RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

IRSN
INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 26 juin 2023

Monsieur le Président de l'Autorité de sûreté nucléaire

AVIS IRSN N° 2023-00094

Objet : **EDF – REP – EPR de Flamanville – INB 167 – Système de protection – Suite de l'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] Avis IRSN n° 2022-00230 du 14 décembre 2023.
[3] Lettre ASN - CODEP-DCN-2022-017678 du 3 juin 2022.
[4] Lettre ASN - CODEP-DCN-2023-010746 du 4 avril 2023.
[5] Lettre ASN - CODEP-DCN-2023-027931 du 3 mai 2023.

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 (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. Les deux plus récentes ont porté sur les évolutions du processus de développement décrit dans le PQS menées dans le cadre de l'avis en référence [1], puis sur son application dans le cadre de l'avis en référence [2]. À l'issue de ces expertises, l'ASN a formulé des demandes [3] et [4] dont les réponses de l'exploitant restaient encore à analyser. Par ailleurs, EDF devait encore envoyer à l'IRSN des documents prévus relatifs aux dernières activités du processus.

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 FA3, l'Autorité de sûreté nucléaire (ASN) sollicite l'avis de l'IRSN [5] sur :

- la réalisation des activités définies par le PQS, ce point est examiné au § 2 ;
- la vérification de l'absence de dépendances non spécifiées[1] pour chacune des sorties du PS-F1A faisant suite à l'avis [1] de l'IRSN, ce point est examiné au § 3 ;
- la vérification de la déclinaison des exigences fonctionnelles dans les documents de conception du PS-F1A, dont la méthodologie avait été expertisée dans l'avis en référence [2] ; ce point est examiné au § 3 ;
- les compléments fournis par EDF sur la modification et la validation de la librairie de macroblocs[2] du PS-F1A qui sont également analysés dans le § 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.

Les documents issus des phases de développement reçus par l'IRSN depuis son précédent avis en référence [2] sont les résultats des campagnes de vérification et de validation pour les trois versions 7, 7.1 et 7.2 du PS-F1A, la version 7.2 étant utilisée pour la mise en service de l'EPR FA3. Chaque campagne est composée principalement de deux phases, une pour les tests de validation du logiciel et une pour les tests de validation et d'intégration du système.

La phase de validation du logiciel consiste à tester chaque composant logiciel impacté par les modifications des exigences fonctionnelles. Ainsi, environ la moitié des composants du logiciel du PS-F1A ont évolué au cours des versions 7, 7.1 et 7.2 et ont donc nécessité au moins une réexécution de la procédure de test associée. L'IRSN a examiné certains résultats de test en écart par rapport à l'attendu et qui font l'objet d'une justification de leur innocuité de la part d'EDF. Afin de se positionner sur l'acceptabilité de ces écarts, l'IRSN a utilisé ses outils logiciels pour examiner de façon détaillée le comportement ou la couverture de la validation des composants du logiciel du PS-F1A concernés par ces écarts. De cet examen, l'IRSN estime que les justifications apportées par EDF sont satisfaisantes, car les causes identifiées concernent des limitations technologiques de ses outils de test ou des erreurs dans la rédaction de certains scénarii de test qui ne remettent pas en cause la validité du logiciel. L'IRSN s'est, par ailleurs, assuré que l'enchaînement des activités de validation du logiciel est réalisé conformément au PQS et estime ainsi que la réalisation de cette phase est satisfaisante pour la mise en service.

[1] 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.

[2] Le constructeur appelle un macrobloc un assemblage de blocs simples génériques à la plateforme TXS (tels que des blocs logiques « ET » ou « OU ») afin de construire un macrobloc spécifique au projet de l'EPR FA3.

