RÉPUBLIQUE FRANÇAISE

AUTORITÉ DE SÛRETÉ NUCLÉAIRE

DIRECTION DES CENTRALES NUCLEAIRES

Paris, le 15 octobre 2009

Réf. : Dép-DCN-0568-2009

EDF – Monsieur le directeur
de la division ingénierie nucléaire
Site Cap Ampère
1, place Pleyel
93282 SAINT DENIS CEDEX

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

Réf. : [1] Lettre DEP-DCN-0021-2009 du 15 janvier 2009
[2] Avis du GPR réf. DEP-MEA-0119-2009 du 17 juillet 2009
[3] Lettre DEP-DCN-0028-2008 du 8 février 2008

Monsieur le directeur,

Comme annoncé dans la lettre citée en référence [1], le groupe permanent d'experts pour les réacteurs nucléaires (GPR) s'est réuni à la demande de l'ASN 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.

Le GPR a ainsi examiné :

- la robustesse de l'architecture du contrôle-commande considérée dans son ensemble, en particulier la déclinaison du principe de défense en profondeur et les dispositions d'indépendance retenues ;
- l'aptitude des réseaux et des automates de la plateforme Téléperm XS à accueillir des fonctions de sûreté classées au niveau F1A ;
- l'aptitude des réseaux et des automates de la plateforme SPPA T2000 à accueillir des fonctions de sûreté classées aux niveaux F1B et F2 ;
- le processus de réalisation du contrôle-commande ;
- l'étendue des moyens de conduite permettant de pallier la perte de certaines parties du contrôle-commande ;
- la qualification et la fiabilité des matériels des plateformes Téléperm XS et SPPA T2000 ;
- la diversité entre ces deux plateformes.

Le GPR a reçu une information sur les architectures de contrôle-commande retenues dans différents projets de réacteurs EPR en cours de construction ou envisagés à l'étranger.

Le GPR a rendu son avis en référence [2] à l'issue de la réunion du 18 juin 2009.

L'ASN estime que la démonstration de sûreté repose sur la capacité de l'ensemble du contrôle-commande à assurer intégralement et fidèlement les performances dont la nécessité est précisée par l'analyse fonctionnelle du réacteur et dont la faisabilité est démontrée pour toutes les actions humaines impliquées.

A cette fin, l'ASN considère qu'EDF doit :

- justifier la conformité de chaque élément de la solution technologique retenue, et notamment de chacune des deux plateformes, aux exigences de conception correspondant au classement de sûreté;
- assurer la robustesse de l'architecture d'ensemble du contrôle-commande pour ne pas faire reposer la démonstration de sûreté sur un système de contrôle-commande unique ou un type unique de composant complexe.

Plateformes de contrôle-commande

L'ASN note qu'EDF a apporté les éléments nécessaires pour compléter sa démonstration de l'aptitude de la plateforme Téléperm XS à accueillir des fonctions classées F1A.

L'ASN estime que la diversité technologique des deux plateformes Téléperm XS et SPPA T2000 - élément important de la robustesse de l'architecture - est satisfaisante.

En revanche, l'ASN constate que la conformité au classement de sûreté de la plateforme SPPA T2000 n'est pas démontrée à ce jour, tant pour la partie afférente aux automatismes qui doit assurer des fonctions de sûreté classées au niveau F1B et F2 que pour la partie afférente à la conduite qui doit assurer des fonctions de sûreté classées au niveau F2.

La plateforme SPPA T2000 n'ayant pas été conçue spécifiquement pour assurer des fonctions de sûreté nucléaire, une « preuve par l'analyse » doit être apportée pour garantir a posteriori l'atteinte des objectifs de sûreté qui lui sont assignés. Cette preuve apparaît particulièrement critique pour cette plate-forme constitutive du moyen de conduite principal, qui utilise de nombreux logiciels industriels et commerciaux et généralise les communications bidirectionnelles par réseaux, entre eux et avec des équipements de classements de sûreté différents.

Architecture du contrôle-commande

L'ASN constate la complexité de l'architecture proposée par EDF qui, par une utilisation étendue de réseaux informatiques, relie entre eux des systèmes appartenant à des classes de sûreté ou des niveaux de défense en profondeur différents. Dans ces conditions, l'ASN considère nécessaire l'introduction d'éléments de robustesse supplémentaires, suffisamment complets et reposant sur des équipements d'un niveau de confiance adéquat.

