GROUPE PERMANENT D'EXPERTS

POUR LES REACTEURS NUCLEAIRES

Avis

relatif à l'examen de l'architecture générale du contrôle-commande du réacteur EPR Flamanville 3 et des plateformes associées

18 juin 2009

Réunion tenue à Paris le 18/06/2009

I

Conformément à la demande du Président de l'Autorité de sûreté nucléaire, par sa lettre ASN DEP – DCN – 0021 – 2009 du 15 janvier 2009, le Groupe permanent d'experts pour les réacteurs nucléaires s'est réuni le 18 juin 2009 pour examiner l'architecture générale du contrôle-commande du réacteur EPR Flamanville 3 et les plateformes retenues pour sa mise en œuvre. En complément, le Groupe permanent a été informé des dispositions retenues ou envisagées pour l'architecture de contrôle-commande dans différents projets de réacteur EPR en cours de construction ou en définition à l'étranger.

Au cours de l'instruction technique, l'exploitant a pris un certain nombre d'engagements complémentaires à son dossier initial, transmis à l'Autorité de Sûreté Nucléaire.

II

Le Groupe permanent a pris connaissance de l'analyse, par l'Institut de radioprotection et de sûreté nucléaire (IRSN), des dispositions prises ou prévues par Electricité de France pour permettre au contrôle-commande du réacteur EPR de Flamanville 3 de répondre aux objectifs de sûreté correspondants, tant pour ce qui concerne son architecture générale que ses équipements principaux (c'est-à-dire les deux plateformes retenues).

Le Groupe permanent a notamment entendu les conclusions de l'IRSN sur les sujets suivants :

- 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 calculateurs de conduite de la plateforme SPPA T2000 à accueillir des fonctions classées F2,
- l'aptitude des réseaux et automates de la plateforme SPPA T2000 à accueillir des fonctions classées F1B,
- l'aptitude des réseaux et automates de la plateforme Teleperm XS à accueillir des fonctions classées F1A (en complément de l'examen lors des réunions du 1er juillet 2004 et du 1er décembre 2005),
- 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 Teleperm XS et SPPA T2000,
- la diversité entre ces deux plateformes,
- un éclairage sur les architectures de contrôle-commande retenues dans différents projets de réacteurs EPR en cours de construction ou envisagés à l'étranger.

III

Le Groupe permanent considère que la démonstration de sûreté passe par la capacité de l'ensemble du contrôle-commande à réaliser intégralement et fidèlement les performances dont la nécessité est indiquée par l'analyse fonctionnelle de la tranche et dont la faisabilité est démontrée pour toutes les actions humaines impliquées.

A cette fin, le contrôle-commande proposé par Electricité de France doit reposer notamment sur les deux dispositions suivantes :

- 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;
- 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 CONTROLE-COMMANDE

Le Groupe permanent note que, depuis la réunion du 1er décembre 2005, l'exploitant a apporté les éléments nécessaires pour compléter sa démonstration de l'aptitude de la plateforme Teleperm XS à accueillir des fonctions classées F1A.

En revanche, le Groupe permanent note que la conformité au classement de sûreté de la plateforme SPPA T2000 n'est pas démontrée à ce jour tant pour la partie automatismes qui doit assurer des fonctions classées F1B que pour la partie conduite qui doit assurer des fonctions classées F2 et que l'exploitant s'est engagé à apporter des justifications complémentaires à ce sujet. Le Groupe permanent souligne à ce sujet l'importance de la démonstration. 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.

Le Groupe permanent estime que, pour atteindre ces objectifs, l'exploitant devra notamment étayer son analyse détaillée du fonctionnement et de la documentation de la plateforme par une démonstration point par point de la conformité de chacun des composants de cette plateforme :

- aux préconisations des normes internationales CEI 62138 et CEI 61513 ainsi qu'à la RFS II.4.1a (RFS « logiciels ») pour la partie de la plateforme devant réaliser des fonctions classées F1B ;
- aux préconisations des normes internationales CEI 62138 et CEI 61513 pour la partie de la plateforme devant réaliser des fonctions classées F2.

Cette démonstration apparaît particulièrement importante pour les calculateurs du moyen de conduite principal, qui utilisent de nombreux logiciels industriels et commerciaux non développés dans une optique de sûreté, et généralisent les communications bidirectionnelles par réseaux, entre eux et avec des équipements de classements différents. Elle devra être maintenue dans le temps en tenant compte du cycle de vie des constituants logiciels prédéveloppés du moyen de conduite principal (MCP).

Le Groupe permanent estime par ailleurs que la diversité technologique des deux plateformes Teleperm XS et SPPA T2000 - élément important de la robustesse de l'architecture - est satisfaisante bien que ces deux équipements partagent une certaine proximité en termes d'historique industriel.

