RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

IRSN
INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 16 mars 2023

Monsieur le Président de l'Autorité de sûreté nucléaire

AVIS IRSN N° 2023-00042

Objet	:	**Projet EPR2 - Instruction anticipée en vue d'une demande d'autorisation de création d'une paire de réacteurs de type EPR2 : Interfaces homme machine (IHM).**
Réf.	**:**	Lettre ASN – CODEP-DCN-2022- 052632 du 2 décembre 2022.

1. CONTEXTE

À la suite de l'instruction du dossier d'options de sûreté (DOS) du réacteur EPR NM, EDF a proposé une évolution majeure pour l'interface homme machine (IHM) du réacteur de type EPR2. Cette évolution consiste à utiliser dans la salle de commande un même moyen de conduite principal (MCP) informatisé, de classe[1] de sûreté 2, tant pour la conduite en fonctionnement normal qu'en situations incidentelles et accidentelles. Ceci implique notamment que les informations sont remontées au MCP par une interface également de classe de sûreté 2. Concernant le MCP, les choix techniques retenus par EDF pour l'EPR2 s'appuient sur un système d'exploitation et un logiciel graphique tous deux issus de l'aéronautique ainsi qu'un ensemble de logiciels issus de l'informatique de conduite développée pour les réacteurs de 1450 MWe.

Par la lettre citée en référence, l'Autorité de sûreté nucléaire (ASN) sollicite l'avis de l'Institut de radioprotection et de sûreté nucléaire (IRSN) sur les choix technologiques et les processus de développement retenus par EDF pour la réalisation d'une plateforme de contrôle-commande informatisée de classe de sûreté 2 destinée à l'IHM principale de l'EPR2 (appelée IHM C2 dans la suite).

Pour répondre à la demande de l'ASN, l'IRSN a examiné la conformité des processus de développement retenus pour l'IHM C2 aux normes internationales (CEI 61513 et 62138) et à la règle fondamentale de sûreté (RFS II.4.1.a) applicables en la matière. Les choix technologiques concernant les logiciels pré-existants et les outils logiciels utilisés d'une part, ainsi que certains choix technologiques novateurs d'autre part, ont également fait l'objet d'une analyse de l'IRSN. Les conclusions de l'expertise réalisée par l'IRSN présentées ci-après tiennent compte des engagements pris par EDF concernant des justifications à apporter sur la plateforme de contrôle-commande de la classe de sûreté 2 qu'il entreprend de développer.

L'IRSN souligne dès à présent que le dossier présenté par EDF porte sur un prototype de plateforme de contrôle-commande et d'IHM, pour lequel des éléments restent à définir. En particulier, les plans et procédures détaillées

[1] Les systèmes de contrôle-commande importants pour la sûreté sont classés selon l'une des trois affectations possibles (1, 2, 3) suivant l'importance pour la sûreté des fonctions qu'ils assurent, la classe 1 correspondant au niveau le plus élevé.

des processus de développement ou encore le choix de certains matériels comme le processeur et la carte du calculateur reste à définir. Ainsi, l'IRSN ne préjuge pas des conclusions de son expertise du produit final.

2. EXAMEN DU PROCESSUS DU DÉVELOPPEMENT

Un système de contrôle-commande doit être matériellement fiable, disposer d'un logiciel de qualité et réaliser une logique exempte d'erreurs pour garantir qu'il assurera les fonctions de sûreté qui lui sont attribuées. Comme pour tout logiciel classé de sûreté, une logique exempte d'erreurs ne peut pas être garantie par le seul examen du système réalisé, les méthodes de détection d'erreurs par test et par analyse ne permettant pas de détecter exhaustivement les erreurs de conception. En conséquence, et comme le requiert l'état de l'art, EDF et ses partenaires industriels doivent définir et appliquer un processus de développement rigoureux permettant de justifier de l'atteinte du niveau de qualité requis pour le logiciel réalisé.

