INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Fontenay-aux-Roses, le 31 janvier 2018

Monsieur le Président de l'Autorité de sûreté nucléaire

Avis IRSN/2018-00026

Objet : EPR Flamanville 3 - Examen de la qualification fonctionnelle renforcée des composants électriques programmés réalisant des fonctions de sûreté classées F1

Réf. Lettre ASN CODEP-DCN-2017-019590 du 16 mai 2017

Dans le cadre de l'instruction de la demande d'autorisation de mise en service du réacteur EPR de Flamanville (EPR-FA3), l'Autorité de sûreté nucléaire (ASN) a souhaité recueillir, par lettre en référence, l'avis de l'Institut de radioprotection et de sûreté nucléaire (IRSN) concernant, d'une part les dossiers de qualification fonctionnelle renforcée (DQFR) des composants électriques programmés (CEP) réalisant des fonctions de sûreté classées F1, d'autre part l'analyse faite par EDF relative à l'utilisation sur plusieurs niveaux de la défense en profondeur d'un même modèle de CEP.

# 1 CONTEXTE ET ENJEUX DE SÛRETÉ LIÉS À L'UTILISATION DES CEP

Les CEP, parfois aussi appelés « composants intelligents », sont de petits composants électriques. Il s'agit typiquement de capteurs, d'actionneurs, de relais ou encore d'afficheurs, qui ont comme caractéristique commune d'utiliser de la technologie numérique (logiciels, circuits numériques complexes…) pour réaliser des fonctions plus précises et plus sophistiquées que leurs équivalents en technologie conventionnelle. En raison de leurs avantages (meilleure précision, autotests, facilités de paramétrage, possibilité de communication par réseaux informatiques…), le recours à ce type de composants intelligents est croissant.

Les systèmes de contrôle-commande de l'EPR-FA3 qui réalisent des fonctions de sûreté classées au plus haut niveau (F1) utilisent ainsi quelques CEP.

Pour contribuer à l'accomplissement des fonctions classées de sûreté F1, les CEP doivent, comme leurs homologues réalisés en technologie conventionnelle, faire l'objet d'une qualification dite environnementale, destinée à démontrer leur bon fonctionnement dans toutes les conditions d'ambiance (température, séisme…) où ils sont requis. Cet aspect est examiné par

**Adresse Courrier**
BP 17
92262 Fontenay-aux-Roses
Cedex France

**Siège social**
31, av. de la Division Leclerc
92260 Fontenay-aux-Roses

Standard +33 (0)1 58 35 88 88

RCS Nanterre 8 440 546 018

l'IRSN dans le cadre plus global de l'évaluation de la qualification environnementale des équipements électriques.

Cependant, le recours à la technologie numérique introduit une certaine complexité dans des composants qui sont relativement simples lorsqu'ils sont réalisés en technologie conventionnelle. La démonstration de sûreté d'un CEP soulève ainsi une problématique proche de celle associée aux automates numériques utilisés pour réaliser des fonctions classées de sûreté. Les quelques essais de bon fonctionnement réalisés lors des campagnes de qualification ne suffisent pas à exclure, avec un niveau de confiance suffisant, une erreur dans la conception de la partie programmée. La démonstration nécessite ainsi la mise en œuvre d'une démarche spécifique afin d'éviter l'introduction d'erreurs aux différentes étapes du processus de développement du CEP et de la compléter par une approche méthodique de recherche et suppression de celles qui auraient, malgré tout, été introduites.

Enfin, pour renforcer la démonstration de sûreté, lorsqu'un même modèle de CEP est largement utilisé dans l'installation, les conséquences d'une défaillance de cause commune (DCC) qui affecterait simultanément tous les exemplaires de ce modèle doivent être analysées. Si ces conséquences remettent en cause la défense en profondeur, alors d'autres mesures de protection doivent être envisagées pour atteindre le même objectif de sûreté.

# 2 ANALYSE DE L'IRSN

**Analyse des DQFR de chaque modèle de CEP classé F1 pour l'EPR-FA3**

EDF a transmis, pour chaque modèle de CEP contribuant à la réalisation de fonctions de sûreté classées F1, un dossier de qualification fonctionnelle renforcée qui apporte les réponses techniques aux exigences de sûreté spécifiques à la technologie numérique.

