RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

IRSN
INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 14 décembre 2022

Monsieur le Président de l'Autorité de sûreté nucléaire

AVIS IRSN N° 2022-00230

Objet : **EDF – EPR de Flamanville – INB 167 : Système de protection – Examen de l'application du processus de développement à la version de mise en service.**

Réf. **:**
[1] Avis IRSN n° 2022-00010 du 26 janvier 2022.
[2] Lettre ASN – CODEP-DCN-2022-020057 du 20 avril 2022.
[3] Lettre ASN – CODEP-DCN-2021-030820 du 8 juillet 2021.
[4] Avis IRSN n° 2022-00154 du 21 juillet 2022.

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 spécification, de conception, de vérification et de validation.

L'Institut de radioprotection et de sûreté nucléaire (IRSN) a déjà mené plusieurs expertises sur le PS-F1A de l'EPR FA3 depuis le démarrage du projet, la dernière ayant porté sur les évolutions du processus de développement décrit dans le PQS a été menée dans le cadre de l'avis en référence [1]. Dans celui-ci, l'IRSN a estimé que ce

[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.

IRSN Siège social, 31, av. de la Division Leclerc - 92260 Fontenay-aux-Roses - Standard +33 (0)1 58 35 88 88 - RCS Nanterre B 440 546 018
Adresse courrier : BP 17 – 92262 Fontenay-aux-Roses Cedex – France

processus et les engagements pris par EDF pour l'améliorer étaient satisfaisants, mais qu'EDF devait encore s'assurer de l'absence de dépendances non spécifiées[2] pour chacune des sorties du PS-F1A.

Par ailleurs, EDF a identifié récemment un écart lié à une mauvaise déclinaison dans le PS des exigences fonctionnelles associées à la fonction d'injection de sécurité.

Afin de se prononcer sur la raisonnable assurance de la qualité de développement et de réalisation du système de protection qu'EDF prévoit d'implémenter pour la mise en service du réacteur EPR de Flamanville, l'Autorité de sûreté nucléaire (ASN) sollicite l'avis de l'IRSN [2] sur :

- la bonne réalisation des versions 7 à 7.2 de ce système, conformément au PQS ;
- les engagements pris par EDF, lors de l'instruction relative à l'avis en référence [1], et les suites données à la détection de l'écart lié à la réalisation de la fonction d'injection de sécurité ;
- les actions menées par EDF à la suite des demandes qu'elle a formulées [3] dans le cadre d'une inspection.

L'IRSN expose dans les chapitres suivants son expertise de la bonne réalisation des versions développées selon les dernières versions du PQS, puis des actions déclinées des engagements d'EDF lors de l'instruction relative à l'avis en référence [1], et enfin des actions réalisées à la suite de l'inspection de l'ASN [3].

2. APPLICATION DU PROCESSUS DE DÉVELOPPEMENT

Le processus de développement du PS F1A a pour principales données d'entrée les documents de spécification des exigences fonctionnelles qui décrivent le fonctionnement attendu du PS-F1A. Ces documents sont élaborés « en amont » par des équipes de spécialistes du fonctionnement du réacteur, distinctes des équipes en charge de la réalisation du contrôle-commande. Ces dernières équipes appliquent alors le processus de développement décrit dans le PQS afin de décliner, sans introduire d'erreur, ces exigences fonctionnelles dans les documents élaborés lors des phases de développement, dans le programme du logiciel, et dans les documents de vérification et de validation. Plus précisément, depuis la version 2 du PS-F1A, le développement d'une version consiste principalement à gérer les évolutions des exigences fonctionnelles. Ainsi, l'application du processus de développement consiste à réaliser des modifications ciblées des documents et du programme, puis à vérifier et valider ces modifications. La vérification et la validation d'une version du PS-F1A est réalisée par une équipe du contrôle-commande indépendante de l'équipe réalisant son développement.

L'IRSN estime que la déclinaison des exigences fonctionnelles dans les documents et dans le programme produit lors des phases du cycle de vie du PS-F1A est réalisée de façon globalement satisfaisante. Les expertises menées par l'IRSN sur les documents du constructeur montrent que les exigences fonctionnelles sont correctement déclinées et progressivement détaillées jusqu'à être introduites dans le programme. La cause de chaque évolution documentaire est suffisamment tracée et justifiée et, lorsqu'un écart est détecté, les justifications apportées avec les actions mises en œuvre pour que ce type d'écart soit détecté au plus tôt et systématiquement corrigé dans le cycle de vie du PS-F1A sont satisfaisantes.

