AUTORITÉ DE SÛRETÉ NUCLÉAIRE
Direction des centrales nucléaires

RÉPUBLIQUE FRANÇAISE

Référence courrier : CODEP-DCN-2021-030820

Montrouge, le 8 juillet 2021

Monsieur le Directeur du projet Flamanville 3
EDF – Direction du projet Flamanville 3
97 avenue Pierre BROSSOLETTE
92120 MONTROUGE

Objet : Contrôle des installations nucléaires de base
Thème : Surveillance des AIP relatives au développement du logiciel du système de protection
Code : INSSN-DCN-2021-0297

Références :

[1] Arrêté du 7 février 2012 modifié fixant les règles générales relatives aux installations nucléaires de base
[2] 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
[3] Note Framatome NLE-F DC 113 - Teleperm XS based I&C systems quality plan
[4] Lettre ASN CODEP-DCN-2020-006024 du 14 février 2020 - Inspection INSSN-DCN-2020-0299
[5] Règle fondamentale de sûreté II.4.1.a relative aux logiciels des systèmes électriques classés de sûreté du 15 mai 2000
[6] Note Framatome NLE-F DM 10022 indice H – Verification Method for Teleperm XS Engineering Documents
[7] Note Framatome NLE-F DM 10030 indice B – TXS Engineering Procedure – Configuration Management
[8] Note EDF ECDD110065 indice H – MAN2 PR21 – Maîtriser les écarts sur nos activités

Monsieur le Directeur,

Dans le cadre des attributions de l'Autorité de sûreté nucléaire (ASN) fixées à l'article L. 592-22 du code de l'environnement et en vertu du second alinéa de l'article L. 596-14 du même code, une inspection a eu lieu le 7 juin 2021 dans les locaux de Framatome, fournisseur du logiciel du système de protection de Flamanville 3. Cette inspection portait sur la réalisation des activités importantes pour la protection (AIP), telles que définies dans l'arrêté en référence [1], afférentes au développement du logiciel du système de protection du réacteur EPR de Flamanville, ainsi que sur leur surveillance par EDF.

J'ai l'honneur de vous communiquer, ci-dessous, la synthèse de l'inspection ainsi que les principales demandes et observations qui résultent des constatations faites à cette occasion par les inspecteurs.

15, rue Louis Lejeune · CS 70013 · 92541 Montrouge cedex · France
Téléphone : +33 (0) 1 46 16 40 00 / Courriel : info@asn.fr
asn.fr

Synthèse de l'inspection

Le logiciel du système de protection du réacteur EPR de Flamanville assure des fonctions nécessaires à l'atteinte de l'état contrôlé en cas de transitoire, d'incident ou d'accident de référence. Ainsi, conformément aux Directives techniques en référence [2], le concepteur, Framatome, a mis en place des règles pour le développement de ce logiciel. Le développement du logiciel comporte les activités de conception, mais également les activités de vérification et de validation (V&V). Les règles pour le développement du logiciel de protection de Flamanville 3 sont décrites dans le plan qualité (PQS) en référence [3], lequel identifie les AIP soumises à la surveillance d'EDF conformément à l'arrêté en référence [1]. Pour assurer cette surveillance, EDF a recours à l'assistance d'Edvance.

L'inspection du 7 juin 2021 a porté sur l'application du processus de V&V, la gestion des écarts, le recueil et l'exploitation du retour d'expérience, la gestion des compétences et la surveillance d'EDF. Une inspection de l'ASN, portant également sur le développement du logiciel de système de protection, s'était déroulée dans les locaux de Framatome le 20 janvier 2020 et avait fait l'objet de la synthèse transmise par courrier en référence [4].

