IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 18 juin 2014

Monsieur le Président de l'Autorité de sûreté nucléaire

Avis/IRSN N° 2014-00240
Objet : Réacteurs électronucléaires – EDF – Réacteur EPR de Flamanville 3 – Système de protection
Réf. Lettre ASN CODEP-DCN-2013-054214 du 22 novembre 2013

Par lettre citée en référence, l'Autorité de sûreté nucléaire (ASN) a demandé l'avis de l'Institut de radioprotection et de sûreté nucléaire (IRSN) sur « *l'acceptabilité sur le plan de la sûreté des éléments structurants de la conception et du développement de la partie classée F1A du système de protection (PS-F1A)* » du réacteur EPR de Flamanville 3 (EPR-FA3), en particulier sur :

- « *la suffisance des données d'entrée nécessaires au développement du PS-F1A ;*
- *le processus de développement du PS-F1A, particulièrement sur ses logiciels ;*
- *l'architecture du système PS-F1A ;*
- *la stratégie de test du PS-F1A ;*
- *la version de travail du chapitre 7.3 du rapport de sûreté relatif au PS.* »

La demande de l'ASN porte sur la version V2 du PS-F1A.

Contexte

Le PS-F1A réalise les fonctions automatiques, manuelles et de surveillance nécessaires pour atteindre l'état contrôlé en cas d'événements PCC-2, 3 ou 4 : arrêt automatique du réacteur (AAR), déclenchement de fonctions de sauvegarde telles que l'injection d'eau borée, le démarrage des diesels principaux, le délestage et le relestage séquencé des actionneurs, l'élaboration des permissifs, etc. Il joue donc un rôle essentiel pour la sûreté.

Il est interfacé principalement avec le procédé, mais communique cependant avec d'autres systèmes de contrôle-commande comme le moyen de conduite principal (MCP) et le moyen de conduite de secours (MCS), par exemple pour les fonctions de surveillance et les permissifs, les systèmes d'automatismes de tranche (PAS) et d'automatismes de sûreté (SAS) ou encore des systèmes de contrôle-commande spécifiques comme celui de la turbine.

Données d'entrée du développement du PS-F1A

Le développement du PS-F1A doit satisfaire des besoins dont certains, en particulier fonctionnels, relèvent de métiers autres que le contrôle-commande. Une erreur ou une ambiguïté affectant les données d'entrée du développement, pouvant par exemple résulter d'une incompréhension entre spécialistes de domaines différents, est susceptible de se propager jusqu'au système final ; il est donc

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

essentiel que les données d'entrée nécessaires au développement soient systématiquement identifiées et documentées de façon adéquate.
Les catégories de données d'entrée nécessaires sont : la spécification des fonctions de contrôle-commande et de service (par ex. support à la maintenance) allouées au PS-F1A, les contraintes sur la conception (résultant par ex. du classement de sûreté et des requis d'indépendance), les interfaces avec les autres systèmes et avec les utilisateurs, les conditions d'environnement et la démonstration d'aptitude requise (par ex. conformité à certains textes para-réglementaires et analyse de la tolérance aux défaillances).

L'IRSN considère que les données d'entrée retenues par EDF pour développer le PS-F1A couvrent les catégories nécessaires : fonctions, contraintes sur la conception, interfaces, etc. Elles sont exprimées de façon claire (compréhensible par une personne n'ayant pas participé au projet mais possédant la connaissance générale du domaine) et précise (sans ambiguïté). Elles sont vérifiables et permettent de définir un système réalisable. L'IRSN considère donc que ces données d'entrée sont suffisantes. Leur analyse fonctionnelle du point de vue des études d'accident ne fait pas l'objet de cet avis, conformément à la demande de l'ASN en référence.
L'IRSN a estimé que certains aspects du processus de transmission des données d'entrée fonctionnelles aux équipes de développement du PS-F1A devaient être précisés. Au cours de l'instruction technique, EDF a fourni les précisions nécessaires et a indiqué que ces précisions seraient intégrées lors de la révision du processus.