Toutefois, l'IRSN a noté que plusieurs écarts relevés par le constructeur, dont celui lié à la fonction d'injection de sécurité, étaient dus à des incohérences entre les exigences fonctionnelles amont et leur déclinaison dans les documents du cycle de vie du PS-F1A. Selon l'IRSN, ce point est particulièrement sensible car il s'agit de l'interface entre les métiers, à savoir les spécialistes du fonctionnement du réacteur et les spécialistes du contrôle-commande. De plus, certaines exigences décrites de façon particulièrement complexe peuvent conduire à des erreurs d'interprétations de la part de l'équipe contrôle-commande. Ces erreurs ne peuvent alors être piéger

[2] Les spécifications du logiciel spécifient les traitements que le logiciel doit effectuer et par conséquent spécifient de quelles entrées du système dépendent une sortie donnée. Si la réalisation du logiciel introduit d'autres dépendances que celles spécifiées, celles-ci doivent pouvoir se justifier.

que par une vérification exhaustive et rigoureuse de la part de l'équipe contrôle-commande indépendante. Or les écarts détectés ont remis en cause la suffisance de la vérification réalisée. Dans ce contexte, EDF a engagé une vérification complète de la déclinaison des exigences fonctionnelles dans les documents de spécifications fonctionnelles pour la version 7.2 du PS-F1A. L'IRSN estime que cette vérification complète était indispensable pour justifier du niveau de qualité attendu du PS-F1A. Lors de ces travaux, EDF et le constructeur ont identifiés quelques différences entre les exigences fonctionnelles et la réalisation du PS-F1A. Pour chacune d'elles, EDF a transmis des éléments visant à justifier que le réacteur peut démarrer avec le PS-F1A en l'état et, le cas échéant, a précisé les mesures compensatoires devant être mises en place. L'analyse de ces éléments sera intégrée à la prochaine expertise de l'IRSN sur le PS-F1A prévue avant la mise en service de l'EPR FA3.

La validation d'une version du PS-F1A est menée principalement en deux étapes par l'équipe indépendante de l'équipe du développement. La première étape consiste à valider le logiciel en réalisant des tests sur un simulateur de chacun des modules du logiciel définis à la conception. La seconde étape consiste à valider le système en réalisant des tests d'intégration et fonctionnels sur une cible matérielle, réplique identique du système complet implanté sur le réacteur EPR de Flamanville. Ainsi tout écart découvert lors du cycle de développement, en vérification ou en validation, ou encore lors des essais d'ensemble du réacteur, fait l'objet d'une correction du système.

Concernant la qualité de cette validation, l'IRSN considère que les tests modulaires comme les tests d'ensemble ont évolué de façon satisfaisante pour prendre en compte les modifications des exigences fonctionnelles. La complétude des tests, leur approche modulaire et la méthode d'analyse des tests n'ont pas été remises en cause lors des différentes versions du système. Pour appuyer cette conclusion, l'IRSN a réalisé des analyses avec ses propres outils sur des échantillons du PS-F1A, que ce soit pour évaluer la couverture fonctionnelle de la validation logicielle, pour contre-expertiser les analyses de précision des fonctions récursives, ou encore pour vérifier de façon formelle la validité de certaines hypothèses de conception prises par le constructeur dans les conditions de fonctionnement en mode dégradé. Cependant, selon l'IRSN, deux éléments de la validation, détaillés ci-après, devraient être améliorés.

Le premier élément concerne un point d'amélioration de la validation du logiciel pour s'assurer du respect des objectifs de couverture de chaque test qui nécessite encore des échanges avec EDF.

Le deuxième élément porte sur la validation spécifique de la librairie de macroblocs[3] utilisés pour le développement du logiciel du PS-F1A. L'IRSN estime que la validation unitaire de chacun des macroblocs utilisés dans le PS-F1A devrait être effectuée, avant la mise en service du réacteur EPR de Flamanville, conformément aux préconisations du PQS. Sur ce point, EDF a pris l'engagement, rappelé en annexe 2, qui répond en partie à la problématique soulevée. **En effet, il ne couvre pas certaines parties de logiciel développées de manière libre sur la base de macrobloc et pour lesquelles il n'existe pas de test spécifique de validation. Ce point fait l'objet de la recommandation en annexe 1.**

En outre, l'IRSN considère qu'EDF devrait s'assurer que les macroblocs utilisés dans le PS-F1A sont bien ceux de la dernière version de la librairie, ce qui fait l'objet de l'observation en annexe 3.

