IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

16 juin 2011

Synthèse de l'analyse par l'IRSN de l'architecture et des plateformes du contrôle-commande du réacteur EPR de Flamanville 3

1. Contexte

1.1. Systèmes et fonctions du contrôle-commande

Le contrôle-commande est l'ensemble des capteurs, dispositifs de visualisation et de commande, calculateurs, relais et actionneurs qui permettent de connaître en permanence l'état d'un réacteur nucléaire et de le piloter. Il est organisé en « systèmes » dont certains participent aux fonctions fondamentales de sûreté : maîtrise de la réactivité, évacuation de la puissance résiduelle, confinement des substances radioactives.

Le degré d'automatisation des fonctions confiées au contrôle-commande varie du « tout automatique » au « manuel » (commande par les opérateurs d'un actionneur donné) en passant par l'enclenchement manuel d'automatismes parallèles ou séquentiels (actionneur isolé, groupe d'actionneurs tels que ceux correspondant à une pompe principale et à sa pompe de graissage, fonction complète…).

Les fonctions et systèmes de contrôle-commande sont « classés » en fonction de leur importance pour la sûreté (pour l'EPR : F1A (plus haut niveau), F1B, F2, non classé)) ; à chaque classe correspondent des exigences de conception, de vérification et de maintenance appropriées.

1.2. Exemples de systèmes de contrôle-commande classés de l'EPR

Le Système de Protection (PS), classé au plus haut niveau F1A, met en œuvre les fonctions automatiques à court terme (une demi-heure) en cas d'incident ou d'accident : il surveille en permanence l'état du réacteur sans participer à son pilotage et, si des limites prédéfinies sont franchies, il arrête le réacteur et déclenche les actions de sauvegarde nécessaires telles que l'injection d'eau borée.

Le Système d'Automatismes de Sûreté (SAS), de classement intermédiaire F1B, assure les fonctions post-accidentelles manuelles et automatiques nécessaires à moyen et long termes après la phase à court terme gérée de façon entièrement automatique par le Système de Protection.

Le Système d'Automatismes de tranche (PAS), classé F2, assure des fonctions de contrôle et de régulation en fonctionnement normal, ainsi que des fonctions de limitation destinées à éviter si possible l'arrêt automatique du réacteur par le Système de Protection.

Le Moyen de Conduite Principal (MCP), classé F2, fournit aux opérateurs l'interface informatisée qui leur permet de connaître l'état du réacteur et de le piloter.

Le Moyen de Conduite de Secours (MCS), classé F1B, fournit aux opérateurs l'interface conventionnelle (boutons poussoirs, voyants, afficheurs, etc.) qui leur permet d'amener le réacteur à l'arrêt sûr en cas de défaillance du MCP.

1.3. Plateformes de contrôle-commande

Les systèmes informatisés tels que PS, SAS ou MCP sont construits à partir d'ensembles de composants préexistants, dénommés « plateformes », développés et validés une fois pour toutes :

- cartes électroniques : interfaces avec différents capteurs et actionneurs, calculateurs, communications, affichages…,
- bibliothèques de logiciels fournissant des fonctions standardisées : accès à un capteur, communications, blocs de calcul tels que filtres, votes…,
- outils d'ingénierie permettant de configurer les composants matériels et logiciels standardisés nécessaires à un besoin donné, de développer les logiciels non standardisés nécessaires… ;
- outils de maintenance permettant de modifier des points de consigne, de diagnostiquer des pannes…

Les concepteurs du contrôle-commande construisent les systèmes tels que le PS en configurant les plateformes (choix du nombre de calculateurs, du nombre et du type de cartes, disposition des réseaux…) et en leur ajoutant les « logiciels d'application » spécifiques au cas considéré. Ces logiciels d'application n'ont à traiter que les fonctions de contrôle-commande proprement dites, et non les fonctions internes liées à l'électronique, à l'accès aux capteurs, à l'autosurveillance…

Le contrôle-commande de l'EPR utilise deux plateformes :

- le Teleperm XS ou TXS, fourni par AREVA, est utilisé pour le Système de Protection (PS, classé F1A) et d'autres systèmes, par exemple le Contrôle-Commande Accidents Graves (CCAG, classé F2). Cette plateforme a été développée spécifiquement pour les besoins des systèmes de sûreté nucléaires[1] ;
- le SPPA-T2000, fourni par SIEMENS, est utilisé pour le Système d'Automatismes de Sûreté (SAS, classé F1B), le PAS et le MCP (classés F2) ainsi que d'autres systèmes non classés. Cette plateforme a été développée selon les bonnes pratiques industrielles, mais pas spécifiquement selon les exigences nucléaires. Elle bénéficie d'un retour d'expérience favorable dans l'industrie.