La complexité de l'architecture proposée par EDF rend difficile l'élaboration d'une démonstration de sûreté satisfaisante. Compte tenu, d'une part de cette complexité et de cette difficulté, d'autre part de l'importance du contrôle-commande pour la sûreté du réacteur, l'ASN estime que l'acceptabilité du contrôle-commande proposé par EDF est subordonnée à :

- la prise en compte effective des évolutions demandées dans l'annexe 1 ;
- la fourniture de l'ensemble des justifications complémentaires demandées dans l'annexe 2 ;
- la réalisation des actions que vous avez prévu d'effectuer pour améliorer et justifier la robustesse du contrôle-commande.

L'analyse de ces éléments par l'ASN et son appui technique constitue un préalable à l'examen de la recevabilité de votre future demande de mise en service du réacteur EPR de Flamanville 3. Cette analyse se fondera essentiellement sur le respect des principes de sûreté rappelés en annexe 3, et qui vous avaient été communiqués par lettre citée en référence [3]. Elle prendra en considération les positions exprimées par les Autorités de sûreté d'autres pays, avec lesquelles l'ASN est en contact étroit.

Compte tenu de l'ampleur et de la complexité des démonstrations restant à fournir pour justifier le respect de ces principes, l'ASN estime que la certitude d'aboutir *in fine* à une démonstration de sûreté acceptable fondée sur l'architecture actuellement prévue n'est pas acquise. C'est pourquoi, outre les efforts que vous poursuivez pour justifier la conception proposée, il vous appartient d'examiner dès à présent des dispositions de conception différentes, notamment pour faire face au cas où les démonstrations de sûreté relatives au classement de la plateforme SPPA T2000 et des réseaux de communication ne seraient pas acceptables. Vous présenterez à l'ASN les principales orientations envisageables pour fin 2009.

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

Le directeur général,

Jean-Christophe NIEL

LISTE DE DIFFUSION

Copies externes :

- Groupe permanent d'experts pour les réacteurs nucléaires /M. le président
- IRSN/DSR
- IRSN/DSR/SAMS
- IRSN/DSDRE
- IRSN/DG
- EDF/DIN
- EDF/DPN

Copies internes :

- ASN : MM. les membres du collège de l'ASN
- ASN/DG : J-C. Niel ; O. Gupta
- ASN/Division territoriale de Caen
- ASN/DCN : G. Wack ; S. Peiro ; F. Ménage ; S. Petit
- MEA : Secrétariat des GPE

Demandes d'évolution de l'architecture

A. Défense en profondeur

A.1. Conduite des situations de fonctionnement RRC-A et RRC-B (niveau 2 du contrôle-commande)

L'ASN rappelle que les situations de fonctionnement RRC-A et RRC-B, même hautement improbables, sont pleinement intégrées dans la démonstration de sûreté que vous devez produire pour Flamanville 3.

L'ASN constate que, dans la conception actuelle du contrôle-commande, le moyen de conduite principal (MCP) constitue l'unique moyen de conduite de ces situations de fonctionnement, ce qui n'est pas acceptable au titre du respect du principe de défense en profondeur.

Demande n° 1	**L'ASN vous demande de diversifier les moyens de conduite des situations de fonctionnement RRC-A et RRC-B. A ce titre, vous examinerez quelles sont les fonctions nécessaires à la conduite de ces situations de fonctionnement qui doivent être également disponibles au MCS (ou sur la platine accidents graves pour ce qui concerne certaines situations RRC-B). Vous transmettrez la solution retenue et les justifications associées avant juin 2010.**

B. Robustesse de l'architecture du contrôle-commande de Flamanville 3

B.1. Plate-forme de contrôle-commande SPPA T2000 - Conception du système SAS

L'ASN constate que l'analyse détaillée de la conception du système SAS a révélé que le classement sismique de fonctions a structuré en grande partie la définition de l'architecture de ce système.

Cette approche vous a donc conduit à regrouper au sein du même calculateur SAS des fonctions de classement différent F1B et F2 au seul motif du classement au séisme de ces fonctions classées F2.

L'ASN constate que ce choix structurant du développement du système SAS constitue un écart par rapport à l'approche préconisée par la norme CEI 61513, pour laquelle le classement de sûreté F1B des fonctions portées par le système SAS doit constituer la base structurante de sa conception pour en limiter la complexité.

