IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 19 novembre 2014

Monsieur le Président de l'Autorité de sûreté nucléaire

Avis IRSN N° 2014-00413
Objet : Réacteurs électronucléaires – EDF
Palier P4 – États techniques « VD2-VD3 »
Rénovation du contrôle-commande.
Réf. : Courrier ASN CODEP-DCN-2014-030734 du 7 juillet 2014

Par sa lettre citée en référence, l'Autorité de sûreté nucléaire (ASN) a souhaité recueillir l'avis de l'Institut de radioprotection et de sûreté nucléaire (IRSN) sur l'acceptabilité au plan de la sûreté, de la radioprotection et de la protection de l'environnement des modifications PNPP 2447-2448-2449. Ces modifications, qui s'intègrent dans le cadre du réexamen associé aux troisièmes visites décennales du des réacteurs de 1300 MWe (VD3 1300), concernent respectivement la rénovation du système de protection du réacteur (RPR), du système de mesure de puissance neutronique (RPN), et du système de commande des grappes de contrôle du réacteur (RGL).

Contexte et contour de l'analyse

Dans le cadre de son projet de modernisation du contrôle-commande des réacteurs de 1300 MWe, EDF a décidé de rénover les systèmes RPR et RPN (classe de sûreté 1E), ainsi que la partie importante pour la sûreté non classée (IPS-NC) du système RGL. Ces rénovations sont principalement motivées par l'obsolescence de certains matériels et la volonté de donner à ces systèmes la capacité d'intégrer des évolutions fonctionnelles.

Ces trois systèmes sont principalement constitués de calculateurs programmés effectuant des traitements d'automatismes et de régulations. Le principe général retenu pour ces rénovations est celui d'un remplacement « calculateur par calculateur » à interfaces identiques. Les systèmes rénovés réalisent, avec la même répartition entre les nouveaux calculateurs, les fonctions assurées par les anciens ainsi que quelques nouvelles fonctions liées aux modifications introduites dans le cadre du réexamen de sûreté associé à la VD3 1300.

Les systèmes RPR, RPN et RGL rénovés sont basés sur une nouvelle plateforme de contrôle-commande.

Adresse courrier
BP 17
92262 Fontenay-aux-Roses
Cedex France

Siège social
31, av. de la Division Leclerc
92260 Fontenay-aux-Roses
Standard +33 (0)1 58 35 88 88
RCS Nanterre B 440 546 018

Conformément aux différents points de la demande en référence, le présent avis aborde successivement :

- l'aptitude de la nouvelle plateforme à accueillir des fonctions de classe de sûreté 1E ;
- le développement des systèmes RPR et RPN rénovés réalisé à l'aide de cette plateforme ;
- le développement de la partie rénovée du système RGL ;
- la cohérence d'ensemble du contrôle-commande du réacteur suite à ces modifications.

Les modifications ont fait l'objet d'une qualification matérielle aux conditions d'ambiance et au séisme. L'évaluation de cette qualification n'entre pas dans le cadre du présent avis.

Aptitude de la nouvelle plateforme à accueillir des fonctions de contrôle-commande de classe de sûreté 1E

Une plateforme de contrôle-commande comprend des composants génériques (cartes électroniques et logiciel embarqué, composants réseau, alimentations électriques, châssis, câbles, etc.) et des outils logiciels permettant de réaliser des systèmes particuliers (par ex. un système de protection ou d'instrumentation nucléaire), nommés « applications », à partir de ces composants.

Les cartes électroniques fournissent des capacités de calcul, d'interface avec le procédé (acquisitions d'entrées ou émission de sorties, analogiques ou tout-ou-rien), d'interfaces spécialisées (pilotage de moteurs, comptage d'impulsions, etc.) et de communication (lignes série asynchrones, réseaux).
Le logiciel système opérationnel prend en charge les fonctions techniques de la plateforme, indépendantes des calculs fonctionnels des applications : initialisation des cartes, accès cyclique aux entrées et aux sorties, communications, autotests, etc.

L'IRSN considère que l'expérience du constructeur de la nouvelle plateforme montre sa maîtrise technique et que les concepts structurants de cette plateforme sont clairs et adaptés au besoin des applications de sûreté de classe 1E. L'IRSN estime à cet égard que le processus de développement suivi par le constructeur est conforme à la règle fondamentale de sûreté applicable aux « logiciels des système électriques classés de sûreté » (RFS II.4.1.a) d'une part, aux exigences normatives de la Commission électrotechnique internationale (CEI 61513, CEI 60880 et CEI 62566) d'autre part. Ce processus est pleinement acceptable pour les logiciels, les circuits électroniques programmables et les systèmes classés 1E. En particulier, l'IRSN considère que :

- le processus de développement suivi par le constructeur est organisé en phases bien délimitées et définit les activités et les produits intermédiaires de façon à prévenir les erreurs et à faciliter la vérification ;
- les documents techniques génériques, par exemple les règles de conception et de programmation, sont techniquement pertinents pour maîtriser la qualité et la sûreté des produits ;
- la répartition des rôles et l'indépendance entre équipes de conception et de vérification sont claires et adéquates ;
- les dispositions de gestion de configuration garantissent la disponibilité des informations et le contrôle des modifications, pour les produits techniques et pour la documentation des activités ;

- les outils de conception et de vérification sont conformes à l'état de l'art ; ils permettent par exemple une analyse précise de phénomènes internes tels que les échanges sur les réseaux.

