CHAPITRE 7
CONTROLE COMMANDE

SOMMAIRE

TABLEAUX :

.7.1 PRINCIPES DE CONCEPTION DU CONTROLE COMMANDE

0. EXIGENCES DE SÛRETÉ

0.1. CLASSIFICATION FONCTIONNELLE

Le classement de sûreté constitue la démarche formalisée et structurée qui permet d'identifier et de différencier les exigences spécifiques pour les systèmes et les matériels, en lien avec leur contribution aux objectifs de sûreté. La démarche est présentée dans la section 3.2.1.

S'agissant du contrôle-commande, un double classement a été adopté pour définir une classe de sûreté s'appliquant à une entité fonctionnelle (Classement système) et une autre s'appliquant à une entité technologique (Classement matériel).

Ces deux classements sont explicités ci-dessous :

- classement des systèmes contrôle-commande (F1A, F1B, F2): Ce classement fait référence à un ensemble d'éléments interconnectés constitué pour atteindre un objectif donné afin de réaliser une fonction définie.
- classement des matériels de contrôle-commande (E1A, E1B, E2) : ce classement fait référence à un ensemble d'éléments interconnectés constitué pour atteindre les performances attendues pour un ensemble défini de fonctions.

La relation qui existe entre le « classement fonctionnel », le « classement des systèmes de contrôle-commande » et le « classement des matériels de contrôle-commande » est précisée au tableau **TAB–7.1.1**.

Ce tableau indique les exigences essentielles à appliquer afin de réaliser les fonctions de sûreté requises et ce conformément au classement fonctionnel.

Des exigences de non perturbation portant sur les sous-systèmes de contrôle-commande moins classés vis-à-vis des sous-systèmes de contrôle-commande mieux classés, doivent être respectées conformément aux requis du RCC-E (paragraphe C 5232) :

« les sous-systèmes ayant des classes de sûreté différentes à l'intérieur d'un même système programmé doivent être organisés de façon telle qu'une défaillance d'un sous-système de classe inférieure ne dégrade pas les fonctions de sous-systèmes de classe supérieure ».

Cette exigence s'étend aux interfaces entre systèmes de contrôle-commande :

« les échanges d'information doivent être conçus de telle manière que le fonctionnement et la communication de données de fonctions classées de sûreté de classe supérieure ne puissent pas être perturbées par la communication de données avec des systèmes de classe inférieure ».

Toutes les fonctions F1 de contrôle-commande sont requises opérables en cas de séisme. Les fonctions F2 de contrôle-commande peuvent être ou non requises opérables en cas de séisme, c'est pourquoi on peut être amené à utiliser la distinction suivante dans les notations :

- fonctions F2 avec requis d'opérabilité en cas de séisme : fonctions F2E,
- fonctions F2 sans requis d'opérabilité en cas de séisme : fonctions F2N.

Le sous-chapitre 3.2 fournit de plus amples explications quant aux classements des fonctions, systèmes et équipements.

0.2. FONCTIONS DE SÛRETÉ

Les systèmes de contrôle-commande participent au respect des fonctions de sûreté suivantes :

- contrôle de la réactivité,
- évacuation de la puissance résiduelle,
- confinement des substances radioactives.

Pour le contrôle-commande, ces fonctions concernent :

- les fonctions F1A : Ces fonctions sont principalement assurées par :
  - le Système de Protection du réacteur PS assurant l'Arrêt Automatique du Réacteur, les Actions de Sauvegarde et les fonctions support de sauvegarde (cf. section 7.3.1),
  - le Système de gestion de Priorité et de Contrôle de l'Actionnement PACS (cf. section 7.3.6),
  - au niveau des systèmes de conduite, des structures d'accueil de commandes classées de sûreté F1A au Moyen de Conduite de Secours MCS, et au Pupitre Inter-Postes Opérateurs PIPO (cf. section 7.3.4) ; les commandes de basculement MCP/MCS, nécessaires à l'activation des commandes F1A implantées au MCS, sont également classées F1A.

  On compte également parmi les équipements de contrôle-commande assurant des fonctions F1A :
  - une interface dénommée Système de Pré-traitement de l'Instrumentation Procédé PIPS. Elle assure le découplage et le conditionnement des informations procédé classées de sûreté F1A et destinées à des systèmes moins classés,
  - certaines protections prioritaires des composants de systèmes F1A,
  - des équipements de contrôle-commande dédiés associés aux diesels principaux.
- Les fonctions F1B : ces fonctions sont principalement assurées par :
  - le Système d'Automatisme de Sûreté SAS de tranche (cf. section 7.3.2),
  - le Moyen de Conduite de Secours MCS (cf. section 7.3.3), complété par le Pupitre de Surveillance Inter Synoptique PSIS (cf. section 7.3.5), et le « signe de vie » F1B assurant la surveillance et la détection de la perte du MCP (**Réf [11]**).

  On compte également parmi les systèmes de contrôle-commande assurant des fonctions F1B le système d'automatisme dédié du DEL assurant des fonctions F1B de conditionnement et de ventilation des 4 divisions électriques des BAS/BL.
- les fonctions F2 : Ces fonctions sont principalement assurées par :
  - le Système d'Automatisme de tranche PAS (cf. section 7.4.2),
  - le Système d'Automatisme de Sûreté SAS de tranche (cf. section 7.3.2),
  - le Moyen de Conduite Principal MCP en salle de commande, ainsi qu'en station de repli (cf. section 7.4.1),
  - le système de Limitation, Surveillance et Contrôle du Réacteur RCSL (cf. section 7.4.3),
  - le système Contrôle-Commande Accident Grave CCAG (cf. section 7.4.4),
  - le Pupitre Accident Grave PAG (cf. section 7.4.6),
  - le Système d'Automatisme de Sûreté SAS-RRC-B (cf. section 7.4.5).

  On compte aussi parmi les systèmes de contrôle-commande assurant des fonctions F2, la centrale de détection incendie du système JDT.

0.3. EXIGENCES RELATIVES À LA CONCEPTION

Les exigences de sûreté pour les systèmes de contrôle-commande présentées dans le sous-chapitre 3.2 sont complétées comme suit.

0.3.1. EXIGENCES ISSUES DU CLASSEMENT FONCTIONNEL

0.3.1.1. CLASSEMENT FONCTIONNEL DES SYSTÈMES

Chacun des systèmes de contrôle-commande doit avoir un classement de sûreté conforme aux principes définis au sous-chapitre 3.2.

0.3.1.2. CRITÈRE DE DÉFAILLANCE UNIQUE (ACTIVE)

Le critère de défaillance unique doit être pris en compte dans la conception des systèmes de contrôle-commandes classés de sûreté F1.

Le critère de défaillance unique doit s'appliquer au niveau « système » pour les systèmes classés F1A (y compris durant une maintenance préventive ou un essai périodique du système considéré) et au niveau « fonctionnel » pour les systèmes classés F1B.

Sa prise en compte dans la conception du contrôle-commande fait l'objet du **§ 3.** du présent sous-chapitre.

0.3.1.3. ALIMENTATIONS ÉLECTRIQUES SECOURUES

L'alimentation électrique des systèmes de contrôle-commande classés F1 doit être secourue de sorte que ces systèmes doivent pouvoir continuer à assurer leurs missions même en cas de perte des alimentations électriques principales.

Cette alimentation doit être assurée par la même division à laquelle appartient le matériel de contrôle-commande considéré.

Cette disposition s'applique au cas par cas pour les systèmes de contrôle-commande classés de sûreté F2.

La prise en compte de ces exigences dans la conception commande fait l'objet du **§ 3.** du présent sous-chapitre.

0.3.1.4. QUALIFICATION AUX CONDITIONS DE FONCTIONNEMENT

Les systèmes de contrôle-commande classés doivent être qualifiés selon les exigences définies au sous-chapitre 3.7.

Les systèmes de contrôle-commande doivent être qualifiés en fonction de leur rôle sur le plan de la sûreté et des conditions d'ambiance auxquels ils sont soumis lors de l'accomplissement de leurs missions.

S'agissant de systèmes programmés, une démarche de qualification spécifique est associée et décrite dans la section 7.2.3. Cette démarche de qualification comporte des exigences hiérarchisées en fonction du classement de sûreté des matériels et des logiciels qui les constituent. Elle fournit le cadre de qualification des composants prédéveloppés (matériels et logiciels), fondée sur une spécification validée, des tests spécifiques, un retour d'expérience pertinent.

0.3.1.5. CLASSEMENTS MÉCANIQUE, ÉLECTRIQUE, CONTRÔLE COMMANDE

Les classements mécanique et électrique ne s'appliquent pas aux systèmes de contrôle-commande.

Le classement des systèmes de contrôle-commande se base sur :

- la catégorisation des fonctions de contrôle-commande de sûreté (classes des systèmes et équipements de contrôle-commande associés) conformément au classement des fonctions de sûreté (F1A, F1B, F2),

- la définition de trois classes de sûreté de matériel de contrôle-commande (E1A, E1B, E2) auxquelles s'ajoute une catégorie de matériels non-classés (NC).

Ces classes de sûreté de matériel de contrôle-commande sont définies comme suit :

- le matériel de contrôle-commande devant assurer des fonctions de sûreté F1A doit être classé E1A,
- le matériel de contrôle-commande devant assurer des fonctions de sûreté F1B doit être classé au moins E1B,
- le matériel de contrôle-commande devant assurer des fonctions de sûreté F2 doit être classé au moins E2.

0.3.1.6. CLASSEMENT SISMIQUE

Les systèmes de contrôle-commande doivent être classés au séisme selon les principes définis au sous-chapitre 3.2.

0.3.1.7. RÈGLES ET CODES DE CONCEPTION

Les systèmes de contrôle-commande classés F1 et F2 doivent se conformer au RCC-E, accompagné d'un cahier de Données de Projet (CDP) EPR - note EDF référencée ENSEMD050222 (voir sous-chapitre 1.6).

Le RCC-E s'inscrit en conformité avec les RFS et appelle les trois normes CEI suivantes :

- CEI 61513 : « I&C des systèmes IPS - Prescriptions générales pour les systèmes »,
- CEI 60880 : « I&C des systèmes IPS - Aspects logiciels des systèmes programmés réalisant des fonctions de sûreté de catégorie A »,
- CEI 62138 : « I&C des systèmes IPS – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie B ou C ».

0.3.2. AUTRES EXIGENCES RÉGLEMENTAIRES

0.3.2.1. RÈGLES FONDAMENTALES DE SÛRETÉ

Les RFS suivantes s'appliquent aux systèmes de contrôle-commande :

- RFS II.4.1.a – Logiciels des systèmes électriques classés de sûreté : cette RFS doit être prise en compte pour les systèmes électriques classés F1A et F1B ; les exigences relatives aux « logiciels des systèmes programmés classés 1E » sont à considérer pour les logiciels supportant des fonctions F1A alors que celles relatives aux « logiciels des systèmes programmés classés de sûreté et non classés 1E » sont à considérer pour les logiciels supportant des fonctions F1B.
- RFS IV.2. b – Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté : cette RFS doit être prise en compte pour les systèmes électriques classés F1A et F1B ; les exigences relatives « aux matériels électriques classés 1E » sont à considérer pour les systèmes de contrôle-commande F1A alors que celles relatives aux « matériels électriques classés de sûreté et non classés 1E » sont à considérer pour les systèmes de contrôle-commande F1B.

0.3.2.2. DIRECTIVES TECHNIQUES

Les directives techniques pour la conception et la construction de la nouvelle génération de tranches nucléaires REP énoncées dans la lettre DGSNR/SD2/0729/2004 du 28 septembre 2004 « Options de sûreté du projet de réacteur EPR », en particulier les paragraphes A1.2, A.2.2, B.2.1, B.2.2.2, C.2.1, G.3, G.4, doivent être prises en compte pour la conception des systèmes de contrôle-commande.

0.3.2.3. TEXTES SPÉCIFIQUES EPR

Ces exigences sont complétées par les demandes formulées par l'ASN dans les courriers en **Réf [14]**, **Réf [15]** et **Réf [16]** émis suite aux réunions du 18 juin 2009 et du 16 juin 2011 du Groupe Permanent Réacteurs tenues sur l'architecture du contrôle-commande EPR FA3.

0.3.3. AGRESSIONS

Les systèmes de contrôle-commande doivent être protégés vis-à-vis des conséquences des agressions internes et externes si leur perte remet en cause l'atteinte des objectifs de sûreté des sous-chapitres 3.3 (agressions externes) et 3.4 (agressions internes).

0.4. ESSAIS

Les systèmes de contrôle-commande doivent faire l'objet d'essais pré-opérationnels permettant de vérifier, après montage, leur conformité avec les exigences de conception.

Les systèmes de contrôle-commande classés F1, ainsi que les systèmes de contrôle-commande classés F2 pour les traitements qui ne sont pas sollicités en fonctionnement continu, sont assujettis aux essais périodiques afin de vérifier leur aptitude à remplir leurs fonctions.

0.5. EXIGENCES IHM

En salle de commande principale, l'interface homme-machine classée F1B, constituée par le Moyen de Conduite de Secours MCS, doit pallier l'indisponibilité du Moyen de Conduite Principal MCP. Le MCS doit pouvoir réaliser la démonstration de sûreté déterministe sur l'ensemble des conditions de fonctionnement PCC avec des équipements classés F1. Le MCS doit également, complémenté par les moyens de conduite PIPO et PAG, être en mesure d'assurer la gestion de certaines situations RRC (**Réf [14]**).

Le MCS ainsi que les moyens de conduite PIPO et PAG doivent être indépendants et diversifiés du MCP.

Le moyen appelé « signe de vie » permettant la détection et la signalisation, des défaillances de fonctions et d'équipements essentiels de l'IHM du MCP doit satisfaire aux exigences applicables aux fonctions et équipements F1B.

Le mécanisme de basculement du MCP vers le MCS, doit satisfaire aux exigences applicables aux fonctions et équipements F1A.

En plus de la salle de commande principale, une station de repli doit être mise en place pour le cas d'indisponibilité de la salle de commande principale. En cas d'indisponibilité de la salle de commande, les opérateurs doivent pouvoir assurer la surveillance et le repli de la tranche en état sûr à partir des postes opérateurs en station de repli.

Par ailleurs les moyens d'IHM du contrôle-commande doivent respecter les exigences d'interface homme-machine décrites au chapitre 17.

1. BASES DE CONCEPTION

1.1. ÉLÉMENTS STRUCTURANT LA CONCEPTION DE L'ARCHITECTURE DE CONTRÔLE COMMANDE

L'approche pour la conception de l'architecture de contrôle-commande afin d'atteindre les objectifs de sûreté est basée sur :

- la structuration de l'architecture de contrôle-commande en niveaux ;

- la prise en compte des exigences associées au classement fonctionnel de sûreté (cf. sous-chapitre 3.2) aux systèmes de contrôle-commande, comprenant en particulier :
  - l'application du critère de défaillance unique aux systèmes de contrôle-commande,
  - les principes de secours des alimentations électriques,
  - les requis de tenue au séisme,
- la catégorisation des fonctions de contrôle-commande de sûreté,
- le concept de défense en profondeur appliqué à l'architecture du contrôle-commande,
- la prise en compte des exigences de diversification et de traitement des risques de défaillances de cause commune,
- la gestion de la priorité entre les fonctions de contrôle-commande,
- la non perturbation entre systèmes et sous-systèmes classés de sûreté,
- la prise en compte des exigences vis-à-vis de l'IHM.

Les dispositions assurant le respect de ces exigences sont décrites dans les paragraphes à suivre.

1.2. ORGANISATION DU CONTRÔLE COMMANDE EN NIVEAUX

Les systèmes et équipements de contrôle-commande sont structurés en trois niveaux :

- niveau 0 : niveau d'interface avec le procédé. Il comprend principalement les fonctions de mesurage et d'actionnement (qui ont pour tâche de contrôler tant les actionneurs que les cellules électriques).
- niveau 1 : niveau abritant les automatismes. Il couvre les fonctions automatiques ainsi que les fonctions d'interface avec les autres systèmes et équipements.
- niveau 2 : niveau supervision et conduite de la tranche. Il comprend les fonctions permettant à l'opérateur de surveiller et conduire le procédé.

1.3. PRISE EN COMPTE DES EXIGENCES ASSOCIÉES AU CLASSEMENT DE SÛRETÉ

Parmi les exigences listées au **§ 0.3.** associées au classement de sûreté, celles structurant directement l'architecture sont les suivantes :

1.3.1. APPLICATION DU CRITERE DE DÉFAILLANCE UNIQUE

Conformément aux exigences de sûreté du , le critère de défaillance unique est pris en compte dans la conception des systèmes de contrôle-commande classés F1 par l'intégration d'un degré de redondance suffisant, d'une structure et de dispositions adéquates telles que la séparation physique et électrique, l'isolement et l'autonomie.

1.3.2. APPLICATION DE L'EXIGENCE DE SECOURS DES ALIMENTATIONS ÉLECTRIQUES

L'alimentation électrique des systèmes de contrôle-commande classés F1 ainsi que de certains systèmes de contrôle-commande classés F2 est secourue comme suit en cohérence avec les exigences de sûreté du paragraphe 0 du sous–chapitre 8.3, et avec les exigences de sûreté stipulées dans le **§ 0.3.1.3.** :

- L'alimentation des équipements de contrôle-commande considérés est secourue par la même division que celle à laquelle il appartient.
- L'alimentation des équipements de contrôle-commande considérés est secourue dans chaque division par un système d'alimentation sans coupure qui fournit une énergie électrique fiabilisée avec deux heures d'autonomie à pleine charge.

- L'alimentation des équipements de contrôle-commande considérés est secourue, en cas de manque de tension externe et d'échec ou d'impossibilité d'îlotage, dans chacune des divisions, par un groupe diesel principal disposant de [] jours d'autonomie à pleine charge.
- L'alimentation des équipements de contrôle-commande considérés est secourue, en cas de manque de tension Généralisé, de l'alimentation du contrôle-commande dans chacune des divisions 1 et 4, par un groupe diesel d'ultime secours disposant de [] heures d'autonomie à pleine charge.
- L'alimentation des systèmes de contrôle-commande participant à la gestion du scénario d'accident grave par perte de toutes les sources d'alimentation électrique externes et de toutes les sources internes de secours (diesels), est secourue par un système d'alimentation électrique dédié accident grave, fiabilisée avec [] heures d'autonomie à pleine charge.

De plus, les alimentations électriques de chaque système de contrôle-commande dans les divisions de l'îlot nucléaire, sont diversifiées par une double alimentation électrique continue et alternative. Cette disposition est issue du REX de l'incident de[] (document en **Réf [3]**) et pallie le risque de mode commun sur les sources électriques.

1.3.3. CONCEPTION RÉSISTANT AU SÉISME DE DIMENSIONNEMENT

Les principes d'allocation des fonctions de contrôle-commande selon le classement sismique des systèmes de contrôle-commande est le suivant :

- Les fonctions de contrôle-commande pour lesquelles l'opérabilité en cas de séisme est requise doivent être allouées dans des systèmes de contrôle-commande classés séisme SC1.
  - Toutes les fonctions de contrôle-commande classés de sûreté F1 sont allouées dans des systèmes dont le classement séisme est SC1.
  - Les fonctions de contrôle-commande classées F2E, donc requises opérables en cas de séisme, peuvent être allouées dans des systèmes de contrôle-commande classés de sûreté F1 sous réserve de non perturbation des traitements prioritaires F1 (cette disposition pratique permet de simplifier le contrôle-commande, notamment dans le cas où les fonctions F2E agissent sur les mêmes actionneurs que les fonctions F1).
- Les autres fonctions de contrôle-commande, i. e. non requises opérables en cas de séisme, doivent être allouées (au cas par cas) dans des systèmes de contrôle-commande classés séisme SC2, ou non classés séisme. Un classement SC2 de ces systèmes garantit que ces derniers ne puissent, en cas de séisme, porter atteinte aux systèmes de contrôle-commande classés SC1.

1.4. DÉFINITION DES CATÉGORIES DE FONCTIONS

Les fonctions de contrôle-commande sont réparties selon les principales catégories suivantes :

- les fonctions de contrôle,
- les fonctions LCO (Conditions limites d'exploitation),
- les fonctions de limitation,
- les fonctions d'aide opérateur,
- les fonctions de protection,
- les fonctions de gestion post-accidentelle,
- les fonctions spécifiquement conçues pour contrôler les agressions internes et externes,
- les fonctions assurant la gestion des situations de fonctionnement RRC-A,
- les fonctions assurant la gestion des situations d'accident grave.

Les fonctions du régime normal d'exploitation regroupent les fonctions gérant les conditions de fonctionnement de référence au plus PCC-1 ; elles recouvrent :

- les fonctions de contrôle qui sont les fonctions utilisées pour l'exploitation de la tranche dans toutes les situations de tranche,
- les fonctions d'aide opérateur qui sont des fonctions qui apportent une aide significative à l'opérateur pour l'exploitation de la tranche,
- Les fonctions LCO sont les fonctions mises en œuvre afin d'éviter une exploitation prolongée au delà des limites prises en compte dans la démonstration de sûreté. Ces fonctions initient des mesures correctives en cas de violation des conditions limites d'exploitation (LCO).
- Les fonctions de limitation sont des fonctions automatiques préventives apportant des mesures correctives afin d'éviter la sollicitation des fonctions de protection du PS et d'améliorer la disponibilité de la tranche.

Les fonctions de protection sont les fonctions qui sont nécessaires pour réduire les conséquences d'un événement initiateur PCC et rejoindre l'état contrôlé à la suite de la détection d'un tel PCC.

Les fonctions de gestion post-accidentelle sont les fonctions nécessaires pour ramener la tranche de l'état contrôlé à l'état sûr et la maintenir dans cet état après tout événement initiateur PCC-2 à PCC-4.

Les fonctions spécifiquement conçues pour contrôler les agressions internes et externes, sont les fonctions nécessaires à la prévention et au traitement des conséquences des agressions internes et externes (exemple : incendie, séisme,…).

Les fonctions RRC-A sont des fonctions spécifiques mises en œuvre afin de réduire les conséquences des différents conditions de fonctionnement avec défaillances multiples listées au chapitre 19 du RDS.

Les fonctions de gestion de l'accident grave sont des fonctions mises en œuvre pour éliminer pratiquement les situations d'accident avec fusion du cœur conduisant à des rejets précoces importants et limiter les conséquences des accidents avec fusion basse pression.

1.5. CONCEPT DE DÉFENSE EN PROFONDEUR

La sûreté de la tranche s'appuie sur le concept de défenseur en profondeur qui comprend les niveaux décrits en section 3.1.1.

Des exigences d'indépendance entre les fonctions appartenant à des lignes de défense différentes sont établies afin de respecter les critères de sûreté déterministes et les objectifs de sûreté des études probabilistes. Selon les chiffres de fiabilité pris en compte dans le Modèle de Défaillance (cf. chapitre 18), le traitement des initiateurs dont la fréquence d'occurrence est élevé peut nécessiter jusqu'à trois lignes de défense pour atteindre les objectifs de sûreté probabilistes.

Le tableau **TAB–7.1.2** présente les trois lignes de défense en profondeur qu'on retient pour les fonctions de contrôle-commande EPR (regroupées en catégorie de fonctions), définies en regard des trois grands objectifs de sûreté que sont :

- la prévention des incidents, accidents,
- la prévention du risque de fusion du cœur,
- la prévention du risque de rejets importants et précoces et limitations de conséquences en cas d'accident avec fusion du coeur.

Les fonctions de contrôle-commande participant à une séquence d'événements donnée sont ainsi allouées aux trois lignes de défense suivantes :

- ligne I : prévention des incidents et accidents : Cette ligne de défense préventive regroupe les fonctions de contrôle, d'aide opérateur, de limitation et de LCO (fonctions de surveillance des principaux paramètres du réacteur pris en compte comme conditions initiales des études de sûreté).
- ligne II : prévention du risque de fusion du cœur / combustible : Cette ligne de défense dite principale ou MAIN, regroupe les fonctions visant à atténuer l'effet des événements PCC-2 à

PCC-4 : fonctions de protection et de gestion post-accidentelle, ainsi que des agressions internes et externes et des situations de fonctionnement RRC-A,

- ligne III : prévention des risques de rejets importants et précoces : Cette ultime ligne de défense permet d'atténuer les conséquences et de limiter les rejets radiologiques en cas de fusion du cœur (situations accident grave).

La prise en compte à la conception d'un objectif de fiabilité globale du dispositif général de défense en profondeur est atteint :

- par la fiabilisation de chacune des lignes de défense en profondeur et des systèmes de contrôle-commande sur lesquels elles s'appuient pris isolément (redondance, diversification de certaines fonctions de protection),
- par une indépendance adéquate des lignes de défense entre elles de par l'organisation structurelle des systèmes et équipements de contrôle-commande (voir document en **Réf [7]**).

Le concept de défense en profondeur retenu pour le contrôle-commande, est présenté et justifié dans le document en **Réf [4]**.

Le concept de défense en profondeur est enfin renforcé par un certain nombre de mesures de robustesse listées dans le **§ 2.**, non requis au titre de la démonstration déterministe de sûreté et non nécessaires à l'atteinte des objectifs probabilistes de sûreté, mais permettant d'accroître la couverture de cumuls hautement improbables de défaillances du contrôle-commande supplémentaires.

1.6. DIVERSIFICATION ET TRAITEMENT DES RISQUES DE DÉFAILLANCE DE CAUSE COMMUNE

Les résultats des Etudes Probabilistes de Sûreté (EPS) peuvent conduire à rechercher à améliorer la fiabilité de certains systèmes, notamment en introduisant une certaine diversification.

L'utilisation de deux plates-formes de contrôle-commande diversifiées permet de prendre en compte de telles exigences de diversification sur certaines chaînes de contrôle-commande, dont le besoin est analysé au regard du respect des objectifs probabilistes.

C'est notamment le cas de la diversification de l'AAR pour certaines séquences ATWS.

Par la suite, la plate-forme de contrôle-commande diversifiée de celle assurant les fonctions de protection classées F1A est appelée « contrôle-commande standard ».

Par ailleurs, un faible niveau de risque de défaillances de causes communes qui pourraient être introduites au sein de chaque plate-forme de contrôle-commande retenue dans l'architecture du contrôle-commande, est recherché. Les documents en **Réf [5]** et **Réf [6]** fournissent la méthodologie et les justifications de l'atteinte de cet objectif.

Comme stipulé dans le RCC-E, ces exigences amènent à introduire « des mesures appropriées et proportionnées à l'importance des fonctions pour la sûreté pour faire face aux DCC afin d'atteindre et de maintenir la fiabilité requise ».

La diversification des plates-formes de contrôle-commande retenues pour EPR FA3 : plate-forme du système de protection de technologie TELEPERM XS, plate-forme du contrôle commande standard de technologie SPPA T2000, est démontrée dans le document en **Réf [1]** .

1.7. PRIORITÉ

Des commandes contradictoires (commande de sûreté vs commande d'exploitation ; commande manuelle vs commande automatique d'exploitation, etc.) peuvent être émises par les différentes fonctions de contrôle-commande à un même instant vers l'actionneur.

Une hiérarchisation prenant en compte le niveau de priorité défini pour chaque commande est établie conformément aux exigences de sûreté, et est traduite par des fonctions de vote aux sein des automates et des cellules électriques.

Les commandes de classement supérieur ont la priorité sur celles de moindre classement, induisant la hiérarchie suivante :

- commandes F1A prioritaires sur
- commandes F1B prioritaires sur
- commandes F2 prioritaires sur
- commandes Non Classées.

Les fonctions de gestion de priorité de commande sont détaillées dans la section 7.3.6 consacrée au système PACS.

1.8. NON PERTURBATION ENTRE SYSTÈMES ET SOUS-SYSTÈMES CLASSÉS

La conception du contrôle-commande doit garantir qu'une défaillance d'un système de classe inférieure ou d'un sous-système de classe inférieure à l'intérieur d'un même système programmé ne dégrade pas les fonctions des systèmes ou sous-systèmes de classe supérieure.

Entre systèmes de classes de sûreté différentes, cette exigence se traduit notamment par les dispositions suivantes :

- L'architecture des outils de programmation et de supervision, non classés, ainsi que leurs conditions d'utilisation, sont conçues afin de garantir la non perturbation du fonctionnement des systèmes de contrôle-commande classés. Ces dispositions font l'objet des documents en **Réf [8]** et **Réf [9]** en ce qui concerne les garanties de non perturbation des systèmes SAS par les systèmes moins classés, et des documents en **Réf [12]** et **Réf [13]** en ce qui concerne les garanties de non perturbation du MCP par les systèmes moins classés.
- Un mécanisme de validation classé F1B assure la non perturbation des traitements du système de protection par les commandes manuelles issues du MCP (F2), dont le rôle est d'inhiber ou d'activer certaines fonctions F1A du système de protection. Ces dispositions font l'objet du document en **Réf [10]**.

Au sein d'un même sous-système cette exigence se traduit par le fait que les fonctions de différentes catégories affectées au même sous-système sont développées selon les exigences correspondant à la classe de sûreté la plus élevée conformément au paragraphe 6.1.2.4 de la norme CEI 61513.

1.9. EXIGENCES IHM

Les dispositions assurant le respect des exigences formulées au **§ 0.5.** sont prises en compte dans la conception des moyens de conduite :

- en salle de commande principale, interface homme-machine classée F1B, couvrant l'indisponibilité du Moyen de Conduite Principal MCP sur l'ensemble des conditions de fonctionnement PCC ainsi que certaines situations RRC, avec les moyens de conduite PIPO / PAG,
- indépendance et diversification entre le MCP et l'ensemble MCS/PAG/PIPO,
- mise en place du « signe de vie » F1B. Ce dernier fait l'objet de la **Réf [11]**, qui en détaille la couverture,
- mécanisme de basculement F1A du MCP vers le MCS,
- mise en place d'une station de repli pour le cas d'indisponibilité de la salle de commande principale,
- respect des exigences d'interface homme-machine décrites au chapitre 17.

2. DISPOSITION DE ROBUSTESSE

2.1. PRINCIPE D'INTÉGRATION DE LA ROBUSTESSE DANS LA CONCEPTION

Des dispositions de robustesse sont introduites dans la conception du contrôle-commande. Elles visent à accroître la tolérance de l'architecture du contrôle-commande aux cumuls de situations de fonctionnement PCC-2, 3, 4, ou de certaines situations RRC, avec une situation hautement hypothétique de défaillance généralisée du contrôle commande standard.

Ces dispositions relèvent de la robustesse dans la mesure où elles ne sont pas requises au titre de la démonstration déterministe de sûreté et non nécessaires à l'atteinte des objectifs probabilistes de sûreté. Elles s'appuient par conséquent sur l'ensemble des équipements de contrôle-commande disponibles, classés ou non classés de sûreté, ainsi que sur des actions opérateur en local.

2.2. DISPOSITIONS NOYAU DUR

Un « Noyau dur » de fonctions insensibles à la perte totale du contrôle-commande standard est introduit en tant que disposition de robustesse complémentaire. Les fonctions constituant cette disposition sont implantées dans un équipement dédié, de technologie TELEPERM XS, qui constitue le système CC-ND : Contrôle-Commande Noyau Dur (décrit au sous-chapitre 7.2). Les fonctions implantées au sein du système CC-ND couvrent au titre de la robustesse, en cumul de la perte totale du contrôle-commande standard :

- des transitoires de catégories de fonctionnement PCC-2 à PCC-4,
- des situations RRC-A n'impliquant pas la défaillance d'une fonction F1 allouée au système de protection.

Les fonctions implantées au système CC-ND, complétées d'actions en local, visent à l'atteinte d'un état dit stable évitant la fusion du cœur et caractérisé par :

- le respect les critères de sûreté « cœur » de chaque catégorie d'accidents (première barrière),
- la préservation de l'intégrité du circuit primaire (deuxième barrière) pour les incidents les plus probables (PCC-2),
- le maintien de l'isolement de l'enceinte de confinement (troisième barrière) pour toutes les situations envisagées.

Les fonctions implantées au système CC-ND assurant la gestion des accidents impactant la piscine de désactivation suivent les objectifs de conception suivants :

- maintien permanent de la sous-criticité de la piscine de désactivation,
- absence de découvrement des assemblages combustible,
- maintien d'une marge significative vis-à-vis de l'ébullition de l'eau de la piscine de désactivation (PCC-2).

Les fonctions implantées au système CC-ND sont non classées de sûreté.

2.3. ROBUSTESSE DE LA CONDUITE DES SITUATIONS RRC-B À LA PERTE DU CONTRÔLE COMMANDE STANDARD

Par ailleurs, la conduite des situations d'accident grave est rendue robuste à la perte totale du contrôle-commande standard grâce à l'ensemble des moyens de contrôle commande subsistants et à la valorisation de certaines commandes opérateur en local. Cette robustesse est démontrée dans le document en **Réf [2]**.

3. TEL QUE RÉALISÉ

Il n'y a aucun écart entre le réalisé et les principes de conception définis dans ce chapitre.

LISTE DES RÉFÉRENCES

[1] ECECC050092 D, « Justification de la diversité entre la plate-forme SPPA-T2000 / S5 (F2) et la plate-forme TELEPERM XS (F1A) »

[2] ECEF093025 A, « Liste des fonctions à assurer en situation RRC-B et allocations associées dans les entités de contrôle-commande »

[3] ECEF070310 A, « Evolutions de la distribution électrique EPR suite au REX de l'incident [] du 25/07/06 »

[4] ECECC080669 C, « Architecture du contrôle-commande EPR FA3 : principes de conception et de défense en profondeur »

[5] ENSECC080054 A, « Analyse des DCCn au sein des systèmes supportant des fonctions classées de sûreté F1A (PS) de l'architecture de contrôle-commande de l'EPR FA3 »

[6] H-P1A-2007-02803 1.0, « Analyse des défaillances de cause commune dans l'architecture du Contrôle-commande basé sur la plate-forme SPPA T2000 et réalisant des fonctions classées de sûreté F1B (SAS) »

[7] ECECC080586 B, « Note de justification de l'indépendance des systèmes de contrôle-commande basés sur la plate-forme SPPA-T2000 »

[8] DN 2.2.25, "Justification of non perturbation of SAS by lower classified equipments"

[9] DN 2.5.04, " Description des mécanismes de chargement et vérification de la conformité du code chargé "

[10] ECECC091165 E, « Système de protection FA3 - Spécification technique du moyen matériel indépendant du MCP servant à valider les commandes informatisées du PS»

[11] ECECC091339, « Note de principes de surveillance F1B du MCP : Signe de vie étendu »

[12] DN 2.2.21 "Justification of non perturbation for [] and the Terminal Bus by []"

[13] DN 2.5.02, "Description of code loading mechanisms on MCP components and means to ensure the conformity of code loaded"

[14] Courrier Dép-DCN-0568-2009 - Réacteurs nucléaires à eau sous pression - Projet EPR - Flamanville 3 - Architecture générale du contrôle-commande et des plates-formes associées - Courrier ASN du 15/10/09

[15] Courrier CODEP-DCN-2010-036901 - Réacteurs nucléaires à eau sous pression - Projet EPR - Flamanville 3 – Démonstration de sûreté associée à la plate-forme de contrôle-commande SPPA T2000 - Courrier ASN du 9/07/10

[16] Courrier CODEP-DCN-2011–052544 — Réacteurs à eau sous pression — Projet EPR-Flamanville 3 — Architecture du contrôle-commande et plates-formes associées — Courrier ASN du 04/04/12

TAB–7.1.1 RELATION ENTRE CLASSEMENT FONCTIONNEL, CLASSEMENT SYSTÈME DE CONTRÔLE-COMMANDE ET CLASSEMENT MATÉRIEL DE CONTRÔLE-COMMANDE - EXIGENCES APPLICABLES AUX MATÉRIELS DE CONTRÔLE-COMMANDE

	Classement fonctionnel	**Classement système de contrôle-commande - Exigences applicables aux systèmes de contrôle-commande**	**Classement matériel de contrôle-commande - Exigences applicables aux matériels de contrôle-commande (qui réalise la fonction du plus haut niveau de classement)**
CLASSE DE SÛRETÉ	**F1A :** Cf. sous-chapitre 3.2	**F1A :** Cf. section 3.2.1	**Matériel E1A :** Conception et réalisation conformes aux exigences communes spécifiques déclinées dans le RCC-E (voir sous-chapitre 1.6). Programme d'Assurance de la Qualité appliqué aux activités liées au cycle de vie global du système. Qualification aux conditions de fonctionnement. Protection contre les agressions internes et externes. Qualification sismique. Aptitude aux essais périodiques. Aucune perte de fonction due à une défaillance même pendant la maintenance préventive ou les essais périodiques. Combinaison d'une défaillance unique avec la maintenance préventive ou l'essai périodique. Une défaillance ne doit pas générer d'événements PCC 3 ou PCC 4 même pendant la maintenance préventive ou les essais périodiques.

	Classement fonctionnel	**Classement système de contrôle-commande - Exigences applicables aux systèmes de contrôle-commande**	**Classement matériel de contrôle-commande - Exigences applicables aux matériels de contrôle-commande (qui réalise la fonction du plus haut niveau de classement)**
CLASSE DE SÛRETÉ	**F1B :** Cf. sous-chapitre 3.2	**Au moins F1B :** Cf. section 3.2.1	**Matériel E1B :** Conception et réalisation conformes aux exigences communes spécifiques déclinées dans le RCC-E (voir sous-chapitre 1.6). Programme d'Assurance de la Qualité appliqué aux activités liées au cycle de vie global du système. Qualification aux conditions de fonctionnement. Protection contre les agressions internes et externes. Qualification sismique. Aptitude aux essais périodiques. Aucune perte de fonction due à une défaillance même pendant la maintenance préventive ou les essais périodiques (au cas par cas). Combinaison d'une défaillance unique avec la maintenance préventive ou l'essai périodique au niveau de la fonction. Une défaillance ne doit pas générer d'événements PCC 3 ou PCC 4 même pendant la maintenance préventive ou les essais périodiques.

	Classement fonctionnel	**Classement système de contrôle-commande - Exigences applicables aux systèmes de contrôle-commande**	**Classement matériel de contrôle-commande - Exigences applicables aux matériels de contrôle-commande (qui réalise la fonction du plus haut niveau de classement)**
CLASSE DE SÛRETÉ	**F2 :** Cf. sous-chapitre 3.2	**Au moins F2 :** Cf. section 3.2.1	**Matériel E2 :** Les conception et réalisation doivent être conformes aux exigences définies par le code de conception et de construction. Un Programme d'Assurance de la Qualité doit être appliqué aux activités liées au cycle de vie global du système. Qualification aux conditions de fonctionnement. Tolérance des agressions internes et externes au cas par cas. *Lorsqu'un système F2 est utilisé pour mitiger les conséquences d'une agression interne ou externe, il ne doit pas être affecté (de manière inadmissible) par l'agression.* Qualification sismique au cas par cas. Aptitude aux essais périodiques (pour les traitements qui ne sont pas sollicités en fonctionnement continu). Prise en compte de la défaillance unique non requise au titre de la sûreté. *Lorsqu'un système F2 est utilisé en secours, il doit être séparé du système pour lequel il constitue un secours lorsqu'il peut être affecté par l'événement initiateur ou par les conséquences.* Une défaillance ne doit pas générer d'événements PCC-3 ou PCC-4 même pendant la maintenance préventive ou les essais périodiques.

TAB–7.1.2 RELATION ENTRE PRINCIPALES CATÉGORIES DE FONCTIONS DE CONTRÔLE-COMMANDE ET LIGNES DE DÉFENSE EN PROFONDEUR

<table>
<tr><th colspan="2">Catégorie de fonctions du contrôle-commande</th><th>Ligne de défense en profondeur</th></tr>
<tr><td colspan="2">NOP / LCO</td><td>Fonctions de contrôle en conduite normale et d’aide à l’opérateur.

Fonctions LCO (Conditions limites d’exploitation).</td><td rowspan="2">I. Prévention des incidents et accidents</td></tr>
<tr><td colspan="2">LIM</td><td>Fonctions de limitation.</td></tr>
<tr><td rowspan="3">MAIN</td><td>PCC 2 à 4</td><td>Fonctions de la ligne principale de défense visant à atténuer l'effet des événements PCC (PCC- 2 à PCC-4) :

- fonctions de protection (fonctions nécessaires pour atténuer les conséquences d’un PCC et rejoindre l’état contrôlé),

- fonctions de gestion post-accidentelle (fonctions nécessaires pour ramener la tranche de l’état contrôlé à l’état sûr).</td><td rowspan="3">II. Prévention du risque de fusion du cœur/combustible</td></tr>
<tr><td>Agressions</td><td>Fonctions spécifiquement conçues pour contrôler agression externe ou interne.</td></tr>
<tr><td>RRC-A</td><td>Fonctions RRC-A de réduction du risque de fusion du cœur, permettant d’atteindre l’état final.</td></tr>
<tr><td colspan="2">RRC-B

Accident grave</td><td>Fonctions de réduction du risque permettant de limiter les rejets radiologiques en cas d’accident grave.</td><td>III. Prévention du risque de rejets importants et précoces</td></tr>
</table>

7.2 ARCHITECTURE GÉNÉRALE DES SYSTÈMES ET ÉQUIPEMENTS DE CONTRÔLE-COMMANDE

SOMMAIRE

TABLEAUX :

FIGURES :

.7.2.1 ARCHITECTURE GÉNÉRALE DU CONTRÔLE-COMMANDE

1. VUE D'ENSEMBLE

L'architecture générale du contrôle-commande est présentée en figure **FIG–7.2.1.1**.

L'architecture générale du contrôle-commande est structurée en niveaux :

Niveau 0 : l'interface avec le procédé

Le procédé comprend :

- L'instrumentation incluant les capteurs, transducteurs et l'acquisition de données dans la mesure où elle est mise en œuvre dans les transducteurs numériques.
- Les cellules électriques et les actionneurs.
- Les interfaces entre le niveau 0 et le niveau 1 de l'architecture de contrôle-commande :
  - Interfaces PIPS : système de découplage, duplication et conditionnement des informations partagées entre plusieurs équipements de contrôle-commande,
  - Interface PACS : système de gestion de priorité et de contrôle de l'actionnement.

Niveau 1 : les automates

Comprenant l'acquisition de données, les traitements d'automatismes, la surveillance et la commande, mis en oeuvre dans :

- Des systèmes spécifiques ou « dédiés », non classés (turbine, alternateur,…), F2 (centrales de détection incendie du système JDT), F1B (système DEL assurant la distribution d'eau glacé des divisions électriques et de contrôle-commande des BAS/BL) ou F1A (contrôle-commande dédié des diesels principaux),
- Les systèmes du contrôle-commande chaudière et du contrôle-commande standard classés F2 et NC :
  - PAS : système d'automatisme de tranche et du BTE,
  - RCSL : système de limitation, de surveillance et de contrôle du réacteur,
  - SAS RRC-B : système d'automatisme de sûreté pour les situations d'accident grave,
  - CCAG : Contrôle-Commande Accident Grave,
  - CC-ND : Contrôle-Commande Noyau Dur.
- Les systèmes du contrôle-commande chaudière et du contrôle-commande standard classés F1 :
  - PS : Système de protection du réacteur,
  - SAS de tranche : Système d'automatisme de Sûreté.

Niveau 2 : supervision et conduite de la tranche

Comprenant le traitement des données relatif à l'Interface Homme Machine (IHM) pour la surveillance et la conduite du procédé implémenté dans :

- Le système classé F2 MCP : Moyen de Conduite Principal, assurant la surveillance et la conduite du procédé :

- en salle de commande principale,
- en station de repli.

- Le système classé F1B MCS : Moyen de Conduite de Secours, comprenant une structure d'accueil de quelques commandes F1A ; les commandes de basculement MCP/MCS, nécessaires à l'activation des commandes F1A implantées au MCS, sont également classées F1A.
- Des systèmes de conduite et/ou supervision connexes à ces deux systèmes :
  - un système dédié classé F2 PAG : Pupitre Accident Grave,
  - un système classé F1A PIPO : Pupitre Inter-Postes Opérateurs,
  - un système classé F1B PSIS : Pupitre de Signalisation Inter Synoptiques.

En outre, le contrôle-commande niveau 2 assure l'interface avec les applications hors temps réel, également appelées applications de niveau 3, non classées de sûreté (comme des application d'aide à la conduite ou d'archivage). Cette interface est sécurisée afin d'interdire toute compromission du contrôle commande des niveaux 0, 1 et 2 depuis les systèmes d'information du niveau 3.

2. BASES DE CONCEPTION

2.1. EXIGENCES DE SÛRETÉ

Les principes de classement de contrôle-commande sont indiqués au sous-chapitre 3.2.

L'instrumentation du procédé est classée suivant les fonctions spécifiques à assurer.

Les exigences fonctionnelles de contrôle-commande sont définies au sous-chapitre 7.1.

Les exigences de sûreté relatives aux systèmes de contrôle-commande sont également définies au sous-chapitre 7.1 et abordées dans les sous-chapitres 7.3 et 7.4.

Il est rappelé, qu'afin de réduire le risque de défaillance de mode commun, les dispositions suivantes et structurantes du point de vue de l'architecture générale du contrôle-commande, sont prises en compte :

- Au niveau 2 du contrôle-commande, couverture de la défaillance du système MCP par l'ensemble des moyens de conduite niveau 2 indépendants et diversifiés MCS/PAG/PIPO (voir paragraphe 0.5 du sous-chapitre 7.1),
- Au niveau 1 du contrôle-commande, diversification de certaines fonctions du contrôle-commande, comme évoqué en paragraphe 1 du sous-chapitre 7.1 ; celle-ci est assurée au travers de l'utilisation de deux plates-formes de contrôle-commande technologiquement diversifiées : plate-forme de technologie TELEPERM XS, plate-forme de technologie SPPA T2000.

2.2. EXIGENCES DE DISPONIBILITÉ

Les objectifs de disponibilité pour les fonctions type de contrôle-commande sont définis dans le sous-chapitre sous-chapitre 18.1 (modèle de défaillance de contrôle-commande) afin de constituer une liste communément acceptée de valeurs cibles de disponibilité.

Les exigences de disponibilité concernent les systèmes de contrôle-commande plutôt que l'architecture de contrôle-commande elle-même. Se référer aux sous-chapitre 7.3 et sous-chapitre 7.4 pour les exigences liées à la disponibilité.

2.3. PERFORMANCES REQUISES

Performances des systèmes de contrôle-commande de niveau 1

Les automatismes de contrôle-commande de niveau 1, sont soumis à des exigences de performances en précision et en temps de réponse qui dépendent des fonctions qu'ils réalisent. Les performances requises en termes de temps de réponse et de précision découlent des exigences fonctionnelles.

En ce qui concerne les requis de temps de réponse, conformément au RCC-E C5000 (voir sous-chapitre 1.6) :

- le comportement des logiciels des automatismes de CC qui supportent les fonctions F1A, comme le système de protection PS doit être déterministe. Ce comportement est caractérisé en particulier par un temps de réponse prédéterminé, dans tous les modes de fonctionnement,
- le comportement des logiciels des automatismes de CC qui supportent les fonctions F1B, comme le système de SAS de tranche, doit, par conception, être prédictible. Ce comportement est caractérisé en particulier par un temps de réponse maintenu dans des marges définies d'incertitude, dans tous les modes de fonctionnement.

Performances des systèmes de contrôle-commande de niveau 2

Les délais d'exécution des commandes depuis les moyens de conduite de niveau 2 étant essentiellement déterminés par le délai de réaction de l'opérateur (analyse de la situation et action), les exigences de performance des moyens de conduite sont principalement liées aux exigences d'ergonomie qui visent à réduire les risques d'erreur opérateur :

- Précision et présentation des informations : une information suffisante et appropriée est fournie aux opérateurs pour une compréhension claire de l'état réel de la tranche, et pour une évaluation claire des effets de leurs interventions,
- Temps de réponse : les informations issues du niveau 1 et la prise en compte des actions opérateurs au niveau 1 doivent être affichées au niveau des différentes interfaces homme machine (Postes opérateur du MCP, MCS, PIPO ou PAG en salle de commande principale, postes de repli du MCP en station de repli) dans un délai compatible avec la prévention des erreurs opérateurs.

3. DESCRIPTIF DE L'ARCHITECTURE DE CONTRÔLE-COMMANDE

3.1. NIVEAU 0

Vue d'ensemble

La figure **FIG–7.2.1.2** fournit un schéma simplifié des liaisons et interfaces électriques intervenant entre le niveau 0 et le niveau 1 du contrôle-commande, dans les chaînes fonctionnelles d'élaboration des ordres.

Principes d'interfaçage avec le niveau 0 : instrumentation

Les capteurs (analogiques et logiques), les transducteurs et l'acquisition de données sont des composants de l'instrumentation qui comporte principalement :

- Instrumentation classique de procédé :
  - mesure de pression,
  - mesure de débit,
  - mesure de niveau,
  - mesure de température,
  - mesure de la vitesse de rotation,
  - mesure de tension,
  - mesure de fréquence,

- mesure de position.

- Instrumentation In-Core.
- Instrumentation Ex-Core.
- Mesure de position des barres.
- Mesure de niveau cuve.
- Surveillance des corps migrants et des vibrations.
- Détection de radioactivité.
- Instrumentation accidentelle.
- Instrumentation liée à la surveillance de la concentration en Bore.

L'instrumentation comprend des chaînes de mesure de différentes importances au regard de la sûreté ; le classement d'une chaîne de mesure individuelle dépend du classement le plus élevé des fonctions de Contrôle-commande dans lesquelles cette mesure est utilisée.

Les principes d'interfaçage de l'instrumentation au niveau 0 avec le niveau 1 de contrôle-commande, ainsi que les principes de classement sûreté associés sont exposés ci-après :

- Les capteurs redondés entre divisions sont physiquement indépendants, ou séparés géographiquement (en général implantés dans des divisions différentes), séparés au niveau câblage (cheminement des mesures aux automates).
- Au niveau des capteurs partagés entre fonctions de contrôle-commande gérées par des systèmes de classes de sûreté différentes et/ou pour lesquels portent des requis d'indépendance, un découplage est réalisé via une interface dédiée, appelée PIPS : les signaux sont découplés, isolés galvaniquement et mis en forme, tous ces traitements ayant la classe la plus élevée. Ensuite chaque système utilisateur effectue sa propre acquisition de façon indépendante. En particulier tout capteur F1A se trouve découplé au niveau du PIPS.
- Pour les informations partagées entre fonctions sur lesquelles ne portent pas de requis d'indépendance, l'acquisition est réalisée dans le systèmes de contrôle-commande support de la fonction de Contrôle-commande dans laquelle cette mesure est utilisée et dont le classement est le plus élevé, puis elle est transférée aux autres systèmes via le réseau de tranche dans le cas général, et si nécessaire en fil à fil pour les fonctions de contrôle-commande à fortes exigences de temps de réponse.
- Outre le PIPS, sont présentes dans l'architecture des interfaces de conditionnement dédiées à l'instrumentation de certains systèmes élémentaires : interfaces RPI du RGL (position des grappes), interfaces du RIC (température sortie cœur, flux nucléaire incore), interfaces du RPN (flux nucléaire excore).

Principes d'interfaçage avec le niveau 0 : interface actionneurs

Les cellules électriques constituent l'interface principale du contrôle-commande avec les actionneurs (hormis les cas d'actionneurs à commande directe) et sont regroupées en :

- Classe EE1 (classe sismique 1) : pour les fonctions de contrôle-commande F1,
- Classe EE2 (classe sismique 1) : pour les fonctions de contrôle-commande F2E,
- Classe EE2 (classe sismique 2 ou NC) : pour les fonctions de contrôle-commande F2N,
- Classe NC (classe sismique 2 ou NC) : pour les fonctions de contrôle-commande NC.

Les actionneurs et cellules électriques redondants d'une fonction de contrôle-commande F1 sont séparés physiquement ou géographiquement.

Les fonctions assurant la gestion de priorité et de contrôle de l'actionnement (PACS : Priority and Actuator Control System) sont allouées pour partie dans les systèmes PAS, SAS, SAS RRC-B, pour partie dans la cellule électrique.

Les quatre fonctions du PACS sont les suivantes :

- Gestion de priorité des commandes (automatiques ou manuelles) de l'actionneur, quelle que soit leur origine (PS, PAS, SAS, SAS RRC-B, CCAG, MCP, MCS, IHM locale,…) et leur fonction, et élection (en cas de commandes simultanées) de la commande ayant le niveau de priorité le plus élevé,
- Commande de l'organe conditionnant le fluide de manœuvre de l'actionneur,
- Surveillance de l'actionneur (gestion de la position de l'actionneur et des défauts de mouvement de l'actionneur),
- Protection prioritaire des composants de l'actionneur.

La section 7.3.6 relative au système PACS fournit de plus amples informations concernant l'allocation des fonctions du PACS dans les différentes entités de contrôle-commande.

3.2. NIVEAU 1

Vue d'ensemble

Les fonctions d'automatismes sont implémentées dans les systèmes de niveau 1 suivants :

- Système d'automatisme de contrôle de tranche et du BTE (PAS – Process Automation System),
- Système de limitation, de surveillance et de contrôle du réacteur (RCSL - Reactor Control, Surveillance and Limitation System),
- Système de protection du réacteur (PS – Protection System),
- Système d'automatisme de sûreté de tranche (SAS - Safety Automation System),
- Système d'automatisme de sûreté RRC-B (SAS-RRC-B- Safety Automation System RRC-B),
- Système de contrôle-commande accident grave (CCAG - Contrôle-commande Accident Grave),
- Des systèmes de contrôle-commande dédiés (contrôle-commande dédié des diesels principaux, contrôle-commande dédié du DEL, centrale de détection incendie JDT),
- Le système de contrôle-commande noyau dur (CC-ND – Contrôle Commande Noyau Dur).

Le tableau **TAB–7.2.1.1** donne une vue d'ensemble de la répartition des catégories de fonctions de contrôle-commande dans les systèmes de contrôle-commande classés.

Système d'automatisme de contrôle de tranche (PAS)

Le rôle principal du PAS est la surveillance et les traitements d'automatismes de la tranche et du BTE dans toutes les conditions normales de fonctionnement. Il assure des fonctions automatiques de LCO (conditions limites d'exploitation) et des fonctions de limitation (sauf celles relatives au cœur qui sont implantées au RCSL).

Le PAS assure la gestion des fonctions F2N et NC de la tranche (à l'exception des fonctions chaudière classées F2N allouées au RCSL et des fonctions NC allouées à d'autres systèmes spécifiques dits « dédiés », tels que le contrôle-commande de la turbine ou de l'alternateur par exemple).

Il intègre principalement :

- Les fonctions automatiques et manuelles utilisées en régime normal,
- Les fonctions de régulation du fonctionnement normal,

- Les fonctions d'aide à la conduite opérateur,
- Certaines limitations,
- Les LCO hors LCO cœur,
- Des fonctions de traitement/affichage des informations et alarmes,
- Des fonctions directement liées au contrôle de la radioactivité pendant le fonctionnement normal.

Les fonctions du PAS sont surveillées et commandées par les opérateurs via le MCP. Si le MCP devient indisponible en PCC-1 (fonctionnement normal), certaines fonctions du PAS requises pour maintenir la tranche dans des conditions de fonctionnement stable peuvent être assurées à partir du MCS (cf. **§ 3.3.** et **§ 4.**).

Le PAS est implémenté dans un système numérique classé F2/NC, au sein de la plate-forme de contrôle-commande de technologie SPPA T2000.

Il ne comporte pas de fonctions requises opérables en cas de séisme. Il est classé SC2 pour le classement sismique.

Système de limitation, de surveillance et de contrôle du réacteur (RCSL)

Le RCSL est principalement dédié aux fonctions de contrôle-commande F2 et NC relatives à la conduite et la surveillance du réacteur. Celles-ci incluent notamment :

- Fonctions de contrôle du Cœur,
- Fonctions automatiques de LCO (conditions limites d'exploitation) et fonctions de limitation pour les paramètres du cœur et du circuit primaire nécessitant une action sur les grappes.

De plus, le RCSL réalise certaines fonctions assurant la gestion des situations de fonctionnement RRC-A.

Les fonctions de commande des actionneurs pour les commandes de grappes sont mises en oeuvre dans le RCSL ; les fonctions de commande des autres actionneurs contrôlés par le RCSL sont implémentées dans d'autres systèmes de niveau 1 et le RCSL communique avec ceux-ci par le réseau de tranche ou en fil à fil.

Le RCSL est implémenté dans un système numérique classé F2 de technologie TELEPERM XS.

Il ne comporte pas de fonctions requises opérables en cas de séisme. Il est classé SC2 pour le classement sismique.

Système de protection du réacteur (PS)

Le PS assure la surveillance dans toutes les conditions de fonctionnement de la tranche (PCC) des paramètres de sûreté, permettant en cas d'apparition d'événement initiateur de rejoindre l'état contrôlé. Plus précisément, il assure :

- Les fonctions automatiques F1A de protection et de sauvegarde,
- Les fonctions automatiques F1A de contrôle des systèmes support de sauvegarde,
- Les fonctions manuelles de contrôle-commande F1A.

Le PS assure aussi des fonctions manuelles de RAZ classées F1B liées aux automatismes F1A et transmet également des informations sur les paramètres de sûreté au MCS (F1B) et au MCP (F2).

De plus, le PS réalise certaines fonctions nécessaires à la gestion des situations de fonctionnement RRC-A ainsi que les fonctions automatiques associées au CC-ND (cf. **§ 4.7.**).

Les paramètres, les signaux initiateurs et les ordres du PS sont présentés à l'opérateur au MCP et au MCS. Des verrouillages sont prévus dans le PS pour interdire les actions manuelles et le réarmement de fonctions automatiques depuis le MCP ou le MCS si les conditions du procédé ne l'autorisent pas.

Le PS est implémenté dans un système numérique classé de sûreté F1A de technologie TELEPERM XS.

Il comporte des fonctions requises opérables en cas de séisme. Il est classé SC1 pour le classement sismique.

Système d'automatisme de sûreté de tranche (SAS)

Les fonctions principales assurées par le SAS de tranche sont :

- Les fonctions de gestion post-accidentelle (manuelles et automatiques) nécessaires pour amener la tranche lors d'un événement initiateur de l'état contrôlé à l'état d'arrêt sûr (F1B),
- Les fonctions relatives aux systèmes supports F1 qui ne changent pas d'état lors d'un évènement (systèmes de sûreté autonomes, par exemple la ventilation),
- Certaines fonctions de commande pouvant provoquer un événement de type PCC-3 ou PCC-4, classées F1B,
- Des fonctions directement liées au contrôle de la radioactivité pendant le fonctionnement normal,
- Les fonctions F2 classées séisme (F2E), spécifiquement conçues pour contrôler les agressions internes et externes,
- Certaines fonctions F2 de gestion des situations RRC-A.

Les paramètres, les signaux initiateurs, les ordres et les comptes-rendus du SAS sont présentés à l'opérateur au travers du MCP et du MCS. Des verrouillages (E1B) sont prévus dans le SAS pour interdire le déclenchement d'actions manuelles et le réarmement de fonctions dans le SAS depuis le MCP si les conditions procédé ne l'autorisent pas.

Le SAS est implémenté dans un système numérique classé F1B de technologie SPPA T2000.

Il comporte des fonctions requises opérables en cas de séisme. Il est classé SC1 pour le classement sismique.

Système d'automatisme de sûreté de gestion des situations AG (SAS-RRC-B)

Le système SAS-RRC-B est un système dédié à la gestion des situations accidents graves à l'exception du scénario Accident grave de perte des alimentations électriques internes et externes (PTAE), dont la gestion est assurée par le système CCAG.

Le SAS-RRC-B contribue aux fonctions de sûreté suivantes :

- la dépressurisation du circuit primaire,
- la mitigation du risque hydrogène,
- la dépressurisation de l'enceinte et l'évacuation de la puissance résiduelle,
- la limitation des rejets dans l'environnement.

Le SAS-RRC-B est implémenté dans un système numérique classé F2E de technologie SPPA T2000.

Il comporte des fonctions requises opérables en cas de séisme. Il est classé SC1 pour le classement sismique.

Le système de contrôle-commande accident grave (CCAG)

Le système CCAG fournit les commandes et informations nécessaires à la gestion d'un scénario couplé ou dû à une perte totale des alimentations électriques internes et externes (PTAE). Le CCAG est destiné à couvrir le scénario PTAE [] après basculement au pupitre AG.

Le système CCAG est implémenté dans un système numérique classé F2E de technologie TELEPERM XS.

Il comporte des fonctions requises opérables en cas de séisme. Il est classé SC1 pour le classement sismique.

Systèmes de contrôle-commande dédiés classés de sûreté

Les systèmes de contrôle-commande dédiés assurent des fonctions particulières non prises en charge par le contrôle-commande chaudière (basé sur la plate-forme TELEPERM XS) ni par le contrôle-commande standard (basé sur la plate-forme SPPA T2000) car spécifiques et réalisées en standard dans un lot de fourniture matérielle.

Dans le cas général les contrôle-commande dédiés sont autonomes (leurs fonctions sont indépendantes des autres systèmes de contrôle-commande), liées aux matériels dont ils assurent le contrôle-commande, et majoritairement reliés en fil à fil avec le reste du contrôle-commande.

Des contrôle-commande dédiés classés de sûreté, sont réalisés en technologie conventionnelle. Ils sont assimilés au matériel dont ils assurent le contrôle ou la surveillance. Par exemple, les contrôle-commandes dédiés classés de sûreté F1A des diesels sont constitués de relayage conventionnel pour assurer le pilotage des actionneurs F1A des diesels principaux.

Les seuls contrôle-commandes dédiés de technologie numérique et classés de sûreté sont :

- Le système de contrôle-commande dédié des groupes froids DEL F1B, de technologie FRAMATOME Teleperm XS. Il assure la distribution d'eau glacée des divisions électriques et de contrôle-commande des BAS/BL. Il comporte des fonctions requises opérables en cas de séisme. Il est classé SC1 pour le classement sismique.
- Les centrales de détection incendie du système JDT F2, de technologie []. Il comporte des fonctions requises opérables en cas de séisme. Il est classé SC1 pour le classement sismique.

Le système de contrôle-commande Noyau dur CC-ND

Le système CC-ND fournit au titre de la robustesse du contrôle-commande (voir paragraphe 2 du sous-chapitre 7.1), des moyens nécessaires à la gestion des situations de cumuls :

- de l'occurrence hautement hypothétique, de perte totale du contrôle-commande standard (de technologie SPPA T2000),
- avec des transitoires de catégories de fonctionnement PCC-2 à PCC-4, ou des situations RRC-A n'impliquant pas la défaillance d'une fonction F1 allouée au système de protection PS (de technologie TELEPERM XS).

Le système CC-ND est implémenté dans un système numérique dédié non classé (NC), de technologie TELEPERM XS.

Il comporte, en complément des fonctions déjà prévues dans le système de protection PS (de technologie TELEPERM XS), les fonctions manuelles et les signalisations nécessaires pour l'atteinte de l'état stable visé, caractérisé au sous-chapitre 7.1. Ces fonctions et ces signalisations sont des fonctions équivalentes à celles disponibles au SPPA-T2000 et sont opérationnelles après activation manuelle préalable du système CC-ND au MCS.

Le système CC-ND est classé SC2 pour le classement sismique.

Le document de spécification détaillée en **Réf [2]** fournit de plus amples informations sur le système CC-ND.

3.3. NIVEAU 2

Vue d'ensemble

Le traitement des données au niveau 2 sert principalement à l'Interface Homme-Machine (IHM) pour la surveillance et la conduite de la tranche.

Les fonctions sont implémentées dans les systèmes de contrôle-commande suivants :

- Le Moyen de Conduite Principale (MCP), en salle de commande, en station de repli et au BTE,
- Le Moyen de Conduite de Secours (MCS),
- Le Pupitre Inter Postes Opérateurs (PIPO),
- Le Pupitre de Signalisation Inter-Synoptiques (PSIS),
- Le Pupitre Accident Grave (PAG).

Le tableau **TAB–7.2.1.1** donne une vue d'ensemble de l'allocation des catégories de fonctions de contrôle-commande dans les systèmes de contrôle-commande.

Moyen de conduite principal (MCP)

Le rôle principal du MCP est de permettre aux opérateurs de surveiller et de conduire la tranche dans toutes les conditions de fonctionnement : régime normal, PCC et RRC-A et accident grave.

Le MCP a accès aux informations de l'ensemble des systèmes de niveau 1 et les présente aux équipes de conduite sur les équipements d'IHM suivants :

- Postes opérateur informatisés en mode conduite permettant la conduite et la supervision de la tranche en Salle de Commande principale,
- Postes de supervision informatisés (visualisation uniquement) en Salle de Commande principale,
- Écrans grands formats (visualisation uniquement) permettant une vision commune de l'état et des paramètres de la tranche en Salle de Commande principale,
- Postes opérateurs informatisés permettant la supervision et la conduite de la tranche dans la Station de Repli,
- Poste de supervision informatisé (visualisation uniquement) dans le local technique de crise (LTC),
- Postes opérateurs minimaux (POM) disposant de connexions mobiles dans certains locaux comme le local maintenance (visualisation uniquement),
- Poste opérateur minimal fixe en Salle de Commande (visualisation uniquement),
- Poste de conduite informatisé déporté dans les locaux de contrôle-commande du BAN, configuré sur un jeu d'actionneurs limité,
- Postes de conduite informatisés déportés dans les locaux de contrôle-commande du BTE permettant la conduite de la partie BTE,
- Imprimantes, archivage,
- Equipements d'interface avec le niveau 3 (serveur XU).

Le MCP avertit les opérateurs en cas d'anomalies sur le procédé et les systèmes, et les guide dans la conduite à tenir.

La plupart des actionneurs de la tranche peuvent être commandés par le MCP via les systèmes de niveau 1.

Les commandes sont exécutées par les opérateurs à partir des écrans et sont envoyées aux systèmes de niveau 1 qui agissent à la fois sur les actionneurs E2/NC et de sûreté E1.

En cas d'événement initiateur, PCC-2 à 4 ou RRC-A ou accident grave, les opérateurs surveillent sur les écrans du MCP le déclenchement automatique des fonctions de protection ou de réduction de risque et au besoin réalisent à partir des écrans du MCP :

- Le réarmement des fonctions F1 exécutées automatiquement dans le PS et le SAS,
- Les fonctions manuelles de gestion post-accidentelle dans les systèmes de niveau 1 du contrôle-commande,
- Les fonctions manuelles de réduction du risque RRC-A dans les systèmes de niveau 1,
- Les fonctions manuelles RRC-B par le SAS RRC-B.
- Les fonctions de conduite nécessaires en cas d'événement initiateur PCC-2 à PCC-4, ainsi que certaines situations RRC-A et accident grave, sont secourues, en cas de perte du MCP, par les fonctions implantées au MCS qui constitue le moyen de conduite F1B de la démonstration de sûreté, complété par les moyens de conduite PIPO/PAG en ce qui concerne la gestion des situations RRC-A et accident grave.