Demande n° 2	**L'ASN vous demande de limiter, voire supprimer, la présence de fonctions de classement inférieur à F1B dans le système SAS. Toute intégration d'une fonction de classement inférieur à F1B devra être identifiée et justifiée en termes de sûreté. Vous transmettrez la solution retenue et les justifications associées avant juin 2010.**

B.2. Renforcement des dispositions de « noyau dur » au sein de la plate-forme Téléperm XS (niveau 1 du contrôle-commande)

L'ASN considère que l'architecture du contrôle-commande du réacteur EPR doit être robuste à l'égard de la défaillance totale de la plateforme SPPA T2000, et ceci pour l'ensemble des conditions de fonctionnement retenues dans la démonstration de sûreté.

Demande n° 3	**L'ASN vous demande d'une part d'étendre les dispositions dites de « noyau dur » mises en place au sein de la plate-forme de contrôle-commande Téléperm XS aux situations RRC-A (hormis celles impliquant la défaillance d'une fonction classée F1 allouée au système de protection PS), d'autre part de réaliser une analyse approfondie de l'ensemble des situations de fonctionnement PCC et RRC-A afin de définir la stratégie de conduite associée à ces dispositions (moyens de détection de la perte de la plateforme SSPA T2000, critères d'initiation des actions "noyau dur " associées, état sûr visé). Vous transmettrez la solution retenue et les justifications associées avant juin 2010.**

B.3. Mise en œuvre de fonctions classées de sûreté F1A ou F1B au moyen de conduite principal MCP

L'ASN constate que la stratégie commune à toutes les fonctions pilotées par l'opérateur consiste à utiliser de manière préférentielle le moyen de conduite principal MCP, classé de sûreté F2, pour conduire toutes les situations de fonctionnement, tant que celui-ci est jugé disponible ou que ses erreurs ou défaillances ne sont pas détectées.

Dans diverses situations de fonctionnement du réacteur, l'ASN constate que l'opérateur peut inhiber ou activer certaines fonctions classées de sûreté F1A du système de protection PS à partir du MCP. Cette disposition génère le risque qu'un dysfonctionnement d'une fonction de sûreté classée F2 provoque un dysfonctionnement d'une fonction de sûreté classée F1A.

Demande n° 4	**L'ASN vous demande de réaliser un dispositif de validation des commandes qui inhibent ou permettent l'activation des fonctions F1A du système de protection par un moyen câblé totalement indépendant du MCP. Vous transmettrez la solution retenue et les justifications associées avant juin 2010.**

La norme CEI 61513 précise que les systèmes doivent être conçus de telle manière que les erreurs et défaillances soient détectées suffisamment tôt pour assurer la disponibilité requise pour le système.

L'ASN constate que, à ce stade de conception du MCP, la couverture des autotests, ainsi que l'étude des conséquences des défaillances matérielles et des erreurs logicielles du MCP, ne garantissent pas le respect des exigences de la norme CEI 61513 rappelées précédemment.

Demande n° 5	**L'ASN vous demande de mettre en œuvre un moyen classé F1B permettant de détecter avec une fiabilité suffisante les erreurs et défaillances du MCP afin d'indiquer aux opérateurs la nécessité de conduire le réacteur à partir du MCS. Les dispositions architecturales retenues, notamment fondées sur une extension du signe de vie et sur l'autosurveillance du MCP, ainsi que leur déclinaison dans les procédures de conduite du réacteur, seront présentées et justifiées avant juin 2010.**

C. Défense en profondeur

C.1. Conduite des situations de fonctionnement RRC-A et RRC-B

L'ASN considère que l'ensemble des dispositions architecturales et matérielles du contrôle-commande permettant de faire face aux situations de fonctionnement RRC-A et RRC-B, doivent bénéficier d'un niveau de confiance élevé à la conception.

Demande n° 6	**A ce titre, l'ASN vous demande, avant juin 2010, de préciser les moyens mis à la disposition de l'exploitant en situation de fonctionnement RRC-B en cas de perte totale de la plate-forme de contrôle-commande SPPA T2000. Vous vous prononcerez également sur l'intérêt ou non de les étendre, en justifiant votre position.**

Demandes de justifications complémentaires

D. Indépendance des fonctions de contrôle-commande de classement différent

La norme CEI 61513 précise que la conception du système doit garantir que les exigences des sous-systèmes ou équipements des classes supérieures sont remplies, même en cas de défaillance d'équipements de classes inférieures.

