RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

IRSN
INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 26 janvier 2022

Monsieur le Président de l'Autorité de sûreté nucléaire

AVIS IRSN N° 2022-00010

Objet	:	**EPR de Flamanville : Processus de développement du système de protection - Examen du plan qualité système applicable à la version de mise en service.**
Réf.	**:**	Lettre ASN – CODEP-DCN-2021-041912 du 13 septembre 2021.

1. CONTEXTE

Le système de protection (PS) du réacteur EPR de Flamanville (EPR FA3) est un système de contrôle-commande, basé sur la technologie numérique, qui participe à la maîtrise de la réactivité, à l'évacuation de la puissance résiduelle et au confinement des substances radioactives. Sa partie classée F1A[1] (PS-F1A) réalise les fonctions automatiques, manuelles et de surveillance nécessaires pour atteindre l'état contrôlé dans les conditions de fonctionnement de référence ; elle joue donc un rôle essentiel pour la sûreté.

Afin d'être apte à remplir ses missions de sûreté, le PS-F1A doit atteindre les objectifs de fiabilité exigés, ce qui implique une spécification, une conception et une réalisation de qualité, y compris pour son logiciel, de manière à réaliser une logique exempte d'erreur. Ce dernier point est important car il ne peut pas être complètement démontré en examinant, testant et analysant uniquement le système achevé. Ainsi, un processus de développement rigoureux et adéquat doit également être défini et appliqué. Ce processus est tracé dans un plan qualité système (PQS). Selon l'état de l'art des systèmes numériques classés F1A décrit dans les normes nucléaires de la Commission électrotechnique internationale, ce processus doit être découpé en phases de développement, de vérification et de validation.

L'Institut de radioprotection et de sûreté nucléaire (IRSN) a consacré plusieurs expertises au PS-F1A de l'EPR FA3 depuis le démarrage du projet. Celles de 2005, de 2014 et de 2016 ont notamment porté sur les différentes versions du PQS du PS-F1A et l'IRSN avait conclu que le PQS était satisfaisant.

Depuis 2016, les fonctions du PS-F1A et le PQS ont évolué à plusieurs reprises. La version actuelle du PQS est celle appliquée pour développer la version du PS-F1A qui sera utilisée à la mise en service de l'EPR FA3.

[1] Pour l'EPR, le classement F1A du système correspond au plus haut niveau de rigueur dans les activités de développement et dans les justifications. Ce classement est lié à l'importance pour la sûreté de chacune des fonctions du contrôle-commande. Cette importance s'apprécie au regard du rôle de la fonction dans l'obtention et le maintien de la sûreté, des conséquences potentielles de sa défaillance lorsqu'elle est sollicitée et de la probabilité de cette défaillance.

Afin de pouvoir se prononcer sur le caractère adapté du processus de développement du PS-F1A de l'EPR FA3 décrit dans le PQS, l'Autorité de sûreté nucléaire (ASN) a souhaité recueillir, par lettre citée en référence, l'avis de l'IRSN sur :

- les dispositions en termes de chronologie et d'indépendance entre les différentes activités de développement ;
- le caractère adapté du PQS pour garantir la cohérence des spécifications et de leur implémentation avec les hypothèses de la démonstration de sûreté ;
- le caractère adapté du processus d'analyse d'impact des modifications, compte tenu du lot de modifications important prévu dans la version de mise en service de l'EPR FA3 depuis 2016.

L'IRSN expose dans les chapitres suivants les évolutions et évènements susceptibles de remettre en cause les conclusions des expertises précédentes, à savoir les principales évolutions du PQS depuis 2016, puis deux évènements particuliers survenus sur l'EPR.

2. ÉVOLUTIONS DU PLAN QUALITÉ SYSTÈME

Depuis la dernière expertise du PS-F1A menée en 2016, celui-ci a subi de nombreuses évolutions fonctionnelles conduisant à plusieurs nouvelles versions du système. En parallèle, le constructeur a décidé de plusieurs évolutions du processus de développement du PS-F1A décrit dans le PQS.