L'analyse de l'IRSN a tout d'abord porté sur les DQFR des dix modèles de CEP réalisant des fonctions classées F1, ainsi que sur un modèle réalisant des fonctions classées F2, mais dont le DQFR revendique un niveau de classement F1.

L'IRSN note que les DQFR fournissent les éléments permettant de s'assurer que :

- l'organisation du développement et le niveau de détail de la spécification des fonctions permettent de se prémunir de l'introduction de défauts dans les CEP ;
- la complexité des CEP n'est pas plus importante que ce qui est nécessaire à l'accomplissement des fonctions qui leur sont dévolues, et la complexité ajoutée par des fonctions secondaires des CEP non utilisées reste limitée et n'est pas de nature à remettre en cause l'accomplissement de la ou des fonctions principales ;
- la vérification et la validation du fonctionnement des CEP permettent de rechercher et d'éliminer les défauts qui auraient malgré tout été introduits lors du développement ;
- l'emploi des CEP se limitera à celui d'un modèle équivalent en technologie conventionnelle, en s'interdisant l'utilisation ou en inhibant, lorsque cela est possible, toute fonctionnalité avancée propre aux CEP, telle que la communication par réseau informatique ;
- les risques d'un mauvais paramétrage sont maîtrisés par des procédures adéquates ;
- le retour d'expérience de l'utilisation des CEP est pertinent par rapport à l'utilisation prévue pour l'EPR-FA3 et constitue même, pour certains, un argument de bon fonctionnement à part entière.

**A l'issue de son analyse, l'IRSN estime que les justifications apportées dans les dossiers de qualification fonctionnelle renforcée sont satisfaisantes pour démontrer l'aptitude des CEP analysés à réaliser les fonctions de sûreté classées F1 pour l'EPR-FA3.**

Plus globalement, l'IRSN souligne l'effort fait par EDF pour limiter autant que possible le recours à des CEP pour la réalisation des fonctions classées F1 pour l'EPR-FA3 alors que l'utilisation de ce type de composants, par nature plus complexes que leurs homologues non programmés, est à présent d'un usage courant dans d'autres secteurs industriels.

**Analyse de la répartition des CEP dans l'architecture du contrôle-commande de l'EPR-FA3**

Lors de l'analyse menée dans le cadre de l'instruction de la réunion du groupe permanent d'experts pour les réacteurs du 1er décembre 2005, l'IRSN avait soulevé le besoin de renforcer la démonstration de sûreté en analysant les conséquences d'une DCC qui affecterait simultanément tous les exemplaires d'un modèle de CEP réalisant des fonctions classées F1. Cette préoccupation avait conduit EDF à s'engager à :

- « *identifier, pour chaque événement initiateur, les lignes de défense dans lesquelles chaque modèle de Composants Electriques Programmés (CEP) est utilisé ;*
- *éviter l'utilisation, pour un événement initiateur donné, d'un même modèle de CEP dans plusieurs lignes de défense.* »

EDF a ainsi inventorié tous les CEP réalisant des fonctions classées de sûreté F1 et F2 et a analysé de façon systématique leur répartition dans les trois lignes de défense visant à prévenir respectivement les incidents et les accidents, la fusion du cœur et des rejets précoces importants. L'inventaire fait ressortir 14 modèles de CEP, dont dix modèles réalisant des fonctions classées F1. Dans la majorité des cas, EDF a conclu que, pour un événement initiateur donné, la perte éventuelle d'un même modèle de CEP ne remet pas en cause la gestion de l'événement. Pour aboutir à cette conclusion, EDF a apporté des justifications montrant que la fonction de sûreté est assurée par d'autres moyens fonctionnellement diversifiés. Dans les quelques cas où ces justifications n'ont pas pu être apportées, EDF a conclu à la nécessité de diversifier une partie des CEP redondants par une autre technologie.

**L'IRSN estime, d'une part que la méthodologie d'EDF pour s'assurer de la prise en compte exhaustive des CEP dans l'analyse est satisfaisante, d'autre part que cette analyse et les justifications d'EDF sont également satisfaisantes. L'IRSN estime ainsi que la démonstration présentée par EDF est acceptable et que la perte simultanée de tous les exemplaires d'un même modèle de CEP cumulée à un événement initiateur ne remet pas en cause la gestion de ces événements.**

Pour le Directeur général et par délégation,

Thierry PAYEN

Adjoint à la Directrice des systèmes, des nouveaux réacteurs et des démarches de sûreté