2.1. CONFORMITÉ AUX NORMES CEI61513 ET CEI62138

La norme CEI61513 précise les exigences et recommandations portant sur l'architecture, le processus de développement et les choix technologiques des systèmes de contrôle-commande classés de sûreté. En complément, la norme CEI62138 précise les exigences à appliquer pour le développement de logiciel et l'utilisation de logiciels pré-existants. En effet, le prototype de plateforme présenté par EDF est principalement constitué de composants logiciels pré-existants, et le processus de développement pour intégrer ces composants est supporté par de nombreux outils. Sur la base des éléments transmis par EDF, l'IRSN a pu évaluer les orientations prises par le projet EPR2, notamment sur le processus de développement et les dispositions prévues en termes de qualification des logiciels et des différents outils.

Le processus de développement de l'IHM C2 de l'EPR2 s'appuie sur le retour d'expérience de la méthodologie mise en œuvre par EDF dans le cadre du projet de modernisation des systèmes de contrôle-commande d'une centrale nucléaire à l'étranger. Bien que la norme employée dans ce projet soit différente de la norme CEI61513, **l'IRSN considère que la capitalisation de ce retour d'expérience est un point positif**.

La méthodologie mise en œuvre par EDF est itérative (réalisation de plusieurs versions successives du logiciel) et progressive (introduction de composants d'une version à l'autre). Le processus de développement est défini dans le plan de gestion du cycle de vie et de sûreté (SLMP) de l'IHM C2 qui adopte une approche système, qui traite l'ensemble des composants de la plateforme de contrôle-commande. L'IRSN considère que les phases de développement décrites dans le SLMP correspondent au modèle de phases du cycle de vie préconisé par la CEI61513.

Si la pratique industrielle conduit souvent à des processus de développement itératifs, l'IRSN note que le SLMP est lui-même élaboré de manière « itérative et progressive ». Pour l'IRSN, il peut être difficile de justifier qu'une version d'un développement satisfait a posteriori à un plan et des procédures ayant évolués dans le cadre d'une nouvelle version du SLMP. Sur ce point, EDF a précisé que les composants du produit prototype existant de l'IHM C2 et leurs documentations sont conformes au SLMP version P1 qui sera utilisé pour la réalisation de l'IHM C2 de l'EPR2, et ne nécessitent donc pas de mise à jour. **EDF a par ailleurs pris l'engagement N° 1 en annexe, que l'IRSN estime acceptable.**

EDF prévoit pour l'IHM C2, de s'appuyer sur une version déjà certifiée dans le domaine de l'aéronautique d'un système d'exploitation et d'un logiciel de type hyperviseur[2]. Ce dernier permet la virtualisation du système d'exploitation et la séparation, sur un même calculateur, des fonctions temps-réel (classe 2) des fonctions

[2] Un hyperviseur est une version réduite d'un système d'exploitation qui s'interface entre les couches logicielles d'un système d'exploitation classique et le matériel.

d'administration (classe 3)[3], comme la mise à jour des logiciels. Si l'IRSN considère satisfaisante cette stratégie, il note cependant que le système d'exploitation et l'hyperviseur utilisés pour l'IHM C2 seront différents des versions certifiées pour l'aéronautique sur deux points. Le premier concerne le choix du processeur (et de la carte) qui semble différent des processeurs pour lesquels une version certifiée du système d'exploitation existe, le second est relatif au besoin d'une douzaine de primitives supplémentaires pour la gestion des interfaces avec le logiciel applicatif, non présentes dans la version actuelle du système d'exploitation certifié. Dans les deux cas, cela signifie que le système d'exploitation devra être modifié par rapport à la version certifiée. Comme le système d'exploitation est un élément central et important dans le fonctionnement du calculateur, l'IRSN considère que chaque modification du système d'exploitation classé C2 doit être associée à une analyse d'impact sur son fonctionnement interne et sur les autres fonctions non modifiées. EDF devra justifier du maintien du périmètre de certification du système d'exploitation dans le dossier de qualification. **Sur ce point, EDF a pris l'engagement N° 2 en annexe que l'IRSN estime satisfaisant**.