Des mesures sont prévues au MCP et dans les systèmes de niveau 1 pour éviter tout ordre intempestif dû aux défaillances internes du MCP ou dû à une agression interne. Ainsi des boutons de validation sont implantés en Salle de commande et en station de repli afin de valider les ordres venant du MCP destinés au PS.

Le MCP est classé F2 et implémenté dans un système numérique avec une interface Homme-Machine informatisée de technologie SPPA T2000.

Les matériels et l'architecture de l'interface homme-machine informatisée des postes opérateurs en Salle de Commande principale respectent les exigences applicables aux systèmes F1B ; les fonctions de commandes et de surveillance des postes opérateurs en Salle de Commande principale et en Station de Repli sont requises opérables en cas de séisme (classe sismique 1 SC1), les autres fonctions telles que l'impression, l'archivage,… ne sont pas soumises à des exigences d'opérabilité en cas de séisme.

Le MCP est indépendant du MCS.

Moyen de Conduite de Secours (MCS)

Le MCS est l'interface homme-machine classée de sûreté permettant l'exécution des fonctions F1 et F2E de conduite et de supervision nécessaires pour amener et maintenir la tranche dans un état d'arrêt sûr en cas d'indisponibilité du MCP.

Le MCS permet :

- En cas d'indisponibilité du MCP en PCC-1 (en raison de défaillances internes au MCP) de contrôler et surveiller la tranche pour un temps limité en fonctionnement en puissance en régime permanent et, si le retour à la normale du MCP n'est pas atteint, d'amener et de maintenir la tranche dans un état d'arrêt sûr (classe F2 / NC),
- En cas d'évènements de PCC-2 à PCC-4 et d'indisponibilité du MCP :
    - De surveiller les fonctions de sûreté de la tranche, notamment les fonctions automatiques F1 de protection et les fonctions post-accidentelles,
    - D'engager les fonctions manuelles nécessaires pour amener la tranche de l'état contrôlé à l'état d'arrêt sûr (classe F1B),
    - D'engager quelques fonctions manuelles classées F1A car nécessaires pour amener la tranche à l'état contrôlé dans certaines situations,

- De surveiller et commander les systèmes supports des systèmes de sûreté nécessaires à la conduite post-accidentelle,
- D'engager les fonctions de protection contre l'incendie dans l'îlot nucléaire (classement F2E).

- En cas de certaines séquences RRC-A ou accident grave et d'indisponibilité du MCP, de participer à la conduite de ces situations, en valorisant également les autres moyens de conduite diversifiés du MCP (PIPO/PAG).

Au titre de la robustesse, en cas de situations PCC-2 à PCC-4 ou de séquence RRC-A sans perte du système PS, avec en cumul la perte, hautement improbable, du contrôle-commande standard, la conduite vers un état stable de la chaudière est également assurée au MCS via le CC-ND et complétée par la réalisation de certaines actions en local.

Normalement, le MCS n'est pas utilisé lorsque le MCP est disponible sauf exceptions :

- lors d'essais périodiques (F2),
- en conditions accidentelles pour la surveillance des principaux paramètres de sûreté et l'état des systèmes de sûreté.

Tant que le MCP est disponible, les alarmes présentes sont visualisées sur le MCP et le MCS, mais les alarmes du MCS sont acquittées automatiquement.

Tant que les commandes du MCS ne sont pas nécessaires, elles sont désactivées afin de réduire le risque d'ordre intempestif dû à une agression interne ou en raison de défaillances internes au MCS.

Les commandes du MCS sont activées par les commandes de transfert situées dans la zone de Conduite de Secours et qui sont indépendantes et séparées des moyens de commandes sur le procédé. Une défaillance unique ou une agression interne du mécanisme de transfert ne génère pas de signaux et d'ordres intempestifs.

En cas d'indisponibilité du MCP :

- Les commandes manuelles sont transmises via le MCS aux systèmes de niveau 1 ; tous les ordres en provenance du MCP sont inhibés afin d'éviter des ordres intempestifs en raison d'une défaillance du MCP ou lors d'une intervention de maintenance sur le MCP,
- Les fonctions liées aux alarmes désactivées sur le MCS (signal sonore, acquittement à l'apparition et à la disparition) sont activées.

En cas de perte totale du contrôle-commande standard, un mécanisme de basculement spécifique active les commandes et signalisations nécessaires à la conduite spécifique de cette situation hautement hypothétique.

Le MCS est classé F1B. Sa technologie est majoritairement conventionnelle et sa gestion est assurée par le système KSC. Il comprend une structure d'accueil de quelques commandes F1A. Ses matériels sont classés séisme SC1.

Il est fonctionnellement indépendant du MCP et implanté en Salle de Commande.

Autres moyens de conduite et de surveillance

- **Pupitre Accident Grave PAG**
  Le PAG est l'interface homme-machine classée de sûreté permettant d'exécuter les fonctions F2E de conduite et de supervision assurant la gestion des accidents graves avec perte totale des alimentations électriques internes et externes (PTAE).
  Le moyen de conduite PAG est classé de sûreté F2E. Sa technologie est conventionnelle et sa gestion est assurée par le système KSC. Ses matériels sont classés Séisme 1.
  Il est fonctionnellement indépendant du MCP ainsi que du MCS et implanté en Salle de Commande.

- **Pupitre de Signalisation Inter-Synoptiques PSIS**
  Le PSIS est l'interface homme-machine classée de sûreté assurant les missions de sûreté suivantes :

  - Signaler les éventuels dysfonctionnements du Moyen de conduite principal MCP détectés via le « signe de vie » F1B.
  - Fournir les signalisations nécessaires à la défaillance des fonctions de sûreté du PS, permettant d'orienter la conduite depuis le MCP des situations RRC-A d'ATWS avec perte PS.

  Au titre de la robustesse du contrôle-commande à la perte totale du contrôle-commande standard, le PSIS gère par ailleurs les signalisations nécessaires à la détection de cette situation, nécessaires à l'orientation des opérateurs dans une stratégie de conduite spécifique.
  Le PSIS est classé de sûreté F1B. Sa technologie est conventionnelle. Ses matériels sont classés Séisme 1.
  Il est fonctionnellement indépendant du MCP et implanté en Salle de Commande.

- **Pupitre Inter-Postes Opérateurs PIPO**
  Le PIPO est l'interface homme-machine classée de sûreté permettant de lancer manuellement les commandes d'AAR, par câblage direct sur les disjoncteurs d'AAR, et le déclenchement secondaire général. Ces commandes manuelles sont valorisées dans les scénarios d'indisponibilité de la salle de commande nécessitant de basculer la conduite sur les postes de Repli en Station de Repli.
  Le PIPO assure par ailleurs, au titre de la conduite des situations d'accident grave les commandes manuelles d'isolement enceinte phase 2 (IE2). Ces commandes sont de la même façon câblées en fil à fil en aval du système de protection.
  Le PIPO permet également l'autorisation des ordres d'ouverture des vannes de décharge 900t/h.
  Le PIPO est classé de sûreté F1A. Il héberge des commandes classées fonctionnellement de F1A (il s'agit des commandes câblées d'AAR) à NC. Sa technologie est conventionnelle. Ses matériels sont classés séisme SC1.
  Il est fonctionnellement indépendant du MCP et du MCS et PAG et implanté en Salle de Commande.

Récapitulatif des moyens de conduite selon leurs différentes implantations

La figure **FIG–7.2.1.5** fournit la répartition géographique des différents moyens de conduite de niveau 2.

- **Moyens de conduite depuis la Salle de Commande principale (SdC)**
  Les fonctions de conduite et de supervision de la tranche sont assurées dans la Salle de Commande (SdC) dans toutes les situations de fonctionnement (sauf indisponibilité de la SdC).
  Pour ces tâches, la SdC est équipée :

  - De postes de travail informatisés pour la conduite et la surveillance de la tranche,
  - Du synoptique comprenant des écrans MCP grand format permettant une vue d'ensemble de l'état et des principaux paramètres de la tranche,
  - D'une zone de conduite de secours comportant les équipements d'IHM conventionnels du MCS,
  - D'une zone de conduite dédiée accident grave (scénario de perte totale des alimentations électriques internes et externes - PTAE) comportant les équipements d'IHM conventionnels du PAG,
  - Du Pupitre Inter Poste Opérateur permettant l'envoi des ordres F1A d'Arrêt Automatique Réacteur et de Déclenchement Secondaire, en cas d'évacuation de la SdC vers la SdR,
  - Du Pupitre de Surveillance interSynoptique de technologie conventionnelle, signalant, en particulier, les dysfonctionnements du MCP (signe de vie),
  - D'une structure d'accueil au MCS, de commandes manuelles F1A permettant d'atteindre l'état contrôlé.

Le schéma permettant de visualiser l'installation des différents équipements de contrôle-commande en salle de commande fait l'objet de la figure **FIG–7.2.1.4**.

- **Moyens de Conduite depuis la Station de repli (SdR)**
  En cas d'indisponibilité de la SdC en raison d'une agression interne, les opérateurs assurent la surveillance et la conduite de la tranche à partir de la Station de Repli.
  Pour la surveillance et la conduite de la tranche, la Station de Repli est équipée :
  - De moyens permettant de désactiver les équipements de conduite en SdC (MCS et PAG) ; des dispositifs techniques et administratifs empêchent l'activation intempestive ou non autorisée de cette fonction,
  - De postes de repli (PdR) informatisés (de même conception que ceux installés en SdC, configurés en mode conduite en cas d'indisponibilité de la SdC) à partir desquels les opérateurs peuvent amener la tranche dans un état d'arrêt sûr et la surveiller,
  - D'un poste de conduite informatisé en mode supervision (visualisation uniquement),
  - Des boutons de validation des ordres du MCP à destination du PS.

  L'ensemble des équipements et systèmes supports de contrôle-commande nécessaires pour la conduite depuis la Station de Repli sont séparés de la zone de la Salle de commande et sont en particulier dans des secteurs d'incendie différents.
- **Moyens de supervision depuis le Local Technique de Crise (LTC)**
  Le LTC est un local utilisé par l'équipe de crise en cas d'accident afin d'accueillir un effectif supplémentaire pour l'analyse des conditions de la tranche et le soutien à la gestion post-accidentelle.
  Le LTC est équipé d'un poste opérateur informatisé du MCP ayant accès à toutes les informations mais sur lequel les fonctions de commandes sont bloquées.
- **Moyens de conduite décentralisés dans d'autres locaux**
  Certains moyens de conduite et de supervision peuvent être installés localement, proches des équipements à commander et/ou à surveiller (Salle de Commande BTE et BAN par exemple).
  Des postes opérateurs minimaux (POM) informatisés disposent par ailleurs de points de connexion mobiles dans les locaux suivants : local maintenance, local consignation (Voir figure **FIG–7.2.1.3** précisant l'Implantation géographique des systèmes de contrôle-commande dans les locaux).

3.4. COMMUNICATION ENTRE SYSTÈMES DE CONTRÔLE-COMMANDE

Vue d'ensemble des communications au sein du contrôle-commande

Les échanges de données entre les systèmes de Contrôle-commande de niveau 1 d'une part, et entre ces derniers et le MCP d'autre part, s'effectuent dans le cas général par les différents réseaux de communications numériques de l'architecture. Selon le classement de sûreté des informations échangées, et le rattachement des systèmes émetteurs ou récepteurs de ces informations à l'une ou l'autre des plates-formes de contrôle-commande, ces réseaux peuvent être :

- les réseaux des plates-formes de contrôle-commande de technologie TELEPERM XS (F1A, F1B, F2),
- les réseaux de technologie SPPA T2000, comprenant pour les communications au sein du niveau 1 le réseau Plant-Bus (F2), et SAS-Bus (F1B), pour les communications au sein du niveau 2, le réseau Terminal-Bus (F2).

Les échanges entre systèmes de contrôle-commande de niveau 1 s'effectuent pour des besoins particuliers en fil à fil (par exemple pour des contraintes de temps de réponse).

Les échanges de données entre le MCS et les systèmes d'automatismes de niveau 1 (PS, SAS, CC-ND) sont assurés par des liaisons fil à fil. Il en est de même pour les autres interface de conduite ou de signalisation PAG, PSIS, PIPO.

Des passerelles de communication assurent l'interface entre les réseaux des deux plates-formes de technologie TELEPERM XS et SPPA T2000.

Dans la mesure du possible, les échanges internes à un système de contrôle-commande (y compris l'échange de données entre divisions) sont gérés par le système lui-même sans faire appel aux ressources externes.

La figure **FIG–7.2.1.1** fournit l'architecture de principe des communications sus-décrites.

La figure **FIG–7.2.1.3** précise la topologie des différents réseaux assurant l'acheminement des informations au sein de l'architecture.

Réseaux de communications du contrôle-commande au niveau 1

Les réseaux du système de protection, classés E1A, E1B, E2, sont dédiés aux échanges internes au système PS. Il en est de même pour le système RCSL. Ces communications sont décrites dans les sections des sous-chapitre 7.3 et sous-chapitre 7.4 concernant ces systèmes.

Le réseau de tranche Plant-Bus est classé E2. Le réseau de tranche est conçu pour résister à une défaillance unique ainsi qu'aux agressions internes dans une division au titre de la disponibilité.

Le réseau de tranche de sûreté SAS bus du contrôle-commande standard est classé E1B. Il est dédié aux échanges interne au système SAS de tranche classé E1B, et est conçu pour résister à une défaillance unique ainsi qu'aux agressions internes dans une division.

Réseaux de communication du contrôle-commande au niveau 2

Le seul réseau de communication au niveau 2 est le Terminal-Bus classé E2. Ce réseau est conçu pour résister à une défaillance unique ainsi qu'aux agressions internes dans une division au titre de la disponibilité.

Communications avec le niveau 0

Les interfaces avec le niveau 0 sont réalisées en fil à fil.

3.5. TECHNOLOGIE DES SYSTÈMES

Deux plates-formes de contrôle-commande numériques intégrées, diversifiées sont utilisées pour assurer l'essentiel des fonctions de contrôle-commande classées de sûreté :

- La plate-forme des systèmes du contrôle-commande chaudière : Cette plate-forme est utilisée pour les systèmes PS, CCAG, RCSL, CC-ND. La technologie de cette plate-forme numérique de contrôle-commande est TELEPERM XS de FRAMATOME.
- La plate forme des systèmes du contrôle-commande standard : Cette plate-forme est utilisée pour les systèmes de niveau 1 PAS, SAS et SAS RRC-B ainsi que pour les systèmes informatisés de conduite de niveau 2 MCP recouvrant les postes opérateur informatisés de la Salle de Commande, de la Station de Repli et du Local technique de crise, de technologie SPPA T2000.

Ces deux plate-forme sont diversifiées sur le plan matériel et logiciel. Elles permettent d'écarter le risque d'une Défaillance de Cause Commune entre les deux plates-formes et par conséquent de répondre aux besoins de diversification des fonctions de contrôle-commande au sein de l'architecture.

A chacune de ces plates-formes est rattaché un ensemble d'outils d'ingénierie, configuration et supervision plus amplement décrits au sous-chapitre 7.6. Ces ensembles d'outils, non classés, sont conçus pour ne pas introduire de perturbation sur les fonctions classées du contrôle-commande.

Une partie des fonctions de contrôle-commande classées sont assurées par des contrôle-commande dédiés (systèmes de contrôle-commande des diesels principaux F1A, système de contrôle-commande dédié F1B du DEL, centrale de détection incendie JDT F2). Ces contrôle-commande dédiés sont de

technologie automate différente ou bien de technologie conventionnelle (ie. non programmée), sans requis associés de diversification vis-à-vis des systèmes rattachés aux plates-formes principales de contrôle-commande.

Certaines fonctions de contrôle-commande classées sont assurées par des composants électriques programmés (CEP), définis comme étant conformément au RCC-E (Chapitre C5333), des éléments de contrôle-commande à base de logique programmée, assurant une fonction principale dédiée et définie à la conception, fonctionnellement autonome, paramétrable mais non programmable par l'utilisateur. Il est recommandé d'éviter d'utiliser, pour un initiateur donné, un même modèle de CEP dans plusieurs lignes de défense.

Le MCS ainsi que les moyens de conduite attenants PAG, PIPO et de signalisation PSIS sont en technologie conventionnelle. Toutefois, l'utilisation d'équipements en technologie numérique au MCS et au PAG n'est pas exclue (enregistreurs par exemple).

Le système de contrôle-commande CC-ND est réalisé dans la technologie TELEPERM XS. Bien que non classé, il hérite par conséquent des caractéristiques techniques et de fiabilité de cette plate-forme.

4. MODES D'EXPLOITATION

4.1. EXPLOITATION NORMALE

La figure **FIG–7.2.1.5** donne une vue d'ensemble des systèmes de contrôle-commande utilisés en exploitation normale.

Ceux participant à la surveillance et au contrôle de la tranche en exploitation normale sont recensés ci-après :

- Le PAS, le SAS et le RCSL exécutent l'ensemble des fonctions d'automatisme en exploitation normale. Les commandes actionneurs vont directement du PAS et du SAS aux cellules et du RCSL aux mécanismes de contrôle des grappes.
- Le MCP avec ses équipements d'IHM en SdC et en locaux déportés permet aux opérateurs de surveiller et de contrôler l'état de la tranche et les fonctions de contrôle-commande nécessaires à l'exploitation normale de celle-ci.

Pour la surveillance de l'état du PS et du SAS en exploitation normale, le MCP reçoit des informations de ces systèmes à travers les réseaux.

Indisponibilité du MCP

En cas d'indisponibilité du MCP en raison de défaillances internes à celui-ci, l'équipe de conduite décide, notamment sur la base des messages et alarmes générées par les fonctions d'auto-surveillance du MCP et la fonction « signe de vie » du MCP (fonction de surveillance classée F1B, dont la signalisation est localisée au PSIS), de transférer la conduite de la tranche du MCP (zone de conduite principale) au MCS (zone de conduite de Secours). Le MCS est mis en service en mettant en oeuvre les fonctions décrites au paragraphe **§ 3.3.**.

La conduite et la surveillance de la tranche en fonctionnement en puissance en régime permanent sont assurées pour un temps limité sur le MCS. Si un retour à la normale du MCP ne peut pas être atteint, les opérateurs amènent et maintiennent la tranche dans un état d'arrêt sûr grâce aux systèmes MCS, SAS, PS et PAS (ce dernier pour certaines fonctions requises pour maintenir la tranche dans des conditions de fonctionnement stable).

4.2. CONDITIONS DE FONCTIONNEMENT DE RÉFÉRENCE

En conditions de fonctionnement de référence (PCC-2 à PCC-4), il faut distinguer deux modes de conduite :

- Conduite avec l'ensemble des systèmes de contrôle-commande disponibles,
- Conduite uniquement avec les systèmes de contrôle-commande de sûreté F1.

Conduite d'accident avec l'ensemble des systèmes de contrôle-commande disponible.

La figure **FIG–7.2.1.6** donne une vue d'ensemble des systèmes de contrôle-commande participant à la surveillance et au contrôle de la tranche lorsque l'ensemble des systèmes de contrôle-commande est disponible.

Les évènements internes PCC-2 à PCC-4 sont détectés par le PS. Les fonctions de contrôle-commande de protection nécessaires avant toute action manuelle sont initiées automatiquement et mises en œuvre par le PS.

Si des actions manuelles sont nécessaires pour atteindre l'état contrôlé ou l'état d'arrêt sûr, les opérateurs sont alertés par les alarmes générées par le PS ou le SAS et affichées au MCP.

Les fonctions de contrôle-commande dans le PAS, le SAS et le PS sont surveillées et contrôlées sur les écrans du MCP pour la gestion de la situation post-accidentelle avec l'aide des images et des procédures de conduite et sur la base des informations fournies par tous les systèmes de niveau 1.

Conduite uniquement avec les systèmes de contrôle-commande F1.

Les évènements internes PCC-2 à PCC-4 sont détectés par le PS. Les fonctions de contrôle-commande de protection nécessaires avant toute action manuelle sont initiées automatiquement et mises en œuvre par le PS (cf. figure **FIG–7.2.1.7**).

Si des actions manuelles sont nécessaires pour atteindre l'état contrôlé ou l'état d'arrêt sûr, les opérateurs en sont informés par les alarmes générées par le PS ou le SAS et présentées au MCS.

Les fonctions post-accidentelles manuelles sont initiées au MCS, les actions correspondantes sont réalisées dans le PS ou le système SAS. Les échanges classés de sûreté F1B entre équipements SAS, nécessaires à l'accomplissement des fonctions de sûreté au sein du contrôle-commande standard, transitent par le réseau interne au système SAS (SAS-Bus), classé de sûreté E1B.

4.3. AGRESSIONS INTERNES ET EXTERNES

Les systèmes de contrôle-commande doivent être protégés contre les agressions internes ou externes en suivant les exigences définies aux sous-chapitres 3.3 et 3.4 du RDS.

Indisponibilité de la Salle de Commande.

En cas de dégradation des conditions d'ambiance suite à une agression, rendant la présence de l'opérateur impossible la décision d'évacuer la SdC est prise par l'équipe de conduite. Un basculement de la conduite vers la station de repli est alors nécessaire afin d'amener la tranche à l'état de repli. Les actions effectuées du point de vue contrôle-commande sont les suivantes (cf. figure **FIG–7.2.1.8**) :

- préalablement à l'évacuation de la SdC, lancement de l'AAR (Arrêt automatique réacteur) depuis le PIPO,
- passage en station de repli :
  - basculement de commutateurs localisés en SdR ayant pour effet de désactiver le MCS et le PAG afin d'éviter des actions aberrantes qui pourraient émaner de ces derniers,
  - actions appropriées permettant d'isoler les postes opérateur du MCP de la salle de commande principale, du reste du MCP, afin d'éviter des actions aberrantes qui pourraient émaner de ces postes,
  - en exploitation normale, les écrans des postes de repli sont en veille afin de pouvoir être opérationnels rapidement. Les opérateurs surveillent et contrôlent le passage de la tranche à

l'état d'arrêt sûr sur les écrans des postes de repli. Le mode d'exploitation des systèmes de niveau 1 est similaire au fonctionnement normal (cf. § 4.1.) à l'exception du système RCSL.

La station de repli assure les moyens de conduite en tout état de tranche et pour les situations jusqu'à PCC-1. Parmi les situations supérieures ou égales à PCC-2, seul l'incident PCC-2 par manque de tension externe (situation MDTE) est à prendre en compte en cumul de la conduite depuis la station de repli.

Agressions internes dans les systèmes de niveau 2.

La démonstration de robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

Agression interne dans les systèmes de niveau 1.

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

Agressions externes.

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.3.

4.4. CONDITIONS DE RÉDUCTION DES RISQUES RRC-A

Le besoin de mesures de réduction des risques ou d'enclenchement de fonctions automatiques RRC-A est signalé aux opérateurs par le MCP.

Dans le cas général, les fonctions de contrôle-commande RRC-A manuelles sont engagées au MCP et exécutées par les systèmes de contrôle-commande de niveau 1.

De façon générale, l'allocation des fonctions de contrôle-commande associées aux dispositions RRC-A au niveau 1 est réalisée au cas par cas, sur la base d'une analyse d'exigences fonctionnelles qui précise les requis d'indépendance ou de diversification éventuels par rapport au système de contrôle-commande dont la défaillance intervient dans la séquence RRC-A étudiée. Par défaut, le système SAS de tranche est l'allocation préférentielle des fonctions mitigant les situations RRC-A. Quelques fonctions de contrôle-commande permettant la gestion des situations RRC-A se trouvent assurées par d'autres systèmes de niveau 1 comme par exemple les fonctions F2 RRC-A d'ATWS par blocage mécanique des grappes d'arrêt, allouées au PS.

Certaines situations RRC-A peuvent également être conduites au MCS.

4.5. MANQUE DE TENSION GÉNÉRALISÉ (SITUATION RRC-A DE MDTG)

Le mode d'exploitation de contrôle-commande décrit ci-dessous concerne le scénario RRC-A de Manque De Tension Généralisé (MDTG).

Le Manque De Tension Externe (MDTE) est détecté par le PS qui déclenche l'arrêt automatique du réacteur (par la chute des grappes) et le démarrage des diesels principaux.

Si suite à des défaillances, aucun diesel ne démarre, tous les systèmes et équipements de contrôle-commande dans toutes les divisions sont alimentés par les batteries []. Dans cette phase, il n'y a pas de ventilation dans les divisions et dans la SdC et seuls quelques actionneurs, dont l'alimentation est secourue par les batteries, sont alimentés.

Les 2 diesels d'ultime secours SBO (dans la division 1 ou 4) sont démarrés automatiquement par le SPPA-T2000 ou manuellement au MCP et les fonctions de contrôle-commande RRC-A niveau 1 sont exécutées par le SAS de tranche. Des dispositions sont prévues afin d'empêcher que des ordres de

priorité plus élevés (par exemple signal de délestage du diesel principal) ne verrouillent les actionneurs nécessaires dans cette situation, ou ne compromettent le démarrage des diesels SBO.

Lorsque le courant pour la batterie, l'éclairage et la ventilation de la SdC et des locaux d'automatisme dans une division (1 ou 4) sont fournis par le diesel d'ultime secours, l'alimentation de tous les équipements de contrôle-commande dans les autres divisions non ventilées est coupée par intervention locale au niveau des tableaux électriques afin d'éviter tout comportement aberrant qui pourrait compromettre les fonctions de contrôle-commande de RRC-A nécessaires.

Les opérateurs surveillent et contrôlent la tranche depuis la SdC via les divisions du MCP ou du MCS alimentées grâce aux informations en provenance de l'instrumentation allouée à ces divisions et traitées dans les parties restant opérationnelles du PS, SAS ou du PAS. Ils peuvent commander les actionneurs via les automatismes niveau 1 dans la mesure où ceux-ci sont alimentés.

4.6. CONDITIONS DE GESTION DES ACCIDENTS GRAVES

La gestion des accidents graves est assurée par les moyens de contrôle-commande suivants (voir figure **FIG–7.2.1.9**) :

Pour le scénario d'accident grave lié à la perte totale des alimentations électriques internes et externes (PTAE) ces moyens comprennent (au-delà des deux heures d'autonomie sur batteries dont dispose le contrôle-commande) :

- les armoires d'automatismes CCAG dédiés, installées en divisions de contrôle-commande 1 et 4,
- l'instrumentation nécessaire découplée des autres systèmes de contrôle-commande,
- les moyens d'information nécessaires en accident grave et installés au Pupitre AG, comprenant en particulier les moyens de commandes d'ouverture des 2 vannes de décharge Accident Grave (activés par commutateurs de basculement).

Ces équipements sont alimentés par une source électrique secourue par batterie []. Ils sont utilisés lorsque le basculement MCP / PAG (accolé au MCS) a été réalisé.

Avant basculement au PAG ([] après le début de la Perte Totale des Alimentations Electrique), et [] au retour d'une source d'alimentation électrique, les moyens de conduite normaux sont utilisés. Certains automatismes et actions sont réalisés [] tels que l'isolement enceinte, la mise en service de l'EDE,…

Pour les autres scénarios d'accidents graves, les moyens de contrôle-commande suivants sont utilisés :

- Le MCP pour la conduite au niveau 2.
- Afin de garantir l'indépendance de la ligne de défense contrôle-commande portant les fonctions dédiées aux situations accident grave vis-à-vis des lignes de défense traitant les situations PCC et RRC-A, deux automates SAS dédiés accident grave en divisions 1 et 4 sont utilisés.
- Le SAS de tranche et les automates dédiés AG permettent la gestion de l'ensemble des séquences d'accident grave hormis le scénario PTAE décrit plus haut.

4.7. COUVERTURE AU TITRE DE LA ROBUSTESSE DE LA DÉFAILLANCE TOTALE DU CONTRÔLE-COMMANDE STANDARD

Comme mentionné au paragraphe 2 du sous-chapitre 7.1, des dispositions de robustesse, non requises au titre de la démonstration déterministe de sûreté et non nécessaires à l'atteinte des objectifs probabilistes de sûreté, permettent d'accroître la couverture de cumuls hautement improbables de défaillance du contrôle-commande et conditions de fonctionnement PCC2-4 et RRC-A et accident grave.

Perte totale du contrôle commande standard en situations de fonctionnement de référence PCC-2 à PCC-4

En cas de perte totale du contrôle-commande standard, et de situations de fonctionnement de référence PCC-2 à PCC-4 :

- Les événements initiateurs sont détectés par le PS et les fonctions de contrôle-commande de protection nécessaires dans les 30 premières minutes sont initiées automatiquement et mises en œuvre par le PS (cf. figure **FIG–7.2.1.10**).
- Une signalisation de la perte du contrôle-commande standard localisée au PSIS avertit les opérateurs et permet de les orienter dans la stratégie de conduite spécifique noyau dur. Cette disposition fait l'objet du document **Réf [1]**.
- Après basculement en conduite « noyau dur », cette dernière, réalisée depuis les moyens de conduite conventionnels (MCS, PAG) en s'appuyant au niveau 1 sur les systèmes de contrôle-commande de technologie TELEPERM XS (CC-ND, PS, CCAG), permet d'atteindre l'état stabilisé caractérisé au paragraphe 2 du sous-chapitre 7.1.

Perte totale du contrôle commande standard dans les situations de réduction des risques RRC-A

En cas de perte totale du contrôle-commande standard, et de situation de réduction des risques RRC-A, de la même façon :

- la perte totale du contrôle-commande standard est détectée au PSIS,
- les actions nécessaires sont initiées après basculement en conduite « noyau dur » depuis le MCS ou le PAG, les fonctions correspondantes sont réalisées dans le PS, le CCAG ou le CC-ND.

Ces fonctions permettent d'atteindre un état final stabilisé (défini au paragraphe 2 du sous-chapitre 7.1) sur l'ensemble des conditions de défaillances multiples RRC-A à l'exception de celles impliquant la défaillance d'une fonction F1 allouée à un système de technologie TELEPERM XS.

Perte totale du contrôle commande standard dans les situations de réduction des risques AG

La conduite des situations d'accident grave cumulée à la perte du SPPA T2000 reste réalisable à partir :

- des moyens de contrôle-commande disponibles sur la plateforme TELEPERM XS :
  - CCAG/PAG notamment pour couvrir la situation d'accident grave initiée par la perte totale des alimentations électriques internes et externes (PTAE),
  - PS/MCS dans les autres situations,
- de la commande d'isolement enceinte phase 2, localisée au PIPO, et câblée directement en amont du niveau 0 du contrôle-commande,
- de l'instrumentation nécessaire à la conduite des situations accident grave dont l'acquisition est dupliquée dans le TELEPERM XS et accessible moyennant le basculement au CCAG sur le PAG,
- d'un certain nombre d'actions à réaliser en local, au niveau des cellules électriques.

L'ensemble de ces fonctions de contrôle-commande permettent de garantir l'intégrité de l'enceinte de confinement sur les situations accident grave.

5. TEL QUE RÉALISÉ

Il n'y a aucun écart entre le réalisé et les principes de conception définis dans ce chapitre.

LISTE DE RÉFÉRENCES

[1] ECECC100458 A, « Principe de surveillance du système SPPA T2000 en vue d'orienter la conduite sur les dispositions Noyau Dur »

[2] PELLFDC10 F, « Spécification détaillée du Contrôle-Commande Noyau Dur »

[3] Règles de Conception et de Construction des matériels Électriques (RCC-E), édition de décembre 2005

[4] ENSEMD050222 – Cahier de données de projet complétant les exigences du RCC-E décembre 2005 pour EPR

[5] Norme CEI 61513 - Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes - exigences du chapitre 6

[6] Norme CEI 60880 - Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A

[7] Norme CEI 62138 - Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B (chapitre 6) ou C (chapitre 5)

[8] Règle Fondamentale de Sûreté (RFS) II.4.1.a relative aux logiciels des systèmes électriques classés de sûreté, dite RFS logiciels

TAB–7.2.1.1 ALLOCATION DES CATÉGORIES DE FONCTIONS AUX SYSTÈMES

Catégories de fonctions de contrôle-commande	Classe de la Fonction	Systèmes niveau 1	Systèmes niveau 2
Fonctions de contrôle en conduite normale et d'aide à l'opérateur	Au plus F2	RCSL ou PAS *	MCP
Fonctions LCO (Conditions limites d'exploitation) de surveillance des principaux paramètres du réacteur pris en compte comme conditions initiales des études de sûreté	F2	RCSL ou PAS *	MCP
Fonctions de limitation	F2	RCSL ou PAS *	MCP
Fonctions de protection réacteur Exception (cf sous-chapitre 3.2) : les fonctions support aux fonctions F1A déjà en service avant l'événement, dont le fonctionnement n'est pas influencé par l'événement et dont l'opérabilité n'est pas affectée par les conséquences directes ou indirectes de l'événement, peuvent être classées F1B.	F1A F1B	PS	MCS (F1A) MCP (avec commandes câblées) et MCS PSIS (signe de vie pour basculer au MCS)
Fonctions de gestion post-accidentelle	F1B	SAS ou PS	MCP (avec commandes câblées pour les commandes PS), MCS PSIS (signe de vie pour basculer au MCS)
Fonctions directement liées au contrôle de la radioactivité pendant le fonctionnement normal	F2	SAS ou PAS	MCP et MCS ou postes de conduite locaux
Fonctions de commande pouvant provoquer un événement de type PCC-3 ou PCC-4 (voir sous-chapitre 3.2)	F1B	SAS	MCP et MCS PSIS (signe de vie pour basculer au MCS)

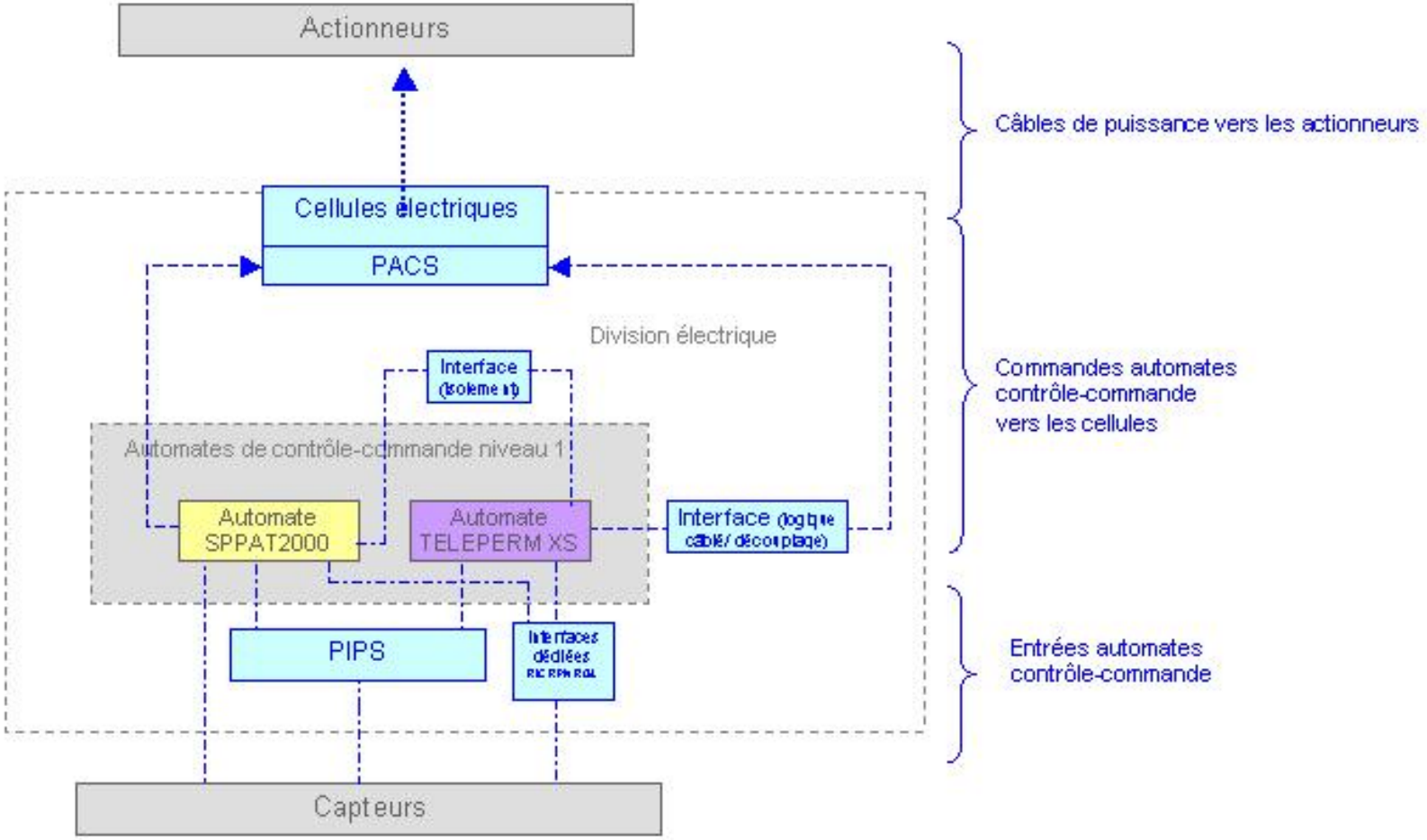
Catégories de fonctions de contrôle-commande	Classe de la Fonction	Systèmes niveau 1	Systèmes niveau 2
Fonctions spécifiquement conçues pour contrôler les agressions internes et externes	F2	SAS, PAS	MCP PIPO (évacuation salle de commande)
Fonctions assurant la gestion des situations de fonctionnement RRC-A	F2	RCSL, SAS ou PS	MCP MCS PSIS (signe de vie pour basculer au MCS)
Fonctions assurant la gestion des situations de fonctionnement accident grave	F2	SAS, PS SAS RRC-B ou CCAG	MCP ou PAG
Fonctions de robustesse visent à l'atteinte d'un état dit stable évitant la fusion du cœur en cas de perte du contrôle-commande standard	NC	CC-ND	MCS (après basculement),PIPO

* la fonction d'initialisation peut également être allouée au PS

TAB–7.2.1.2 ALLOCATION DES SYSTÈMES DE CONTRÔLE-COMMANDE DANS LES LOCAUX

FIG–7.2.1.1 ARCHITECTURE GÉNÉRALE DU CONTRÔLE-COMMANDE

FIG–7.2.1.2 SCHÉMA SIMPLIFIÉ DES LIAISONS ET INTERFACES ÉLECTRIQUES INTERVENANT DANS LA CHAINE FONCTIONNELLE D'ÉLABORATION DES ORDRES



FIG–7.2.1.3 IMPLANTATION GÉOGRAPHIQUE DES ÉQUIPEMENTS DE CONTRÔLE-COMMANDE

FIG–7.2.1.4 INSTALLATION DES ÉQUIPEMENTS DE CONTRÔLE-COMMANDE EN SALLE DE COMMANDE

FIG–7.2.1.5 EXPLOITATION NORMALE

FIG–7.2.1.6 EXPLOITATION DURANT LA MITIGATION D'ACCIDENT AVEC L'ENSEMBLE DES SYSTÈMES DE CC DISPONIBLES

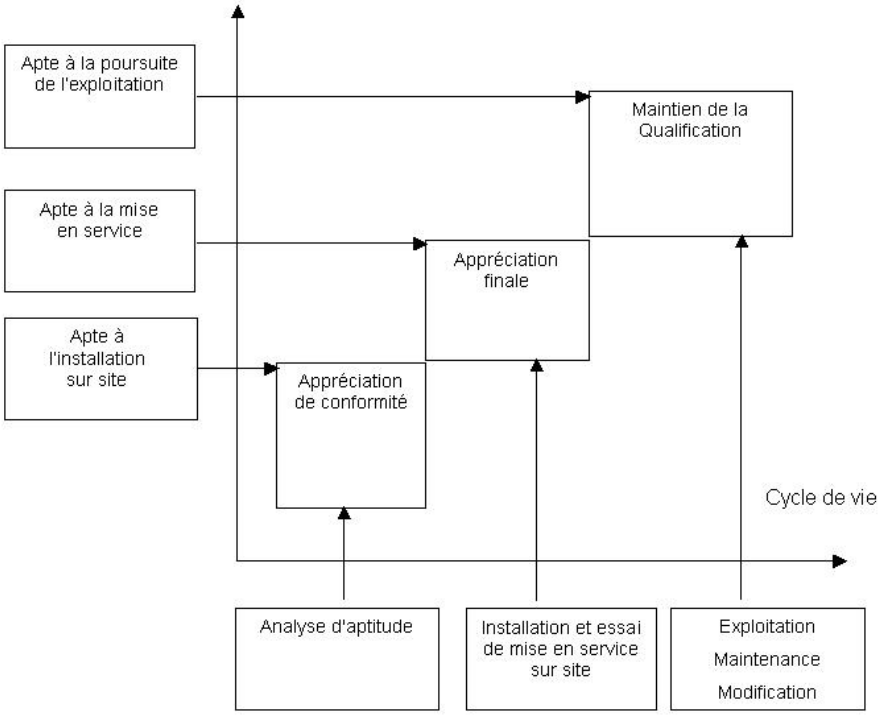
FIG–7.2.1.7 EXPLOITATION AVEC SYSTÈMES DE CC DE SÛRETÉ F1 UNIQUEMENT

FIG–7.2.1.8 CONDUITE À LA STATION DE REPLI

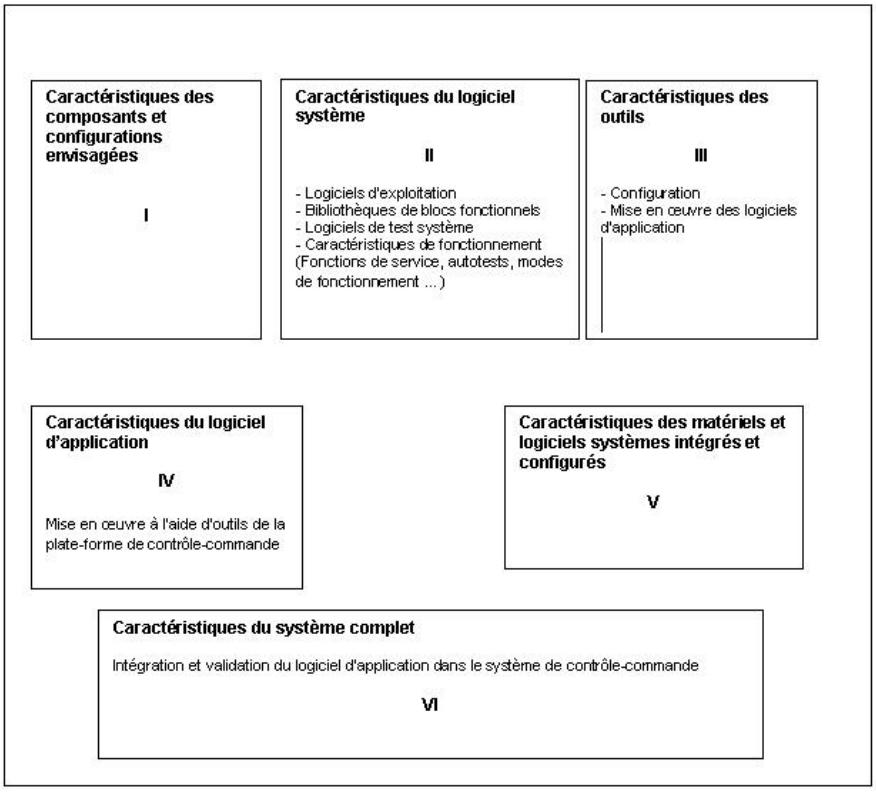
FIG–7.2.1.9 CONDUITE DES ACCIDENTS GRAVES

FIG–7.2.1.10 PERTE TOTALE DU CONTRÔLE-COMMANDE STANDARD (ROBUSTESSE)

FIG–7.2.1.11 QUALIFICATION ET CYCLE DE VIE DES ÉQUIPEMENTS DE CC



FIG–7.2.1.12 APPRÉCIATION DE CONFORMITÉ



SOMMAIRE

TABLEAUX :

FIGURES :

.7.2.2 INSTALLATION DES ÉQUIPEMENTS

1. ALIMENTATION DU CONTRÔLE-COMMANDE

L'alimentation électrique secourue de tranche, y compris l'alimentation secourue en courant continu et courant alternatif pour les équipements de contrôle-commande est décrite au chapitre 8.

Alimentation des armoires de contrôle-commande :

L'alimentation secourue des armoires de contrôle-commande est réalisée par des convertisseurs c.a./c.c, et par application du Rex de l'incident Forsmark, des convertisseurs c.c/c.c. Les convertisseurs sont alimentés par quatre tableaux 400 V c.a. secourus par batterie et par quatre tableaux 220 V c.c. secourus par batterie, et en cas de défaillance des convertisseurs c. c./c. a. via une commutation électronique à partir des quatre tableaux 400V régulés.

Ils sont installés dans les [] bâtiments diesel 1 à 4. Par exception les armoires de contrôle-commande localisés dans []BTE et du BL[] sont alimentées depuis des tableaux de l'îlot conventionnel, compte tenu de l'admissibilité d'un sous-classement de ces tableaux en regard des fonctions de sûreté assurées par les systèmes de contrôle-commande installés dans ces locaux.

En général, un ensemble d'armoires de contrôle-commande est alimenté à partir de deux convertisseurs : un convertisseur c.a./c.c., et un convertisseur c.c./c.c. redondants, alimentés par deux tableaux redondants, dont un pouvant être alimenté par la même division ou la division voisine (c'est à dire 1 +2 et 3 +4). Chacun des deux convertisseurs est capable d'alimenter l'ensemble complet d'armoires de contrôle-commande. Ils sont installés dans des armoires d'alimentation séparées comprenant plusieurs convertisseurs. [] Les groupes d'armoires de chacune des plates-formes de contrôle-commande (TELEPERM XS / SPPA T2000) disposent d'alimentations distinctes.

Le second niveau de tension utilisé pour polariser les signaux d'entrée/sortie est de 24 Vcc.

Alimentation pour IHM :

L'alimentation en c.a. sans coupure pour l'IHM est fournie par quatre tableaux 400 V c.a. qui sont eux alimentés à partir des quatre tableaux 400 V c.a. secourus par batterie et en cas de défaillance des convertisseurs c.c./c.a. via une commutation électronique à partir des quatre tableaux 400V régulés.

L'alimentation en c.a. est fournie à partir des 4 divisions pour les équipements d'IHM (Ecrans grand format (Synoptique), postes opérateur informatisés du MCP) en SdC, [], à partir des divisions 1 et 4 pour les postes de repli informatisés en SdR et à partir des divisions 1 et 4 pour les unités de traitement du MCP (PU du contrôle-commande standard)[].

2. IMPLANTATION ET INSTALLATION DES ÉQUIPEMENTS

Affectation des systèmes de contrôle-commande aux bâtiments de l'EPR :

L'implantation des principaux équipements de contrôle-commande est fournie par le tableau **TAB–7.2.2.2**.

La figure **FIG–7.2.2.3** fournit une visualisation de la répartition des systèmes de contrôle-commande dans les différents locaux ainsi que leurs interfaces de communication.

Les systèmes de contrôle-commande de l'îlot nucléaire sont principalement disposés dans []. Cependant, une partie des systèmes de contrôle-commande, par exemple l'instrumentation, le contrôle-commande pour les engins de manutention est installée dans le BR et le BK, dans le BAN ou le BTE. Les équipements de contrôle-commande qui doivent rester opérationnels [] sont principalement installés dans les divisions 2 et 3 du BAS. Ainsi deux des quatre divisions des systèmes de contrôle-commande et de l'IHM classés F1 y compris la SdC y sont situées.

A l'intérieur du bâtiment, les principales agressions qui pourraient endommager de manière conséquente une des divisions de contrôle-commande sont : l'incendie, l'inondation. Le respect des exigences de sûreté associées aux agressions internes est réalisé notamment par une séparation physique dans des divisions distinctes et par des mesures conçues spécialement pour empêcher la propagation des agressions.

Ainsi, une séparation spatiale en 4 divisions est requise pour les 4 trains du PS tandis que pour le SAS, cette séparation dépend des systèmes mécaniques commandés qui sont affectés aux 4 divisions. Les pupitres du MCS sont installés en SdC. Le MCP fournit l'ensemble des moyens de conduite nécessaires pour l'exploitation de la tranche à partir de la SdC et en cas d'indisponibilité de la SdC à partir de la Station de repli. Les systèmes de contrôle-commande classés F1 sont regroupées dans [].

Le PAS est installé dans les locaux d'armoires de contrôle-commande des divisions 1 à 4 des BL ainsi que dans les locaux de contrôle-commande du BTE et du BLNC.

Le SAS est réparti dans les locaux d'armoires de contrôle-commande des divisions 1 à 4 du BL selon l'allocation des équipements électriques et mécaniques correspondant, ainsi que dans les bâtiments diesels (1 à 4).

Le SAS-RRC-B est réparti dans les locaux d'armoires de contrôle-commande des divisions 1 et 4 des BL.

Le PS est installé dans les locaux d'armoires de contrôle-commande des divisions 1 à 4 des BL.

Le RCSL est installé dans les locaux d'armoires de contrôle-commande des divisions 1 et 4 des BL, ainsi qu'en division 2 et 3 en ce qui concerne les unités d'acquisition des informations.

Le CCAG est réparti dans [].

Le CC-ND est réparti dans [].

Il est prévu une réserve en terme d'espace, d'alimentation et de climatisation dans chaque local d'armoires de contrôle-commande pour les éventuelles modifications. Ceci permet la préparation de la mise en œuvre des évolutions sans affecter l'exploitation de la tranche ou les systèmes de sûreté.

Les unités de traitements du MCP (PU) sont installées dans les [] divisions 1 et 4 des BL pour le contrôle-commande de tranche et dans le BTE pour le PAS BTE.

Les équipements de contrôle-commande directement liés aux équipements d'IHM ou qui sont fréquemment utilisés par le personnel, sont installés principalement au niveau []. Ceci concerne notamment les périphériques du MCP, mais également les équipements de contrôle d'accès, la surveillance incendie, les systèmes vidéo et téléphoniques. Les périphériques pour les systèmes de surveillance c'est à dire la surveillance des corps migrants, la surveillance des vibrations du GTA, l'oscillo-perturbographe, le système de calcul de cartographie des flux, une partie de la détection de la radioactivité sont installés dans []. La figure **FIG–7.2.2.4** décrit l'installation des équipements en salle de commande.

Les équipements de contrôle-commande utilisés pour l'îlot conventionnel (CI) ou le BOP (autres ouvrages de site) sont installés respectivement dans [] de l'îlot conventionnel (BLNC) ou [] au BOP.

Les outils de configuration et de diagnostic des équipements de contrôle-commande sont installés [] dans le BAS/BL [] mais également dans le BTE pour la gestion de la partie BTE du PAS.

Les équipements et systèmes de contrôle-commande commandés en local sont installés à proximité []. La surveillance de leurs principales fonctions et des dysfonctionnements est réalisée à partir du MCP.

Les équipements de contrôle-commande des systèmes de manutention (par exemple machine de chargement combustible, pont roulant) sont [].

Salle de Commande Principale (SdC) :

La Salle de Commande principale (SdC) est située, pour une exploitation pratique dans toutes les conditions de tranche, []. Elle est ainsi protégée contre le rayonnement, [] et les séismes. Tout équipement installé dans la SdC qui est appelé à fonctionner ou pas à la suite d'un séisme est conçu pour ne pas engendrer de situation préjudiciable aux opérateurs dans la réalisation des leurs tâches i. e garder leur stabilité – (classe sismique 2 a minima). L'indépendance fonctionnelle et la séparation physique sont prises en compte lorsque les équipements de classes de sûreté différentes sont à proximité les uns des autres en SdC conformément au chapitre 17.

La ventilation et l'alimentation sur quatre trains ainsi que l'éclairage sont conçus pour maintenir les conditions opérationnelles de la SdC et la surveillance de la tranche dans toutes les conditions PCC et RRC-A et accident grave. Les conditions d'environnement en SdC sont de nature à permettre aux opérateurs de travailler efficacement et confortablement. L'aménagement du niveau SdC assure l'accès des opérateurs en SdC dans toutes les conditions d'exploitation de la tranche. L'évacuation de la SdC est possible par des chemins courts vers le niveau inférieur où se trouve la Station de Repli.

L'espace en SdC est suffisant pour permettre à l'équipe de conduite de réaliser toutes les actions nécessaires. L'aménagement des différentes zones opérationnelles facilite la coordination et la communication entre les membres de l'équipe de conduite.

L'aménagement du niveau de la SdC prend en compte une limitation du besoin d'accès à la SdC par d'autres membres du personnel de la tranche tout en préservant la capacité nécessaire d'échange de l'effectif de la SdC avec les rondiers et les équipes de maintenance ainsi qu'avec d'autres personnels se trouvant dans les autres locaux, tels que le bureau du Chef d'exploitation, le local de maintenance contrôle-commande, le local de consignation et le local de surveillance des systèmes périphériques.

Les postes opérateur informatisés, le synoptique, le MCS, les moyens de communication, et le moyen central de signalisation Incendie sont installés en Salle de Commande.

Locaux annexes :

Le local technique de crise (LTC) se situe en dehors de la SdC et possède un accès indépendant.

Les sanitaires et une cuisine sont également à proximité de la SdC.

La documentation est disponible dans les bureaux, en SdC et dans le LTC.

Des moyens de commande locaux sont installés si une des conditions suivantes est remplie :

[]

Station de Repli (SdR) :

Les agressions internes conduisant à l'indisponibilité de la SdC requièrent l'utilisation des postes opérateurs en station de repli pour amener et maintenir la tranche en état d'arrêt sûr. Par hypothèse de conception, il n'y a pas de cumul d'inhabitabilité de la SdC (due à un incendie par exemple) avec une situation incidentelle ou accidentelle, la seule exception prise en compte est la perte des sources externes.

Afin d'assurer l'indépendance de la Station de Repli par rapport à la SdC, celle-ci est installée dans un secteur de feu différent [] avec un accès distinct. Les unités de traitement du MCP sont situées dans [] des divisions 1 et 4 afin d'être robuste à une agression interne. Les liaisons, par exemple les gaines de ventilation entre les secteurs de feu, sont conçues pour ne pas propager le feu.

Les postes opérateurs informatisés et les équipements de communication (téléphone) sont installés dans la Station de Repli.

Interconnexions de contrôle-commande entre les différents locaux de contrôle-commande :

Les interconnexions de contrôle-commande entre les différents locaux de contrôle-commande et à l'intérieur d'un local de contrôle-commande sont isolées électriquement selon le principe suivant :

- L'équipement de contrôle-commande classé E1 représente un îlot basse tension dans chaque division, isolé électriquement de l'équipement E1 des autres divisions et contre une surtension éventuelle de l'installation, des tableaux électriques, des équipements de contrôle-commande dans les autres bâtiments et des équipements de contrôle-commande dans le même local mais de classement inférieur (E2/NC).
- L'équipement de contrôle-commande classé E2/NC représente un second îlot basse tension dans les mêmes locaux d'armoires de contrôle-commande. La propagation de surtension d'une autre division ou d'un autre bâtiment est évitée grâce à un isolement électrique.

Cet isolement est réalisé par :

- l'utilisation d'opto-coupleurs, de modules d'isolement ou de câble en fibres optiques dans le cas des connexions câblées,
- l'utilisation de fibres optiques dans le cas des connexions par bus.

Des barrières résistantes au feu pendant [] minutes suivant l'ETC-F sont installées entre les locaux d'armoires de contrôle-commande des différents secteurs de feu et entre les gaines techniques et les traversées de câble des différentes divisions.

Armoires de contrôle-commande :

L'aménagement [] du BAS prévoit suffisamment d'espace pour l'ensemble des armoires de contrôle-commande à installer dans l'îlot nucléaire.

A l'intérieur de ces locaux, les armoires de contrôle-commande pour le même système de contrôle-commande sont disposées côte à côte pour former un groupe d'armoires, dans les limites imposées par les exigences de séparation ou d'isolement entre armoires requises du point de vue de la défense en profondeur, ou du classement de sûreté.

Lors de l'installation des différents composants électroniques à l'intérieur des armoires, les exigences suivantes concernant l'IEM sont généralement prises en compte :

[]

Toutes les armoires, pupitres de commandes et panneaux sont liés par leur châssis au ferraillage ou à la structure acier du bâtiment conformément au paragraphe 2 du sous-chapitre 8.4.

Les équipements de contrôle-commande sont conçus pour répondre aux exigences de dimensionnement suivant leur classement sismique. Les armoires des équipements de contrôle-commande classés séisme SC1 sont qualifiées séisme quant au spectre du sol associé. Les armoires des équipements de contrôle-commande classés séisme SC2 sont conçues et qualifiées afin de n'avoir aucune influence sur les armoires E1 en cas de séisme (pas d'effet missile).

Cheminement des câbles de contrôle-commande :

Le câblage de contrôle-commande utilise plusieurs connexions réseau indépendantes en plus du câblage conventionnel, notamment pour l'interconnexion des différents systèmes de contrôle-commande. Elles peuvent être décrites comme suit :

1) niveau 2 – connexion réseau Niveau 2 du MCP aux écrans des postes opérateurs,
2) niveau de communication principal (réseau de tranche) – connexions réseau entre les quatre divisions du BAS/BL, les bâtiments diesel, l'îlot conventionnel (BLNC), le BAN et le BTE,
3) les connexions de réseau entre une division du BAS/BL et une autre division,

Par exemple, connexions point à point des équipements de contrôle-commande classés E1 y compris entre les cartes d'E/S vers le panneau conventionnel du MCS.

4) Connexions réseau au sein d'une division du BAS/BL.

Tous les câbles entre les armoires à l'intérieur []. Les câbles entre [] ou à partir des [] vers le procédé sont tirés dans des goulottes de divisions différentes. Les interconnexions de contrôle-commande entre divisions font appel aux réseaux locaux en fibres optiques sans parties métalliques. Si des câbles en cuivre sont utilisés, le RCC-E impose que par le biais de dispositifs d'isolement une agression interne associée à une défaillance unique ne puisse pas causer la perte du contrôle-commande F1 sur plus de deux divisions.

Les câbles de contrôle-commande de contrôle et de mesure ainsi que les câbles réseau (fibre-optique ou coaxial) doivent être séparés des câbles de basse et moyenne tension conformément aux recommandations du paragraphe 1 du sous-chapitre 8.4. Un cheminement séparé dans des goulottes ou des gaines métalliques sur des chemins de câble indépendants est requis uniquement pour les signaux de détection du flux neutronique et du rayonnement.

Les signaux F1 alloués dans des divisions différentes, ne passent pas par le même câble, la même sous-distribution ou la même traversée électrique et sont protégés contre la propagation d'une agression interne. Ils n'utilisent pas le même boîtier de raccordement ou le même câble que les signaux F2/NC ou sont distinctement séparés l'un de l'autre au moins sur les principaux cheminements. Le câblage vers la SdC concerne principalement les câbles de raccordement au panneau conventionnel du MCS qui cheminent par [] au travers de goulottes / Chemins de câbles dédiés à chaque division. Le câblage des unités de traitement du MCP (situés en divisions 1 et 4) vers la SdC et la Station de Repli est séparé par division grâce à des goulottes de câbles indépendantes afin de faire face aux agressions internes.

Des câbles de contrôle-commande conventionnels blindés mis à la terre sont utilisés entre le []. Le concept de mise à la terre, basé sur une boucle de terre autour de chaque bâtiment et un réseau maillé connecté aux équipements de contrôle-commande entre les bâtiments comprend une protection contre la foudre conformément au paragraphe 2 du sous-chapitre 8.4.

Du câble à fibres optiques est utilisé comme moyen de transmission dans les applications où une insensibilité aux interférences électriques ou électromagnétiques, une isolation galvanique entre systèmes ou divisions et une longueur de bus jusqu'à [] m sont requis. Grâce à l'utilisation de plusieurs réseaux, les applications peuvent être raccordées par des passerelles, des routeurs ou des switche.

Des moyens de séparation sont utilisés pour les réseaux locaux à fibres optiques d'interconnexion traversant une division avec forte concentration de données (par exemple le réseau de tranche ou le réseau de niveau 2). Les réseaux locaux sont tolérants à une défaillance unique (réseau local redondant ou bus en anneau) afin d'obtenir un haut niveau de fiabilité pour la transmission de données et sont disposés dans différents chemins de câble afin de faire face aux agressions internes. Ces dispositions garantissent :

- en ce qui concerne le réseau Plant bus, qu'un incendie dans une division du BAS/BL ne doit pas entraîner de dysfonctionnement des systèmes de sûreté, connectés au Plant bus, situés dans les autres divisions,
- en ce qui concerne le réseau SAS Bus, qu'un incendie dans une division du BAS/BL ne doit pas entraîner de dysfonctionnement des systèmes de sûreté, connectés à ces réseaux, situés dans les divisions voisines,
- en ce qui concerne les réseaux du Système de Protection, qu'un incendie dans une division du BAS/BL ne doit pas entraîner d'autre perte que celles des informations et actionneurs gérés par cette division. L'information générée par une autre division, transitant éventuellement par la division affectée par l'incendie, à destination d'une troisième division, doit être protégée des conséquences de l'incendie.

3. CONDITIONS D'AMBIANCE

Les conditions d'ambiance (température, hygrométrie) dans ces locaux sont définies au sous-chapitre 9.4.

L'éclairage normal et de secours ainsi que l'éclairage des chemins d'évacuation sont décrits au sous-chapitre 9.5.

Les principes de conception permettant d'assurer une protection efficace de ces locaux contre les interférences électromagnétiques (IEM) et la foudre sont définis au paragraphe 2 du sous-chapitre 8.4.

Les locaux IHM sont pourvus de plusieurs zones d'éclairage qui peuvent être réglées manuellement pour fournir un éclairage suffisant aux opérateurs pour réaliser les tâches qui leur sont attribuées (cf. paragraphe 3 du sous-chapitre 17.2).

4. TEL QUE RÉALISÉ

Il n'y a aucun écart entre le réalisé et les principes de conception définis dans ce chapitre.