Concernant l'application du processus de V&V, le contrôle par sondage réalisé a permis aux inspecteurs de constater que certaines dispositions prévues par les notes méthodologiques référencées dans le PQS en référence [3] n'étaient pas respectées. Ces constats remettent en cause le principe d'évitement d'erreurs décrit dans la règle fondamentale de sûreté en référence [5], concourant à la démonstration de la fiabilité d'un logiciel, et conduisant à réaliser des efforts de rigueur pendant le développement d'un logiciel. Le contrôle des inspecteurs ayant été réalisé par sondage, il convient de mener un recensement des écarts aux processus de V&V ainsi qu'une analyse pour en évaluer les conséquences sur la fiabilité du logiciel.

Concernant la gestion des écarts, les inspecteurs considèrent que le processus de Framatome, qui conduit à identifier des actions visant à corriger les écarts, à en prévenir la répétition et à contrôler l'absence d'écarts similaires sur le logiciel développé est satisfaisant. Par ailleurs, l'examen par sondage réalisé par les inspecteurs montre que ces actions sont réalisées, et que leur réalisation fait l'objet d'une traçabilité adaptée. Toutefois, les inspecteurs ont constaté qu'un écart, détecté lors des essais de démarrage en 2019, n'avait pas fait l'objet d'une fiche de non-conformité par Framatome, et avait seulement fait l'objet d'un constat par EDF.

Concernant le recueil et l'exploitation du retour d'expérience, Framatome et Edvance ont présenté aux inspecteurs leurs processus respectifs visant à partager le retour d'expérience au sein des différents projets de réacteur EPR. EDF a également présenté comment elle examine si un réacteur EPR est concerné par le retour d'expérience issu d'un réacteur en fonctionnement. Les inspecteurs notent que ces processus permettent de mettre en relation les acteurs des différents projets, favorisant ainsi le partage du retour d'expérience. Toutefois, ils considèrent qu'un écart survenu sur un projet étranger, et qui, après analyse, s'avère être également présent sur le projet EPR de Flamanville, doit systématiquement conduire à une fiche d'écart et à son traitement spécifiquement au projet EPR de Flamanville.

Concernant la gestion des compétences, les inspecteurs notent que, dans la continuité de ce qui avait été observé en 2020, Framatome a poursuivi ses efforts afin de renforcer ses équipes de conception et

de V&V, ce qui est satisfaisant. De plus, les inspecteurs ont pu observer l'outil de gestion des compétences de Framatome, qui lui permet d'avoir une vision globale du niveau de compétences de chacun de ses agents, pour chacune des compétences identifiées. Cet outil qui présente des avantages pourrait toutefois être accompagné d'éléments détaillant par exemple les cibles et seuils de compétences à atteindre, ainsi que des critères objectifs permettant d'évaluer le niveau de compétences des agents.

Enfin, concernant la surveillance, dont une large partie fait l'objet d'une assistance par Edvance, les inspecteurs ont constaté qu'elle se limitait à un contrôle documentaire. Dans son courrier en référence [4], l'ASN avait pourtant demandé à EDF d'inclure, dans son programme de surveillance, la vérification du PQS en référence [3]. Les inspecteurs ont également constaté que les compétences ne faisaient pas l'objet d'une surveillance par EDF.

En conclusion, les inspecteurs ont constaté des lacunes dans l'application du PQS qui soulèvent des interrogations quant au processus de vérification et de validation mis en œuvre pour le développement du logiciel du système de protection. Ils considèrent qu'EDF doit engager rapidement une analyse détaillée de la bonne application du PQS, afin d'en déterminer les écarts, et d'en tirer les conclusions pertinentes sur son programme de surveillance et sur la fiabilité du logiciel du système de protection. En effet, les inspecteurs rappellent que les dispositions prévues par le plan qualité en référence [3] participent à la démonstration de la qualité du développement du logiciel. Par ailleurs, les inspecteurs considèrent que le processus de gestion des écarts de Framatome permet une compréhension fine de l'étendue et des causes des écarts, et qu'il constitue un outil d'amélioration du développement du logiciel satisfaisant. Toutefois, certains événements survenus doivent faire l'objet d'un enregistrement d'écart par Framatome.