L'IRSN considère que la plateforme utilisée pour la rénovation du contrôle-commande du palier 1300 MWe répond aux exigences de fonctionnement sûr et de déterminisme de la RFS II.4.1.a et de la norme CEI 60880, requis pour les systèmes de classe 1E, notamment parce que :

- les principes de fonctionnement de la plateforme confèrent à chaque unité et réseau associé un comportement cyclique et séquentiel, et que la rigueur de la conception et de la vérification garantit une réalisation conforme à ces principes ;
- le comportement cyclique et séquentiel de chaque unité n'est pas influençable par les autres unités, ni par des facteurs potentiellement communs à plusieurs (transitoires du procédé, temps écoulé depuis la mise sous tension, etc.), ce qui prévient les défaillances de cause commune (DCC) par propagation ou par coïncidence dues à d'hypothétiques défauts résiduels ;
- la plateforme possède les fonctionnalités nécessaires en matière de testabilité : autotest permanent du matériel avec passage en position prédéfinie et signalisation en cas de détection, gestion d'indicateurs de validité des signaux applicatifs et support aux tests périodiques ;
- les outils de paramétrage et de maintenance permettent les interactions nécessaires à l'exploitation sans compromettre le fonctionnement sûr et déterministe des unités.

L'IRSN estime que les méthodes et les outils mis en œuvre par le constructeur pour vérifier les composants logiciels et les circuits électroniques programmables, ainsi que pour valider les systèmes, sont techniquement pertinents et complémentaires, justifiés et documentés, conformes à l'état de l'art des systèmes de sûreté et donc pleinement acceptables pour des systèmes de classe 1E.

La surveillance spécifique exercée par EDF sur les logiciels de systèmes de classe 1E apporte un niveau additionnel d'indépendance des équipes et des méthodes, et utilise en particulier des outils d'analyse formelle scientifiquement innovants. Elle confirme, selon un point de vue complémentaire, les résultats de V&V (vérification et validation) obtenus par le constructeur. L'IRSN considère donc que les résultats de V&V, concluant à la validation de la nouvelle plateforme, sont acceptables ; ils confirment de façon crédible la pertinence de ses mécanismes, la qualité de sa conception et l'absence autant que faire se peut de défauts logiques simples ou susceptibles de provoquer une DCC.

L'IRSN estime également que les outils et les méthodes associés à la nouvelle plateforme pour développer ses applications sont conformes aux exigences normatives et à l'état de l'art. Elles sont acceptables pour développer des applications classées 1E, telles que les systèmes RPR et RPN rénovés.

Enfin, l'IRSN estime acceptables la fiabilité matérielle de la nouvelle plateforme et les méthodes permettant de calculer les fréquences de pannes sûres et non sûres, fonction par fonction, d'un système classé 1E réalisé avec cette plateforme.

L'IRSN conclut que la nouvelle plateforme est pleinement acceptable pour développer des fonctions de contrôle-commande de classe 1E ou de catégorie A selon la CEI.

Développement des systèmes RPR et RPN rénovés

Le système RPR, de classe 1E, du palier 1300 MWe participe aux fonctions de sûreté de maîtrise de la réactivité, d'évacuation de la puissance résiduelle et de confinement des substances radioactives. Il a pour rôle d'élaborer des actions de protection et de sauvegarde avec les signalisations associées, à partir des informations issues des capteurs de protection appartenant à l'instrumentation (RPN, RGL…).

La partie numérique du système RPR, constituée de calculateurs programmés regroupés dans quatre unités d'acquisition et de traitement de protection (UATP) redondantes, est complètement rénovée.

Chaque calculateur des UATP est remplacé par un nouveau calculateur. De nouveaux réseaux de protection remplacent les liaisons série et les mémoires partagées actuelles pour la transmission des informations entre les quatre UATP. Ce même type de réseau est également introduit pour transmettre au système RPR les mesures neutroniques élaborées par les chaînes de puissance du système RPN. Une nouvelle unité d'acquisition reçoit les mesures réalisées par les armoires d'instrumentation de la position des barres de contrôle du système RGL.