Le système d'exploitation contient également les couches logicielles des « logiciels pilotes » (appelés communément « drivers ») des composants matériels réalisant les entrées-sorties du calculateur, ce qui incluent les drivers interfaces « USB Clavier-Souris », les drivers interfaces « série Clavier-Souris » et la pile de communication sur réseau internet. L'IRSN souligne la grande difficulté à qualifier un logiciel pilote USB qui peut être très complexe. Or la maîtrise des logiciels pilotes est indispensable à la maîtrise du comportement du système d'exploitation, et en conséquence, à la maîtrise des fonctions portées par ce système. De plus, selon l'IRSN, EDF doit démontrer que l'impact des collisions et réémissions sur les réseaux de communication est limité, borné et en toute circonstance sans conséquence sur les fonctionnalités de l'IHM C2. **Sur ces sujets, EDF a pris les engagements N° 3, N° 4 et N° 5 en annexe que l'IRSN estime satisfaisants**.

Parmi les autres logiciels pré-existants, l'IRSN a noté qu'une nouvelle version du composant d'administration du système d'exploitation (ADS)[4] était prévue pour prendre en compte notamment les résultats de l'étude de prédictibilité[5] de ce composant. Pour l'IRSN, EDF doit s'assurer que les mécanismes de synchronisation des différentes tâches utilisés par ce composant ne peuvent conduire à un blocage des tâches à exécuter, ce qui nécessite une analyse de la part d'EDF concernant la qualité de la conception du composant ADS. **Sur ce point, EDF a pris l'engagement N° 6 en annexe que l'IRSN estime satisfaisant.**

La catégorisation des outils logiciels dans le « plan d'assurance qualité » est une exigence de la norme CEI62138, qui vise à distinguer les outils susceptibles d'introduire des défauts (catégorie 1), ceux pouvant conduire à ne pas les détecter (catégorie 2) et ceux exempts d'impact (catégorie 3). Les exigences appliquées pour la sélection et l'utilisation de ces outils sont adaptées selon leur catégorie. Au cours de l'expertise, l'IRSN a constaté que des outils classés en catégorie 3 relevaient en fait de la catégorie 2. **Sur ce point, EDF a pris l'engagement N° 7 en annexe que l'IRSN estime satisfaisant.**

Par ailleurs, EDF prévoit que seuls les outils de la catégorie 1 fassent l'objet d'un dossier de qualification. Pour l'IRSN, l'assurance de la qualité du logiciel est portée autant par les activités de développement du logiciel que par les activités de vérification et de validation (V&V). Si les activités de V&V sont supportées (partiellement ou totalement) par des outils, il convient que ceux-ci aient un niveau de justification ou de qualification adapté à la fonction attendue dans le processus. **Sur ce sujet, EDF a pris l'engagement N° 8 en annexe que l'IRSN estime acceptable.**

---

[3] Le produit industriel final visé intégrera sur le même processeur multicœur deux versions différentes du système d'exploitation temps-réel, l'une classée C2, l'autre classée C3, et un hyperviseur.

[4] ADS : Il joue un rôle d'interface avec le système d'exploitation (gestion des tâches, ordonnancement des tâches, gestions des mémoires partagées…).

[5] Application de règles permettant de garantir qu'un système programmé effectue les actions qui lui sont assignées dans le logiciel d'application, dans les temps requis. L'étude de prédictibilité est demandée par la RFS II.4.1.a.

Parmi les outils utilisés, le compilateur Ada et sa libraire sont des outils de catégorie 1 qui font l'objet d'une analyse très détaillée qui couvre le cycle de vie de réalisation, la documentation d'utilisation et la documentation des tests de conformité. Le retour d'expérience est important notamment dans l'avionique[6] certifiée, et concerne de nombreuses plateformes. **L'IRSN considère que le travail d'analyse dans la démarche de qualification du compilateur Ada est satisfaisant.**

Le logiciel graphique de l'IHM C2 inclut un générateur de code certifié pour l'avionique qui utilise une librairie pour l'interface avec la carte graphique. Ce générateur de code est notamment certifié en tant qu'outil de développement pour les logiciels respectant la norme de l'aviation DO-178C DAL A et la norme CEI61508 SIL3, ce qui permet à EDF de revendiquer un niveau de certification CEI60880 qui est d'un niveau supérieur aux exigences de qualification d'un logiciel pré-existant de classe 2. L'IRSN constate que cette conclusion d'EDF est fondée uniquement sur un rapport de mise en correspondance des exigences de la norme CEI61508 SIL3 avec celles de la norme CEI60880. Pour l'IRSN, EDF devrait s'assurer que la démarche de certification du générateur de code répond bien à la norme CEI60880 ou à la norme CEI62138, **ce qui fait l'objet de son engagement N° 9 présenté en annexe**. De même, l'IRSN considère que la démarche de certification de la librairie et de ses composants devrait être conforme aux exigences de qualification d'un logiciel pré-existant de classe 2. **Sur ce point, EDF a pris l'engagement N° 10 en annexe que l'IRSN estime satisfaisant.**

