

Synthèse du rapport de l'IRSN portant sur l'architecture du contrôle-commande du réacteur EPR de Flamanville 3 et les plateformes associées

À la demande de l'Autorité de Sûreté Nucléaire (ASN), l'IRSN a examiné les dispositions détaillées retenues par EDF pour la définition de l'architecture du contrôle-commande du réacteur Flamanville 3, premier réacteur de type EPR à être construit en France, et la mise en œuvre de cette architecture. Cet examen a abouti aux conclusions suivantes qui ont été présentées le 18 juin 2009 au Groupe Permanent pour les Réacteurs nucléaires (GPR).

Pour pouvoir être exploité de manière sûre, un réacteur a besoin de capteurs pour connaître l'état du procédé, d'automates pour traiter ces informations, ainsi que de commandes d'actionneurs pour agir en retour sur le procédé, soit directement et sans intervention de l'opérateur (cas des régulations et des séquences automatiques), soit après un « dialogue » avec l'opérateur en salle de conduite. Pour le réacteur EPR de Flamanville 3, comme cela est déjà le cas pour les tranches du palier N4, ce « dialogue » s'effectuera dans une large mesure au moyen d'une interface homme-machine (IHM) informatisée disposant de ses propres calculateurs.

Ces équipements contribuent à des degrés divers à la sûreté de l'installation. L'architecture du contrôle-commande, c'est-à-dire la manière dont ces équipements sont regroupés dans des systèmes, ou au contraire rendus indépendants (physiquement, électriquement, technologiquement, logiquement), doit donc être telle qu'aucun aléa plausible ne puisse conduire à une situation non prévue dans la démonstration de sûreté.

L'IRSN a examiné la robustesse de l'architecture du contrôle-commande du réacteur EPR de Flamanville 3 en passant en revue les dispositions prévues par EDF pour chaque type d'équipement et pour chaque type d'aléa.

Globalement, cet examen technique, rendu complexe notamment par le recours du concepteur à de nombreux équipements informatisés et par la recherche d'une certaine optimisation de l'architecture, a mis en évidence la présence de dispositions pertinentes de robustesse mais a également conduit l'IRSN à identifier plusieurs points qui doivent faire l'objet d'évolutions.

En premier lieu, l'IRSN estime qu'EDF doit renforcer l'indépendance des équipements de la classe de sûreté intermédiaire (F1B) par rapport aux équipements de la classe de sûreté la plus faible (F2) et aux équipements non classés de sûreté.

De plus, l'IRSN estime qu'EDF doit compléter la démonstration du classement F2 des calculateurs de l'IHM informatisée, qui s'avère difficile du fait de leur complexité. Par ailleurs, il préconise qu'au titre de la défense en profondeur, EDF dispose, pour une gamme plus large de situations, d'un moyen permettant de faire face à un dysfonctionnement de ces calculateurs.

Pour la réalisation de la partie informatisée du contrôle-commande, EDF a prévu d'utiliser deux plateformes¹.

¹ Une plateforme de contrôle-commande est une gamme d'équipements compatibles entre eux. Avec les outils d'ingénierie associés, elle permet de réaliser des systèmes de contrôle-commande par assemblage et mise en configuration d'équipements existants. Seules restent à programmer les fonctions d'applications spécifiques au système que l'on souhaite réaliser.

La première de ces plateformes (SPPA T2000) est un produit industriel éprouvé mais qui n'a pas été conçu spécifiquement pour des applications dans le domaine nucléaire. Dans les documents examinés, cette plateforme est utilisée pour réaliser des fonctions non classées de sûreté, mais aussi des fonctions de la classe de sûreté intermédiaire (F1B). EDF a donc établi un dossier visant à montrer l'aptitude de cette plateforme à réaliser ces fonctions F1B.

Après analyse de ce dossier, l'IRSN estime qu'EDF doit encore fournir des compléments significatifs aux démonstrations proposées ainsi qu'une partie importante de la documentation de développement et de vérification.

De plus, l'IRSN estime qu'EDF assure une meilleure séparation entre les outils de maintenance et les systèmes de sûreté lors de l'exploitation des installations.

Au titre de la défense en profondeur, l'IRSN recommande également qu'EDF consolide les dispositions permettant de faire face à une défaillance totale des équipements de cette plateforme afin de couvrir les situations de dimensionnement les moins probables (RRC-A).

La seconde plateforme est la plus importante pour la sûreté car elle est notamment utilisée pour réaliser le système de protection (système de la classe de sûreté la plus élevée, c'est-à-dire F1A).

Spécifiquement conçue pour les besoins de la sûreté nucléaire, cette plateforme a déjà fait l'objet d'examen par l'IRSN et d'avis du GPR, en juin 2004 puis en décembre 2005. EDF a transmis les compléments de démonstration jugés alors nécessaires ; l'IRSN considère qu'ils sont satisfaisants.

L'IRSN a intégré dans son examen l'éclairage apporté par les solutions proposées pour les projets de réacteurs EPR en Finlande et aux Etats-Unis. Les différences constatées résultent essentiellement de contextes réglementaires et industriels différents et aucune des dispositions envisagées à l'étranger n'apporte de solution répondant à l'ensemble des questions soulevées par l'analyse détaillée de l'IRSN.

En conclusion, le contrôle-commande du réacteur EPR de Flamanville 3 utilise des technologies plus complexes et s'avère plus intégré que ceux des paliers précédents. En particulier, les éléments suivants compliquent la démonstration de sûreté:

- l'adoption d'une approche reposant sur l'utilisation de deux plateformes industrielles ;
- la mise en réseaux systématique de tous les équipements informatisés ;
- le choix de conduire la tranche de manière privilégiée dans toutes les situations avec une IHM informatisée dont la sophistication permet d'assister fortement l'opérateur mais ne permet pas de lui attribuer un classement de sûreté élevé.

L'IRSN considère que cette évolution vers davantage de complexité soulève des problèmes de fond et que de futures conceptions ne devraient pas continuer à évoluer dans ce sens.