LISTE DES RÉFÉRENCES

[1] ECECC100458 A, « Principe de surveillance du système SPPA T2000 en vue d'orienter la conduite sur les dispositions Noyau Dur »

[2] PELLFDC10 F, « Spécification détaillée du Contrôle-Commande Noyau Dur »

[3] Règles de Conception et de Construction des matériels Électriques (RCC-E), édition de décembre 2005

[4] ENSEMD050222 – Cahier de données de projet complétant les exigences du RCC-E décembre 2005 pour EPR

[5] Norme CEI 61513 - Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes - exigences du chapitre 6

[6] Norme CEI 60880 - Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A

[7] Norme CEI 62138 - Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B (chapitre 6) ou C (chapitre 5)

[8] Règle Fondamentale de Sûreté (RFS) II.4.1.a relative aux logiciels des systèmes électriques classés de sûreté, dite RFS logiciels

TAB–7.2.2.1 ALLOCATION DES CATÉGORIES DE FONCTIONS AUX SYSTÈMES

Catégories de fonctions de contrôle-commande	Classe de la Fonction	Systèmes niveau 1	Systèmes niveau 2
Fonctions de contrôle en conduite normale et d'aide à l'opérateur	Au plus F2	RCSL ou PAS *	MCP
Fonctions LCO (Conditions limites d'exploitation) de surveillance des principaux paramètres du réacteur pris en compte comme conditions initiales des études de sûreté	F2	RCSL ou PAS *	MCP
Fonctions de limitation	F2	RCSL ou PAS *	MCP
Fonctions de protection réacteur Exception (cf sous-chapitre 3.2) : les fonctions support aux fonctions F1A déjà en service avant l'événement, dont le fonctionnement n'est pas influencé par l'événement et dont l'opérabilité n'est pas affectée par les conséquences directes ou indirectes de l'événement, peuvent être classées F1B.	F1A F1B	PS	MCS (F1A) MCP (avec commandes câblées) et MCS PSIS (signe de vie pour basculer au MCS)
Fonctions de gestion post-accidentelle	F1B	SAS ou PS	MCP (avec commandes câblées pour les commandes PS), MCS PSIS (signe de vie pour basculer au MCS)
Fonctions directement liées au contrôle de la radioactivité pendant le fonctionnement normal	F2	SAS ou PAS	MCP et MCS ou postes de conduite locaux
Fonctions de commande pouvant provoquer un événement de type PCC-3 ou PCC-4 (voir sous-chapitre 3.2)	F1B	SAS	MCP et MCS PSIS (signe de vie pour basculer au MCS)
Fonctions spécifiquement conçues pour contrôler les agressions internes et externes	F2	SAS, PAS	MCP PIPO (évacuation salle de commande)

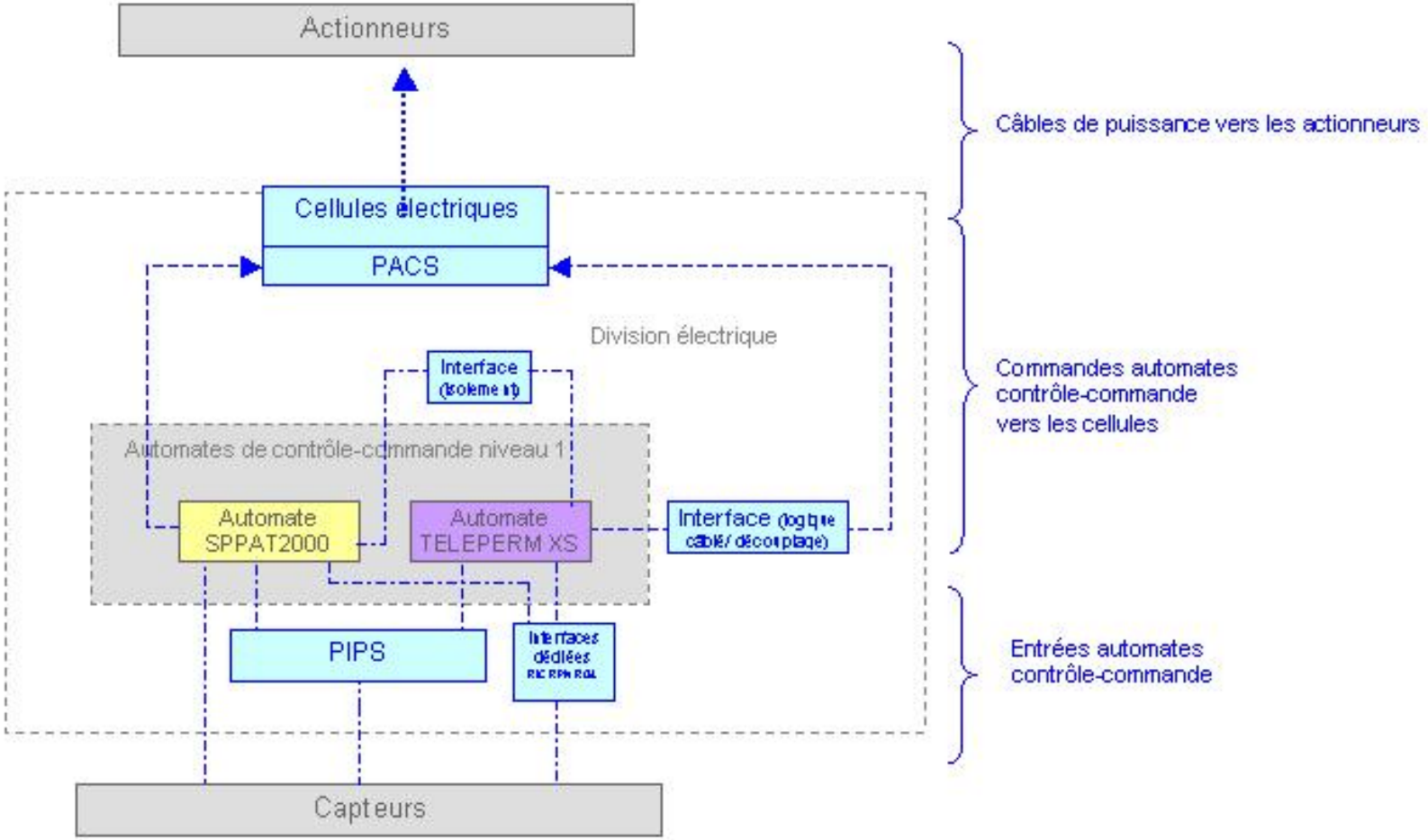
Catégories de fonctions de contrôle-commande	**Classe de la Fonction**	**Systèmes niveau 1**	**Systèmes niveau 2**
Fonctions assurant la gestion des situations de fonctionnement RRC-A	F2	RCSL, SAS ou PS	MCP MCS PSIS (signe de vie pour basculer au MCS)
Fonctions assurant la gestion des situations d'accident grave	F2	SAS, PS SAS RRC-B ou CCAG	MCP ou PAG
Fonctions de robustesse visent à l'atteinte d'un état dit stable évitant la fusion du cœur en cas de perte du contrôle-commande standard	NC	CC-ND	MCS (après basculement),PIPO

* la fonction d'initialisation peut également être allouée au PS

TAB–7.2.2.2 ALLOCATION DES SYSTÈMES DE CONTRÔLE-COMMANDE DANS LES LOCAUX

FIG–7.2.2.1 ARCHITECTURE GÉNÉRALE DU CONTRÔLE-COMMANDE

FIG–7.2.2.2 SCHÉMA SIMPLIFIÉ DES LIAISONS ET INTERFACES ÉLECTRIQUES INTERVENANT DANS LA CHAINE FONCTIONNELLE D'ÉLABORATION DES ORDRES



FIG–7.2.2.3 IMPLANTATION GÉOGRAPHIQUE DES ÉQUIPEMENTS DE CONTRÔLE-COMMANDE

FIG–7.2.2.4 INSTALLATION DES ÉQUIPEMENTS DE CONTRÔLE-COMMANDE EN SALLE DE COMMANDE

FIG–7.2.2.5 EXPLOITATION NORMALE

FIG–7.2.2.6 EXPLOITATION DURANT LA MITIGATION D'ACCIDENT AVEC L'ENSEMBLE DES SYSTÈMES DE CC DISPONIBLES

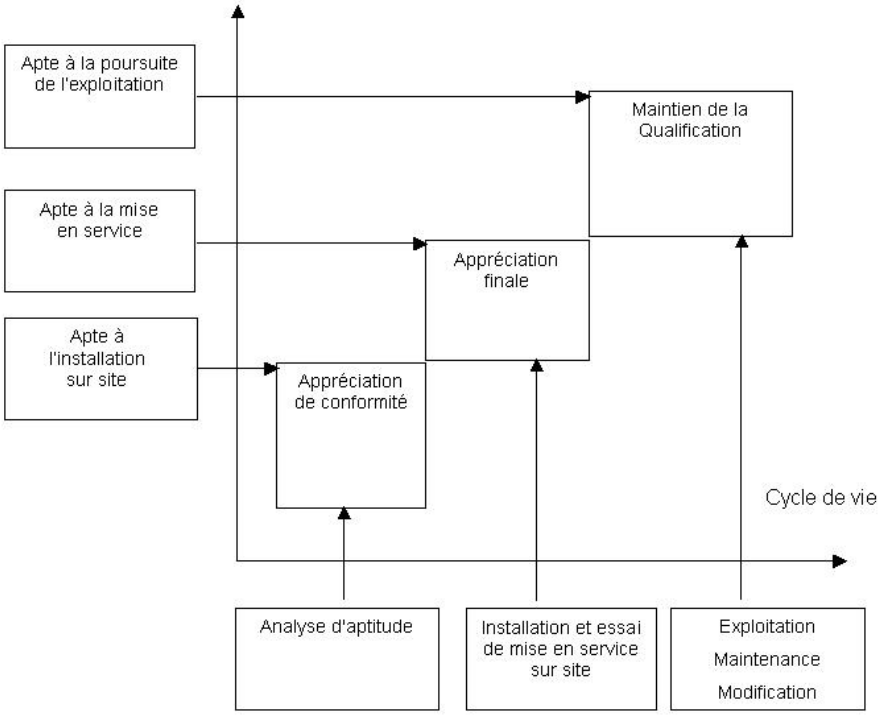
FIG–7.2.2.7 EXPLOITATION AVEC SYSTÈMES DE CC DE SÛRETÉ F1 UNIQUEMENT

FIG–7.2.2.8 CONDUITE À LA STATION DE REPLI

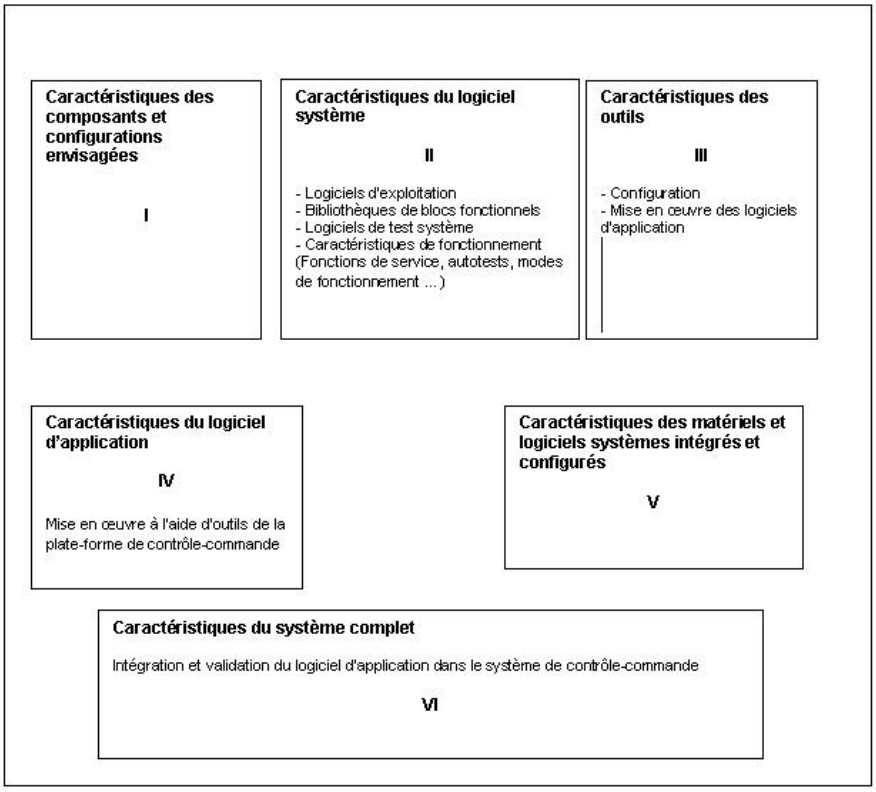
FIG–7.2.2.9 CONDUITE DES ACCIDENTS GRAVES (SITUATIONS D'ACCIDENT GRAVE)

FIG–7.2.2.10 PERTE TOTALE DU CONTRÔLE-COMMANDE STANDARD (ROBUSTESSE)

FIG–7.2.2.11 QUALIFICATION ET CYCLE DE VIE DES ÉQUIPEMENTS DE CC



FIG–7.2.2.12 APPRÉCIATION DE CONFORMITÉ



SOMMAIRE

FIGURES :

.7.2.3 PRINCIPES DE QUALIFICATION DES DIFFÉRENTS ÉQUIPEMENTS ET SYSTÈMES DE CONTRÔLE-COMMANDE

1. INTRODUCTION

Définition de la Qualification

La qualification des équipements de contrôle-commande est le processus par lequel on s'assure avec un degré de certitude élevé que ces équipements sont capables de répondre en permanence aux exigences de conception en matière de performances requises pour la sûreté dans les conditions d'environnement spécifiées au moment où l'on en a besoin.

La qualification ne concerne que les équipements classés de sûreté. Un équipement de contrôle-commande doit être qualifié si son classement contrôle-commande est E1A, E1B ou E2. Il est également possible qu'un équipement dont le classement contrôle-commande est Non Classé (NC) doive être qualifié s'il y a un requis fonctionnel d'intégrité (typiquement intégrité sous sollicitation sismique). La qualification à réaliser dans ce dernier cas est réduite à une qualification matérielle (voir § 5.) limitée à ce qui est nécessaire pour démontrer l'intégrité.

Définitions

Appréciation

Jugement basé sur la preuve de l'aptitude des équipements de contrôle-commande à remplir une mission particulière ou un type de mission.

Architecture d'un système de contrôle-commande

Structure organisant un système de contrôle-commande (paragraphe 3.36 de CEI61513 Réf [3]).

Équipement

Une ou plusieurs parties d'un système. Un composant système est une partie déterminée et définissable (et généralement amovible) d'un système (paragraphe 3.17 de CEI61513 Réf [3]).

Nota : Cette définition dévie de celle donnée dans la CEI 60780. Cet écart est justifié par le fait que la CEI 61513 Réf [3] considère que l'équipement fait partie du système alors que la CEI 60780 considère que l'équipement est l'objet de la qualification.

Évaluation

Attribution d'une valeur qualitative ou quantitative aux caractéristiques d'un système.

Famille d'équipements

Ensemble de composants matériels et logiciels pouvant travailler de manière complémentaire dans une ou plusieurs architectures définies (configurations). Le développement des configurations spécifiques à la centrale et du logiciel d'application associé peut être réalisé par des outils logiciels. Une famille de composants fournit normalement un certain nombre de fonctionnalités standard (bibliothèque des fonctions d'application) qui peuvent être combinées pour générer un logiciel d'application spécifique (paragraphe 3.18 de CEI 61513 Réf [3]).

Nota : Le terme « plate-forme de contrôle-commande » est utilisé dans la suite pour désigner une « famille d'équipements ».

Fonction d'application

Fonction d'un système de contrôle-commande qui accomplit une tâche relative au processus sous contrôle plutôt qu'au fonctionnement du système lui-même (paragraphe 3.1 de CEI 61513 **Réf [3]**).

Logiciel d'application

Partie du logiciel d'un système de contrôle-commande qui exécute des fonctions d'application (paragraphe 3.2 de CEI 61513 **Réf [3]**).

Logiciel système

Partie du logiciel d'un système de contrôle-commande, d'un équipement ou d'une famille d'équipements conçue pour faciliter le développement, l'exploitation et la modification de ces systèmes et des programmes associés (paragraphe 3.33 de CEI 62138 **Réf [5]**).

Plate-forme de contrôle-commande

Le terme « plate-forme de contrôle-commande » est utilisé dans la suite pour désigner une « famille d'équipements ».

Système de contrôle-commande

Système exécutant des fonctions de contrôle-commande ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même. Sa technologie est électrique et/ou électronique et/ou électronique programmable.

Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources propres ou partagées (paragraphe 3.35 de CEI 61513 **Réf [3]**).

2. QUALIFICATION ET CYCLE DE VIE

Une étude de la faisabilité de la qualification de l'équipement de contrôle-commande s'assure que :

- La qualification est faisable dans le contexte des exigences applicables pour le classement visé,
- Les exigences qui doivent être appréciées seront vérifiées par un processus limité d'un bon rapport coût / efficacité par une personne ou une machine,
- Tout développement nouveau répondra aux exigences de sûreté dès le départ,
- La qualification pourra être maintenue aussi longtemps que la fonction de sûreté à laquelle participe le système de contrôle-commande est nécessaire.

Suivant le stade du cycle de vie (voir **FIG–7.2.3.1**) :

- Une appréciation de conformité garantit que le système de contrôle-commande répond aux exigences applicables. Elle termine la phase de conception et permet l'installation du système sur site,
- Une appréciation finale garantit qu'après ses installation et essais sur site, le système de contrôle-commande réalise les fonctions de sûreté telles qu'elles sont requises et est donc apte à la mise en service,
- Le système de contrôle-commande est maintenu dans le temps en état qualifié ce qui permet de poursuivre son exploitation.

2.1. APPRÉCIATION DE CONFORMITÉ

Le concepteur peut sélectionner un équipement de contrôle-commande pré-existant ou développer un nouvel équipement. Dans les deux cas, l'équipement doit être apte à assurer les fonctions de sûreté spécifiées.

L'équipement de contrôle-commande peut être un composant unique ou appartenir à une plate-forme de contrôle-commande configurée pour réaliser les différents types de fonctions d'applications attendues.

Analyse d'aptitude

Avant l'acceptation de la spécification du système de contrôle-commande, l'analyse d'aptitude évalue et apprécie la conformité de cette spécification au cahier des charges.

Appréciation de conformité

Sur la base de l'analyse d'aptitude, la qualification est mise en oeuvre afin d'apprécier la conformité des caractéristiques du système de contrôle-commande à sa spécification.

La personne réalisant l'appréciation ainsi que le concepteur doivent se mettre d'accord afin de limiter l'analyse et les tests à mettre en œuvre à l'étendue définie par les critères d'acceptation pertinents.

2.2. APPRÉCIATION FINALE

Les contrôles d'installation et essais de mise en service sur site démontrent que le système de contrôle-commande s'intègre de manière fonctionnelle au sein de l'architecture de contrôle-commande de la tranche et fonctionne avec les équipements contrôlés conformément aux exigences des fonctions de sûreté.

L'appréciation finale démontre que le système de contrôle-commande est capable de répondre en permanence aux exigences de conception en matière de performances requises pour la tâche de sûreté dans les conditions d'environnement existantes au moment où l'on en a besoin.

2.3. MAINTIEN DE LA QUALIFICATION

La qualification doit être maintenue pendant la durée de vie opérationnelle du système de contrôle-commande, en particulier dans les cas suivants :

- Modifications de la configuration matérielle du système de contrôle-commande,
- Remplacement de matériel / logiciel du système de contrôle-commande,
- Modifications et extensions du logiciel d'application,
- Modifications des outils s'ils sont utilisés pour les évaluations lors de la qualification,
- Modification des interfaces.

Du point de vue du comportement du matériel dans le temps, la stratégie de maintien de la pérennité de la qualification repose sur deux critères :

- Tout d'abord, une maintenance préventive du matériel afin de remplacer des composants identifiés comme sensibles par le constructeur contribue à l'accomplissement de ce maintien. De manière périodique, les composants électromécaniques tels que les ventilateurs ou les relais doivent être remplacés selon les prescriptions du manuel de maintenance du matériel. Des tests périodiques sont également préconisés pour vérifier les propriétés fonctionnelles de certains composants (tels que les condensateurs des blocs d'alimentation) afin de décider si leur remplacement est nécessaire.
- Ensuite, la mise en place d'un Observatoire du Vieillissement du Contrôle-Commande (OVCC) à partir de la première Visite Décennale, permet d'anticiper l'arrivée en fin de vie d'un matériel. Cet

observatoire composé d'experts de plusieurs unités d'EDF, a pour mission, de réaliser un bilan technique (vieillissement, obsolescence) et économique (coûts d'indisponibilité et de maintenance) des différentes plate-formes de contrôle-commande. Au regard des constats effectués, un plan d'action est mis en oeuvre à l'horizon de la prochaine visite décennale.

2.4. DOCUMENTATION ASSOCIÉE À LA QUALIFICATION

La documentation qui doit être associée à la qualification est définie au sous-chapitre 3.7. Le **§ 6.** précise lorsque nécessaire la documentation complémentaire qui concerne la qualification fonctionnelle d'un système de contrôle-commande.

3. PROCESSUS DE QUALIFICATION

La qualification d'un équipement de contrôle-commande consiste à s'assurer que :

1) Dans les conditions normales (nominales) d'utilisation et aux conditions limites d'influence (avalanches d'informations par exemple), l'équipement remplit le service spécifié,
2) Soumis aux conditions limites d'environnement (perturbations électriques et électromagnétiques, tensions d'alimentation, conditions climatiques, séisme,…), l'équipement continue à remplir son service,
3) La dégradation éventuelle de ce service au cours du temps restera acceptable.

Lorsque l'équipement à qualifier est suffisamment simple (relais, capteur, enregistreur, régulateur, positionneur, actionneur, cellule électrique, …), l'ensemble des actions associées à cette démonstration porte le terme générique de qualification. Notons qu'un équipement programmé n'est généralement pas considéré suffisamment simple, même lorsqu'il s'agit d'un relais, capteur, enregistreur, régulateur, positionneur, actionneur, ou d'une cellule électrique.

Lorsque l'équipement à qualifier est un système de contrôle-commande dont les fonctionnalités sont plus complexes, on désigne communément par « qualification fonctionnelle » le point 1 (le système remplit correctement le service spécifié dans les conditions normales d'utilisation et aux conditions limites d'influence), les points 2 et 3 (fonctionnement aux limites d'environnement - comportement dans le temps) étant désignés par le terme « qualification matérielle ».

La qualification fonctionnelle peut être réalisée par essais, analyses et/ou retour d'expérience. Elle consiste en une validation des fonctions du système, une évaluation de leurs possibilités de combinaison pour remplir le service spécifié et une évaluation des caractéristiques de fonctionnement du système.

La qualification matérielle, réalisée préférentiellement par essais, comprend la vérification du fonctionnement du système aux limites d'environnement extérieur mais aussi lors de défauts internes (comportement sur défaut interne - capacité à signaler ces défauts au personnel de conduite).

La qualification implique des procédures techniques.

4. PRINCIPES DE QUALIFICATION

La qualification d'un équipement de contrôle-commande peut être réalisée au travers :

- d'essais,
- d'analyses,
- d'expérience opérationnelle.

Ces possibilités peuvent être utilisées individuellement ou en association selon les caractéristiques de l'équipement de contrôle-commande concerné.

4.1. ESSAIS

Deux grandes sortes d'essais interviennent dans la qualification d'un équipement de contrôle-commande : les essais de qualification et les essais de recette ou de validation.

Essais de qualification

Les essais de qualification visent la qualification matérielle (voir § 5.) de l'équipement de contrôle-commande. Ils sont réalisés sur un échantillon d'équipements de même conception que ceux qui seront installés sur site.

Les essais de qualification de l'équipements de contrôle-commande mettant en oeuvre les conditions simulées de l'environnement sont la méthode privilégiée pour démontrer que les caractéristiques de l'échantillon sont conformes aux caractéristiques attendues même lorsque soumis aux facteurs d'influence sous lesquels ceux-ci doivent pouvoir remplir leur rôle.

Essais de recette ou de validation

Les essais de recette ou de validation sont réalisés afin de couvrir les fonctionnalités attendues de l'équipement de contrôle-commande sur le palier EPR. Ces essais sont typiquement réalisés hors site sur l'équipement destiné au site ou sur une plateforme représentative. Ils sont complétés par les essais de mise en service sur site.

4.2. ANALYSE

L'analyse intervient dans quasiment toutes les étapes du processus de qualification. Ci-dessous quelques exemples d'application de l'analyse.

L'analyse est la méthode de base pour l'évaluation du développement matériel et logiciel c'est-à-dire que cette analyse évalue la conception matérielle et logicielle, les essais des composants, la vérification/validation et la documentation.

L'analyse (par exemple : analyse des effets de défaillances, analyse de charge critique…) est appropriée pour l'évaluation des caractéristiques qui ne peuvent pas être évaluées par les essais.

L'étude des résultats des essais et l'analyse suivant les critères d'acceptation entraînent l'appréciation de conformité aux caractéristiques testées.

4.3. RETOUR D'EXPÉRIENCE

Un équipement de contrôle-commande en technologie conventionnelle (par opposition à un équipement programmé) qui a déjà été mis en service avec succès peut être qualifié pour un service égal ou moins sévère (c'est-à-dire avec des conditions de fonctionnement moins sévères avec un rôle fonctionnel similaire) sur la base de son retour d'expérience opérationnel.

Le retour d'expérience opérationnel peut également participer à l'évaluation de la qualité des éléments pré-existants y compris les logiciels.

Le retour d'expérience opérationnel sera évalué sur la base :

- Du temps de service cumulé de l'équipement de contrôle-commande pré-existant,
- De l'historique des rapports d'erreur et des modifications de l'équipement de contrôle-commande pré-existant.

Le retour d'expérience nécessite une collecte précise des données archivées ci-dessus y compris les données concernant une utilisation similaire. La traçabilité des documents nécessite l'implication en amont des fournisseurs et utilisateurs.

5. QUALIFICATION MATÉRIELLE

Les principes exposés au sous-chapitre 3.1 ainsi qu'au sous-chapitre 3.7 s'appliquent pour la qualification matérielle des équipements de contrôle-commande.

Notons néanmoins que pour cette qualification matérielle :

- Les équipements de contrôle-commande des niveaux 1 et 2 ne sont pas qualifiés à l'ambiance dégradée, seuls les équipements de niveau 0 (instrumentation / actionneurs) peuvent être qualifiés à l'ambiance dégradée si nécessaire,
- Une même procédure est appliquée quel que soit le classement contrôle-commande des équipements concernés (E1A, E1B ou E2). En revanche, la procédure varie selon d'autres critères, en particulier le classement sismique,
- La qualification est de préférence réalisée par essais.

La qualification matérielle est réalisée :

- Sur une configuration matérielle réelle ou, si la taille en est déraisonnable (ce qui est généralement le cas pour les architectures distribuées), sur une configuration matérielle représentative,
- Avec des logiciels d'application réels ou d'animation.

Lorsque l'équipement à qualifier appartient à une plate-forme de contrôle-commande, la qualification matérielle est réalisée sur une configuration matérielle représentative de l'usage qui sera fait de cette plate-forme sur les différents systèmes de contrôle-commande classés de sûreté. Un logiciel d'animation est alors utilisé, il doit permettre de s'assurer que l'équipement continue à remplir son service y compris s'il est soumis aux conditions limites d'environnement et après vieillissement.

Les qualifications pré-existantes sont utilisées autant que possible.

Nota : Lorsque le fournisseur de l'équipement annonce ne pas respecter certaines exigences, les essais de qualification sont réalisés de façon à vérifier que les performances garanties par le constructeur sont tenues ; si ces valeurs sont jugées acceptables, une dérogation peut permettre de prononcer la qualification.

6. QUALIFICATION FONCTIONNELLE D'UN ÉQUIPEMENT DE CONTRÔLE-COMMANDE

Les procédures de qualification fonctionnelle d'un équipement de contrôle-commande diffèrent selon qu'il s'agit :

- d'équipements conventionnels,
- de composants électriques programmés,
- d'équipements programmés.

6.1. ÉQUIPEMENTS CONVENTIONNELS

Les équipements de contrôle-commande sont dits « conventionnels » lorsqu'ils ne contiennent pas de logiciel.

La complexité des fonctions qui peuvent être implantées au sein des équipements conventionnels est suffisamment limitée pour qu'il soit possible de réaliser la recette ou validation des fonctionnalités attendues de l'équipement sur le palier EPR par des essais « boîte noire » au niveau du système de contrôle-commande complètement intégré.

Les essais de recette ou de validation sont typiquement réalisés hors site mais sur l'équipement destiné au site. Le système est apte à l'installation sur site une fois ces essais réussis.

La recette ou validation hors site est complétée par les essais de mise en service sur site.

6.2. COMPOSANTS ÉLECTRIQUES PROGRAMMÉS

Un composant électrique programmé (CEP) est un élément constitutif électrique qui intègre un ou plusieurs composants ou modules électroniques embarquant du logiciel (cf. RCC-E E 1400 **Réf [1]**).

Le RCC-E C 5333 **Réf [1]** indique que les CEP ont les caractéristiques suivantes :

- Contenir de l'électronique programmée,
- Assurer une fonction principale dédiée et définie à sa conception,
- Être un composant fonctionnellement autonome,
- Être paramétrable mais non programmable par l'utilisateur.

Par exemple, les relais, les capteurs, les enregistreurs, les régulateurs, les positionneurs, les actionneurs, les cellules électriques sont des CEP lorsqu'ils ont les caractéristiques énumérées ci-dessus.

Pour un CEP, il est reconnu que la qualification fonctionnelle par essais « boîte noire » n'est pas suffisante c'est pourquoi une qualification fonctionnelle renforcée (cf. RCC-E C 5333-4) vient s'y ajouter. Une gradation d'exigences est établie selon le classement contrôle-commande visé (voir **§ 6.3.**), certaines exigences étant à définir au cas par cas.

La qualification fonctionnelle renforcée analyse la conception, le processus de développement et de modification ainsi que le retour d'expérience du CEP. Cette analyse peut amener à réaliser des tests complémentaires sur le CEP lorsque les tests déjà conduits par le concepteur se révèlent insuffisants. Les évaluations pré-existantes sont utilisées autant que possible.

La qualification fonctionnelle renforcée se matérialise par la constitution d'un Dossier de Qualification Fonctionnelle Renforcée (DQFR).

6.3. ÉQUIPEMENTS PROGRAMMÉS

Un système de contrôle-commande qui contient du logiciel et qui ne possède pas les caractéristiques d'un CEP est un système programmé.

Le RCC-E **Réf [1]** C 5000 définit les exigences applicables aux systèmes programmés avec une gradation selon le classement contrôle-commande visé. Le RCC-E s'appuie notamment sur les exigences du chapitre 6 de la norme CEI 61513 **Réf [3]**.

La correspondance entre le classement contrôle-commande du palier EPR et les classes génériques des matériels de contrôle-commande du RCC-E et normes CEI est définie dans les données de projet EPR **Réf [2]**. Elle s'établit comme suit :

- E1A à Classe 1 (C1),
- E1B à Classe 2 (C2),
- E2 à Classe 3 (C3).

Concernant plus particulièrement les logiciels, le RCC-E s'appuie notamment sur les exigences graduées définies dans les normes CEI suivantes :

- CEI 60880 **Réf [4]**- Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A (classement fonctionnel F1A sur EPR – classement contrôle-commande E1A),

- CEI 62138 Réf [5] chapitre 6 - Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B (classement fonctionnel F1B sur EPR – classement contrôle-commande E1B),
- CEI 62138 Réf [5] chapitre 5 - Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie C (classement fonctionnel F2 sur EPR – classement contrôle-commande E2).

La RFS numéro II.4.1.a Réf [6], dite RFS logiciels et relative aux logiciels des systèmes électriques classés de sûreté, fait partie du référentiel para réglementaire applicable au palier EPR. Elle est considérée comme applicable moyennant les transpositions de classement 1E/F1A et classé de sûreté non 1E/F1B (voir Chap1.7). Le RCC-E décline en terme de règles opérationnelles les principes de la RFS logiciels.

Les systèmes programmés de contrôle-commande sont aujourd'hui presque exclusivement construits à partir de plate-formes de contrôle-commande pré-existantes, c'est donc ce cas qui sera considéré en priorité.

Si le système n'a pas été développé conformément aux codes et normes susmentionnés ou suivant des exigences comparables, la démonstration nécessite une analyse à posteriori des logiciels, de la façon dont ils ont été développés et de leur retour d'expérience. Les écarts constatés entre les exigences et les dispositions prises par le concepteur sont analysés au cas par cas.

Les différentes caractéristiques des systèmes, logiciels et outils sont distinguées comme indiqué sur la figure FIG–7.2.3.2. Ces caractéristiques sont appréciées et évaluées pour assurer qu'elles sont conformes aux spécifications du système de contrôle-commande à qualifier ainsi qu'aux codes et normes applicables.

6.3.1. CARACTÉRISTIQUES DES COMPOSANTS ET CONFIGURATIONS ENVISAGÉES

Les caractéristiques de la plate-forme sont analysées, autant que possible sur la base des évaluations pré-existantes, pour déterminer si les composants et les configurations autorisées couvrent les caractéristiques attendues du système de contrôle-commande à qualifier. Le niveau d'appréciation dépend du classement contrôle-commande de l'équipement.

Sont appréciées et évaluées :

- Les fonctionnalités afin de démontrer que l'équipement est capable de remplir les fonctions d'application désirées,
- Les caractéristiques de performance liées à la vitesse et à la précision avec lesquelles l'équipement exécute les fonctions d'application. Les performances peuvent être évaluées en même temps que les fonctionnalités puisqu'une évaluation indépendante est dans de nombreux cas impossible,
- La fiabilité de l'équipement. Ceci dépend de :
    - La fiabilité du matériel qui peut être calculée sur la base des données relatives à la fiabilité des composants et de l'architecture du système de contrôle-commande à qualifier,
    - Le niveau de sûreté du logiciel pouvant être évaluée par une analyse qualitative du processus de développement afin de démontrer un niveau suffisant de confiance dans le logiciel (voir § 6.3.2. et § 6.3.4.).

6.3.2. CARACTÉRISTIQUES DU LOGICIEL SYSTÈME

L'évaluation de la confiance dans le logiciel système est particulièrement importante pour l'appréciation du niveau de sûreté atteignable pour les fonctions d'application désirées.

Le logiciel système doit être cohérent par rapport au niveau de sûreté estimé sur la base de la fiabilité matérielle du système.

L'analyse de la confiance dans le logiciel système est fortement liée au processus de développement.

Le développement suit des exigences par étapes. Ces exigences concernent par exemple :

- La conception architecturale matérielle et logicielle,
- Le processus de développement,
- Le processus de vérification et de validation,
- L'utilisation appropriée des composants du marché fournis par d'autres fabricants (processeurs fabriqués par Intel, Motorola,...),
- Des tests de validation complémentaires.

L'appréciation et l'évaluation de la confiance est basée sur une analyse de la documentation de développement. Cette analyse, graduée selon le classement visé, vérifie la conformité aux codes et normes applicables (voir **§ 6.3.**).

Les systèmes de contrôle-commande construits à partir de plate-formes de contrôle-commande représentent les cas les plus complets et les plus courants. Ainsi, cette évaluation est réalisée en analysant la documentation de la plate-forme. Les évaluations pré-existantes sont utilisées autant que possible pour l'appréciation de la confiance que l'on peut avoir dans le logiciel système.

6.3.3. CARACTÉRISTIQUES DES OUTILS

L'appréciation et l'évaluation des outils dépendent :

- De la tâche supportée par l'outil (transformation de code source en code exécutable, vérification et validation du logiciel d'application, service, configuration matérielle …),
- Des conséquences des erreurs éventuelles introduites par l'outil,
- Des possibilités de détecter les erreurs éventuelles introduites par l'outil lors des vérifications.

Une appréciation et une évaluation de ces outils sont nécessaires si toutes les conditions ci-dessous sont vraies :

- La sortie outil peut directement introduire une erreur dans le code exécutable,
- Un processus et des méthodes de développement alternatifs n'existent pas pour atténuer les conséquences d'erreurs introduites par l'outil,
- La sortie outil n'est pas systématiquement vérifiée.

L'appréciation et l'évaluation, graduées selon le classement visé, vérifient la conformité aux exigences des codes et normes (voir **§ 6.3.**) applicables aux outils. Elles considèrent en particulier l'expérience opérationnelle de l'outil en conditions d'utilisations similaires. Les évaluations pré-existantes sont utilisées autant que possible pour l'appréciation de la confiance que l'on peut avoir dans les outils.

6.3.4. CARACTÉRISTIQUES DU LOGICIEL D'APPLICATION

L'appréciation et l'évaluation de la confiance que procure le logiciel d'application s'assure :

- Que le logiciel d'application est développé par étapes prédéfinies,
- Que les étapes de vérification et de validation sont intégrées au processus de développement du logiciel d'application.

L'appréciation et l'évaluation sont graduées selon le classement visé et vérifient la conformité aux codes et normes applicables (voir **§ 6.3.**).

Habituellement, le logiciel d'application est spécifié et développé à partir de diagrammes fonctionnels. Le code exécutable est généré automatiquement à partir de ces diagrammes. L'ensemble du processus de développement est sous-tendu par les outils associés à la plate-forme de contrôle-commande.

A partir du diagramme fonctionnel, la spécification du logiciel d'application est réalisée sur la base de bibliothèques de blocs fonctionnels réutilisables (ces bibliothèques font partie du logiciel système et sont appréciées et évaluées avec lui). La représentation de cette spécification dans la base de données du logiciel d'application constitue le point de départ de la génération automatique du code applicatif du système programmé. Cette manière de mettre en oeuvre le logiciel d'application facilite l'évaluation de la confiance puisque la spécification du logiciel d'application peut être vérifiée par les ingénieurs procédés. Elle est recommandée pour toutes les classes de système de contrôle-commande.

6.3.5. CARACTÉRISTIQUES DES MATÉRIELS ET LOGICIELS SYSTÈMES INTÉGRÉS ET CONFIGURÉS

Certaines caractéristiques du système de contrôle commande dépendent également des configurations, du fonctionnement et des procédures de maintenance spécifiques au palier EPR.

La conformité de ces configurations spécifiques avec les spécifications du système ainsi qu'avec les codes et normes applicables (voir **§ 6.3.**) complétés des données de projet du palier EPR **Réf [2]** est appréciée et évaluée.

6.3.6. CARACTÉRISTIQUES DU SYSTÈME COMPLET

Avant la mise en service sur site, l'ensemble du logiciel (système et application) est intégré dans les équipements.

Le code exécutable du logiciel (système et application) est validé sur les équipements destinés au site ou sur une plateforme représentative. Ces activités sont typiquement réalisées sur des installations d'essais hors site.

L'appréciation et l'évaluation démontrent que la recette ou validation est réalisée et documentée conformément au plan de validation du système de contrôle-commande. Le système est alors apte à l'installation sur site.

La recette ou validation hors site est complétée par les essais de mise en service sur site.

LISTE DES RÉFÉRENCES

[1] Règles de Conception et de Construction des matériels Électriques (RCC-E), édition de décembre 2005

[2] ENSEMD050222 – Cahier de données de projet complétant les exigences du RCC-E décembre 2005 pour EPR

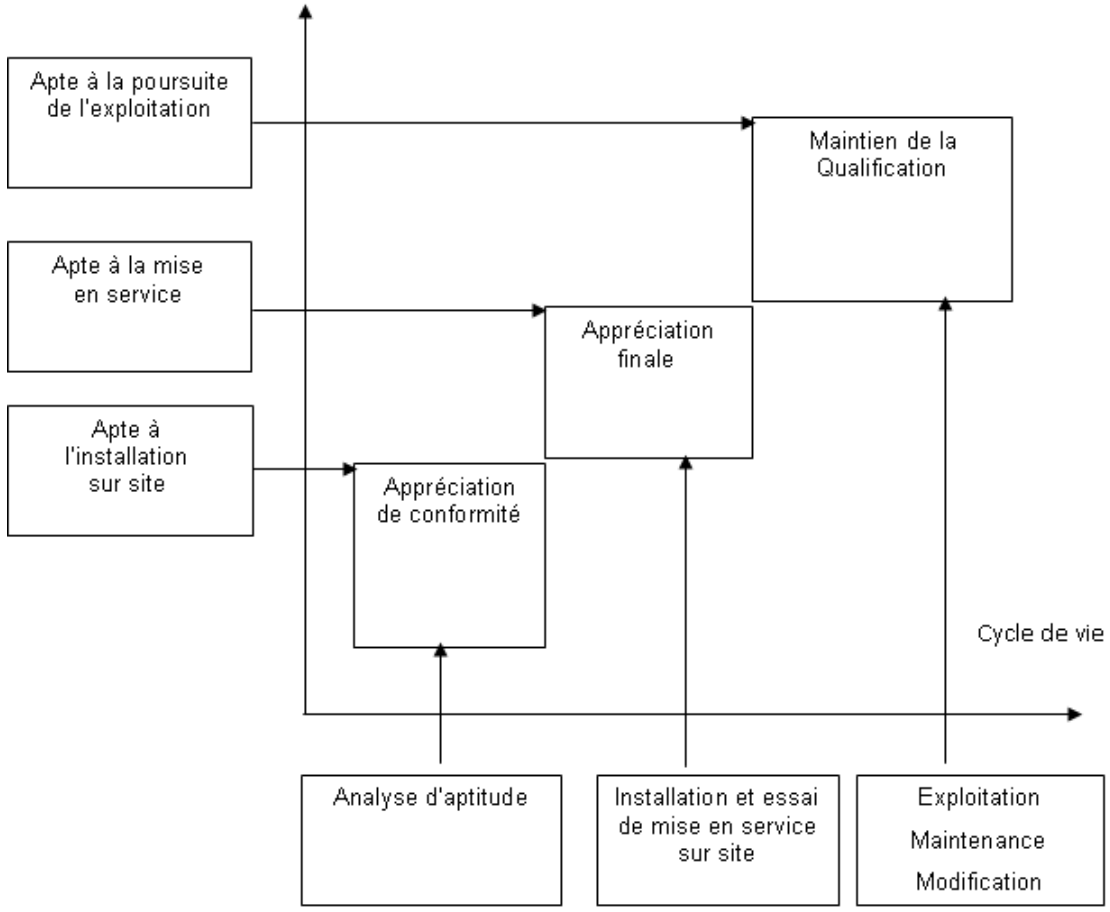
[3] Norme CEI 61513 : 2001 - Centrales nucléaires – Instrumentation et contrôle-commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes - exigences du chapitre 6

[4] Norme CEI 60880 : 2006 - Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A

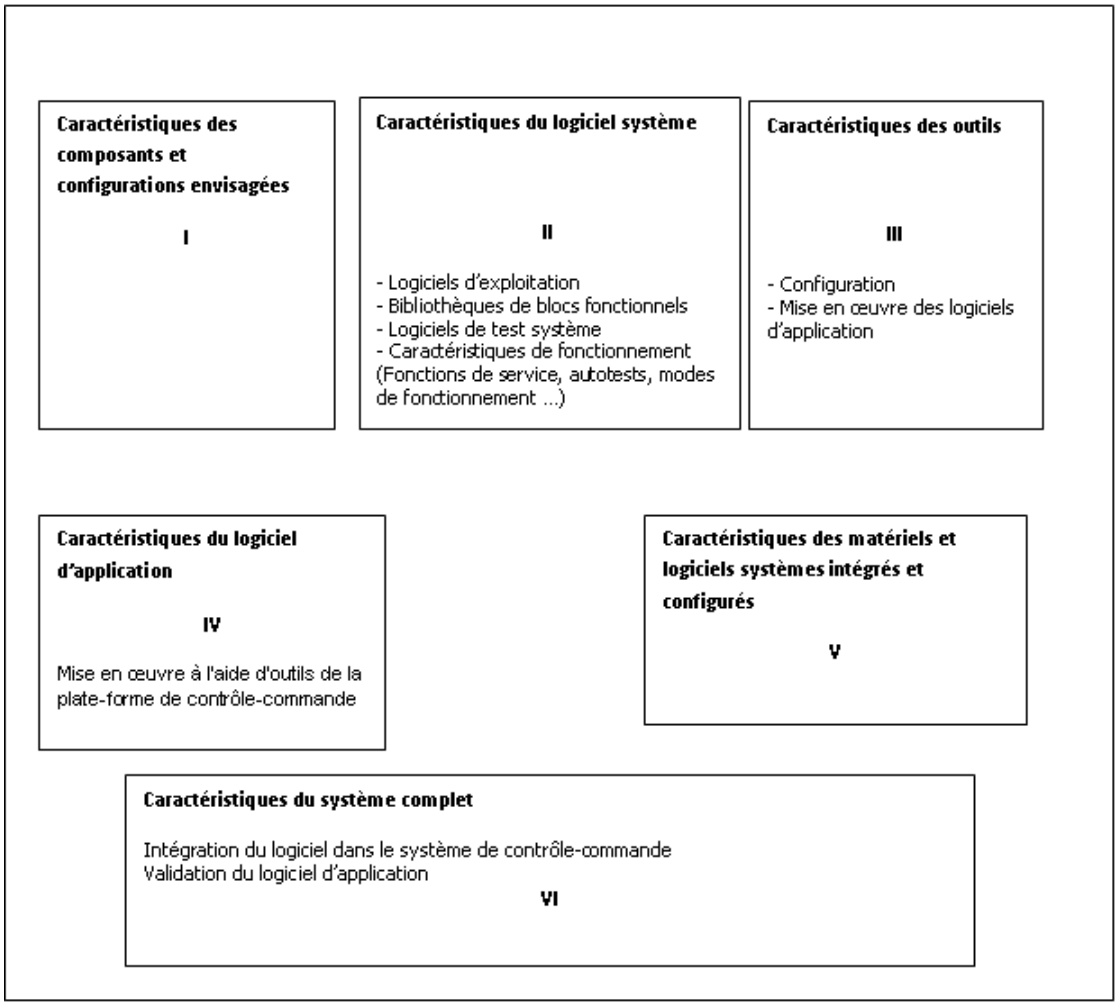
[5] Norme CEI 62138 : 2004 - Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B (chapitre 6) ou C (chapitre 5)

[6] Règle Fondamentale de Sûreté (RFS) II.4.1.a relative aux logiciels des systèmes électriques classés de sûreté, dite RFS logiciels

FIG–7.2.3.1 QUALIFICATION ET CYCLE DE VIE DES ÉQUIPEMENTS DE CC



FIG–7.2.3.2 APPRÉCIATION DE CONFORMITÉ



7.3 LES SYSTÈMES DE CONTRÔLE COMMANDE CLASSÉS F1

SOMMAIRE

TABLEAUX :

FIGURES :

.7.3.1 ARCHITECTURE DU SYSTÈME DE PROTECTION (PS)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

Le système de protection, dans son ensemble, doit contribuer aux fonctions de sûreté suivantes :

- contrôle de la réactivité,
- évacuation de la puissance résiduelle,
- confinement des substances radioactives.

Le système de protection (PS) a pour rôle de mettre en œuvre les fonctions automatiques, les actions [] ainsi que les fonctions de surveillance nécessaires pour atteindre l'état contrôlé en cas d'évènements PCC-2, 3 ou 4.

Le système de protection doit également mettre en œuvre certaines fonctions nécessaires après l'atteinte de l'état contrôlé, pour amener le réacteur dans un état d'arrêt sûr après des évènements PCC-2, 3 ou 4.

Il doit enfin mettre en œuvre certaines fonctions requises pour l'atteinte de l'état final (RRC-A).

Le système de protection doit être capable de gérer les échanges de données avec les autres systèmes de contrôle commande (PIPS, RPI, RPN, RIC, BCMS, PAS, SAS, RCSL, HKS, RMAD, KRT, contrôle-commande CCAG, contrôle-commande GPA, contrôle-commande diesel, contrôle-commande turbine, MCP, MCS, PSIS).

0.2. CRITÈRES FONCTIONNELS

Le système de protection est un système essentiel pour satisfaire la démonstration de sûreté des analyses d'accidents.

0.2.1. Contrôle de la réactivité

Le système de protection doit permettre le contrôle de la réactivité en contrôlant les principaux paramètres du réacteur et en activant les fonctions importantes pour la sûreté suivantes :

- arrêt automatique du réacteur (chute des grappes),
- démarrage de l'injection d'eau borée par le RBS,
- isolement du RCV afin de prévenir les dilutions,
- isolement des lignes ARE afin d'éviter un sur-refroidissement en cas d'événement conduisant à un déséquilibre entre la puissance produite par le cœur et la puissance extraite aux GV,
- isolement des lignes VVP afin de limiter le pic de criticité en cas d'événement conduisant à une augmentation excessive du débit de vapeur.

Ces actions doivent permettre au réacteur d'atteindre la sous criticité requise dans les états contrôlés pour les conditions d'accident PCC-2 à 4. Pour les évènements RRC-A, le système de protection doit accomplir certaines fonctions de sûreté requises à court terme dans la définition de l'accident.

0.2.2. Évacuation de la puissance résiduelle

Le système de protection doit permettre l'évacuation de la puissance du cœur en contrôlant les principaux paramètres du réacteur et en activant les fonctions importantes pour la sûreté suivantes :

- démarrage de l'injection de sécurité,
- évacuation de la puissance par le circuit secondaire,
- démarrage de l'alimentation du secondaire des générateurs de vapeur par l'ASG.

Ces actions doivent permettre de respecter les critères de sûreté pour les événements PCC-2 à 4. Pour les évènements RRC-A, le PS doit accomplir certaines fonctions de sûreté à court terme requises dans la définition de l'accident.

0.2.3. Confinement des substances radioactives

Le système de protection doit permettre le confinement des substances radioactives en contrôlant les principaux paramètres du réacteur et en activant les fonctions importantes pour la sûreté suivantes :

- isolement de l'enceinte,
- isolement du circuit primaire principal et des lignes vapeurs VVP,
- relèvement du point de consigne pour l'isolement des lignes VDA,
- protection contre les surpressions primaires et secondaires.

Ces actions doivent permettre de conserver des marges suffisantes vis-à-vis des limites acceptables de rejets radiologiques suite à n'importe quel événement pour lequel l'intégrité du circuit primaire principal n'est pas garantie.

Le système de protection doit permettre de détecter les situations accidentelles susceptibles de mettre en péril l'intégrité des circuits primaire et secondaire. Dans la plupart des cas, l'arrêt automatique du réacteur, associé à des dispositifs de sauvegarde agissant par limitation directe ou indirecte de la pression permet de garantir cette intégrité. S'il y a un risque de rupture fragile de la cuve, le système de protection doit limiter l'accroissement de pression dans le circuit primaire.

0.3. EXIGENCES DE CONCEPTION

0.3.1. Exigences résultant du classement sûreté

0.3.1.1. Classement sûreté

Le système de protection doit être classé conformément aux principes de classement présentés au sous-chapitre 3.2.

0.3.1.2. Critère de défaillance unique (active et passive)

La défaillance unique, qu'elle soit active ou passive après 24h, doit s'appliquer aux équipements du système de protection assurant des fonctions F1.

En conséquence, le système de protection doit être constitué de trains redondants susceptibles d'assurer les fonctions de sûreté malgré la perte d'un train. Les trains de protection redondants doivent être localisés dans des divisions séparées de manière à prévenir une défaillance de cause commune en cas d'agression interne ou externe affectant une division.

Le découplage électrique doit être assuré entre les trains redondants.

Les fonctions support doivent être autant que possible indépendantes. Chaque train redondant est alimenté électriquement par sa propre source secourue.

Le système de protection doit assurer ses fonctions malgré l'application du critère de défaillance unique cumulé à la maintenance préventive ou aux tests périodiques.

Les cas de cumuls de défaillance unique, de maintenance préventive, d'essais périodiques et d'agression interne ou externe, pour lesquels les fonctions de sûreté du système de protection doivent être assurées, sont définis selon le chapitre 3.

0.3.1.3. Alimentations électriques secourues

Comme pour les autres systèmes de sûreté, l'alimentation électrique des équipements redondants du système de protection doit être secourue par diesels, de façon à ce que leur fonction de sûreté soit assurée même en cas de perte de tension réseau.

De plus, le système de protection doit être alimenté par une alimentation électrique de tension adéquate et non interruptible afin de garantir la continuité des fonctions de sûreté en cas de perte de tension réseau.

0.3.1.4. Qualification aux conditions de fonctionnement

Les équipements assurant les fonctions de sûreté du PS doivent être qualifiés aux conditions d'ambiance pour lesquelles leur fonctionnement est requis.

La qualification est faite selon les règles présentées au sous-chapitre 3.7.

0.3.1.5. Classement des équipements mécaniques, électriques et de contrôle-commande

Le classement mécanique n'est pas applicable au système de protection.

Les équipements électriques et de contrôle commande doivent être classés conformément aux principes de classement présentés au sous-chapitre 3.2.

0.3.1.6. Classement sismique

Le système de protection doit être classé conformément aux principes de classement présentés au sous-chapitre 3.2.

Le PS est classé SC1 pour le classement sismique. Le dimensionnement est défini de manière à garantir que les fonctions de sûreté des systèmes et composants nécessaires à l'atteinte d'un état d'arrêt sûr ne sont pas affectées par un séisme de dimensionnement.

0.3.2. Autres exigences réglementaires

0.3.2.1. Textes officiels

Le système de protection du réacteur est concerné par les textes officiels suivants :

- le décret 2007-534 du 10/04/2007 autorisant la création de l'installation nucléaire de base dénommée Flamanville 3, comportant un réacteur nucléaire de type EPR, sur le site de Flamanville (Manche) :
  - Art. 2, Section III-1.1.3 : « En cas d'évolution anormale des paramètres physiques liés à la réactivité, des dispositifs automatiques permettent l'arrêt du réacteur, notamment en cas de dépassement significatif de la puissance thermique maximale de fonctionnement du réacteur. »,
  - Art. 2, Section III-2.1.3.a : « Des dispositifs automatiques provoquent l'arrêt du réacteur en cas d'évolution anormale des paramètres physiques relatifs à l'inventaire en eau ou à l'efficacité du refroidissement du cœur. »,
- le document général «Options de Sûreté du projet de réacteur EPR» (lettre DGSNR/SD2/0729/2004) est applicable au système de protection.

0.3.2.2. Règles fondamentales de sûreté

L'application des RFS est présentée au sous-chapitre 1.7.

Les Règles fondamentales de sûreté suivantes sont applicables au système de protection de l'EPR.

- II.4.1.a "Logiciel des systèmes électriques classés de sûreté"
- IV.2.b "Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté".

0.3.2.3. Directives techniques

En plus des exigences générales indiquées au chapitre A.1 "approche générale de la sûreté", les exigences applicables au PS sont présentées aux sections A.2.2, B.2.2.2, B.2.3.1, B.2.3.2 et G3 des Directives Techniques (voir les sections extraites ci-dessous de la section 1.7.0).

- A.2.2 - redondance et diversité dans les systèmes de sûreté :
  « Pour les événements qui ne sont pas maîtrisés par les systèmes d'exploitation et/ou par les fonctions de limitation, des systèmes de protection et sauvegarde sont nécessaires pour ramener et maintenir le réacteur dans un état sûr en termes de sous-criticité, de refroidissement du cœur et de confinement des substances radioactives. La fiabilité de ces systèmes doit être cohérente avec l'objectif général de réduction des fréquences d'occurrence des accidents, en tenant compte des fréquences estimées des événements initiateurs et des durées des actions correspondantes de ces systèmes. » ;
  « Cette fiabilité doit être obtenue par une combinaison adéquate de redondance et de diversification. Une attention adéquate doit être portée au fait que les possibilités de défaillances de mode commun limitent les possibilités de réduction des indisponibilités en ajoutant des trains identiques (sur ce point, il est souligné qu'il n'est probablement pas possible de démontrer que l'indisponibilité d'un système de sûreté redondant constitué de trains identiques est inférieure à 10-4 par demande), et au fait que la diversification peut conduire à des systèmes plus complexes et à des difficultés de maintenance ; de plus, une attention appropriée doit être portée aux systèmes supports lors de l'évaluation des bénéfices liés à la mise en place d'équipements et de systèmes diversifiés. » ;
  « Une attention particulière doit être portée à la réduction des possibilités de défaillances de cause commune. Séparation physique et séparation géographique doivent être mises en œuvre autant qu'il est possible. Les fonctions de support (énergie, contrôle, refroidissement, etc.) doivent aussi être le plus possible indépendantes. Un accent tout particulier doit être mis sur la redondance et la diversification des sources électriques. De plus, des dispositions (incluant une diversification matérielle et logicielle) doivent être mises en œuvre au niveau de l'architecture générale du contrôle-commande pour limiter les défaillance de cause commune d'origine logicielle. ».
- B.2.2.2 - systèmes de sûreté informatisés :
  « Pour obtenir la haute fiabilité nécessaire pour les systèmes de contrôle-commande, le concepteur doit, lorsque des systèmes informatisés sont utilisés, mettre en place des exigences de sûreté spécifiques, pour la qualification de tels systèmes informatisés pour chaque classe de sûreté, y compris des règles de conception pour les logiciels. » ;
  « Les trois principes principaux pour la conception de calculateurs pour des systèmes de sûreté sont l'évitement de défauts, l'élimination des défauts et la tolérance aux défauts. » ;
  « L'évitement des défauts peut être mis en œuvre dans une approche de construction par des règles et directives strictes applicables durant tout le cycle de vie d'un système, incluant la spécification du système (matériels, logiciels et intégration), la production (conception, codage des logiciels et mise en place des matériels, essais), l'exploitation et la maintenance » ;
  « L'évitement des défauts doit être complété par une approche analytique pour l'élimination des défauts. Ceci inclut des procédures non formelles comme des inspections, des relectures, des audits, des revues de même que des procédures formelles comme des preuves d'exactitude, des analyses statiques et différents essais d'intégration. » ;
  « Pour faire face aux défauts résiduels qui subsisteraient en dépit de toutes les mesures prises pour l'évitement et l'élimination des défauts, la tolérance aux défauts doit être introduite dans la

conception. Pour les matériels, ceci peut être atteint par la redondance et la diversification. La diversification doit être examinée pour obtenir la tolérance aux défauts des logiciels. ».

- B.2.3.1 - fonction de contrôle de la réactivité :
« En tout état de cause, la fiabilité de la fonction d'arrêt d'urgence doit être suffisamment élevée pour contribuer à « pratiquement éliminer » les séquences de fusion du cœur à haute pression. Nonobstant le rôle du système de boration supplémentaire, des moyens adéquats doivent être mis en œuvre dans cet objectif, tels qu'une diversification des composants principaux du système d'arrêt d'urgence (mesures physiques, signaux et traitements associés, disjoncteurs d'arrêt d'urgence). ».
- B.2.3.2 - fonction d'évacuation de la puissance résiduelle :
« De plus, les caractéristiques de conception de la mesure de niveau d'eau dans les boucles nécessitent une attention particulière ; des moyens diversifiés devraient être mis en place. ».
- G3 - conception des dispositifs de contrôle-commande :
« En principe, la démonstration de sûreté devrait être faite en considérant les moyens utilisés normalement par les opérateurs dans la salle de commande principale. Cependant, la mise en place dans la salle de commande principale d'une interface homme-machine conventionnelle classée F1B pour pouvoir réaliser la démonstration de sûreté avec des équipements classés F1 alors que les opérateurs utiliseraient une interface homme-machine informatisée classée F2, pourrait être acceptée pour autant que :

  a) le matériel et l'architecture de l'interface homme-machine informatisée satisfassent aux exigences applicables aux systèmes F1B,

  b) le logiciel correspondant satisfasse à des exigences de qualification détaillées à proposer par le concepteur,

  c) les moyens mis en œuvre pour la détection et la signalisation des défaillances de fonctions et d'équipements F2 essentiels de l'interface homme-machine informatisée satisfassent aux exigences applicables aux fonctions et équipements F1B. ».

0.3.2.4. Normes applicables

Les normes suivantes essentielles au développement et à la conception des systèmes de contrôle commande F1A sont applicables au système de protection :

- IEC 60880 : *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*
- IEC61513 : *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*
- IEC61226 : *Centrales nucléaires de puissance - Instrumentation et contrôle-commande importants pour la sûreté – Classification des fonctions d'instrumentation et de contrôle-commande*

La norme suivante essentielle au développement et à la conception des systèmes de contrôle-commande F1b et F2 est applicable au système de protection :

- EC62138 : *Centrales nucléaires – Instrumentation et contrôle- commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

0.3.2.5. Règles de conception électrique

Les règles de conception pour les équipements électriques ainsi que les règles spécifiques à appliquer à l'ensemble contrôle-commande sont fournies dans le RCC-E complété des données de projet du réacteur EPR définies dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.3.3. Agressions internes et externes

0.3.3.1. Agressions internes

Le système de protection doit être protégé contre les agressions internes, conformément aux éléments présentés dans le sous-chapitre 3.4.

0.3.3.2. Agressions externes

Le PS doit être protégé contre les agressions externes, conformément aux éléments présentés dans le sous-chapitre 3.3.

0.3.4. ESSAIS

0.3.4.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du système de protection.

0.3.4.2. Surveillance en exploitation

Sans objet.

0.3.4.3. Essais périodiques

Le système de protection doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitres IX des Règles Générales d'Exploitation.

1. MISSIONS

Le système de protection met en œuvre les fonctions automatiques, [] et de surveillances classées F1A. Il met en œuvre également certaines des fonctions F1B, ainsi que certaines fonctions F2 spécifiques au PS.

Les fonctions F1A sont utilisées après un événement initiateur (PCC-2, 3, 4) pour atteindre l'état contrôlé. Ce sont principalement :

- Le déclenchement automatique de l'arrêt automatique du réacteur,
- La commande automatique des systèmes de sauvegarde et des systèmes auxiliaires associés,
- La génération de signaux en cas de détection de situations exigeant une action [],
- Le déclenchement des fonctions de contrôle commande [] F1A.

2. FONCTIONS SUPPORTÉES

2.1. FONCTIONS D'ARRÊT AUTOMATIQUE DU RÉACTEUR ET DE LA TURBINE

Les fonctions suivantes sont classées F1A :

- AAR sur puissance linéique élevée,
- AAR sur bas RFTC,
- AAR sur qualité élevée,
- AAR sur augmentation rapide du flux neutronique,
- AAR sur niveau de puissance thermique cœur élevé,
- AAR sur basse vitesse GMPP,

- AAR sur très bas débit boucle,
- AAR sur bas débit boucle,
- AAR sur haut flux neutronique (Niveau intermédiaire),
- AAR sur bas temps de doublement (Niveau intermédiaire),
- AAR sur puissance linéique élevée vis-à-vis de l'Interaction Pastille Gaine,
- AAR sur Faible marge à la saturation,
- AAR sur Nombre élevé de collectrons invalides,
- AAR sur pression pressuriseur (GE) < MIN2p,
- AAR sur pression pressuriseur (GE) > MAX2p,
- AAR sur niveau pressuriseur (GE) > MAX1p,
- AAR sur pression branche chaude (GL) < MIN1p,
- AAR sur chute de pression GV > MAX1p,
- AAR sur chute de pression GV > MAX0p,
- AAR sur pression GV < MIN1p,
- AAR sur pression GV > MAX1p,
- AAR sur niveau GV (GE) < MIN1p,
- AAR sur niveau GV (GE) > MAX1p,
- AAR sur pression enceinte > MAX1p,
- AAR [](via PIPO),
- AAR sur signal d'injection de sûreté,
- AAR sur signal de démarrage ASG (1GV),
- Arrêt turbine sur compte rendu d'AAR.

La fonction suivante est non classée :

- AAR sur secondaire indisponible.

2.2. FONCTIONS DE SAUVEGARDE

Ces fonctions sont nécessaires pour l'atteinte de l'état contrôlé en complément de l'AAR (mise en service de systèmes de sauvegarde, isolement de systèmes,...).

Les fonctions suivantes sont classées F1A :

- démarrage IS :
  - sur pression pressuriseur < MIN3p,
  - sur delta Pression de saturation < MIN1p,
  - sur niveau de circuit primaire < MIN1p,
  - sur niveau de circuit primaire < MIN3p.
- injection par les accumulateurs sur pression branche chaude > MAX4p et signal IS,
- isolement du circuit primaire principal sur signal d'IS,
- refroidissement de l'IRWST sur signal d'IS,
- arrêt GMPP :

- sur delta P GMPP < MIN1p et signal IS,
- sur niveau GV (GL) < MIN 3p,
- sur haute pression enceinte anticipé et (signal chute Pression VVP > MAX1p ou signal pression GV < MIN1p).
- sur signal d'isolement enceinte phase 2.

- démarrage RBS :
  - sur pression GV < MIN5p,
  - sur pression pressuriseur < MIN4p,
  - sur commande [],
  - sur signal d'anti-dilution (en condition d'arrêt standard ou en puissance) et signal d'AAR.
- isolement RBS :
  - sur niveau pressuriseur > MAX1p,
  - sur niveau GV (GE) > MAX3p.
- isolement de l'aspiration d'un train RIS/RA en mode RA : :
  - sur niveau compartiment BR < MIN1p + commande groupée « manutention combustible »,
  - sur niveau puisard BAS > MAX1p,
  - sur augmentation pression BAS > MAX1p.
- isolement de la décharge RCV basse pression :
  - sur signal IS,
  - sur température BC (GL) > MAX1p ou température BF (GL) > MAX2p et un train RRA connecté,
  - sur signal d'anti-dilution en condition GMPP arrêtées.
- arrêt d'un train RIS/RA en mode RA :
  - sur delta pression saturation < MIN2p,
  - sur niveau circuit primaire < MIN2p.
- ouverture VDA pour refroidissement partiel :
  - sur signal IS,
  - sur niveau GV (GE) > MAX2p.
- ouverture VDA sur pression GV > MAX1p,
- isolement VDA sur pression GV < MIN3p,
- augmentation du point de consigne VDA sur niveau GV (GE) > MAX2p, refroidissement partiel terminé,
- démarrage ASG :
  - sur niveau GV (GL) < MIN2p,
  - sur signal perte alimentation externe et signal IS.
- isolement ASG :
  - sur niveau GV (GL) > MAX1p,

  - sur commande [].

- fermeture vanne isolement vapeur :
  - sur chute de pression GV > MAX1p,
  - sur pression GV < MIN1p,
  - sur niveau GV (GE) > MAX2p, refroidissement partiel terminé,
  - sur pression enceinte > MAX4p.
- isolement ARE grand débit :
  - sur signal d'AAR,
  - sur niveau GV (GE) > MAX1p,
  - sur chute de pression GV > MAX2p,
  - sur pression GV < MIN2p,
  - sur pression enceinte > MAX3p,
  - sur signal d'anti-dilution (en condition d'arrêt standard ou en puissance) et signal d'AAR.
- isolement ARE petit débit :
  - sur niveau GV (GE) > MAX0p et signal AAR,
  - sur chute de pression GV > MAX2p,
  - sur pression GV < MIN2p,
  - sur pression enceinte > MAX3p,
  - sur signal d'anti-dilution (en condition d'arrêt standard ou en puissance) et signal d'AAR.
- isolement ARE :
  - sur chute de pression GV > MAX2p,
  - sur pression GV < MIN2p,
  - sur pression enceinte > MAX3p,
  - sur niveau GV (GE) > MAX0p et signal AAR,
  - sur signal d'anti-dilution (en condition d'arrêt standard ou en puissance) et signal d'AAR.
- isolement enceinte phase 1 :
  - sur pression enceinte > MAX1p,
  - sur signal IS.
  - sur signal d'isolement enceinte phase 2.
- isolement enceinte phase 2 sur pression enceinte > MAX2p,
- ouverture soupapes sécurité pressuriseur pour la protection contre les ruptures fragiles cuve :
  - sur signal pression branche chaude (GL) > MAX1p,
  - sur signal pression branche chaude (GL) > MAX2p,
  - sur signal pression branche chaude (GL) > MAX3p.
- arrêt ligne de charge RCV :
  - sur niveau pressuriseur > MAX1p,
  - sur chute de pression GV > MAX2p,

  - sur signal IS,
  - sur pression branche chaude (GL) > MAX0p,
  - sur niveau GV (GE) > MAX2p, refroidissement partiel terminé.

- isolement de l'injection aux joints GMPP :
  - sur niveau pressuriseur > MAX2p,
  - sur pression branche chaude (GL) > MAX0p,
  - sur niveau GV (GE) > MAX2p, refroidissement partiel terminé.

- isolement de la décharge RCV haute pression :
  - sur température aval échangeur HP > MAX1p,
  - sur niveau pressuriseur < MIN1p et signal d'AAR,
  - sur signal d'anti-dilution (en condition d'arrêt standard ou en puissance ou GMPP arrêtées) et niveau pressuriseur < MIN PAD,
  - sur signal IS.

- isolement du ballon RCV et de la station d'hydrogénation sur signal d'anti-dilution (en condition d'arrêt standard ou en puissance ou GMPP arrêtées),
- isolement de la purge :
  - sur niveau GV (GL) < MIN2p,
  - sur niveau GV (GE) < MIN1p,
  - sur signal IS + signal perte alimentation électrique externe.

- anti-dilution à l'arrêt, GMPP arrêtées,
- anti-dilution en condition d'arrêt standard,
- anti-dilution en condition de puissance,
- alarme Haut flux neutronique (CNS),
- surveillance de l'activité dans les lignes vapeur,
- protection des pompes ASG,
- démarrage [] d'un train ISMP en état E,
- verrouillage des consommateurs vapeur sur compte rendu d'AAR,
- régulation de pré-positionnement de la vanne réglante VDA,
- isolement des circuits non strictement nécessaires à la mitigation de l'accident et véhiculant du fluide actif hors de l'enceinte sur signal Haute Activité Primaire (HAP),
- Contrôle de pression par le VDA sur pression GV.

2.3. FONCTIONS DES SYSTÈMES SUPPORT AUX FONCTIONS DE SAUVEGARDE

Les fonctions suivantes de gestion des systèmes support sont classées F1A :

- conditionnement du hall diesel principal,
- confinement du BK sur signal activité élevée BK,
- confinement du BR sur signal activité élevée BR en phase d'arrêt,
- refroidissement DWK du matériel de sureté RBS,
- refroidissement DWL du matériel de sureté RIS BP,

- refroidissement DWL du matériel de sureté RIS MP,
- refroidissement DVL du matériel de sureté RRI,
- isolement PTR signal bas niveau piscine de désactivation,
- isolement du RPE dans le BR,
- confinement du BAS sur détection fuite puisard RIS,
- ouverture des vannes PTR de trop-plein piscine BR et de vidange du compartiment des lances,
- arrêt du système de nettoyage des filtres à coquillage sur signal IS,
- régulation de sauvegarde de la température du RRI,
- basculement du refroidissement des barrières thermiques :
  - sur basse pression aval SEC,
  - sur débit RRI sur la ligne principale < MIN1,
  - sur température RRI > MAX1.

fonctions de gestion des diesels :

- démarrage diesel,
- arrêt diesel,
- séquence de délestage/relestage,
- basculement des disjoncteurs,
- délestage de la division voisine en cas de lignage des interconnexions,
- déconnexion des diesels MDTG en test périodique en cas de MDTE,
- relestage des fonctions support F1B.

2.4. []

[]

- []

2.5. FONCTIONS CONTRIBUANT À LA RÉALISATION DES DISPOSITIONS POST-ACCIDENTELLES

Ces fonctions contribuent à la réalisation des dispositions post-accidentelles pour atteindre et maintenir l'état d'arrêt sûr.