❖

A. Demandes d'actions correctives

A.1. Réalisation des AIP et surveillance associée

Le PQS en référence [3] liste les AIP relatives au développement du logiciel de protection du réacteur EPR de Flamanville. Parmi les AIP recensées, figurent notamment les activités d'ingénierie visant à détailler et implémenter les spécifications du système. Les règles et méthodes associées à ces activités d'ingénierie sont définies dans la note de méthodologie en référence [6]. La note de méthodologie en référence [7], quant à elle, définit des règles et méthodes concernant la gestion de la configuration du logiciel. Ces notes sont référencées dans le PQS en référence [3].

Les inspecteurs ont contrôlé par sondage le respect des procédures décrites dans les notes méthodologiques en références [6] et [7]. Ils ont observé que certaines exigences décrites dans ces procédures n'étaient pas respectées. En particulier :

- le « *verification package header* », pour la vérification des diagrammes fonctionnels logiques, ne figure pas parmi les documents d'entrée. Ce document, requis par la note de méthodologie en référence [6], identifie le contenu du paquet à vérifier et enregistre les échanges entre les équipes de conception et de V&V ;
- l' « *indicator sheet* » n'est produite à aucune étape du cycle en V. Ce document, requis par la note de méthodologie en référence [6], synthétise les anomalies détectées à chaque vérification ;
- l'analyse d'impact d'une modification du logiciel, sur les procédures de tests déjà réalisées, n'est pas réalisée telle qu'elle est requise par la note de méthodologie en référence [7].

En séance, les représentants de Framatome ont indiqué aux inspecteurs qu'aucune analyse, ni demande de dérogation, n'avait été formulée pour justifier l'acceptabilité du non-respect de ces exigences.

L'ASN rappelle que, comme indiqué par la règle fondamentale de sûreté en référence [5], la démonstration de la fiabilité d'un logiciel est notamment apportée par le principe d'évitement d'erreurs pendant le développement de ce dernier, qui conduit par exemple à réaliser des efforts de rigueur concernant la formalisation et la réalisation des phases du cycle de développement. Compte tenu de l'importance du logiciel du système de protection dans la démonstration de sûreté, l'ASN considère que son développement doit respecter les règles et méthodes issues du PQS en référence [3] et des notes de méthodologie afférentes.

Par ailleurs, l'article L. 593-6-1 du code de l'environnement dispose que « *l'exploitant assure une surveillance des activités importantes pour la protection des intérêts mentionnés au même article L. 593-1 lorsqu'elles sont réalisées par des intervenants extérieurs* ». De plus, le I de l'article 2.2.2 de l'arrêté en référence [1] précise que la surveillance exercée sur les intervenants extérieurs doit permettre à l'exploitant de s'assurer « *que les opérations qu'ils réalisent, ou que les biens ou services qu'ils fournissent, respectent les exigences définies* ».

Interrogés par les inspecteurs, vos représentants ont indiqué que la surveillance réalisée sur ces AIP était limitée à un examen documentaire, et qu'ainsi, aucune surveillance de la bonne application des règles et méthodes prescrites par le PQS en référence [3] ou par les notes méthodologiques afférentes n'était réalisée. Votre surveillance ne vous permet donc pas de vous assurer que les opérations réalisées respectent les exigences fixées par les notes méthodologiques, dont les notes en référence [6] et [7].

Dans sa lettre en référence [4], l'ASN vous avait demandé (demande A.2) « *d'inclure, dans le programme de surveillance, la vérification du respect du plan qualité* », constatant qu' « *en l'état, votre surveillance ne permet pas de contrôler que les AIP sont réalisées selon les règles préconisées par le plan qualité en référence* ». Malgré cette demande de l'ASN, votre programme de surveillance ne prévoit toujours pas d'activité de surveillance du respect du plan qualité.

En l'absence de la mise en œuvre de cette action corrective, l'ASN considère que la bonne application du plan qualité du logiciel de protection du réacteur EPR de Flamanville n'est pas établie.