Processus de développement du PS-F1A

Afin d'être apte à remplir ses missions de sûreté, le PS-F1A doit autant que possible être matériellement fiable, disposer d'un logiciel de qualité et réaliser une logique exempte d'erreur. Ce dernier point est particulièrement délicat, car il ne peut pas être complètement garanti par le seul examen, par tests et analyses, du PS-F1A : afin d'atteindre la confiance voulue, un processus de développement rigoureux et adéquat doit également être défini et appliqué.

L'IRSN considère que le processus de développement du PS-F1A est conforme à l'état de l'art du domaine (normes de la Commission Electrotechnique Internationale : IEC 60880 et IEC 61513), aux exigences para-réglementaires françaises (Règle Fondamentale de Sûreté II.4.1.a) et aux exigences du rapport de sûreté. En particulier, l'IRSN estime qu'il est organisé de façon claire, en étapes permettant de maîtriser la progression du développement et de vérifier chaque produit intermédiaire, et qu'il présente des avancées notables par rapport à l'état de l'art en matière de validation.

Toutefois, l'IRSN a estimé que certaines modalités de vérification de la conception détaillée devaient être précisées. EDF a amendé son processus au cours de l'instruction technique, en tenant compte des remarques de l'IRSN concernant par exemple l'indépendance de l'équipe de validation par rapport à l'équipe de développement et les méthodes de vérification des différents types de composants.

De plus, l'IRSN estime que le rôle d'EDF dans l'approbation des tests devrait être renforcé ; **ce point fait l'objet de l'observation n°1.**

Architecture du système PS-F1A

L'architecture du PS-F1A, c'est-à-dire son organisation en unités (calculateurs) interconnectées sur lesquelles sont distribuées les fonctions requises, doit contribuer à satisfaire les exigences de

fonctionnalité et de performance, tolérer les aléas postulés (défaillance unique, indisponibilité pour cause de maintenance préventive, agression, etc.) et participer à la défense en profondeur.

EDF a indiqué que le PS-F1A est organisé en 4 divisions identiques comprenant les unités et réseaux classés F1A, ainsi que des unités de surveillance et d'interface avec les autres systèmes, classées F1B. Chaque division comporte les unités classées F1A suivantes :

- cinq Unités d'acquisition et de traitement (APU0 à APU4), différentes, chargées d'acquérir les mesures, d'élaborer les grandeurs physiques, de les comparer aux seuils et de transmettre les résultats aux Unités logiques des actionneurs (ALUs) ;
- deux Unités d'acquisition déportées (RAU1 et RAU2), redondantes, chargées d'acquérir les mesures des collectrons et de les transmettre aux APUs 0 et 1 ;
- une Unité d'acquisition et de traitement des positions de grappes (RPU), qui ne fait pas partie du PS-F1A mais transmet ses mesures aux APUs 0, 1, 2 et 4 ;
- deux ALUs redondantes (A1 et A2) recevant les résultats des APUs 0 à 2 des 4 divisions ; elles effectuent les votes (en général, en 2 parmi 4) sur les résultats homologues des 4 divisions, le calcul des permissifs et enfin l'élaboration des sorties vers les dispositifs d'AAR et vers les actionneurs de sauvegarde et de support ;
- deux ALUs redondantes (B1 et B2) effectuant les opérations similaires sur les résultats des APUs 3 et 4.

Ces unités sont organisées en deux sous-systèmes indépendants dans chaque division. Les fonctions d'AAR diversifiées, basées sur des signaux physiques différents pour détecter un même événement, sont allouées à des sous-systèmes différents. Les sorties des ALUs sont combinées dans le relayage d'interface pour piloter les dispositifs d'AAR et les actionneurs de la division.

