MWe : Le mégawatt électrique est l'unité utilisée pour la puissance fournie au réseau électrique par une centrale nucléaire.

RCV : Système de contrôle chimique et volumétrique (du circuit primaire).

Réaction en chaîne : Dans le domaine du nucléaire, une réaction en chaîne se produit lorsqu'un neutron cause la fission d'un atome fissile produisant un nombre de neutrons supérieur ou égal à 1, qui à leur tour causent d'autres fissions.

REP : Réacteur à eau sous pression.

Réservoir PTR : Réservoir d'eau borée de grande capacité qui alimente notamment les circuits d'injection de sécurité (RIS) et d'aspersion dans l'enceinte (EAS) en cas d'accident.

RIS : Système d'injection de sécurité d'eau borée dans le cœur.

RRI : Système de réfrigération intermédiaire

Salle des machines : bâtiment abritant le turbo-alternateur qui produit l'électricité

Sievert : Unité légale d'équivalent de dose (ou dose efficace) qui permet de rendre compte de l'effet biologique produit par une dose absorbée donnée sur un organisme vivant. L'équivalent de dose n'est pas une quantité physique mesurable ; elle est obtenue par le calcul. Elle dépend de l'énergie transmise aux tissus, du type de rayonnement et du tissu traversé.

SEC : Système d'alimentation en eau brute secourue (assure le refroidissement de l'eau du système RRI)

Taux de combustion : rapport exprimant le nombre de noyaux fissiles ayant subi une fission sur le nombre initial de ces noyaux.

TEG : Système de traitement des effluents gazeux ; il recueille les effluents gazeux provenant du circuit primaire.

VD3 : 3ème visite décennale d'un réacteur nucléaire.

Crédit photo

Page 4 : photo EDF - médiathèque 2008

Pages 26 et 27 : 2 photos EDF-CNPE de Fessenheim

Pages 37, 38, 39 : 5 photos, EDF-CNPE de Flamanville

Pages 44 et 46 : 2 photos AREVA

Pages 45 et 46 : 2 photos EDF

Page 52 : Photo EDF-CNPE Cruas-Meysse

Page 57 : 2 photos EDF

Page 60 : photo EDF

page 2, 5, 7, 9, 11, 14, 15, 19, 22, 25, 30, 31, 34, 42, 49, 52, 59, 63, 65, 66 : illustration IRSN