2.2. CONFORMITÉ À LA RFS II.4.1.A

L'objet de la Règle fondamentale de sûreté II.4.1.a est « Principes et exigences à prendre en compte pour la conception, la réalisation, la mise en œuvre et l'exploitation des logiciels des systèmes électriques classés de sûreté ». Elle est structurée en énonçant le principe et les exigences à satisfaire pour les systèmes classés 1E (classe 1 pour l'EPR2) et pour les systèmes classés non 1E (classe 2 pour l'EPR2).

Pour la classe 2, le principe à satisfaire est celui de la prédictibilité. La démarche présentée par EDF consiste principalement à calculer le temps de réponse de la partie applicative, sans modélisation précise du fonctionnement interne du système d'exploitation. Pour l'IRSN, la démonstration de la prédictibilité doit concerner le logiciel dans son ensemble, à savoir la partie applicative, les logiciels pré-existants, le système d'exploitation et tous les composants. En conséquence, l'IRSN considère que la démonstration du respect du principe de prédictibilité de la RFS II.4.1.a pour les logiciels de classe 2 de l'EPR2 doit prendre en compte le fonctionnement interne du système d'exploitation. **Sur ce point, EDF a pris l'engagement N° 11 en annexe qui est satisfaisant.**

La prédictibilité repose également sur la maîtrise du fonctionnement du système multitâche. L'IRSN considère que les pratiques mises en œuvre pour garantir un fonctionnement cyclique de ce système sont satisfaisantes. À cet égard, l'IRSN a noté qu'une mesure de l'utilisation dynamique de la mémoire pendant l'exécution des tests du logiciel dans son environnement réel faisait défaut. À la fin de l'expertise, **EDF s'est engagé à la mettre en œuvre (*cf.* engagement N° 12 en annexe), ce qui est satisfaisant.**

Par ailleurs, l'utilisation d'un processeur multicœur (*cf.* § 3 ci-après) conduit à des difficultés additionnelles dans la mesure et l'estimation du temps de traitement d'un logiciel sur un cœur du processeur, son exécution n'étant pas totalement indépendante des traitements effectués sur les autres cœurs. Ainsi, pour l'IRSN, la démonstration de prédictibilité doit inclure des marges justifiées pour la détermination des temps d'exécution maximum à utiliser dans le calcul des temps de réponse du logiciel, tenant compte de l'architecture matérielle du processeur choisi. De plus, l'IRSN estime que la mesure des temps d'exécution devrait être fondée sur une méthode d'analyse des chemins d'exécution les plus longs du logiciel. **Sur ces points, EDF a pris les engagements N° 13 et 14 en annexe que l'IRSN estime satisfaisants**.

[6] L'avionique est l'ensemble des équipements électroniques, électriques et informatiques qui aident au pilotage des aéronefs.

3. CONSIDÉRATIONS SUPPLÉMENTAIRES CONCERNANT LES CHOIX TECHNOLOGIQUES

EDF propose d'utiliser une architecture matérielle fondée sur un processeur multicœur pour le moyen de conduite principal de classe de sûreté 2. Les processeurs multicœurs sont des systèmes multiprocesseurs intégrés sur une même puce de silicium. Ces processeurs multicœurs sont en conséquence bien plus performants et intégrés que les processeurs classiques (i.e. monocœur). Toutefois, les activités de vérification et de validation d'un composant logiciel s'appuient sur une exécution séquentielle du logiciel. Ainsi, il est nécessaire de démontrer que les différentes sources d'interférences d'un processeur multicœur avec le composant logiciel ne remettent pas en cause les résultats de son processus de V&V. Cette démonstration est possible en définissant des règles de conception du logiciel appropriées pour cet objectif, et par l'application rigoureuse de ces règles. Sous réserve des engagements pris par EDF et de la vérification que le choix définitif du processeur multicœur ne remet pas en cause les hypothèses permettant la démonstration de la prédictibilité, l'IRSN estime que l'utilisation d'un processeur multicœur est correctement appréhendée par EDF dans son dossier.