L'IRSN considère que l'architecture du PS-F1A est satisfaisante, car :

- elle permet d'héberger dans une architecture matérielle claire et symétrique les fonctions d'architectures différentes qui lui sont allouées (4 trains, 2 trains, cas particuliers comme les fonctions d'isolement, etc.), avec les interfaces et les performances requises ;
- elle contribue à la défense en profondeur par ses capacités d'autosurveillance, de reconfiguration et de signalisation, par son organisation en deux sous-systèmes indépendants valorisant la diversification fonctionnelle de l'AAR au sein du PS-F1A et par sa diversité technologique avec le SAS valorisant les fonctions de ce dernier qui diversifient l'AAR en cas de défaillance du PS-F1A ;
- elle tolère une défaillance unique avec des choix adéquats d'orientation dans le sens de l'action ou non selon les cas ;
- elle tolère le cumul d'une défaillance unique avec la maintenance préventive ou l'essai périodique des capteurs et actionneurs ;
- elle satisfait les exigences du rapport de sûreté en matière de prévention des actions intempestives, grâce à l'autosurveillance des unités de calcul et des réseaux, à l'utilisation étendue de votes en 2 parmi 4 qui éliminent l'impact de la plupart des défaillances uniques, à la redondance des unités de vote elles-mêmes (ALUs) et à la combinaison de leurs sorties dans un relayage simple et fiable.

Lors de l'instruction technique, EDF a indiqué que les essais périodiques des unités du PS-F1A (APU, ALU, etc.) ne seront effectués que dans les états E et F du réacteur, afin de garantir la disponibilité

des fonctions quand elles sont requises, même en présence de cumuls d'aléas. L'IRSN approuve cette décision et estime que la maintenance préventive devrait suivre les mêmes règles. **Ce point fait l'objet de l'observation n°2.**

Par ailleurs, l'IRSN a estimé que le traitement de certaines défaillances multiples de réseaux, résultant par exemple d'un incendie localisé à un point de convergence des réseaux, n'était pas totalement satisfaisant. Lors de l'instruction, EDF a présenté les améliorations de la détection d'indisponibilité des réseaux qu'il prévoyait d'intégrer dans le PS-F1A. L'IRSN estime les propositions d'améliorations d'EDF satisfaisantes.

De plus, l'IRSN constate que chaque Unité d'acquisition et de traitement des positions de grappes (RPU) acquiert de façon non redondante les positions d'une partie des grappes. L'IRSN estime que cette particularité de l'architecture nécessite des justifications complémentaires concernant l'impact d'une défaillance sur les mesures ; **ce point fait l'objet de l'observation n°3**.

Enfin, la démonstration de tolérance des fonctions à l'incendie est basée sur le passage en position de repli des unités affectées par l'incendie ou leur destruction, situations caractérisées par l'absence d'émission d'ordres (en particulier intempestifs). L'IRSN estime toutefois que leur comportement transitoire en début d'incendie doit être analysé. **Ce point fait l'objet de la recommandation n°1**.

Stratégie de test du PS-F1A

Le processus de vérification et de validation du PS-F1A s'appuie sur des moyens tels que les analyses et le test. Ce dernier joue un rôle essentiel, principalement pour la validation, car il constitue la seule technique permettant d'exécuter le logiciel complet installé dans les calculateurs réels.

Les sorties d'un système programmé tel que le PS-F1A peuvent dépendre de la valeur courante et du passé de centaines d'entrées, ce qui définit un nombre de cas extrêmement élevé. Leur test exhaustif est donc définitivement irréalisable, quels que soient les moyens alloués.

Une stratégie de test doit donc être élaborée et justifiée pour démontrer la capacité du PS-F1A à accomplir ses fonctions de sûreté sans devoir exécuter tous les cas possibles. EDF a amendé sa stratégie au cours de l'instruction technique, en tenant compte des remarques de l'IRSN sur la complémentarité des actions de validation effectuées sur simulateur et sur banc matériel, ainsi que sur la validation des réseaux du PS-F1A. Concernant cette dernière action effectuée sur la version V1 et non sur la version V2, l'IRSN émet toutefois **l'observation n°4**.