ARCHITECTURE GENERALE DU CONTROLE-COMMANDE

Le Groupe permanent souligne la complexité de l'architecture proposée par l'exploitant 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, le Groupe permanent considère nécessaire l'introduction d'éléments de robustesse supplémentaires suffisamment complets et reposant sur des équipements d'un niveau de confiance adéquat, qui font l'objet des recommandations jointes.

ARCHITECTURES DE CONTROLE-COMMANDE RETENUES POUR LES PROJETS DE REACTEUR EPR ENVISAGES A L'ETRANGER

Le Groupe permanent note que les différences d'architecture constatées entre le projet FA3 et les réacteurs EPR en cours de construction ou de définition à l'étranger sont principalement associées à des contextes réglementaire et industriel différents.

Dans tous les cas des dispositions complémentaires ont été apportées à la conception de base. Les dispositions retenues ou envisagées n'apportent toutefois pas à ce jour de solution évidente répondant à l'ensemble des questions soulevées par l'analyse détaillée de Flamanville 3.

IV

En conclusion, le groupe permanent souligne que l'architecture proposée par EDF pour le contrôle-commande de l'EPR Flamanville 3 est complexe. Elle nécessite en tout état de cause la mise en œuvre de dispositions de robustesse complémentaires.

Le Groupe permanent souligne que les engagements pris par l'exploitant représentent un travail important à réaliser maintenant dans des délais très courts.

Recommandations

Plateforme de contrôle-commande SPPA T2000

Recommandation 1

Afin de limiter les possibilités de perturbation du MCP et du «Terminal bus» classés F2 par des équipements non classés, le Groupe permanent recommande que :

- après chaque connexion d'une station d'ingénierie, EDF vérifie que l'état de chaque calculateur du MCP est conforme à la configuration globale validée ;
- EDF démontre que les autres équipements non classés connectés au Terminal bus ne permettent pas de reprogrammer, reconfigurer, ou de changer le mode de fonctionnement des calculateurs F2 du MCP.

EDF présentera la solution retenue et les justifications d'ici janvier 2010.

Recommandation 2

Le Groupe permanent recommande que la conception du SAS F1B garantisse que les exigences de ce système soient remplies même en cas de défaillance d'équipements moins classés.
EDF présentera la solution retenue et les justifications sous un an.

Recommandation 3

Le Groupe permanent recommande que la conception du SAS RRC-B garantisse que les exigences de ce système soient remplies même en cas de défaillance d'équipements moins classés.
EDF présentera la solution retenue et les justifications sous un an.

Recommandation 4

Le Groupe permanent recommande qu'EDF inclue dans la démonstration de prédictibilité du SAS F1B, y compris la prédictibilité du temps de réponse, toutes les situations de fonctionnement résultant des variations du procédé, des demandes issues des équipements auxquels il est connecté et de tous ses traitements internes.
EDF présentera la solution retenue et les justifications d'ici janvier 2010.

Dispositions de robustesse de l'architecture de contrôle-commande

Recommandation 5

Le Groupe permanent considère que l'architecture du contrôle-commande du réacteur EPR doit être robuste vis-à-vis de la défaillance totale de la plateforme SPPA T2000 pour l'ensemble des conditions de fonctionnement retenues dans la démonstration de sûreté. A ce titre, il recommande que, sous un an, EDF étudie la couverture des situations RRC-A par le noyau dur actuel et évalue l'intérêt de l'étendre si nécessaire.

Recommandation 6

Le Groupe permanent recommande que le MCP ne constitue pas l'unique moyen de conduite de la tranche dans les situations RRC-A et RRC-B et donc qu'EDF examine quelles sont les fonctions nécessaires à la conduite de ces situations qui devraient être également disponibles au MCS (ou sur la platine accidents graves pour ce qui concerne certaines situations RRC-B).
EDF présentera la solution retenue et les justifications sous 1 an.

Recommandation 7

Le Groupe permanent recommande qu'EDF réalise 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.
EDF présentera la solution retenue et les justifications sous 1 an.

Recommandation 8

Le Groupe permanent considère que les dispositions relatives aux conditions de fonctionnement RRC-B, qui font partie intégrante de la démonstration de sûreté sur le réacteur EPR et qui constituent l'ultime ligne de défense, doivent être conçues de manière à bénéficier d'un niveau de confiance élevé.
A ce titre, il recommande qu'EDF précise les moyens à la disposition de l'exploitant en situation RRC-B en cas de perte totale du SPPA T2000 et se prononce sur l'intérêt de les étendre.
EDF présentera la solution retenue et les justifications sous 1 an.