L'IRSN estime que la plupart de ces évolutions ne remettent pas en cause les conclusions de ses précédentes expertises. Cependant, certaines évolutions du processus de développement, qui ont été appliquées lors du développement des versions du PS-F1A postérieures à 2016 ne permettent pas, selon l'IRSN, de respecter le niveau de qualité nécessaire au classement F1A. EDF en a convenu au cours de l'expertise et a décidé de ne plus les mettre en œuvre pour les versions ultérieures. L'IRSN estime que la décision d'EDF est satisfaisante, mais rappelle néanmoins que le processus est tel que chaque version dépend de l'historique des versions précédentes. De cette façon, un niveau de qualité insuffisant d'une version antérieure impacte de fait toutes les versions ultérieures. Ainsi, même si le PQS appliqué pour la version de mise en service de l'EPR FA3 est acceptable, il reste nécessaire qu'EDF s'assure du niveau de qualité adéquat de l'ensemble du PS-F1A. **L'expertise de ce sujet se poursuit.**

3. VÉRIFICATION ET VALIDATION DU LOGICIEL

Un écart a été relevé au cours d'un essai de démarrage visant à s'assurer du bon comportement du réacteur dans les situations accidentelles de perte d'alimentation électrique externe. Lors de cet évènement, l'alimentation électrique des actionneurs de sauvegarde doit basculer sur les groupes électrogènes disponibles. À cette fin, le PS-F1A réalise la fonction « Mise en service des diesels principaux » ayant pour rôle d'assurer ce basculement d'alimentation électrique et de donner l'ordre de démarrage des groupes électrogènes. Or lors de l'essai, le disjoncteur du groupe électrogène en maintenance a été intempestivement fermé, conduisant à un démarrage anormal de ce dernier. Le mauvais comportement de la fonction « Mise en service des diesels principaux » a été attribué à une erreur de réalisation du logiciel du PS-F1A, ce qui a conduit l'IRSN à reprendre l'analyse de la suffisance des activités de vérification et validation du cycle de développement du PS-F1A.

Plus précisément, la fonction « Mise en service des diesels principaux », spécifiée par EDF, a été correctement déclinée dans la spécification logicielle du PS-F1A, mais son implémentation dans le logiciel est erronée dans la version utilisée pour les essais de démarrage. Cette implémentation est assurée par un atelier de développement du logiciel qui permet de transcrire la réalisation graphique du schéma logique des fonctions de sûreté à assurer par le système PS en lignes de code. Ces schémas sont réalisés manuellement et intègrent de nombreuses entrées, dépendances et sorties. Le démarrage anormal du groupe électrogène est associé à la mauvaise réalisation graphique du schéma logique dans lequel des dépendances erronées ont été introduites.

Cette erreur n'a pas été détectée aux étapes de vérification du logiciel et des tests de validation du logiciel. À la suite, EDF a engagé des actions qui ont permis d'améliorer la vérification visuelle du logiciel par des dispositions graphiques destinées à attirer l'attention du vérificateur sur certains points essentiels. Cependant, la question soulevée par cet écart est que le processus de vérification et de validation actuel ne permet pas de vérifier que chaque sortie de la partie du logiciel testée lors de l'étape des tests détaillés du logiciel dépend bien exclusivement des entrées spécifiées. Ainsi, pour l'IRSN, les actions mises en place par EDF et le constructeur n'apportent pas la garantie systématique de cette vérification.

Au cours de l'expertise, EDF s'est engagé à présenter, à l'échéance de mi-2022, pour une mise en œuvre après la mise en service de l'EPR FA3, une proposition de vérification efficace et systématique permettant de détecter sur chaque sortie du PS-F1A, la dépendance non spécifiée d'une entrée. L'IRSN note les efforts d'EDF, mais estime que le délai associé est trop tardif pour prévenir les conséquences fonctionnelles potentielles, telles qu'un dysfonctionnement d'un système de sauvegarde, que pourrait avoir une autre erreur non détectable par le processus de développement actuel du logiciel du PS-F1A**. Pour l'IRSN, la garantie de l'absence de ce type d'erreur dans le logiciel du PS-F1A doit être apportée en préalable à la mise en service du réacteur. À ce titre, l'IRSN formule la recommandation présentée en Annexe 1.**

4. RÔLE DE L'ÉQUIPE INDÉPENDANTE DE VÉRIFICATION ET VALIDATION

Selon le consensus international sur les meilleures pratiques de développement des systèmes numériques classés F1A, l'indépendance de l'équipe de vérification et validation par rapport à l'équipe de conception et réalisation est un élément essentiel.

Au cours du projet de l'EPR FA3, l'IRSN a relevé que les évolutions du PQS ont eu tendance à réduire le rôle de l'équipe indépendante de vérification et validation dans les analyses de performances du PS-F1A. Sur ce point, EDF s'est engagé (*cf.* engagement n° 1 rappelé en annexe 2) à ce qu'une vérification indépendante des performances du système de protection soit réalisée avant la mise en service du réacteur, ce qui est satisfaisant.

