IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Avis DSR/2010-152

4 mai 2010

# Avis de l'IRSN sur la démonstration de sûreté de la plateforme SPPA-T2000

Par lettre du 21 avril 2010, l'Autorité de sûreté nucléaire (ASN) a demandé l'avis de l'IRSN :

- sur la recevabilité des éléments transmis par EDF concernant la plateforme SPPA-T2000, en réponse aux demandes formulées par l'ASN le 15 octobre 2009 ;
- sur la suffisance et l'aptitude des éléments de réponse relatifs aux parties de cette plateforme classées de sûreté F1B à satisfaire ces demandes.

Cet avis présente les conclusions de l'évaluation menée par l'IRSN pour répondre à ces deux questions.

EDF a prévu d'utiliser la plateforme SPPA-T2000 pour assurer des fonctions de conduite classées F2 (au Moyen de Conduite Principal, MCP) et implémenter des automatismes classés F2 et F1B, en particulier au Système d'Automatisme de Sûreté (SAS de tranche) classé F1B.
Les éléments de réponse transmis par EDF concernent d'une part le classement F2 des parties de la plateforme destinées à implémenter le MCP, et d'autre part le classement F1B des parties de la plateforme destinées à implémenter les automatismes.

En réponse à la première interrogation, pour ce qui concerne le classement F2 des parties de la plateforme destinées à implémenter le MCP, les documents transmis par EDF traitent les domaines techniques suivants :

- cartographie de la documentation de développement,
- conformité aux normes CEI 61513 et CEI 62138, dont les chapitres correspondant à la catégorie C de la CEI constituent les exigences de niveau F2 applicables à la plateforme ; justification d'aptitude des composants logiciels du commerce utilisés ; matrice de conformité aux normes,
- conformité du réseau Terminal Bus aux exigences F2,
- détection des dysfonctionnements du MCP (surveillance, signe de vie, intercomparaison avec le MCS),
- non-perturbation du MCP par les équipements non classés,
- conformité du MCP à une configuration validée.

L'IRSN estime que ces documents sont recevables au regard des demandes de l'ASN, pour les parties de la plateforme destinées à implémenter le MCP selon les exigences F2.

Pour répondre à la deuxième interrogation, concernant « *la suffisance et l'aptitude des éléments de réponse (d'EDF) relatifs aux parties de la plateforme SPPA-T2000 classées de sûreté F1B* », l'IRSN a réalisé une évaluation détaillée de ces éléments. Cette évaluation est présentée dans une annexe technique dont les conclusions sont reprises ci-après.
Les exigences de sûreté F1B comportent d'une part la conformité aux chapitres applicables des normes CEI 61513 et CEI 62138, et d'autre part la conformité à la RFS II.4.1.a.
Un effort considérable a été effectué depuis 2009 par EDF et par le constructeur pour identifier systématiquement la documentation du développement initial et la traduire en anglais, afin de démontrer la conformité aux normes CEI mentionnées ci-dessus.

L'IRSN considère que cette documentation (plus de cent documents techniques) est recevable (aspects traités, niveau de détail), ce qui complète la réponse positive à la première interrogation.
L'IRSN estime que cette documentation montre globalement une qualité adéquate de la conception de la plateforme, mais que le respect de toutes les exigences normatives en matière de vérification n'est pas prouvé à ce jour.
En effet, la plateforme ayant été développée conformément à un processus d'assurance qualité industriel et non selon les exigences nucléaires, cet effort a posteriori ne peut pallier les manques remontant à l'époque du développement initial, concernant en particulier la démonstration de suffisance de la vérification et de la validation. Ainsi, EDF n'a pas fourni la description détaillée des tests concernant les composants logiciels et leurs interactions dans le système complet, ni l'analyse de la couverture de ces tests.

La norme CEI 62138 permet de compenser ces lacunes par l'utilisation appropriée de moyens de démonstration complémentaires (test, retour d'expérience, certification). Ces moyens, employés par EDF, ne compensent pas les lacunes à ce jour ; en effet, leur mise en œuvre ne respecte pas complètement les exigences de cette norme destinées à garantir leur adéquation dans les conditions particulières visées, en l'occurrence celles de Flamanville 3, en termes de version des logiciels, de configuration et de sollicitation par les applications et par le procédé. Suite à la transmission du projet de l'annexe technique de cet avis, EDF a proposé de fournir des réponses aux points mentionnés par l'IRSN concernant la certification (dès à présent et en juillet 2010) et le retour d'expérience (au cours du second semestre 2010).

Au sujet de la conformité à la RFS II.4.1.a, l'IRSN estime correcte l'analyse d'EDF selon laquelle la démonstration de prédictibilité constitue dans le cas présent la seule exigence relative à la plateforme non couverte par les normes CEI 61513 et CEI 62138.
EDF a déduit des exigences fonctionnelles applicables au SAS de tranche que la prédictibilité correspond à l'existence d'une borne supérieure connue et convenable au temps de réponse. L'IRSN considère que cette approche est acceptable.
L'IRSN estime que le modèle de prédictibilité présenté en 2010 est clair et complet, qu'il prend en compte les facteurs influençant le temps de réponse et les modes non « normaux » demandés par l'IRSN, et que les constituants du temps de réponse sont analysés de façon suffisamment détaillée. Sa validité est toutefois limitée, formellement, par les lacunes en matière de documentation de vérification des composants de la plateforme mentionnées ci-avant.
Cependant, l'IRSN estime que la démonstration de prédictibilité, basée sur la documentation de conception, est acceptable.

En conclusion, concernant la première interrogation, les éléments fournis par EDF relatifs à la plateforme SPPA-T2000 sont recevables.
En réponse à la deuxième interrogation, l'effort considérable effectué pour démontrer la conformité aux exigences applicables des parties de la plateforme SPPA-T2000 classées de sûreté F1B n'a pas complètement abouti dans les délais fixés par l'ASN, mais a toutefois permis d'accroître la confiance placée dans leur conception et de démontrer leur prédictibilité.
L'IRSN estime donc que la plateforme SPPA-T2000 peut être utilisée pour réaliser le SAS de tranche de Flamanville 3, à condition d'être secourue au titre de la robustesse par un moyen basé sur une plateforme conforme aux exigences nucléaires, tel que l'extension de « noyau dur » sous réserve d'une évaluation détaillée de son adéquation fonctionnelle.