1.4. Architecture du contrôle-commande

Les systèmes de contrôle-commande sont organisés selon l'architecture schématisée sur la figure présentée ci-dessous.

[1] Par exemple en respectant les exigences de la norme CEI 60880 pour le développement des logiciels.

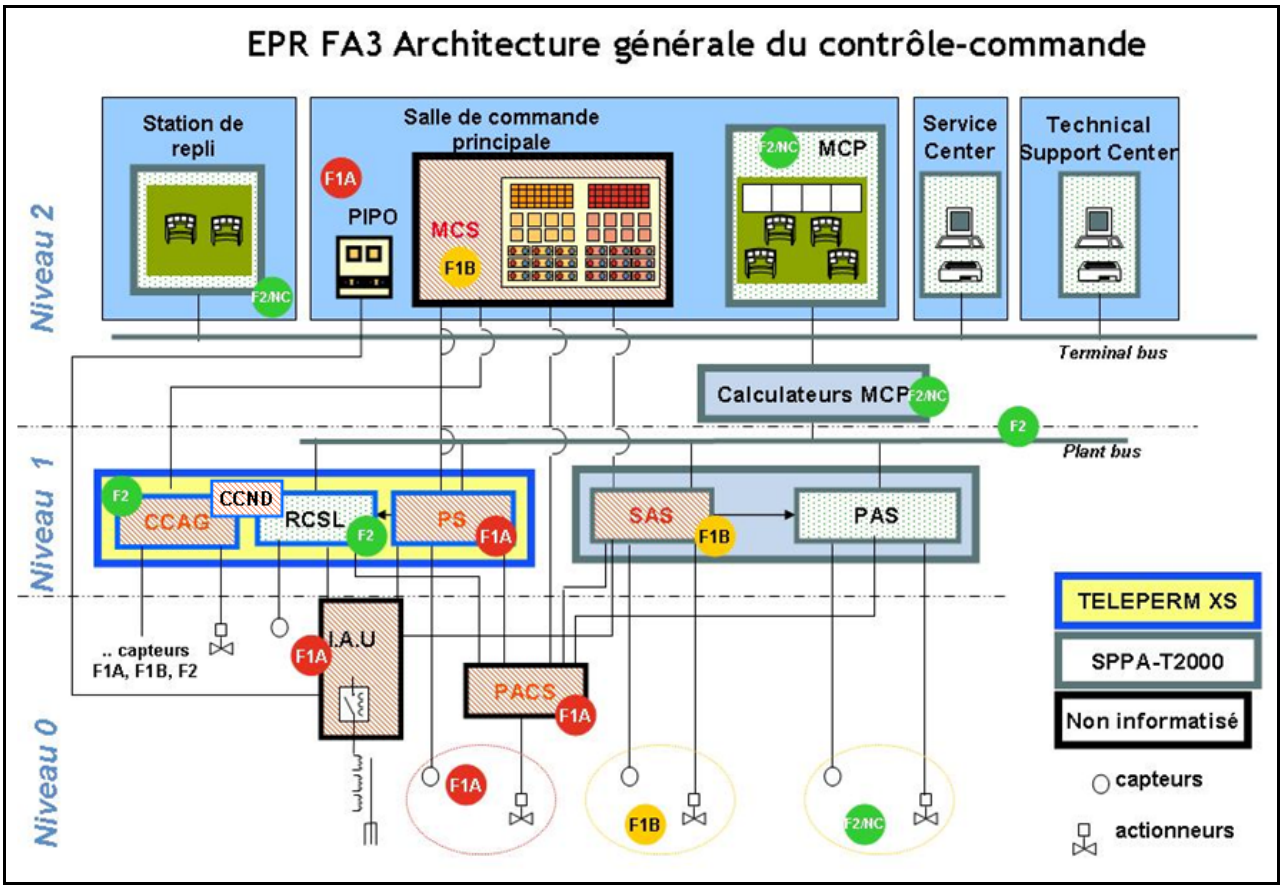
Cette architecture comporte les systèmes déjà mentionnés (PS, SAS, PAS, MCP, MCS, CCAG) et d'autres tels que le RCSL (fonctions de limitation destinées à prévenir le besoin d'actions de protection du PS), le PACS (gestion des priorités pour les actionneurs recevant des commandes de différents systèmes) et le Contrôle-Commande Noyau Dur (CCND), nouveau système qui sera présenté plus loin.