Les fonctions suivantes sont classées F1B :

- élaboration et affichage au MCS (exemple : marge à la saturation, niveau cuve),
- isolement enceinte [],
- RAZ des dispositions de conduite post-accidentelle,
- isolement de la barrière thermique des GMPP,

La fonction suivante est classée F2 :

- isolement enceinte [] phase 2 (via PIPO).

2.6. FONCTIONS D'INITIATION RRC-A

Ces fonctions sont nécessaires pour la gestion des séquences RRC-A.

Les fonctions suivantes sont classées F2 :

- signal d'ATWS suite à blocage mécanique des grappes,
- arrêt GMPP sur signal ATWS et Niveau GV GE < MIN1p,
- démarrage automatique du RBS :
  - sur signal ATWS,
  - sur haut flux neutronique (niveau source).
- basculement automatique du refroidissement des moteurs des pompes ISBP 1 et 4 de RRI vers DEL sur température RRI élevé ou bas débit RRI,
- inhibition [] des actions PS liées au démarrage de l'ISBP, du RBS et de l'ASG lors du démarrage du diesel d'ultime secours,
- démarrage automatique de l'ISBP à débit réduit.

La fonction suivante est classée F1B :

- arrêt automatique des pompes ISBP en mode RA sur température RRI élevé ou bas débit RRI.

3. BASE DE CONCEPTION

3.1. CRITÈRES DE CONCEPTION

3.1.1. Redondance

Quand deux fonctions de contrôle-commande classées F1A ont des actions antagonistes sur le même matériel, celle qui a la priorité sur l'autre est dite « non explicitement orientée sûreté » (NUSO : Non Unequivocally Safety Oriented). Toutes les autres fonctions de contrôle-commande de sûreté sont dites « explicitement orientées sûreté » (USO : Unequivocally Safety Oriented).

Les fonctions suivantes sont NUSO :

- isolement ASG,
- isolement VDA sur pression GV < MIN3p,
- démarrage RBS.

Les autres fonctions sont USO.

La partie F1 du système de protection est conçue de manière à résister à une simple défaillance même pendant la maintenance ou un test périodique. Afin de tolérer une défaillance unique ainsi que la maintenance tout en limitant le plus possible les déclenchements intempestifs, une redondance d'ordre quatre est nécessaire. De plus, les quatre trains de protection doivent être implantés dans des divisons distinctes pour éviter les défaillances dites de mode commun en cas d'agression interne touchant l'une des fonctions (pour les fonctions F1A, le système doit rester disponible malgré l'application d'une défaillance unique, dans le cas d'une agression initiant un PCC pour lequel le système est requis).

Le degré de redondance des fonctions et des matériels correspondants appartenant aux systèmes mécanique/fluide doit être préservé dans l'association avec le contrôle-commande[].

Actuellement, le niveau de fiabilité/disponibilité en termes de non-déclenchement à la sollicitation est défini au sous-chapitre 18.1.

3.1.2. Indépendance

Selon le RCCE (édition 2005), trois sortes d'indépendance sont prises en compte dans un système de contrôle-commande :

- l'indépendance entre les trains du système de contrôle-commande,
- l'indépendance entre les matériels de classes de sûreté différentes,
- l'indépendance entre les fonctions diversifiées.

En plus des exigences relatives aux différentes sortes d'indépendance à l'intérieur du système de protection, il faut également tenir compte de l'indépendance entre le système de protection et les autres systèmes de contrôle-commande.

3.1.2.1. Indépendance des quatre trains du système de protection

Selon le RCCE (édition 2005) et pour limiter les conséquences d'une défaillance unique sur une fonction redondante touchée, les fonctions redondantes et les matériels associés, y compris leurs systèmes supports (alimentation électrique, par ex.) doivent être indépendants les uns des autres.

Cette exigence suppose le respect des mesures suivantes :

- Le matériel redondant du système de protection doit être physiquement placé dans des divisions différentes.
- Des mesures de protection spécifiques doivent être prévues (par ex. mur de protection ou tubage de protection) pour assurer la séparation physique des points de mesure proches les uns des autres.
- Pour éviter la propagation des conséquences de l'agression interne d'une division à une autre et pour limiter les effets d'une défaillance simple aux fonctions redondantes touchées, les interconnexions entre divisions seront limitées le plus possible.
- Quand les connexions entre fonctions séparées par les divisions sont nécessaires (par ex. vote majoritaire), la communication des données entre divisions sera découplée électriquement (par ex. fibre optique) et physiquement (par ex. barrières anti-feu).
- Les commandes et informations erronées en provenance d'une division perturbée seront ignorées par les divisions non perturbées (par ex. par vote majoritaire).

3.1.2.2. Indépendance entre matériels de différentes classes de sûreté

Selon le RCCE (édition 2005), les matériels de classes de sûreté différentes dans le système de protection doivent être indépendants, de telle sorte qu'une défaillance d'un équipement de classe inférieure ne perturbe pas les fonctions du matériel de classe supérieure.

Cette exigence suppose le respect des mesures suivantes :

- Pour le système de protection, les connexions entre matériels de classes de sûreté différentes doivent être limitées le plus possible (par ex. limiter l'utilisation commune de mesures et composants).
- L'utilisation commune de composants doit autant que possible être évitée. A défaut, le matériel d'utilisation commune doit être affecté, classé et conçu en fonction des exigences de la classe la plus élevée.
- Les connexions entre matériels E1 et matériels E2 ou NC doivent être électriquement découplées.

3.1.2.3. Indépendance entre fonctions diverses

Quand la diversité fonctionnelle est requise, un degré d'indépendance suffisant doit être atteint.

Cette exigence suppose le respect des mesures de conception suivantes :

- L'instrumentation, les unités de traitement et le câblage de chacune des fonctions doivent être séparés.
- La diversité du matériel d'instrumentation peut être envisagée quand les fonctions diverses utilisent la même grandeur physique (décision au cas par cas).

3.1.2.4. Indépendance entre le système de protection et les autres systèmes de contrôle-commande

Le système de protection appartient à la ligne de défense principale. Une indépendance suffisante par rapport aux autres lignes de défense doit être assurée du fait de cette appartenance.

Cette exigence suppose le respect des mesures de conception suivantes :

- Des dispositions doivent être prises pour découpler les connexions entre le système de protection et les systèmes de contrôle-commande classés F2 ou NC. Si des grandeurs physiques communes sont partagées par le système de protection et d'autres systèmes de contrôle-commande, des dispositions doivent être prises pour découpler les connexions.
- Un capteur peut être utilisé à la fois pour des fonctions de protection dans le PS et pour des fonctions de régulation dans un autre système de contrôle-commande. La défaillance de ce capteur pourrait entrainer une mauvaise régulation. Un transitoire pourrait donc être généré et en conséquence déclencher une fonction de protection en relation avec le capteur défaillant.
  Ce transitoire doit être évité sauf si cette fonction de protection reste disponible malgré la défaillance du capteur, combinée à une intervention de maintenance préventive ou un essai périodique (critère de défaillance unique).
  Pour éviter un tel transitoire, et donc le déclenchement de la fonction de protection, la fonction de régulation doit être rendu robuste vis à vis d'une défaillance capteur.

3.1.3. Détection des états dégradés

Des mesures appropriées doivent être prises pour détecter et identifier les défaillances qui se produisent, ceci afin d'éviter les longues périodes d'exploitation dans une configuration de contrôle-commande dégradée qui risque d'aboutir à une perte de fonction à la suite d'une accumulation de défaillances.

C'est pourquoi des autotests et des essais périodiques du matériel chargé des fonctions F1 et F2 (RRC-A) doivent être prévus pour détecter toute défaillance susceptible d'empêcher la fonction concernée de jouer son rôle.

3.2. EXIGENCES DE DISPONIBILITÉ

3.2.1. Déclenchement intempestif en amont du dernier voteur

Pour les fonctions F1A, toute défaillance en tout endroit du système de protection en amont du dernier voteur ne doit pas générer d'ordre intempestif qui conduirait à un déclenchement intempestif, même pendant une intervention de maintenance ou un essai périodique.

3.2.2. Déclenchement intempestif en aval du dernier voteur

Pour les fonctions F1A, le risque de déclenchement intempestif des actionneurs correspondants à cause des matériels en aval du dernier voteur (celui-ci compris) doit être réduit le plus possible.

3.3. PERFORMANCES REQUISES

3.3.1. Temps de réponse

Pour les fonctions automatiques, le temps de réponse inclut :

- T1b : temps de réponse du conditionnement des capteurs en entrée du PS,

- T2 : temps de traitement des unités PS aux entrées des disjoncteurs pour les fonctions d'AAR, et aux cellules d'actionneurs pour les fonctions de sauvegarde.

Pour la plupart des fonctions de protection, le temps de réponse est inférieur ou égal à [] ms, par exemple :

- les fonctions de protection : AAR sur bas/très bas débit boucle primaire, ont un temps de réponse inférieur ou égal à []ms,
- la fonction de protection AAR sur basse vitesse GMPP a un temps de réponse inférieur ou égal à []ms,
- les fonctions de protection en relation avec les alimentations électriques (diesel, disjoncteurs) ont un temps de réponse inférieur ou égal à []ms.

Pour certaines fonctions, le temps de réponse est différent, par exemple :

- la fonction AAR sur « Bas RFTC » a un temps de réponse inférieur ou égal à []ms,
- la fonction « Isolement ARE grand débit sur signal d'AAR » a un temps de réponse inférieur ou égal à []ms,
- les fonctions de protection suivantes ont un temps de réponse inférieur ou égal à []ms :
  - AAR sur Niveau de puissance thermique cœur élevé,
  - démarrage IS sur delta Pression de saturation < MIN1p,
  - arrêt d'un train RIS/RA en mode RA sur delta pression saturation < MIN2p,
  - ouverture VDA (refroidissement partiel) sur signal IS,
  - isolement enceinte phase 1 sur pression enceinte > MAX1p ou signal IS,
  - AAR sur bas temps de doublement (niveau intermédiaire),
  - AAR sur haut flux nucléaire (niveau intermédiaire),
  - les fonctions en relation avec les chaînes d'anti-dilution.

Il n'y a pas d'exigences de temps de réponse pour les permissifs.

En règle générale, il n'y a pas d'exigences de temps de réponse pour les fonctions automatiques F1B ou F2.

Cependant, la fonction « Signal d'ATWS suite à blocage mécanique des grappes » a un temps de réponse inférieur ou égal à []ms.

Les temps de réponse pour les fonctions de communication au niveau 2 sont les suivantes :

- temps de transmission d'un signal d'une unité PS F1A à la passerelle SPPA T2000 (CM104) : 1 s,
- temps de transmission d'un signal d'une unité PS F1A au MCS ou du MCS à une unité PS F1A : 1,5 s.

3.3.2. Précision

Les actions automatiques de protection sont déclenchées sur franchissement d'un seuil correspondant aux points de consigne de l'instrumentation. Ces points de consignes sont déterminés en tenant compte d'une certaine marge par rapport aux limites de sûreté prescrites dans les spécifications techniques d'exploitation. Ces marges tiennent compte de :

- l'incertitude de l'instrumentation,

- la dérive éventuelle entre deux calibrages,
- la dynamique des transitoires considérés,
- le temps de réponse des chaînes de protection.

La précision des capteurs en entrée des chaînes de protection est donc définie de façon à ce que le franchissement des seuils puisse être détecté avec la précision requise.

3.3.3. Répartition des fonctions

Pour respecter la norme CEI 60880, Annexe B, des tâches applicatives ayant des temps de réponse différents ne doivent pas être confiées à la même unité de traitement.

Pour limiter la complexité du logiciel, les fonctions doivent être réparties entre plusieurs unités de traitement.

S'il apparaît que, pour un accident spécifique, deux signaux existants peuvent déclencher l'action de protection requise (diversité fonctionnelle), la structure du système de protection doit en tenir compte afin de prévoir des matériels distincts pour la mise en œuvre des différentes chaînes d'initiation.

3.3.4. Communication

Selon le RCCE (édition 2005) C5000, le comportement du logiciel du système de protection qui supporte les fonctions F1A doit être déterministe. Un système de contrôle-commande est dit déterministe si on peut connaître, par analyse de sa conception, de son architecture et de son implémentation, et avec un grand degré de précision et de certitude, son comportement dans tous les modes d'exploitation requis.

Le système de transmission de données utilisé dans la partie F1A du système de protection doit avoir un comportement déterministe.

En conséquence les unités de contrôle-commande assurant des fonctions F1A ont les principales caractéristiques suivantes :

- Le traitement du logiciel d'application des unités en communication sur les réseaux inter-unités est strictement cyclique.
- Les réseaux inter-unités ont une charge maximum calculable.

3.4. EXIGENCES RELATIVES AUX CONDITIONS D'AMBIANCE

3.4.1. Conditions normales

Le matériel doit pouvoir fonctionner dans les conditions ambiantes données dans le sous-chapitre 9.4.

3.4.2. Conditions accidentelles

Comme prescrit par le § 0.3.1.4., les matériels qui assurent une fonction F1 doivent pouvoir rester opérationnel dans des conditions post-accidentelles.

De même, un matériel assurant une fonction F2 doit pouvoir rester opérationnels dans des conditions post-accidentelles.

3.5. EXIGENCES RELATIVES À L'INTERFACE HOMME-MACHINE

L'accès aux unités d'affichage vidéo, ordinateurs, claviers, souris, lecteurs de disquettes ou de CD-ROM, disques durs, imprimantes, etc. ayant un lien avec le matériel du système de protection doit être contrôlé par des moyens physiques tels que clés, cartes magnétiques ou à puce, etc.

Chaque fois que le travail sur l'un de ces matériels est interrompu, le matériel doit être verrouillé de nouveau.

Aucun accès immédiat au logiciel du système de protection proprement dit n'est possible. En conséquence :

- L'accès n'est possible que par l'intermédiaire du matériel d'interface utilisé pour les essais, la configuration ou la consultation des données.
- Ce matériel d'interface est connecté au système de protection sans qu'il soit nécessaire d'ouvrir les armoires de contrôle-commande.

Le but de cette restriction est de limiter le nombre total d'accès physiques nécessaires aux modules électroniques du système de protection.

La déconnexion du matériel d'interface n'est possible qu'après avoir déverrouillé un dispositif de verrouillage spécifique.

L'accès au logiciel du système de protection se fait par l'intermédiaire d'un module de filtrage installé dans le matériel d'interface.

Le module de filtrage demande à tout utilisateur demandant l'accès au logiciel :

- le mot de passe général,
- le nom de l'utilisateur,
- le mot de passe personnel de l'utilisateur.

Le mot de passe personnel de l'utilisateur n'est connu que de l'utilisateur. Celui-ci peut en changer quand il le souhaite en respectant une périodicité minimale entre changements.

La gestion des accès est effectuée au niveau du matériel d'interface. Elle permet :

- le contrôle du nom et du mot de passe personnel des opérateurs,
- l'accès à certaines zones du logiciel du système de protection en fonction du nom de l'utilisateur. Il inclut les autorisations de lecture et d'écriture,
- l'accès à une ligne unique,
- le contrôle des traces automatiques des opérations (traces de l'accès et des opérations quand l'accès est accordé),
- Etc.

L'éditeur doit organiser le logiciel et le matériel du système de protection de façon à interdire l'accès aux zones du logiciel autres que celles nécessaires pour les essais, la configuration et la consultation des données.

[] Tout accès au logiciel de ces unités ne peut être exécuté que dans des modes de fonctionnement spécifiques validés par des clés physiques. (voir § 5.).

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

4.1.1. Généralités

Le système de protection doit être conçu pour :

- limiter la quantité de matériel (cartes électroniques, ...) et le nombre de connexions réseau,
- garantir le respect des exigences globales de temps de réponse des fonctions, par ex. en limitant la charge des réseaux.

4.1.2. Structure fonctionnelle

Pour ce paragraphe, se reporter aux figures FIG–7.3.1.2 et FIG–7.3.1.3.

Le système de protection exécute quatre types de fonctions F1A :

- le déclenchement automatique de l'arrêt automatique du réacteur,
- la commande automatique des fonctions de sauvegarde,
- la commande des systèmes support,
- les commandes [].

Il accomplit quelques fonctions F1B, qui sont principalement :

- le calcul de la marge à la saturation,
- une partie de la surveillance post-accidentelle, avec possibilité de faire la synthèse des informations (réduction de la redondance) dans les divisions 1 et 4,
- la gestion des commandes [] F1B qui agissent sur les dispositifs F1A du PS,
- la gestion des commandes groupées F1B [],
- Etc.

Il accomplit quelques fonctions F2, qui sont principalement :

- la gestion des alarmes relatives au PS,
- les fonctions nécessaires à la gestion des séquences RRC-A.

Les explications qui suivent s'appliquent aux quatre divisions de la centrale et aux quatre trains du système de protection.

4.1.2.1. Capteur(s) et transmetteur(s)

Les mesures réalisées par les capteurs et transmetteurs sont acquises et distribuées au PS par les armoires de conditionnement.

Selon le type de capteurs, les armoires de conditionnement assurent :

- l'alimentation électrique des capteurs et des modules de découplage si nécessaire,
- le conditionnement requis pour fournir les différents types de signaux normalisés qui peuvent être utilisés par les convertisseurs analogique/numérique (A/N) du PS.

4.1.2.2. Acquisition des mesures

Convertisseurs Analogique/Numérique (A/N) :

Le système de protection convertit les mesures analogiques en valeurs numériques (format de données exploitables par les unités informatisées).

Transmission des données :

Dans le cas général, il n'y a pas d'échange de données analogiques entre les quatre divisions du système de protection après la conversion A/N (voir figure FIG–7.3.1.2). Toutefois, certaines fonctions, comme la fonction de surveillance de la distribution de la puissance à l'intérieur du cœur, requièrent l'échange d'informations analogiques à ce niveau (voir figure FIG–7.3.1.3).

Premier niveau de traitement :

Chaque signal est vérifié. En cas de violation non attendue de la gamme de mesure ou en cas de détection d'une anomalie dans l'acquisition (détection de fil coupé par exemple), le signal est invalidé pour le traitement.

Chaque entrée numérisée est traitée pour produire la valeur physique de la mesure utilisée par le traitement. Les résultats de la numérisation et de la conversion en valeurs physiques sont également transmis à d'autres systèmes de contrôle-commande et aux équipements de maintenance.

4.1.2.3. Commandes [] du MCP et du MCS

Le système de protection reçoit des commandes [] du MCP, ainsi que du MCS pour remettre à zéro certaines actions déclenchées automatiquement par le système de protection ou pour démarrer certaines actions de protection.

Les commandes [] envoyées depuis le MCS ou depuis le MCP sont validées par un signal acquis au PS et élaboré à partir des commutations MCP/MCS et Salle de Commande/Station de Repli. Ce signal est acquis par les ALUs pour les commandes F1A et par les unités MSI pour les commandes F2/F1B.

Les commandes F1A sont envoyées du MCS directement aux ALUs. Les commandes F1B du MCS sont acquises par les unités PI puis envoyées aux unités MSI, et celles du MCP sont envoyées au Gateway puis au MSI.

Les commandes venant du MCP doivent être validées []. Les signaux correspondants sont envoyés aux unités MSI.

Le système de protection reçoit des commandes [] du PIPO (Pupitre Inter Poste Opérateur) pour les commandes d'AAR et d'isolement enceinte phase 2. Ces commandes sont disponibles en permanence tant que la salle de commande est opérationnelle. Ces commandes sont envoyées aux ALUs.

4.1.2.4. Traitement des signaux de déclenchement

La première étape est la collecte des données provenant du module d'acquisition de la division concernée ou, dans certains cas spéciaux, provenant également des trois autres divisions (certaines fonctions ayant besoin des informations des quatre trains, voir le point Transmission des données ci-dessus). Les données numériques sont traitées en fonction des exigences fonctionnelles.

La dernière étape du traitement des signaux de déclenchement est la comparaison avec un seuil pour produire une information binaire, appelée signal de déclenchement dans la suite du document, qui indique si le seuil est atteint ou non.

Si une anomalie est détectée dans le traitement des signaux de déclenchement, le signal de déclenchement est invalidé.

4.1.2.5. Traitement des signaux d'activation

Chaque division collecte les signaux de déclenchement redondants dans les quatre divisions du PS. Ces signaux sont traités par une logique de vote [] pour produire des ordres de déclenchement. Différents cas sont possibles et sont représentés en figure **FIG–7.3.1.5**. Cette logique de vote doit être conçue pour être dégradée de façon appropriée si un ou plusieurs signaux sont invalidés.

Les différents ordres de déclenchement élaborés par les différentes voies de déclenchement sont validés/inhibés par des permissifs. Il en résulte un signal d'activation.

Les résultats du votre majoritaire (c'est-à-dire l'ordre de déclenchement), ainsi que le signal d'activation sont également transmis aux autres systèmes de contrôle-commande (voir tableau **TAB–7.3.1.2**) et aux équipements de maintenance.

4.1.2.6. Traitement des boucles de régulation

La grandeur physique régulée est acquise par un module d'acquisition dans une ou plusieurs divisions, puis les valeurs correspondantes sont transmises dans une division aux unités de traitement. Différents cas sont possibles et sont représentés en figure **FIG–7.3.1.5**, par exemple : fonctions de régulation VDA, régulation de température du RRI.

4.1.3. Composition

Pour ce paragraphe, se reporter aux figures **FIG–7.3.1.3**, **FIG–7.3.1.4**, **FIG–7.3.1.8** et **FIG–7.3.1.9**.

Les figures **FIG–7.3.1.3**, **FIG–7.3.1.4** et **FIG–7.3.1.8** donnent une idée de l'«architecture matérielle».

La figure **FIG–7.3.1.6** montre la relation entre la « structure fonctionnelle » et l'«architecture matérielle» du système de protection.

La figure **FIG–7.3.1.9** montre un schéma d'architecture complet du PS. Les différentes unités qui composent le système de protection sont décrites ci-après :

4.1.3.1. Unités d'acquisition déportées (RAU)

Ces unités sont dédiées à l'acquisition des mesures des collectrons (SPND : Self Powered Neutron Detector) et à la transmission de ces mesures aux unités de traitement dans toutes les divisions.

Les unités RAU sont classées F1A.

4.1.3.2. Unités d'acquisition et de traitement (APU)

Ces unités sont dédiées principalement à l'acquisition des capteurs F1A, mais des capteurs F1B peuvent aussi être acquis, et aux traitements relatifs aux acquisitions tels que conversion du signal, validation du signal ou détection de seuil.

De plus, l'APU effectue certains calculs en relation avec les fonctions de sûreté (ex. : calcul du RFTC).

Elles génèrent les signaux de déclenchements ensuite traités en ALU.

Les unités APU sont classées F1A.

4.1.3.3. Unités logiques des actionneurs (ALU)

Les ALU génèrent les signaux d'activation en sortie du PS. Pour cela, les ALU réalisent les votes entre les signaux de déclenchement provenant des APU de plusieurs divisions ainsi que les traitements des boucles de régulation. Les résultats de ces traitements peuvent être validés ou inhibés par des permissifs.

Les unités ALU sont classées F1A.

4.1.3.4. Interfaces de service et de surveillance (MSI)

Ces unités sont dédiées à la surveillance du PS et à la gestion des interfaces avec les systèmes extérieurs au PS (ex. : MCS, SAS, PAS).

Les unités MSI sont classées F1B.

4.1.3.5. Unités d'interface avec le MCS (PI)

Ces unités sont dédiées à la transmission des données entre le PS et le MCS.

Les unités PI sont classées F1B.

4.1.3.6. Unités d'interfaces entre le MCP et le PAS / SAS (TXS Gateway)

Les Gateway assurent les échanges avec le MCP et assurent l'interface avec le SAS et avec le PAS.

Les Gateway sont classées F2.

4.1.3.7. Répartition fonctionnelle

Le système de protection met en œuvre deux sortes de fonctions :

- des fonctions à trois niveaux qui exigent des échanges de données entre les divisions immédiatement après leur acquisition,
- des fonctions à deux niveaux qui n'exigent pas d'échange des données des mesures acquises.

Dans le cas des fonctions à trois niveaux, la structure fonctionnelle sera implémentée dans les unités suivantes :

- acquisition des mesures assurée par les unités d'acquisition déportées,
- traitement des signaux de déclenchement assuré par les unités d'acquisition et de traitement,
- traitement des signaux d'activation assuré par les unités logiques des actionneurs.

Dans le cas des fonctions à deux niveaux, la structure fonctionnelle sera implémentée dans les unités suivantes :

- acquisition des mesures assurée par les unités d'acquisition et de traitement,
- traitement des signaux de déclenchement assuré par les unités d'acquisition et de traitement,
- traitement des signaux d'activation assuré par les unités logiques des actionneurs.

Dans le cas de fonctions de régulation, la partie acquisition des données de mesure est assurée par une APU. Tout le reste de la structure fonctionnelle est implémenté dans les ALUs (voir figure **FIG–7.3.1.6**). La vanne réglante est pilotée par un dispositif dit "Maître / esclave" qui intègre les deux ALUs.

4.1.3.8. Description générale

La partie F1A du système de protection est composée de plusieurs unités : RAU – APU et ALU, décrites aux **§ 4.1.3.1.** à **§ 4.1.3.3.**. Les unités F1A communiquent entre elles par réseaux.

Pour tirer parti de l'existence de deux signaux pour une action de sûreté donnée, la partie F1A du système de protection est organisée en deux sous-systèmes indépendants (voir figure **FIG–7.3.1.3**).

Les données des capteurs seront acquises par la RAU ou l'APU du sous-système A ou B. Les données d'un capteur peuvent également être acquises par les deux sous-systèmes (voir figure **FIG–7.3.1.4**).

Les actionneurs peuvent être commandés soit par le sous-système A, soit par le sous-système B, soit par les deux (voir figure **FIG–7.3.1.4**).

- l'arrêt automatique du réacteur :
  - est commandé au niveau de l'ALU du sous-système A,
  - est commandé au niveau de l'ALU du sous-système B.
- les systèmes de sauvegarde sont commandés au niveau de l'ALU du sous-système A ou B,
- les fonctions des systèmes support sont commandées au niveau de l'ALU des sous-systèmes A ou B.

Les fonctions des diesels sont commandées au niveau de l'ALU des sous-systèmes A et B.

La partie F1B du système de protection est composée de plusieurs unités dédiées :

- PI assure l'interface entre le PS et le MCS,
- MSI assure la gestion du transfert des informations ainsi que certains traitements (par exemple : le calcul de la marge à la saturation).

La partie F2 du système de protection est composée de passerelles assurant le transfert des données avec le SPPA T2000 (TXS Gateway).

La partie non classée du système de protection est composée des unités de service assurant les essais, le diagnostic et la maintenance.

Dans chaque division, ces unités sont connectées les unes aux autres par réseaux.

De plus, les unités d'interface (PI) []doivent être connectées aux quatre unités MSI pour permettre la synthèse des informations.

Les unités (MSI) assurent l'interface avec les matériels moins classés :

- interface avec le RCSL dans les quatre divisions,
- interface avec les PI[],
- interface avec l'unité de service qui supporte l'IHM du PS pour les essais, le diagnostic et la maintenance.

4.1.3.9. Conformité aux exigences réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

La conformité aux textes officiels spécifiquement applicables au système, listés dans le **§ 0.3.2.**, est assurée par la mise en œuvre de signaux automatiques d'arrêt du réacteur, tels que décrits au **§ 2.1.**.

La conformité aux directives techniques spécifiquement applicables au système, listées dans le **§ 0.3.2.**, est assurée notamment par les éléments suivants :

- concernant l'exigence de redondance et de diversité dans les systèmes de sûreté : voir **§ 3.1.1.**, **§ 3.1.2.** et **§ 3.1.3.**,
- concernant la qualification des systèmes de contrôle-commande, les principes de qualification des équipements des systèmes de contrôle-commande sont énoncés dans la section 7.2.3,
- concernant la validation du système, les fonctions d'autocontrôle du système sont présentées aux **§ 5.** et **§ 6.**.

4.1.3.10. Système tel que réalisé

A ce stade de la fabrication, de l'installation, et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.2. IMPLANTATION

Afin de respecter les exigences de séparation géographique, les quatre trains du système de protection et le matériel électrique de contrôle-commande sont installés à l'intérieur des quatre bâtiments de sauvegarde. []

4.3. INTERFACES AVEC LE RESTE DU CONTRÔLE-COMMANDE

Le système de protection est implémenté au niveau 1 de la structure des automatismes. Il est en interface avec les autres systèmes des niveaux 0, 1 et 2

En figure **FIG–7.3.1.1** sont représentés les principaux interfaces et liens externes au système de protection et au système de protection F1A. Les descriptions qui suivent se rapportent à cette figure.

4.3.1. Interface du système de protection avec le reste du contrôle-commande

4.3.1.1. Entrées

Le système de protection reçoit des commandes [] du MCP, du MCS et du PIPO.

Le système de protection acquiert des données (analogiques, binaires,…) issues de signaux transmis par les systèmes de conditionnement, les autres systèmes de contrôle-commande.

Le système de protection reçoit des signaux binaires de compte-rendu des cellules électriques.

Le système de protection échange les informations nécessaires pour la mise en service, la maintenance et les essais périodiques avec le [].

Le système de protection transmet (via MSI) les informations entre le CCAG et le PAS.

Le système de protection reçoit du coffret de changement de mode CPU les signaux d'autorisation de changement de paramètres et de passage en mode TEST ou DIAGNOSTIQUE.

Le tableau **TAB–7.3.1.1** donne un aperçu des informations fournies par les autres systèmes de contrôle-commande au système de protection (PS).

4.3.1.2. Sorties

Le système de protection fournit des informations au MCS, au MCP et au PSIS.

Le système de protection fournit aux cellules des actionneurs les signaux de commande visant à modifier la position des actionneurs.

Le système de protection transmet des ordres aux actionneurs d'arrêt automatique du réacteur (disjoncteurs et contacteurs) pour la réalisation de l'AAR.

Le système de protection transmet l'ordre de déclenchement à la turbine.

Le système de protection fournit des informations au système de contrôle, de surveillance, et de limitation du réacteur (RCSL), à l'automate de tranche (PAS), à l'automate de sûreté (SAS), au contrôle-commande diesel, au contrôle-commande GPA, au contrôle-commande KRT, au contrôle-commande CCAG, au HKS, au RPN ainsi qu'au RPI.

Le système de protection fournit des informations à l'équipement RMAD lors des phases de divergence.

Le tableau **TAB–7.3.1.2** donne un aperçu des données du système de protection à destination des autres systèmes de contrôle-commande.

4.3.2. Interfaces entre le système de protection F1A et son environnement

Le PS – FA1 est en interface avec :

- les unités MSI classées F1,
- les autres systèmes extérieurs au PS des niveaux 0, 1 et 2.

4.3.2.1. Interface entre le PS –F1A et le PS non F1A

Chaque unité du système de protection F1A est connectée par réseau au MSI de la même division. Les unités MSI assure l'interface entre :

- le PS-F1A et les autres unités du PS moins classées (unités PI, Unité de service…),
- le PS–F1A et les autres systèmes de contrôle-commande moins classés.

Le PS-F1A échange à travers la MSI des informations en provenance du MCP, du MCS, du SPPA T2000, des contrôles-commandes GPA, et HKS.

Le système de protection échange à travers la MSI les informations nécessaires pour la maintenance et les essais périodiques avec l'unité de service.

4.3.2.2. Interface entre le PS – F1A et les autres systèmes de contrôle-commande

4.3.2.2.1. Entrées

Le système de protection F1A reçoit des commandes [] du MCS et du PIPO.

Le système de protection F1A acquiert des données (analogiques, binaires) transmis par les systèmes de conditionnement.

Le système de protection F1A acquiert également des signaux transmis par le SPPA T2000 en fil à fil.

Le tableau **TAB–7.3.1.3** donne un aperçu des informations fournies en entrées du PS-F1A.

4.3.2.2.2. Sorties

Le système de protection F1A fournit des informations en fil à fil au MCS.

Le système de protection fournit aux cellules des actionneurs, les signaux de commande visant à modifier la position des actionneurs.

Le système de protection F1A transmet des ordres aux actionneurs d'arrêt automatique du réacteur (disjoncteurs et contacteurs) pour la réalisation de l'AAR.

Le système de protection F1A transmet l'ordre de déclenchement à la turbine.

Le système de protection F1A fournit des informations en fil à fil au système de contrôle, de surveillance, et de limitation du réacteur (RCSL), au système RPN, à l'automate de tranche (PAS), à l'automate de sûreté (SAS), au contrôle-commande diesel, au RDTME, et au klaxon situé dans le bâtiment réacteur.

Le tableau **TAB–7.3.1.4** donne un aperçu des données du système de protection F1A à destination des autres systèmes de contrôle-commande.

5. MODES DE FONCTIONNEMENT

Le système de protection est composé d'un ensemble d'unités (APU, ALU, etc.) dont l'élément principal est une CPU.

La description suivante concerne le mode de fonctionnement des unités.

La figure **FIG–7.3.1.7** donne des détails sur les modes de fonctionnement et leurs interactions.

Les modes de fonctionnement d'une unité sont les suivants :

DEMARRAGE : au démarrage du processeur, les multiples étapes d'une routine d'initialisation sont exécutées. Dans un premier temps, un contrôleur d'amorçage bas niveau commande l'initialisation du

matériel et déclenche une série complète d'autotests de démarrage. Après un démarrage réussi du noyau du système d'exploitation, le module INIT de l'environnement d'exploitation (RTE) prend le contrôle de la CPU pour terminer la phase d'initialisation du RTE.

Si l'initialisation échoue, le fonctionnement cyclique ne démarre pas et le module INIT effectue une boucle sans fin sans activer les signaux de sortie. L'opérateur de maintenance est informé de cet état via l'unité de service.

Une fois l'initialisation réussie, le processeur de fonctions bascule en mode de fonctionnement cyclique. L'activation des signaux de sortie [].

Au redémarrage d'une unité RAU, RPI, APU, ALU, MSI, PI, ses sorties sont inhibées automatiquement [], ceci afin de permettre aux éventuels algorithmes dynamiques de se stabiliser et de réduire les risques d'actions intempestives.

FONCTIONNEMENT CYCLIQUE : le fonctionnement cyclique est le mode normal d'un processeur de fonctions. Il reste dans cet état tant qu'il n'est pas redémarré, []. Le passage aux autres modes de fonctionnement ne peut être déclenché que par l'unité de service.

En fonctionnement cyclique, n'importe quel signal sélectionné peut être affiché dans les diagrammes de programmation affichés sur l'unité de service.

La modification des paramètres est réalisable également dans ce mode, [] avant que certaines valeurs de consigne ne puissent être changées. La modification de paramètres en ALU n'est possible que sur une unité à la fois.

Pendant le fonctionnement du système de contrôle-commande, seuls les paramètres désignés au préalable comme étant modifiables peuvent être changés par l'unité de service, par exemple pour optimiser une boucle de régulation ou adapter les paramètres en cas d'exploitation en prolongation de cycle.

TEST : ce mode est utilisé pour le dépannage. Une validation spécifique [] est une condition préalable pour passer en mode « TEST ». Lorsqu'une unité est en mode « TEST », le traitement cyclique des fonctions applicatives est interrompu.

Si une unité d'une division est en mode TEST, les unités correspondantes des autres divisions peuvent continuer à traiter les fonctions PS.

Les fonctions de traitement sont activées selon les conditions du test à l'aide de commandes supplémentaires envoyées par l'unité de service :

- activation / désactivation des traitements d'entrée / sortie,
- activation / désactivation des fonctions d'envoi et de réception de messages,
- activation / désactivation du traitement de certains modules des diagrammes de fonctions,
- pré-positionnement des données dans les mémoires,
- suivi des signaux.

La sortie du mode « TEST » s'effectue toujours par une réinitialisation du processeur et un redémarrage automatique. Après un temps de démarrage d'environ 10 secondes, le traitement se poursuit en mode de fonctionnement cyclique, sorties inhibées jusqu'à ce que l'opérateur de maintenance effectue l'acquittement.

DIAGNOSTIC : Une validation spécifique par l'opérateur (gérée par un jeu de clés physiques) est une condition préalable pour passer en mode « DIAGNOSTIC ». En mode « DIAGNOSTIC », toutes les fonctions du mode « TEST » sont accessibles. Les fonctions supplémentaires sont principalement relatives au chargement logiciel. Dans des cas très exceptionnels des routines de test spécifiques peuvent être chargées et exécutées.

La sortie du mode « DIAGNOSTIC » se fait toujours par réinitialisation du processeur, suivie d'un redémarrage automatique. De même que pour le mode « TEST », après un temps de démarrage d'environ 10 secondes, le traitement se poursuit en mode de fonctionnement cyclique, sorties inhibées, jusqu'à ce que l'opérateur de maintenance effectue l'acquittement.

Clés physiques de validation

Un jeu de clés physiques, communes aux 4 divisions du PS permet de valider les modes TEST et DIAGNOSTIC ainsi que la modification des paramètres, il se compose de :

- une clé permettant de sélectionner l'unité sur laquelle on souhaite intervenir,
- une clé autorisant la modification des paramètres,
- une clé autorisant le passage en mode TEST ou DIAGNOSTIC,
- un sélecteur permet de choisir la division sur laquelle on souhaite intervenir (un seul choix possible).

Le verrouillage à clé ainsi que le sélecteur de division est non classé.

6. TECHNOLOGIE UTILISÉE

Le matériel utilisé pour implémenter le système de protection est la plate-forme de contrôle-commande numérique TELEPERM XS de FRAMATOME.

Le système numérique de contrôle-commande TELEPERM XS est destiné aux applications relatives à la sûreté des centrales nucléaires. Il a été mis au point pour l'équipement des nouvelles centrales nucléaires, ainsi que pour la modernisation des systèmes de contrôle-commande des centrales existantes.

Les avantages majeurs de l'emploi de processeurs numériques dans les systèmes de sûreté sont :

- la détection précoce des anomalies par des autocontrôles cycliques,
- la détection précoce des anomalies par un meilleur contrôle des périphériques (transducteurs, interfaces périphériques),
- la protection contre les signaux erronés par des moyens de détection des anomalies pour la transmission série des données,
- une plus grande tolérance aux anomalies que les systèmes câblés, grâce à une fonction de détermination de l'état des signaux pour repérer les signaux erronés,
- le traitement numérique des signaux, insensible à la dérive ou aux interférences électromagnétiques,
- le découplage galvanique par l'utilisation de la fibre optique pour la transmission série des données,
- l'automatisation de l'ingénierie et de la documentation de la centrale, garantissant une homogénéité maximale de la documentation.

7. ALIMENTATION ÉLECTRIQUE

7.1. EXIGENCES

Le système de protection doit être alimenté par une alimentation ininterruptible de tension adéquate [].

Chaque armoire doit être connectée à deux alimentations continues redondantes. Les arrivées de ces alimentations doivent être isolées les unes des autres, par exemple à l'aide de diodes.

En fonctionnement normal, les deux alimentations doivent être alimentées par l'alimentation ininterruptible (UPS) de la division correspondante. D'autre part, l'une des deux alimentations peut être connectée à l'alimentation ininterruptible (UPS) de la division voisine.

Pour permettre un conditionnement normalisé des signaux, l'alimentation et la sortie des signaux de télémesures doivent être normalisées.

7.2. ALIMENTATION ÉLECTRIQUE DES ARMOIRES TXS

[]

Les alimentations électriques redondantes [] sont fournies par 2 tableaux électriques :

- []
- []

En cas de perte des alimentations externes, un diesel d'urgence est disponible pour chaque division. De plus le [] peut être alimenté par un tableau [] d'une autre division.

TAB–7.3.1.1 DONNÉES D'ENTRÉE DU SYSTEME DE PROTECTION FOURNIES PAR D'AUTRES SYSTÈMES DE CONTRÔLE-COMMANDE

[]

TAB–7.3.1.2 DESTINATION DES DONNÉES DE SORTIE DU SYSTÈME DE PROTECTION

TAB–7.3.1.3 DONNÉES D'ENTRÉE DU SYSTEME DE PROTECTION F1A FOURNIES PAR D'AUTRES UNITES DU SYSTEME DE PROTECTION ET PAR D'AUTRES SYSTÈMES DE CONTRÔLE-COMMANDE

[]

TAB–7.3.1.4 DESTINATION DES DONNÉES DE SORTIE DU SYSTÈME DE PROTECTION F1A

[]

FIG–7.3.1.1 INTERFACES ET RELATIONS ENTRE LE SYSTÈME DE PROTECTION ET LES AUTRES SYSTÈMES DES NIVEAUX 0, 1 ET 2

[]

[]

FIG–7.3.1.2 STRUCTURE FONCTIONNELLE GÉNERALE (DIVISION 1) DU SYSTÈME DE PROTECTION (PS)

FIG–7.3.1.3 ARCHITECTURE MATERIELLE DE LA PARTIE F1A DU SYSTEME DE PROTECTION (PS)

FIG–7.3.1.4 INTERFACES MATERIELLES DU SYSTEME DE PROTECTION (PS)

FIG–7.3.1.5 ARCHITECTURE FONCTIONNELLE

FIG–7.3.1.6 RELATION ENTRE STRUCTURE FONCTIONNELLE ET ARCHITECTURE MATÉRIELLE

[]

FIG–7.3.1.7 MODES DE FONCTIONNEMENT D'UNE UNITÉ

[]

FIG–7.3.1.8 FLUX D'INFORMATION ENTRE LES DIFFÉRENTES PARTIES DU PS

FIG–7.3.1.9 ARCHITECTURE MATÉRIELLE

SOMMAIRE

FIGURES :

.7.3.2 ARCHITECTURE DU SYSTÈME D'AUTOMATISME DE SÛRETÉ (SAS)

0. EXIGENCES DE SÛRETÉ

Le système de contrôle-commande SAS est assujetti aux exigences de sûreté applicables aux systèmes de contrôle commande E1B, du fait de sa gestion du contrôle-commande associé aux fonctions de sûreté F1B (non gérées par le PS).

Le système SAS assure le traitement des actions automatiques et manuelles, et la surveillance associée, nécessaires à l'accomplissement des fonctions de sûreté énoncées ci-dessous.

0.1. FONCTIONS DE SÛRETÉ

Le SAS participe aux trois fonctions fondamentales de sûreté (maîtrise de la réactivité, évacuation de la puissance résiduelle et confinement des substances radioactives) au titre de la gestion des traitements de contrôle-commande associés aux fonctions suivantes :

- Les fonctions de gestion post-accidentelle (manuelles et automatiques) nécessaires pour amener la tranche lors d'un événement initiateur de l'état contrôlé à l'état d'arrêt sûr (F1B),
- Les fonctions relatives aux systèmes supports F1 qui ne changent pas d'état lors d'un évènement (systèmes de sûreté autonomes, par exemple la ventilation),
- Certaines fonctions de commande pouvant provoquer un évènement de type PCC-3 ou PCC-4, classées F1B,
- Les fonctions directement liées au contrôle de la radioactivité pendant le fonctionnement normal,
- Les fonctions F2 classées séisme (F2E), en particulier : les fonctions spécifiquement conçues pour contrôler les agressions internes et externes,
- Certaines fonctions de gestion des situations RRC-A,
- La fonction assurant la surveillance du MCP par un signe de vie F1B (voir paragraphe 0.2.4.2 de la section 7.4.1).

Le SAS est rattaché à la 2ème ligne de défense en profondeur dite de prévention du risque de fusion du coeur (voir section 7.1.1).

0.2. EXIGENCES RELATIVES À LA CONCEPTION

Au titre des fonctions F1B dont il assure les traitements des automatismes et des commandes manuelles et la surveillance liée (dont les fonctions de « gestion de priorité des commandes » et « surveillance de l'actionneur » du PACS définies en section 7.3.6) , le système SAS doit satisfaire aux exigences énoncées ci-après. Ces exigences doivent être respectées pour l'ensemble des fonctions gérées par le système SAS.

0.2.1. Exigences issues des classements fonctionnel et mécanique

0.2.1.1. Classement fonctionnel du système

Le système SAS doit être classé de sûreté, conformément au classement indiqué au sous-chapitre 3.2.

0.2.1.2. Critère de défaillance unique (active)

Le critère de défaillance unique doit s'appliquer au système SAS sur un plan fonctionnel (voir section 3.2.1), par l'intégration d'un degré de redondance suffisant, d'une structure et de dispositions adéquates.

D'autre part, si les essais périodiques du système sont possibles et réalisés (conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation) alors que le système doit pouvoir être sollicité au titre du traitement de fonctions de sûreté F1B, ils doivent être combinés avec l'application du critère de défaillance unique (au niveau de la fonction pour les systèmes F1B) pour définir la redondance à mettre en oeuvre.

0.2.1.3. Alimentations électriques secourues

L'alimentation électrique des équipements SAS doit être secourue par les groupes diesels principaux dans les quatre divisions et par les diesels d'ultime secours dans les divisions 1 et 4.

Par ailleurs, cette alimentation est du type « sans coupure », garantissant une alimentation même pendant le basculement alimentation normale / alimentation par diesel. De sorte que les fonctions de sûreté dont le système SAS gère les automatismes et la surveillance puissent être assurées sans discontinuité de service.

L'alimentation est diversifiée par deux sources d'alimentation alternative et continue pour chaque automate dans chacune des divisions où il se trouve implanté. Cette diversification est issue du REX [] et pallie le risque de mode commun sur les sources électriques.

En général, le système SAS est alimenté par la même division que celle du procédé dont il assure le pilotage, chaque division étant indépendante électriquement et physiquement des trois autres de façon à garantir une absence de mode commun entre divisions.

0.2.1.4. Qualification aux conditions de fonctionnement

Les équipements SAS doivent rester opérationnels en conditions post-accidentelles, et doivent en conséquence respecter les exigences de qualification définies au sous-chapitre 3.7.

Par ailleurs, ces équipements doivent être opérationnels pour les conditions environnementales normales et extrêmes des locaux automates dans lesquels ils sont implantés. Ces conditions sont définies au sous-chapitre 9.4.

0.2.1.5. Classement mécanique, électrique, contrôle-commande

Les classements mécanique et électrique ne s'appliquent pas aux équipements de contrôle-commande.

Conformément aux principes définis au sous-chapitre 3.2, le classement de contrôle-commande des équipements SAS est E1B.

0.2.1.6. Classement sismique

Le SAS comporte des fonctions requises opérables en cas de séisme. Les équipements le constituant, sont donc classés séisme 1 (SC1) opérables.

0.2.1.7. Exigence supplémentaire

Sans objet.

0.2.2. Autres exigences

0.2.2.1. Règles fondamentales de sûreté

La règle fondamentale de sûreté RFS II.4.1.a "Logiciels des systèmes électriques classés de sûreté", et plus spécialement sa partie "Logiciels des systèmes programmés classés de sûreté et non classés 1E" doit être prise en compte dans la conception et la réalisation du système SAS.

La règle fondamentale de sûreté RFS IV.2.b "Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté", et plus spécialement sa partie "matériels électriques classés de sûreté et non classés 1E" doit être prise en compte dans la conception et la réalisation du système SAS.

0.2.2.2. Directives techniques

Les directives techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/04 "Options de sûreté du projet de réacteur EPR" (et plus spécifiquement G3.4 et G3.7) doivent être prises en compte à la conception du système SAS.

0.2.2.3. Textes spécifiques EPR

Les matériels SAS doivent être conformes aux exigences énoncées dans le RCC-E complété des données de projet EPR définies dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.2.3. Agressions

0.2.3.1. Exigences — protection vis-à-vis des agressions internes

Les fonctions du système SAS doivent être protégées vis à vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.2.3.2. Exigences — protection vis-à-vis des agressions externes

Les fonctions du système SAS doivent être protégées vis à vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du système SAS.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Le système SAS doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

La mission du SAS est d'assurer la gestion des fonctions d'automatisme, des commandes manuelles, et de surveillance liée, requises F1B et F2E (définies au § 0.1.) des îlots nucléaire et conventionnel.

2. FONCTIONS ASSURÉES

Les fonctions de contrôle commande traitées par le SAS sont les suivantes :

- Traitements des données : acquisition, conditionnement et mise à disposition,
- Traitements de calculs applicatifs : régulations, élaboration de commandes individuelles et groupées (simultanées ou séquentielles), hiérarchisation des priorités de commande, élaboration d'informations diverses à destination des autres unités de contrôle-commande, etc.

- Traitements de surveillance : traitement des comptes-rendus d'état et de défauts, élaboration des alarmes et signalisations.

3. BASE DE CONCEPTION

3.1. EXIGENCES DE DISPONIBILITÉ

Les principales exigences conditionnant la disponibilité du SAS sont liées à la fiabilité et à la maintenabilité du système, qui se traduisent par :

- Limiter les pertes du SAS dues à la panne de l'un de ses composants (par la redondance de ses composants notamment),
- Faciliter l'entretien et la réparation du SAS pour réduire au minimum sa période d'indisponibilité.

3.2. PERFORMANCES REQUISES

Les exigences concernant les temps de réponse du SAS dépendent des fonctions réalisées par ce système.

Les allocations des traitements de contrôle-commande sont établies de manière à respecter l'exigence de temps de réponse de chacune des fonctions à réaliser.

3.3. EXIGENCES RELATIVES À L'ENVIRONNEMENT

Les conditions environnementales que les équipements SAS doivent supporter sont liées à la température et à l'humidité relative des locaux abritant ces matériels. Ces caractéristiques environnementales sont définies au sous-chapitre 9.4, autant pour les conditions normales que pour les conditions extrêmes.

3.4. EXIGENCE RELATIVE À L'INTERFACE HOMME-MACHINE

SAS non concerné.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

La structure et la composition du SAS sont dictées par les exigences de sûreté applicables. Par ailleurs, l'allocation des fonctions en son sein, est dictée par les exigences fonctionnelles. Ces exigences fonctionnelles portent sur :

- Le classement fonctionnel des traitements (typiquement : F1B et F2 pour le SAS),
- La division électrique (en correspondance avec celle des actionneurs et capteurs à gérer),
- La typologie des traitements à effectuer (pouvant conditionner le choix du type de cartes d'entrée/ sortie par exemple),
- La performance requise des traitements (temps de réaction, temps de propagation, précision),
- Les regroupements / exclusions de traitement, qui requièrent que certains traitements soient groupés (en regard d'un requis de perte simultanée de ces traitements lors d'un dysfonctionnement de la partie du système de CC qui les gèrent), ou inversement, que certains groupes de traitement soient gérés par des unités matérielles SAS différentes (en regard d'un requis de maintien en service d'un groupe de traitements, malgré la perte de certains autres lors du dysfonctionnement),
- La défense en profondeur.

Par ailleurs, la structure du SAS prend en compte la segmentation du procédé piloté, dicté par le nombre, l'emplacement géographique et la typologie des interfaces des actionneurs et capteurs à gérer.

Pour une fonction de sûreté donnée, différentes combinaisons sont possibles, par exemple :

[]

Afin d'éviter qu'une défaillance interne au SAS ait un effet sur plus d'un train mécanique, en général, chaque train mécanique est commandé par un sous-ensemble du SAS situé dans la même division que le train mécanique.

4.2. INSTALLATION

Les équipements SAS sont répartis dans les 4 divisions. Ils sont installés dans les [] divisions 1 à 4 du bâtiment BAS-BL, et dans les [] des bâtiments diesel.

Les équipements SAS sont répartis :

- En correspondance avec l'emplacement et la division des organes (actionneurs et capteurs) gérés,
- En correspondance avec les alimentations électriques des quatre divisions,
- Selon l'espace disponible pour leur implantation.

4.3. INTERFACE AVEC LES AUTRES FONCTIONS DE CONTRÔLE-COMMANDE

Le SAS échange des informations avec :

- Les IHM : MCS et MCP (en SdC et SdR), échanges liés à la conduite par les opérateurs,
- Les systèmes PAS, RCSL et PS : échanges liés à la gestion des automatismes de la tranche,
- Le système CCND : échanges au titre de la robustesse de la défaillance totale du contrôle-commande standard,
- Les outils d'ingénierie, de diagnostic et de maintenance décrits en section 7.6.1,
- L'instrumentation procédé : échanges liés à l'acquisition des mesures et états,
- Les cellules électriques (tableaux électriques) et les organes de commande réglants (électro-positionneurs, etc.) : échanges liés à la commande des actionneurs,
- Les systèmes "dédiés" ([]) : échanges liés à la gestion des automatismes de la tranche et surveillance d'équipements.

5. CONFIGURATIONS OPÉRATIONNELLES

La configuration (d'un point de vue matériel et fonctionnel) du SAS est indépendante de l'état de la tranche. L'allocation des traitements dépend seulement des critères fonctionnels et des principes d'allocation des traitements du système de CC. La configuration du SAS est, de ce point de vue, constante.

La configuration du SAS n'est dépendante que du dispositif suivant : en cas de défaut de fonctionnement d'une carte active, le système commute automatiquement sur la seconde carte, qui était en attente. Ce principe s'applique à toute carte redondée du SAS (cartes CPU et cartes de gestion de la communication).

6. TECHNOLOGIE

La plate-forme de contrôle commande retenue pour la réalisation du contrôle commande standard EPR est la plate-forme SPPA –T2000 développée par [].

6.1. SYSTÈME D'AUTOMATISME []

Le système [] se compose d'un ensemble d'unités d'automatisme (UA).

Une UA est composée :

- d'un couple d'unités centrales redondantes (dites AP, Automation Processor), chaque AP est indépendante et contient :
  - une alimentation (PSU, Power Supply Unit),
  - une carte CPU [] réalisant les traitements,
  - deux cartes de communication (CP [], Communication Processor) permettant d'interfacer l'UA avec les réseaux Plant Bus respectivement SAS Bus,
  - un module d'interface avec l'un des deux bus d'UA,
- de racks de cartes d'entrées/sorties contenant :
  - des modules FUM (module FUM, FUnction Module),
  - deux modules d'interface (IM [], Interface Module) permettant la connexion du rack aux deux bus d'UA,
  - un bus de fond de panier assurant la liaison entre les modules FUM et les modules d'interface,
- de deux bus d'UA (ou d'armoire, une UA pouvant être répartie sur une à deux armoires), chaque bus étant connecté à une AP et à l'ensemble des racks de modules FUM composant l'UA,
- une carte de signalisation des défauts (DEDA).

Les 2 AP redondantes communiquent entre elles au moyen d'une paire de modules d'interface IM [] (côté AP-A) et IM [] (côté AP-B), via le « redundancy link » (voir **FIG–7.3.2.1**).

Un bus d'armoire redondant et un bus de fond de panier redondant dans chaque rack assurent la communication entre les différents modules.

Les cartes d'entrées/sorties utilisées sont :

- FUM [], cartes d'acquisition capteurs TOR,
- FUM [], cartes de commande actionneurs TOR,
- FUM [], cartes d'acquisition capteurs ANA,
- FUM [], cartes d'acquisition capteurs de température,
- FUM [], cartes de commande actionneurs ANA,
- FUM [], cartes d'entrées/sorties TOR pour échanges en fil à fil,
- FUM [], cartes d'entrées/sorties ANA pour échanges en fil à fil et acquisition de signaux ANA en tension.

6.2. INTERFACES RÉSEAUX

Les UA du SAS :

- sont connectées au SAS Bus, réseau redondé matériellement et classé F1B. Ce dernier est dédié aux échanges d'informations classées jusqu'à F1B, entre automates SAS ; le premier brin SAS Bus connecte entre eux les AP-A du SAS et le second connecte entre eux les AP-B du SAS.
- sont reliées au Plant Bus, classé F2, pour les échanges d'informations à destination ou en provenance du niveau 2, et pour les échanges avec les UA PAS.

La connexion au réseau de tranche Plant Bus est indépendante des réseaux SAS Bus.

Les différents éléments sont connectés aux réseaux via des commutateurs réseaux ([]) : les CP [] sont connectés respectivement au Plant Bus et au SAS Bus via des [].

6.3. GESTION DE LA REDONDANCE

Chaque UA possède 2 AP redondantes, l'une est dite « maître » et l'autre « esclave ». Les 2 AP sont synchronisées et effectuent les traitements en parallèle, à partir des mêmes données d'entrée (informations reçues des cartes FUM et/ou des cartes CP []). Les communications réseau avec d'autres UA et avec le niveau 2 sont réparties entre les 2 cartes CP [] des AP maître et esclave.

Une défaillance détectée entraîne des séquences de diagnostic et de redémarrage des AP, et peut conduire à permuter les rôles maître/esclave des AP.

L'ensemble de cette architecture permet ainsi de répondre aux exigences de disponibilité, énoncées dans le **§ 3.1.**.

7. ALIMENTATION ÉLECTRIQUE

Les armoires SAS sont alimentées de manière redondante à partir de deux sources électriques différentes, par des convertisseurs AC/DC et DC/DC indépendants. La première source électrique est fournie par le tableau de distribution principal [] V AC triphasé, et la seconde est fournie par le tableau de sous-distribution [] V DC.

Les tableaux [] réputés « sans coupure » et alimentant les armoires SAS sont secourus par les diesels principaux (LHP/Q/R/S) dans les quatre divisions et par les diesels d'ultime secours (LJP/LJS) dans les divisions 1 et 4. Leur classement de sûreté est EE1 et leur classification sismique est la classe 1, ce qui est adapté à l'alimentation de consommateurs F1B.

Le niveau de tension automate (après transformation) est de [] V DC.

Chaque train mécanique est contrôlé par un sous-ensemble du SAS situé et alimenté par la même division que le train mécanique.

Le réglage à la tension exigée par les armoires SAS est réalisé en interne aux armoires dédiées à leur alimentation. Ces armoires d'alimentation sont situées dans [].

8. DISPOSITIONS PRISES POUR RÉALISER LES TESTS PÉRIODIQUES

Le SAS fait l'objet d'un programme d'essais périodiques conformément aux exigences de la section «généralités» du chapitre IX des RGE permettant notamment de vérifier la disponibilité des fonctions de sûreté définies au **§ 0.1.**.

9. ANALYSE DE SÛRETÉ

Le système est conforme aux exigences de sûreté spécifiés au **§ 0.** et au sous-chapitre 7.1.

10. SYSTÈME TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

FIG–7.3.2.1 CONFIGURATION D'UNE UA SAS

FIG–7.3.2.2 INTERFACE AP/FUM POUR LE SAS

SOMMAIRE

FIGURES :

.7.3.3 ARCHITECTURE DU MOYEN DE CONDUITE DE SECOURS (MCS)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

Le MCS contribue aux fonctions de sûreté supportées par le contrôle-commande (voir paragraphe 0 du sous-chapitre 7.1). Il est le moyen de conduite de secours de la tranche en cas de défaillance partielle ou totale du MCP en salle de commande principale.

Ainsi, il dispose de toutes les fonctions nécessaires et suffisantes pour atteindre et maintenir un état sûr et ce dans tous les profils de fonctionnement et conditions de fonctionnements PCC-2 à PCC-4.

Plus précisément, il permet :

- des actions de conduite incidentelle / accidentelle manuelles F1B nécessaires à l'atteinte de l'état sûr,
- la surveillance et le contrôle manuel des systèmes support des systèmes de sauvegarde indispensables à la conduite post incidentelle/ accidentelle,
- des actions manuelles F2 de lutte contre les incendies,
- la surveillance de fonctions F1B (protections automatiques et fonctions de gestion incidentelle/ accidentelle F1B).

Le MCS peut également être utilisé lors de situations RRC-A et d'accident grave tel que décrit au sous-chapitre 7.2.

Le MCS est par ailleurs la structure d'accueil de quelques fonctions F1A qui permettent :

- des actions de conduite incidentelle/ accidentelle manuelles F1A permettant d'atteindre l'état contrôlé en PCC-2 à PCC-4,
- la surveillance de fonctions F1A (protections automatiques et fonctions de gestion incidentelle/ accidentelle F1A).

Les armoires KSC ([]) MCS font l'acquisition des commandes de basculement MCP < - > MCS et SdC < - > SdR, ainsi que celles de validation des commandes du MCS.

Elles transmettent ensuite l'information du moyen de conduite actif (MCP ou MCS) ainsi que la validation des commandes du MCS aux systèmes de contrôle-commande le nécessitant.

0.2. EXIGENCES DE CONCEPTION

0.2.1. Exigences issues des classements fonctionnel et mécanique

0.2.1.1. Classement fonctionnel du système

Le MCS supporte des fonctions de conduite et contrôle de la tranche de différents classements :

- non classé,
- F2,
- F1B.

Le MCS est donc, selon les sous-chapitres 3.2 et 7.1, classé de sûreté F1B et doit satisfaire aux exigences de sûreté des paragraphes ci-après.

Les parties du MCS supportant les quelques fonctions F1A (voir **§ 0.1.** de cette section) présentent les requis de sûreté associés au classement F1A.

0.2.1.2. Critère de défaillance unique (active et passive)

Fonctions F1A :

Les parties du MCS supportant des fonctions F1A doivent être conçues pour respecter le critère de défaillance unique, au niveau du système, par l'intégration d'un degré de redondance suffisant, de structures et de dispositions adéquates. Ces parties restent ainsi opérationnelles en cas de cumul d'une défaillance unique sur une division et d'une indisponibilité d'une division pour maintenance.

Les moyens de commandes E1A du MCS sont assujettis aux exigences d'indépendance, de séparation physique et électrique entre les différentes divisions de contrôle-commande dont ils dépendent.

Fonctions F1B :

Les parties du MCS assurant des fonctions F1B doivent être conçues pour respecter le critère de défaillance unique, au niveau fonctionnel, par l'intégration d'un degré de redondance suffisant, de structures et de dispositions adéquates. Ces parties restent ainsi opérationnelles en cas de cumul d'une défaillance unique sur une division et d'une indisponibilité d'une division pour maintenance.

Les moyens de commandes et de signalisations E1B du MCS sont assujettis aux exigences d'indépendance, de séparation physique et électrique entre les différentes divisions de contrôle-commande dont ils dépendent.

Fonctions F2 et NC :

Le critère de défaillance unique n'est pas applicable pour les fonctions F2 et NC.

De plus, les commandes du MCS sont activées par les commandes de transfert MCP< - >MCS, qui sont indépendantes et séparées des moyens de commande, afin d'exclure qu'une défaillance unique ou un risque interne puisse générer des signaux et des ordres intempestifs.

0.2.1.3. Alimentations électriques secourues

L'alimentation électrique des équipements MCS requérant d'être secourus est secourue. Par ailleurs, cette alimentation est du type « sans coupure », garantissant une alimentation même pendant le basculement alimentation normale / alimentation secourue, de sorte que les fonctions de sûreté accomplies par le MCS puissent être assurées sans discontinuité de service.

Les équipements du MCS sont alimentés par la même division électrique que la division de contrôle-commande dont ils dépendent, chaque division étant indépendante électriquement et physiquement des autres de façon à garantir une absence de mode commun entre divisions.

Toutefois, certains enregistreurs hébergent des signaux en provenance de plusieurs divisions électriques : ils sont alors alimentés par une seule division.

0.2.1.4. Qualification aux conditions de fonctionnement

Les matériels supportant les fonctions du MCS sont qualifiés selon les exigences définies à la section 3.7.1, et en fonction des conditions d'ambiance normales et accidentelles auxquelles ils sont soumis lors de l'accomplissement de leur mission (cf. paragraphe 1.1.2).

0.2.1.5. Classement mécanique, électrique, contrôle-commande

Le MCS n'est pas concerné par le classement mécanique (M).

Le MCS n'est pas concerné par le classement électrique (EE).

Conformément au sous-chapitre 7.1 concernant le classement contrôle-commande :

- le matériel constitutif du MCS assurant des fonctions F1A est classé E1A,
- le matériel constitutif du MCS assurant des fonctions F1B est au moins classé E1B,
- le matériel constitutif du MCS assurant des fonctions F2 est au moins classé E2,
- le matériel constitutif du MCS assurant des fonctions non classées est au moins non classé.

0.2.1.6. Classement sismique

Le système MCS appartient à la classe sismique 1 (SC1) opérable et remplit les exigences correspondantes selon le sous-chapitre 3.2.

0.2.1.7. Exigences supplémentaires

Sans objet.

0.2.2. Autres exigences réglementaires

0.2.2.1. Règles Fondamentales de Sûreté

La Règle Fondamentale de Sûreté RFS IV.2.b « Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté » est prise en compte dans la conception et la réalisation du MCS.

0.2.2.2. Directives Techniques

Les Directives Techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/2004 "options de sûreté du projet réacteur EPR" sont prises en compte à la conception du MCS.

En particulier, la recommandation G3.5 des Directives Techniques indique que le MCS est le moyen de conduite utilisé pour la démonstration de sûreté.

0.2.2.3. Textes spécifiques EPR

Le MCS satisfait aux exigences énoncées dans le RCC-E édition décembre 2005 complétées des données de projet EPR définies dans l'additif « Cahier de données de projet EPR » (voir sous-chapitre 1.6).

0.2.3. Agressions

Le MCS est protégé contre les défaillances de mode commun pouvant résulter des agressions internes ou externes en suivant les exigences définies aux sous-chapitres 3.3 (agressions externes) et 3.4 (agressions internes).

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du MCS.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Les parties du MCS assurant des fonctions F1A et F1B font l'objet d'essais périodiques.

Les parties du MCS assurant des fonctions F2 qui ne sont pas sollicitées en continu sont aptes à la réalisation d'essais périodiques.

Le MCS doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

Le Moyen de Conduite de Secours (MCS) est le système de contrôle-commande en charge de fournir les moyens de surveillance et de commande nécessaires pour pallier une indisponibilité du MCP ou des moyens de conduite du MCP en salle de commande principale. Les moyens de surveillance et conduite supportés par le MCS ne sont pas les moyens privilégiés par l'équipe de conduite pour surveiller et conduire la tranche.

En outre, le MCS est le moyen de conduite classé de sûreté utilisé pour la démonstration de sûreté, il doit par conséquent disposer des moyens nécessaires à la conduite des situations de référence PCC-2 à PCC-4.

La mission principale du MCS est par conséquent de fournir à l'équipe de conduite les commandes et informations nécessaires pour faire face aux situations suivantes :

- En cas de courte période d'indisponibilité des moyens de conduite du MCP en salle de commande principale, voire d'indisponibilité totale du MCP en situation normale (PCC-1) : surveiller et conduire l'installation en maintenant le niveau de puissance constant.
- En cas de plus longue période d'indisponibilité des moyens de conduite du MCP en salle de commande principale, voire d'indisponibilité totale du MCP en situation normale (PCC-1) : atteindre et maintenir un état sûr de l'installation et permettre la mise à l'arrêt de l'îlot conventionnel.
- En cas d'indisponibilité des moyens de conduite du MCP en salle de commande principale, voire d'indisponibilité totale du MCP en situation PCC-2 à PCC-4 : surveiller et initier les fonctions de conduite incidentelle/ accidentelle appropriées pour passer de l'état contrôlé à l'état sûr et maintenir cet état sûr.

En cas d'incendie dans l'îlot nucléaire, si l'équipe de conduite conduit au MCS, les fonctions de lutte contre l'incendie peuvent être initiées depuis le MCS.