Suite à son analyse, l'IRSN considère que :

- les environnements de test du PS-F1A par simulation et sur banc matériel sont acceptables ;
- les tests encadrent de façon précise et complète chaque étape d'intégration du matériel, du logiciel système et du logiciel applicatif du PS-F1A ;
- l'approche modulaire de la stratégie de test de validation est adaptée ;
- la méthode d'analyse des tests de validation constitue une avancée importante dans ce domaine.

L'IRSN considère donc que la stratégie de test, rigoureuse et innovante, va au-delà des pratiques recommandées par le consensus international et permet d'atteindre un haut niveau de confiance dans la capacité à détecter d'éventuelles erreurs de conception du PS-F1A.

Version de travail du rapport de sûreté

Le rapport de sûreté identifie les risques présentés par l'installation et analyse en particulier les dispositions prévues pour prévenir ou limiter les conséquences des incidents et des accidents. Il est donc le document de référence synthétisant la démonstration de sûreté.

L'IRSN considère que le sous-chapitre 7.3.1 de la version de travail du rapport de sûreté, relatif au PS, est acceptable, mais que certains aspects devraient être améliorés pour le rendre plus autoportant et clarifier la démonstration de sûreté. **Ce point fait l'objet de l'observation n°5.**

Conclusion

L'IRSN estime acceptables du point de vue de la sûreté les éléments structurants de la conception et du développement de la partie classée F1A du système de protection (version V2) tels que déclarés par EDF, sous réserve de la recommandation formulée en annexe.

Pour le directeur général, par ordre
Sylvie CADET-MERCIER

Directrice des systèmes, des nouveaux réacteurs et des démarches de sûreté

Annexe à l'avis IRSN/2014-00240 du 18 juin 2014

Recommandation

Recommandation n°1

L'IRSN recommande qu'EDF démontre, à échéance de la demande d'autorisation de mise en service de l'EPR-FA3, que les unités du PS-F1A affectées par un incendie passent en position de repli ou sont détruites, sans phase transitoire d'émission d'ordres erratiques.

Annexe à l'avis IRSN/2014-00240 du 18 juin 2014

Observations

Observation n°1

L'IRSN estime qu'EDF ne devrait pas seulement être informé des détails des tests effectués par le constructeur et de leurs résultats mais devrait également les approuver.

Observation n°2

L'IRSN estime qu'EDF devrait préciser que la maintenance préventive des unités du PS-F1A est autorisée uniquement dans les états E et F du réacteur.

Observation n°3

L'IRSN estime qu'EDF devrait qu'EDF devrait justifier que la défaillance unique d'une unité d'acquisition des positions de grappes (RPU) conduit au maximum à une mesure erronée mais considérée comme valide.

Observation n°4

L'IRSN estime que les tests complémentaires des réseaux de communications internes au PS-F1A, effectués sur sa version V1, devraient être effectués à nouveau sur la version utilisée au démarrage du réacteur EPR-FA3.

Observation n°5

L'IRSN estime que les évolutions suivantes devraient être intégrées au rapport de sûreté (RDS) :

- référencer explicitement les normes de la Commission Electrotechnique Internationale applicables au PS-F1A ;
- modifier le titre du sous-chapitre 7.3.1 pour ne pas le limiter à la seule architecture ;
- expliciter les cumuls de défaillance unique, de maintenance préventive, d'essai périodique et d'agression tolérés par le PS-F1A et les hypothèses nécessaires à cette tolérance ;
- justifier le choix de la fonction prioritaire pour les fonctions F1A ayant des actions antagonistes ;
- identifier les interfaces du PS-F1A, et non uniquement celles du PS ;
- intégrer les unités d'acquisition et de traitement des positions de grappes au PS, conformément à leur situation matérielle et logicielle, ou justifier le choix contraire ;
- décrire les exigences du PS vis-à-vis des systèmes supports autres que les alimentations électriques.