Le Pupitre Inter Postes Opérateurs (PIPO) est un ensemble de commandes manuelles câblées permettant aux opérateurs d'arrêter le réacteur s'ils doivent évacuer la salle de commande principale pour aller à la station de repli représentée en haut à gauche de la figure.

La boîte « IAU » symbolise les interrupteurs et disjoncteurs qui permettent au Système de Protection d'arrêter automatiquement le réacteur en coupant l'alimentation des électroaimants qui maintiennent les barres d'absorbants neutroniques, ce qui provoque leur descente dans le réacteur et stoppe la réaction en chaîne.

Des locaux dédiés abritent les moyens informatiques d'ingénierie et de diagnostic.

La figure ci-dessous indique le classement des systèmes et la plateforme utilisée pour les réaliser : TXS (cadre bleu), SPPA-T2000 (cadre gris) ou technologie conventionnelle à relais (cadre noir).



2. Méthode IRSN d'analyse du contrôle-commande

L'analyse du contrôle-commande comporte trois volets rappelés ci-après.

2.1. Evaluation de la capacité de chaque système à remplir ses fonctions

Il s'agit de s'assurer que les exigences assignées à chaque système sont bien identifiées et formalisées, que la conception garantit leur satisfaction dans tous les cas et que les actions de vérification et de validation apportent une autre garantie de cette adéquation. L'IRSN analyse ainsi les documents d'exigences, de conception, de vérification et de validation, les programmes informatiques en tant que de besoin, l'adéquation des plans de test…[2]

Dans le cas du contrôle-commande numérique, un aspect essentiel de cette évaluation concerne les plateformes qui sont conçues pour permettre des applications diverses et possèdent donc de nombreuses fonctionnalités : compatibilité avec des capteurs et actionneurs ayant des interfaces variées, large gamme de traitements élémentaires, communications, aptitude à l'autosurveillance et au diagnostic notamment. Cette approche permet aux logiciels d'application de n'effectuer « que » les traitements strictement fonctionnels : les aspects « informatiques » sont concentrés dans les plateformes. Une part importante de l'évaluation de l'IRSN a donc porté sur les plateformes.

2.2. Evaluation de l'architecture du contrôle-commande

Il s'agit dans un premier temps de s'assurer que chaque fonction demandée au contrôle-commande a été correctement allouée à un ou plusieurs systèmes de classements appropriés, que les interfaces des différents systèmes sont bien identifiées et cohérentes, que les interactions entre systèmes produisent les comportements globaux attendus…

Il s'agit ensuite d'évaluer la robustesse de l'architecture face aux défaillances envisageables et ses capacités en termes de défense en profondeur : bien que chaque système soit réalisé de façon à garantir son bon fonctionnement, sa défaillance est postulée (perte de la capacité d'effectuer ses fonctions) et est évaluée la capacité de l'architecture :

- à détecter cette défaillance,
- à empêcher sa propagation à d'autres systèmes,
- à la tolérer au moyen de redondances matérielles (duplication des éléments considérés) ou fonctionnelles (autres moyens permettant d'atteindre différemment le même objectif).

Les communications entre systèmes constituent un élément essentiel de l'architecture, car elles peuvent introduire des chemins de propagation des défaillances.