Demande A.1 : Je vous demande d'engager rapidement une revue de la bonne application, par Framatome, des règles et méthodes prescrites dans le PQS en référence [3] et dans les notes qu'il référence. Vous me transmettrez la liste des écarts à ces règles et méthodes, ainsi que leur mode de traitement.

Demande A.2 : Je vous demande d'analyser l'effet cumulé des écarts identifiés en réponse à la demande A.1 du présent courrier sur la fiabilité de la conception du logiciel du système de protection du réacteur EPR de Flamanville. Vous me transmettrez les conclusions de cette analyse.

Demande A.3 : Je vous demande d'inclure, dans le programme de surveillance, la vérification du respect des règles et méthodes décrites dans le PQS en référence [3] et dans les notes qu'il référence. Vous justifierez la pertinence et le caractère suffisant de ce programme de surveillance, notamment à la lumière des conclusions des réponses aux demandes A.1 et A.2 du présent courrier.

L'article 2.5.5 de l'arrêté en référence [1] dispose que « *Les activités importantes pour la protection, leurs contrôles techniques, les actions de vérification et d'évaluation sont réalisés par des personnes ayant les compétences et qualification nécessaires. À cet effet, l'exploitant prend les dispositions utiles en matière de formation afin de maintenir ces compétences et qualifications pour son personnel, et, en tant que de besoin, les développer, et s'assure que les intervenants extérieurs prennent des dispositions analogues pour leurs personnels accomplissant les opérations susmentionnées* ».

Les inspecteurs ont interrogé vos représentants sur la vérification des compétences des intervenants extérieurs réalisant, contrôlant et vérifiant les AIP relatives au développement du logiciel du système de protection de l'EPR de Flamanville. Vos représentants ont indiqué aux inspecteurs qu'aucune action n'était conduite afin de s'assurer que Framatome, ou son sous-traitant, prenne des dispositions, en matière de formation, permettant de satisfaire aux exigences de l'article 2.5.5.

Demande A.4 : Je vous demande de vous assurer que les intervenants extérieurs réalisant, contrôlant, vérifiant et évaluant les AIP relatives au développement du logiciel du système de protection de l'EPR de Flamanville prennent des dispositions qui satisfont aux exigences de l'article 2.5.5 de l'arrêté en référence [1].

A.2. Gestion des écarts

Le système de gestion intégrée de Framatome prévoit l'ouverture d'une fiche de non-conformité (NCR) lors de la détection d'un écart. Une fois la NCR ouverte, Framatome procède à une analyse des causes profondes de l'écart et à la définition d'actions visant à le corriger, à en prévenir la répétition, et à s'assurer de son caractère isolé.

Les inspecteurs ont contrôlé par sondage la gestion des écarts, par Framatome et EDF, relatifs au développement du logiciel du système de protection de l'EPR de Flamanville. Ils ont constaté qu'un écart, concernant la programmation de signaux de mise en conformité, n'avait pas fait l'objet d'une NCR. Interrogés par les inspecteurs, ni vos représentants ni les représentants de Framatome n'ont été en mesure de justifier le fait qu'aucune NCR n'avait été créée. Votre système de gestion intégrée prévoit, par la note en référence [8], que la détection d'un écart fait l'objet d'une demande d'ouverture d'un écart chez le fournisseur.

Demande A.5 : Je vous demande de veiller à l'enregistrement d'un écart par Framatome lorsqu'un écart sur un de ses produits est détecté. Vous me transmettrez la NCR relative à l'écart susmentionné.

Les inspecteurs ont également interrogé vos représentants et les représentants de Framatome sur les écarts détectés sur les projets étrangers, et également présents sur l'EPR de Flamanville. Ces derniers ont indiqué aux inspecteurs que ces cas ne conduisaient pas systématiquement à l'enregistrement d'un écart propre au réacteur EPR de Flamanville, et que, le cas échéant, l'écart était traité uniquement par voie curative, en implémentant une modification identique à celle implémentée sur le réacteur pour lequel l'écart avait été détecté.