Enfin, compte tenu de l'avancement de la réalisation de la version V7.2 du PS F1A, certains éléments sont encore manquants dans le dossier d'EDF, tels que les résultats de la campagne de vérification et validation, les résultats des analyses outillées, ainsi que les conclusions de l'analyse des causes profondes des écarts ayant conduit à la vérification complète des exigences fonctionnelles implémentées dans le PS-F1A. L'IRSN se prononcera sur ces éléments lors de son prochain avis sur le PS-F1A lorsqu'ils seront disponibles.

[3] Pour le PS, les macroblocs sont composés de plusieurs blocs génériques fournis par le constructeur de la plateforme et proposés au développeur du système sous une forme préassemblée dans une librairie dédiée.

3. SUITES DE L'EXPERTISE DU PROCESSUS DE DÉVELOPPEMENT

Dans son avis précédent sur le PS-F1A [1], l'IRSN recommandait 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.

Pour y répondre, EDF et son constructeur ont développé un outil spécifique pour analyser le logiciel du PS-F1A, avant la mise en service du réacteur, et vérifier que chaque sortie des modules du logiciel ne dépend que des entrées spécifiées. **L'IRSN estime que les objectifs et la méthodologie employée pour cette nouvelle étape de vérification systématique intégrée au processus de validation du logiciel sont satisfaisants.** Les résultats de cette phase de vérification sont attendus en amont du démarrage du réacteur.

Par ailleurs, dans le cadre cette précédente expertise du PS-F1A, EDF s'est engagé à réaliser une vérification indépendante pour l'analyse de temps de réponse préliminaire, l'analyse de la charge de calcul, et l'analyse de précision. L'IRSN constate qu'EDF a mis à jour le PQS conformément à son engagement, ce qui est satisfaisant. Toutefois, concernant les documents d'analyses, si l'IRSN ne remet pas en cause les conclusions du constructeur, il ne peut pas formellement constater que c'est effectivement l'équipe indépendante qui a réalisé ce travail, car les documents fournis à l'IRSN ne permettent pas de l'identifier. Ainsi, la consultation du système de gestion documentaire électronique du constructeur est nécessaire. L'IRSN continuera son expertise de ce sujet dans le cadre de son prochain avis sur le PS-F1A.

De plus, EDF a caractérisé l'imprécision maximale des algorithmes de calculs récursifs du PS-F1A. Pour cela, il a réalisé une analyse numérique de la stabilité des algorithmes itératifs vis-à-vis des erreurs d'arrondis et a défini un critère d'acceptabilité. Des analyses complémentaires ont été effectuées par EDF, lorsque ce critère n'est pas vérifié. L'IRSN estime que le critère défini par EDF est acceptable et que les résultats de l'analyse numérique démontrent qu'il n'y a pas de risque d'erreur de calcul pour la plupart des algorithmes récursifs qui ne vérifient pas ce critère. Toutefois, pour un des algorithmes, la méthode employée est spécifique. Elle est basée à la fois sur l'identification des conditions amenant les erreurs les plus grandes et sur une caractérisation par un test de validation fonctionnel correspondant à la valeur de l'erreur maximale dans l'algorithme. L'IRSN estime que la précision de cet algorithme est satisfaisante dans la plage de fonctionnement nominal. Ce dernier point fait l'objet d'un engagement dans le cadre d'une autre expertise de l'IRSN [4].

4. SUITES DE L'INSPECTION CHEZ LE CONSTRUCTEUR

Les inspecteurs de l'ASN, accompagnés de l'IRSN, ont conduit une inspection le 7 juin 2021 chez Framatome [3], constructeur du logiciel du PS-F1A de l'EPR de Flamanville, alors que la version 7 était en cours de développement à cette date. Cette inspection portait sur la réalisation des activités importantes pour la protection des intérêts, afférentes au développement du logiciel du PS-F1A, ainsi que sur leur surveillance par EDF. Elle a mis en évidence des écarts dans l'application du processus, qui ont notamment conduit l'ASN à demander à EDF d'effectuer une revue complète de l'application des règles et méthodes prescrites dans le PQS, puis une analyse de l'effet cumulé des écarts identifiés sur la fiabilité de la conception du logiciel du PS-F1A. Cette revue menée par le constructeur et EDF a mis en évidence un certain nombre d'écarts supplémentaires à ceux identifiés en inspection, entre les actions menées par les équipes d'une part et les règles et méthodes prescrites d'autre part. EDF et le constructeur ont alors justifié que ces écarts étaient acceptables ou les ont corrigés. L'IRSN estime que les améliorations apportées à l'application du PQS sont satisfaisantes.