Enfin, l'IRSN considère que le choix d'une technologie de type hyperviseur est cohérent avec le choix d'une architecture de processeur multicœur car cela conduit à séparer au niveau de l'architecture logicielle les différentes exécutions sur chaque cœur du processeur, et surtout, permet de détecter toute tentative de violation de cette séparation. Pour la même raison, l'IRSN considère que l'utilisation d'un hyperviseur est cohérente avec l'objectif de faciliter la démonstration de l'innocuité du système d'exploitation classé C3 sur le système d'exploitation classé C2.

4. CONCLUSION

La réalisation d'une plateforme de contrôle-commande informatisée de classe de sûreté 2 destinée à l'IHM principale de l'EPR2 constitue une amélioration de sûreté par rapport aux autres réacteurs du parc en fonctionnement, car cette IHM permet de disposer d'un moyen de conduite principal classé de sûreté pour réaliser la conduite post-accidentelle.

Concernant la conformité du processus de développement de cette plateforme aux normes CEI61513 et CEI62138, l'IRSN considère que des compléments restent à apporter pour justifier cette conformité, notamment pour les processus de développement qui concernent les logiciels pré-existants et les outils logiciels. L'IRSN prend note des engagements d'EDF visant à renforcer les étapes du développement notamment des outils logiciels et de l'intégration de logiciels pré-existants.

Concernant la conformité à la RFS II.4.1.a, l'IRSN estime que les principes exposés sont globalement satisfaisants, mais que des compléments d'études et de justification de la part d'EDF au regard de la démonstration de la prédictibilité sont encore nécessaires. L'IRSN prend note des engagements d'EDF qui permettront d'apporter ces compléments.

Concernant les choix technologiques, l'IRSN estime qu'ils sont cohérents avec l'objectif d'intégrer deux versions différentes du système d'exploitation temps-réel sur le même processeur multicœur, aussi l'utilisation de l'hyperviseur apparaît adaptée.

Enfin, l'IRSN rappelle que cette expertise anticipée est fondée sur une version prototype de l'IHM C2 et qu'un certains nombres d'éléments restent encore à définir de la part d'EDF. Ainsi, l'IRSN ne préjuge pas des conclusions à venir sur le produit final de l'IHM C2.

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

Hervé BODINEAU
2023.03.16
19:36:48 +01'00'

ANNEXE À L'AVIS IRSN N° 2023-00042 DU 16 MARS 2023

Engagements principaux d'EDF

Engagement N° 1

EDF s'est engagé à transmettre le SLMP P1 au moment de la signature du contrat de réalisation de l'IHM C2 EPR2. EDF s'est engagé à transmettre, au plus un an[7] après la signature du contrat de réalisation de l'IHM C2 EPR2, le SLMP P2 qui sera utilisé pour développer le produit à venir. Ce SLMP va principalement évoluer par ajout de chapitres qui ne concernent pas les développements faits de 2018 à 2023 mais si tel était le cas, leur conformité au SLMP serait assurée.

Engagement N° 2

EDF s'est engagé à fournir, au plus tard trois ans après le début du contrat de réalisation IHM C2 EPR2, le dossier de qualification. Ce dossier de qualification présentera la justification que l'ajout des primitives n'affecte pas le fonctionnement de la partie certifiée du système d'exploitation. En amont, EDF s'est engagé à fournir, au plus tard un an après la signature du contrat de réalisation de l'IHM C2 EPR2, la stratégie de qualification de système d'exploitation.

Engagement N° 3

EDF s'est engagé à définir, au plus tard un an après la signature du contrat de réalisation de l'IHM C2 EPR2, la stratégie de qualification retenue pour les logiciels pilotes Clavier-Souris : USB, port série ou PS2.

Engagement N° 4

EDF s'est engagé à apporter, au plus tard quatre ans après la signature du contrat de réalisation de l'IHM C2 EPR2, la garantie que chaque logiciel pilote utilisé dans les systèmes classés C2 est qualifié avec des plans et procédures adaptés aux enjeux suivant la norme CEI 62138.