Ainsi, ces écarts ne conduisent ni à une analyse des causes techniques organisationnelles et humaines propres au projet EPR de Flamanville, ni à la définition d'actions visant à en prévenir la répétition, ou à s'assurer de leur caractère isolé.

L'ASN rappelle que le I de l'article 2.6.3 de l'arrêté en référence dispose que : « *L'exploitant s'assure, dans des délais adaptés aux enjeux, du traitement des écarts, qui consiste notamment à :*

- *déterminer ses causes techniques, organisationnelles et humaines ;*
- *définir les actions curatives, préventives et correctives appropriées ;*
- *mettre en œuvre les actions ainsi définies ;*
- *évaluer l'efficacité des actions mises en œuvre.*

Cependant, pour les écarts dont l'importance mineure pour la protection des intérêts mentionnés à l'article L. 593-1 du code de l'environnement est avérée, le traitement peut se limiter à la définition et à la mise en œuvre d'actions curatives. »

Demande A.6 : Je vous demande de veiller à l'enregistrement d'un écart à chaque fois qu'un écart détecté sur un réacteur EPR étranger est également présent sur le réacteur EPR de Flamanville et de le gérer conformément aux exigences décrites dans le chapitre VI du titre II de l'arrêté en référence [1].

B. Compléments d'information

B.1. Caractère suffisant des effectifs dédiés aux activités de conception et de V&V

Le II de l'article 2.5.2 de l'arrêté en référence [1] dispose que « *Les activités importantes pour la protection sont réalisées selon des modalités et avec des moyens permettant de satisfaire a priori les exigences définies pour ces activités et pour les éléments importants pour la protection concernés et de s'en assurer a posteriori.* ».

Les inspecteurs ont constaté que Framatome avait recours à un sous-traitant afin de l'assister dans la réalisation des activités de conception et de V&V. Les représentants de Framatome ont indiqué aux

inspecteurs que chaque livrable produit par un sous-traitant était assimilé et contrôlé par un personnel de Framatome. Interrogés sur les effectifs cibles à atteindre, au sein de Framatome, afin d'être en mesure de réaliser les activités de conception et de V&V, Framatome a répondu qu'il y avait seulement un objectif de croissance par rapport aux années précédentes.

Par ailleurs, les différents écarts détectés tardivement sur les précédentes versions du logiciel, ainsi que les constats à l'origine de la demande A1 du présent courrier, interrogent sur la bonne réalisation des activités de développement du TXS.

Au regard de ces éléments, les inspecteurs s'interrogent sur la façon dont Framatome évalue les effectifs et le temps nécessaires à la réalisation des activités, en particulier des activités de V&V.

Demande B.1 : Je vous demande de me préciser comment les effectifs et le temps nécessaires à la réalisation des activités de V&V et de conception des versions 7 et 7.1 sont évalués, au regard du volume d'activités et des exigences, règles et méthodes associées à ces dernières.

C. Observations

C.1. Caractère suffisant de la surveillance documentaire

Le programme de surveillance documentaire mené par Edvance prévoit trois niveaux de surveillance :

- surveillance de niveau 1 : vérification de forme du document ;
- surveillance de niveau 2 : vérification de niveau 1 et du fond du document (validité de la méthode de l'étude et vérification des ordres de grandeur des résultats obtenus) ;
- surveillance de niveau 3 : vérification de niveau 2 avec une analyse détaillée du contenu de l'étude (vérification des calculs effectués et contre calculs si nécessaire).

Les inspecteurs ont examiné en séance un écart survenu lors des essais de démarrage, concernant la spécification des capteurs du niveau de la cuve du réacteur. D'après l'analyse conduite dans le cadre du traitement de cet écart, une erreur d'interprétation de la spécification en serait à l'origine. Ce document avait fait l'objet d'une surveillance de niveau 1.