Par ailleurs, compte tenu du retour d'expérience de l'EPR, l'IRSN a estimé qu'une caractérisation de l'imprécision maximale des algorithmes de calculs récursifs devait être réalisée avant la mise en service. En effet, des dérives des valeurs calculées ont été observées au cours du temps par rapport aux valeurs physiques réelles attendues. Sur ce point, EDF a pris les engagements n° 1 et 2 rappelés en Annexe 2, qui sont satisfaisants et devraient permettre d'apporter les garanties nécessaires sur la précision des calculs réalisés par le PS-F1A.

Enfin, au cours du projet de l'EPR FA3, l'équipe de vérification et validation a mis au point des méthodes spécifiques de vérification avec l'aide des équipes de spécification de certaines fonctions complexes du PS-F1A, sans que ces méthodes soient indiquées dans le PQS, ce qui n'est pas satisfaisant. Sur ce point, EDF a pris l'engagement n° 3 rappelé en annexe 2 qui est jugé acceptable.

5. CONCLUSION

L'IRSN estime que le processus de développement du PS-F1A décrit dans le plan qualité système appliqué pour développer la version de mise en service de l'EPR de Flamanville, ainsi que les engagements pris par EDF pour améliorer ce processus sont satisfaisants. **Néanmoins, compte tenu de l'historique des évolutions du PQS, l'examen du niveau de qualité adéquat de l'ensemble du PS-F1A est toujours en cours. Enfin, l'IRSN estime nécessaire que, avant la mise en service du réacteur EPR de Flamanville, EDF s'assure de l'absence de dépendances non spécifiées pour chacune des sorties du PS-F1A**.

IRSN
Le Directeur général
Par délégation
Thierry PAYEN
Adjoint au Directeur de l'expertise de sûreté

VALIDATION ELECTRONIQUE CERTIFIÉE IRSN

THIERRY PAYEN
2022.01.26
16:54:52 +01'00'

ANNEXE 1 À L'AVIS IRSN N° 2022-00010 DU 26 JANVIER 2022

Recommandation de l'IRSN

L'IRSN recommande que, avant la mise en service de l'EPR de Flamanville, EDF applique la méthode qu'il aura définie pour la vérification efficace et systématique permettant de détecter, sur chaque sortie du PS-F1A, la dépendance non spécifiée d'une entrée.

ANNEXE 2 À L'AVIS IRSN N° 2022-00010 DU 26 JANVIER 2022

Engagements de l'exploitant

Engagement N° 1

À l'échéance de la mise en service, EDF confirme qu'une vérification indépendante sera réalisée pour :

- l'analyse de temps de réponse préliminaire du système de protection ;
- l'analyse de charge CPU[2] du système de protection ;
- l'analyse de précision du système de protection.

La mise à jour du PQS en ce sens sera transmise pour fin janvier 2022.

Engagement N° 2

EDF confirme qu'une caractérisation de l'imprécision maximale des algorithmes de calculs récursifs sera réalisée à l'échéance de la mise en service. Cette analyse sera réalisée selon les étapes suivantes :

- l'identification de la liste des algorithmes récursifs pour lesquels un risque de dérive de calcul est à craindre et les éléments de justification associés. Ces éléments seront transmis pour fin février 2022 ;
- l'exécution des algorithmes avec risque de dérive sur SIVAT[3] afin de caractériser l'imprécision et justifier le caractère acceptable vis-à-vis de la démonstration de sûreté. L'ensemble de ces analyses et leurs résultats seront tracés dans une note dédiée. Celle-ci sera transmise pour mi-2022 ;
- enfin, les résultats pour l'algorithme de concentration en bore dont le risque de dérive est avéré seront fournis pour fin janvier 2022.

EDF confirme de plus que la méthodologie de validation de la précision des algorithmes numériques du PS sera mise à jour pour la prochaine version VC1 du système de protection F1A.

Engagement N° 3

EDF confirme que le besoin d'impliquer le spécificateur de la logique du VDA[4] en cas de modification de cette dernière sera tracé dans une checklist. Cette checklist sera référencée dans le PQS applicable à partir de la version VC1 du système de protection.

[2] Central processing unit.

[3] SIVAT : Logiciel de simulation utilisé pour tester le logiciel du PS-F1A.

[4] Vanne de décharge à l'atmosphère du circuit secondaire de l'EPR.