

DIRECTION DES CENTRALES NUCLEAIRES

Paris, le 4 avril 2012

Réf. : CODEP-DCN-2011-052544

Monsieur le Directeur
Division Production Nucléaire
EDF
Site Cap Ampère – 1 place Pleyel
93 282 SAINT-DENIS CEDEX

Objet : Réacteurs nucléaires à eau sous pression – Projet EPR – Flamanville 3
Architecture du contrôle-commande et plates-formes associées

Réf. : [1] Lettre ASN Dép-SD2/N°0171/2006 du 27 mars 2006
[2] Lettre ASN Dép-DCN-0568-2009 du 15 octobre 2009
[3] Lettre ASN CODEP-DCN-2010-036901 du 9 juillet 2010
[4] Lettre EDF/DIN du 23 décembre 2009 du Directeur de la DIN
[5] Lettre ASN CODEP-DCN-2011-035230 du 10 juin 2011
[6] Avis GPR CODEP-MEA-2011-038333 du 8 juillet 2011
[7] Lettre EDF ECEP111402 du 10 juin 2011

Monsieur le Directeur,

En amont de la délivrance du décret d'autorisation de création n°2007-534 du réacteur Flamanville 3 (FLA3) de type EPR, le Groupe permanent d'experts pour les réacteurs nucléaires (GPR) s'est réuni le 1^{er} décembre 2005 afin d'examiner les principes généraux retenus pour l'architecture générale du contrôle-commande qui comprend deux plates-formes associées :

- la plate-forme appelée « Téléperm XS » (TXS) développée spécifiquement pour l'industrie nucléaire et dédiée notamment aux fonctions de protection du réacteur en situations d'incidents ou d'accidents ;
- la plate-forme appelée « SPPA T2000 » développée pour l'industrie conventionnelle et utilisée notamment pour des fonctions liées au fonctionnement normal du réacteur et pour certaines fonctions de protection du réacteur en situations d'incidents ou d'accidents.

A cette occasion, le GPR a également examiné l'architecture du système de protection et de la plate-forme TXS. A l'issue de cette réunion, l'ASN a considéré, par lettre en référence [1], que le choix de la plate-forme TXS pour le réacteur EPR de Flamanville 3 constituait une base acceptable pour le développement du système de protection du réacteur.

Le 18 juin 2009, le GPR s'est réuni afin de se prononcer sur les choix de conception détaillée retenus par EDF pour la définition et la mise en œuvre de l'architecture du contrôle-commande du réacteur EPR de Flamanville 3. A l'issue de cette réunion, l'ASN a pris position par lettre en référence [2] sur l'architecture du contrôle commande et sur l'aptitude des plates-formes TXS et SPPA T2000 à accueillir des fonctions classées de sûreté :

- s'agissant de la plate-forme TXS, l'ASN a considéré que sa conception était satisfaisante et permettait d'accueillir des fonctions de sûreté de classement F1A ;
- en revanche, l'ASN a considéré que la conformité au classement de sûreté de la plate-forme SPPA T2000 n'était pas démontrée et vous a demandé de définir des dispositions de conception différentes de celles initialement présentées par EDF.

L'instruction de la capacité de la plate-forme SPPA T2000 à accueillir les fonctions de sûreté de classement F2¹ et F1B² s'est poursuivie en 2010. Par lettre en référence [3], l'ASN a considéré que les documents que vous avez transmis contenaient les éléments nécessaires pour démontrer la capacité de la plateforme SPPA-T2000 à accueillir des fonctions de sûreté classées F2, même si ces éléments restaient à analyser de manière plus détaillée. L'ASN a en revanche estimé que la démonstration de la capacité de la plate-forme à accueillir des fonctions de sûreté classées F1B n'était pas acquise. L'ASN vous a ainsi demandé de mettre en œuvre les « dispositions de conception différentes » proposées dans le courrier en référence [4].

Celles-ci vous ont amené à développer le système dénommé « noyau dur », destiné à faire face à la situation de perte totale de la plateforme SPPA-T2000 cumulée à certaines situations accidentelles. Ce dispositif s'est notamment traduit par l'introduction, au sein de la plateforme TXS, d'un système dénommé « contrôle-commande noyau dur » (CCND), qui regroupe certaines fonctions classées de sûreté jusqu'alors non implantées sur la plate-forme TXS.

*

A la suite du courrier en référence [2], l'ASN a demandé par courrier en référence [5] au GPR d'examiner la qualification de la plateforme de contrôle-commande SPPA-T2000 du réacteur EPR de Flamanville 3 et son impact sur le noyau dur.