Si le traitement de l'écart est satisfaisant, sa survenue interroge sur la capacité de la surveillance à contrôler le respect des exigences définies, et sur la pertinence du niveau retenu pour la surveillance de ce document. En effet, le I de l'article 2.2.2 de l'arrêté en référence [1] dispose que : « *L'exploitant exerce sur les intervenants extérieurs une surveillance lui permettant de s'assurer :*

- *qu'ils appliquent sa politique mentionnée à l'article 2.3.1 et qui leur a été communiquée en application de l'article 2.3.2 ;*
- *que les opérations qu'ils réalisent, ou que les biens ou services qu'ils fournissent, respectent les exigences définies ;*
- *qu'ils respectent les dispositions mentionnées à l'article 2.2.1.*

Cette surveillance est proportionnée à l'importance, pour la démonstration mentionnée au deuxième alinéa de l'article L. 593-7 du code de l'environnement, des activités réalisées. Elle est documentée dans les conditions fixées à l'article 2.5.6. Elle est exercée par des personnes ayant les compétences et qualifications nécessaires. »

Observation 1 : Le retour d'expérience issu des écarts détectés devrait être intégré dans la construction du programme de surveillance. En particulier, il devrait conduire à une

ré-interrogation du niveau de surveillance retenu et des exigences définies que cette surveillance vise à contrôler.

C.2. Gestion des compétences

Les inspecteurs ont examiné la matrice de compétences utilisées par Framatome pour gérer les compétences de ses équipes en charge de la conception et de la V&V du logiciel du système de protection de l'EPR de Flamanville. Chaque compétence identifiée fait l'objet de quatre niveaux, dont les prérequis associés ne sont pas caractérisés. Les agents chargés de la réalisation ou du contrôle d'une AIP doivent au moins être de niveau deux dans chacune des compétences requises identifiées.

Les inspecteurs ont constaté que l'évaluation du niveau de compétences était réalisée à partir d'une autoévaluation de l'agent, suivie d'un entretien avec sa hiérarchie. Interrogés par les inspecteurs, les représentants de Framatome ont indiqué qu'il n'existait pas de critère permettant d'évaluer un niveau de compétences.

Observation 2 : Le niveau de compétences des agents réalisant, contrôlant, vérifiant et évaluant les AIP relatives au développement du logiciel du système de protection de l'EPR de Flamanville, pourrait être évalué au regard de critères objectifs, pour une compétence donnée.

C.3. Complétude du bilan de surveillance

Lors de l'examen du bilan de surveillance d'Edvance, les inspecteurs ont constaté qu'un nombre plus important de documents que celui indiqué dans le bilan de surveillance avait été surveillé. En particulier, certains documents transmis pour information font l'objet d'une surveillance, sans que cette dernière ne soit valorisée dans le bilan de surveillance.

Observation 3 : Le bilan de surveillance d'Edvance pourrait être complété par les documents effectivement surveillés bien qu'ils n'aient pas été initialement identifiés dans le programme de surveillance.

❖

Vous voudrez bien me faire part de vos observations et réponses concernant ces points dans un délai qui n'excèdera pas deux mois. Pour les engagements que vous seriez amené à prendre, je vous demande de bien vouloir les identifier clairement et de préciser, pour chacun, l'échéance de réalisation.

L'examen des réponses aux demandes A.1 et A.2 du présent courrier sera intégré à l'instruction en cours relative au contrôle-commande. Cet examen constitue un préalable à la prise de position de l'ASN sur la demande d'autorisation de mise en service du réacteur.

Conformément à la démarche de transparence et d'information du public instituée par les dispositions de l'article L. 125-13 du code de l'environnement, je vous informe que le présent courrier sera mis en ligne sur le site Internet de l'ASN (www.asn.fr).

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

Signé par :

Le directeur de la Direction des centrales nucléaires,

Rémy CATTEAU