[2] A ce sujet, voir par exemple : Analyse de sûreté des systèmes informatisés : l'approche de l'IRSN

Idéalement, les communications entre systèmes de classements différents (a fortiori d'un « moins classé » à un « plus classé ») et entre systèmes assurant des fonctions différentes (a fortiori si l'un agit en secours de l'autre) devraient être évitées. Toutefois certaines communications sont indispensables, pour des raisons trouvant parfois leur origine en dehors du contrôle-commande. Par exemple :

- pour des raisons liées à un processus physique, certains actionneurs (vannes…) doivent être pilotés par des systèmes de classements différents selon que l'installation est en fonctionnement normal ou incidentel, ce qui nécessite la mise en place d'un système gérant les priorités au niveau des actionneurs (le PACS) ; ce système classé au plus haut niveau (F1A) reçoit donc des entrées du Système de Protection pour le fonctionnement incidentel, mais aussi de systèmes moins classés pour le fonctionnement normal ;
- pour des raisons ergonomiques, le MCP est utilisé par les opérateurs pour piloter le réacteur aussi bien en situation normale qu'en situation accidentelle, ce qui évite de les surcharger à un instant critique en leur imposant de changer de poste de travail lors d'un accident. Le MCP est donc nécessairement connecté à la fois à des systèmes classés F2 utilisés en fonctionnement normal et à des systèmes classés F1B utilisés en fonctionnement post-accidentel.

Les évaluateurs ne peuvent donc pas se limiter à interdire toute communication de façon dogmatique : ils doivent examiner l'utilité des communications prévues par le concepteur et s'assurer qu'elles ne compromettent pas la robustesse de l'architecture ; ceci nécessite une analyse détaillée.

Une présentation plus détaillée de cette démarche, appliquée au réacteur EPR de Flamanville 3, peut être consultée sur le site d'Eurosafe[3].

2.3. Qualification matérielle

Il s'agit de s'assurer que les matériels de contrôle-commande sont aptes à fonctionner pendant la durée prévue et dans les conditions d'environnement correspondant à leurs fonctions : température, humidité, rayonnement, séisme… Ce volet, plus usuel, n'est pas davantage présenté ici.

3. Rappel : évaluation de la plateforme Teleperm XS

La plateforme Teleperm XS a été développée spécifiquement selon les exigences imposées aux systèmes de sûreté nucléaire. Elle a fait l'objet d'évaluations par l'IRSN et d'avis du groupe permanent d'experts pour les réacteurs nucléaires (GPR) en juin 2004 puis en décembre 2005. EDF a transmis les compléments de démonstration jugés nécessaires, et l'IRSN a considéré dans son rapport préparé pour la réunion du GPR de juin 2009[4] qu'ils sont satisfaisants.

---

[3] Assessment of the overall Instrumentation & Control architecture of the EPR FA3 project.

[4] Synthèse du rapport de l'IRSN sur l'architecture et les plateformes du contrôle-commande du réacteur EPR en construction sur le site de Flamanville.

La plateforme Teleperm XS est donc jugée apte à réaliser des fonctions classées F1A, en particulier celles du Système de Protection.

4. Evaluation de la plateforme SPPA-T2000

Dans l'EPR de Flamanville 3, la plateforme SPPA-T2000 sert à réaliser :

- des fonctions de régulation et d'actionnement classées F1B (SAS) et F2 (PAS), en utilisant plus spécifiquement un ensemble de cartes électroniques et de logiciels dénommé « AS 620B »,
- des fonctions d'interface homme-machine classées F2 (MCP), en utilisant un ensemble de « stations de travail » (écran, clavier, ordinateur) et de logiciels dénommé « OM 690 ».

Dans son rapport présenté au GPR de juin 2009, l'IRSN avait souligné que cette plateforme bénéficiait d'un bon retour d'expérience, mais que la documentation de conception et de validation présentée (à l'époque) était insuffisante au regard des exigences de sûreté nucléaire.

De plus, l'interface homme-machine préférentiellement utilisée par les opérateurs pour réaliser les fonctions de conduite post-accidentelle classées F1B est le MCP (Moyen de Conduite Principal), sauf en cas de détection d'un dysfonctionnement motivant la décision d'utiliser le MCS (Moyen de Conduite de Secours, classé F1B). Le MCP n'étant classé que F2, l'IRSN avait estimé que ses éventuelles défaillances devaient être détectées par un moyen efficace classé F1B.

Après la réunion du GPR de juin 2009, EDF, AREVA NP et SIEMENS ont fourni un effort considérable (environ 13 000 heures de travail) pour, en particulier :

- démontrer que la conception et la validation des automates AS620B du SPPA-T2000 (utilisés pour réaliser le SAS classé F1B et le PAS classé F2) sont conformes aux exigences de sûreté nucléaire, en particulier aux exigences de la CEI 62138 et de la règle fondamentale de sûreté (RFS) II.4.1.a ;
- compléter la démonstration de la « prédictibilité » de l'AS620B (au sens de la RFS-II.4.1.a) ;
- justifier la suffisance des tests de l'AS620B ;
- modifier la plateforme pour introduire un moyen F1B de détection des défaillances plausibles du MCP, en couvrant ses fonctions de base et ses équipements.