Le MCS peut également être utilisé lors de certaines situations RRC-A et d'accident grave ainsi qu'en cas de perte du contrôle-commande standard (conduite « noyau dur ») tel que décrit au sous-chapitre 7.2.

Lorsque le MCP est utilisé par l'équipe de conduite pour surveiller et conduire la tranche en salle de commande principale, le MCS peut être sollicité. Par exemple :

- lors des essais périodiques liés au MCS,
- en situation incidentelle/ accidentelle, pour la surveillance des principaux paramètres de sûreté et de l'état des systèmes de sûreté (recherche d'informations sur un support diversifié par rapport au MCP).

2. FONCTIONS SUPPORTÉES

Le MCS supporte les fonctions de commande et de surveillance suivantes :

- affichage des informations sur le procédé,

- fonctions de commande,
- affichage et gestion des alarmes,
- enregistrement de données analogiques,
- fonctions d'interface (filtrage, transmission de données),
- fonction de test,
- fonction de basculement (transfert de la conduite du MCP au MCS et activation de la conduite noyau dur),
- fonction d'inhibition du basculement au MCS lors du transfert de la conduite en station de repli (SdR).

Les armoires KSC MCS supportent la transmission des informations suivantes aux systèmes de contrôle-commande le nécessitant :

- transfert de la conduite du MCP au MCS incluant l'inhibition du MCS lors du transfert de la conduite en SdR,
- validation des commandes,
- gestion des alarmes,
- fonction de test.

Les armoires KSC MCS ND supportent la transmission des signalisations nécessaires au ND (noyau dur) au MCS, ainsi que la transmission des informations suivantes aux systèmes de contrôle-commande le nécessitant :

- activation de la conduite ND,
- commandes nécessaires à la conduite ND,
- fonction de test ND.

3. PRINCIPES DE CONCEPTION

3.1. DISPOSITIONS PARTICULIÈRES

Les dispositions de conception particulières qui sont prises en compte pour le MCS sont les suivantes :

- Le MCS est indépendant du MCP de sorte qu'aucun dysfonctionnement du MCP ne puisse avoir de conséquence sur le MCS.
- Lorsque le MCS est actif (voir « ETAT 2 » du paragraphe § 5. de cette section), les commandes du MCP sont désactivées.
- La perte du MCS suite à perte d'habitabilité de la salle de commande principale ne mène pas à la perte des postes opérateurs de la station de repli.
- Le MCS respecte les exigences d'interface homme-machine décrites au chapitre 17 et au paragraphe § 3.5. de cette section.

3.2. EXIGENCE DE DISPONIBILITÉ

Le MCS est conçu comme un système de contrôle-commande indépendant du MCP, afin de pouvoir être disponible en cas de perte du MCP.

Les moyens de surveillance et conduite supportés par le MCS ne sont pas les moyens privilégiés par l'équipe de conduite pour conduire la tranche.

3.3. PERFORMANCES REQUISES

Le MCS, en tant qu'équipement de niveau 2, est soumis à des exigences de performances en temps de réponse principalement liées aux facteurs humains. Ainsi, les informations issues du niveau 1 et la prise en compte des actions opérateurs au niveau 1 sont affichées au MCS dans un délai de l'ordre de la seconde.

3.4. EXIGENCES D'ENVIRONNEMENT

Le MCS est installé dans la salle de commande principale, les conditions d'environnement auxquelles il est soumis sont donc celles de ce local.

On distingue deux catégories :

- Les conditions d'environnement auxquelles les équipements sont soumis. Ceci inclut la température et l'humidité relative de la pièce.
- La contribution de l'équipement aux conditions ambiantes. Cette catégorie inclut le niveau de bruit et la chaleur dégagée.

3.5. EXIGENCES LIÉES À L'INTERFACE HOMME-MACHINE

Outre les performances indiquées au paragraphe **§ 3.3.** de cette section, l'aménagement du MCS prend en compte les critères ergonomiques (compatibilité avec les tâches de l'opérateur) ainsi que les contraintes d'indépendance (principalement séparation physique) des équipements appartenant à et alimentés par des divisions différentes et soumis à des niveaux de classement différents.

La liste détaillée des différentes informations et commandes qui sont implantées au MCS est déterminée en analysant les tâches qui doivent être accomplies sur ce moyen de conduite. Des éléments liés aux moyens situés au MCS peuvent être trouvés dans les chapitres 13 et 17.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Le MCS est composé de 3 panneaux horizontaux (voir figure **FIG–7.3.3.1**) regroupant :

- sur la partie haute : les alarmes,
- au centre : les signalisations, des voyants d'état, des mesures et les acquittements des alarmes,
- sur la partie basse, directement accessible aux opérateurs : les commandes et leurs signalisations, des acquittements ainsi que quelques voyants d'état.

Le matériel utilisé est décrit au **§ 6.** de cette section. Un découpage vertical (voir figure **FIG–7.3.3.2**) permet quant à lui un regroupement fonctionnel de ces moyens de commande et d'information. On trouve ainsi au MCS onze Zones Fonctionnelles (ZF).

4.2. INSTALLATION

Le MCS est installé dans la salle de commande principale.

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CONTRÔLE-COMMANDE

Le MCS présente deux types d'interfaces :

- l'interface avec l'opérateur dans la salle de commande principale,
- l'interface avec le niveau d'automatisme (PAS, SAS de tranche, SAS RRC-B, PS, CCND).

L'interface avec le niveau d'automatisme est réalisé au moyen des armoires KSC MCS et/ou KSC MCS ND, comme expliqué au § 5. de cette section.

5. MODES DE FONCTIONNEMENT

Le MCP, en salle de commande principale, est le moyen de conduite privilégié de la tranche.

L'équipe de conduite opère depuis le MCS en cas d'indisponibilité des postes opérateurs en salle de commande principale ou en cas d'indisponibilité globale du MCP.

En cas de perte de la salle de commande principale due à un événement interne (comme le feu), le MCS et les moyens de commande du MCP en salle de commande principale ne sont plus disponibles. Dans cette situation, l'équipe de conduite utilise les moyens de commande MCP de la station de repli.

Les principes de transfert entre ces différents moyens de conduite sont régis par des procédures de conduite. Les opérateurs disposent pour cela de deux séries de commutateurs :

- [] commutateurs situés au MCS en Salle de commande principale permettent de basculer du MCP au MCS (et vice-versa),
- [] commutateurs (dédiés au MCS) situés en station de repli permettent de basculer de la salle de commande principale à la station de repli (et vice-versa).

En effet, trois commutateurs permettent, [], de pallier une défaillance matérielle tout en étant capable de choisir le moyen de commande actif. Ainsi, en l'absence de défaillance, le basculement de deux commutateurs sur trois suffit à initier un transfert.

La commutation MCP <-> MCS :

L'activation des commandes du MCS est réalisée [] depuis le MCS en positionnant les [] commutateurs MCP/MCS en position MCS.

Il est réalisable :

- quel que soit l'état de la tranche,
- si la conduite se fait en salle de commande principale, c'est-à-dire que les commutateurs SdC/ SdR doivent être en position SdC (voir ci-dessous).

La logique de transfert MCP vers MCS permet d'obtenir dans cet ordre les deux états suivants des commandes et d'information :

- ETAT 1 - *MCS passif / MCP actif*
  - la signalisation au MCS est opérationnelle et cohérente avec le MCP,
  - les mesures sur indicateurs et enregistreurs sont opérationnelles au MCS et cohérentes avec le MCP,
  - les alarmes sont visibles et auto-acquittées (acquittement sonore et visuel) au MCS,
  - les commandes au MCS sont inhibées (exceptées les commandes de basculement et de test).
- ETAT 2 - *MCS actif / MCP inactif*
  - la signalisation au MCS est opérationnelle et cohérente avec le MCP (lorsque celui-ci est toujours opérationnel),
  - les mesures sur indicateurs et enregistreurs sont opérationnelles au MCS et cohérentes avec le MCP (lorsque celui-ci est toujours opérationnel),

- les alarmes sont visibles et acquittables au MCS (acquittement sonore et acquittement visuel),
- les commandes au MCS sont opérationnelles,
- les commandes au MCP sont inhibées.

La logique de transfert du MCS vers le MCP permet d'obtenir dans l'ordre inverse chacun de ces deux états.

La commutation Salle de Commande principale (SdC) <-> Station de Repli (SdR) :

[]

La logique de transfert de la station de repli vers la salle de commande principale permet de réactiver la commutation MCP < - > MCS en salle de commande principale.

Les armoires KSC MCS font l'acquisition des commandes suivantes :

- commutation MCP< - >MCS et SdC< - >SdR,
- validation des commandes du MCS,
- activation du test MCS,
- acquittement visuel et sonore des alarmes du MCS.

En fonction de l'état de ces commandes, ces armoires élaborent ensuite les informations suivantes qu'elles transmettent aux autres systèmes de contrôle-commande (PAS, SAS de tranche, etc.) :

- moyen de conduite actif : MCP ou MCS,
- validation des commandes du MCS,
- activation du test MCS,
- acquittement visuel et sonore des alarmes du MCS.

En raison des ces missions, les armoires KSC MCS et par extension le système KSC, sont classées F1A.

L'activation de la conduite Noyau Dur (ND)

L'activation de la conduite au noyau dur est réalisée [] depuis le MCS, en basculant les trois commutateurs « activation ND ».

La logique de transfert conduite ND inactive vers conduite ND active permet d'obtenir dans cet ordre les deux états suivants des informations remontées au MCS :

- ETAT 1 — *Conduite ND inactive*
  - les signalisations du MCS nécessaires au ND sont interceptées par l'armoire KSC MCS ND qui ne remonte au MCS que celles en provenance du SPPA-T2000.
- ETAT 2 — *Conduite ND active*
  - les signalisations du MCS nécessaires au ND sont interceptées par l'armoire KSC MCS ND qui ne remonte au MCS que celles en provenance du CCND.

Dans ces deux états, les commandes nécessaires au ND passées depuis le MCS sont interceptées par l'armoire KSC MCS ND qui les redistribue à la fois au SPPA-T2000, et au CCND ou au PS.

La logique de transfert conduite ND inactive vers conduite ND active permet d'obtenir dans l'ordre inverse chacun de ces deux états.

Ainsi, les armoires KSC MCS ND font l'acquisition des commandes suivantes :

- commutation vers « activation ND »,
- commandes du MCS nécessaires à la conduite ND,
- activation du test ND.

En fonction de l'état de ces commandes, ces armoires déterminent les informations du système de contrôle-commande (SPPA-T2000 ou CCND) à remonter au MCS et elles transmettent ensuite les informations suivantes :

- information conduite ND active ou non transmise aux CCND, PS, SPPA-T2000 et aux actionneurs commandés par le CCND,
- activation du test ND transmis au CCND,
- commandes du MCS nécessaires à la conduite ND transmises à la fois au SPPA-T2000 et au CCND ou au PS.

6. TECHNOLOGIE

La solution technique de référence pour le MCS est basée sur l'utilisation d'une technologie conventionnelle.

Toutefois, l'utilisation de composants électriques programmés (CEP) n'est pas exclue ponctuellement : enregistreurs ou afficheurs par exemple.

Comme indiqué au **§ 4.1.** de cette section, on distingue plusieurs familles de matériels au MCS :

6.1. LES BOÎTIERS D'ALARMES

Les alarmes sont présentées sous forme de verrines de couleur de [] mm. On les trouve exclusivement sur la [] MCS (voir **§ 4.1.** de cette section).

Il existe [] couleurs différentes de verrines permettant de distinguer la gravité des alarmes : [].

Pour renforcer l'apparition et la disparition d'alarmes, [] signalisations 'sonores' sont utilisées au MCS.

6.2. LES BOÎTIERS DE SIGNALISATIONS

Les boîtiers de signalisations sont des boîtiers de [] mm comportant des LED de couleurs.

Ces boitiers comportent [] couples de LED []. On les retrouve sur le panneau central et le panneau du bas (voir **§ 4.1.** de cette section).

6.3. LES BOÎTIERS DE VOYANTS D'ÉTAT

Les voyants d'état, de couleur [], donnent des informations sur :

[]

6.4. LES BOITIERS DE MESURES

Les mesures sont présentées à l'opérateur soit sur indicateur, soit sur enregistreur.

Les indicateurs sont de [] types :

[]

6.5. LES BOITIERS DE COMMANDES, DE CHOIX ET D'ACQUITTEMENTS

Les commandes et acquittements sont portés par [] grandes familles :

[]

7. ALIMENTATION ÉLECTRIQUE

Le mode de polarisation des boutons poussoirs, LED, afficheurs numériques, etc. diffère en fonction du système de contrôle-commande avec lequel ils sont en interface :

[]

Ainsi, pour ces éléments de signalisation, aucune alimentation externe supplémentaire n'est nécessaire.

Seuls les [] nécessitent une alimentation externe supplémentaire. Ils sont alimentés par des sources de courant cohérentes avec le système de contrôle-commande avec lequel ils sont en interface. Des dispositions d'isolement sont prises pour maintenir la séparation électrique des équipements du MCS appartenant à des divisions différentes ou à des parties de niveaux de classement différents.

Certains enregistreurs hébergent des signaux en provenance de plusieurs divisions électriques : ils sont alors alimentés par une seule division.

8. DISPOSITIONS PRISES POUR LA RÉALISATION D'ESSAIS PÉRIODIQUES

Le MCS fait l'objet d'essais périodiques, selon le paragraphe **§ 0.3.3.** de cette section.

Les essais périodiques sont réalisés dans l'ETAT 1 en basculant le commutateur de « Test Lampes ».

Le test de chacune des fonctions de sûreté devant faire l'objet d'essais périodiques permettra de vérifier l'acquisition par les automates de niveau 1 de l'ordre de commande et l'intégrité des chaînes de retour d'information (signalisations, voyants d'état, mesures…) entre les automatismes de niveau 1 et le MCS.

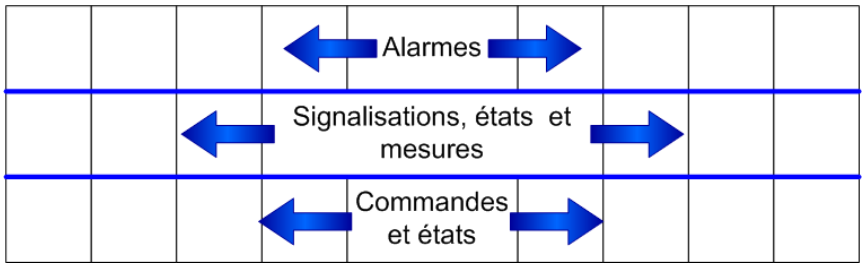
9. ANALYSE DE SÛRETÉ

Le MCS est conforme aux exigences de sûreté dont il est redevable.

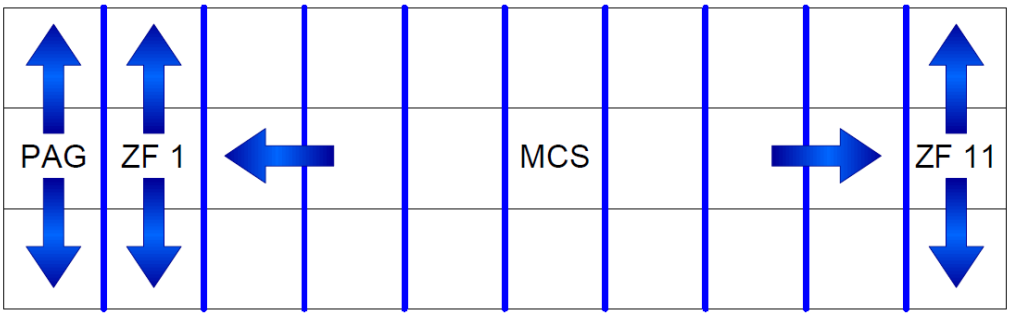
10. TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

FIG–7.3.3.1 DÉCOUPAGE HORIZONTAL DU MCS (PANNEAUX)



FIG–7.3.3.2 DECOUPAGE VERTICAL DU MCS (ZONES FONCTIONNELLES)



SOMMAIRE

.7.3.4 ARCHITECTURE DU PUPITRE INTER POSTES OPÉRATEURS (PIPO)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

Le Pupitre Inter Postes Opérateurs (PIPO) est un panneau de commande de technologie conventionnelle localisé en salle de commande principale entre les deux postes opérateurs principaux.

Il permet aux opérateurs :

[]

0.2. EXIGENCES RELATIVES À LA CONCEPTION

0.2.1. Exigences issues des classements fonctionnel et mécanique

0.2.1.1. Classement fonctionnel du système

Le PIPO supporte des fonctions de conduite et contrôle de la tranche de différents classements :

- F1A,
- F2,
- non classé.

Le PIPO est donc, selon les sous-chapitres 3.2 et 7.1, classé de sûreté F1A et satisfait aux exigences de sûreté des paragraphes ci-après.

0.2.1.2. Critère de défaillance unique (active et passive)

Fonctions F1A

Les parties du PIPO supportant des fonctions F1A sont conçues pour respecter le critère de défaillance unique, au niveau du système, par l'intégration d'un degré de redondance suffisant, de structures et de dispositions adéquates. Ces parties restent ainsi opérationnelles en cas de cumul d'une défaillance unique sur une division et d'une indisponibilité d'une division pour maintenance.

Les moyens de commandes E1A du PIPO sont assujettis aux exigences d'indépendance, de séparation physique et électrique entre les différentes divisions de contrôle-commande dont ils dépendent.

Fonctions F2 et NC

Le critère de défaillance unique n'est pas applicable pour les fonctions F2 et NC.

0.2.1.3. Alimentations électriques secourues

L'alimentation électrique des équipements du PIPO requérant d'être secourus est secourue.

Les équipements du PIPO sont alimentés par la même division électrique que la division de contrôle-commande dont ils dépendent, chaque division étant indépendante électriquement et physiquement des autres de façon à garantir une absence de mode commun entre divisions.

0.2.1.4. Qualification aux conditions de fonctionnement

Les matériels supportant les fonctions du PIPO sont qualifiés selon les exigences définies à la section 3.7.1, et en fonction des conditions d'ambiance normales et accidentelles auxquelles ils sont soumis lors de l'accomplissement de leur mission (cf. paragraphe 1.1.2).

0.2.1.5. Classements mécanique, électrique, contrôle-commande

Le PIPO n'est pas concerné par le classement mécanique (M).

Le PIPO n'est pas concerné par le classement électrique (EE).

Conformément au sous-chapitre 7.1 concernant le classement contrôle-commande :

- le matériel constitutif du PIPO assurant des fonctions F1A est classé E1A,
- le matériel constitutif du PIPO assurant des fonctions F2 est au moins classé E2,
- le matériel constitutif du PIPO assurant des fonctions non classées est au moins non classé.

0.2.1.6. Classement sismique

Le PIPO appartient à la classe sismique 1 (SC1) opérable et remplit les exigences correspondantes, selon le sous-chapitre 3.2.

0.2.1.7. Exigences supplémentaires

Sans objet.

0.2.2. Autres exigences réglementaires

0.2.2.1. Règles fondamentales de sûreté

La Règle Fondamentale de Sûreté RFS IV.2.b "Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté" est prise en compte dans la conception et la réalisation du PIPO.

0.2.2.2. Directives techniques

Les Directives Techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/2004 "options de sûreté du projet réacteur EPR" sont prises en compte à la conception du PIPO (en particulier la G3.4).

0.2.2.3. Textes spécifiques EPR

Le PIPO satisfait aux exigences énoncées dans le RCC-E édition décembre 2005 complétées des données de projet EPR définies dans l'additif « Cahier de données de projet EPR » (voir sous-chapitre 1.6).

0.2.3. Agressions

Le PIPO est protégé contre les défaillances de mode commun pouvant résulter des agressions internes ou externes en suivant les exigences définies aux sous-chapitres 3.3 (agressions externes) et 3.4 (agressions internes).

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du PIPO.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Les parties du PIPO assurant des fonctions F1A font l'objet d'essais périodiques.

Les parties du PIPO assurant des fonctions F2 qui ne sont pas sollicitées en continu sont aptes à la réalisation d'essais périodiques.

Le PIPO doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

Le PIPO est utilisé dans le cadre de ses fonctions de sûreté en cas :

- de perte d'habitabilité de la salle de commande principale dans le cadre du transfert de la conduite de la tranche à la station de repli,
- de situation accident grave : perte totale des alimentations électriques extérieures et intérieures,
- de situation RRC-A : perte totale d'alimentation en eau des GV,
- de situation RRC-A cumulée à la perte de la partie numérique du système de protection.

2. FONCTIONS SUPPORTÉES

Le PIPO supporte les fonctions de commande suivantes :

[]

3. PRINCIPES DE CONCEPTION

3.1. DISPOSITIONS PARTICULIÈRES

Les dispositions de conception particulières qui sont prises en compte pour le PIPO sont les suivantes :

- La perte du PIPO en cas d'inhabitabilité de la salle de commande principale ne mène pas à la perte des postes opérateurs de la station de repli.
- Le basculement en SdR inhibe les commandes d'isolement enceinte phase 2.
- Le PIPO respecte les exigences d'interface homme-machine décrites au chapitre 17 et au paragraphe § 3.5. de cette section.

3.2. EXIGENCE DE DISPONIBILITÉ

Le PIPO est conçu comme un système de contrôle-commande indépendant du MCP, afin que ses fonctions de sûreté soient disponibles en cas de perte du MCP.

Le PIPO est conçu comme un système de contrôle-commande indépendant du MCS, afin que ses fonctions de sûreté soient disponibles en cas de perte du MCS.

Le PIPO est conçu comme un système de contrôle-commande indépendant des parties numériques des systèmes de contrôle-commande.

3.3. PERFORMANCES REQUISES

L'utilisation des liaisons câblées pour la transmission des données, ainsi que l'absence de traitement informatisé de données, assurent les performances en temps de réponse requises.

3.4. EXIGENCES D'ENVIRONNEMENT

Le PIPO est installé dans la salle de commande principale, les conditions d'environnement auxquelles il est soumis sont donc celles de ce local.

On distingue deux catégories :

- Les conditions d'environnement auxquelles les équipements sont soumis. Ceci inclut la température et l'humidité relative de la pièce.
- La contribution de l'équipement aux conditions ambiantes. Cette catégorie inclut le niveau de bruit et la chaleur dégagée.

3.5. EXIGENCES LIÉES À L'INTERFACE HOMME-MACHINE

L'aménagement du PIPO prend en compte les critères ergonomiques (compatibilité avec les tâches de l'opérateur) ainsi que les contraintes d'indépendance (principalement séparation physique) des équipements appartenant à et alimentés par des divisions différentes et soumis à des niveaux de classement différents.

La liste détaillée des différentes commandes qui sont implantées au PIPO est déterminée en analysant les tâches qui sont accomplies sur ce moyen de conduite.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Le PIPO est composé de dispositifs de commande conventionnels (boutons poussoirs, commutateurs, ...) qui sont reliés par des liaisons fil à fil en amont du niveau 0 de l'architecture du contrôle-commande ou au niveau 1 de l'architecture de contrôle-commande.

Le matériel est décrit au § 6. de cette section.

4.2. INSTALLATION

Le PIPO est installé dans la salle de commande principale entre les deux postes opérateurs principaux.

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CONTRÔLE-COMMANDE

Le PIPO présente trois types d'interfaces :

- l'interface avec l'opérateur dans la salle de commande principale,
- l'interface avec le niveau 1 (niveau d'automatisme),
- l'interface avec le matériel électrique.

5. MODES DE FONCTIONNEMENT

A l'exception des commandes d'isolement enceinte phase 2 qui sont inhibées en cas de passage en SdR, le PIPO n'est ni soumis à la commutation MCP/MCS ni à la commutation SdC/SdR (voir section 7.3.3).

6. TECHNOLOGIE

La technologie du PIPO est basée sur les moyens de commande utilisés au MCS (voir section 7.3.3).

Plus particulièrement, on utilise des boîtiers de [] mm comportant :

- un bouton poussoir de gros diamètre ([]) capoté,

ou

- un commutateur de choix à plusieurs positions.

7. ALIMENTATION ÉLECTRIQUE

Les équipements du PIPO sont alimentés directement par le niveau 1 et ne nécessitent pas d'alimentation externe supplémentaire.

Des dispositions d'isolement sont prises pour maintenir la séparation électrique des équipements du PIPO appartenant à des divisions différentes ou à des parties de niveaux de classement différents.

8. DISPOSITIONS PRISES POUR LA RÉALISATION D'ESSAIS PÉRIODIQUES

Le PIPO fait l'objet d'essais périodiques, selon le **§ 0.3.3.** de cette section.

Des dispositions sont prises pour bloquer les signaux de commande pendant les essais, de façon à tester la ligne de commande de l'actionneur sans commander physiquement ce dernier.

9. ANALYSE DE SÛRETÉ

Le PIPO est conforme aux exigences de sûreté dont il est redevable.

10. TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

SOMMAIRE

.7.3.5 ARCHITECTURE DU PANNEAU DE SIGNALISATION INTER-SYNOPTIQUES (PSIS)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

Le PSIS contribue aux fonctions de sûreté supportées par le contrôle-commande (voir paragraphe 0 du sous-chapitre 7.1). Il constitue l'interface homme-machine classée de sûreté permettant :

- L'affichage de l'indisponibilité détectée par le « signe de vie » (F1B) d'un ou plusieurs postes de conduite informatisés ayant des conséquences sur l'organisation de l'équipe de conduite et conditionnant éventuellement la nécessité de conduire l'installation à partir du MCS,
- L'affichage de l'information (F2) informant les opérateurs que le système de protection (PS) n'est plus en mesure d'assurer ses fonctions de sûreté et leur permettant ainsi de conduire, au MCP, les situations RRC-A d'ATWS avec perte PS,
- L'affichage de l'information (F2) indiquant aux opérateurs que le SPPA-T2000 n'est plus en mesure d'assurer ses fonctions de sûreté et leur permettant ainsi de conduire au MCP.

0.2. EXIGENCES RELATIVES À LA CONCEPTION

0.2.1. Exigences issues des classements fonctionnel et mécanique

0.2.1.1. Classement fonctionnel du système

Le PSIS supporte des fonctions de contrôle de la tranche de différents classements :

- F1B,
- F2.

Le PSIS est donc, selon les sous-chapitre 3.2 et sous-chapitre 7.1, classé de sûreté F1B et satisfait aux exigences de sûreté des paragraphes ci-après.

0.2.1.2. Critère de défaillance unique (active et passive)

Fonctions F1B

Les parties du PSIS assurant des fonctions F1B sont conçues pour respecter le critère de défaillance unique, au niveau fonctionnel, par l'intégration d'un degré de redondance suffisant, de structures et de dispositions adéquates. Ces parties restent ainsi opérationnelles en cas de cumul d'une défaillance unique sur une division, et d'une indisponibilité d'une division pour maintenance.

Les moyens de signalisations E1B du PSIS sont assujettis aux exigences d'indépendance, de séparation physique et électrique entre les différentes divisions de contrôle-commande dont ils dépendent.

Fonctions F2

Le critère de défaillance unique n'est pas applicable pour les fonctions F2.

0.2.1.3. Alimentations électriques secourues

Les fonctions F1B et F2 du PSIS sont assurées en cas de perte des alimentations électriques.

0.2.1.4. Qualification aux conditions de fonctionnement

Les matériels supportant les fonctions du PSIS sont qualifiés selon les exigences définies au sous-chapitre 3.7, et en fonction des conditions d'ambiance normales et accidentelles auxquelles ils sont soumis lors de l'accomplissement de leur mission (cf. paragraphe 1.3.4).

0.2.1.5. Classements mécanique, électrique, contrôle-commande

Le PSIS n'est pas concerné par le classement mécanique (M).

Le PSIS n'est pas concerné par le classement électrique (EE).

Selon le sous-chapitre 7.1 concernant le classement contrôle-commande (E):

- le matériel constitutif du PSIS assurant des fonctions F1B est au moins classé E1B,
- le matériel constitutif du PSIS assurant des fonctions F2 est au moins classé E2.

0.2.1.6. Classement sismique

Le PSIS appartient à la classe sismique 1 (SC1) opérable et remplit les exigences correspondantes selon le sous-chapitre 3.2.

0.2.1.7. Exigences supplémentaires

Sans objet.

0.2.2. Autres exigences réglementaires

0.2.2.1. Règles Fondamentales de Sûreté

La Règle Fondamentale de Sûreté RFS IV.2.b "Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté" est prise en compte dans la conception et la réalisation du PSIS.

0.2.2.2. Directives Techniques

Les Directives Techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/2004 "options de sûreté du projet réacteur EPR" (voir sous-chapitre 1.7) sont prises en compte à la conception du PSIS.

En particulier, la recommandation G3.5 des Directives Techniques indique que les moyens mis en oeuvre pour la détection et la signalisation des défaillances de fonctions et d'équipements F2 essentiels de l'interface homme-machine informatisée doivent satisfaire aux exigences applicables aux fonctions et équipements F1B.

0.2.2.3. Textes spécifiques EPR

Le PSIS satisfait aux exigences énoncées dans le RCC-E édition décembre 2005 complétées des données de projet EPR définies dans l'additif "Cahier de données de projet EPR" (voir sous–chapitre 1.6).

0.2.3. Agressions

Le PSIS est protégé contre les défaillances de mode commun pouvant résulter des agressions internes ou externes en suivant les exigences définies aux sous-chapitres 3.3 (agressions externes) et 3.4 (agressions internes).

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Le PSIS fait l'objet d'essais pré-opérationnels, permettant de vérifier après montage la conformité des performances du système avec les exigences de conception.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Les parties du PSIS assurant des fonctions F1B et F2 (non sollicitées en continu) font l'objet d'essais périodiques.

1. MISSIONS

Le PSIS est l'interface homme-machine classée de sûreté permettant de remonter les signaux de surveillance des principaux systèmes de contrôle-commande et d'orienter ainsi l'équipe de conduite.

2. FONCTIONS SUPPORTÉES

Le PSIS supporte les fonctions de surveillance suivantes :

[]

3. PRINCIPES DE CONCEPTION

3.1. DISPOSITIONS PARTICULIÈRES

Sans objet.

3.2. EXIGENCE DE DISPONIBILITÉ

La partie du PSIS affichant les informations issues du « signe de vie » du MCP est conçue de façon à pouvoir afficher ses informations en cas de perte du MCP.

La partie du PSIS affichant les informations issues de la surveillance du SPPA-T2000 est conçue de façon à pouvoir afficher ses informations en cas de perte du SPPA-T2000.

La partie du PSIS affichant les informations issues de la surveillance du PS est conçue de façon à pouvoir afficher ses informations en cas de perte du PS.

3.3. PERFORMANCES REQUISES

Le PSIS, en tant qu'équipement de niveau 2, est soumis à des exigences de performances en temps de réponse principalement liées aux facteurs humains. Ainsi, les informations issues du niveau 1 sont affichées au PSIS dans un délai de l'ordre de la seconde.

3.4. EXIGENCES D'ENVIRONNEMENT

Le PSIS est installé dans la salle de commande principale, les conditions d'environnement auxquelles il est soumis sont donc celles de ce local.

On distingue deux catégories :

- Les conditions d'environnement auxquelles les équipements sont soumis. Ceci inclut la température et l'humidité relative de la pièce.
- La contribution de l'équipement aux conditions ambiantes. Cette catégorie inclut le niveau de bruit et la chaleur dégagée.

3.5. EXIGENCES LIÉES À L'INTERFACE HOMME-MACHINE

L'aménagement du PSIS prend en compte les critères ergonomiques (compatibilité avec les tâches de l'opérateur), les contraintes d'indépendance (principalement séparation physique) des équipements appartenant à et alimentés par des divisions différentes ou soumis à des niveaux de classement différents.

La liste détaillée des différentes informations qui sont implantées au PSIS est déterminée en analysant les tâches qui sont accomplies sur ce moyen de conduite.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Le PSIS est constitué d'un panneau composé de plusieurs signalisations regroupées par fonction de surveillance.

Le matériel est décrit au § 6. de cette section.

4.2. INSTALLATION

Le PSIS est installé dans la salle de commande principale entre les deux écrans synoptiques centraux.

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CONTRÔLE-COMMANDE

Le PSIS présente deux types d'interfaces :

- l'interface avec l'opérateur dans la salle de commande principale,
- l'interface avec le niveau d'automatisme (PS, SPPA-T2000, CCND).

La remontée des signalisations lumineuses en provenance du SPPA—T2000 passe par les armoires KSC MCS.

5. MODES DE FONCTIONNEMENT

Le PSIS est toujours opérationnel.

Chaque voyant possède deux modes de fonctionnement :

- Allumé,
- Eteint.

6. TECHNOLOGIE

La solution technique de référence pour le PSIS est basée sur l'utilisation d'une technologie conventionnelle.

Les signalisations sont réalisées au moyen de verrines de différentes couleurs de [] mm.

7. ALIMENTATION ÉLECTRIQUE

Les éléments du PSIS sont reliés par des liaisons fil à fil au niveau 1 de l'architecture du contrôle-commande et ne nécessitent pas d'alimentation externe.

Des dispositions d'isolement sont prises pour maintenir la séparation électrique des équipements du PSIS appartenant à des divisions différentes ou à des parties de niveaux de classement différents.

8. DISPOSITIONS PRISES POUR LA RÉALISATION D'ESSAIS PÉRIODIQUES

Le PSIS fait l'objet d'essais périodiques, selon le **§ 0.3.3.** de cette section.

Les essais périodiques sont réalisés [].

9. ANALYSE DE SÛRETÉ

Le PSIS est conforme aux exigences de sûreté dont il est redevable.

10. TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

SOMMAIRE

FIGURES :

.7.3.6 FONCTION DE GESTION DE PRIORITÉS ET DE CONTRÔLE DE L'ACTIONNEMENT (PACS)

0. EXIGENCES DE SÛRETÉ

Le PACS est l'entité fonctionnelle chargée de la commande et de la surveillance du mouvement de l'actionneur, pour toutes les situations de tranche.

En regard de la sûreté, le PACS doit assurer les fonctions d'automatisation liées à la commande et à la surveillance de l'actionneur participant à l'accomplissement d'une fonction de sûreté.

Les fonctions du PACS sont les suivantes (voir détail de ces fonctions et de leur répartition au § 2.) :

- *Gestion de priorité des commandes*, qui se décline en deux sous-fonctions : l'une hiérarchisant les commandes traitées par l'automate (PAS, SAS, SAS RRC-B, CCAG) et l'autre hiérarchisant les commandes traitées par la cellule électrique alimentant l'actionneur en énergie,
- *Commande de l'organe de coupure*,
- *Surveillance de l'actionneur*,
- *Protection essentielle des composants.*

Ces fonctions sont gérées par deux équipements, comme suit :

- Automate PAS, SAS, SAS RRC-B ou CCAG (selon requis fonctionnel): assure une partie de la gestion de la fonction "*Gestion de priorité des commandes*", et la gestion de la fonction "*surveillance de l'actionneur*",
- Cellule électrique : assure l'autre partie de la gestion de la fonction *"Gestion de priorité des commandes",* et la gestion de la fonction *"Commande de l'organe de coupure"* et de la fonction *" Protection essentielle des composants"*.

Au titre des fonctions que gère le PACS, il est requis du même niveau de classement fonctionnel que celui de la commande la plus classée pilotant l'actionneur. Par exemple, le PACS d'un actionneur assujetti à une commande de delestage (ou à une commande RPR) F1A aura lui-même un classement F1A.

Les exigences de sûreté assujettissant le PACS s'appliquent conjointement au PAS / SAS / SAS RRC-B / CCAG et à la cellule électrique, comme suit :

- PACS F2 : exigences identiques à celles définies en section :
  - 7.3.2 (pour le SAS, lorsque actionneur classé F2E) paragraphe "Exigences de sûreté", autant pour les fonctions PACS gérées par le SAS que pour celles gérées par la cellule (hormis exigences de classement détaillées aux paragraphes "classement mécanique, électrique et contrôle-commande" et "classement sismique" ci-après, applicables uniquement aux cellules),
  - 7.4.2 (pour le PAS, lorsque actionneur classé F2N) paragraphe "Exigences de sûreté", autant pour les fonctions PACS gérées par le PAS que pour celles gérées par la cellule (hormis exigences de classement détaillées aux paragraphes "classement mécanique, électrique et contrôle-commande" et "classement sismique" ci-après, applicables uniquement aux cellules),
  - 7.4.4 (pour le CCAG) paragraphe "Prescriptions de sûreté", autant pour la fonction PACS gérée par le CCAG (surveillance de l'actionneur) que pour celles gérées par la cellule (hormis exigences de classement détaillées aux paragraphes "classement mécanique, électrique et contrôle-commande" et "classement sismique" ci-après, applicables uniquement aux cellules),

- 7.4.5 (pour le SAS RRC-B) paragraphe "Exigences de sûreté", autant pour les fonctions PACS gérées par le SAS RRC-B que pour celles gérées par la cellule (hormis exigences de classement détaillées aux paragraphes "classement mécanique, électrique et contrôle-commande" et "classement sismique" ci-après, applicables uniquement aux cellules),

- PACS F1B : exigences identiques à celles définies en section 7.3.2 paragraphe "Exigences de sûreté", autant pour les fonctions PACS gérées par le SAS que pour celles gérées par la cellule (hormis exigences de classement détaillées aux paragraphes "classement mécanique, électrique et contrôle-commande" et "classement sismique" ci-après, applicables uniquement aux cellules, selon principe énoncé par la remarque « Important » ci-dessous),
- PACS F1A :
  - Pour les fonctions PACS gérées par le PAS (actionneur non assujetti à des automatismes et commandes F1B ou F2E) : exigences définies en section 7.4.2 paragraphe "Exigences de sûreté",
  - Pour les fonctions PACS gérées par le SAS (actionneur assujetti à des automatismes et commandes F1B ou F2E) : exigences définies en section 7.3.2 paragraphe "Exigences de sûreté",
  - Pour les fonctions PACS gérées par le SAS RRC-B (actionneur assujetti à des automatismes et commandes F2E Accident Grave) : exigences définies en section 7.4.5 paragraphe "Exigences de sûreté",
  - Pour la fonction PACS gérée par le CCAG (actionneur assujetti à des automatismes et commandes F2E AG) : exigences définies en section 7.4.4 paragraphe "Prescriptions de sûreté",
  - Pour les fonctions PACS gérées par la cellule (fonctions F1A) : selon présent paragraphe (voir « Note » ci dessous),
- PACS NC (actionneur NC) : pas d'exigence de sûreté.

Classement : les principes de classement sont énoncés au sous-chapitre 3.2, et sont déclinés pour le PACS aux paragraphes "Classement fonctionnel du système", "Classement mécanique, électrique, contrôle-commande" et "Classement sismique" ci-après.

Indépendance : appliquée au PACS, l'exigence d'indépendance pouvant exister entre entités de commande relevant de niveaux de défense en profondeur requis indépendants (conformément à la note [5]) se traduit par la mise en œuvre :

- D'une ligne de commande dédiée à chaque unité d'automatisme (acheminée par liaison filaire),
- D'une fonction de vote entre unités d'automatisme requises indépendantes, reposant sur une technologie non informatisée.

Diversification : appliquée au PACS, l'exigence de diversification pouvant être requise par les études EPS se traduit par la mise en œuvre d'unités d'automatisme reposant sur des plate-formes diversifiées (Teleperm TXS et SPPA-T2000).

Nota : pour alléger la lecture, on ne définit dans la présente section 7.3.6 que les exigences de sûreté applicables aux fonctions PACS F1 ou F2 que gèrent la cellule électrique. Les exigences applicables aux unités d'automatisme F2 et F1B (PAS / SAS / SAS RRC-B et CCAG) sont définies dans leurs sections respectives (selon ci-dessus).

0.1. FONCTIONS DE SÛRETÉ

Le PACS participe aux trois fonctions fondamentales de sûreté (maîtrise de la réactivité, évacuation de la puissance résiduelle et confinement des substances radioactives) au titre de la gestion des

traitements de contrôle-commande assurant la commande et la surveillance de chacun des actionneurs participant à une fonction de sûreté.

Le PACS doit assurer les fonctions d'automatisme F1A (pour les fonctions non gérées par le PS), et à ce titre est classé E1A.

0.2. EXIGENCES RELATIVES À LA CONCEPTION

Au titre des fonctions F1A dont il gère les traitements d'automatisme, le PACS doit satisfaire aux exigences suivantes.

0.2.1. EXIGENCES ISSUES DES CLASSEMENTS FONCTIONNEL ET MÉCANIQUE

0.2.1.1. CLASSEMENT FONCTIONNEL DU SYSTÈME

Le PACS doit être classé de sûreté, conformément au principe de classement indiqué au sous-chapitre 3.2.

0.2.1.2. CRITÈRE DE DÉFAILLANCE UNIQUE (ACTIVE)

Conformément à la note [5], seul le critère de défaillance unique active s'applique au contrôle-commande.

Le critère de défaillance unique doit s'appliquer au PACS, afin de garantir un degré de redondance adéquat.

D'autre part, si les essais périodiques des fonctions PACS sont possibles et réalisés tel que défini par le chapitre IX des Règles Générales d'Exploitation, et déclinés au paragraphe "Dispositions prises pour réaliser les essais périodiques" ci-après, alors que le PACS doit pouvoir être sollicité au titre du traitement de fonctions de sûreté F1, ils doivent être combinés avec l'application du critère de défaillance unique pour définir la redondance à mettre en oeuvre. Cela se traduit par l'application d'un degré de redondance adéquat sur les actionneurs, et en correspondance sur la fonction PACS gérant chacun d'entre eux.

Indépendance et séparation physique : le PACS doit être assujetti à ces exigences, qui conduisent concernant ses équipements matériels, à une indépendance physique et électrique des quatre divisions de contrôle-commande dont ils dépendent. Chaque PACS, propre à un actionneur, doit être indépendant des autres PACS : il n'y a aucun échange entre eux. Des dispositions doivent être prises pour découpler les différents équipements matériels mis en œuvre pour assurer les fonctions PACS et éviter les défaillances de cause commune. Ainsi, les liaisons entre automate (PAS, SAS, SAS RRC-B CCAG et CCND), automate de protection (PS) et cellule électrique sont assurées par fil.

0.2.1.3. ALIMENTATIONS ÉLECTRIQUES SECOURUES

L'alimentation électrique du contrôle-commande intégré à la cellule électrique doit être secourue par les groupes diesels principaux. Par ailleurs, cette alimentation doit être du type sans coupure, garantissant une alimentation même pendant le basculement alimentation normale / alimentation par diesel. De sorte que les fonctions de sûreté dont le PACS gère l'automatisation puissent être assurées sans discontinuité de service.

Le PACS doit être alimenté par la même division que celle de l'actionneur dont il assure le pilotage, chaque division étant indépendante électriquement et physiquement des trois autres de façon à garantir une absence de mode commun entre divisions.

0.2.1.4. QUALIFICATION AUX CONDITIONS DE FONCTIONNEMENT

Les équipements PACS doivent rester opérationnels en conditions post-accidentelles, et doivent en conséquence respecter les exigences de qualification définies au sous-chapitre 3.7.

Par ailleurs, ces équipements doivent être opérationnels pour les conditions environnementales normales et extrêmes [] dans lesquels ils sont implantés. Ces conditions sont définies au sous–chapitre 9.4.

Les principes permettant d'assurer la Compatibilité Electro-Magnétique des cellules électriques [] sont exprimés au paragraphe 2 du sous-chapitre 8.4.

0.2.1.5. CLASSEMENT MÉCANIQUE, ÉLECTRIQUE, CONTRÔLE-COMMANDE

Le classement mécanique ne s'applique pas aux équipements électriques (donc concernant le PACS, ni aux automates, ni aux cellules électriques).

Les cellules électriques sont assujetties à :

- Un classement électrique, du fait de leur fonction d'alimentation en tension des actionneurs. Ce classement est le suivant, conformément aux principes définis au sous-chapitre 3.2 :
  - Classement EE1 pour une cellule recevant au moins une commande F1,
  - Classement EE2 pour une cellule recevant au moins une commande F2 (et pas de commande F1).
- Un classement de contrôle-commande, du fait qu'elles intègrent le contrôle-commande assurant les traitements d'automatisme des fonctions PACS énoncées dans le paragraphe "Fonctions assurées" ci-après. Ce classement est le suivant, conformément aux principes définis au sous-chapitre 3.2 :
  - Classement E1A pour une cellule recevant au moins une commande F1A,
  - Classement E1B pour une cellule recevant au moins une commande F1B (et aucune commande F1A),
  - Classement E2 pour une cellule recevant une commande F2 (et aucune commande F1).

0.2.1.6. CLASSEMENT SISMIQUE

La cellule électrique doit être :

- Classée séisme 1 (SC1), lorsqu'elle gère des fonctions F1 ou F2E, assujetties au requis d'opérabilité en cas de séisme,
- Classée séisme 2 (SC2), lorsqu'elle gère des fonctions F2N (donc sans requis d'opérabilité en cas de séisme) et pourrait engendrer l'agression d'un équipement SC1 lors d'un séisme.

0.2.1.7. EXIGENCE SUPPLÉMENTAIRE

Sans objet.

0.2.2. AUTRES EXIGENCES

0.2.2.1. RÈGLES FONDAMENTALES DE SÛRETÉ

PACS non concerné.

0.2.2.2. DIRECTIVES TECHNIQUES

Les directives techniques pour la conception et la construction de la prochaine génération de réacteurs nucléaires à eau sous pression énoncées par le document [7] et rappelées au sous-chapitre 1.7 (et plus spécifiquement les points A1.2, A2.2, B2.1, B2.2, C2.1, F1.1, G3 et G4) doivent être prises en compte à la conception du PACS.

0.2.2.3. TEXTES SPÉCIFIQUES EPR

Les matériels gérant les fonctions PACS doivent être conformes aux exigences énoncées dans le RCC-E complété des données de projet EPR définies dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.2.3. AGRESSIONS

0.2.3.1. Exigences — protections vis à vis des agressions internes

Les fonctions du système PACS doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4

0.2.3.2. Exigences — protections vis à vis des agressions externes

Les fonctions du système PACS doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3

0.3. ESSAIS

0.3.1. ESSAIS PRE-OPERATIONNELS

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du PACS.

0.3.2. SURVEILLANCE EN EXPLOITATION

Sans objet.

0.3.3. ESSAIS PERIODIQUES

Les fonctions de contrôle-commande gérées par le PACS doivent faire l'objet d'essais périodiques (tel que défini par le chapitre IX des Règles Générales d'Exploitation), pour les traitements de contrôle-commande associés aux fonctions F1, et F2 lorsque non sollicitées en fonctionnement continu.

1. MISSIONS

Le PACS est l'entité fonctionnelle qui assure la commande de l'actionneur (gestion de priorité des commandes et commande de l'organe de coupure), la surveillance de son mouvement, et la protection des composants de la partie électrique. Il est en charge :

- Au titre de la commande de l'actionneur :
  - De l'élection de la commande la plus prioritaire (en cas de commandes simultanées) parmi l'ensemble des commandes assujettissant l'actionneur,
  - De la commande de l'organe de coupure,
- Au titre de la surveillance de l'actionneur : de la gestion de la position de l'actionneur et de ses défauts de mouvement (temps de manœuvre excessif ou incohérence entre position attendue et position réelle de l'actionneur),
- Au titre de la protection des composants : de la détection des dysfonctionnements pouvant endommager la partie électrique de l'actionneur ou son alimentation électrique.

2. FONCTIONS ASSURÉES

En correspondance avec les missions définies au paragraphe précédent, le PACS assure les quatre fonctions suivantes :

- *Gestion de priorité des commandes* : hiérarchisation de l'ensemble des commandes (automatiques et manuelles) assujettissant l'actionneur, quelles que soient leur origine et leur fonction, et élection (en cas de commandes simultanées) de la commande ayant le niveau de priorité le plus élevé. La commande élue est envoyée vers la fonction PACS "*commande de l'organe de coupure*" (voir ci après).
  La hiérarchie des commandes est la suivante (de la plus à la moins prioritaire, en listant l'ensemble des commandes possibles, toutes n'étant pas systématiques, et en considérant un actionneur F1A) :
  - Commande "*protection essentielle des composants*" (protections prévenant l'endommagement de la partie électrique de l'actionneur, ou de son raccordement électrique),
  - Commande de sûreté de délestage (suite à perte alimentation électrique de puissance),
  - Commande de sûreté de protection réacteur (arrêt). Pour certains actionneurs, la commande de protection réacteur (marche) est prioritaire sur la commande de protection réacteur (arrêt),
  - Commande de sûreté de protection réacteur (marche). Pour certains actionneurs, la commande de protection réacteur (arrêt) n'est pas prioritaire sur la commande de protection réacteur (marche),
  - Commande []. Utilisée en situation de démarrage de l'installation, ou en exploitation (commande en cas d'indisponibilité automate),
  - Commande de protection organe (issue du procédé : température très haute d'une batterie chauffante, par ex.),
  - Commande d'exploitation (issue du procédé : niveau bas enclenchant une pompe de remplissage, par ex.),
  - Commandes [] centralisées. La priorité entre IHM MCP/SdR et MCS est gérée par un dispositif (voir note [6]) assurant l'exclusivité du moyen de commande.

- *Commande de l'organe de coupure* : commande de l'organe conditionnant le fluide de manœuvre de l'actionneur. Cette commande est reçue de la fonction "*Gestion de priorité des commandes*". Selon spécification fonctionnelle du système élémentaire et typologie de l'actionneur (un ou deux sens de marche), la gestion de cette commande peut être monostable (adoption de la position de repos sur disparition de la commande) ou bistable (maintien en position de l'actionneur sur disparition de la commande).
- *Surveillance de l'actionneur* : gestion d'une part de la position de l'actionneur, et d'autre part de ses défauts de mouvement. Cette dernière fonction détecte un dysfonctionnement de manœuvre de l'actionneur : temps de mouvement anormalement long, et discordance entre position souhaitée et position réelle de l'actionneur,
- *Protection essentielle des composants* : élaboration de la commande qui traduit un dysfonctionnement de la partie opérative de l'actionneur (défaut de court-circuit ou de surcharge, défaut d'isolement, etc.). Elle prévient un risque d'endommagement de l'actionneur ou de son alimentation électrique. Cette commande est appliquée à la fonction PACS "*gestion de priorité des commandes*", où lui est affecté le plus haut niveau de priorité.

Projetés sur l'architecture matérielle, les traitements des fonctions PACS sont répartis de la façon suivante :

- L'automate PAS / SAS / SAS RRC-B / CCAG élabore les commandes automatiques hors F1A, et acquiert les commandes [] issues des IHM centralisées (MCP / PdR, MCS et PAG). En cas de simultanéité de commande, il élit la commande prioritaire selon hiérarchie définie ci-avant (fonction "*gestion de priorité des commandes*"). La commande élue est envoyée à la cellule électrique. [].
  D'autre part, le PAS / SAS / SAS RRC-B et CCAG assure la surveillance de la position de l'actionneur et l'élaboration des défauts de mouvement (fonction "*surveillance de l'actionneur*"). L'automate CCND ne gère pas de traitement de surveillance de l'actionneur.
- La cellule électrique élabore les protections essentielles de composants (fonction "*protection essentielle des composants*"), et reçoit la (les) commande (s) issue (s) du PS, la commande envoyée par le PAS / SAS / SAS RRC-B / CCAG ou CCND et la commande issue de l'IHM [].

Fonction de sélection entre automate SPPA-T2000 et CCND

Le scénario au titre duquel le CCND est requis postulant une défaillance généralisée de la plate-forme SPPA-T2000, une fonction [] de sélection SPPA-T2000 / CCND assure l'exclusivité de la voie de commande sélectionnée. Cette commutation est intégrée à la cellule électrique de chacun des actionneurs concernés.

Cette fonction de sélection relève de la fonction PACS "*Gestion de priorité des commandes*".

Nota : la fonction "*gestion de priorité des commandes*" est assurée pour partie par le PAS / SAS / SAS RRC-B, et pour partie par la cellule électrique. L'élaboration des commandes F1A (par l'automate PS) ne relève pas des fonctions du PACS. Ces commandes sont acquises par la fonction PACS "*gestion de priorité des commandes*".

La figure **FIG–7.3.6.1** précise l'allocation des fonctions PACS en regard des architectures fonctionnelle et matérielle, pour un actionneur F1A à deux sens de marche.

3. BASE DE CONCEPTION

3.1. EXIGENCE DE DISPONIBILITÉ

Les principales exigences conditionnant la disponibilité du PACS sont liées à la fiabilité et la maintenabililté des équipements gérant ses fonctions, et se traduisent par :

- Limiter les pertes du PACS dues à la panne d'un de ses composants (par la redondance de ses composants notamment),
- Faciliter l'entretien et la réparation des équipements PACS pour réduire au minimum sa période d'indisponibilité.

3.2. PERFORMANCES REQUISES

Les études d'accident définissent pour les chaînes de protection la durée admissible s'écoulant entre l'acquisition de l'initiateur procédé et la manœuvre de l'actionneur.

La cellule électrique participe au respect de ce requis, au titre de la durée s'écoulant entre la réception de la commande de sûreté par la cellule et la sollicitation de l'actionneur induite par la manœuvre de l'organe de coupure.

3.3. EXIGENCES LIÉES À L'ENVIRONNEMENT

Les conditions environnementales auxquelles sont soumis les équipements gérant les fonctions du PACS dépendent des locaux où ils sont implantés :

- Locaux [] :
  Les caractéristiques de température et d'humidité auxquelles seront soumis les équipements PAS/SAS/SAS RRC-B ou CCAG ([]) sont précisées au sous– chapitre 9.4, autant pour les conditions normales que pour les conditions extrêmes.
- Locaux [] :
  Les caractéristiques de température et d'humidité auxquelles seront soumis les cellules électriques ([]) sont précisées au sous–chapitre 9.4, autant pour les conditions normales que pour les conditions extrêmes.
- Les locaux (automates ou tableaux électriques) dans lesquels sont implantés les équipements gérant les fonctions PACS ne sont soumis à aucun agresseur physico-chimique autres que la température et l'humidité.

3.4. EXIGENCE LIÉES À L'INTERFACE HOMME-MACHINE

PACS non concerné.

4. ALLOCATION DES FONCTIONS DU PACS

4.1. STRUCTURE ET COMPOSITION

Les quatre fonctions du PACS sont traitées pour partie par l'automate PAS / SAS / SAS RRC-B ou CCAG, selon requis fonctionnel), et pour partie par la cellule électrique.

- Concernant les fonctions traitées par le PAS, structure et composition sont définis en section 7.4.2 paragraphe "structure et composition",
- Concernant les fonctions traitées par le SAS, structure et composition sont définies en section 7.3.2 paragraphe "structure et composition",
- Concernant les fonctions traitées par le SAS RRC-B, structure et composition sont définies en section 7.4.5 paragraphe "structure et composition",
- Concernant la fonction traitée par le CCAG, structure et composition sont définies en section 7.4.4 paragraphe "structure et composition".

Structure et composition de la cellule électrique : chaque actionneur électrique est géré par une cellule débrochable (avec dans certains cas uniquement le débrochage de l'organe de coupure), implantée dans un tableau électrique basse ou haute tension.

La cellule est définie dans le respect :

- Des exigences définies au paragraphe "Exigences relatives à la conception" ci-avant,
- Des caractéristiques électriques de l'actionneur alimenté,
- Du type d'alimentation requis (secourue ou non secourue, voir chapitre 8).

4.2. INSTALLATION

Les équipements traitant les fonctions PACS seront implantés :

[]

4.3. INTERFACES AVEC LES SYSTÈMES DE CONTRÔLE-COMMANDE

Les fonctions PACS sont gérées par une entité PAS/SAS/SAS RRC-B/CCAG - cellule électrique, qui échange des informations avec :

- Les IHM centralisées :
  - MCP/PdR,
  - MCS et PAG.
- L'IHM locale (enfichable sur la cellule électrique), au titre du démarrage de l'installation et de la commande en cas de dysfonctionnement automate,
- Le PAS / SAS / SAS RRC-B et CCAG (pour les fonctions de contrôle commande autres que celles gérées au titre du PACS : élaboration des commandes automatiques, élaboration des défauts autres que ceux de mouvement, etc.),
- Le PS (pour la gestion des commandes de sûreté),
- Le (ou les) organe(s) de coupure (conditionnant l'alimentation électrique de l'actionneur),

- Les capteurs issus du procédé.

5. CONFIGURATIONS OPÉRATIONNELLES

La configuration (d'un point de vue matériel et fonctionnel) du PACS est indépendante de l'état de la tranche. L'allocation des traitements au sein des différents équipements gérant les fonctions PACS (automate et cellule électrique) dépend seulement de critères fonctionnels et des fonctionnalités natives de ces 2 équipements. La configuration du PACS est constante.

6. TECHNOLOGIE

La technologie du PACS est définie par celle des équipements matériels qui traitent ses fonctions.

- Les automates PAS / SAS et SAS RRC-B sont portés par une plate-forme SPPA T2000 du fournisseur SIEMENS.
- L'automate CCAG est porté par une plate-forme TELEPERM XS (TXS) du fournisseur FRAMATOME.
- Les fonctions PACS assurées par la cellule sont gérées :
  - En technologie conventionnelle (relayage) pour les fonctions "*gestion de priorités des commandes*" et "*commande de l'organe de coupure*",
  - En technologie conventionnelle (relayage) ou en technologie numérique (uniquement pour les actionneurs du BLNC alimentés en HTA) pour la fonction "*Protection essentielle des composants*".

7. ALIMENTATION ÉLECTRIQUE

Elle relève des principes d'alimentation électrique des différents équipements qui assurent le traitement des fonctions du PACS soit :

- Automate PAS / SAS / SAS RRC-B et CCAG :
  - Chaque automate reçoit une alimentation redondée issue d'une part d'une armoire redresseur (AC/DC) et d'autre part d'une armoire convertisseur (DC/DC).
  - Ces deux armoires sont alimentées par des sources de nature différente et diversifiées (400V AC pour l'une et 220V DC pour l'autre) issues de tableaux électriques différents (LA. et LV.). Ces tableaux sont secourus d'une part par des batteries de 2 h pour les PAS, SAS et SAS RRC-B et [], et d'autre part par les diesels principaux (automates des divisions 1 à 4, et automates des sections 2 et 3) et par les diesels SBO (automates des divisions 1 et 4) :
- Cellule électrique : elle est alimentée :
  - Pour la tension de puissance : par une alimentation qui, selon le requis fonctionnel, est secourue ou pas,
  - Pour la tension de commande, qui alimente le contrôle commande interne à la cellule, par une alimentation qui suit le même principe d'élaboration que celle des automates (selon ci-dessus). A partir de cette alimentation, le fournisseur du tableau électrique élabore la tension de commande mise à disposition de chaque cellule du tableau, soit 48V DC pour les tableaux BT et 220V DC pour les tableaux HT.

8. DISPOSITIONS PRISES POUR RÉALISER LES TESTS PÉRIODIQUES

Selon RCC-E (voir sous-chapitre 1.6), les fonctions F2 (au cas par cas), F1B et F1A, doivent être périodiquement testées. A ce titre, et fonction de son classement, le PACS, en temps qu'élément de la

chaîne de commande de l'actionneur, est assujetti à des tests périodiques permettant de vérifier l'intégrité de la chaîne de commande.

Ce test s'applique à la fonction globale, et comprend :

- L'initiateur du test (commande manuelle IHM ou action mécanique locale sur un capteur, selon les cas),
- Le PACS, se composant de l'automate (PAS / SAS / SAS RRC-B ou CCAG,) et de la cellule électrique (comprenant le ou les organes de coupure),
- L'actionneur, dont on vérifie le mouvement suite à sollicitation lors du test.

Nota : si la mise en configuration de l'actionneur concerné ne peut pas être effectuée (par exemple lors du fonctionnement de la tranche) des dispositions seront prises pour que le test n'entraîne pas la commande effective de l'actionneur.

Les principes fondamentaux liés aux tests périodiques sont énumérés ci-après :

- Autant que possible, le test périodique devra être réalisé à partir de la salle de commande principale si les tests ont une action sur le processus, ou si les tests concernent l'interface homme-machine elle-même, sans nécessiter d'intervention locale.
- Quand un actionneur de sauvegarde reçoit des commandes de plusieurs systèmes (par exemple les PS et SAS ou PAS), le test de cet actionneur devra être réalisé autant que possible d'un de ces systèmes uniquement. Le test des commandes venant des autres systèmes devra être réalisé sans manœuvrer réellement.
- Les tests qui impliquent le mouvement de l'actionneur, et requièrent l'utilisation d'une l'IHM pour envoyer les commandes et vérifier l'information en retour, imposent la participation du personnel. Ces essais devraient demeurer manuels (aucune configuration automatique, en préambule aux test des systèmes mécaniques pour les essais).

9. ANALYSE DE SÛRETÉ

Le PACS, compte tenu des éléments présentés dans les présentes sections, est conforme aux exigences de sûreté dont il est redevable.

10. TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

FIG–7.3.6.1 ALLOCATION DES FONCTIONS PACS EN REGARD DES ARCHITECTURES FONCTIONNELLE ET MATÉRIELLE

7.4 LES SYSTÈMES DE CONTRÔLE-COMMANDE CLASSÉS F2 OU NC

SOMMAIRE

TABLEAUX :

FIGURES :

.7.4.1 ARCHITECTURE DU MOYEN DE CONDUITE PRINCIPAL (MCP)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

La contribution du MCP aux fonctions de sûreté supportées par les systèmes de contrôle commande est décrite dans le paragraphe 0.1 du sous-chapitre 7.1 (alinéa sur les fonctions F2). Ainsi, en ce qui concerne la démonstration de sûreté, le système MCP a pour mission de fournir à l'équipe de conduite les informations et commandes nécessaires pour surveiller et conduire la tranche en situation PCC1 (dans des conditions et les limites du fonctionnement normal de l'installation) et dans les situations RRC-A et d'accident grave. Le MCP doit alors être conçu afin de supporter des fonctions F2 et NC.

Le MCP est également le moyen de conduite privilégié pour assurer une conduite optimisée de l'installation en situation PCC-2 à PCC-4 (cf. chapitre 13 pour plus de détails).

0.2. EXIGENCES RELATIVES À LA CONCEPTION

0.2.1. Exigences issues des classements fonctionnel et mécanique

0.2.1.1. Classement fonctionnel du système

Le MCP supporte des fonctions de conduite et de surveillance F2 et NC. Il doit être classé de sûreté F2/NC, conformément au classement indiqué au sous-chapitre 3.2.

Le MCP étant le moyen de conduite privilégié pour assurer une conduite optimisée de l'installation en situation PCC-2 à PCC-4 :

- Le matériel et l'architecture de l'interface homme-machine informatisée des postes opérateurs en salle de commande principale doivent satisfaire aux exigences applicables aux systèmes F1B ;
- Le logiciel correspondant doit satisfaire à des exigences de qualification détaillées à proposer par le concepteur ;
- Les moyens doivent être mis en oeuvre (en dehors du MCP) pour la détection et la signalisation des défaillances des unités de traitement du MCP, et ces moyens doivent satisfaire aux exigences applicables aux fonctions et équipements F1B.

0.2.1.2. Critère de défaillance unique (active et passive)

Le critère de défaillance unique n'est pas requis pour les fonctions F2 du MCP. De par l'application des exigences F1B aux matériels et à l'architecture de l'interface homme-machine informatisée des postes opérateurs en salle de commande, le critère de défaillance unique doit être respecté par l'architecture formée par ce sous-ensemble de matériels du MCP.

0.2.1.3. Alimentations électriques secourues

De par le classement F2 du MCP, l'exigence d'une alimentation électrique secourue des équipements MCP doit être définie au cas par cas.

De par l'application des exigences F1B aux matériels et à l'architecture de l'interface homme-machine informatisée des postes opérateurs en salle de commande, l'alimentation électrique des matériels correspondants doit être secourue par les groupes diesel principaux. De plus, cette alimentation doit être du type « sans coupure » pendant tous les modes de fonctionnement possibles et les transitoires correspondants.

0.2.1.4. Qualification aux conditions de fonctionnement

Les équipements MCP doivent être qualifiés en fonction de leur classement de sûreté, et doivent en conséquence respecter les exigences de qualification (intégrité, disponibilité, …) définies à la section 3.7.1 et ce pour les conditions d'ambiances normales et extrêmes auxquels ils sont soumis lors de l'accomplissement de leur mission (cf. paragraphe 1.1.2).

0.2.1.5. Classements mécanique, électrique, contrôle-commande

Les classements mécanique et électrique ne s'appliquent pas aux équipements de contrôle-commande.

Selon le sous-chapitre 7.1 concernant le classement contrôle-commande :

- Les équipements du MCP :
  - Assurant des fonctions F2 doivent être classées E2,
  - Assurant des fonctions NC doivent être non classées.

Les équipements du MCP n'assurant pas de fonctions F1B, le classement E1B n'est pas évoqué ici.

Le tableau **TAB–7.4.1.1** en annexe détaille le classement contrôle-commande des matériels du MCP.

0.2.1.6. Classement sismique

Une partie des matériels du MCP doivent appartenir à la classe sismique 1 :

- De par l'application des exigences F1B aux matériels et à l'architecture de l'interface homme-machine informatisée des postes opérateurs en salle de commande ;
- Au titre de la défense en profondeur, les postes de la station de repli étant identiques à ceux de la salle de commande principale, le projet a retenu une exigence de classement séisme des fonctions de commande et de supervision de la station de repli de l'EPR (les fonctions d'impression, d'archivage – si elles sont requises pour la station de repli – ne sont pas qualifiées séisme).

Les autres équipements du MCP doivent appartenir à la classe sismique 2 au titre de la non agression des matériels appartenant à la classe sismique 1.

Les dispositions d'installation assurent l'intégrité des matériels du MCP pendant et après un séisme. Et par requis fonctionnel la conduite au MCP doit être opérationnelle après un séisme.

Le tableau **TAB–7.4.1.2** en annexe détaille le classement sismique et le requis d'opérabilité après séisme des matériels du MCP.

0.2.2. Autres exigences

0.2.2.1. Règles Fondamentales de Sûreté

Le MCP n'est pas concerné.

0.2.2.2. Directives Techniques

Les directives techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/2004 « options de sûreté du projet réacteur EPR » doivent être prises en compte à la conception du MCP (en particulier les chapitres G3.5 et A2.3).

0.2.2.3. Textes EPR spécifiques

Le MCP doit satisfaire aux exigences énoncées dans le RCCE édition décembre 2005 complétées des données de projet EPR définies dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.2.3. Agressions

0.2.3.1. Exigences - protection vis-à-vis des agressions internes

Les fonctions du MCP doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.2.3.2. Exigences – protection vis-à-vis des agressions externes

Les fonctions du MCP doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.2.4. Essais

0.2.4.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du MCP.

0.2.4.2. Surveillance en exploitation

Le moyen classé F1B mis en œuvre pour détecter et signaler les défaillances éventuelles des postes opérateurs utilisés en salle de commande permet de surveiller en salle de commande le bon fonctionnement des unités de traitement du MCP.