Toutefois, si la méthode de validation du logiciel est satisfaisante pour la mise en service du réacteur EPR FA3, l'IRSN considère qu'elle pourrait être améliorée en ce qui concerne la vérification de l'atteinte des objectifs des tests, cette vérification étant parfois effectuée de manière indirecte. En effet, quelques signaux à vérifier, spécifiés dans les objectifs de tests, ne sont pas observables. Sur ce point, EDF a pris un engagement à échéance de la visite complète n° 1 (VC1), au titre de l'amélioration continue de la validation, que l'IRSN estime satisfaisant car les fonctions concernées par des vérifications indirectes relèvent du fonctionnement en mode dégradé[3] du système de protection. **Cependant, pour l'IRSN, une analyse des avantages et des inconvénients d'une évolution du processus de spécification des tests de validation du logiciel visant à observer tous les signaux utilisés dans les objectifs de test mériterait d'être effectuée par EDF.**

La phase de validation et d'intégration du système consiste à tester le PS-F1A dans son ensemble de façon à s'assurer qu'il fonctionne conformément à ses exigences fonctionnelles et de performance[4]. La garantie forte apportée par cette phase est l'exécution de tous les tests de validation et d'intégration du système sur la version 7.2 du PS-F1A. Ainsi, non seulement les parties du système ayant évolué sont validées selon les nouvelles exigences fonctionnelles, mais la non-régression des autres parties est aussi assurée. Au cours de cette phase, plusieurs tests ont produit des résultats non conformes aux attentes pour lesquels EDF a justifié qu'ils étaient associés à des erreurs dans la rédaction de certains scénarii de test et qu'ils ne remettaient pas en cause la validité du logiciel, ce dont l'IRSN convient. Par ailleurs, l'IRSN s'est assuré que l'enchaînement des activités de validation et d'intégration du PS-F1A est réalisé conformément au PQS et estime ainsi que la réalisation de cette phase est satisfaisante pour la mise en service.

Pour clôturer la campagne de validation et de vérification, dont les deux phases décrites précédemment font partie, le constructeur a établi un rapport de vérification et de validation justifiant que toutes les activités exigées par le PQS ont bien été réalisées par les intervenants spécifiés. Ce rapport synthétise aussi tous les résultats obtenus lors de l'exécution de ces activités. L'IRSN estime que la réalisation de la campagne de V&V est conforme au PQS.

Par ailleurs, EDF réalise une analyse systématique visant à garantir l'absence d'erreur d'exécution du logiciel, ce qui constitue un élément supplémentaire au processus de développement du constructeur pour garantir que le PS-F1A fonctionne conformément à ses spécifications. Bien que cette analyse n'ait pas été conclusive sur tous les points, elle n'a pas révélé de défaut ayant un impact sur le fonctionnement du système dans les conditions précises de son utilisation à Flamanville, ce que l'IRSN estime satisfaisant.

3. EXPERTISE DES ACTIONS MENÉES À LA SUITE DES AVIS CITÉS EN RÉFÉRENCE

EDF et le constructeur se sont engagés, à la suite de l'avis [1], à développer un outil dédié à la vérification de l'absence de dépendances non spécifiées pour chacune des sorties du PS-F1A. EDF a réalisé complètement cette analyse et en a transmis les résultats qui révèlent la présence d'une erreur de conception dans le logiciel du PS-F1A. Cette erreur n'a été piégée ni par les actions de vérification ni par les phases de validation et d'intégration, ce qui renforce la pertinence d'intégrer cette vérification systématique de dépendances dans le PQS. EDF justifie toutefois que cette erreur de conception du PS-F1A a un impact négligeable sur la sûreté et ne projette de la corriger qu'en VC1, ce que l'IRSN estime satisfaisant.

Par ailleurs, une erreur dans la déclinaison des exigences fonctionnelles dans le système de protection a été constatée par EDF lors des essais de démarrage du réacteur [2]. La correction de ce défaut a motivé la réalisation

[3] Le PS-F1A est conçu pour pouvoir fonctionner en mode dégradé, c'est-à-dire en manipulant certains signaux d'entrée invalides (défauts de capteurs par exemple).