La partie non numérique (i.e. logique câblée) du système RPR, constituée des armoires des unités logiques de sauvegarde (ULS) qui réalisent les votes entre divisions en aval de la partie numérique pour les actions de sauvegarde n'est pas rénovée. Toutefois, elle subit des modifications pour intégrer les évolutions fonctionnelles issues du réexamen de sûreté associé à la VD3, telles que l'isolement de l'alimentation de secours des générateurs de vapeur (ASG) sur signal « très haut niveau GV » en cas de rupture de tube (RTGV). Ainsi, deux armoires de conception et de technologie identique à l'existant (logique dynamique à panne orientée) sont ajoutées dans chacune des deux voies.

Les armoires qui réalisent l'interface entre le RPR et les systèmes non classés vers lesquels il émet des informations, sont remplacées par des armoires intégrant des unités spécialisées chargées de rendre la liaison unidirectionnelle (du plus classé vers le moins classé).

Le système RPN a pour fonction de sûreté principale la mesure du flux neutronique dans la cuve du réacteur. Il transmet au système RPR les mesures du flux neutronique et la puissance corrigée qu'il a calculées. Une autre partie de ce système, qui n'est pas de classe 1E, déclenche également des alarmes, détermine la puissance corrigée/recalée, envoie les signalisations neutroniques en salle de commande et vers les coffrets audio utilisés lors des phases de chargement et de déchargement de combustible.

L'architecture initiale du système RPN, avec trois chaînes d'instrumentation (niveaux neutroniques source, intermédiaire et de puissance) est conservée. Les détecteurs et la plupart des équipements de la salle de commande liés au système RPN ne sont pas remplacés. La partie classée 1E du système RPN est totalement rénovée. Les armoires de technologie analogique sont remplacées par des armoires de technologie numérique. Une nouvelle armoire de contrôle, IPS-NC, contient également une interface homme-machine dédiée aux opérations de maintenance et de surveillance du RPN. Les interfaces actuelles sont pour la grande majorité conservées en l'état. Les interfaces modifiées sont la liaison « Chaîne niveau puissance » vers le système RPR qui devient un réseau de protection dédié et quelques liaisons spécifiques destinées pour la plupart à la signalisation.

L'IRSN estime que l'architecture des systèmes RPR et RPN rénovés est acceptable dans la mesure où le niveau de redondance des chaînes de protection et de sauvegarde, et la non-perturbation des parties 1E par des matériels moins classés sont préservés par la rénovation. La capacité de ces systèmes à faire l'objet d'essais périodiques en fonctionnement est, elle aussi, conservée avec une simplification des opérations à réaliser.

Le développement d'un système programmé de classe 1E doit suivre un processus rigoureux conforme aux exigences de la RFS II.4.1.a et aux normes CEI précédemment citées. Cette démonstration a été apportée par EDF de manière générique pour la nouvelle plateforme, de sorte que pour les systèmes RPR et RPN, elle ne reste à apporter que pour le développement des « applications ».

A cet égard, l'IRSN estime que le processus prévu par EDF et les concepteurs pour le développement des « applications » que constituent les systèmes RPR et RPN, ainsi que le processus effectivement suivi, sont conformes aux préconisations des normes CEI, tant pour les aspects système que logiciel, et explicitent clairement les activités respectives des deux concepteurs.

L'IRSN estime de plus que les documents qui définissent les données d'entrée du processus de développement des systèmes RPR et RPN (spécification des fonctions à réaliser, exigences de sûreté, interface…) sont globalement clairs, complets et cohérents. L'IRSN note que ces documents ont fait l'objet d'une validation et que les exigences qu'ils contiennent sont tracées tout au long du processus de développement.

La conception des systèmes RPR et RPN, tant sur les aspects matériels que logiciels, n'appelle pas de remarque de la part de l'IRSN ; cette activité étant très étroitement encadrée par l'utilisation de la nouvelle plateforme et le processus de développement associé.

Pour chacun des calculateurs 1E de ces systèmes, le programme informatique automatiquement généré à l'issue de la conception (code source) a fait l'objet de vérifications de la part d'EDF. L'IRSN note que ces vérifications réalisées à l'aide d'outils d'analyse formelle scientifiquement innovants constituent une avancée technique notable en terme de vérification de code source et apportent une garantie forte du très haut niveau de qualité des logiciels des systèmes RPR et RPN.

Les normes CEI recommandent la réalisation de campagnes d'essais successives au cours desquelles un système 1E progressivement intégré est vérifié étape par étape. L'IRSN estime que les différentes campagnes de test menées sur les systèmes RPR et RPN sont suffisamment complémentaires, exhaustives, avec des procédures de test clairement identifiées. Les essais sur un banc de test dédié, très nombreux, sont particulièrement détaillés, ce qui est essentiel dans la mesure où ces essais sont pris comme référence pour la campagne suivante (requalification sur site). Suite à l'examen de l'ensemble des résultats d'essais, l'IRSN n'a pas de remarque sur ces programmes de requalification qui apparaissent complets, précis et détaillés sur les essais réalisés et les matériels et fonctions couverts pour le train P4 du palier 1300 MWe.