Concernant l'effet cumulé des écarts identifiés, l'IRSN estime que ce point est couvert par l'action de grande envergure menée par EDF pour vérifier la déclinaison de toutes les exigences fonctionnelles dans le PS-F1A, détaillée dans le paragraphe 2, dont l'analyse des résultats sera effectuée dans le cadre du prochain avis sur le PS-F1A.

5. CONCLUSION

Dans le cadre de la présente expertise du PS-F1A de l'EPR de Flamanville, l'IRSN a examiné l'application du processus de développement du constructeur sur les versions produites depuis la dernière expertise en 2016. Pour ce faire, l'IRSN a analysé la conception détaillée de certaines fonctions du PS-F1A choisies par échantillonnage, leur implémentation et leur validation. Ainsi, l'IRSN conclut que les exigences fonctionnelles et leurs évolutions successives au cours des versions du PS-F1A sont déclinées dans les documents du cycle de développement de façon satisfaisante. Toutefois, l'expertise a mis en évidence des points d'application du processus qui nécessitent encore quelques approfondissements, pour certains, et des améliorations, pour d'autres. Pour ces derniers, l'exploitant s'est engagé à réaliser des actions que l'IRSN estime satisfaisantes, mais non suffisantes.

L'IRSN s'est également assuré que les actions d'améliorations prises par EDF dans le cadre de son précédent avis sur le PS-F1A et à la suite de l'inspection chez le constructeur ont été mises en œuvre de façon satisfaisante. L'IRSN considère que les actions et méthodes présentées pour y répondre, ainsi que les résultats déjà disponibles sont acceptables.

Enfin certains éléments sont encore manquants dans le dossier d'EDF, tels que les résultats de la campagne de vérification et validation, les résultats des analyses outillées, ainsi que les conclusions de l'analyse des causes profondes des écarts ayant conduit à vérifier complètement les exigences fonctionnelles. L'expertise de la déclinaison du processus de développement et de la qualité in fine obtenue du PS-F1A se poursuit.

IRSN
Le Directeur général
Par délégation
Hervé BODINEAU
Adjoint au Directeur de l'expertise de sûreté

Hervé BODINEAU
2022.12.14
11:47:58 +01'00'

ANNEXE 1 À L'AVIS IRSN N° 2022-00230 DU 14 DÉCEMBRE 2022

Recommandation de l'IRSN

L'IRSN recommande qu'EDF justifie, avant la mise en service de l'EPR de Flamanville, que tous les macroblocs non représentés dans les diagrammes logiques fonctionnels (DFL) et implémentés librement comme des variantes des macroblocs « DOR[4] », « 1NV[5] », « 1SV[6] » et « extremum[7] » sont suffisamment testés lors de la validation du logiciel (étape S-23 du PQS).

[4] DOR : Ou logique dynamique, permettant de détecter un changement d'état de 0 vers 1 d'une entrée.

[5] 1NV : Voteur 1 parmi N entrées avec l'état de la sortie forcé à « valide ».

[6] 1SV : Voteur 1 parmi N entrées avec l'état de la sortie traité spécifiquement.

[7] Extremum : Détection du 1er ou 2nd minimum ou maximum parmi N entrées.

ANNEXE 2 À L'AVIS IRSN N° 2022-00230 DU 14 DÉCEMBRE 2022

Engagement principal de l'exploitant

Une validation explicite et unitaire de chaque macrobloc de la librairie SPACE NLE-F DC 220 sera réalisée à échéance du démarrage. En particulier, les instances des MACROS3 spécifiées dans la librairie seront toutes validées afin de démontrer que la validation actuelle par analogie complétée par la validation visuelle puis fonctionnelle de la base SPACE projet utilisant ces macroblocs est suffisante. La mise à jour des documents de spécification NLE-F DC 231 et rapports de test associés NLE-F DC 232 vous seront transmis pour fin mars 2023. De plus, la description du document NLE-F DC 231 [D-B3.1] donnée en step S-B3 du PQS des systèmes TXS NLE-F DC 113 sera précisée, afin d'indiquer explicitement que le périmètre de validation des tests unitaires est limité aux macroblocs de la librairie SPACE. La mise à jour du PQS vous sera transmise dans le cadre du licensing de la V8 TXS (VC1).

ANNEXE 3 À L'AVIS IRSN N° 2022-00230 DU 14 DÉCEMBRE 2022

Observation de l'IRSN

Concernant les macroblocs dont l'implémentation a évolué au cours des indices de la librairie NLE F DC 220, l'IRSN considère qu'EDF devrait justifier que le logiciel du PS en version 7.2 utilise l'implémentation des macroblocs décrite dans le dernier indice (L) de la librairie NLE F DC 220.