La spécification du moyen de surveillance en exploitation classé F1B est détaillée dans la note d'étude ECECC091339 indice C.

Le principe de la surveillance « signe de vie » est le suivant. [].

Le signe de vie couvre également le processus hébergeant le calcul de la situation de tranche (situation utilisée pour valider les alarmes fonctionnelles). [].

0.2.4.3. Essais périodiques

Les parties classées du MCP doivent être conçues pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

Le moyen de conduite principal (MCP) est le système de contrôle commande supportant les moyens informatisés de commande et de surveillance de l'installation, il inclut :

- Les postes opérateurs et le synoptique (SYN) installés dans la salle de commande principale ;
- Le poste opérateur installé dans le local technique de crise (LTC) à des fins de surveillance ;
- Les postes opérateurs installés dans la Station de Repli (SdR) ;
- Les postes opérateurs minimum (avec un nombre réduit d'écrans) qui peuvent être installés en compléments des moyens de conduite informatisés dans des situations de tranche particulières (par exemple, mise en service) ou pour des activités spécifiques (par exemple, maintenance) ;
- Le poste opérateur REN/RES installé dans le BAN ;
- Le poste opérateur BTE installé dans le BTE.

En outre, le MCP enregistre les signaux et les événements significatifs qui se produisent dans la tranche et assure l'interface avec les applications hors temps réel (également appelées applications de niveau 3).

La mission principale du MCP est par conséquent de fournir à l'équipe de conduite, quelle que soit la situation de tranche, les commandes et informations adaptées à ses activités. Cette mission nécessitant une interaction avec des opérateurs, l'interface homme-machine du MCP doit être conforme aux critères ergonomiques prenant en compte les aptitudes cognitives et physiologiques du personnel de conduite.

2. FONCTIONS SUPPORTÉES

Afin d'atteindre l'objectif énoncé dans le paragraphe précédent, le MCP offre les fonctionnalités suivantes :

- Fonctions d'affichage
  - Affichage des images, des modes opératoires, des fiches d'alarmes, des fiches techniques et des listes,
  - Navigation entre les différentes images,
  - Désignation de l'objet avec lequel l'opérateur doit interagir,
  - Rafraîchissement des images (couleur, forme des objets…) à partir des informations process,
  - Visualisation et traçage des courbes,
  - Impression de différentes images ou listes.
- Fonctions de contrôle commande
  - Envoi des commandes opérateurs vers les systèmes de contrôle commande,
    Pour éviter tout ordre intempestif dû à une éventuelle défaillance interne du MCP ([]), toute transmission de commandes opérateurs à destination du système de protection est assujettie à une validation préalable classée F1B par l'opérateur. Cette validation s'appuie sur un dispositif câblé indépendant du MCP (Cf. sous-chapitre 7.3),
  - Affichage des comptes rendus des commandes,
  - Permettre la présentation des données à l'opérateur.
- Fonctions d'alarme
  - Avertir les opérateurs dès l'apparition d'une alarme,
  - Gérer les listes d'alarmes,
  - Permettre l'accès aux fiches d'alarme.
- Fonctions de traitement
  - Gestion de(s) base(s) de données,
  - Lancement de traitements en cas de changement d'état,
  - Élaboration d'information si nécessaire (situations, alarmes, information de synthèse…).
- Fonctions d'interface
  - Acquérir et filtrer les informations process par l'intermédiaire du niveau d'automatisme,
  - Envoi d'ordre vers le procédé par l'intermédiaire du niveau d'automatisme.
- Fonction d'archivage
  - Archivage des données logiques et analogiques,

- Récupération des données archivées.

- Fonctions administratives et de maintenance
  - Fournir une aide à la maintenance,
  - Fournir une aide pour l'analyse (par exemple analyse des accès aux PO, …),
  - Assurer les tâches de sécurité informatique (par exemple la gestion des accès aux PO, …),
  - Gestion des introductions de données en fonctionnement,
  - Auto surveillance.

Le tableau **TAB–7.4.1.3** en annexe détaille le classement de sureté des fonctions du MCP.

3. PRINCIPES DE CONCEPTION

3.1. EXIGENCES DE DISPONIBILITÉ

Les objectifs principaux pour l'architecture du MCP sont disponibilité, flexibilité et maintenabilité. En particulier, cela signifie que le MCP est suffisamment flexible et redondant pour :

- Empêcher la plupart des pertes du MCP suite à la défaillance d'un de ses équipements,
- Permettre la ré-allocation de l'espace de travail (écrans, postes opérateurs, …) quand certains équipements (écran, ordinateur…) sont indisponibles,
- Faciliter les opérations d'entretien et de réparation afin de réduire au minimum la période d'indisponibilité du MCP,
- Permettre l'ajout d'autres composants (poste opérateur complémentaire par exemple) pendant des phases spécifiques (par exemple mise en service, maintenance).

3.2. PERFORMANCES REQUISES

Le niveau d'automatisme du système de contrôle-commande est soumis à des requis de performances pour assurer des protections d'équipements et des régulations sur le procédé. Ces requis sont précisés au sous-chapitre 7.2.

Les exigences de performance des systèmes de contrôle-commande de niveau 2 sont traitées en section 7.2.1.

3.3. EXIGENCES D'ENVIRONNEMENT

Les conditions ambiantes dépendent en grande partie de l'emplacement des différents équipements (salle de commande principale, Station de Repli ou locaux d'armoires de CC).

On distingue deux catégories :

- Les conditions d'environnement auxquelles les équipements sont soumis. Ceci inclut la température et l'humidité relative de la pièce ;
- La contribution de l'équipement aux conditions ambiantes. Cette catégorie inclut le niveau de bruit et la chaleur dégagée.

Pour le cas particulier des équipements de visualisation, certaines conditions environnementales particulières telles que l'éclairage doivent être considérées d'un point de vue ergonomique. Les dispositions qui doivent être prises sont étudiées dans le cadre de la démarche Facteur Humain (cf. sous-chapitre 17.2 pour la prise en compte dans le programme Facteur Humain notamment au travers des études d'aménagement, et sous-chapitre 17.4 pour la définition des exigences relatives aux conditions d'ambiance).

3.4. EXIGENCES CONCERNANT L'INTERFACE HOMME-MACHINE

Du point de vue Facteur Humain :

- Le MCP doit disposer des fonctionnalités permettant de mettre en œuvre les résultats de la démarche facteur humain (par exemple sur les traitements, le type de données supporté, l'organisation des données, l'agencement de l'imagerie, les moyens de navigation, le système d'alarme, les mécanismes d'aide à la conduite…) ;
- Le MCP doit fournir aux opérateurs de conduite un environnement de travail comprenant une interface respectant les exigences ergonomiques de l'état de l'art (organisation des différents moyens de conduite dans la salle de commande, agencement des postes de travail, moyens de dialogue, moyens de communications…).

Ces exigences sont prises en considération dans le cadre du programme Facteur Humain détaillé dans le sous-chapitre 17.2.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Pour remplir sa mission, le MCP s'appuie sur les ressources suivantes (logiciel et/ou matériel) :

- Interfaces graphiques pour l'interface homme-machine ;
- Interfaces réseaux pour l'échange de données ;
- Base(s) de donnée(s) temps réel (informations élaborées ou issues du process, et leurs attributs, données de l'interface homme-machine) ;
- Périphériques d'archivage et d'impression ;
- Système d'exploitation ;
- Logiciel applicatif.

Ces ressources sont utilisées par les équipements suivants :

- Postes opérateurs de conduite ;
- Postes de surveillance dans la salle de commande principale et au local technique de crise (LTC) ;
- Un synoptique (SYN) en salle de commande principale, constitué de grands écrans ;
- Les postes opérateurs minimum pendant des phases ou des tâches spécifiques (ex : mise en service) ;
- Équipements permettant l'impression ;
- Équipements permettant l'archivage ;
- Interfaces avec les outils d'ingénierie ;
- Interfaces avec d'autres applications (niveau 3) ;
- Réseaux pour l'échange de données entre le MCP et les systèmes de niveau 1 ou 3.

Les postes opérateurs se composent d'écrans standard, rafraîchis par des unités de traitement selon le contenu de(s) base(s) de données, et de dispositifs de pointage et de saisie (souris, claviers, etc..).

[]

Le nombre de postes de travail, ainsi que leur composition détaillée (le nombre d'écrans par exemple), leur positionnement dans la salle de commande, dans le local technique de crise ou dans la SdR, résulte des résultats du programme Facteur Humain.

Le synoptique (SYN) est considéré comme partie intégrante du MCP, il est par conséquent soumis au même classement de sûreté (c.-à-d. F2/NC) et peut être considéré comme un poste opérateur configuré en mode supervision. De fait, lorsque le MCP est considéré comme indisponible pour la conduite, le synoptique l'est également. Cela est pris en compte, tout particulièrement pour la conception du MCS (cf. sous-chapitre 17.4).

Les fonctions de contrôle commande supportées par le MCP (cf. le § 2.) sont réparties parmi les équipements énumérés précédemment pour répondre aux exigences de sûreté et de disponibilité :

- Les fonctions F2 sont implémentées sur les équipements ou groupe d'équipements E2, les fonctions non classées sont de préférence implémentées sur un équipement non classé ;
- Les constituants des MCP et MCS sont suffisamment différents pour réduire au minimum les risques de mode commun. Cette mesure est complétée par des dispositions appropriées concernant l'installation des matériels (cf. sous-chapitre 7.1) ;
- Les moyens de traitement nécessaires pour commander et superviser la tranche depuis les postes opérateur en SdR sont installés dans [] ;
- L'architecture du MCP (au moins la partie exécutant le noyau F2) est dite à tolérance de panne, c'est-à-dire qu'elle prend en compte des critères de redondance et d'indépendance suffisants, de sorte que les pannes les plus probables ne puissent pas causer la perte des fonctions d'IHM.

4.2. INSTALLATION

Les équipements graphiques du MCP sont répartis ainsi :

Dans le Bâtiment des Auxiliaires de Sauvegarde (BAS) :

- Dans la salle de commande principale :

  []

- Dans le local technique de crise (LTC) :

  []

- Dans la SdR :

  []

- En Salle de Maintenance :

  []

- En Salle de consignation :

  []

- En Salle Calculateur Division 2 :

  []

- En Salle Calculateur Division 3 :

  []

- En Bâtiment Electrique 1 (BL1) :

  []

- En Bâtiment électrique 4 (BL4) :

  []

Dans le Bâtiment des Auxiliaires Nucléaires (BAN) :

[]

Dans le Bâtiment de Traitement des Effluents (BTE) :

[]

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CC

Le MCP présente 3 types d'interfaces avec les autres systèmes de CC :

- L'interface avec le niveau 1 (PS/SAS/PAS/RCSL),
- L'interface avec les outils d'ingénierie et de maintenance (du MCP),
- L'interface avec les applications de niveau 3.

5. MODES DE FONCTIONNEMENT

Du point de vue du contrôle-commande, **les différents modes de fonctionnement du MCP** sont les suivants :

- La configuration standard du MCP est :

  []

- Défaillance non critique d'un équipement du MCP : dans cette configuration, une partie du MCP est défaillante mais les équipements encore disponibles sont suffisants pour réaliser une ré-affectation des fonctions de conduite permettant ainsi d'utiliser le MCP pour commander et surveiller la tranche. Les situations caractéristiques sont les suivantes :

  []

En complément de ces dispositions, les activités de maintenance sont étudiées afin de réduire le temps nécessaire pour remplacer ou réparer le matériel en défaut :

- Indisponibilité du MCP : en cas de perte fortuite du MCP ou de l'arrêt programmé du MCP pour maintenance, la conduite est transférée du MCP au MCS. Ce transfert est géré par des procédures. En ce qui concerne le seul domaine du contrôle-commande, ces procédures explicitent les actions particulières à réaliser pour se prémunir contre l'émission d'ordres intempestifs par le MCP et leur prise en compte par le process.
- Indisponibilité de la salle de commande principale : en cas de perte de la salle de commande [], les équipements du MCS et du MCP situés dans la salle de commande principale ne sont plus disponibles. Dans ce cas, l'équipe de conduite utilise les moyens de conduite situés à la SdR. Comme pour la situation précédente, des actions adaptées sont prises pour empêcher l'émission d'ordres intempestifs depuis la salle de commande principale. La configuration du MCP est alors la suivante :

  []

La manière dont les différents équipements du MCP sont utilisés pour la conduite ou la supervision de la tranche dans les situations particulières exposées ici est détaillée dans le chapitre 17.

Les différentes configurations (particulièrement la différence entre une indisponibilité du MCP et une défaillance non critique d'un de ces composants) sont déterminées en fixant le minimum d'équipements requis pour conduire l'installation depuis le MCP (le nombre minimum d'écrans

nécessaires pour conduire à partir d'un poste opérateur, nombre minimum de postes opérateurs en mode supervision et en mode conduite pour pouvoir conduire l'installation …). Ces conditions minimales dépendent de la manière dont les différents équipements sont utilisés, c'est pourquoi elles sont principalement déterminées au travers du programme Facteur Humain.

6. TECHNOLOGIE

Le contrôle-commande standard utilise la plate-forme SIEMENS SPPA-T2000 tel que :

- [] supporte les automatismes de niveau 1 : SAS, PAS et SAS RRC-B,
- [] supporte les automatismes de niveau 2 et l'interface graphique : MCP.

Le MCP se compose de différents équipements informatiques implantés dans plusieurs locaux de la tranche et reliés en réseau via le Terminal Bus. L'architecture générale du MCP est détaillée sur les figures **FIG–7.4.1.1** et **FIG–7.4.1.2**.

Le dispositif câblé de validation des commandes à destination du système de protection utilise des boutons poussoir en technologie conventionnelle directement câblés sur les MSI du système protection (cf. section 7.3.1).

6.1. ÉQUIPEMENTS NON GRAPHIQUES

Tous les postes opérateurs sont connectés par réseau à des calculateurs redondants dédiés au fonctionnement du MCP. Le PU (Processing Unit) est le calculateur de traitements et les SU (Server Unit), RAID (Redundancy Array of Independent Disk), SUJB (Server Unit JukeBox) et JukeBox sont les calculateurs d'archivage et d'affichage et de gestion des MOP, FA, FTA. [].

6.1.1. Processing Unit

Dans le fonctionnement du MCP, le PU remplit les tâches suivantes :

- Interface avec les automates de niveau 1 (émission des ordres opérateurs, réception des informations émises par le niveau 1),
- Gestion des données temps-réel, des évènements significatifs (alarmes, situations de tranche...), des actions opérateurs,
- Gestion centralisée des alarmes,
- Traitements de données au niveau 2,
- Enregistrement des données temps-réel, des évènements significatifs et des actions opérateurs,
- Surveillance des calculateurs du MCP,
- Serveur de son du système de sonorisation informatisé.

Les PU sont des serveurs [] fonctionnant sous le système d'exploitation [].

6.1.2. Server Unit et RAID

Dans le fonctionnement du MCP, le SU remplit les tâches suivantes :

- Gestion des fichiers HTML. Les fonds de plan des FA, MOP et FTA sont enregistrés sur le RAID. Par suite les états d'avancements des MOP, les statuts des MOP et les statuts des FA sont également gérés par le SU et enregistrés sur les disques RAID,
- Gestion de l'archivage sur les disques RAID et sur DVD des données procédé ou calculées, des évènements significatifs (Alarmes, Situations de tranche ...), des actions opérateurs, etc...
- Gestion de la restitution des données archivées dans les disques RAID et sur DVD,

- Garantie de la capacité d'archivage, de la restitution rapide et de la qualité des archives (serveur applicatif pour l'analyse des données).

Nota : l'archivage n'a pas d'impact sur les tâches de conduite.

Les SU sont des serveurs [] fonctionnant sous le système d'exploitation [].

6.1.3. Server Unit JukeBox et JukeBox

Dans le fonctionnement du MCP, le SUJB gère les données mises en mémoire sur DVD. Le Jukebox permet la gravure et le stockage des DVD.

6.1.4. External Unit

Le XU assure l'interface d'échange de données entre le MCP et le niveau 3. Il permet de transmettre des données d'état de tranche vers l'extérieur et également de recevoir de l'extérieur des données de consignation.

Les XU sont des serveurs [] fonctionnant sous le système d'exploitation [].

6.1.5. Terminal Bus

Le Terminal Bus est un réseau Ethernet [].

Les commutateurs réseaux [] du Terminal Bus sont reliés par fibre optique. [] commutateurs sont alors configurés pour la surveillance de l'anneau. [].

En fonctionnement normal, la logique de surveillance du commutateur en mode gestion de la redondance ouvre l'anneau et émet sur le réseau des trames de tests. Les retours des trames de tests sont surveillés par les [] commutateurs. [].

Le Terminal Bus est donc un réseau robuste à une défaillance simple d'un quelconque élément.

6.2. ÉQUIPEMENTS GRAPHIQUES

Les équipements graphiques du MCP sont les postes opérateurs ([]), le synoptique et les périphériques d'impressions ([]).

Un poste opérateur (y compris le synoptique) est un équipement composé des matériels suivants :

- De 2 à 5 Ecrans,
- Clavier et souris,
- Calculateurs :

  []

- Commutateurs :

  []

- Matériel de sonorisation (carte son, amplificateur et haut-parleur).

6.2.1. Operating Terminal (OT)

Dans le fonctionnement d'un poste opérateur, un OT remplit les tâches suivantes :

- Gestion des droits utilisateurs,

- Gestion de l'IHM (rafraîchissement des indicateurs, des données des images de conduite, etc. ...). Les fonds de plan des images de conduite sont enregistrés dans l'OT,
- Gestion des alarmes,
- Gestion du clavier et du déplacement de la souris sur les écrans du PO.

Nota 1 : L'OT Bus Switch assure la connexion entre l'OT et les TC et le [].

Nota 2 : Le [] permet d'interfacer le couple clavier souris à l'ensemble des TC du PO . L'affectation du TC « actif » est piloté par les OT du PO.

Les OT sont des serveurs [] fonctionnant sous le système d'exploitation [].

6.2.2. Thin Client (TC)

Dans le fonctionnement d'un poste opérateur, un TC remplit les tâches suivantes :

- Affichage sur un écran des signalisations et des données transmises par un OT,
- Connexion avec les OT pour le passage des commandes,
- Gestion du système de sonorisation informatisé.

6.2.3. Configurations matérielles

Les figures FIG–7.4.1.3, FIG–7.4.1.4, FIG–7.4.1.5, FIG–7.4.1.6 et FIG–7.4.1.7 présentées en annexe décrivent les architectures informatiques des équipements graphiques du MCP.

7. ALIMENTATION ÉLECTRIQUE

L'alimentation des équipements du MCP est de type secourue et à tolérance de micro-coupure.

La partie « calculateurs » du MCP (qui n'est pas situé en salle de commande) est alimentée électriquement par les divisions 1 et 4 de sorte que la perte d'une de ces deux sources d'alimentation ne conduise pas à la perte totale du MCP. Les postes opérateurs en salle de commande sont alimentés par les divisions 1, 2, 3 et 4, de sorte que la distribution électrique en salle de commande principale permet de minimiser l'impact sur les équipements situés en salle de commande d'une perte d'alimentation électrique d'une division. Les équipements graphiques de la SdR sont alimentés par les divisions 1 et 4, de sorte que la perte d'une de ces deux sources d'alimentation ne conduit pas à la perte totale des équipements de la SdR. Les équipements graphiques du LTC sont alimentés par la division 3.

8. DISPOSITIONS PRISES POUR LA RÉALISATION DES ESSAIS PÉRIODIQUES

Le MCP fait l'objet d'un programme d'essais périodiques conformément aux exigences de la section « généralités » du chapitre IX des RGE permettant notamment de vérifier le respect de l'ensemble des critères fonctionnels définis au § 0.2..

9. ANALYSE DE SÛRETÉ

Le MCP tel que réalisé est conforme aux exigences de sûreté dont il est redevable.

10. SYSTÈME TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

TAB–7.4.1.1 CLASSEMENT CONTRÔLE-COMMANDE DES ÉQUIPEMENTS DU MCP

Equipements de tranche		**Classements CC**
Postes Opérateurs 5 écrans SdC/SdR		E2
Synoptique		NC
Postes Opérateurs Minimaux		NC
Poste opérateur 2 écrans SdR		E2
Poste opérateur LTC		NC
Poste opérateur REN-RES		NC
Calculateurs de traitements (PU / OT)		E2
Calculateurs d'archivage	(SU / RAID)	E2
	(SUJB / Jukebox)	NC
Terminal Bus		E2
Imprimantes		NC
Equipements de sonorisation des postes opérateurs		NC
Calculateurs d'interface avec l'extérieur (XU)		NC
Equipements au BTE		**Classement CC**
Poste opérateur BTE		NC
Calculateurs de traitements au BTE (PU / OT)		NC
Calculateurs d'archivage au BTE	(SU / RAID / SUJB)	NC
Terminal Bus au BTE		NC
Imprimante au BTE		NC
Equipements de sonorisation du poste opérateur du BTE		NC

TAB–7.4.1.2 CLASSEMENT SISMIQUE DES ÉQUIPEMENTS DU MCP

Equipements de tranche		Classements SC	Requis
Postes Opérateurs 5 écrans SdC/SdR		SC1	Opérabilité
Synoptique		SC2	Stabilité
Postes Opérateurs Minimaux		SC2	Stabilité
Poste opérateur 2 écrans SdR		SC1	Opérabilité
Calculateurs de traitements (PU / OT)		SC1	Opérabilité
Calculateurs d'archivage	(SU / RAID)	SC1	Opérabilité
	(SUJB / Jukebox)	SC2	Stabilité
Terminal Bus		SC1	Opérabilité
Imprimantes en SdC/SdR		SC2	Stabilité
Calculateurs d'interface avec l'extérieur (XU)		SC2	Stabilité
Equipements de sonorisation des postes opérateurs		SC2	Stabilité

TAB–7.4.1.3 CLASSEMENT DE SÛRETÉ DES FONCTIONS DU MCP

Fonction	Classement de sûreté
Affichage	F2
Afficher des images de conduite, des courbes, des listes, des fiches d'alarmes, des modes opératoires, des fiches techniques additionnelles, ...	
Rafraîchir des images de conduite, des courbes et des listes en temps réel	
Désigner l'objet avec lequel l'opérateur interagit	
Naviguer entre les différentes images	
Impression	NC
Imprimer des images de conduite, des listes, des fiches d'alarmes, des modes opératoires, des fiches techniques additionnelles, ...	
Contrôle-commande	F2
Envoyer des commandes	
Afficher les comptes rendus de commandes	
Alarme	F2
Avertir les opérateurs d'alarmes en apparition / en disparition	
Gérer les listes d'alarmes	
Traitement	F2
Gérer de(s) base(s) de données	
Élaborer des informations et lancer des traitements en cas de changement d'état (Situations de tranche …)	
Surveillance	NC
Auto-surveillance	
Interface	NC
Transmettre des informations depuis le contrôle-commande de tranche vers l'extérieur	
Acquérir des informations depuis l'extérieur vers le contrôle-commande de tranche	

Archivage	NC
Archivage des données logiques et analogiques	
Récupération des données archivées	
Administration et Maintenance	NC
Fournir une aide à l'analyse et à la maintenance	
Assurer les tâches de sécurité informatique (par exemple la gestion des accès aux PO, …)	
Gérer les introductions de données en fonctionnement	

FIG–7.4.1.1 ARCHITECTURE GÉNÉRALE DU MCP DE TRANCHE

FIG–7.4.1.2 ARCHITECTURE GÉNÉRALE DU MCP AU BTE

[]

FIG–7.4.1.3 STRUCTURE INFORMATIQUE D'UN PO 5 ÉCRANS

[]

Nota : les supports physiques de raccordement des matériels sont : [].

FIG–7.4.1.4 STRUCTURE INFORMATIQUE DU SYNOPTIQUE

[]

Nota : les supports physiques de raccordement des matériels sont : [].

FIG–7.4.1.5 STRUCTURE INFORMATIQUE D'UN POM

[]

Nota : les supports physiques de raccordement des matériels sont : [].

FIG–7.4.1.6 STRUCTURE INFORMATIQUE DU PO []

[]

Nota : les supports physiques de raccordement des matériels sont : [].

FIG–7.4.1.7 STRUCTURE INFORMATIQUE DES PO REN/RES ET PO BTE

[]

Nota : les supports physiques de raccordement des matériels sont : [].

SOMMAIRE

FIGURES :

.7.4.2 ARCHITECTURE DU SYSTÈME D'AUTOMATISME DE TRANCHE (PAS)

0. EXIGENCES DE SÛRETÉ

Le système de contrôle-commande PAS est assujetti aux exigences de sûreté applicables aux systèmes de contrôle commande F2, du fait de sa gestion du contrôle-commande associé aux fonctions de sûreté F2.

Le système PAS assure le traitement des actions automatiques et manuelles, et la surveillance associée, nécessaires à l'accomplissement des fonctions de sûreté énoncées ci-dessous.

0.1. FONCTIONS DE SÛRETÉ

Le PAS participe aux trois fonctions fondamentales de sûreté (maîtrise de la réactivité, évacuation de la puissance résiduelle et confinement des substances radioactives) au titre de la gestion des fonctions F2N (à l'exception des fonctions chaudière classées F2N allouées au RCSL) de l'îlot nucléaire et du site.

Il intègre principalement :

- les fonctions automatiques et manuelles utilisées en régime normal,
- les fonctions de régulation du fonctionnement normal,
- les fonctions d'aide à la conduite opérateur,
- certaines limitations,
- les LCO hors LCO cœur,
- des fonctions de traitement/affichage des informations et alarmes.

De plus, il réalise la surveillance et le contrôle des fonctions classées F2N.

Le PAS intègre aussi les fonctions NC, non contributives aux fonctions fondamentales de sûreté, de la tranche (à l'exception de fonctions NC allouées à d'autres systèmes spécifiques dits « dédiés », tels que le contrôle-commande de la turbine ou de l'alternateur par exemple).

Le PAS est rattaché à la 1ère ligne de défense en profondeur dite de prévention des incidents et accidents (voir section 7.1.1).

La gestion des fonctions F2 classées séisme (F2E) est dédiée au système SAS (voir section 7.3.2).

0.2. EXIGENCES RELATIVES À LA CONCEPTION

Au titre des fonctions F2 dont il assure la gestion des automatismes et des commandes manuelles et la surveillance liée (dont les fonctions de « gestion de priorité des commandes » et « surveillance de l'actionneur » du PACS définies en section 7.3.6), le système PAS doit satisfaire aux exigences énoncées ci-après. Ces exigences doivent être respectées pour l'ensemble des fonctions d'automatisme gérées par le système PAS .

0.2.1. EXIGENCES ISSUES DES CLASSEMENTS FONCTIONNEL ET MÉCANIQUE

0.2.1.1. CLASSEMENT FONCTIONNEL DU SYSTÈME

Le système PAS doit être classé F2 de sûreté, conformément au classement indiqué au sous-chapitre 3.2.

0.2.1.2. CRITÈRE DE DÉFAILLANCE UNIQUE (ACTIVE)

Le critère de défaillance unique ne s'applique pas au système PAS (ne gérant pas de fonctions F1).

0.2.1.3. ALIMENTATIONS ÉLECTRIQUES SECOURUES

L'exigence d'une alimentation électrique secourue des équipements PAS doit être définie au cas par cas. Dans le cas où cette exigence doit être satisfaite, l'alimentation doit être secourue par les groupes diesels principaux. Par ailleurs, cette alimentation doit alors être du type « sans coupure », garantissant une alimentation même pendant le basculement alimentation normale / alimentation par diesel.

En règle générale, le système PAS est alimenté par la même division / section que celle du procédé dont il assure le pilotage.

0.2.1.4. QUALIFICATION AUX CONDITIONS DE FONCTIONNEMENT

Les équipements PAS doivent rester opérationnels en conditions post-accidentelles, et doivent en conséquence respecter les exigences de qualification définies au sous-chapitre 3.7.

Par ailleurs, ces équipements doivent être opérationnels pour les conditions environnementales normales et extrêmes des locaux automates dans lesquels ils sont implantés. Ces conditions sont définies au sous-chapitre 9.4.

0.2.1.5. CLASSEMENT MÉCANIQUE, ÉLECTRIQUE, CONTRÔLE-COMMANDE

Les classements mécanique et électrique ne s'appliquent pas aux équipements de contrôle-commande.

Conformément aux principes définis au sous-chapitre 3.2, le classement de contrôle-commande des équipements PAS est E2.

Les équipements PAS gérant des traitements non classés sont Non Classés (NC), vu du « classement » de contrôle-commande.

0.2.1.6. CLASSEMENT SISMIQUE

Le PAS ne comporte pas de fonctions requises opérables en cas de séisme (fonctions F2N).

Les équipements PAS implantés dans des locaux où ils cohabitent avec des équipements classés séisme 1 (SC1) doivent être classés séisme 2 (SC2) avec un requis de stabilité au titre de la non agression de matériels SC1 en cas de séisme.

0.2.1.7. EXIGENCE SUPPLÉMENTAIRE

Sans objet

0.2.2. AUTRES EXIGENCES

0.2.2.1. RÈGLES FONDAMENTALES DE SÛRETÉ

Système PAS non concerné.

0.2.2.2. DIRECTIVES TECHNIQUES

Les directives techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/04 "Options de sûreté du projet de réacteur EPR" (et plus spécifiquement G3.4 et G3.7) doivent être prises en compte à la conception du système PAS.

0.2.2.3. TEXTES SPÉCIFIQUES EPR

Le système PAS doit satisfaire aux exigences énoncées dans le RCC-E (voir sous-chapitre 1.6).

0.2.3. AGRESSIONS

0.2.3.1. Exigences — protection vis-à-vis des agressions internes

Les fonctions du système PAS doivent être protégées vis à vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.2.3.2. Exigences — protection vis-à-vis des agressions externes

Les fonctions du système PAS doivent être protégées vis à vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du système PAS.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Le système PAS doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

La mission du PAS est d'assurer la gestion des fonctions de contrôle commande requises F2N et NC (définies au § 0.1.) de la tranche.

2. FONCTIONS ASSURÉES

Les fonctions de contrôle commande assurées par le PAS sont les suivantes :

- traitements des données : acquisition, conditionnement et mise à disposition,
- traitements de calculs applicatifs : régulations, élaboration de commandes individuelles et groupées (simultanées ou séquentielles), hiérarchisation des priorités de commande, élaboration d'informations diverses à destination des autres unités de contrôle-commande, etc.
- traitements de surveillance : traitement des comptes-rendus d'état et de défauts, élaboration des alarmes et signalisations.

3. BASE DE CONCEPTION

3.1. EXIGENCES DE DISPONIBILITÉ

Les principales exigences conditionnant la disponibilité du PAS sont liées à la fiabilité et à la maintenabilité du système, qui se traduisent par :

- limiter les pertes du PAS dues à la perte de l'un de ses composants (par la redondance de ses composants notamment),
- faciliter la maintenance et la réparation du PAS pour réduire au minimum sa période d'indisponibilité.

3.2. PERFORMANCES REQUISES

Les exigences concernant les temps de réponse du PAS dépendent des fonctions réalisées par ce système.

Les allocations des traitements de contrôle-commande sont établies de manière à respecter l'exigence de temps de réponse de chacune des fonctions à réaliser.

3.3. EXIGENCES RELATIVES À L'ENVIRONNEMENT

Les conditions environnementales que les équipements PAS doivent supporter sont liées à la température et à l'humidité relative des locaux abritant ces matériels. Ces caractéristiques environnementales sont définies au sous-chapitre 9.4, autant pour les conditions normales que pour les conditions extrêmes.

3.4. EXIGENCES RELATIVES À L'INTERFACE HOMME MACHINE

PAS non concerné.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

La structure et la composition du PAS sont dictées par les exigences de sûreté applicables. Par ailleurs, l'allocation des fonctions en son sein, est dictée par les exigences fonctionnelles.

Ces exigences fonctionnelles portent sur :

- le classement fonctionnel des traitements (qui dans le cas du PAS peuvent être F2 ou NC),
- la division ou section électrique (en correspondance avec celle des actionneurs et capteurs à gérer),
- la typologie de traitements à effectuer (pouvant conditionner le choix du type de cartes d'entrée/ sorties par exemple),
- la performance requise des traitements (temps de réaction, temps de propagation, précision),
- les regroupements / exclusions de traitement, qui requièrent que certains traitements soient groupés (en regard d'un requis de perte simultanée de ces traitements lors d'un dysfonctionnement de la partie du système de CC qui les gèrent), ou inversement, que certains groupes de traitement soient gérés par des unités matérielles PAS différentes (en regard d'un requis de maintien en service d'un groupe de traitements, malgré la perte de certains autres lors du dysfonctionnement),
- la défense en profondeur.

Par ailleurs, la structure du PAS prend en compte la segmentation du procédé piloté, dicté par le nombre, l'emplacement géographique et la typologie des interfaces des actionneurs et capteurs à gérer.

Pour une fonction de sûreté donnée, il y a différentes combinaisons possibles, par exemple :

[]

Afin d'éviter qu'une défaillance interne ait un effet sur plus d'un train mécanique, en règle générale, chaque train mécanique est commandé par un sous-ensemble du PAS situé dans la même division ou section que le train.

4.2. INSTALLATION

Les équipements gérant les fonctions PAS sont installés dans les [] divisions 1 à 4 des bâtiments BAS-BL, dans [] l'îlot conventionnel (BLNC), et dans [] du BTE.

Les équipements PAS sont répartis :

- en correspondance avec l'emplacement et la division/section des organes (actionneurs et capteurs) gérés,
- en correspondance avec les alimentations électriques des divisions ou sections,
- selon l'espace disponible pour leur implantation.

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CC

Le PAS échange des informations avec :

- l'instrumentation procédé : échanges liés à l'acquisition des mesures et états,
- les IHM, MCP (en SdC et SdR) et MCS : échanges liés à la conduite par les opérateurs,
- les systèmes RCSL, PS, SAS et SAS RRC-B : échanges liés à la gestion des automatismes de la tranche,
- les outils d'ingénierie, de diagnostic et de maintenance décrits en section 7.6.1,
- les cellules électriques (tableaux électriques) et les organes de commande réglants (électro-positionneurs, etc.) : échanges liés à la commande des actionneurs,
- les systèmes "dédiés" (armoires du CC turbine, etc.) : échanges liés à la gestion des automatismes de la tranche et surveillance d'équipements.

5. CONFIGURATIONS OPÉRATIONNELLES

La configuration (d'un point de vue matériel et fonctionnel) du PAS est indépendante de la situation. L'allocation du traitement dépend seulement des critères fonctionnels et des principes d'allocation des traitements du système de contrôle commande. La configuration du PAS est, de ce point de vue, constante.

La configuration du PAS n'est dépendante que du dispositif suivant : en cas de défaut de fonctionnement d'une carte active, le système commute automatiquement sur la seconde carte, qui était en attente. Ce principe s'applique à toute carte redondée du PAS (cartes CPU et cartes de gestion de la communication).

6. TECHNOLOGIE

La plate-forme de contrôle commande retenue pour la réalisation du contrôle commande standard EPR est la plate-forme SPPA –T2000 développée par [].

6.1. SYSTÈME D'AUTOMATISME AS620B

Le système [] se compose d'un ensemble d'unités d'automatisme (UA).

Une UA est composée :

- d'un couple d'unités centrales redondantes (dites AP, Automation Processor), chaque AP est indépendante et contient :
  - une alimentation (PS, Power Supply),
  - une carte CPU [] réalisant les traitements,
  - une carte de communication (CP [], Communication Processor) permettant d'interfacer l'UA avec les réseaux Island Bus/Plant Bus,
  - un module d'interface (IM []) avec l'un des deux bus d'UA,
- de racks de cartes d'entrées/sorties contenant :
  - des modules FUM (FUnction Module),
  - deux modules d'interface (IM [], Interface Module) permettant la connexion du rack aux deux bus d'UA,
  - un bus de fond de panier assurant la liaison entre les modules FUM et les modules d'interface,
- de deux bus d'UA (ou d'armoire, une UA pouvant être répartie sur une à deux armoires), chaque bus étant connecté à une AP et à l'ensemble des racks de modules FUM composant l'UA,
- une carte de signalisation des défauts (DEDA).

Les 2 AP redondantes communiquent entre elles au moyen d'une paire de modules d'interface IM[] (côté AP-A) et IM[] (côté AP-B), via le « redundancy link » (voir **FIG–7.4.2.1**).

Un bus d'armoire redondant et un bus de fond de panier redondant dans chaque rack assurent la communication entre les différents modules.

Les cartes d'entrées/sorties utilisées sont :

- FUM [], cartes d'acquisition capteurs TOR,
- FUM [], cartes de commande actionneurs TOR,
- FUM [], cartes d'acquisition capteurs ANA,
- FUM [], cartes d'acquisition capteurs de température,
- FUM [], cartes de commande actionneurs ANA,
- FUM [], cartes d'entrées/sorties TOR pour échanges en fil à fil,
- FUM [], cartes d'entrées/sorties ANA pour échanges en fil à fil et acquisition de signaux ANA en tension.

6.2. RÉSEAUX

Les UA du PAS :

- ne sont pas reliées au SAS Bus,
- sont reliées entre elles, par des « Island Bus » (les UA d'une même division/section et appartenant au PAS sont regroupées en îlot) et par un «Plant Bus BTE » pour les UA du PAS BTE.

Les différents éléments sont connectés aux réseaux via des commutateurs réseaux ([]) ; les CP [] sont connectés aux Island Bus ou au Plant Bus BTE via des [] ; les Island Bus et le Plant Bus BTE sont connectés au Plant Bus respectivement via des [] et des CM [].

6.3. GESTION DE LA REDONDANCE

Chaque UA possède 2 AP redondantes, l'une est dite « maître » et l'autre « esclave ». Les 2 AP sont synchronisées et effectuent les traitements en parallèle, à partir des mêmes données d'entrées (informations reçues des cartes FUM et/ou des cartes CP []). Les communications réseau avec d'autres UA et avec le niveau 2 sont réparties entre les 2 cartes CP [] des AP maître et esclave.

Une défaillance détectée entraîne des séquences de diagnostic et de redémarrage des AP, et peut conduire à permuter les rôles maître/esclave des AP.

L'ensemble de cette architecture permet ainsi de répondre aux exigences de disponibilité, énoncées dans le paragraphe 3.1.

7. ALIMENTATION ÉLECTRIQUE

Les armoires PAS sont alimentées de manière redondante à partir de deux sources électriques différentes, par des convertisseurs AC/DC et DC/DC indépendants. La première source électrique est fournie par le tableau de distribution principal [] V AC triphasé, et la seconde est fournie par le tableau de sous-distribution [] V DC.

L'alimentation des armoires du PAS n'est pas nécessairement requise secourue. Cependant, cette alimentation est secourue pour des considérations de disponibilité globale du CC et d'exploitation de la tranche. [].

Ainsi, les tableaux [] réputés « sans coupure » et alimentant les armoires PAS de l'îlot nucléaire sont secourus par les diesels principaux (LHP/Q/R/S) dans les quatre divisions et par les diesels de secours (LJP/LJS) dans les divisions 1 et 4.

Quant aux tableaux [] alimentant les armoires PAS de l'îlot conventionnel et du site, ils sont secourus par les diesels principaux (LHQ/LHR), mais ne sont pas alimentés par les diesels de secours ; en outre ils bénéficient de batteries d'une autonomie de []h pour assurer le caractère sans coupure de l'alimentation. Ces tableaux ne sont pas classés de sûreté (NC).

Le niveau de tension automate (après transformation) est de [] V DC. Chaque train mécanique est contrôlé par un sous-ensemble du PAS, situé dans et alimenté par la même division ou section que le train mécanique.

Le réglage à la tension exigée par les armoires PAS est réalisé en interne aux armoires dédiées à leur alimentation. [].

8. DISPOSITIONS PRISES POUR RÉALISER LES TESTS PÉRIODIQUES

Le PAS fait l'objet d'un programme d'essais périodiques conformément aux exigences de la section «généralités» du chapitre IX des RGE permettant notamment de vérifier la disponibilité des fonctions de sûreté définies au **§ 0.1.**.

9. ANALYSE DE SÛRETÉ

Le système est conforme aux exigences de sûreté spécifiées au paragraphe 0 et au sous-chapitre 7.1.

10. SYSTÈME TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

FIG–7.4.2.1 CONFIGURATION D'UNE UA PAS

FIG–7.4.2.2 INTERFACE AP / FUM POUR LE PAS

SOMMAIRE

TABLEAUX :

FIGURES :

.7.4.3 ARCHITECTURE DU SYSTÈME DE CONTRÔLE, DE SURVEILLANCE ET DE LIMITATION DU RÉACTEUR (RCSL)

0. PRESCRIPTIONS DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

Le système RCSL doit participer aux fonctions de sûreté suivantes :

- contrôle de la réactivité,
- évacuation de la puissance résiduelle.

0.2. CRITÈRES FONCTIONNELS

0.2.1. Contrôle de la réactivité

Le système RCSL doit assurer :

- les fonctions de contrôle du cœur, en particulier le contrôle automatique des grappes,
- les fonctions de limitation des conditions opérationnelles (LCO) liées au cœur,
- les fonctions de limitation des paramètres du cœur,
- les fonctions permettant de gérer la séquence RRC-A de perte du PS,
- les fonctions permettant de gérer la séquence RRC-A de dilution.

Il doit assurer la surveillance du cœur et déclencher si nécessaire un arrêt partiel du réacteur.

0.2.2. Évacuation de la puissance résiduelle

Le système RCSL doit assurer :

- les fonctions de limitation primaire / secondaire,
- la fonction RRC-A de chute automatique de toutes les grappes en cas de perte totale de l'eau alimentaire.

0.3. EXIGENCES RELATIVES À LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Le classement fonctionnel du RCSL fait l'objet d'une exception aux règles de classement. Le classement du RCSL jouant un rôle vis-à-vis de la sûreté est présenté dans la section 3.2.1.

0.3.1.2. Critère de défaillance unique (active et passive)

Le critère de défaillance unique ne s'applique pas au RCSL.

0.3.1.3. Alimentationélectrique de secours

Le RCSL ne requiert pas d'alimentations électriques secourues.

0.3.1.4. Qualification aux conditions accidentelles

Les équipements assurant une fonction de sûreté F2 doivent être qualifiés pour rester fonctionnels dans des conditions post-accidentelles.

Les exigences résultantes pesant sur ces équipements (intégrité, disponibilité, capacité de fonctionnement, etc.) sont présentées dans le sous-chapitre 3.7.

0.3.1.5. Classements des équipements mécaniques, électriques et de contrôle-commande

Le classement mécanique ne s'applique pas au système RCSL.

Les classements électrique et de contrôle commande doivent suivre les règles formulées dans la section 3.2.1. Il en ressort que le classement électrique du système doit être EE2.

Le classement contrôle-commande est le suivant :

- E2 pour la partie F2,
- NC pour la partie NC.

0.3.1.6. Classement sismique

Le système RCSL ne nécessite pas de classement sismique SC1.

0.3.2. Exigences réglementaires

0.3.2.1. Textes officiels

Le document général "Options de sûreté du projet de réacteur EPR" (lettre DSIN 079/2000) s'applique au système RCSL.

0.3.2.2. Règles fondamentales de sûreté

L'application des règles fondamentales de sûreté est présentée dans le sous-chapitre 1.7.

0.3.2.3. Directives techniques

Parallèlement aux prescriptions générales indiquées dans le chapitre A.1 "Approche générale de la sûreté", les exigences s'appliquant au système RCSL sont présentées dans les sections suivantes (voir section 1.7.0) :

- A.2.1 – comportement du réacteur en régime transitoire :
  « La mise en service non nécessaire de systèmes de sûreté doit être évitée autant qu'il est possible. Pour éviter de telles actions, l'introduction de fonctions de limitation appropriées peut être judicieuse, c'est-à-dire des fonctions de maîtrise supplémentaires qui agissent quand les systèmes de régulation d'exploitation ne sont pas capables de garder les variables contrôlées à l'intérieur des limites spécifiées pour le fonctionnement normal. »
- G3 – conception de l'ensemble contrôle-commande :
  « En principe, la démonstration de sûreté devrait être faite en considérant les moyens utilisés normalement par les opérateurs dans la salle de commande principale. Cependant, la mise en place dans la salle de commande principale d'une interface homme-machine conventionnelle classée F1B pour pouvoir réaliser la démonstration de sûreté avec des équipements classés F1 alors que les opérateurs utiliseraient une interface homme-machine informatisée classée F2, pourrait être acceptée pour autant que :

  a) le matériel et l'architecture de l'interface homme-machine informatisée satisfassent aux exigences applicables aux systèmes F1B,

b) le logiciel correspondant satisfasse à des exigences de qualification détaillées à proposer par le concepteur,

c) les moyens mis en œuvre pour la détection et la signalisation des défaillances de fonctions et d'équipements F2 essentiels de l'interface homme-machine informatisée satisfassent aux exigences applicables aux fonctions et équipements F1B. »

0.3.2.4. Règles de conception électriques

Les règles de conception pour les équipements électriques ainsi que les règles spécifiques à appliquer à l'ensemble du contrôle-commande sont fournies dans le RCC-E complété des données de projet du réacteur EPR définies dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.3.3. Agressions internes et externes

0.3.3.1. Agressions internes

Le système RCSL doit être protégé vis-à-vis des conséquences des agressions internes si sa perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Le système RCSL doit être protégé vis-à-vis des conséquences des agressions externes si sa perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.4. ESSAIS

0.4.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du système RCSL.

0.4.2. Surveillance en exploitation

Sans objet.

0.4.3. Essais périodiques

Le système RCSL doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

Les équipements F2 qui ne sont pas sollicités en continu doivent être vérifiés périodiquement.

1. MISSIONS

Le système RCSL doit assumer une tâche d'exploitation, c'est-à-dire une tâche qui contribue au fonctionnement normal de la centrale (PCC-1).

2. FONCTIONS SUPPORTÉES

Comme défini dans le paragraphe 3.2 de la section 7.2.1, le système RCSL est affecté aux fonctions de contrôle-commande F2 et NC pour le contrôle et la surveillance du fonctionnement du cœur. Cela inclut :

- des fonctions de contrôle du cœur,
- des fonctions LCO liées au cœur,

- des fonctions de limitation liées au cœur,
- des fonctions de limitation primaire / secondaire,
- la fonction permettant de gérer la séquence RRC-A de perte totale en eau alimentaire,
- des fonctions permettant de gérer la séquence RRC-A de perte du PS,
- des fonctions permettant de gérer la séquence RRC-A de dilution.

La liste des fonctions d'application typiques liée à chaque type de fonction d'application effectuée par le système RCSL est proposée dans le tableau **TAB–7.4.3.2**.

3. BASES DE CONCEPTION

3.1. PERFORMANCES REQUISES

Les exigences concernant le temps de réponse du RCSL dépendent des fonctions réalisées.

De manière générale :

- toutes les fonctions LCO ont une exigence de temps de réponse de [] (mis à part la fonction LCO de désalignement de grappe, la fonction LCO sur la température moyenne et la fonction LCO sur la limite d'insertion),
- les fonctions de contrôle n'ont pas d'exigence de temps de réponse (mis à part la fonction de contrôle du flux neutronique et la fonction de contrôle de surveillance de la température moyenne),
- les fonctions de limitation liées au cœur et les fonctions de limitation primaire/secondaire ont toutes une exigence de temps de réponse qui leur est propre,
- les fonctions permettant de gérer les séquences RRC-A de perte PS ont toutes une exigence de temps de réponse qui leur est propre, la plus contraignante étant celle de chute de toutes les grappes sur perte d'eau alimentaire,
- les fonctions permettant de gérer les séquences RRC-A de dilution ont toutes une exigence de temps de réponse qui leur est propre, la plus contraignante étant celle de la chaîne de prévention de la dilution.

3.2. EXIGENCES RELATIVES AUX CONDITIONS D'AMBIANCE

Voir sous-chapitre 9.4.

3.3. EXIGENCES RELATIVES A L'INTERFACE HOMME-MACHINE

L'interface homme-machine fournira aux équipes de contrôle-commande les fonctions suivantes :

- les fonctions relatives à la mise en service et à la maintenance,
- les fonctions relatives à la configuration.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Le système RCSL est composé (cf. figure **FIG–7.4.3.2**) :

- d'unités d'acquisition, distribuées dans les quatre divisions,
- d'une paire d'unités de traitement,[]
- de deux paires d'unités de commande,[]

- d'unités d'interface avec le PAS/SAS et le MCP[]

Description

Un résumé descriptif du système RCSL est donné dans le tableau **TAB–7.4.3.1**.

[]

4.2. IMPLANTATION

Le niveau de traitement du RCSL est également implanté à l'intérieur des [] des bâtiments des auxiliaires de sauvegarde 1 à 4.

L'unité de service (service unit) est installée dans le [].

4.3. INTERFACES AVEC LE RESTE DU CONTRÔLE-COMMANDE

Le système RCSL fait partie du niveau 1 de l'architecture de contrôle-commande. Ses frontières avec les autres systèmes de contrôle-commande des niveaux 0, 1 et 2 sont représentées sur la figure **FIG–7.4.3.1**.

Le système RCSL reçoit :

- du système de pré-traitement et de conditionnement (PIPS) :
  - des mesures de capteurs.
- du RPI (Système de Mesure de Positions des Grappes) :
  - la postion mesurée de chaque grappe.
- du système de protection (PS) :
  - un signal AAR,
  - un signal ATWS,
  - des signaux de limitation.
- du système de mesure de flux neutronique incore (RIC) :
  - les mesures de collectrons.
- du système de mesure de flux neutronique excore (RPN) :
  - les mesures des chambres neutroniques de puissance.
- du PAS/SAS :
  - des paramètres de procédé.
- des unités de contrôle de grappes (RodPilot®) :
  - des compte-rendus sur le mouvement des grappes.
- du CC Turbine :
  - des signaux donnant l'état de la turbine.
- du MCP :
  - des commandes [] sur des régulations automatiques,
  - les changements de séquence des grappes de contrôle,

- des consignes.

- du CC GPA :
  - des informations sur l'état de la connexion au réseau.
- du boîtier de paramétrisation (RGL) :
  - les signaux de paramétrisation du RCSL.

Le système RCSL fournit :

- au PAS/SAS :
  - des commandes et consignes,
  - le signal de chute partielle (KAE).
- aux unités de contrôle de grappes (RodPilot®) :
  - des commandes de mouvement (insertion, extraction) ou de chute de grappe.
- au MCP :
  - des paramètres de procédé,
  - des alarmes prétraitées,
  - l'état des mécanismes de grappes,
  - l'état des régulations automatiques,
  - l'état du système RCSL (auto-surveillance).
- au RMAD :
  - les positions des grappes et des groupes,
- au boîtier sonore (RGL) :
  - l'information nécessaire pour la sonorisation du mouvement des grappes.
- au MCS :
  - via le PAS/SAS : une alarme « chute toute grappes sur perte totale d'eau alimentaire ».
- au RDTME :
  - un signal déclenché sur chute de grappe initiée par le RCSL.
- au CC Turbine :
  - des commandes et consignes.
- au CC GPA :
  - des commandes et consignes.

5. MODES DE FONCTIONNEMENT

Le système RCSL est composé d'un ensemble d'unités dont l'élément principal est une CPU. La description suivante concerne le mode de fonctionnement des unités.

La figure FIG–7.4.3.3 donne des détails sur les modes de fonctionnement et leurs interactions.

Les modes de fonctionnement d'une unité sont les suivants :

DÉMARRAGE : au démarrage du processeur, les multiples étapes d'une routine d'initialisation sont exécutées. Dans un premier temps, un contrôleur d'amorçage bas niveau commande l'initialisation du matériel et déclenche une série complète d'autotests de démarrage. Après un démarrage réussi du noyau du système d'exploitation, le module INIT de l'environnement d'exploitation (RTE) prend le contrôle de la CPU pour terminer la phase d'initialisation du RTE.

Si l'initialisation venait à échouer, le fonctionnement cyclique ne démarre pas, le module INIT effectue une boucle sans fin sans activer les signaux de sortie et l'opérateur de maintenance est informé de cet état via l'unité de service.

Une fois l'initialisation terminée, le processeur de fonctions bascule en mode de fonctionnement cyclique. [].

Au redémarrage d'une unité (AU, CU, DU et MSI), ses sorties sont inhibées automatiquement [], ceci afin de permettre aux éventuels algorithmes dynamiques de se stabiliser et de réduire les risques d'actions intempestives.

FONCTIONNEMENT CYCLIQUE : le fonctionnement cyclique est le mode normal d'un processeur de fonctions. Il reste dans cet état tant qu'il n'est pas redémarré, []à la suite d'une exception causée par une défaillance matérielle aléatoire ou une coupure de courant. Le passage aux autres modes de fonctionnement ne peut être déclenché que par l'unité de maintenance.

En fonctionnement cyclique, n'importe quel signal sélectionné peut être affiché dans les diagrammes de programmation affichés sur l'unité de maintenance.

La modification des paramètres est réalisable également dans ce mode, sous couvert de validation spécifique par l'opérateur (gérée par une clé physique), instaurant ainsi une barrière administrative avant que certaines valeurs de consigne ne puissent être changées. Pendant le fonctionnement du système de contrôle-commande, seuls les paramètres désignés au préalable comme étant modifiables peuvent être changés par l'unité de maintenance, par ex. pour optimiser une boucle de régulation ou adapter les paramètres en cas d'exploitation en prolongation de cycle.

TEST : ce mode est utilisé pour le dépannage. Une validation spécifique est une condition préalable pour passer en mode « TEST » tout en tenant compte des conditions de fonctionnement de la centrale (décision de l'équipe de quart) et des modes de fonctionnement du système TELEPERM XS dans les autres trains.

Lorsqu'une unité est en mode « TEST », le traitement cyclique des fonctions applicatives est interrompu.

Les fonctions de traitement sont activées selon les conditions du test à l'aide de commandes supplémentaires envoyées par l'unité de maintenance :

- activation / désactivation des drivers d'entrée / sortie,
- activation / désactivation des fonctions d'envoi et de réception de messages,
- activation / désactivation du traitement de certains modules des diagrammes de fonctions,
- pré-positionnement des données dans les mémoires d'entrée et de sortie,
- suivi des signaux.

La sortie du mode de fonctionnement « TEST » s'effectue toujours par une réinitialisation du processeur et un redémarrage automatique. Après un temps de démarrage d'environ 10 secondes, le traitement se poursuit en mode de fonctionnement cyclique, sorties inhibées jusqu'à ce que l'opérateur de maintenance effectue l'acquittement.

DIAGNOSTIQUE : Une validation spécifique est une condition préalable pour passer en mode « DIAGNOSTIQUE » tout en tenant compte des conditions de fonctionnement de la centrale (décision de l'équipe de quart) et des modes de fonctionnement du système TELEPERM XS dans les autres trains.

En mode « DIAGNOSTIQUE », toutes les fonctions du mode « TEST » sont accessibles. Les fonctions supplémentaires sont principalement relatives au chargement logiciel. Dans des cas très exceptionnels des routines de test spécifiques peuvent être chargées et exécutées.

La sortie du mode « DIAGNOSTIQUE » se fait toujours par réinitialisation du processeur, suivie d'un redémarrage automatique. De même que pour le mode « TEST », après un temps de démarrage d'environ 10 secondes, le traitement se poursuit en mode de fonctionnement cyclique, sorties inhibées, jusqu'à ce que l'opérateur de maintenance effectue l'acquittement.

D'un point de vue système, les modes de fonctionnement sont les suivants :

- le RCSL est considéré en fonctionnement normal si toutes ses unités sont en fonctionnement cyclique,
- le RCSL est considéré en fonctionnement dégradé si une ou plusieurs unités sont en défaut,
- le RCSL est considéré hors service si toutes ses unités sont éteintes.

Clés physiques de validation

Un ensemble de clés physique, communes aux 4 divisions du RCSL permet d'autoriser les modes TEST et DIAGNOSTIC ainsi que la modification des paramètres.

- une clé permet de choisir la division (1 à 4) pour la modification des paramètres ou le passage en mode TEST ou DIAGNOSTIC,
- une clé permet la modification des paramètres,
- une clé permet le passage en mode TEST ou DIAGNOSTIC.

Le choix de la division puis l'activation par clé de la modification des paramètres, des modes TEST ou DIAGNOSTIC autorise ces actions sur une division seulement.

Les signaux issus de ces verrouillages à clé ont le même niveau de classement que les unités d'acquisition (MSI). Le coffret de changement de mode, abritant ces clés est lui non classé.

6. TECHNOLOGIE UTILISÉE

La technologie utilisée pour implémenter le système RCSL est le TELEPERM XS (CC numérique)[].

7. ALIMENTATION ÉLECTRIQUE

Le système RCSL doit être alimenté par une alimentation ininterruptible à la tension appropriée : [].

Chaque armoire est raccordée à deux alimentations [] redondantes. Les arrivées de ces alimentations doivent être isolées l'une de l'autre, par exemple à l'aide de diodes. En fonctionnement normal, les deux alimentations [] doivent être alimentées par l'alimentation ininterruptible (UPS) de la division correspondante.

Une description des alimentations électriques des armoires TXS est donnée dans la section 7.3.1 (relative au système de protection).

8. DISPOSITIONS MISES EN ŒUVRE AU TITRE DE LA MAINTENANCE ET DES ESSAIS PÉRIODIQUES

L'unité de service (service unit) est utilisée pour la maintenance et les essais périodiques.

9. TEL QUE RÉALISÉ

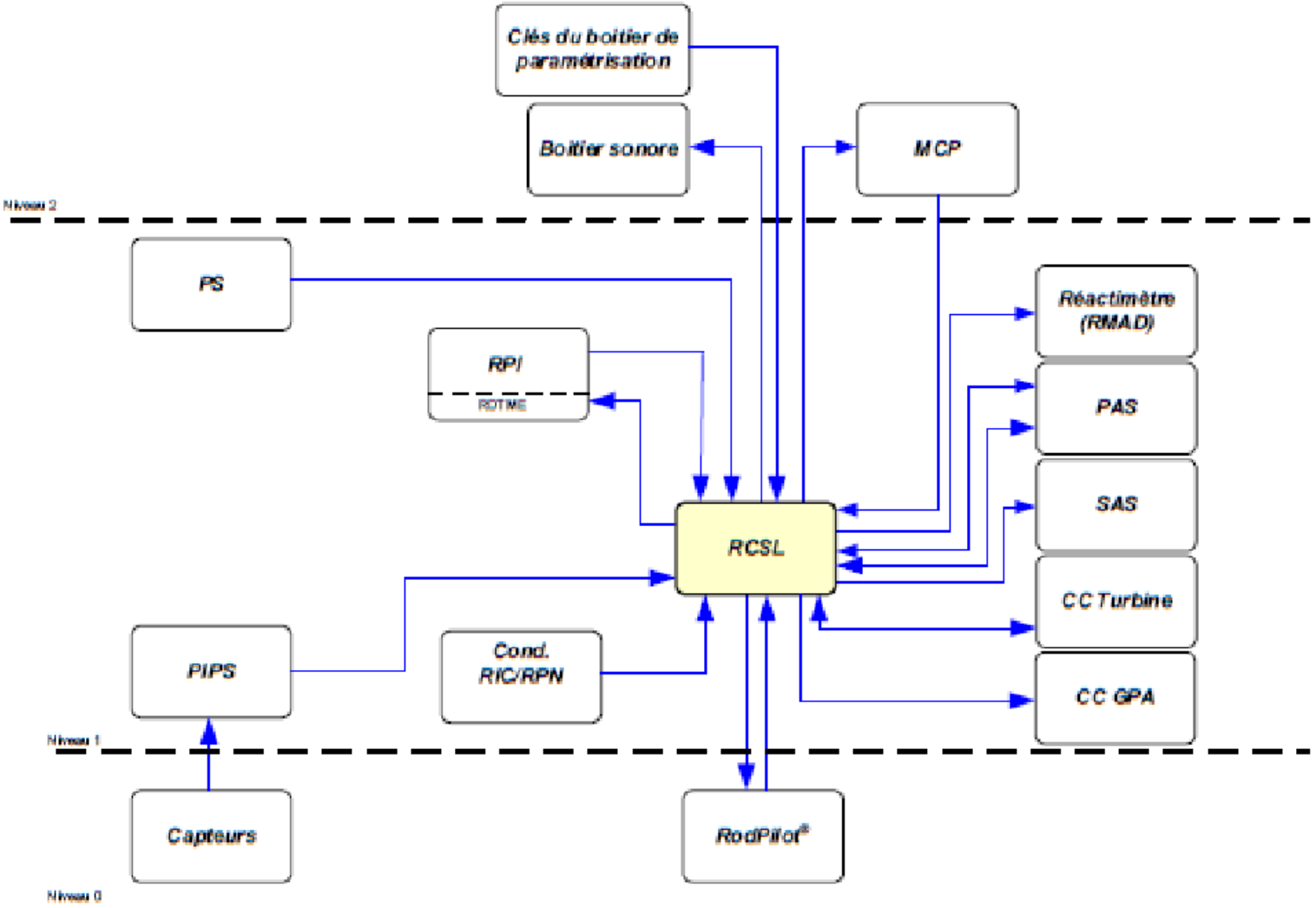
A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

TAB–7.4.3.1 DESCRIPTION DU SYSTÈME RCSL

TAB–7.4.3.2 FONCTIONS D'APPLICATION TYPIQUES ASSURÉES PAR LE SYSTÈME RCSL

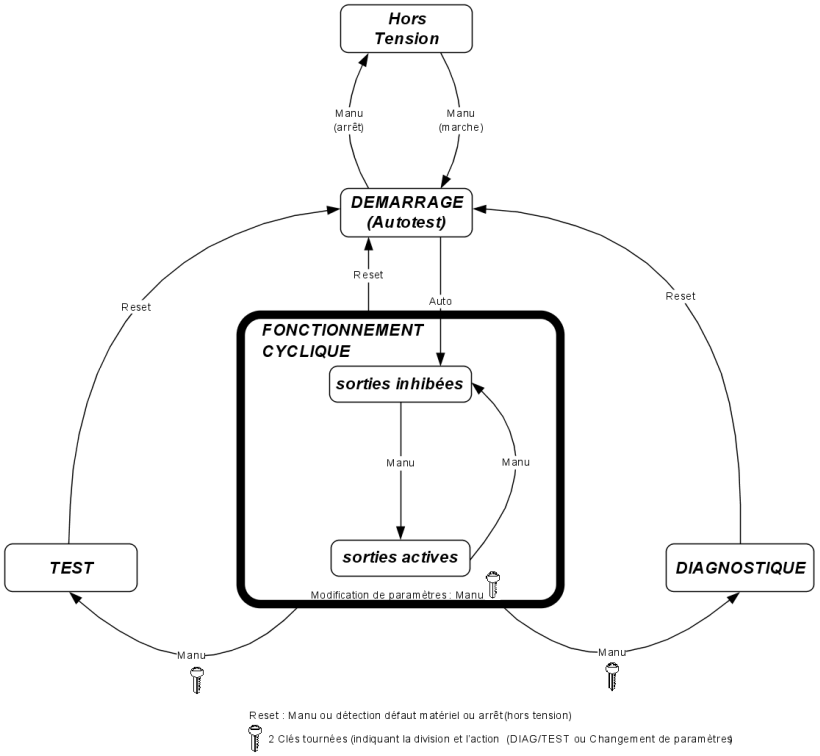
Application typique	**Type de fonctions d'application**			
Fonctions	Fonction de contrôle	Fonctions de surveillance LCO	Fonction de Limitation	Fonction permettant de gérer les séquences RRC-A
Asservissement	X			
Commande en boucle ouverte	X	X	X	X
Élaboration d'alarme	X	X	X	X
Contrôle des grappes	X	X	X	X
Gestion des priorités	*Non spécifique à un type de fonction d'application*			

FIG–7.4.3.1 INTERFACES DU SYSTÈME RCSL



FIG–7.4.3.2 ARCHITECTURE DU SYSTÈME RCSL

FIG–7.4.3.3 MODES DE FONCTIONNEMENT D'UNE UNITÉ



SOMMAIRE

TABLEAUX :

FIGURES :

.7.4.4 ARCHITECTURE DU CONTRÔLE-COMMANDE ACCIDENT GRAVE (CCAG)

0. PRESCRIPTION DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

On appelle accident grave toute séquence conduisant a minima à la fusion partielle du cœur et par conséquent susceptible d'engendrer des rejets important dans l'environnement.

Le Contrôle Commande Accident Grave (CCAG), mis en place dans le RPR, doit fournir les commandes et informations nécessaires à la conduite du scénario d'accident grave cumulé ou dû à une Perte Totale des Alimentations Electriques (PTAE) après épuisement des batteries [].

Le CCAG, associé aux autres systèmes dédiés accidents graves, constitue le chemin sûr dans l'objectif de conserver l'intégrité de l'enceinte et ainsi de limiter les rejets radioactifs dans l'environnement.

0.2. CRITÈRES FONCTIONNELS

Lors d'un scénario accident grave de type PTAE, le CCAG doit mettre en œuvre les commandes et informations nécessaires afin de réaliser les fonctions listées ci-après :

- ouverture [] des vannes de décharge accident grave,
- démarrage [] de la pompe d'injection de soude,
- lignage [] sur le préfiltre EDE,
- surveillance de la température de sortie cœur,
- surveillance de la localisation du corium,
- régulation des chaufferettes des trains à iode EDE,
- surveillance de l'hydrogène,
- surveillance de la pression enceinte,
- surveillance de la radioactivité dans l'enceinte,
- surveillance de la température en amont du réchauffeur file iode EBA,
- surveillance de la température en amont du réchauffeur file iode DWL,
- surveillance de la piscine de désactivation.

Le CCAG réalise également, au titre de la robustesse, des fonctions accidents graves, nécessaires en cas de perte du contrôle-commande standard cumulé ou non à une situation de perte totale des alimentations électriques :

- ouverture [] des volets ETY,
- mise en service [] des ventilateurs et des réchauffeurs EDE.

0.3. EXIGENCES RELATIVES À LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Le CCAG doit être classé conformément aux principes présentés à la section 3.2.1.

Le CCAG doit permettre la surveillance et la conduite de la tranche en situation d'accident grave et assure dans ce contexte des fonctions classées F2. Il porte par conséquent une exigence de classement F2.

Ces fonctions doivent rester opérationnelles après un séisme.

0.3.1.2. Critère de défaillance unique (active et passive)

Le critère de défaillance unique ne s'applique pas au CCAG.

0.3.1.3. Alimentation électriquede secours

Le CCAG doit être alimenté par une alimentation électrique de tension adéquate et non interruptible (batteries AG) afin de garantir la gestion de l'accident grave en cas de Perte Totale des Alimentations Electriques (PTAE).