Après examen, l'IRSN a considéré que les automates AS620B de la plateforme SPPA-T2000 sont aptes à réaliser les fonctions classées F1B du SAS, et a fortiori les fonctions classées F2 du PAS.

L'IRSN a également considéré que les modifications apportées à la plateforme permettent de détecter avec une confiance suffisante les éventuelles défaillances du MCP (classé F2) et d'informer les opérateurs de la nécessité d'utiliser le MCS (de technologie conventionnelle, classé F1B).

5. Evaluation de l'architecture

5.1. Séparation des systèmes de classements différents

Dans son rapport pour la réunion du GPR de juin 2009[5], l'IRSN avait estimé qu'une meilleure séparation devait être assurée entre les outils de maintenance et les systèmes de sûreté classés F2 et F1B pendant les phases d'exploitation des installations.

Après la réunion du GPR de juin 2009, EDF, AREVA NP et SIEMENS ont en particulier :

- modifié la plateforme de façon à garantir que les outils de maintenance et de diagnostic (non classés) ne pourront pas perturber le fonctionnement des automates AS620B du SAS (classé F1B) pendant les phases d'exploitation ;
- modifié la plateforme pour permettre de vérifier que la configuration des logiciels du MCP et de leurs paramètres, par exemple après une intervention avec les moyens d'ingénierie non classés, est conforme à la référence validée ;
- analysé l'influence des outils de maintenance et de diagnostic (non classés) sur le MCP classé F2 et montré qu'elle est en général compatible avec la capacité de traitement du MCP, ou conduit au pire à l'indisponibilité temporaire d'un calculateur dans un ensemble comportant plusieurs calculateurs redondants.

Après analyse, l'IRSN a considéré que les modifications apportées et les procédures mises en place ont permis de démontrer :

- **que les outils d'ingénierie et de diagnostic ne perturberont pas les fonctions des systèmes classés durant l'exploitation ;**
- **que la configuration du MCP après une intervention de maintenance restera conforme à l'état validé.**

L'instruction technique menée par l'IRSN avait également fait apparaître une autre difficulté relative à la séparation entre systèmes de classements différents : le MCP (Moyen de Conduite Principal, classé F2) peut transmettre au PS (Système de Protection, classé F1A) des commandes concernant l'activation ou la désactivation de certaines protections en fonction de l'état du réacteur. Par exemple une pression d'eau faible dans le circuit primaire lors du fonctionnement en puissance est anormale et nécessite des actions du Système de Protection (en particulier l'arrêt du réacteur) ; toutefois, une telle pression faible est normale lors du démarrage, quand le circuit primaire n'est pas encore sous pression, et la protection correspondante doit être désactivée dans cette phase. Ceci illustre le besoin d'un équilibre entre l'interdiction de transmettre des informations d'un système moins classé (le MCP) à un système plus classé

[5] Synthèse du rapport de l'IRSN sur l'architecture et les plateformes du contrôle-commande du réacteur EPR en construction sur le site de Flamanville.

(le PS) et la nécessité d'offrir aux opérateurs un poste de travail performant (le MCP) pour leur permettre d'effectuer leurs tâches dans les meilleures conditions.

EDF a proposé que les commandes transmises par le MCP au PS ne soient prises en compte que si l'opérateur appuie sur bouton poussoir classé F1 et indépendant du MCP. De plus l'opérateur vérifiera la bonne prise en compte de la commande par le PS.

Après analyse, l'IRSN a considéré que la solution proposée par EDF est acceptable.

5.2. Défense en profondeur

La capacité de la plateforme SPPA-T2000 à accueillir les fonctions F1B du SAS (gestion post-accidentelle) n'étant pas démontrée en 2009, l'ASN avait alors demandé à EDF d'étudier des dispositions de conception différentes pour faire face à une éventuelle défaillance de cette plateforme (il s'agissait par exemple de dupliquer ces fonctions dans un autre système, de technologie apte au classement F1B).

