AUTORITÉ DE SÛRETÉ NUCLÉAIRE
Direction des centrales nucléaires

RÉPUBLIQUE FRANÇAISE

Référence courrier :
CODEP-DCN-2022-017678
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 3 juin 2022

Objet : Réacteur EPR de Flamanville 3
Thème : Processus de développement du système de protection

Références :
[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. S du 30 mars 2021: "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 d'experts pour les réacteurs des 15 et 15/12/2016
[6] Lettre ASN CODEP-DCN-2020-006024 : INSSN-DCN-2020-0299 – Surveillance des AIP relatives au développement du logiciel du système de protection
[7] Lettre ASN CODEP-DCN-2021-030820 : INSSN-DCN-2021-0297 – Surveillance des AIP relatives au développement du logiciel du système de protection

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, 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 l'avis de l'IRSN et du groupe permanent d'experts pour les réacteurs nucléaires sur le contrôle-commande ([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 références [6] et [7], l'ASN a engagé une instruction de la conception de la version du système de protection que vous prévoyez d'implanter pour 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 sur les suites des inspections en références [6] et [7]. Elle doit permettre à l'ASN de prendre position sur la qualité du système de protection, préalablement à l'autorisation de mise en service du réacteur.

À ce stade de l'instruction, je considère que le plan qualité utilisé pour le développement de la version que vous prévoyez d'implanter pour la mise en service du réacteur est adapté aux fonctions qu'assure le système de protection. Toutefois, compte tenu des évolutions successives du plan qualité ces dernières années, il apparaît que les versions précédentes du système de protection pourraient ne pas toutes avoir été développées selon un processus adapté. Les mises à jour successives du logiciel étant partielles, elles ne permettent pas toujours d'identifier et de corriger les éventuelles erreurs introduites lors du développement des versions précédentes.

Par ailleurs, les essais de démarrage ont permis de détecter un écart qui met en lumière le risque, pour un signal de sortie, de dépendre d'un signal d'entrée non spécifié. Vous trouverez en annexe une demande à ce sujet.

L'ASN poursuit, avec l'appui de l'IRSN, l'examen de la conception et de la qualité du développement du logiciel de protection. Vos réponses au présent courrier seront intégrées à cet examen.

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

Signé par le directeur des centrales nucléaires,

Remy CATTEAU

ANNEXE À LA LETTRE CODEP-DCN-2022-017678

A. Signal de sortie dépendant d'une entrée non spécifiée

Un écart de réalisation du logiciel du système de protection a été détecté lors des essais de démarrage, lorsque la version 6 du logiciel était implantée. Cet écart a mis en évidence la dépendance d'un signal de sortie à un signal d'entrée non prévu par les spécifications fonctionnelles et logicielles, pouvant ainsi entrainer un comportement inattendu du système de protection, lequel assure notamment des fonctions classées F1A.

L'analyse de cet écart a permis d'établir que ce dernier avait été introduit lors du développement de la version 3. Ni les activités de V&V consécutives à la conception de cette version, ni le développement des versions ultérieures n'ont permis de détecter cet écart. En effet, les activités de vérification qui consistent en une lecture manuelle des diagrammes et les tests de validation ne permettent pas de détecter ce type d'écart de manière fiable. Par ailleurs, les mises à jour du logiciel étant le plus souvent partielles, elles ne conduisent pas à une vérification complète de ce dernier. Enfin, les essais de démarrage ne constituent pas une ligne de défense robuste pour détecter ce type d'écart car leur objectif est de vérifier que les systèmes respectent les exigences fonctionnelles qui leur sont allouées. La valeur des signaux d'entrée non spécifiés ne constitue pas forcément un paramètre d'intérêt lors de ces derniers.

Compte tenu des enjeux que présente ce type d'écart et de l'absence de ligne de défense robuste permettant de le détecter, je considère que le processus de développement du logiciel doit être complété afin de détecter, par une méthode fiable, les dépendances de sorties à des entrées non spécifiées.

Demande n° 1 : Je note votre engagement de définir une méthode efficace et systématique pour vérifier que les sorties du système de protection classées F1A ne dépendent pas d'une entrée non spécifiée. Je vous demande de mettre en œuvre cette méthode et de me présenter les conclusions de cette vérification au plus tard trois mois avant la date prévue pour la mise en service du réacteur. Vous intégrerez cette vérification au plan qualité du système de protection.