0.3.1.4. Qualification aux conditions accidentelles

Les composants assurant des fonctions F2 doivent être qualifiés selon les règles présentées au sous-chapitre 3.7.

Le CCAG assurant des fonctions F2 doit être qualifié pour rester opérationnel dans les conditions de fonctionnement normales et post-accidentelles.

0.3.1.5. Classement des équipements mécaniques, électriques et de contrôle-commande

Le classement mécanique n'est pas applicable au CCAG.

Les équipements électriques et de contrôle commande doivent être classés conformément aux principes de classement présentés au sous-chapitre 3.2.

0.3.1.6. Classement sismique

Le CCAG doit être classé conformément aux principes de classement présentés au sous-chapitre 3.2.

Le CCAG est classé SC1 pour le classement sismique.

0.3.2. Exigences réglementaires

0.3.2.1. Textes officiels

Le document général « Options de Sûreté du projet de réacteur EPR » (lettre DGSNR/SD2/0729/ 2004) est applicable au contrôle commande accident grave.

0.3.2.2. Règles fondamentales de sûreté

L'application des RFS est présentée à la section 1.7.0.

0.3.2.3. Directives techniques

En plus des exigences générales indiquées au chapitre A.1 "approche générale de la sûreté", les exigences applicables au CCAG sont présentées aux sections A.2.2 (redondance et diversité dans les systèmes de sûreté), B.2.2.2 (systèmes de sûreté informatisés) et G3 (conception des dispositifs de contrôle-commande) des Directives Techniques.

0.3.2.4. Règles de conception électrique

Les règles de conception pour les équipements électriques ainsi que les règles spécifiques à appliquer à l'ensemble contrôle-commande sont fournies dans le RCC-E complété des données de projet du réacteur EPR définies dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.3.3. Agressions internes et externes

0.3.3.1. Agressions internes

Le CCAG doit être protégé vis-à-vis des conséquences des agressions internes si sa perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Le CCAG doit être protégé vis-à-vis des conséquences des agressions externes si sa perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

Le CCAG doit rester opérationnel après un séisme.

0.4. ESSAIS

0.4.1. Essais de démarrage

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du CCAG.

0.4.2. Surveillance en exploitation

Sans objet.

0.4.3. Essais périodiques

Le CCAG doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

On appelle Accident Grave toute séquence conduisant a minima à la fusion partielle du cœur et par conséquent susceptible d'engendrer des rejets importants dans l'environnement.

Le CCAG met en œuvre des fonctions actives et surveilles les fonctions passives visant à limiter les relâchements de radioactivité dans l'environnement dans le cadre du scénario d'accident grave de Perte Totale des Alimentations Electrique (perte du réseau électrique cumulée à la perte des diesels principaux et des diesels d'ultimes secours) après épuisement des batteries [].

Le CCAG est classé F2.

2. FONCTIONS SUPPORTÉES

Le CCAG assure les fonctions mentionnées au § 0.2..

3. BASE DE CONCEPTION

3.1. REDONDANCE

[]

3.2. INDÉPENDANCE

L'indépendance est assurée par une séparation physique et électrique du CCAG[].

3.3. PERFORMANCES REQUISES

3.3.1. Temps de réponse

Les temps de réponse du contrôle-commande sont les suivants :

- affichage sur le Pupitre Accident Grave (PAG)
  Depuis l'acquisition du signal capteur à l'entrée de la carte TXS CCAG jusqu'à l'affichage sur le Pupitre Accident Grave, le temps de réponse doit être inférieur à 1,5 s.
- commande opérateur
  Depuis l'activation de la commande sur le Pupitre Accident Grave jusqu'à la sortie de la carte TXS CCAG, le temps de réponse doit être inférieur à 1,2 s.
- régulation des réchauffeurs
  Depuis l'acquisition des valeurs de température iode jusqu'aux signaux de régulation en sortie de la carte TXS CCAG, le temps de réponse doit être inférieur à 1,0 s.
- ordre automatique d'ouverture des HMD (ETY) et de mise hors service de la pompe EVU
  Depuis l'acquisition des valeurs de pression enceinte par le système de pré-traitement et de conditionnement (PIPS) jusqu' à la sortie de la carte TXS CCAG, le temps de réponse doit être inférieur à 1,0 s.

3.4. EXIGENCES RELATIVES AUX CONDITIONS D'AMBIANCE

3.4.1. Conditions normales

Le matériel doit pouvoir fonctionner dans les conditions ambiantes données au sous–chapitre 9.4.

3.4.2. Conditions accidentelles

Le CCAG doit pouvoir rester opérationnel en cas de séisme.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Le CCAG est composé de deux armoires TXS. L'architecture matérielle et les interfaces avec le PS sont présentées dans la figure FIG–7.4.4.1.

Les interfaces réseaux sont les suivants :

- Les interfaces réseau entre SAU (Severe Accident Unit) permettent d'échanger des données capteurs entre divisions,
- Les interfaces réseau avec les MSI du PS permettent :
  - la communication avec les unités de service pour la maintenance et les tests périodiques,
  - la transmission des données SAU au MCP.

Les MSI, passerelles et unités de service sont utilisées pour les besoins du CCAG mais font partie du PS.

4.2. IMPLANTATION

Le CCAG est implanté à l'intérieur des [].

4.3. INTERFACES AVEC LE RESTE DU CONTRÔLE-COMMANDE

Le CCAG reçoit :

- du système de pré-traitement et de conditionnement (PIPS) :
  - des mesures de capteurs.
- du PAG :
  - des commandes,
  - des positions de commutateur.

Le CCAG fournit :

- au PAG :
  - des valeurs de mesures,
  - des comptes-rendus de commandes,
  - des alarmes,
  - des signaux élaborés par le CCAG.
- aux cellules d'actionneurs :
  - des signaux de commande.

5. MODES DE FONCTIONNEMENT

Le CCAG est composé de deux unités dont l'élément principal est une CPU. La description suivante concerne le mode de fonctionnement des unités.

La figure FIG–7.4.4.2 donne des détails sur les modes de fonctionnement et leurs interactions.

Les modes de fonctionnement d'une unité sont les suivants :

DÉMARRAGE : au démarrage du processeur, les multiples étapes d'une routine d'initialisation sont exécutées. Dans un premier temps, un contrôleur d'amorçage bas niveau commande l'initialisation du matériel et déclenche une série complète d'autotests de démarrage. Après un démarrage réussi du noyau du système d'exploitation, le module INIT de l'environnement d'exploitation (RTE) prend le contrôle de la CPU pour terminer la phase d'initialisation du RTE.

Si l'initialisation échoue, le fonctionnement cyclique ne démarre pas, le module INIT effectue une boucle sans fin sans activer les signaux de sortie et l'opérateur de maintenance est informé de cet état via l'unité de service.

Une fois l'initialisation terminée, le processeur de fonctions bascule en mode de fonctionnement cyclique. [].

Au redémarrage d'une unité SAU, ses sorties sont inhibées automatiquement [].

Cette réactivation des signaux de sortie se fait de deux manières différentes :

- à partir de la SU,
- à l'aide d'un bouton poussoir [].
  En complément du bouton poussoir, [].

Ce dispositif permet d'indiquer à l'opérateur exécutant l'opération de réactivation des sorties que sa commande a bien été prise en compte par le système.

FONCTIONNEMENT CYCLIQUE : le fonctionnement cyclique est le mode normal d'un processeur de fonctions. Il reste dans cet état tant qu'il n'est pas redémarré, [] à la suite d'une exception causée par une défaillance matérielle aléatoire ou une coupure de courant. Le passage aux autres modes de fonctionnement ne peut être déclenché que par l'unité de service.

En fonctionnement cyclique, n'importe quel signal sélectionné peut être affiché dans les diagrammes de programmation affichés sur l'unité de service.

La modification des paramètres est réalisable également dans ce mode, sous couvert de validation préalable par l'opérateur de maintenance (gérée par un jeu de clés physiques). Pendant le fonctionnement du système de contrôle-commande, seuls les paramètres désignés au préalable comme étant modifiables peuvent être changés par l'unité de service, par ex. pour optimiser une boucle de régulation ou adapter les paramètres en cas d'exploitation en prolongation de cycle.

TEST : ce mode est utilisé pour le dépannage. Une validation spécifique par l'opérateur de maintenance (gérée par un jeu de clés physiques) est une condition préalable pour passer en mode « TEST ». Lorsqu'une unité est en mode « TEST », le traitement cyclique des fonctions applicatives est interrompu.

Si une unité SAU est en mode TEST, l'unité SAU de l'autre division peut continuer à traiter les fonctions CCAG.

Les fonctions de traitement sont activées selon les conditions du test à l'aide de commandes supplémentaires envoyées par l'unité de service :

- activation / désactivation des traitements d'entrée / sortie,
- activation / désactivation des fonctions d'envoi et de réception de messages réseau,
- activation / désactivation du traitement de certains modules des diagrammes de fonctions,
- pré-positionnement des données dans les mémoires d'entrée et de sortie,
- suivi des signaux.

La sortie du mode de fonctionnement « TEST » s'effectue toujours par une réinitialisation du processeur et un redémarrage automatique. Après un temps de démarrage d'environ 10 secondes, le traitement se poursuit en mode de fonctionnement cyclique, sorties inhibées jusqu'à ce que l'opérateur de maintenance effectue l'acquittement.

DIAGNOSTIC : Une validation spécifique par l'opérateur de maintenance (gérée par une clé physique) est une condition préalable pour passer en mode « DIAGNOSTIC ». En mode « DIAGNOSTIC », toutes les fonctions du mode « TEST » sont accessibles. Les fonctions supplémentaires sont principalement relatives au chargement logiciel. Dans des cas très exceptionnels des routines de test spécifiques peuvent être chargées et exécutées.

Si une unité SAU est en mode DIAGNOSTIC, l'unité SAU de l'autre division peut continuer à traiter les fonctions CCAG.

La sortie du mode « DIAGNOSTIC » se fait toujours par réinitialisation du processeur, suivie d'un redémarrage automatique. De même que pour le mode « TEST », après un temps de démarrage d'environ 10 secondes, le traitement se poursuit en mode de fonctionnement cyclique, sorties inhibées, jusqu'à ce que l'opérateur de maintenance effectue l'acquittement.

Clés physiques de validation

[]

6. TECHNOLOGIE UTILISÉE

La technologie utilisée pour implémenter le CCAG est la plate-forme de contrôle-commande numérique TELEPERM XS de FRAMATOME.

7. ALIMENTATION ÉLECTRIQUE

7.1. EXIGENCES

Le Contrôle-Commande Accident Grave doit être alimenté par une alimentation ininterruptible de tension adéquate []. Cette source de tension doit être maintenue [] en cas de Perte Totale des Alimentations Électriques.

Chaque armoire doit être connectée à deux alimentations continues redondantes. Les arrivées de ces alimentations doivent être isolées les unes des autres, par exemple à l'aide de diodes.

En fonctionnement normal, les deux alimentations doivent être alimentées par l'alimentation ininterruptible (UPS) de la division correspondante.

7.2. ALIMENTATIONS ÉLECTRIQUES DES ARMOIRES TXS

Une description des alimentations électriques des armoires TXS est donnée dans la section 7.3.1 (relative au système de protection).

Les alimentations électriques redondantes [] sont fournies par 2 tableaux électriques :

[]

En cas de perte des alimentations externes, un diesel principal est disponible pour chaque division.

8. DISPOSITIONS MISES EN OEUVRE AU TITRE DE LA MAINTENANCE ET DES ESSAIS PÉRIODIQUES

L'unité de service est utilisée pour la maintenance et les essais périodiques.

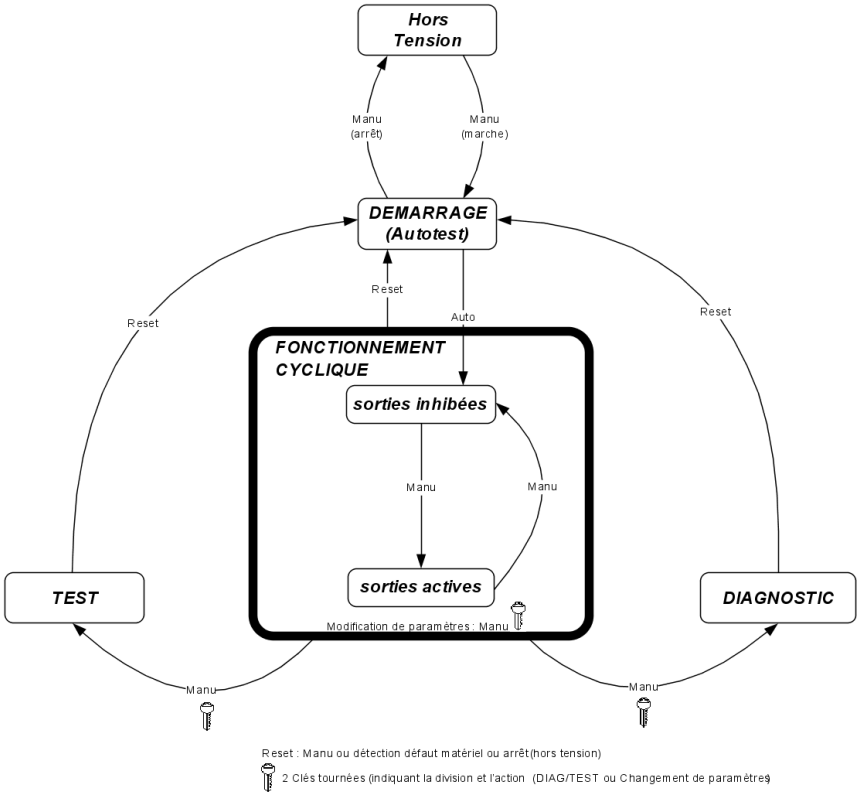
9. TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

TAB–7.4.4.1 DESCRIPTION DU CCAG

FIG–7.4.4.1 ARCHITECTURE ET INTERFACES DU CCAG

FIG–7.4.4.2 MODES DE FONCTIONNEMENT D'UNE UNITÉ



SOMMAIRE

.7.4.5 ARCHITECTURE DU SYSTÈME D'AUTOMATISME RRC-B (SAS RRC-B)

0. EXIGENCES DE SÛRETÉ

Le système de contrôle-commande SAS RRC-B assure le traitement des actions et la surveillance associée, nécessaires à la gestion des scénarios d'accident grave. La conduite d'un accident grave couplé avec une perte totale des alimentations électriques (PTAE) et après épuisement des batteries [] heures, impliquant la perte du SAS RRC-B, est quant à elle assurée par le système CCAG (voir section 7.4.4).

Le système SAS RRC-B est assujetti aux exigences de sûreté applicables aux systèmes de contrôle commande F2, du fait de sa gestion du contrôle-commande associé aux fonctions de sûreté F2.

0.1. FONCTIONS DE SÛRETÉ

Le système SAS RRC-B participe à la catégorie de fonction suivante : prévention des rejets radioactifs importants et précoces. Il contribue aux fonctions de sûreté suivantes :

- Dépressurisation du circuit primaire,
- Mitigation du risque hydrogène,
- Dépressurisation de l'enceinte et évacuation de la puissance résiduelle,
- Limitation des rejets dans l'environnement.

Ces fonctions à assurer en accident grave sont également complétées par un certain nombre de moyens passifs, ou de moyens locaux d'intervention, qui ne requièrent pas d'automatismes de contrôle-commande.

0.2. EXIGENCES RELATIVES À LA CONCEPTION

Au titre des fonctions F2E dont il assure les traitements des automatismes et des commandes manuelles et la surveillance liée (dont les fonctions de « gestion de priorité des commandes » et « surveillance de l'actionneur » définies en section 7.3.6), le système SAS RRC-B doit satisfaire aux exigences énoncées ci-après. Ces exigences doivent être respectées pour l'ensemble des fonctions d'automatisme gérées par le système SAS RRC-B.

0.2.1. EXIGENCES ISSUES DES CLASSEMENTS FONCTIONNEL ET MÉCANIQUE

0.2.1.1. CLASSEMENT FONCTIONNEL DU SYSTÈME

Les fonctions nécessaires pour prévenir les rejets importants et précoces dans les situations d'accident grave assurées par le SAS RRC-B, sont classées F2. Le système SAS RRC-B doit donc être classé de sûreté F2, conformément au classement indiqué au sous-chapitre 3.2.

0.2.1.2. CRITÈRE DE DÉFAILLANCE UNIQUE (ACTIVE ET PASSIVE)

Le critère de défaillance unique ne s'applique pas au système SAS RRC-B (ne gérant pas de fonctions F1).

0.2.1.3. ALIMENTATIONS ÉLECTRIQUES SECOURUES

L'alimentation électrique des équipements SAS RRC-B est secourue par les diesels principaux ainsi que par les diesels SBO d'ultime secours.

Par ailleurs, cette alimentation doit alors être du type « sans coupure », garantissant une alimentation même pendant le basculement alimentation normale / alimentation par diesel.

L'alimentation est diversifiée par deux sources d'alimentation alternative et continue pour chaque automate dans chacune des divisions où il se trouve implanté. Cette diversification est issue du REX de l'incident de [] et pallie le risque de mode commun sur les sources électriques.

Le système SAS RRC-B est par ailleurs alimenté par la même division que celle du procédé dont il assure le pilotage.

0.2.1.4. QUALIFICATION AUX CONDITIONS DE FONCTIONNEMENT

Les équipements SAS RRC-B doivent rester opérationnels en conditions post-accidentelles, et en situations d'accident grave. Ils doivent en conséquence respecter les exigences de qualification définies au sous-chapitre 3.7.

Par ailleurs, ces équipements doivent être opérationnels pour les conditions environnementales normales et accidentelles des locaux automates dans lesquels ils sont implantés. Ces conditions sont définies au sous-chapitre 9.4.

0.2.1.5. CLASSEMENT MÉCANIQUE, ÉLECTRIQUE, CONTRÔLE-COMMANDE

Les classements mécanique et électrique ne s'appliquent pas aux équipements de contrôle-commande.

Le classement de contrôle-commande pour les équipements SAS RRC-B, assurant le traitement des fonctions de sûreté F2, doit être, conformément aux principes définis au sous-chapitre 3.2, un Classement E2.

0.2.1.6. CLASSEMENT SISMIQUE

Les fonctions permettant l'évacuation de la chaleur de l'enceinte de confinement en situation d'accident grave, ainsi que les fonctions support, assurées par le SAS RRC-B, sont classées F2E, ce qui conduit à un classement SC1 pour l'ensemble des matériels SAS RRC-B.

0.2.1.7. RÈGLES ET CODES DE CONCEPTION

Le code de conception appliqué au système SAS RRC-B est le RCC-E, complété des données de projet du réacteur EPR défini dans l'additif CDP EPR (voir sous-chapitre 1.6).

0.2.2. AUTRES EXIGENCES

0.2.2.1. RÈGLES FONDAMENTALES DE SÛRETÉ

Le Système SAS RRC-B est non concerné.

0.2.2.2. DIRECTIVES TECHNIQUES

Les directives techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/04 "Options de sûreté du projet de réacteur EPR" (et plus spécifiquement G3.4 et G3.7) doivent être prises en compte à la conception du système SAS RRC-B.

Conformément aux Directives techniques le système SAS RRC-B, en tant qu'élément de la ligne de défense ultime « accident grave » - voir le sous-chapitre 7.1 la section concernant les principes de défense en profondeur - doit être indépendant des autres systèmes de CC qui participent aux lignes de défense précédentes.

0.2.2.3. TEXTES SPÉCIFIQUES EPR

Conformément aux demandes formulées par l'ASN dans les courriers émis suite à la réunion du 18 juin 2009 du Groupe Permanent Réacteurs tenu sur l'architecture du contrôle-commande EPR FA3,

des exigences de robustesse de l'architecture de contrôle commande accident grave sont introduites, selon les principes ci-dessous :

- La conduite des situations accident grave reste réalisable en cas de perte cumulée du MCP, à partir du Moyen de Conduite de Secours MCS et du Pupitre Accident Grave PAG,
- La gestion des situations accident grave est rendue robuste à la perte complète de la plate-forme de contrôle commande standard SPPA T2000 qui en assure tant que disponible la gestion. Cette robustesse est fondée sur des moyens de contrôle-commande disponibles sur la plateforme de technologie TXS (CCAG/PAG ou PS/MCS) ainsi que d'actions en local.

0.2.3. AGRESSIONS

0.2.3.1. Exigences — protection vis-à-vis des agressions internes

Les fonctions du système SAS RRC-B doivent être protégées vis à vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.2.3.2. Exigences — protection vis-à-vis des agressions externes

Les fonctions du système SAS RRC-B doivent être protégées vis à vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Les essais pré-opérationnels doivent prouver l'adéquation de la conception et des performances du système SAS RRC-B.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Le système SAS RRC-B doit être conçu pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

1. MISSIONS

La mission du SAS RRC-B est d'assurer la gestion des fonctions de contrôle commande F2 requises en cas de situation accident grave avec une conduite opérateur depuis le MCP, à l'exception du scénario accident grave PTAE dont la gestion est assurée par le système CCAG (voir section 7.4.4) après basculement sur le pupitre accident grave PAG (voir section 7.4.6).

2. FONCTIONS ASSURÉES

- Les principes généraux d'allocation des fonctions (actionneurs) / informations (capteurs) permettant la gestion de l'ensemble des séquences accident grave depuis le MCP, hormis le scénario PTAE géré par le CCAG (voir section 7.4.4), sont les suivants :

  []

  Les types de traitements de contrôle commande du SAS RRC-B permettant d'assurer les fonctions implantées au SAS RRC-B sont les suivantes :

- Traitements des données : acquisition, conditionnement et mise à disposition (exemple : acquisition et élaboration de la température sortie cœur) ;
- Traitements de calculs applicatifs : [] ;
- Traitements de surveillance : traitement des comptes-rendus d'état et de défauts, élaboration des alarmes et signalisations.

3. BASE DE CONCEPTION

3.1. EXIGENCE DE DISPONIBILITÉ

Les principales exigences conditionnant la disponibilité du SAS RRC-B sont liées à la fiabilité et à la maintenabilité du système, qui se traduisent par :

- Limiter les pertes du SAS RRC-B dues à la perte de l'un de ses composants (par la redondance de ses composants notamment),
- Faciliter la maintenance et la réparation du SAS RRC-B pour réduire au minimum sa période d'indisponibilité.

3.2. PERFORMANCES REQUISES

Le SAS RRC-B est soumis aux exigences de performance et de précision qui dépendent des fonctions qu'il réalise.

La conception du SAS RRC-B, et son intégration dans l'architecture du contrôle-commande, permet de respecter ces exigences ainsi que les exigences générales de performances formulées au sous-chapitre 7.2.

3.3. EXIGENCES RELATIVES À L'ENVIRONNEMENT

Les conditions environnementales que les équipements SAS RRC-B devront supporter sont liées à la température et à l'humidité relative des locaux abritant ces matériels. Ces caractéristiques environnementales sont définies au sous–chapitre 9.4, autant pour les conditions normales que pour les conditions extrêmes.

3.4. EXIGENCES RELATIVES À L'INTERFACE HOMME MACHINE

SAS RRC-B non concerné.

4. ARCHITECTURE

Le SAS RRC-B est un des systèmes de niveau 1 constitutif de la plate-forme de Contrôle commande standard de technologie SPPA T–2000.

4.1. STRUCTURE ET COMPOSITION

La structure et la composition du SAS RRC-B sont dictées par des exigences fonctionnelles.

Ces exigences fonctionnelles portent sur :

- Le classement fonctionnel des traitements (qui dans le cas du SAS RRC-B est F2E),
- La division électrique (en correspondance avec celle du procédé, actionneurs et capteurs, à gérer) : le SAS RRC-B est affecté dans les divisions 1 et 4 de l'îlot nucléaire,
- La typologie des traitements à effectuer (pouvant conditionner le choix du type de cartes d'entrées/sorties par exemple),

- La performance requise des traitements (temps de réaction, temps de propagation, précision),
- Les regroupements / exclusions de traitement : les traitements sont alloués dans une même unité d'automatisme,
- La défense en profondeur : il s'agit ici de garantir par conception que les traitements du SAS RRC-B soient réalisables de façon autonome, et restent insensibles à des défaillances d'automates appartenant aux autres lignes de défense. Cet objectif est atteint par une acquisition directe des informations nécessaires ou qui conditionnent certains traitements, sans passer par des échanges inter-automates, par une double acquisition des informations nécessaires mais non dédiées, par le paramétrage des valeurs de replis en fonction de la position sûre visée, etc.

4.2. INSTALLATION

Les équipements gérant les fonctions SAS RRC-B sont installés dans les armoires de contrôle commande des divisions[].

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CC

Le SAS RRC-B échange des informations avec :

- L'instrumentation procédé : échange liés à l'acquisition des mesures et états,
- L'IHM MCP et le MCS : échanges liés à la conduite opérateur. La conduite des situations d'accident grave en cas de perte du MCP. Dans cette situation les commandes et signalisations disponibles au PAG ou PIPO sont valorisées,
- Les systèmes PAS/SAS : échanges liés à la gestion des automatismes de la tranche, ne compromettant pas l'autonomie des fonctions assurées par les automates SAS RRC-B,
- Les cellules électriques (tableaux électriques) et les organes de commande réglants (électro-positionneurs, etc.) : échanges liés à la commande des actionneurs.

En termes d'interfaces réseau, le SAS RRC-B, contrairement au système SAS de tranche classé E1B, ne dispose pas d'interface réseau SAS Bus mais d'une seule interface réseau Plant Bus E2.

5. CONFIGURATIONS OPÉRATIONNELLES

La configuration (d'un point de vue matériel et fonctionnel) du SAS RRC-B est indépendante de la situation. L'allocation du traitement dépend seulement des critères fonctionnels et des principes d'allocation des traitements du système de contrôle commande. La configuration du SAS RRC-B est, de ce point de vue, constante.

La configuration du SAS RRC-B n'est dépendante que du dispositif suivant : en cas de défaut de fonctionnement d'une carte active, le système commute automatiquement sur la seconde carte, qui était en attente. Ce principe s'applique à toute carte redondée du SAS RRC-B (cartes CPU et cartes de gestion de la communication).

6. TECHNOLOGIE

Le SAS RRC-B est un des systèmes de niveau 1 constitutif de la plate-forme de contrôle–commande standard de technologie SPPA–T2000, développé par [].

La description relative à la technologie du système SAS (section 7.3.2), et celle relative à la technologie du PAS (section 7.4.2), sont applicable au système SAS RRC-B aux différences près suivantes concernant les interfaces réseau :

- Le SAS RRC-B ne dispose pas d'interface réseau SAS Bus, à la différence du SAS ;
- Le SAS RRC-B est interfacé directement au Plant Bus, à la différence du PAS, dont les unités d'automatismes sont regroupées en îlots dans chaque division/section).

7. ALIMENTATION ÉLECTRIQUE

[]

Chaque train mécanique est contrôlé par un sous-ensemble du SAS RRC-B, situé dans et alimenté par la même division que le train mécanique.

Le réglage à la tension exigée par les armoires SAS RRC-B est effectué en interne aux armoires assurant leur alimentation. [].

8. DISPOSITIONS PRISES POUR RÉALISER LES TESTS PÉRIODIQUES

Le SAS RRC-B fait l'objet d'un programme d'essais périodiques conformément aux exigences de la section «généralités» du chapitre IX des RGE permettant notamment de vérifier la disponibilité des fonctions de sûreté définies au **§ 0.1.**.

9. ANALYSE DE SÛRETÉ

Le système SAS RRC-B, compte tenu des éléments présentés dans la présente section, ainsi que dans le sous-chapitre 7.1, est conforme aux exigences de sûreté dont il est redevable (ces dernières étant formulées au **§ 0.** ainsi que dans le sous-chapitre 7.1).

10. SYSTÈME TEL QUE REALISE

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

SOMMAIRE

.7.4.6 ARCHITECTURE DU PUPITRE ACCIDENT GRAVE (PAG)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

Le Pupitre Accident Grave (PAG) contribue aux fonctions de sûreté supportées par le contrôle-commande (voir paragraphe 0 du sous-chapitre 7.1). Il constitue l'interface homme-machine, classée de sûreté, du CCAG fournissant à l'équipe de conduite les informations et commandes nécessaires à la gestion des situations d'accident grave correspondant aux scénarios de Perte Totale des Alimentations Electriques (PTAE) (perte des sources externes, diesels principaux et diesels d'ultime secours).

Plus précisément, il doit permettre :

- D'autoriser et de transmettre des actions de conduite manuelles F2 nécessaires pour la limitation des conséquences des situations Accident Grave de PTAE,
- De surveiller des fonctions F2 nécessaires pour la limitation des conséquences des situations Accident Grave de PTAE.

0.2. EXIGENCES RELATIVES À LA CONCEPTION

0.2.1. Exigences issues des classements fonctionnel et mécanique

0.2.1.1. Classement fonctionnel du système

Le PAG supporte des fonctions de conduite et contrôle de la tranche de classements au maximum F2. Il est donc, selon les sous-chapitres 3.2 et 7.1, classé de sûreté F2 et doit satisfaire aux exigences de sûreté des paragraphes ci-après.

0.2.1.2. Critère de défaillance unique (active et passive)

Le critère de défaillance unique n'est pas applicable pour les fonctions F2.

0.2.1.3. Alimentations électriques secourues

Les alimentations du PAG et du mécanisme de mise en service de ses commandes sont secourues pendant []h[].

Les équipements du PAG sont alimentés par la même division électrique que la division de contrôle-commande dont ils dépendent, chaque division étant indépendante électriquement et physiquement des autres de façon à garantir une absence de mode commun entre divisions.

0.2.1.4. Qualification aux conditions de fonctionnement

Les matériels supportant les fonctions du PAG sont qualifiés en fonction de leur classement de sûreté, selon le sous-chapitre 3.7, et en fonction des conditions d'ambiance normales et accidentelles auxquelles ils sont soumis lors de l'accomplissement de leur mission (cf. paragraphe 1.3.4).

0.2.1.5. Classements mécanique, électrique, contrôle-commande

Le PAG n'est pas concerné par le classement mécanique (M).

Le PAG n'est pas concerné par le classement électrique (EE).

Conformément au sous-chapitre 7.1 concernant le classement contrôle-commande, le matériel constitutif du PAG assurant des fonctions F2 doit au moins être classé E2

0.2.1.6. Classement sismique

Le PAG appartient à la classe sismique 1 (SC1) opérable et remplit les exigences correspondantes selon le sous-chapitre 3.2.

0.2.1.7. Exigences supplémentaires

Sans objet.

0.2.2. Autres exigences réglementaires

0.2.2.1. Règles Fondamentales de Sûreté

Le PAG n'est pas concerné par les Règles Fondamentales de Sûreté (RFS).

0.2.2.2. Directives Techniques

Les directives techniques énoncées dans le document DGSNR/SD2/0729/2004 du 28/09/2004 “options de sûreté du projet réacteur EPR” sont prises en compte à la conception du PAG (en particulier le chapitre G3.4).

0.2.2.3. Textes spécifiques EPR

Le PAG satisfait aux exigences énoncées dans le RCC-E édition décembre 2005 complétées des données de projet EPR définies dans l'additif “Cahier de données de projet EPR” (voir sous-chapitre 1.6)

0.2.3. Agressions

Le PAG est protégé contre les défaillances de mode commun pouvant résulter des agressions internes ou externes en suivant les exigences définies aux sous-chapitres 3.3 (agressions externes) et 3.4 (agressions internes).

0.3. ESSAIS

0.3.1. Essais pré-opérationnels

Le PAG fait l'objet d'essais pré-opérationnels, permettant de vérifier après montage la conformité des performances du système avec les exigences de conception.

0.3.2. Surveillance en exploitation

Sans objet.

0.3.3. Essais périodiques

Les parties du PAG assurant des fonctions F2 qui ne sont pas sollicitées en continu sont aptes à la réalisation d'essais périodiques et sont conçues de manière à permettre la réalisation de ceux-ci conformément aux règles définies dans le chapitre IX des RGE.

1. MISSIONS

Le PAG est le système de contrôle-commande en charge de fournir les moyens de surveillance et de commande du CCAG des divisions 1 et 4 nécessaire pour pallier la Perte Totale des Alimentations Electriques (PTAE) (perte des sources externes, diesels principaux et diesels d’ultime secours).

Il est activé avant les [] heures d'autonomie dont dispose le contrôle-commande standard de niveau 1 (SAS RRC-B) et le MCP et pendant les [] heures suivant l'entrée en accident grave (délai au bout duquel le retour d'une source d'alimentation électrique est postulé).

2. FONCTIONS SUPPORTÉES

Le PAG supporte les fonctions de commande et de surveillance suivantes :

[]

Pour toutes les commandes du PAG, l'activation du PAG réalisée à l'aide des commutateurs prévus à cet effet permet d'autoriser au contrôle-commande accident grave (CCAG) la prise en compte de ces commandes.

De plus, pour des raisons de fiabilisation des commandes à destination des vannes de décharge face à un risque d'intempestifs du CCAG, la transmission de celles-ci aux vannes de décharge est conditionnée une seconde fois en sortie du CCAG à l'activation des vannes 900t RCP du PIPO réalisée à l'aide des commutateurs prévus à cet effet.

3. PRINCIPES DE CONCEPTION

3.1. DISPOSITIONS PARTICULIÈRES

Les dispositions de conception particulières qui doivent être prises en compte pour le PAG sont les suivantes :

- Le PAG est indépendant du MCP de sorte qu'aucun dysfonctionnement du MCP ne puisse avoir de conséquence sur le PAG,
- Un mécanisme d'inhibition permet de forcer le PAG dans l'ETAT 1 (cf. § 5. de cette section) à partir de la station de repli suite à la perte d'habitabilité de la salle de commande principale,
- Le PAG respecte les exigences d'interface homme-machine décrites au chapitre 17 et au § 3.5..

3.2. EXIGENCE DE DISPONIBILITÉ

Le PAG est conçu comme un système de contrôle-commande indépendant du MCP, afin de pouvoir être disponible en cas de perte du MCP.

Les moyens de surveillance et conduite supportés par le PAG ne sont pas les moyens privilégiés par l'équipe de conduite pour conduire la tranche.

3.3. PERFORMANCES REQUISES

Le PAG, en tant qu'équipement de niveau 2, est soumis à des exigences de performances en temps de réponse principalement liées aux facteurs humains. Ainsi, les informations issues du niveau 1 et la prise en compte des actions opérateurs au niveau 1 sont affichées au PAG dans un délai de l'ordre de la seconde.

3.4. EXIGENCES D'ENVIRONNEMENT

Le PAG est installé dans la salle de commande principale, les conditions d'environnement auxquelles il est soumis sont donc celles de ce local.

On distingue deux catégories :

- Les conditions d'environnement auxquelles les équipements sont soumis. Ceci inclut la température et l'humidité relative de la pièce.

- La contribution de l'équipement aux conditions ambiantes. Cette catégorie inclut le niveau de bruit et la chaleur dégagée.

3.5. EXIGENCES LIÉES À L'INTERFACE HOMME-MACHINE

Outre les performances indiquées au § 3.3. de cette section, l'aménagement du PAG prend en compte les critères ergonomiques (compatibilité avec les tâches de l'opérateur) ainsi que les contraintes d'indépendance (principalement séparation physique) des équipements appartenant à et alimentés par des divisions différentes ou soumis à des niveaux de classement différents.

La liste détaillée des différentes informations et commandes qui sont implantées au PAG est déterminée en analysant les tâches qui doivent être accomplies sur ce moyen de conduite. Des éléments liés aux moyens situés au PAG peuvent être trouvés dans les chapitres 13 et 17.

4. ARCHITECTURE

4.1. STRUCTURE ET COMPOSITION

Le PAG est découpé de la même manière que le MCS (voir section 7.3.3).

4.2. INSTALLATION

Le PAG est installé dans la salle de commande principale.

4.3. INTERFACES AVEC LES AUTRES SYSTÈMES DE CONTRÔLE-COMMANDE

Le PAG présente trois types d'interfaces :

- l'interface avec l'opérateur dans la salle de commande principale,
- l'interface avec le niveau d'automatisme (CCAG, coffrets KSC PAG),
- l'interface avec les cellules des vannes de décharge.

5. MODES DE FONCTIONNEMENT

L'équipe de conduite opère depuis le PAG en cas de Perte Totale des Alimentations Electriques (PTAE) (perte des sources externes, diesels principaux et diesels d'ultime secours).

Il est activé avant les [] heures d'autonomie dont dispose le contrôle-commande standard de niveau 1 (SAS RRC-B) et le MCP et pendant les [] heures suivant l'entrée en accident grave (délai au bout duquel le retour d'une source d'alimentation électrique est postulé).

L'activation du PAG :

Pour chaque division (1 et 4), l'activation des commandes du PAG est réalisée [] depuis le PAG en positionnant le commutateur correspondant en position d'activation. Cette information d'activation du PAG est acquise par les coffrets KSC PAG qui les retransmettent ensuite au CCAG.

Cette action est réalisable :

- Quel que soit l'état de la tranche,
- Si la conduite se fait en salle de commande principale (SdC), c'est-à-dire que les commutateurs SdC/SdR doivent être en position SdC (cf. ci-dessous).

Pour chaque division (1 et 4), la logique d'activation du PAG permet d'obtenir dans cet ordre les deux états suivants des commandes et information :

- ETAT 1 - PAG passif :
  - La signalisation au PAG est opérationnelle et cohérente avec le MCP ;
  - Les mesures sur indicateurs et enregistreurs sont opérationnelles au PAG et cohérentes avec le MCP ;
  - Les alarmes sont visibles et auto-acquittées (acquittement sonore et visuel immédiat) au PAG ;
  - Les commandes au PAG sont inhibées (exceptées les commandes d'activation et de test) ;
- ETAT 2 - PAG actif :
  - La signalisation au PAG est opérationnelle et cohérente avec le MCP (lorsque celui-ci est toujours opérationnel) ;
  - Les mesures sur indicateurs et enregistreurs sont opérationnelles au PAG et cohérentes avec le MCP (lorsque celui-ci est toujours opérationnel) ;
  - Les alarmes sont visibles et acquittables au PAG ;
  - Les commandes au PAG sont opérationnelles.

La logique de désactivation du PAG doit permettre d'obtenir dans l'ordre inverse chacun de ces deux états.

L'activation du PAG n'agit ni sur la commutation MCP < - > MCS, ni sur le PIPO, ni sur le PSIS.

Le positionnement en Station de Repli (SdR) de [] commutateurs SdC/SdR (dédiés au PAG) en position SdR [].

6. TECHNOLOGIE

La technologie utilisée est la même que celle utilisée pour le MCS (voir section 7.3.3).

7. ALIMENTATION ÉLECTRIQUE

Les commandes et signalisations propres à une division électrique de l'îlot nucléaire sont alimentées par les équipements de cette division.

Des dispositions d'isolement sont prises pour maintenir la séparation électrique des équipements du PAG appartenant à des divisions différentes ou de niveaux de classement différents.

8. DISPOSITIONS PRISES POUR LA RÉALISATION D'ESSAIS PÉRIODIQUES

Le PAG doit faire l'objet d'essais périodiques, selon le **§ 0.3.3.** de cette section.

Les essais périodiques sont réalisés dans l'ETAT 1 en basculant le commutateur de « Test Lampes ».

Le test de chacune des fonctions de sûreté devant faire l'objet d'essais périodiques permettra de vérifier la chaîne complète de commande, du capteur (commande automatique), ou du PAG (commande manuelle), via les équipements de traitement du contrôle-commande, jusqu'au changement d'état de l'actionneur.

Toutefois si la mise en configuration de l'actionneur concerné ne peut pas être effectuée (par exemple lors du fonctionnement de la tranche) des dispositions sont prises pour bloquer les signaux de commande pendant le test, de façon à tester la ligne de commande de l'actionneur, sans commander physiquement ce dernier.

9. ANALYSE DE SÛRETÉ

Le PAG est conforme aux exigences de sûreté dont il est redevable.

10. SYSTÈME TEL QUE RÉALISÉ

A ce stade de la fabrication, de l' installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

7.5 INSTRUMENTATION

SOMMAIRE

.7.5.0 EXIGENCES DE SÛRETÉ

1. FONCTIONS DE SÛRETÉ

L'instrumentation participe directement aux trois fonctions fondamentales de sûreté :

- Maîtrise de la réactivité,
- Evacuation de la puissance résiduelle,
- Confinement des substances radioactives,

et doit permettre la mesure :

- des paramètres nécessaires aux automatismes,
- des paramètres nécessaires à l'élaboration des informations à disposition des opérateurs pour connaître l'état de la tranche.

2. CRITÈRES FONCTIONNELS

Maîtrise de la réactivité : l'instrumentation doit couvrir l'ensemble des paramètres représentatifs de l'état neutronique du cœur, à savoir :

- le flux neutronique pour les états en puissance, intermédiaires et les états d'arrêt,
- la position des grappes de contrôle et d'arrêt,
- la concentration en bore du circuit primaire.

Evacuation de la puissance résiduelle : l'instrumentation doit couvrir l'ensemble des paramètres représentatifs de la fonction évacuation de la puissance résiduelle. Elle doit permettre de déterminer :

- l'état thermo-hydraulique du cœur (pression primaire, température primaire, débit primaire…),
- l'état du secondaire (pression GV, température secondaire, débit d'eau alimentaire…).

Confinement : l'instrumentation doit couvrir l'ensemble des paramètres permettant de connaître l'état de l'installation vis-à-vis du confinement :

- la pression et la température de l'enceinte,
- la position des vannes d'isolement enceinte,
- le niveau d'activité dans les bâtiments.

Surveillance de l'état de la tranche : l'instrumentation doit permettre de connaître l'état des systèmes opérationnels et de sauvegarde pour s'assurer de leur disponibilité. Les informations correspondantes peuvent être des mesures de pression, débit, niveaux, des positions d'actionneurs.

3. EXIGENCES RELATIVES À LA CONCEPTION

3.1. EXIGENCES ISSUES DES CLASSEMENTS FONCTIONNEL ET MÉCANIQUE

L'instrumentation doit obéir aux mêmes exigences de classement, de respect du critère de défaillance unique et d'essais périodiques que les fonctions classées auxquelles elle participe.

Les exigences liées au classement sont détaillées au sous-chapitre 3.2.

Les exigences liées à la qualification des matériels sont détaillées au sous-chapitre 3.7.

3.2. EXIGENCES RÉGLEMENTAIRES LIÉES À LA SÛRETÉ

Les exigences réglementaires et para-réglementaires spécifiquement applicables à certaines instrumentations sont détaillées dans les sections dédiées à chaque instrumentation (7.5.1 à 7.5.9).

3.2.1. Textes réglementaires

3.2.1.1. Textes officiels

L'instrumentation est concernée spécifiquement par l'article III-1.1.1 du Décret d'Autorisation de Création n°2007-534 du 10 avril 2007 :

« III-1.1.1. La surveillance de la réaction nucléaire
Tant qu'un assemblage de combustible est présent dans la cuve, la concentration de l'eau du circuit primaire en absorbant neutronique soluble est surveillée en permanence.
Dès lors que le combustible nécessaire au fonctionnement normal du réacteur est chargé dans la cuve, la réaction nucléaire est surveillée en permanence. Les moyens de mesure en place permettent d'effectuer cette surveillance au-delà de la puissance thermique de dimensionnement du réacteur.
Ces moyens de mesure et l'intensité des sources de comptage associées sont choisis et maintenus à un niveau de performances tel que l'exploitant n'ait jamais à faire démarrer la circulation de l'eau du circuit primaire principal ni à entreprendre la diminution de la concentration de cette eau en absorbant neutronique soluble sans disposer d'une mesure significative du flux neutronique.
Le suivi de la distribution de puissance dans le cœur est assuré par différents systèmes de mesure neutronique répartis dans et en dehors du cœur ».

3.2.1.2. Prescriptions techniques

Décision n° 2008-DC-0114 de l'Autorité de Sûreté Nucléaire du 26 septembre 2008.

Prescription INB167-22 : *« L'installation dispose de l'instrumentation nécessaire pour vérifier, au cours des essais de démarrage, le comportement attendu de l'installation vis-à-vis de la sûreté. Le contenu de cette instrumentation est justifié dans le cadre d'un dossier de suffisance, en intégrant les besoins requis en tant que tête de série. »*

3.2.2. Textes para-réglementaires

3.2.2.1. Directives techniques

Section G3 – Conception du contrôle-commande

Cette section précise les exigences relatives à l'instrumentation et au contrôle-commande.

Les exigences applicables à l'instrumentation concernent :

- le classement fonctionnel de l'instrumentation,
- la prise en compte du critère de défaillance unique, de la maintenance et de la séparation physique,
- la prise en compte des conséquences des agressions internes et externes sur le contrôle-commande.

3.3. AGRESSIONS

Les matériels d'instrumentation doivent répondre aux mêmes exigences de protection contre les agressions internes et externes que les fonctions et systèmes auxquels ils appartiennent.

4. ESSAIS

L'instrumentation doit être soumise à étalonnage et à un contrôle des connexions lors du montage.

L'instrumentation doit également être testée lors des essais des systèmes et fonctions auxquels elle appartient, et doit faire l'objet d'un recalage éventuel si nécessaire.

SOMMAIRE

.7.5.1 INSTRUMENTATION CLASSIQUE DE PROCÉDÉ

1. EXIGENCES FONCTIONNELLES

L'instrumentation classique de procédé doit fournir les informations nécessaires à la connaissance de l'état de la tranche et des procédés dans le but d'assurer :

- le fonctionnement normal de la tranche,
- la protection du personnel et de la population,
- le contrôle de la tranche en fonctionnement normal, incidentel et accidentel en conjonction avec de l'instrumentation nucléaire spécifique et de l'instrumentation radiologique appropriées.

Il est pris comme hypothèse que l'instrumentation classique de procédé participe à des fonctions de tout niveau de classement de sûreté.

D'une manière générale, l'instrumentation classique de procédé comprend :

- les mesures de pressions,
- les mesures de niveau,
- les mesures de débits,
- les mesures de températures,
- les mesures de vitesse de rotation,
- les mesures de tensions,
- les mesures de fréquences,
- les mesures de positions.

Les exigences fonctionnelles particulières à l'instrumentation concernent :

- le choix de l'instrumentation : l'instrumentation doit être choisie de manière à ce que la gamme de mesure, la précision et les autres paramètres représentatifs soient en cohérence avec la plage et l'amplitude de variation attendue des paramètres de procédés mesurés et son utilisation prévue.
- l'utilisation d'équipements communs : l'installation d'une instrumentation redondante, appartenant à des divisions différentes doit éviter l'utilisation d'équipements communs (par exemple : piquages communs, vannes d'isolement communes, supports communs…).
- l'étalonnage : l'instrumentation doit être conçue de manière à limiter les besoins en étalonnage, et doit être installée de manière à faciliter les interventions. Des essais et des vérifications doivent garantir le bon étalonnage de l'instrumentation. Des dispositions doivent être prises pour éviter les erreurs pendant la maintenance et l'étalonnage.

2. DESCRIPTION DE L'INSTRUMENTATION CLASSÉE DE SÛRETÉ

2.1. MESURE DE PRESSION

Les mesures de pression sont raccordées sur tous les systèmes fluides. Les principes de mesure décrits ci-après s'appliquent principalement aux mesures de pression sur les tuyauteries des systèmes et matériels ou équipements du circuit primaire, sur les générateurs de vapeur et sur le pressuriseur.

Les transmetteurs de pression simple ou différentielle sont reliés aux prises de pression, implantées sur les tuyauteries des systèmes ou sur les appareils (bâches, réservoirs, générateurs de vapeurs, etc.) par des lignes d'impulsion. Une vanne d'instrumentation, implantée au plus près du capteur, a la fonction de vanne d'isolement secondaire. Un dispositif, installé sur la ligne d'instrumentation entre la

vanne d'isolement secondaire et le capteur, permet le rinçage de cette ligne, de ce point vers le système fluide.

Ce dispositif permet également la réalisation d'essais et le calibrage du transmetteur.

La vanne d'isolement primaire est généralement implantée de manière à pouvoir être manœuvrée [].

Les lignes d'instrumentation, pour systèmes en phase fluide, sont posées avec une pente entre la prise d'impulsion et le transmetteur pour permettre le dégazage de la ligne d'instrumentation vers le circuit principal et exclure tout matelas gazeux en amont du transmetteur.

Les transmetteurs requis en situations accidentelles sont conçus pour fonctionner dans ces situations.

Des détecteurs appropriés à la mesure et fonctionnant sur différents principes peuvent être utilisés :

- mesure de pression absolue : i.e. cellules à membrane ou cellules céramiques,
- mesure de pression relative : i.e. cellules capacitives ou mécanismes à tube de Bourdon,
- mesure de pression différentielle : i. e. cellules à membrane. Elles sont constituées de deux membranes sensibles dont le déplacement est converti en un signal électrique.

Un transducteur électrique convertit le signal de sortie du détecteur en un signal électrique proportionnel à la pression.

2.2. MESURE DE DÉBIT

Les principes de mesure utilisés incluent les méthodes suivantes :

- mesure de la pression différentielle aux bornes d'un organe déprimogène (plaques à orifice standards, venturi),
- mesure de la pression différentielle entre des prises d'impulsion implantées en intrados et extrados d'un coude,
- rotamètres,
- compteurs de débit à ultrason,
- compteurs inductifs.

Le signal de sortie des transmetteurs de pression différentielle donne un signal électrique proportionnel à la pression. L'intégration de la racine carrée donnant un signal proportionnel au débit est réalisée au contrôle-commande.

2.3. MESURE DE NIVEAU LIQUIDE

Les techniques employées, pour la mesure des niveaux liquides dans le pressuriseur et dans les générateurs de vapeur, consistent principalement en des mesures de pression différentielle (méthode hydrostatique à colonne de référence humide).

Deux lignes de prise de pression sont raccordées à un transmetteur de pression différentielle. L'une des deux lignes de prise de pression est reliée à la partie basse, en phase eau, du pressuriseur ou du générateur de vapeur et l'autre à la partie supérieure, en phase vapeur. Les mesures de conception appropriées doivent être prises pour exclure tout risque de formation d'un matelas gazeux dans les lignes d'instrumentation et éviter les erreurs de mesure liées à ce phénomène. La ligne de prise de pression, sur la phase vapeur du pressuriseur ou du générateur de vapeur, est conçue sur le principe d'une colonne de référence humide. Elle est équipée d'un pot de condensation. La fonction de ce pot est de condenser la vapeur afin de maintenir un niveau de liquide constant dans la colonne de référence humide dans toutes les conditions d'exploitation. Le pot de condensation doit être installé en point haut de la ligne d'instrumentation, implanté au-dessus de la prise d'impulsion et au plus près de cette dernière. La tuyauterie de liaison, entre le pot et la prise d'impulsion, doit avoir une pente

descendante vers l'appareil et ne pas présenter de point bas afin d'éviter la création d'un bouchon d'eau.

Outre la méthode hydrostatique par pression différentielle, le niveau liquide est aussi mesuré par méthode capacitive. Pour cette méthode de mesure, une sonde en saillie dans le réservoir ou la bâche joue le rôle de capacitance avec l'enceinte de réservoir (ou tube de masse). Les propriétés diélectriques du fluide entre les deux électrodes changent avec le niveau de liquide, ainsi que la résultante du courant haute - fréquence circulant par la capacitance. Ce courant haute - fréquence est converti par le transmetteur en un signal en courant continu proportionnel au niveau liquide.

Les types de mesure de niveau suivants sont également employés :

- mesure de niveau avec colonne de référence sèche,
- mesure de niveau par sonde hydrostatique,
- mesure de niveau pour bâche à l'atmosphère,
- mesure de niveau par bullage,
- mesure de niveau par déplacement (avec plongeur).

2.4. MESURE DE TEMPÉRATURE

Les mesures de température sont réalisées soit par sonde à thermocouple soit par sonde à résistance.

Les thermocouples et thermomètres à résistance, pour les systèmes fluides sous pression, doivent être montés en doigts de gant afin de permettre la dépose des éléments sensibles pour maintenance, sans devoir dépressuriser le système.

Les thermocouples sont employés pour des applications où une acquisition très rapide des données mesurées est requise. Leur faible masse permet un temps de réponse, aux variations de température, beaucoup plus rapide que les thermomètres de résistance.

Les thermomètres à résistance sont constitués d'un isolant minéral et d'un enroulement en platine et doivent être conçus pour résister aux vibrations. Pour obtenir la meilleure précision possible, un montage en circuit quatre fils est utilisé pour les thermomètres à résistance.

2.5. MESURE DE LA VITESSE DE ROTATION

La vitesse est mesurée sur les pompes primaires par le contrôle commande classé de sûreté. Un pôle ferromagnétique est monté sur l'axe de la roue du moteur des pompes de refroidissement du réacteur. Quand l'axe du moteur tourne, un signal pulsé d'une fréquence proportionnelle à la vitesse de l'axe est généré.

2.6. MESURE DE TENSION

Les capteurs pour la mesure de tension en courant alternatif (AC) opèrent sur le principe du redresseur. Les signaux d'entrée et de sortie du capteur sont électriquement isolés l'un par rapport à l'autre. Un étage amplificateur convertit le signal de tension résultant en un signal de courant continu (DC).

D'autres méthodes, pour la mesure de la tension, consistent à transformer le signal en un signal basse tension en utilisant un transformateur. Le signal résultant est alors acquis par un ordinateur, l'amplitude et la valeur efficace (r. m. s.) de la tension AC sont déterminées par des moyens numériques.

2.7. MESURE DE FRÉQUENCE

La variable d'entrée est appliquée à un étage à déclenchement dans le capteur. Le capteur délivre un signal de sortie tension/temps qui est traité par un amplificateur et converti en un signal courant DC proportionnel à la fréquence.

2.8. MESURE DE POSITION SUR LA VANNE DE SÉCURITÉ DU CIRCUIT DE VAPEUR PRINCIPALE

La mesure de position est exécutée par la méthode inductive. Des bobines de détection sont installées dans un ensemble de détecteur conçu spécialement pour équiper cette vanne. Les bobines de détection sont conçues pour les températures d'utilisation de cette vanne.

7.5.2 INSTRUMENTATION INTERNE DU CŒUR

SOMMAIRE

FIGURES :

.7.5.2.1 INSTRUMENTATION INTERNE FIXE DU CŒUR — INSTRUMENTATION POUR L'ÉTABLISSEMENT DES CARTES DE FLUX

La conception mécanique de cette instrumentation relève de la section 5.3.2.

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

L'instrumentation AMS ne contribue à aucune fonction de sûreté.

0.2. CRITÈRES FONCTIONNELS

L'instrumentation AMS ne contribue à aucune fonction de sûreté, elle n'a donc pas de critères fonctionnels associés.

0.3. EXIGENCES RELATIVES A LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Les parties de l'instrumentation AMS jouant un rôle vis-à-vis de la sûreté doivent faire l'objet d'un classement de sûreté conformément aux règles de classement indiquées à la section 3.2.1.

0.3.1.2. Critère de Défaillance Unique (active et passive)

Compte tenu de son classement NC, l'instrumentation AMS n'est pas redevable de l'application du critère de défaillance unique.

0.3.1.3. Alimentation électrique de secours

L'instrumentation AMS ne fait pas l'objet d'une exigence d'alimentation électrique secourue.

0.3.1.4. Séparation physique / géographique

Compte tenu de son classement NC, l'instrumentation AMS ne fait pas l'objet d'une exigence de séparation physique/géographique.

0.3.1.5. Qualification aux conditions accidentelles

Du fait de leur classement NC, les équipements de l'instrumentation AMS ne font pas l'objet d'une exigence de qualification aux conditions accidentelles.

0.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

Les équipements de l'instrumentation AMS redevables d'un classement mécanique, électrique, contrôle-commande et sismique doivent être classés conformément aux règles de classement présentées dans la section 3.2.1.

Les équipements de l'instrumentation AMS redevables d'un classement ESPN doivent être classés conformément à la réglementation applicable (cf. section 3.6.2).

0.3.2. Exigences réglementaires

0.3.2.1. Textes réglementaires

0.3.2.1.1. Textes officiels

L'instrumentation AMS est concernée par le décret 207-534 du 10/04/2007 autorisant la création de l'installation nucléaire de base dénommée Flamanville 3 par les exigences suivantes :

- III-1.1.1c : « Ces moyens de mesure et l'intensité des sources de comptage associées sont choisis et maintenus à un niveau de performances tel que l'exploitant n'ait jamais à faire démarrer la circulation d'eau du circuit primaire principal ni à entreprendre la diminution de la concentration de cette eau en absorbant neutronique soluble sans disposer d'une mesure significative du flux neutronique. »
- III-1.1.1d : « Le suivi de la distribution de puissance dans le cœur est assuré par différents systèmes de mesure neutronique répartis dans et en dehors du cœur. »

0.3.2.1.2. Prescriptions techniques

L'instrumentation AMS n'est pas concernée par une prescription technique spécifique.

0.3.2.1.3. Réglementations internationales

L'instrumentation AMS n'est pas concernée par une réglementation internationale spécifique.

0.3.2.2. Textes para-réglementaires

0.3.2.2.1. Règles fondamentales de sûreté

L'instrumentation AMS n'est pas concernée par une règle fondamentale de sûreté spécifique.

0.3.2.2.2. Directives techniques

L'instrumentation AMS est concernée par la section suivante des Directives Techniques (voir la section ci-dessous de la section 1.7.0) :

- Section B.1.1 : « Le suivi de la distribution de puissance dans le cœur peut être assuré par une instrumentation neutronique fixe dans le cœur, un système de mesure mobile ("aéroball") et une instrumentation neutronique en dehors du cœur. »

0.3.2.3. Textes EPR spécifiques

L'instrumentation AMS n'est pas concernée par un texte spécifique EPR.

0.3.3. Agressions

0.3.3.1. Agressions internes

Les fonctions de l'instrumentation AMS doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Les fonctions de l'instrumentation AMS doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3.4. Diversification

L'instrumentation AMS ne fait pas l'objet d'une exigence de diversification.

0.3.5. Radioprotection

L'instrumentation AMS n'est pas concernée par une exigence de radioprotection.

0.3.6. Exigences liées au fonctionnement, à la maintenance et à l'accessibilité long terme

L'instrumentation AMS n'est pas concernée par une exigence liée au fonctionnement, à la maintenance et à l'accessibilité long terme dans la gestion long terme après accident.

0.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

0.4.1. Essais de démarrage

L'instrumentation AMS doit être conçue pour permettre la réalisation d'essais de démarrage permettant de s'assurer de sa conception adéquate et de ses performances.

0.4.2. Surveillance en exploitation

L'instrumentation AMS n'ayant pas de mission de sûreté, il n'est donc pas nécessaire que sa conception permette une surveillance en exploitation normale des caractéristiques du système afin d'assurer le bon comportement de ses composants et leur disponibilité en fonctionnement normal, incidentel et accidentel.

0.4.3. Essais périodiques

L'instrumentation AMS n'ayant pas de mission de sûreté, elle ne fait donc pas l'objet d'une exigence d'aptitude à la réalisation d'essais périodiques.

0.4.4. Maintenance

L'instrumentation AMS doit être conçue pour permettre la mise en œuvre d'un programme de maintenance conformément au chapitre VIII des RGE.

1. RÔLE DU SYSTÈME

L'instrumentation AMS assure les fonctions opérationnelles suivantes dans les différentes conditions de fonctionnement de l'installation dans lesquelles elle est sollicitée :

1.1. RÔLE DU SYSTÈME PENDANT L'EXPLOITATION NORMALE DE LA TRANCHE

Le principe de l'instrumentation de mesure à billes à propulsion pneumatique AMS (*Aeroball Measuring System*) est de mesurer l'activité (par comptage d'impulsions) de quarante trains de billes en acier irradiés dans le cœur du réacteur. L'activité des trains de billes est mesurée sur la table de mesure, puis utilisée pour calculer les « valeurs d'activation » qui sont proportionnelles à la densité du flux neutronique dans le cœur du réacteur.

Les valeurs d'activation fournies par l'instrumentation AMS sont exploitées par l'outil de réalisation de cartes de flux et de calibrage du contrôle-commande du cœur, pour la détermination de la distribution de puissance cœur ainsi que le calcul des coefficients de calibrage des collectrons et des chaînes de mesure niveau puissance (CNP) qui est effectué à intervalles périodiques pour s'adapter à l'évolution du flux neutronique dans le cœur et à l'épuisement des collectrons en cours de cycle.

L'instrumentation AMS permet ainsi le calibrage des chaînes de protection et de surveillance du cœur.

1.2. RÔLE DU SYSTÈME DANS DES CONDITIONS DE FONCTIONNEMENT PCC2 A PCC4, RRC-A, EN ACCIDENT GRAVE ET SITUATIONS AGRESSIONS

L'instrumentation AMS n'a pas de rôle opérationnel dans les conditions de fonctionnement PCC-2 à PCC-4, RRC-A, situations Accident Grave et d'agression.

2. BASES DE CONCEPTION

2.1. HYPOTHÈSES GÉNÉRALES DE FONCTIONNEMENT

L'exigence principale concernant l'instrumentation AMS est son intégrité mécanique afin d'éviter qu'elle affecte d'autres systèmes se trouvant à proximité.

2.2. HYPOTHÈSES DE DIMENSIONNEMENT

L'instrumentation AMS ne contribue directement ou indirectement à aucune fonction fondamentale de sûreté, ni à la protection contre les agressions, ni à l'élimination pratique.

2.3. AUTRES HYPOTHÈSES

2.3.1. Précision

Via le calibrage des collectrons, l'incertitude de l'instrumentation AMS est prise en compte dans l'incertitude globale des chaînes de protection concernées.

2.3.2. Temps de réponse

L'instrumentation AMS est conçue pour une mesure en discontinu. Elle est activée sur demande par le personnel d'exploitation. Les valeurs d'activation désirées sont fournies environ 10 minutes après l'activation du système (3 minutes d'activation en cœur et 7 minutes de traitement).

3. DESCRIPTION - FONCTIONNEMENT

3.1. DESCRIPTION

3.1.1. Description générale du système

L'instrumentation de mesure à billes (AMS), fonctionnant par intermittence, fournit les données à intervalles spécifiques avec un haut niveau de résolution locale.

L'instrumentation AMS se compose d'un total de quarante sondes de mesure à billes installées dans des assemblages combustibles donnés, répartis dans le cœur.

Un train de billes d'acier[], d'un diamètre d'environ 1,7 mm, se déplace dans un tube de transport des billes logé dans chaque sonde. La longueur d'un train de billes correspond à la hauteur active du cœur.

Lorsqu'ils sont en position de repos, les trains de billes se trouvent au-dessus des butées électromagnétiques de billes au niveau de la passerelle à câbles située au-dessus de la cuve du réacteur. Les trains sont amenés par force pneumatique (à l'aide d'azote) jusqu'à leur position d'activation dans le cœur du réacteur où les billes seront activées par des neutrons (pour une explication détaillée du système de transport de l'instrumentation AMS (voir figures FIG–7.5.2.1.2 et FIG–7.5.2.1.3). Une fois le temps d'irradiation défini écoulé, les trains de billes sont transportés vers un compartiment de mesure où leur activité est mesurée.

Dans le local de mesure, les tubes de transport des billes cheminent vers la table de mesure qui comporte dix lignes de mesure. Quatre tubes de transport de billes sont regroupés en parallèle sous chacune des lignes de mesure. Chacun des quatre tubes de chaque ligne de mesure est affecté à un des quatre sous-systèmes. Seul un des quatre sous-systèmes est mesuré à la fois. Ceci permet de mesurer successivement la totalité des quarante trains de billes activés en différentes positions radiales du cœur, en quatre cycles d'acquisition.

Les trains de billes d'un même sous-système sont mesurés simultanément, les mesures étant effectuées séparément pour chaque train. Pendant les mesures, les trains de billes activés des trois autres sous-systèmes sont en position de repos.

Chacune des dix lignes de détecteurs est divisée longitudinalement en[] égaux. Au centre de chaque segment se trouve un collimateur (voir figure **FIG–7.5.2.1.4**) équipé d'un détecteur PIPS, qui est en silicium « à jonction implantée et passive ».

Sur ordre du contrôle-commande, chaque détecteur est connecté à un amplificateur de charges et à un compteur d'impulsions via des modules relais coaxiaux[].

Les taux de comptage (en coups par seconde) de chaque canal de mesure sont transférés à l'ordinateur de l'instrumentation AMS pour le traitement ultérieur des données. Cet ordinateur effectue également une partie du traitement des données en plus de la commande en boucle ouverte entièrement automatique du système de mesure des billes.

3.1.1.1. Systèmes en interface

Systèmes serveurs

L'instrumentation AMS est servie par le système élémentaire SGN fournissant l'azote qui sert de gaz moteur assurant le transport de chaque train de billes individuel sur demande.

Systèmes servis

L'instrumentation AMS fournit des données à l'outil de réalisation de cartes de flux et de calibrage du contrôle-commande du cœur. Il fournit à ce système les « valeurs d'activation » qui ont été calculées par l'ordinateur AMS après mesure des taux de comptage des trains de billes activés fournis par les détecteurs PIPS de la table de mesure AMS.

3.1.1.2. Signaux et commandes

L'instrumentation AMS transmet différents signaux permettant de contrôler et de surveiller l'état du système. Les signaux qui indiquent les états normaux/anormaux de fonctionnement du système sont transmis au MCP.

Les défauts (signaux binaires) sont transférés au système PAS et affichés sur le MCP.

3.1.2. Description des matériels principaux

Les billes sont transportées entre les doigts des lances d'instrumentation et la table de mesure au moyen d'un système de gaz sous pression. La tuyauterie de l'AMS se compose de deux systèmes : les tubes servant au transport des billes et la tuyauterie de gaz sous pression. La tuyauterie de gaz moteur est raccordée aux deux extrémités du système de tubes de transport via les électrovannes (équipement de commande). Pour cela, une installation spéciale dans les doigts des lances est nécessaire. Voici un aperçu des composants et de leur fonction :

3.1.2.1. Lance

La lance d'instrumentation du cœur est l'unité mécanique de base du système de mesure neutronique interne du cœur. Chaque lance comprend trois ou quatre doigts de gant AMS (selon la position dans le cœur) ainsi qu'un doigt de gant accueillant six collectrons et trois thermocouples (doigt ECI - *Exchange Instrumentation*). Les tubes de guidage et de protection (doigts) sont suspendus à un bâti qui repose sur la plaque supérieure de la structure des internes supérieurs entre les tubes guides des grappes de contrôle.

La figure **FIG–7.5.2.1.5** montre le nombre de lances d'instrumentation, les sondes de mesure à billes et les doigts ECI ainsi que leur répartition dans le cœur.

A l'extrémité inférieure du doigt, le tube de transport des billes dans le doigt de lance se termine par une butée de billes perméable au gaz. Une conduite d'alimentation en gaz étanche et résistant à la pression de l'environnement, concentrique au tube de transport des billes, est raccordée au tube de transport des billes via la butée de billes. Cela permet d'appliquer une contre-pression pour éjecter les trains de billes dans la direction inverse.