En réponse, EDF a prévu la mise en place d'un système dénommé CCND (Contrôle-Commande Noyau Dur étendu), réalisé avec la plateforme Teleperm XS, de façon à garantir la disponibilité des fonctions nécessaires à la conduite post-accidentelle en cas de défaillance totale de la plateforme SPPA-T2000.

Après analyse, compte tenu du fait que l'aptitude de la plateforme SPPA-T2000 à réaliser les fonctions post-accidentelles F1B du SAS est maintenant acquise, l'IRSN a considéré que le CCND est une disposition de robustesse complémentaire relevant de la défense en profondeur ; il n'a donc pas jugé nécessaire que le CCND soit classé au titre de sa contribution à l'architecture du contrôle-commande. Toutefois, l'IRSN a considéré qu'EDF devrait prendre des dispositions pour garantir la pérennité du CCND, notamment en formalisant son existence dans les documents de conception et dans le rapport de sûreté du réacteur EPR de Flamanville 3.

5.3. Maîtrise de la complexité de l'architecture

L'ajout d'un système complémentaire tel que le CCND a pour but d'accroître la tolérance de l'architecture du contrôle-commande aux défaillances du système normal (dans le cas présent, le SAS). Toutefois, il accroît aussi la complexité de cette architecture et peut conduire par exemple :

- à la nécessité d'introduire en aval de ces deux systèmes un dispositif de décision pour gérer le cas d'ordres contradictoires envoyés à un même actionneur en cas de défaillance d'un des deux systèmes. Une éventuelle défaillance de ce dispositif supplémentaire pourrait bloquer les ordres même corrects du système normal et aussi ceux du système de secours ;
- à un nombre accru de matériels, de types de matériels et d'interfaces avec les opérateurs, ce qui est susceptible d'augmenter le risque d'erreurs d'utilisation, de calibration... Le retour d'expérience suggère en effet que les principales contributions aux anomalies de mode commun des systèmes de

sûreté développés conformément à l'état de l'art sont en pratique associées à la maintenance et non à la conception, que ces systèmes soient numériques ou analogiques[6].

Par conséquent, l'intérêt d'un système complémentaire visant à augmenter la tolérance de l'architecture aux défaillances est à apprécier en tenant compte de la complexification de l'architecture et de la maintenance. Une analyse précise des exigences et de la conception du contrôle-commande doit donc être effectuée pour identifier les avantages et les inconvénients d'un système complémentaire.

Dans le cas du CCND, EDF a maîtrisé ces inconvénients :

- en utilisant pour le CCND la technologie sûre et maîtrisée du Système de Protection ;
- en tirant parti des commandes déjà prévues au MCS pour limiter l'ajout d'interfaces avec les opérateurs ;
- et en conservant une technologie conventionnelle à relais pour gérer les éventuelles commandes contradictoires émises par le SPPA-T2000 et le CCND.

Compte tenu des dispositions prises par EDF, l'IRSN a considéré que les avantages de l'introduction du CCND l'emportent sur les inconvénients.

6. Conclusion

L'IRSN a considéré que les deux plateformes de contrôle-commande retenues par EDF pour l'EPR de Flamanville 3, le Teleperm XS et le SPPA-T2000, sont aptes à assurer des fonctions classées respectivement jusqu'à F1A et jusqu'à F1B. L'acceptation de la seconde plateforme, non explicitement développée selon les exigences de sûreté nucléaire, a toutefois nécessité un travail d'analyse et d'adaptation très important.

L'IRSN a également noté les différences de l'architecture proposée pour Flamanville 3 avec les architectures proposées pour les projets de réacteurs EPR en Finlande, au Royaume-Uni et aux Etats-Unis, lors d'échanges techniques avec ses correspondants de ces pays. Les différences résultent essentiellement de contextes réglementaires et industriels différents.

En définitive, l'IRSN a considéré que l'architecture générale du contrôle-commande de l'EPR de Flamanville 3 est acceptable compte tenu des modifications apportées par EDF. Cependant, les nombreuses communications entre systèmes, souvent imposées par des raisons extérieures au contrôle-commande, ont nécessité, en plus de ces modifications, de nombreuses analyses détaillées pour démontrer qu'elles ne remettent pas en cause la robustesse de l'architecture.

[6] Voir par ex. J. Bickel, « Risk Implications of Digital RPS Operating Experience », 2007, AIEA