AUTORITÉ DE SÛRETÉ NUCLÉAIRE
Direction des centrales nucléaires

RÉPUBLIQUE FRANÇAISE

Référence courrier :
CODEP-DCN-2023-010746
Affaire suivie par :
Tél. :
Courriel :

Monsieur le Directeur du projet Flamanville 3
EDF/DIPNN/Direction du projet Flamanville 3
97 avenue Pierre Brossolette
92120 Montrouge cedex

Montrouge, le 4 avril 2023

Objet : Réacteur EPR de Flamanville 3
Thème : Développement du système de protection
Références : cf. annexe 2

Monsieur le Directeur,

Le système de protection est un système de contrôle commande essentiel pour la gestion des situations incidentelles et accidentelles. En effet, ce système, hébergé sur la plateforme Teleperm-XS (TXS) assure notamment les fonctions nécessaires à l'atteinte de l'état contrôlé, et certaines fonctions permettant d'atteindre l'état sûr ou final. Ainsi, conformément aux Directives Techniques en référence [1], le concepteur a mis en place des règles concernant le développement du logiciel de ce système de contrôle commande, recensées dans le plan qualité en référence [2]. Le développement du logiciel comporte les activités de conception, mais également les activités de vérification et de validation (V&V).

Depuis 2005, l'ASN a sollicité à plusieurs reprises le groupe permanent d'experts pour les réacteurs et l'IRSN pour les réacteurs nucléaires, afin notamment d'avoir leur avis sur le plan qualité et les versions alors en vigueur [3], [4] et [5].

Compte tenu des mises à jour successives du contrôle commande depuis le dernier examen du système de protection et des conclusions des inspections en référence [6] et [7], l'ASN a poursuivi l'instruction de la conception de la version du système de protection que vous prévoyez d'implémenter à la mise en service du réacteur EPR de Flamanville. Cette instruction porte en particulier sur le processus de développement décrit dans le plan qualité en référence [2], la qualité de réalisation du logiciel, ainsi que les suites des inspections en référence [6] et [7]. Elle intègre également l'analyse de vos engagements, des réponses aux demandes formulées par l'ASN et du traitement des écarts découverts au cours de l'instruction.

L'ASN vous a fait part de ses premières conclusions par courrier en référence [8]. Le présent courrier comporte les conclusions de l'ASN sur la réalisation des activités définies par le plan qualité en référence [2], et sur les engagements que vous avez pris au cours de l'instruction. Il sera complété par un troisième courrier prévu au second semestre 2023.

À ce stade de l'instruction, je considère que l'application du plan qualité en référence pour le développement de la version du système de protection implémentée sur le réacteur EPR de Flamanville est satisfaisante. L'annexe du présent courrier liste les justifications complémentaires attendues.

Je note également que la complexification des exigences fonctionnelles rend leur implémentation dans les logiciels de contrôle commande plus sensible aux erreurs humaines. Elle limite également l'efficacité des actions de vérification et de validation de leur bonne implémentation. Il conviendra d'anticiper ce point pour vos éventuels futurs projets.

Par ailleurs, lors de l'instruction, vous avez pris deux engagements visant à vérifier :

- que les signaux de sortie du système de protection classé F1A ne dépendent pas de signaux d'entrée non désirés. À cet effet, vous avez développé l'outil Oscar, que je considère adapté pour répondre à la demande de l'ASN du courrier en référence [8]. Cet outil a notamment permis de mettre en lumière un écart portant sur le signal d'activation de l'injection de sécurité dans les états d'arrêt du réacteur ;
- la déclinaison des exigences fonctionnelles dans les diagrammes fonctionnels logiques (DFL). Cette vérification a également permis de détecter des écarts dont vous avez informé l'ASN.

Les résultats de ces vérifications, et le traitement des écarts mentionnés ci-dessus feront l'objet d'une analyse dont les conclusions vous seront transmises par un courrier prévu au second semestre 2023. Ce courrier intégrera également l'analyse des derniers livrables documentaires relatifs à la version 7.2 du système de protection, ainsi que l'analyse de vos réponses aux demandes figurant en annexe 1 du présent courrier.

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

Signé par l'adjointe au directeur des centrales nucléaires,

Stéphanie PEIRO

ANNEXE 1 À LA LETTRE CODEP-DCN-2023-010746

A. Utilisation de macroblocs

Le logiciel du système de protection utilise des blocs exprimant des connexions logiques entre les différents signaux afin de construire les diagrammes fonctionnels logiques. Ces blocs sont généralement issus d'une librairie générique à la plateforme TXS, mais peuvent prendre la forme de macroblocs modifiables par le concepteur et construits à partir des blocs constitutifs de la librairie. Certains de ces macroblocs sont formés par l'assemblage de plusieurs blocs existants et sont recensés dans une librairie SPACE dédiée. Les macroblocs peuvent prendre des formes différentes, et pour certains, considérés comme des logiques libres, le concepteur a la possibilité d'adapter le nombre d'entrées et de sorties. Ces macroblocs, regroupés dans la catégorie MACROS3, existent ainsi sous plusieurs variantes, lesquelles ne figurent pas toutes dans la librairie SPACE.