Engagement N° 5

EDF s'est engagé à apporter, au plus tard quatre ans après la signature du contrat de réalisation de l'IHM C2 EPR2, la garantie que l'impact des collisions et réémissions sur les réseaux de communications est limité, borné et en toute circonstance sans conséquence sur les fonctionnalités des IHM C2. En amont, EDF s'est engagé à fournir, au plus tard un an après la signature du contrat de réalisation de l'IHM C2 EPR2, la stratégie de justification envisagée.

Engagement N° 6

EDF s'est engagé à démontrer, au plus tard quatre ans après la signature du contrat de réalisation IHM C2 EPR2, par analyse du composant ADS, l'impossibilité d'un blocage dû au partage des ressources (processeur, mémoire, canaux de communication, etc.) entre tâches.

[7] EDF a rattaché ses engagements à la date de « début du contrat de réalisation » et mentionné des échéances allant jusqu'à 4 ou 5 ans après cette date. Comme il est actuellement prévu que ce contrat débute au premier semestre 2023, la réponse à certains de ces engagements n'interviendra donc qu'après la date prévue pour la publication du décret d'autorisation de création (2027). Ceci est acceptable pour l'IRSN qui considère que ces points ne constituent pas un prérequis pour l'obtention de ce décret.

Engagement N° 7

EDF s'est engagé à apporter, au plus tard quatre ans après la signature du contrat de réalisation IHM C2 EPR2, la garantie que la liste des outils logiciels utilisés dans le projet de la plateforme de l'IHM C2 est complète et que les informations portant sur leur catégorisation sont conformes au §6.1.4 de la CEI62138. En amont, EDF s'est engagé à fournir, au plus tard un an après la signature du contrat de réalisation IHM C2 EPR2, une version intermédiaire de la liste des outils logiciels.

Engagement N° 8

EDF s'est engagé à démontrer, au plus tard cinq ans après la signature du contrat de réalisation de l'IHM C2 EPR2, que le niveau de qualité des outils logiciels permettant la détection de défaut et nécessaires pour la démonstration de prédictibilité est en adéquation avec les conséquences des défauts dont ils pourraient rater la détection. En amont, EDF s'est engagé à fournir, au plus tard un an après la signature du contrat de réalisation de l'IHM C2 EPR2, la liste des outils logiciels concernés par ces justifications supplémentaires à la norme CEI62138.

Engagement N° 9

EDF s'est engagé à s'assurer que l'outil de génération du code graphique est conforme à la norme CEI 62138 édition 2018 (clause 6.2.4).

Engagement N° 10

EDF s'est engagé à s'assurer que le driver graphique est conforme à la norme CEI 62138 édition 2018 (clause 6.3).

Engagement N° 11

EDF s'est engagé à s'assurer, au plus tard cinq ans après la signature du contrat de réalisation de l'IHM C2 EPR2, que la démonstration du respect du principe de prédictibilité de la RFS II.4.1.a pour les logiciels classés C2 de l'EPR2 s'appuie sur un modèle validé de fonctionnement du système d'exploitation (ordonnancement des tâches, gestion de priorités, gestion de ressources partagées, etc.). En amont, EDF s'est engagé à fournir au plus tard un an après la signature du contrat de réalisation de l'IHM C2 EPR2, la stratégie de représentation du système d'exploitation dans le modèle de prédictibilité.

Engagement N° 12

EDF s'est engagé à ce que la mesure de l'utilisation de la pile sera réalisée par test et que le rapport de test fourni présentera ces résultats.

Engagement N° 13

EDF s'est engagé à s'assurer que la démonstration de conformité à la RFS II.4.1.a des logiciels classés C2 de l'EPR2 inclut des marges justifiées pour la détermination des temps d'exécution maximum utilisés dans le calcul des temps de réponse du logiciel, tenant compte de l'architecture matérielle du processeur choisi.

Engagement N° 14

EDF s'est engagé à s'assurer, au plus tard quatre ans après la signature du contrat de réalisation de l'IHM C2 EPR2, que la mesure des temps d'exécution est fondée sur une méthode d'analyse des chemins d'exécution les plus longs permettant de justifier les temps d'exécution pris en compte pour la démonstration de la prédictibilité.