Lors de ces campagnes d'essais, EDF a détecté un écart de réalisation nécessitant une modification du logiciel du système RPR avant son installation sur le réacteur tête de série. EDF doit donc justifier l'absence de régression entre la version du logiciel RPR évaluée par l'IRSN et celle qui sera

effectivement installée sur le réacteur tête de série. **Ce point fait l'objet de la recommandation n°1.**

Développement du système RGL rénové

Le système RGL réalise la mesure de position et la commande des grappes de contrôle du réacteur.

La partie classée 1E constituée des armoires d'instrumentation de mesure de position des grappes est conservée de même que les liaisons fil-à-fil entre ces armoires et le système RPR.

La partie non classée 1E est rénovée avec une évolution des fonctions et de leur répartition sur différentes armoires. En effet, tous les traitements IPS-NC sont désormais regroupés dans une nouvelle unité de surveillance. Ces traitements sont par exemple les calculs des limites basse et très basse d'insertion et les fonctions de surveillance des positions du groupe R et des groupes de compensation en puissance (GCP). En particulier, des modifications sont apportées à la régulation des GCP et à la surveillance du positionnement des GCP pour prendre en compte de la puissance thermique moyenne filtrée des quatre UATP.

Pour l'examen du système RGL rénové, l'IRSN s'est appuyé sur son analyse des systèmes RPR et RPN, la technologie ainsi que les moyens de développement étant identiques et la démarche retenue pour la validation (système et banc de test) s'inscrivant dans le même processus global.
Sur la base des éléments transmis, l'IRSN considère que la rénovation de la partie non classée 1E du système RGL :

- n'introduit pas de possibilité de perturbation des systèmes ou parties de systèmes plus classés avec lesquels elle interagit ;
- est réalisée sur la base d'une technologie fiable et maitrisée par le concepteur et selon un processus satisfaisant pour un système de ce niveau de classement.

En conséquence, l'IRSN n'a pas de remarque sur la rénovation des parties non classées 1E du système RGL.

Cohérence de l'ensemble des modifications RPR, RPN et RGL

A la demande de l'IRSN, EDF a justifié que la rénovation des systèmes RPR, RPN et RGL n'introduisaient pas de dépendance susceptible de rendre le contrôle-commande du palier 1300 MWe vulnérable à une défaillance de cause commune. Les points clé de cette justification sont :

- une stratégie de rénovation « calculateur par calculateur » qui conserve dans une large mesure l'architecture initiale ;
- le maintien de la diversification technologique entre le RPR rénové et le système Contrôbloc existant qui en assure le secours ;
- le caractère unidirectionnel des réseaux informatiques introduits lors de la rénovation.

En conséquence, l'IRSN estime que la rénovation des systèmes RPR, RPN et RGL (PNPP 2447, 2448 et 2449) n'a pas introduit de possibilité de défaillance de cause commune qui serait susceptible d'affaiblir la robustesse d'ensemble du contrôle-commande, et considère donc que suite à cette rénovation l'architecture d'ensemble du contrôle-commande des tranches 1300 MWe reste acceptable.

Conclusion

Sous réserve de la recommandation formulée en annexe, l'IRSN considère que les modifications PNPP 2447-2448-2449 applicables au train P4 du palier 1300 MWe sont acceptables - telles que déclarées - au plan de la sûreté.

Toutefois, l'IRSN note que si les documents de conception des systèmes RPR, RPN et RGL sont communs aux trains P4 et P'4, ce n'est en revanche pas le cas pour les documents relatifs aux essais de ces systèmes qui n'ont pas tous été transmis à l'IRSN pour ce qui concerne le train P'4. L'extension des conclusions du présent avis aux réacteurs du train P'4 nécessiterait donc une évaluation, par différence, des programmes et résultats d'essais du train P'4.

Pour le Directeur général, par ordre
Frédéric MENAGE
Adjoint au directeur de l'expertise de sûreté

Annexe à l'avis IRSN n°2014-00413 du 19 novembre 2014

Recommandations

Recommandation n°1

L'IRSN recommande qu'EDF justifie, d'ici janvier 2015, la non-régression entre la version 2.0 du RPR évaluée par l'IRSN dans le cadre de la demande de modification PNPP 2447 et la version implémentée sur la TTS du réexamen VD3-1300. Cette justification devra notamment s'appuyer sur une analyse d'impact, la réalisation des essais de validation et de non-régression associés et sur la mise à jour de la documentation de développement.