D.1. Moyen de conduite principal MCP et Terminal Bus

L'ASN constate que le MCP et le réseau Terminal Bus, tous deux classés de sûreté F2, sont connectés en permanence d'une part, à des équipements non classés de sûreté dont ils reçoivent des informations et des commandes, d'autre part au niveau 3 du contrôle-commande par l'intermédiaire de stations d'ingénierie. Par ailleurs, les systèmes de défense actuellement prévus, du type verrouillage logiciel ou pare-feu, ne sont implantés que dans des équipements non classés de sûreté et ne permettent donc pas de garantir le bon fonctionnement du MCP et du Terminal Bus en cas de transmission d'informations ou commandes correctement formatées mais fonctionnellement erronées.

L'ASN constate que l'absence de systèmes de défense interne classés de sûreté F2 au sein du MCP et du Terminal Bus ne permet pas de respecter les exigences de la norme CEI 61513 rappelées précédemment.

Demande n° 7	**Afin de limiter les possibilités de perturbation du MCP et du «Terminal bus» classés de sûreté F2 par des équipements non classés de sûreté, l'ASN vous demande de mettre en place un processus permettant de vérifier qu'après chaque connexion d'une station d'ingénierie, l'état de chaque calculateur du MCP est conforme à la configuration globale validée. Vous présenterez ces éléments au plus tard en janvier 2010.**

Demande n° 8	**L'ASN vous demande de démontrer que les autres équipements non classés de sûreté connectés au Terminal Bus ne permettent pas de reprogrammer, reconfigurer, ou de changer le mode de fonctionnement des calculateurs classés F2 du MCP. Vous présenterez cette démonstration au plus tard en janvier 2010.**

D.2. Plate-forme de contrôle-commande SPPA T2000 - Système d'automatisme de sûreté SAS

L'ASN constate que les automates classés de sûreté F1B du système SAS sont connectés en permanence par réseau à des systèmes de classement inférieur F2 ou non classés.

Par ailleurs, les automates classés de sûreté F2 du système SAS, assurant les fonctions dédiées aux situations de fonctionnement du réacteur RRC-B, sont également connectés en permanence par réseau à des systèmes de classement inférieur non classés.

Aussi, considérant les constats relatifs au MCP et au Terminal Bus présentés au § D.1, l'ASN constate que la démonstration du respect des exigences de la norme CEI 61513 rappelées précédemment n'a toujours pas été produite.

Demande n° 9	**L'ASN vous demande de démontrer que la conception de la partie du SAS classée F1B permet de garantir le respect des exigences de sûreté associées à ce système, même en cas de défaillance d'équipements de classement inférieur. Vous présenterez ces éléments au plus tard en juin 2010.**

Demande n° 10	**L'ASN vous demande de démontrer que la conception de la partie du SAS assurant les fonctions dédiées aux situations de fonctionnement du réacteur RRC-B, classée F2, permet de garantir le respect des exigences de sûreté associées à ce système, même en cas de défaillance d'équipements de classement inférieur. Vous présenterez ces éléments au plus tard en juin 2010.**

D.3. Plate-forme de contrôle-commande SPPA T2000 - Prédictibilité du comportement du système SAS

La règle fondamentale de sûreté II.4.1.a relative aux logiciels des systèmes électriques classés de sûreté requiert une validation du modèle de comportement du système SAS, tenant compte notamment de la conception détaillée et de toutes les situations de fonctionnement pouvant être rencontrées. Cette validation comporte en particulier une démonstration de prédictibilité.

Demande n° 11	**L'ASN vous demande d'inclure dans la démonstration de prédictibilité du système SAS classé F1B, en sus de la prédictibilité du temps de réponse, toutes ses situations de fonctionnement résultant des variations du procédé, des demandes issues des équipements auxquels il est connecté et de tous ses traitements internes. Vous présenterez ces éléments au plus tard en janvier 2010.**

Démarche d'examen

Dans sa démarche d'examen du contrôle-commande du réacteur EPR de Flamanville 3, l'ASN veille notamment au respect des principes suivants :

- d'une façon générale, le principe de défense en profondeur doit guider l'élaboration de l'architecture générale du contrôle-commande afin d'asseoir la démonstration de sûreté et de garantir son maintien lors d'évolutions ultérieures ;
- les fonctions intervenant dans les différents niveaux de la défense en profondeur doivent être indépendantes ;
- l'indépendance doit être déclinée selon les aspects physiques, logiques et technologiques. Elle doit être justifiée par des dispositions telles que la ségrégation, l'isolement, l'autonomie, la diversification ; des dispositions doivent être mises en place pour minimiser les possibilités de défaillances de cause commune en particulier logicielles et de propagation des défaillances par les réseaux de communication.