Le plan qualité en référence [2] prévoit que chaque macrobloc de la librairie SPACE du système de protection soit testé unitairement, avant la validation de la base SPACE. L'instruction a permis de constater que certains de ces macroblocs n'étaient pas testés. Vous avez justifié ce point en vous appuyant sur la note en référence [9] qui prévoit notamment que pour les macroblocs MACROS3, seuls un à trois variants soient retenus pour la validation, et que la validation des macroblocs très similaires à ceux déjà validés peut être prononcée par analogie. Or, le retour d'expérience fait état d'un écart relatif à l'implémentation de certains macroblocs, montrant ainsi la nécessité de vérifier l'absence d'écart similaire.

À cet effet, vous vous êtes engagé [10] à tester unitairement chaque bloc de la librairie SPACE avant la mise en service du réacteur EPR de Flamanville. **Je considère cet engagement satisfaisant dans son principe, mais que des justifications nécessitent d'être apportées pour justifier sa suffisance**. En effet, votre engagement porte sur les macroblocs figurant dans la librairie SPACE dédiée. Or, lorsqu'un bloc de la librairie est modifié, la modification ne s'opère pas automatiquement dans la librairie SPACE du système de protection. Ainsi, le concepteur doit rechercher manuellement les instances de ce bloc dans le logiciel existant (la librairie SPACE du système de protection) et les modifier. Cette tâche, particulièrement fastidieuse, est sensible aux erreurs humaines.

Demande n° 1 : Je vous demande de justifier la robustesse de votre processus de modification des macroblocs recensés dans la librairie figurant dans la base SPACE.

Par ailleurs, les variantes des macroblocs de la catégorie MACROS3 ne sont pas toutes recensées dans la librairie SPACE du système de protection, et ne sont donc pas couvertes par votre engagement. Vous considérez [10] que la vérification et la validation de ces logiques libres sont suffisantes. Si la vérification visuelle dans la base SPACE est identique pour tous les macroblocs, la validation des macroblocs non recensés dans la librairie SPACE repose quant à elle sur les tests F1, dont les objectifs sont différents des tests unitaires prévus sur les blocs de la librairie. Il convient donc de s'assurer de la suffisance des tests F1 pour valider le fonctionnement de ces macroblocs.

Lorsque ces macroblocs apparaissent sous forme de blocs dans les DFL, un critère formel de couverture de test garantit une couverture suffisante des tests de validation. Toutefois, lorsque ces macroblocs n'apparaissent pas sous forme de blocs dans les DFL, aucun critère formel de couverture de test n'est systématiquement défini.

<u>Demande n° 2 :</u> Je vous demande de justifier la suffisance de la validation des macroblocs implémentés librement dans la base SPACE du système de protection et n'apparaissant pas sous la forme de blocs dans les diagrammes fonctionnels logiques.

ANNEXE 2 À LA LETTRE CODEP-DCN-2023-010746

[**1**] Directives techniques pour la conception et la construction de la prochaine génération de réacteurs nucléaires à eau sous pression - Adoptées pendant les réunions plénières du GPR et des experts allemands les 19 et 26 octobre 2000

[**2**] Note Framatome – NLE-F DC 113 ind. U du 2 février 2022: "TELEPERM XS based I&C systems – System Quality Plan

[**3**] Lettre ASN DEP-DCN-0568-2009 du 15 Octobre 2009 – Architecture générale du contrôle commande et des plateformes associées

[**4**] Lettre ASN CODEP-DCN-2016-025904 du 20 Juillet 2016 – Instruction de la demande d'autorisation de mise en service – Système de protection F1A

[**5**] Lettre ASN CODEP-MEA-2016-050705 du 26 Décembre 2016 – Avis et recommandations du Groupe Permanent Réacteurs des 15 et 15/12/2016

[**6**] Lettre ASN CODEP-DCN-2020-006024 du 8 juillet 2021 - INSSN-DCN-2020-0299 : Surveillance des AIP relatives au développement du logiciel du système de protection

[**7**] Lettre ASN CODEP-DCN-2021-030820 du 14 février 2020 - INSSN-DCN-2021-0297 : Surveillance des AIP relatives au développement du logiciel du système de protection

[**8**] Lettre ASN CODEP-DCN-2022-017678 du 3 juin 2022 – Processus de développement du système de protection

[**9**] Note Framatome - NLE-F DC 231 ind. J du 30 novembre 2020 : « Système TXS - Spécifications des tests des Macros logiciels »

[**10**] Courrier EDF D458522053308 du 30 Novembre 2022 – Application du processus de développement du système de protection à la version de mise en service – Projet de rapport de l'IRSN