Le GPR a ainsi examiné, sur la base d'un rapport d'expertise préparé par l'IRSN à la demande de l'ASN, les questions relatives :

- à la capacité des automates AS620B de la plateforme SPPA-T2000 à accueillir des fonctions de sûreté de classement F1B et F2,
- à la nécessité d'attribuer ou non un classement de sûreté au noyau dur, compte tenu des conclusions apportées au point précédent,
- au bilan des avantages et des inconvénients de la mise en place du noyau dur au sein de l'architecture du contrôle commande,
- à l'examen des réponses d'EDF aux demandes de l'ASN formulées par lettre en référence [2] et relatives :
 - au dispositif de validation des commandes du moyen de conduite principal (MCP) transmises au système de protection,
 - à la détection des défaillances du MCP,
 - à la conformité du MCP à une configuration validée,

¹ Selon le rapport préliminaire de sûreté de Flamanville 3 : « Les fonctions de sûreté nécessaires pour atteindre et maintenir un état final pour les séquences d'événements RCC-A sont classées F2 »

² Selon le rapport préliminaire de sûreté de Flamanville 3 : « Toutes les fonctions de sûreté nécessaires au-delà de l'atteinte de l'état contrôlé pour atteindre l'état d'arrêt sûr et pour le maintenir après un événement interne PCC-2 à PCC-4 sont classées F1B. »

- o à l'absence de perturbation du MCP, du terminal bus et du système d'automatisme de sûreté (SAS) par des équipements d'un niveau de classement moindre.

*

* *

Le GPR a rendu à l'ASN son avis en référence [6] à l'issue de la réunion qui s'est tenue le 16 juin 2011.

*

Position de l'ASN

L'ASN estime que les éléments de réponse apportés par EDF concernant, d'une part, la conformité des automates AS620B de la plateforme de contrôle-commande SPPA-T2000 aux exigences techniques associées au niveau de classement F1B et, d'autre part, les demandes formulées dans la lettre en référence [2], sont satisfaisants.

Dans ces conditions, l'ASN estime que les automates AS620B de la plateforme SPPA-T2000 sont aptes à accueillir des fonctions classées F1B et a fortiori F2.

Sous réserve de la prise en compte de la demande formulée dans le présent courrier, l'ASN estime qu'il n'est pas nécessaire, à ce titre, d'imposer une exigence de classement au noyau dur, qui constitue une disposition de robustesse complémentaire relevant de la défense en profondeur. L'ASN attire votre attention sur le fait que la nécessité de classement du système CCND fera l'objet d'une nouvelle évaluation à l'issue de l'analyse fonctionnelle qui doit être menée ultérieurement.

L'ajout d'un système de secours tel que le système CCND accroît la tolérance de l'architecture du contrôle-commande à certaines défaillances du SAS tout en complexifiant l'architecture du contrôle-commande du réacteur EPR de Flamanville 3 ; toutefois, l'ASN estime que les avantages de l'introduction du système CCND, et donc du noyau dur, sont prépondérants.

L'ASN estime que le principe du dispositif de validation des commandes transmises par le MCP au système de protection est acceptable.

L'ASN estime que les dispositions de conception et d'installation (fonctions de chargement et de contrôle de conformité des logiciels applicatifs) proposées par EDF pour garantir la conformité du MCP à une configuration validée sont satisfaisantes.

*

Demande de l'ASN

Le noyau dur comprend un ensemble restreint de fonctions permettant de faire face au cumul d'un incident ou d'un accident avec la perte totale des fonctions classées F1B réalisées par la plateforme SPPA-T2000. Il est constitué du système de protection (PS), du système de contrôle, de surveillance et de limitation du réacteur (RCSL), du système de contrôle-commande accidents graves (CCAG) et du système dédié de contrôle-commande noyau dur (CCND).

Vous avez précisé lors de l'instruction que le noyau dur ne nécessite pas de classement fonctionnel de sûreté car il est destiné à accroître la tolérance de l'architecture de contrôle-commande à des cumuls de défaillances supplémentaires par rapport à ceux postulés dans la démonstration de sûreté déterministe ou à prendre en compte au titre des études probabilistes de sûreté. L'ASN considère néanmoins que le noyau dur doit faire l'objet d'un ensemble de disposition de maintenance et d'essais, afin de garantir la pérennité des fonctions qu'il assure au long de l'exploitation.

L'ASN vous demande de prendre des dispositions pour garantir la pérennité du noyau dur en formalisant son existence et les exigences qui lui sont applicables, notamment en termes de maintenance et d'essais en exploitation, dans les documents de conception et dans le rapport de sûreté.

*

Observation de l'ASN

L'ASN a pris note de vos engagements à fournir les éléments et à réaliser les actions formulés par lettre en référence [7].

*

Vous voudrez bien me faire part de vos observations et réponses concernant ces points dans un délai qui n'excèdera pas deux mois.

Par ailleurs, je vous informe que l'ASN a partagé ses conclusions lors d'une réunion du MDEP en janvier 2012, notamment avec les Autorités de sûreté américaine (NRC), britannique (ONR), et finlandaise (STUK).

Je vous prie d'agréer, Monsieur le Directeur, l'expression de ma considération distinguée.

Le Directeur général,

Jean Christophe NIEL