[4] Les exigences de performance concernent principalement la précision et le temps de réponse du système.

de la toute dernière version du PS-F1A et a conduit EDF et le constructeur à vérifier de manière exhaustive la cohérence entre les exigences fonctionnelles et leur déclinaison dans les documents de conception du PS-F1A. La méthodologie de cette vérification a été expertisée dans l'avis [2] et, depuis, EDF a transmis les résultats qui mettent en évidence plusieurs différences entre les exigences fonctionnelles et les spécifications du PS-F1A. EDF a alors fourni une analyse de l'impact de ces écarts sur la sûreté. Cette analyse montre que dans la plupart des cas, il n'y a aucune différence de fonctionnement et que les cas présentant un fonctionnement en écart ne conduisent à aucun risque pour la sûreté. L'IRSN a examiné en de façon détaillée les éléments de justification apportés par EDF et conclut que le fonctionnement du PS-F1A est satisfaisant en l'état.

Enfin, à la suite de l'avis [2], l'ASN a demandé à EDF de justifier la robustesse du processus de modification des macroblocs et d'apporter des compléments sur la validation de la librairie de macroblocs du PS-F1A. Depuis, EDF a transmis les éléments attendus et la justification apportée montre que les actions nécessaires sont prises pour garantir la bonne implémentation de ces macroblocs. Concernant les compléments sur la validation de la librairie de macroblocs, EDF a identifié les macroblocs concernés par le manque de validation, puis a défini et exécuté de nouveaux tests. L'IRSN estime que les actions prises pour répondre aux deux demandes de l'ASN sont satisfaisantes.

4. CONCLUSION

Le système de protection (PS) de l'EPR de Flamanville est un système de contrôle-commande possédant une partie classée F1A (PS-F1A) qui joue un rôle essentiel pour la sûreté, puisqu'il réalise les fonctions automatiques, manuelles et de surveillance nécessaires pour atteindre l'état contrôlé dans les situations incidentelles et accidentelles relevant des conditions de fonctionnement de référence.

Cet avis finalise l'expertise de l'IRSN sur l'acceptabilité du PS-F1A. Au cours de cette expertise, l'IRSN a commencé par examiner le processus de développement applicable qui avait évolué depuis les expertises antérieures de ce système. Des faiblesses du processus ont été identifiées au niveau de la déclinaison des exigences fonctionnelles amont au système, dans la méthode de validation du logiciel, ainsi que dans l'analyse, la vérification et la validation des performances du système.

EDF et le constructeur du système de protection ont su apporter les améliorations nécessaires au processus et les appliquer à la version du système qui sera utilisée pour la mise en service du réacteur, ce qui est satisfaisant. De plus, EDF a effectué une vérification complète de la cohérence entre les exigences fonctionnelles de sûreté et celles déclinées dans le système de protection. Cette vérification et les actions d'amélioration du processus ont permis d'identifier des écarts dont EDF a justifié l'absence d'impact sur la sûreté.

Lors de l'expertise, l'IRSN a également examiné la mise en œuvre du processus de développement au travers des documents de spécification fonctionnelle, de conception, de spécifications de tests, de rapports de tests et de rapports de vérification et validation (V&V). De plus, dans certains cas, l'IRSN a utilisé ses propres outils pour appuyer ses conclusions, notamment sur la qualité de la validation. L'IRSN note à cet égard que des améliorations de la méthode de vérification de l'atteinte des objectifs de tests lorsque les signaux associés ne sont pas observables sont encore possibles de la part d'EDF.

En conclusion, l'IRSN estime que la version 7.2 du PS-F1A est satisfaisante en l'état pour la mise en service du réacteur EPR de Flamanville.

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

VALIDATION ÉLECTRONIQUE CERTIFIÉE IRSN
Hervé
BODINEAU
2023.06.26
09:53:00 +02'00'