3.1.2.2. Butée de billes

Une butée de billes électromagnétique est installée sur le tube de transport des billes entre la lance et la table de mesure, à proximité de la tête de lance.[] Cette butée de billes constitue une « porte » qui peut être ouverte ou fermée pour le train de billes. Lorsqu'elle est ouverte, le transport des billes peut s'effectuer dans les deux sens possibles, c'est-à-dire vers le cœur ou vers la table de mesure. Lorsque la butée est fermée, le train de billes occupe une position d'attente ou de repos donnée. En position d'attente, le train de billes se trouve sous la butée de billes (pression appliquée dans la direction de la table de mesure) alors qu'en position de repos le train de billes se trouve au-dessus de la butée à billes (pression appliquée dans la direction de la lance, ou bien aucune pression n'est appliquée).

3.1.2.3. Table de mesure

Elle est constituée de dix lignes de mesure. Sous chacune des dix lignes de mesure sont regroupés en parallèle quatre tubes de transport de billes. Chacun des quatre tubes de chaque ligne de mesure est affecté à un des quatre sous-systèmes. Chacun de ces quatre sous-systèmes est équipé de son propre système de commande par vannes avec une alimentation en tension indépendante pour le système de transport pneumatique. Les quatre sous-systèmes peuvent donc être actionnés indépendamment.

La table de mesure comporte également des raccordements pour le remplacement des trains de billes.

3.1.2.4. Équipement de contrôle

L'équipement de contrôle (alimentation en azote) [] où se trouve la table de mesure AMS. Il comporte toutes les vannes nécessaires à la commande du transport des billes. Les conduites de gaz moteur menant à la table de mesure cheminent via cet équipement de contrôle et sont disposées parallèlement aux tubes de transport des billes dans le compartiment de la table de mesure AMS voisin.

L'azote servant de gaz moteur pour le circuit pneumatique est transmis aux quatre sous-systèmes via des détendeurs, des réservoirs tampons équipés de manomètres et de pressostats, des électrovannes, des filtres et des branchements. Chacun des quatre sous-systèmes est équipé d'un système de commande d'électrovannes distinct.

En cas de chute de pression dans le circuit d'alimentation principal, la conduite d'alimentation connectée au circuit d'alimentation principal est automatiquement isolée par une électrovanne. Le transport des billes est quand même assuré par l'azote de réserve provenant des réservoirs tampons.

La conduite d'alimentation en gaz menant aux sous-systèmes individuels est raccordée à deux vannes à trois voies. L'une de ces deux vannes commande le train de gaz moteur menant à la lance d'instrumentation et l'autre commande le train de gaz moteur menant à la table de mesure. Le troisième raccord des deux vannes est branché sur la ligne de décharge commune via un filtre aérosol.

Chaque vanne trois voies est équipée d'une électrovanne à fermeture rapide montée en amont du côté réacteur. En cas de défaillance du système de transport des billes, les modules de contrôle génèrent les alarmes correspondantes transmises en fil-à-fil au système PAS qui sont affichées sur le MCP. De plus, les vannes à fermeture rapide se ferment automatiquement. Ceci garantit qu'aucun transport de billes ne peut avoir lieu dans les sous-systèmes concernés jusqu'à ce que la cause de la défaillance ait été identifiée et qu'on y ait remédié.

Dans les conditions normales de fonctionnement, les vannes à fermeture rapide sont ouvertes par l'ordinateur AMS pour le transport des billes.

3.1.3. Description des dispositions d'installations principales

Les composants de l'instrumentation AMS sont installés dans différentes salles à l'intérieur et à l'extérieur de l'enceinte. Pour une vue d'ensemble détaillée, voir la figure **FIG–7.5.2.1.1**.

A l'intérieur du cœur, les doigts de gant de l'AMS sont répartis comme indiqué sur la figure FIG–7.5.2.1.5. Les quatre différents sous-systèmes sont repérés par des hachures de différentes couleurs.

Afin de pouvoir utiliser les « valeurs d'activation » mesurées par l'instrumentation AMS pour les tâches énumérées dans le « rôle du système » (voir § 1.), les doigts d'instrumentation de l'AMS sont répartis de manière homogène sur toute la section transversale du cœur.

Un niveau de rayonnement important peut exister dans la salle [] si des billes activées sont amenées vers la table de mesure (lors des mesures) (voir figure FIG–7.5.2.1.1). Ceci est signalé dans les salles [] avant le transport des billes pour permettre aux membres du personnel de quitter la salle : visuellement à l'aide d'une lampe clignotante et acoustiquement par un avertisseur sonore.

Les armoires [] fonctionnent avec une source d'alimentation externe [], provenant du bâtiment des tableaux électriques avec une puissance maximale de []. La tension de fonctionnement interne est de []. Les quatre sous-systèmes du système de transport possèdent des convertisseurs distincts.

Les défauts de l'alimentation électrique sont surveillés.

3.2. FONCTIONNEMENT

3.2.1. Fonctionnement en régime normal de la tranche

En régime normal de la tranche, l'instrumentation AMS est en service continu.

3.2.2. Fonctionnement en régime permanent du système

L'instrumentation AMS est conçue pour fonctionner dans les conditions normales de la centrale. Lors du démarrage et du fonctionnement en puissance, les mesures des billes peuvent être effectuées comme indiqué ci-après.

La mesure par billes (*aeroball*) est lancée manuellement. Une fois la mesure lancée, les quarante trains de billes (quatre sous-systèmes) sont transportés de leur position de repos à leur position d'irradiation dans le cœur du réacteur (voir figure FIG–7.5.2.1.2). A cet endroit, ils seront activés par le rayonnement neutronique. Seul le processus d'activation du Vanadium 51 (V-51) présent dans les billes d'acier au vanadium est important pour ce type de mesure. Le Vanadium 52 (V-52) est généré à partir du nucléide V-51 par capture de neutron. Le V-52 est un nucléide instable qui décroît avec une demi-vie radioactive de 3,75 minutes selon le processus :

$$^{52}_{23}V \rightarrow ^{52}_{24}Cr + \beta^- + \gamma$$

Le rayonnement gamma résultant a une énergie caractéristique à 1,434 MeV.

Après une durée d'activation de généralement 3 minutes, tous les trains de billes sont transportés hors du cœur. Trente d'entre eux (trois sous-systèmes) sont arrêtés en position d'attente alors que dix d'entre eux (un sous-système) sont directement amenés à la table de mesure. Aussi, une mesure du temps de transport du premier sous-système (sous-système sélectionné avant le lancement de la mesure par billes et changé après chaque mesure) depuis le cœur jusqu'à la table de mesure est faite. C'est là qu'a lieu la mesure de l'activation. La distribution de l'activité le long des trains de billes est proportionnelle à la densité du flux neutronique et donc à la densité de puissance à l'endroit de l'activation.

La mesure de l'activation est exclusivement effectuée pour le nucléide V-52 en utilisant le rayonnement gamma caractéristique qui accompagne la décroissance bêta du V-52. La décroissance rapide du V-52 permet des mesures successives des billes toutes les 10 minutes environ avec un niveau de précision suffisamment élevé.

Une fois mesurés, les dix trains de billes du premier sous-système sont envoyés à leur position de repos (voir figure FIG–7.5.2.1.2) et les dix trains du sous-système suivant sont transportés de leur

position d'attente à la table de mesure. Cette procédure est répétée jusqu'à ce que les trains des quatre sous-systèmes soient mesurés et transportés à leur position de repos.

Dès la mise en service de l'instrumentation, une mesure en temps réel pour chaque position de mesure de chaque sous-système est effectuée pour calculer les valeurs d'activation exactes à partir des taux de comptage mesurés.

Les valeurs d'activation sont transférées à l'outil de réalisation de cartes de flux et de calibrage du contrôle-commande en respectant les critères de sécurité informatique.

Un réglage des indicateurs et des signaux d'état est réalisé, pour information de l'opérateur. L'opérateur peut obtenir à tout moment des informations sur l'état du système via le terminal d'exploitation. Il existe une surveillance permanente de la pression de N2, de l'humidité et de l'alimentation électrique. Les défaillances détectées doivent être signalées à l'aide du système PAS et affichées sur le MCP. En outre, de plus amples informations sur l'état de l'instrumentation et des messages détaillés concernant les défaillances sont disponibles au niveau du terminal de l'instrumentation AMS.

3.2.3. Fonctionnement en régime transitoire

Sans objet.

3.2.4. Autres régimes de fonctionnement du système

3.2.4.1. Fonctionnement du système lors d'un fonctionnement dégradé de la centrale

L'instrumentation AMS n'est nécessaire que lors du fonctionnement normal en puissance de la centrale. Dans des conditions de fonctionnement anormales de la centrale, l'instrumentation AMS n'est pas utilisée. Il n'est donc pas nécessaire de revenir automatiquement au fonctionnement normal de l'instrumentation AMS après des conditions accidentelles.

3.2.4.2. Défaillance de la totalité ou d'une partie du système

Il existe principalement deux types de défaillances pour ce système (non classé) : les défaillances provoquant la panne de la totalité de l'instrumentation et les défaillances n'affectant qu'une partie de l'instrumentation AMS (et permettant cependant la mesure avec un nombre limité de trains de billes).

Les défaillances qui bloquent la fonctionnalité de base du système sont les suivantes :

- perte de l'alimentation d'un de ses composants de base,
- rupture de l'alimentation en gaz moteur (fuite, perte de pression, etc.),
- problèmes mécaniques du système de transport (défaillance de l'équipement de commande, rupture des tubes de transport, etc.).

En cas de défaillance de la totalité de l'instrumentation, aucune mesure d'activité ne peut être effectuée et donc l'outil de réalisation de cartes de flux et de calibrage du contrôle-commande du cœur ne reçoit plus les informations nécessaires pour accomplir ses tâches (voir § 1.). En particulier, il est impossible d'effectuer un calibrage des collectrons.

En cas de défaillance partielle, l'instrumentation AMS n'est pas exploitable sans analyse d'impact sur la détermination de la distribution de puissance cœur.

4. ANALYSE DE SÛRETÉ

4.1. CONFORMITÉ A LA RÉGLEMENTATION

L'instrumentation AMS est conforme à la réglementation générale en vigueur (voir le sous-chapitre 1.7) et ne fait pas l'objet de dérogations particulières.

4.2. RESPECT DES CRITÈRES FONCTIONNELS

L'instrumentation AMS ne contribue directement ou indirectement à aucune fonction fondamentale de sûreté, ni à la protection contre les agressions, ni à l'élimination pratique.

4.3. CONFORMITÉ AUX EXIGENCES DE CONCEPTION

L'instrumentation AMS est conforme aux exigences de conception évoquées au **§ 0.3.**, notamment pour ce qui concerne :

4.3.1. Exigences issues du classement de sûreté

4.3.1.1. Classement de sûreté

Les classements des équipements de l'instrumentation AMS jouant un rôle vis-à-vis de la sûreté sont présentés dans la section 3.2.2.

4.3.1.2. Critère de défaillance unique (active et passive)

L'instrumentation AMS n'est pas redevable de l'application du Critère de Défaillance Unique.

4.3.1.3. Alimentation électriquede secours

L'instrumentation AMS ne fait pas l'objet d'une exigence d'alimentation électrique secourue.

4.3.1.4. Séparation physique/géographique

L'instrumentation AMS n'est pas redevable de l'application d'une exigence de séparation physique/ géographique.

4.3.1.5. Qualification aux conditions accidentelles

Du fait de leur classement NC, les équipements de l'instrumentation AMS ne font pas l'objet d'une exigence de qualification aux conditions accidentelles.

4.3.1.6. Classement ESPN, mécanique, électrique, contrôle commande et sismique

La conformité des classements mécanique, électrique, contrôle-commande et sismique des équipements de l'instrumentation AMS jouant un rôle vis-à-vis de la sûreté aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

La conformité du classement ESPN des équipements de l'instrumentation AMS aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

4.3.2. Exigences réglementaires

4.3.2.1. Textes réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.1.1. Textes officiels

La conformité aux textes officiels spécifiquement applicables au système, listés dans le **§ 0.3.2.**, est assurée par :

- les opérations de maintenance réalisées afin de maintenir le niveau de performance (cf. **§ 4.4.4.**). De plus les RGE détaillent les exigences de disponibilité des chaînes (cf. chapitre VIII),
- le suivi de la distribution de puissance dans le cœur (cf. **§ 3.1.** et **§ 3.2.**).

4.3.2.1.2. Prescriptions techniques

Sans objet.

4.3.2.1.3. Réglementations internationales

Sans objet.

4.3.2.2. Textes para-réglementaires

La conformité aux textes para-réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.3. Textes EPR spécifiques

L'instrumentation AMS n'est pas concernée par un texte EPR spécifique.

4.3.3. Agressions

4.3.3.1. Agressions internes

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

4.3.3.2. Agressions externes

La démonstration de la robustesse de l'installation aux agressions externes relève du sous-chapitre 3.3.

4.3.4. Diversification

L'instrumentation AMS ne fait pas l'objet d'une exigence de diversification.

4.3.5. Radioprotection

Sans objet.

4.3.6. Fonctionnement, maintenance et accessibilité long terme

Sans objet.

4.3.7. Système tel que réalisé

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

4.4.1. Essais de démarrage

Bien que l'instrumentation AMS soit classée NC, elle fait l'objet d'un programme d'essais de démarrage conformément aux modalités présentées au chapitre 14.

Après installation du système, des essais de mise en service sont effectués pour s'assurer du bon fonctionnement de l'instrumentation AMS et des interfaces. Les essais à effectuer testent :

- les fonctions électriques, la puissance consommée, la signalisation d'erreurs,
- les fonctions de mesure des détecteurs, les amplificateurs,
- les fonctions de transport,
- les interfaces opérateur,

- le transfert de données d'une carte de flux sur support informatique à l'outil de réalisation de cartes de flux et de calibrage,
- la transmission des signaux au MCP.

Ces essais sont effectués lors du premier démarrage de la centrale avec des tests complets pour vérifier les valeurs mesurées.

[]

4.4.2. Surveillance en exploitation

Les mêmes fonctions que celles citées dans le paragraphe précédent sont disponibles pour la vérification du bon fonctionnement et la surveillance du système, notamment après des interventions de la maintenance corrective suite à une défaillance du matériel.

L'essai fonctionnel de l'instrumentation AMS est généralement effectué au moyen des fonctions technologiques. Des essais supplémentaires sur demande permettent de s'assurer que l'instrumentation satisfait aux exigences fonctionnelles et aux exigences de performance.

Les calibrages assistés par ordinateur des détecteurs de rayonnement de l'AMS sont généralement réalisés à l'aide d'une source gamma.

4.4.3. Essais périodiques

Étant donné que l'instrumentation AMS est un système non-classé, aucun essai périodique n'est à réaliser.

4.4.4. Maintenance

L'instrumentation AMS fait l'objet d'un programme de maintenance conformément au chapitre VIII des RGE.

4.4.4.1. Précautions pour les activités de maintenance

L'accessibilité des composants se trouvant dans la salle[], à des fins de maintenance, dépend de l'état du système. Lorsque les billes activées sont amenées sur la table de mesure, par exemple lors d'une mesure des billes, il n'est pas possible d'avoir accès à tous les composants de la salle[] du fait du fort niveau de rayonnement.

La teneur en oxygène de l'air des salles [] doit être mesurée à l'aide d'un appareil portatif avant d'accéder aux salles pour s'assurer de la bonne qualité de l'air.

4.4.4.2. Généralités

Différentes fonctions de surveillance permettent de détecter les dégradations de l'instrumentation AMS. Les différentes indications d'erreur (voir § 3.1.1.2.) et plusieurs programmes d'essai (voir ci-dessous) identifient les problèmes. Une maintenance corrective par un personnel qualifié n'est donc nécessaire qu'en cas d'erreurs signalées.

En outre, les programmes listés ci-dessous servent de programmes de test et de support pour détecter les défaillances, mesurer les paramètres contrôlant l'instrumentation AMS ou pour initialiser les champs de données. Ces fonctions ne peuvent être activées que depuis le poste opérateur dans le local technique de contrôle-commande[].

Programme de mesure d'essai

Cette fonction enregistre les taux de comptage d'une section de mesure sélectionnée pendant une période définie. Cette fonction est utilisée lors du réglage du seuil de discrimination ou pour les diagnostics d'erreur de l'électronique de mesure de l'instrumentation AMS.

Les résultats sont enregistrés dans un fichier qui peut être affiché sur l'écran de l'ordinateur ou imprimé.

Programme de mesure de bruit de fond

Les détecteurs PIPS défectueux peuvent être identifiés à l'aide de ce programme grâce à leur niveau de bruit accru. Lors de la mesure du bruit de fond les trains de billes restent à leur position de repos.

[]

Les résultats sont enregistrés dans un fichier qui peut être affiché sur l'écran de l'ordinateur ou imprimé.

4.4.4.3. Maintenance préventive

Deux opérations différentes garantissent le bon fonctionnement de l'instrumentation AMS.

Ils comportent les étapes suivantes :

- Le calibrage des détecteurs PIPS (semi-conducteurs) sera effectué lors d'un arrêt pour rechargement (sur l'ensemble des détecteurs) ou après un remplacement d'un détecteur en défaillance (seulement sur le détecteur remplacé). Conformément aux instructions d'essai, tous les détecteurs PIPS sont étalonnés sur une source de rayonnement. L'intervalle de temps entre les essais correspond à la durée d'un cycle du combustible mais l'essai peut être effectué sur demande par le système de traitement des données si la précision des valeurs mesurées diminue.
- Le contrôle du système de transport inclut la mesure de la durée d'exécution et la vérification de l'affectation (affectation de la position d'activation dans le cœur et position de mesure sur la table). Cet essai est effectué après chaque ouverture/fermeture des composants du système de transport des billes.

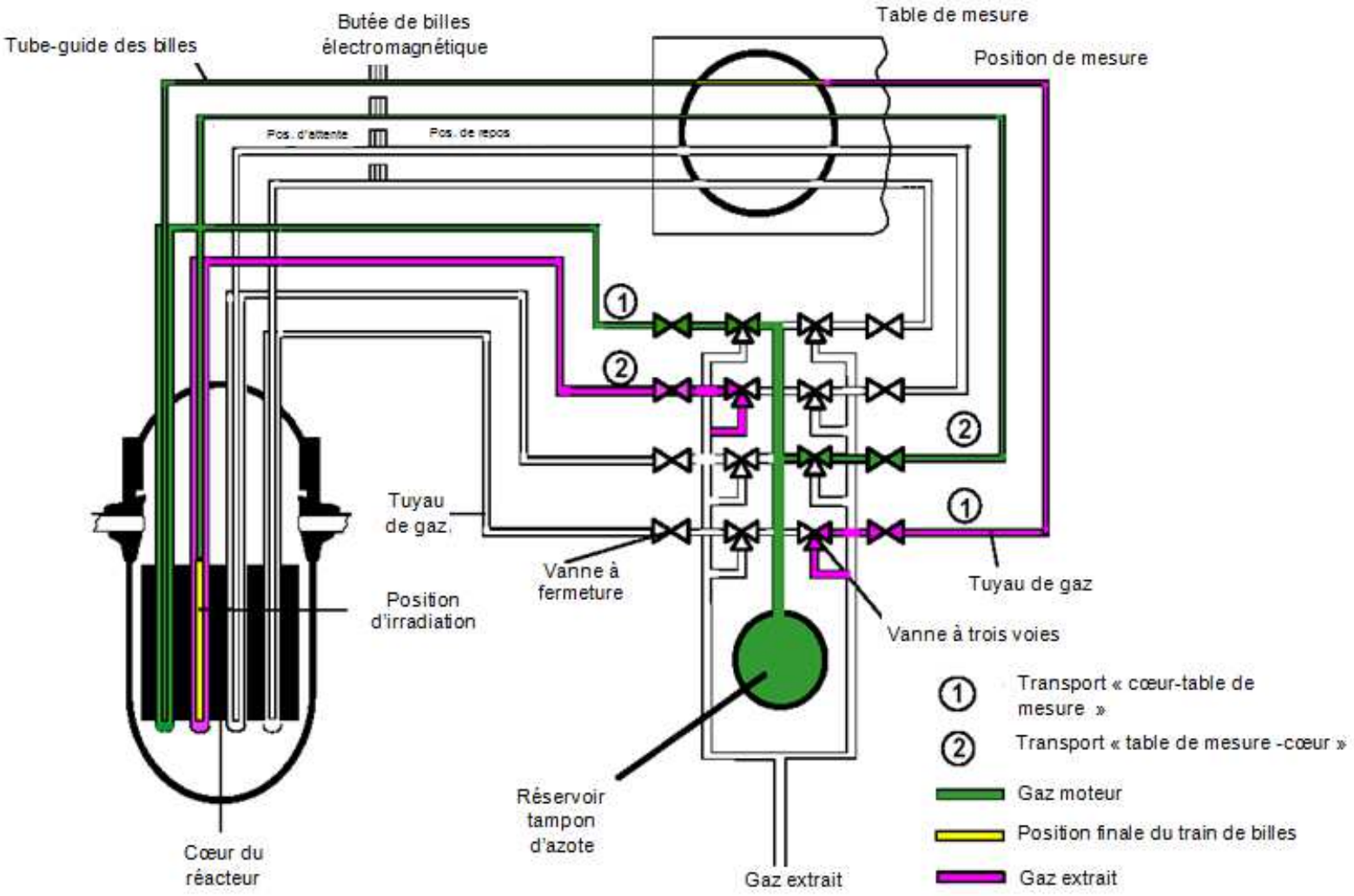
De plus, en cas de non-respect de la durée de transport maximale, la lubrification du système de transport permet de restituer le bon fonctionnement de ce dernier.

5. SCHÉMA DE PRINCIPE

Le schéma de principe de l'instrumentation AMS est présenté en figure **FIG–7.5.2.1.3**.

FIG–7.5.2.1.1 ARCHITECTURE DE L'INSTRUMENTATION AMS

FIG–7.5.2.1.2 SYSTÈME DE TRANSPORT PNEUMATIQUE



FIG–7.5.2.1.3 VUE D'ENSEMBLE SCHÉMATIQUE DE L'INSTRUMENTATION AMS

FIG–7.5.2.1.4 COLLIMATEUR

FIG–7.5.2.1.5 POSITIONS DANS LE CŒUR DE L'INSTRUMENTATION AMS

SOMMAIRE

TABLEAUX :

FIGURES :

.7.5.2.2 INSTRUMENTATION INTERNE FIXE DU CŒUR — COLLECTRONS ET THERMOCOUPLES DE SORTIE CŒUR

La conception mécanique de cette instrumentation relève de la section 5.3.2.

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

0.1.1. Contrôle de la réactivité

La contribution de l'instrumentation interne fixe du cœur au contrôle de la réactivité doit être la suivante :

- fournir une mesure continue du flux neutronique à des positions données dans le cœur dans certaines conditions de fonctionnement de catégorie PCC-2, PCC-3, PCC-4, ainsi que dans le cadre des études spécifiques.

0.1.2. Évacuation de la puissance résiduelle

L'instrumentation interne fixe du cœur ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.1.3. Confinement des substances radioactives

L'instrumentation interne fixe du cœur ne contribue pas directement au confinement des substances radioactives.

0.1.4. Contributions indirectes aux fonctions de sûreté

La contribution indirecte de l'instrumentation interne fixe du cœur à l'évacuation de la puissance résiduelle doit être la suivante :

- fournir la distribution radiale de température dans le cœur dans certaines conditions de fonctionnement de catégorie PCC-2, PCC-3, PCC-4 et RRC-A ainsi qu'en situation d'accident grave et dans le cadre des études spécifiques.

0.1.5. Contributions spécifiques à la protection contre les agressions

L'instrumentation interne fixe du cœur ne contribue pas spécifiquement à la protection contre les agressions.

0.1.6. Contributions à l'élimination pratique

L'instrumentation interne fixe du cœur ne contribue pas directement à l'élimination pratique.

0.2. CRITÈRES FONCTIONNELS

Au titre de ses contributions à l'accomplissement des fonctions de sûreté, l'instrumentation interne fixe du cœur doit satisfaire les critères fonctionnels suivants :

0.2.1. Contrôle de la réactivité

- mesure du flux neutronique :
  L'instrumentation interne fixe du cœur doit fournir, dans la plage de puissance linéique attendue, dans les temps de réponse et les précisions requises, la mesure continue du flux neutronique à des positions données dans le cœur, en PCC-2, PCC-3, PCC-4, ainsi que dans le cadre des

études spécifiques, afin de respecter les critères d'acceptabilité de ces études (cf. sous–chapitre 15.1).

0.2.2. Évacuation de la puissance résiduelle

L'instrumentation interne fixe du cœur ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.2.3. Confinement des substances radioactives

L'instrumentation interne fixe du cœur ne contribue pas directement au confinement des substances radioactives.

0.2.4. Contributions indirectes aux fonctions de sûreté

Au titre de sa contribution indirecte à l'évacuation de la puissance résiduelle, l'instrumentation interne fixe du cœur doit satisfaire les critères fonctionnels suivants :

- distribution radiale de température dans le cœur : l'instrumentation interne fixe du cœur doit fournir, dans la plage de température attendue, dans les temps de réponse et les précisions requises, la distribution radiale de température dans le cœur, en PCC-2, PCC-3, PCC-4 et RRC-A ainsi qu'en situation d'accident grave et dans le cadre des études spécifiques, afin de respecter les critères d'acceptabilité de ces études.

0.3. EXIGENCES RELATIVES À LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Les parties de l'instrumentation interne fixe du cœur jouant un rôle vis-à-vis de la sûreté doivent faire l'objet d'un classement de sûreté conformément aux règles de classement indiquées à la section 3.2.1.

0.3.1.2. Critère de Défaillance Unique (active et passive)

Les fonctions de l'instrumentation interne fixe du cœur classées F1 doivent être robustes à l'application du critère de défaillance unique.

0.3.1.3. Alimentation électrique de secours

L'alimentation électrique des composants de l'instrumentation interne fixe du cœur nécessaire à l'accomplissement des fonctions classées F1 doit être secourue par les groupes diesels principaux.

0.3.1.4. Séparation physique / géographique

Les fonctions classées F1 de l'instrumentation interne fixe du cœur doivent être conçues conformément à l'exigence de séparation physique / géographique de leurs équipements redondants constitutifs :

- séparation physique et électrique des chaînes de mesure redondantes (fonctions F1A et F1B).

0.3.1.5. Qualification aux conditions accidentelles

Les équipements classés de l'instrumentation interne fixe du cœur doivent être qualifiés en fonction des conditions de fonctionnement dans lesquelles ils sont sollicités au titre de leur contribution à l'accomplissement des fonctions de sûreté, conformément aux règles du sous-chapitre 3.7.

0.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

Les équipements de l'instrumentation interne fixe du cœur redevables d'un classement mécanique, électrique, contrôle-commande et sismique doivent être classés conformément aux règles de classement présentées dans la section 3.2.1.

Les équipements de l'instrumentation interne fixe du cœur redevables d'un classement ESPN doivent être classés conformément à la réglementation applicable (cf. section 3.6.2).

0.3.2. Exigences réglementaires

0.3.2.1. Textes réglementaires

0.3.2.1.1. Textes officiels

L'instrumentation interne fixe du cœur est concernée par le texte officiel suivant :

- Décret 2007-534 du 10 avril 2007 autorisant la création de l'installation nucléaire de base dénommée Flamanville 3 :
  - III-1.1.1. Ces moyens de mesure et l'intensité des sources de comptage associées sont choisis et maintenus à un niveau de performances tel que l'exploitant n'ait jamais à faire démarrer la circulation de l'eau du circuit primaire principal ni à entreprendre la diminution de la concentration de cette eau en absorbant neutronique soluble sans disposer d'une mesure significative du flux neutronique (III-1.1.1.c).
  - III-1.1.1. Le suivi de la distribution de puissance dans le cœur est assuré par différents systèmes de mesure neutronique répartis dans et en dehors du cœur (III-1.1.1.d).
  - III-2.1.2. Tant qu'un assemblage de combustible est présent dans la cuve, l'inventaire en eau du circuit primaire et l'efficacité du refroidissement du combustible sont surveillés en permanence.

0.3.2.1.2. Prescriptions techniques

L'instrumentation interne fixe du cœur appartient au noyau dur Fukushima (cf. chapitre 21). A ce titre, il doit respecter la décision n ° 2012-DC-0 283 de l'Autorité de sûreté nucléaire du 26 juin 2012 et décision n°2014-DC-04 03 de l'Autorité de sûreté nucléaire du 21 janvier 2014 (voir section 1.7.0)

0.3.2.1.3. Réglementations internationales

L'instrumentation interne fixe du cœur n'est pas concernée par une réglementation internationale spécifique.

0.3.2.2. Textes para-réglementaires

0.3.2.2.1. Règles fondamentales de sûreté

L'instrumentation interne fixe du cœur n'est pas concernée par une règle fondamentale de sûreté spécifique.

0.3.2.2.2. Directives techniques

L'instrumentation interne fixe du cœur est concernée par les sections suivantes des Directives Techniques (voir les sections ci-dessous extraites de la section 1.7.0 du Rapport De Sûreté) :

- Section B.1.1 – Le suivi de la distribution de puissance dans le cœur peut être assuré par une instrumentation neutronique fixe dans le cœur, un système de mesure mobile (« aéroball ») et une instrumentation neutronique à l'extérieur du cœur,
- Section G3 – Conception du contrôle-commande.
  Cette section précise les exigences relatives à l'instrumentation et au contrôle-commande.
  Les exigences applicables à l'instrumentation concernent :
  - le classement fonctionnel de l'instrumentation,

- la prise en compte du critère de défaillance unique, de la maintenance et de la séparation physique,
- la prise en compte des conséquences des agressions internes et externes sur le contrôle-commande.

0.3.2.3. Textes EPR spécifiques

L'instrumentation interne fixe du cœur n'est pas concernée par un texte spécifique EPR.

0.3.3. Agressions

0.3.3.1. Agressions internes

Les fonctions de l'instrumentation interne fixe du cœur doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Les fonctions de l'instrumentation interne fixe du cœur doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3.4. Diversification

L'instrumentation interne fixe du cœur ne fait pas l'objet d'une exigence de diversification.

0.3.5. Radioprotection

L'instrumentation interne fixe du cœur doit être conçue pour limiter l'exposition du personnel au rayonnement et à la contamination dus aux produits de fission et aux produits de corrosion activés contenus dans le fluide véhiculé.

0.3.6. Exigences liées au fonctionnement, à la maintenance et à l'accessibilité long terme

L'instrumentation interne fixe du cœur n'est pas concernée par une exigence liée au fonctionnement, à la maintenance et à l'accessibilité long terme dans la gestion long terme après accident.

0.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

0.4.1. Essais de démarrage

L'instrumentation interne fixe du cœur doit être conçue pour permettre la réalisation d'essais de démarrage permettant de s'assurer de sa conception adéquate et de ses performances, et notamment du respect des critères fonctionnels qui lui sont assignés au § 0.2..

0.4.2. Surveillance en exploitation

L'instrumentation interne fixe du cœur doit être conçue pour permettre une surveillance en exploitation normale des caractéristiques du système nécessaires à l'accomplissement de ses missions de sûreté afin d'assurer le bon comportement de ses composants et leur disponibilité en fonctionnement normal, incidentel et accidentel.

0.4.3. Essais périodiques

Les parties classées de l'instrumentation interne fixe du cœur doivent être conçues pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

0.4.4. Maintenance

L'instrumentation interne fixe du cœur doit être conçue pour permettre la mise en œuvre d'un programme de maintenance conformément au chapitre VIII des RGE.

1. RÔLE DU SYSTÈME

L'instrumentation interne fixe du cœur se compose de deux sous-systèmes :

- les détecteurs neutroniques autoalimentés appelés « collectrons » ou « SPND » (*Self Powered Neutron Detectors*),
- les thermocouples de sortie du cœur désignés « COT » (*Core Outlet Temperature*).

L'instrumentation interne fixe du cœur assure les fonctions opérationnelles suivantes dans les différentes conditions de fonctionnement de l'installation dans lesquelles il est sollicité :

1.1. RÔLE DU SYSTÈME PENDANT L'EXPLOITATION NORMALE DE LA TRANCHE

Collectrons

Les collectrons fournissent une mesure continue du flux neutronique à des positions données dans le cœur. Les principales informations dérivées des mesures des collectrons sont les suivantes :

- puissance linéique maximale du cœur et sa position,
- RFTC minimal du cœur, distribution axiale de puissance et position,
- déséquilibre axial de puissance,
- interaction Pastille Gaine.

Thermocouples de sortie cœur

Les thermocouples de sortie cœur sont utilisés en fonctionnement normal pour fournir la distribution radiale de la température dans le cœur. Deux types d'informations, dérivées des mesures des thermocouples de sortie cœur, sont fournies à l'opérateur :

- température à la sortie du cœur,
- marge à la saturation à la sortie du cœur (calculée par le système RPR et par le SAS).

1.2. RÔLE DU SYSTÈME DANS DES CONDITIONS DE FONCTIONNEMENT PCC2 A PCC4, RRC-A, EN ACCIDENT GRAVE ET SITUATIONS D'AGRESSIONS

Collectrons

Les collectrons fournissent dans les conditions de fonctionnement PCC-2, PCC-3, PCC-4 et dans le cadre des études spécifiques, une mesure continue du flux neutronique à des positions données dans le cœur.

Thermocouples de sortie cœur

Les thermocouples de sortie cœur fournissent la température de référence (T_{RIC}) du circuit primaire (RCP) utilisée dans les procédures de conduite post-incidentelles et post-accidentelles et elle est également utilisée pour le calcul de la marge à la saturation à la sortie du cœur (ΔTsat).

Dans le cadre de la gestion post-accidentelle, les thermocouples de sortie cœur contribuent à atteindre l'état d'arrêt sûr pour toutes les situations incidentelles et accidentelles, à partir du moment où la cuve est fermée (autrement dit dès lors que les thermocouples de sortie cœur sont connectés).

2. BASES DE CONCEPTION

2.1. HYPOTHÈSES GÉNÉRALES DE FONCTIONNEMENT

Les critères de dimensionnement de l'instrumentation interne fixe du cœur sont principalement les suivants :

- disponibilité des fonctions classées de sûreté lors d'une défaillance ou lors des opérations de maintenance.

Pour répondre à ces critères, l'instrumentation interne fixe du cœur est dimensionnée comme suit :

- indépendance électrique entre les quatre redondances pour traiter les fonctions classées et maintenir ainsi une redondance en cas de défaillance unique cumulée avec la maintenance d'un équipement.

2.2. HYPOTHÈSES DE DIMENSIONNEMENT

2.2.1. Contrôle de la réactivité

- mesure continue du flux neutronique dans le cœur :
  plage de puissance linéique
  La plage de puissance linéique de l'instrumentation interne fixe du cœur est appropriée pour protéger le combustible de tout dommage.
  La plage de puissance linéique [] couvre tous les types de gestion du combustible dans des conditions normales de fonctionnement []jusqu'à l'arrêt automatique du réacteur par la fonction de protection « puissance linéique élevée ».
  La puissance linéique de 590 W/cm correspond à la valeur seuil maximale permettant d'éviter toute fusion au centre de la pastille de combustible dans des conditions PCC-2. Cette limite constitue la limite maximale de la plage de puissance linéique.
  temps de réponse
  Le temps de réponse de l'instrumentation interne fixe du cœur est approprié pour protéger le combustible de tout dommage.
  Le temps de réponse de l'instrumentation interne fixe du cœur se décompose en deux parties :

  - le temps de réponse du détecteur et du transmetteur[] ;
  - le temps de réponse du module de conditionnement et d'émission du signal vers le système RPR ou RGL[].

  Ainsi, le temps de réponse du détecteur et du conditionnement du signal analogique est compatible avec le temps de réponse total de la chaîne.
  précision
  La précision de l'instrumentation interne fixe du cœur est appropriée pour protéger le combustible de tout dommage.
  []

  []

2.2.2. Évacuation de la puissance résiduelle

L'instrumentation interne fixe du cœur ne contribue pas directement à l'évacuation de la puissance résiduelle.

2.2.3. Confinement des substances radioactives

L'instrumentation interne fixe du cœur ne contribue pas directement au confinement de substances radioactives.

2.2.4. Contributions indirectes aux fonctions de sûreté

- Distribution radiale de température dans le cœur :
  plage de température
  La plage de température de l'instrumentation interne fixe du cœur est appropriée pour contribuer à atteindre l'état d'arrêt sûr.
  []

  []

  temps de réponse
  Le temps de réponse de l'instrumentation interne fixe du cœur est approprié pour contribuer à atteindre l'état d'arrêt sûr.
  Le temps de réponse de l'instrumentation interne fixe du cœur se décompose en deux parties :

  - le temps de réponse du thermocouple immergé dans l'eau et du transmetteur[] ;
  - le temps de réponse du module de conditionnement et d'émission du signal vers le système RPR ou SAS[].

  précision
  La précision de l'instrumentation interne fixe du cœur est appropriée pour contribuer à atteindre l'état d'arrêt sûr.
  La précision des signaux de mesure de température dépend de la gamme.
  Les valeurs d'incertitude [] incluent l'ensemble du conditionnement, y compris le calcul de compensation de la jonction froide.

  []

2.3. AUTRES HYPOTHÈSES

Sans objet.

3. DESCRIPTION - FONCTIONNEMENT

3.1. DESCRIPTION

3.1.1. Description générale du système

Collectrons

L'instrumentation des détecteurs de flux neutronique autoalimentés comprend 72 détecteurs au cobalt répartis dans 12 doigts (sondes de mesure).

Le flux neutronique local est mesuré en continu par les détecteurs de flux neutronique autoalimentés (collectrons ou SPND). Pour cela, des ensembles de détection équipés de collectrons fixes sont répartis dans le cœur azimutalement et radialement dans des assemblages combustibles sélectionnés. Un doigt de détecteurs est équipé de six collectrons répartis axialement sur la hauteur du cœur d'un de ces assemblages combustibles. Des détecteurs (n,γ)(γ,e) avec émetteur cobalt sont utilisés.

Les équipements servant à transmettre les signaux émis par les collectrons sont séparés en différents groupes affectés aux divisions redondantes du bâtiment réacteur (BR). Les armoires d'instrumentation équipées des modules de conditionnement du signal sont installées dans chacune des quatre divisions. Le système comprend toute l'instrumentation de conditionnement et de transmission des signaux, électriquement isolés, au matériel de traitement. Un équipement destiné au test des détecteurs et des chaînes d'instrumentation de mesure est également installé dans l'armoire d'instrumentation.

A la sortie de l'armoire de conditionnement, les signaux sont acheminés vers le système RPR et le système RGL via des modules assurant l'isolement entre le système RPR et le système RGL et le découplage entre le conditionnement et le système RPR et entre le conditionnement et le système RGL.

Le flux neutronique maximal produit dans le cœur constitue le critère de conception de la plage de mesure des chaînes.

Thermocouples de sortie cœur

L'instrumentation fixe des thermocouples de sortie cœur est constituée de 36 thermocouples installés dans les 12 sondes de mesure (doigts de détecteurs) des 12 lances d'instrumentation comme indiqué sur la figure **FIG–7.5.2.2.2**.

Chaque doigt de détecteurs est équipé de trois thermocouples. Chaque sonde contient 2 thermocouples avec une gamme de mesure étroite et 1 thermocouple avec une gamme de mesure large.

La température à la sortie des assemblages combustibles est mesurée en continu par les thermocouples. Pour cela, des ensembles de détection (doigts) équipés de thermocouples fixes sont répartis dans le cœur azimutalement et radialement dans les assemblages combustibles sélectionnés. Les thermocouples sont installés[] à la hauteur de la tête de l'assemblage combustible correspondant. Des trous dans le tube de la sonde permettent au réfrigérant primaire de la région de la tête de l'assemblage combustible de circuler jusqu'aux thermocouples à l'intérieur du tube.

L'installation relative aux signaux des thermocouples est séparée en différents groupes qui sont affectés aux divisions redondantes du bâtiment réacteur. À partir des traversées, les signaux sont acheminés vers les divisions redondantes du bâtiment de sauvegarde où sont installées les armoires d'instrumentation qui sont équipées des modules de conditionnement des signaux. Le système comprend toute l'instrumentation servant au conditionnement des signaux afin qu'ils puissent être transmis aux équipements de traitement de manière électriquement isolée.

3.1.1.1. Systèmes en interface

Collectrons

Les signaux de mesure (en courant) provenant des collectrons sont transmis au système RPR (PS) et au système RGL (RCSL). Le signal provenant de chaque collectron est transmis deux fois au système RPR (une fois à chacune des deux unités d'acquisition à distance de chaque division) et une fois au système RGL.

Par ailleurs, des signaux sont transmis pour indiquer l'état de test.

Thermocouples de sortie cœur

Les signaux des thermocouples de sortie cœur de la gamme étroite (6 signaux par division) et de la gamme large (3 signaux par division) sont transmis au système de protection PS (système RPR) et au SAS. De plus, les signaux des thermocouples de sortie cœur de la gamme large des divisions 1 et 4 sont transmis au CCAG (système RPR).

3.1.2. Description des matériels principaux

L'instrumentation interne fixe du cœur est constituée des matériels principaux suivants :

3.1.2.1. Détecteurs et émetteurs

Collectrons

La plage de flux observée par les collectrons []couvre tous les types de gestion du combustible dans des conditions normales de fonctionnement[] jusqu'à l'arrêt automatique du réacteur par la fonction de protection « puissance linéique élevée ».

Compte tenu de leur principe de fonctionnement, les détecteurs utilisés sont des détecteurs à émission. Toutefois, ils sont généralement appelés *détecteurs autoalimentés* car, en fonctionnement, aucune tension de polarisation n'est nécessaire (contrairement, par exemple, aux chambres d'ionisation). Ils peuvent aussi être désignés sous l'appellation détecteurs (n, γ) (γ, e). Le signal de sortie du détecteur est compatible avec les appareils électroniques associés.

Le détecteur est moins sensible aux rayons γ qu'au flux neutronique tout en étant sensible au spectre de neutrons durs en cas de gestion de combustible MOX.

Le rayonnement γ généré dans le combustible nucléaire par les fissions nucléaires produit des électrons Compton dans l'émetteur, l'isolement et le collecteur du détecteur. Étant donné que ce rayonnement provient de n'importe quelle direction, il génère un courant négatif en fonction du matériau des électrodes.

Comme le détecteur, le câble du conducteur []est lui aussi soumis au même rayonnement γ. De ce fait, le conducteur de l'émetteur, utilisé pour la transmission du signal du détecteur situé dans la cuve, génère un courant sur toute la longueur du conducteur dans le cœur du réacteur. Cet effet est compensé par un deuxième conducteur (conducteur de compensation) qui n'a pas de contact avec le matériau de l'émetteur et qui chemine à côté du conducteur de l'émetteur dans les câbles[].

Une compensation du signal de bruit de fond généré par les produits d'activation dans le détecteur (par exemple, le signal de bruit de fond généré par le ^{60}Co pour le détecteur au cobalt) est possible. Le système permet une compensation du signal de bruit de fond.

Le matériau de l'émetteur est le cobalt, ce qui présente l'avantage suivant par rapport aux autres matériaux possibles : le signal des détecteurs au cobalt répond aux variations du flux neutronique sans retard (signaux prompts). Le niveau du signal retardé dépend du flux neutronique à la position de chaque collectron : il est déterminé par le bilan entre la croissance du Co-60 par la capture des neutrons thermiques dans l'émetteur et sa décroissance par la décomposition du Co-60 avec une demi-vie de 5,27 ans. Cette composante retardée représente la composante compensée décrite précédemment.

L'amplification du signal est réglée de manière à permettre l'alimentation efficace des fonctions de contrôle-commande.

La durée de vie d'un détecteur est principalement conditionnée par l'endurance de la résistance d'isolement entre les deux conducteurs intérieurs et la gaine du câble. []

Thermocouples de sortie cœur

Les thermocouples de sortie cœur sont qualifiés pour résister aux événements PCC-1-4 et RRC-A. Ils [] peuvent signaler aux opérateurs l'entrée en accident grave. Les thermocouples de sortie cœur [] peuvent résister à des transitoires rapides[].

[]

La durée de vie d'un thermocouple est déterminée par l'endurance de la résistance d'isolement entre les deux conducteurs internes et la gaine des câbles.

Les sondes de détection sont remplaçables et sont fixées sur les bâtis (*yokes*) d'instrumentation sur lesquels sont également montées les sondes du système de mesure à billes à propulsion pneumatique (Aeroball Measuring System [AMS]). Chaque doigt plonge dans un tube guide de grappe de contrôle de l'assemblage combustible.

3.1.2.2. Lances d'instrumentation

Un doigt de détecteurs avec 6 collectrons et les 3 thermocouples associés est conçu pour être monté sur une lance d'instrumentation qui reçoit également les doigts de sondes AMS (voir section 7.5.2.1). Les sondes sont montées sur un support, le bâti de lance. Pour leur protection mécanique, les sondes de mesure, aussi appelées doigts, sont logées dans des tubes-gaines dont le diamètre extérieur est dimensionné pour entrer dans les tubes guides libres des grappes de contrôle des assemblages combustibles. Pendant le fonctionnement du réacteur, le bâti de lance repose sur la plaque supérieure de la structure interne de cœur, le doigt de lance étant inséré dans un tube guide libre de grappe de contrôle.

Dans la cuve, un câble [] est relié à chaque thermocouple. Le signal des collectrons et celui des thermocouples est acheminé par un câble [] jusqu'à un joint d'étanchéité et passe par la barrière de pression jusqu'à la tête de lance. Là, il est relié à un connecteur qui permet à la ligne de connexion du système d'instrumentation de rechange (ECI) d'être connectée aux 6 collectrons et aux 3 thermocouples de sortie cœur provenant du doigt d'instrumentation. La ligne du système d'instrumentation de rechange (ECI) est un ensemble de câbles [] qui sont résistants aux APRP. Ce système de câbles connecte la lance d'instrumentation à l'armoire de conditionnement en trois étapes : de la tête de lance au panneau de raccordement via les équipements du couvercle de cuve, du panneau de raccordement à la traversée de l'enceinte et de la traversée de l'enceinte à l'armoire de conditionnement.

Quant aux traversées du couvercle de cuve, elles sont multi pôles. Chacune d'elle comporte 9 tubes de câbles pour les 6 collectrons et les 3 thermocouples d'un doigt. Les manchons des câbles [] sont insérés dans ces tubes et soudés. Les gaines de câble de tous les collectrons et thermocouples sont donc connectées électriquement au couvercle de cuve par des assemblages brasés, soudés et boulonnés. Le couvercle de cuve doit donc être choisi comme une mise à la terre potentielle des circuits électroniques.

En cas de défaillance d'un collectron ou d'un thermocouple de sortie cœur, tout le doigt de détecteurs avec les 6 collectrons et les 3 thermocouples doit être remplacé. La conception de la lance permet de remplacer le doigt de détecteurs ainsi que les câbles [] et les connecteurs associés (instrumentation remplaçable).

3.1.3. Description des dispositions d'installations principales

Collectrons

Le nombre maximal de collectrons par doigt est compatible avec le diamètre du tube guide [] d'un assemblage combustible de 17 x 17, le nombre de détecteurs est donc limité à 6 par doigt.

La figure FIG–7.5.2.2.3 indique les emplacements radiaux sélectionnés, la répartition des collectrons dans les divisions du système RPR et la numérotation des collectrons utilisée pour la conception des fonctions de contrôle-commande.

Le tableau TAB–7.5.2.2.1 donne la position axiale des collectrons.

Ce choix répond aux hypothèses de dimensionnement (§ 2.2.) et aux autres hypothèses (§ 2.3.) précisées ci-dessus et aux contraintes mécaniques associées.

Les dimensions des détecteurs (longueur et diamètre) sont compatibles avec le diamètre interne du tube guide et son rayon de courbure.

Le diamètre des détecteurs est suffisamment petit pour être compatible avec l'espace interne prévu pour au moins 6 détecteurs et les câbles associés. La hauteur des détecteurs est inférieure à l'espace entre deux grilles consécutives et suffisamment longue pour réduire le rapport bruit/signal.

Les signaux des collectrons sont représentatifs des paramètres clés du cœur pour un vaste éventail de conditions du cœur (PCC-1, PCC-2, quelques PCC-3 et PCC-4 et certaines études spécifiques) et

pour un large ensemble de gestions du combustible, les collectrons sont répartis de la manière la plus homogène possible.

Le nombre d'assemblages combustibles instrumentés est limité à 12.

Les assemblages combustibles suivants sont exclus :

- les assemblages combustibles périphériques,
- les assemblages combustibles avec des grappes de contrôle (raisons mécaniques),
- les assemblages situés à des emplacements où des facteurs de pic (FQ et FΔH) sont moins susceptibles de se produire dans des conditions normales de fonctionnement (déterminés par calcul).

implantation radiale et axiale :

- Le choix d'implantation permet une mesure de la distribution de la puissance dans des situations symétriques et asymétriques. Pour satisfaire aux exigences fonctionnelles ci-dessus, le cœur est divisé en six zones adjacentes. Une zone correspondant à une tranche axiale du cœur. La limite d'une zone coupe le cœur soit à mi-distance entre deux collectrons successifs, soit en haut ou en bas de la hauteur active du cœur.
- La distribution radiale et azimutale est telle qu'une zone représentative de toute la zone du cœur est couverte par les collectrons (même s'il n'y a pas de collectron au milieu du cœur - voir ci-dessous).
- Les collectrons sont répartis dans les régions supérieures et inférieures afin de détecter le pic de puissance linéique. Ceci est important pour obtenir une distribution axiale précise dans la plupart des conditions normales de fonctionnement où la régulation du cœur fait en sorte de garder la distribution de puissance aussi plate et homogène que possible.
- A haut niveau de puissance et avec toutes les grappes de contrôle extraites, les calculs théoriques de la distribution axiale du flux neutronique montrent que la plupart des distributions axiales résultent de la superposition d'un mode fondamental et d'une première harmonique. Cela signifie que les distances spatiales minimales des maxima et minima dans la distribution axiale du flux sont beaucoup plus grandes que la distance axiale de deux collectrons voisins. (Il n'est donc pas nécessaire d'avoir un détecteur au centre du cœur à des fins de reconstitution).
- Les emplacements axiaux se trouvent toujours entre deux grilles de mélange pour éviter la dépression du flux et l'augmentation γ à proximité des grilles de mélange.
- Outre le pic de puissance linéique, les signaux issus des collectrons sont utilisés pour les calculs du RFTC. Pour cette application, il est nécessaire d'avoir une distribution précise du flux non seulement pour la puissance locale mais aussi pour la puissance intégrée le long du canal chaud.
- Trois collectrons sont placés dans la moitié supérieure du cœur et les trois autres dans la moitié inférieure du cœur pour détecter le pic de puissance linéique dans les moitiés inférieure et supérieure afin de couvrir toutes les distributions de puissance possibles (normales et accidentelles).

Thermocouples de sortie cœur

Les thermocouples de sortie du cœur et les doigts des collectrons dans lesquels ils sont installés sont distribués radialement au-dessus du cœur.

Trois thermocouples sont installés dans chacun des 12 doigts ce qui fait un total de 36 thermocouples. La figure **FIG–7.5.2.2.2** donne l'emplacement axial des thermocouples de sortie cœur.

Les thermocouples sont installés dans les doigts de collectrons de telle sorte qu'ils fournissent la température du fluide quittant le cœur.

L'affectation des thermocouples aux divisions est indiquée sur la figure **FIG–7.5.2.2.1**.

3.2. FONCTIONNEMENT

3.2.1. Fonctionnement en régime normal de la tranche

En régime normal de la tranche au-dessus de 10% Pn, l'instrumentation interne fixe du cœur est en service continu.

3.2.2. Fonctionnement en régime permanent du système

Collectrons

En régime permanent du système, les collectrons mesurent en continu le flux neutronique à des positions données dans le cœur.

Thermocouples de sortie cœur

En régime permanent du système, le système de mesure des thermocouples de sortie cœur indique la température du fluide à la sortie du cœur lorsque le fluide environnant est de l'eau, un mélange diphasique ou de la vapeur d'eau surchauffée. La compensation de la soudure froide prend en compte le cas où la température mesurée fournie par les thermocouples est inférieure à la mesure de la soudure froide, situation pouvant se produire lors d'un arrêt pour rechargement.

3.2.3. Fonctionnement en régime transitoire

Sans objet.

3.2.4. Autres régimes de fonctionnement du système

3.2.4.1. Défaillance de la totalité ou d'une partie du système

Collectrons

Le remplacement d'un collectron défectueux n'étant pas possible pendant le fonctionnement du réacteur, un traitement automatique de validation a été développé pour prendre en compte les configurations dégradées. Le traitement automatique permet de gérer 5 décalages de seuils, en tenant compte du nombre et de la localisation des collectrons défectueux.

Toutes les chaînes d'instrumentation des collectrons peuvent être vérifiées par des générateurs de tests intégrés. Des interrupteurs verrouillables permettent de s'assurer que les tests ne peuvent être effectués que dans une seule chaîne collectron à la fois. Chaque division contient deux générateurs de tests. Les deux générateurs de tests fournissent sur demande les signaux sélectionnables suivants en parallèle aux chaînes d'instrumentation :

- courants (intensités appropriées sélectionnables) dans la branche émettrice des chaînes d'instrumentation,
- courants (intensités appropriées sélectionnables) dans la branche de compensation des chaînes d'instrumentation.

Thermocouples de sortie cœur

Des configurations de fonctionnement dédiées sont mises en œuvre par le système RPR en cas de défaillance partielle ou totale du système de mesure des thermocouples de sortie cœur.

Tous les réglages et toutes les valeurs électriques internes importantes des modules peuvent être vérifiés au moyen d'un appareil de diagnostic. En outre, des signaux simulés peuvent être générés dans le transducteur à la place des signaux des thermocouples.

4. ANALYSE DE SÛRETÉ

4.1. CONFORMITÉ A LA RÉGLEMENTATION

L'instrumentation interne fixe du cœur est conforme à la réglementation générale en vigueur (voir le sous-chapitre 1.7) et ne fait pas l'objet de dérogations particulières.

4.2. RESPECT DES CRITÈRES FONCTIONNELS

4.2.1. Contrôle de la réactivité

Les études de transitoires incidentels/accidentels des sous-chapitres 15.2 et 19.3 faisant intervenir les fonctions de l'instrumentation interne fixe du cœur correspondant aux critères fonctionnels énoncés au § 0.2.1. sont réalisées en considérant, pour les paramètres suivants, des valeurs cohérentes avec les hypothèses de dimensionnement énoncées au § 2.2. (cf. sous-chapitre 15.1) :

- plage de puissance linéique,
- temps de réponse,
- précision.

Pour chaque transitoire concerné, ces études :

- présentent les effets de ces fonctions sur le déroulement du transitoire,
- montrent que le dimensionnement de ces fonctions est tel qu'il contribue au respect de leurs critères d'acceptabilité.

4.2.2. Evacuation de la puissance résiduelle

L'instrumentation interne fixe du cœur ne contribue pas directement à l'évacuation de la puissance résiduelle.

4.2.3. Confinement des substances radioactives

L'instrumentation interne fixe du cœur ne contribue pas directement au confinement des substances radioactives.

4.2.4. Contributions indirectes à l'accomplissement des fonctions de sûreté

Les études de transitoires incidentels/accidentels des sous-chapitres 15.2, 19.1, 19.2 et 19.3 faisant intervenir les fonctions de l'instrumentation interne fixe du cœur correspondant aux critères fonctionnels énoncés au § 0.2.4. sont réalisées en considérant, pour les paramètres suivants, des valeurs cohérentes avec les hypothèses de dimensionnement énoncées au § 2.2. :

- plage de température,
- temps de réponse,
- précision.

Pour chaque transitoire concerné, ces études :

- présentent les effets de ces fonctions sur le déroulement du transitoire,
- montrent que le dimensionnement de ces fonctions est tel qu'il contribue au respect de leurs critères d'acceptabilité.

4.3. CONFORMITÉ AUX EXIGENCES DE CONCEPTION

L'instrumentation interne fixe du cœur est conforme aux exigences de conception évoquées au § 0.3., notamment pour ce qui concerne :

4.3.1. Exigences issues du classement de sûreté

4.3.1.1. Classement de sûreté

Les classements des équipements de l'instrumentation interne fixe du cœur jouant un rôle vis-à-vis de la sûreté sont présentés dans la section 3.2.2.

4.3.1.2. Critère de défaillance unique (active et passive)

Défaillance unique active

La conception de l'instrumentation interne fixe du cœur est conforme à l'exigence de robustesse au critère de défaillance unique active énoncée au **§ 0.3.**, notamment sur les points suivants :

- Le câblage des détecteurs vers les bâtiments électriques est réalisé en utilisant des chemins de câbles redondants.
- Les chaînes d'équipements de contrôle-commande classés E1 sont redondantes.
- Dans chaque division, les équipements de contrôle-commande classés E1A et E1B sont alimentés par deux lignes d'alimentation de courant continu de 24V qui sont électriquement isolées. Cette alimentation est de type « sans coupure ». Des convertisseurs courant alternatif / courant continu redondants qui sont branchés sur ces lignes d'alimentation fournissent aux équipements de contrôle-commande la tension appropriée.

Défaillance unique passive

Sans objet.

4.3.1.3. Alimentation électrique de secours

La conception de l'instrumentation interne fixe du cœur est conforme à l'exigence de secours électrique énoncée au **§ 0.3.**, notamment sur les points suivants :

- En cas de Perte Totale des Alimentations Electriques Externes (MDTE), les armoires électriques sont secourues par les groupes diesels principaux.
- Les armoires électriques des COT sont secourues par des batteries [].
- Les modules de conditionnement des COT gamme large des divisions 1 et 4 se trouvent dans les armoires électriques PIPS AG qui sont secourues par des diesels et des batteries AG.

4.3.1.4. Séparation physique/géographique

La conception de l'instrumentation interne fixe du cœur est conforme à l'exigence de séparation physique/géographique, notamment sur les points suivants :

- Chaque chaîne redondante d'équipements de contrôle-commande classés E1 est installée dans une division séparée physiquement.
- La protection des équipements de contrôle-commande classés E1A et E1B est obtenue grâce à la protection physique des divisions 2 et 3 et grâce à la séparation géographique des divisions 1 et 4 des bâtiments de sauvegarde.

4.3.1.5. Qualification aux conditions accidentelles

Les équipements de l'instrumentation interne fixe du cœur relevant d'une qualification aux conditions accidentelles, sont présentés dans la section 3.7.1.1.2.

4.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

La conformité des classements mécanique, électrique, contrôle-commande et sismique des équipements de l'instrumentation interne fixe du cœur jouant un rôle vis-à-vis de la sûreté aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

La conformité du classement ESPN des équipements de l'instrumentation interne fixe du cœur aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

4.3.2. Exigences réglementaires

4.3.2.1. Textes réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.1.1. Textes officiels

La conformité aux textes officiels spécifiquement applicables au système, listées au **§ 0.3.2.**, est présentée aux **§ 1.** et **§ 3.**.

4.3.2.1.2. Prescription techniques

La conformité de l'instrumentation interne fixe du cœur aux décisions n°2012-D C-0283 du 26 juin 2012 et n°2014-DC-0403 du 21 janvier 2014 est démontrée dans le chapitre 21.

4.3.2.1.3. Réglementations internationales

Sans objet.

4.3.2.2. Textes para-réglementaires

La conformité aux textes para-réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.2.1. Règles fondamentales de sûreté

Sans objet.

4.3.2.2.2. Directives techniques

La conformité aux directives techniques spécifiquement applicables au système, listées au **§ 0.3.2.**, est présentée aux **§ 4.3.1.**, **§ 4.3.3.** et **§ 4.4.4.** (G3).

4.3.2.3. Textes EPR spécifiques

Sans objet.

4.3.3. Agressions

4.3.3.1. Agressions internes

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

4.3.3.2. Agressions externes

La démonstration de la robustesse de l'installation aux agressions externes relève du sous-chapitre 3.3.

4.3.4. Diversification

Sans objet.

4.3.5. Radioprotection

De façon générale, les dispositions de conception de l'installation prises pour limiter l'exposition du personnel au rayonnement et à la contamination due aux produits de fission et de corrosion activés relèvent du chapitre 12.

Lors des opérations de rechargement ou après 10 ans d'exploitation des lances, des dispositions sont à prévoir, notamment :

- Les lances doivent être manipulées sous eau.
- La station d'échange utilisée pour remplacer un doigt de détecteurs ou réparer une lance doit avoir un blindage en plomb pour protéger le personnel.

4.3.6. Fonctionnement, maintenance et accessibilité à long terme

Sans objet.

4.3.7. Système tel que réalisé

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

4.4.1. Essais de démarrage

L'instrumentation interne fixe du cœur fait l'objet d'un programme d'essais de démarrage conformément aux modalités présentées au chapitre 14, permettant notamment de vérifier le respect des critères suivants (cf § 2.2. pour les grandeurs numériques qui seront vérifiées) :

- plage de puissance linéique,
- plage de température,
- précision de la mesure.

Nota : Le temps de réponse de chaque chaîne de mesure est vérifié hors site sur une plateforme d'essai et la précision de la température est vérifiée par une procédure de qualification.

De plus, au titre du chapitre X des Règles Générales d'Exploitation, des calibrages sont réalisés comme suit :

Collectrons

Du fait de l'évolution de la distribution de puissance en cours de cycle, la perte de sensibilité des détecteurs due à la combustion de l'émetteur et à l'accroissement du signal de bruit de fond causé par la décroissance ß du Co 60, il est nécessaire de procéder à des calibrages périodiques des mesures de puissance linéique (W/cm) qui sont dérivées des chaînes d'instrumentation.

Le calibrage des mesures de puissance linéique est effectué à des périodes fixes à l'aide de l'outil de calibrage du contrôle-commande du cœur s'appuyant sur les données du système de mesure à billes à propulsion pneumatique (AMS). Le système AMS fait l'objet d'une description dans la section 7.5.2.1 du rapport de sûreté.

Le calibrage des mesures de puissance linéique est effectué par l'ajustement de facteurs de calibrage qui convertissent les signaux issus des collectrons (un courant mesuré en nA) en puissances linéiques exprimées en W/cm. Cette conversion est effectuée au sein du système RPR et du système RGL. Ainsi, le résultat des mesures effectuées à partir du système AMS est utilisé pour ajuster en conséquence les facteurs de calibrage dans le système RPR et le système RGL, mais ne permet pas de changer les paramètres des chaînes d'instrumentation internes du cœur.

Remarque : les paramètres correspondants sont mis à jour dans les équipements de traitement des systèmes RPR et RGL.

Thermocouples de sortie cœur

Les chaînes de mesure ne font pas l'objet d'un calibrage.

4.4.2. Surveillance en exploitation

Les fonctions suivantes de l'instrumentation interne fixe du cœur sont sollicitées en exploitation normale de la tranche dans des conditions représentatives des conditions de fonctionnement incidentelles, accidentelles ou d'agression dans lesquelles elles sont requises :

- fournir une mesure continue du flux neutronique à des positions données dans le cœur ;
- fournir la distribution radiale de température dans le cœur.

La surveillance de la disponibilité de ces fonctions est donc réalisée dans ce cadre.

Généralités

Vérifications : la surveillance de l'alimentation électrique des modules électroniques et la surveillance de l'insertion des modules génèrent des alarmes en cas de défaillances.

Les fonctions d'auto-surveillance des modules génèrent des alarmes lorsque des défaillances se produisent. Les fonctions de surveillance en question sont les suivantes :

- surveillance de l'insertion des modules,
- surveillance de l'alimentation électrique,
- surveillance des signaux dans les équipements de traitement des signaux (respect des valeurs limite fixées),
- ouverture des portes,
- rupture de fil, court-circuit du capteur ou défaillance du transducteur.

Collectrons

Les équipements de test suivants sont disponibles en face avant des modules de conditionnement du signal :

- indicateurs montrant les conditions de fonctionnement,
- connecteurs de diagnostic pour le branchement d'un dispositif de diagnostic. Toutes les valeurs électriques internes importantes des modules peuvent être vérifiées à l'aide du dispositif de diagnostic,
- alarme de l'armoire générale.

Toutes les alarmes sont disponibles pour les systèmes RPR et RGL.

La température des équipements à l'intérieur des armoires de conditionnement des signaux générés par les collectrons et les thermocouples de sortie cœur est limitée à des valeurs acceptables pour éviter tout dysfonctionnement des équipements et tout vieillissement prématuré. Le refroidissement des armoires est réalisé par convection et conduction naturelle.

Thermocouples de sortie cœur

Les équipements de test suivants sont disponibles au niveau des armoires des transducteurs de température :

- indicateur montrant les conditions de fonctionnement,
- prise de test pour mesurer le signal de sortie des transducteurs,
- connecteur de diagnostic pour le branchement d'un dispositif de diagnostic. Grâce à ce dispositif, tous les réglages et valeurs électriques internes importants des modules peuvent être vérifiés. De plus, des signaux simulés peuvent être générés dans le transducteur à la place des signaux des thermocouples,
- alarme générale des armoires.

La température des équipements à l'intérieur des armoires de conditionnement des signaux générés par les collectrons et les thermocouples de sortie cœur est limitée à des valeurs acceptables pour éviter tout dysfonctionnement des équipements et tout vieillissement prématuré. Le refroidissement des armoires s'effectue par convection et conduction naturelle.

4.4.3. Essais périodiques

Les parties classées de l'instrumentation interne fixe du cœur font l'objet d'essais périodiques conformément au chapitre IX des Règles Générales d'Exploitation.

Collectrons

Des essais périodiques sont effectués à chaque cycle pour vérifier le bon fonctionnement des chaînes d'instrumentation :

- bon fonctionnement de l'électronique de conditionnement des collectrons,
- bonne transmission aux systèmesRPR et RGL des signaux de mesure des collectrons.

Thermocouples de sortie cœur

Des essais périodiques sont effectués à chaque cycle pour vérifier le bon fonctionnement des chaînes d'instrumentation :

- bon fonctionnement de l'électronique de conditionnement COT,
- bon fonctionnement de la transmission des signaux COT aux systèmesRPR et SAS/PAS.

De plus, au titre du chapitre X des Règles Générales d'Exploitation, des calibrages périodiques sont réalisés comme expliqué au § 4.4.1..

4.4.4. Maintenance

L'instrumentation interne fixe du cœur fait l'objet d'un programme de maintenance conformément au chapitre VIII des RGE.

La maintenance corrective (au niveau électronique) des modules électroniques de conditionnement des signaux issus des collectrons et des thermocouples de sortie cœur peut être effectuée pendant le fonctionnement de la centrale. Il est possible d'extraire et d'insérer un module lorsqu'il est sous tension, notamment sans éteindre le module, les autres modules ou l'armoire et sans endommager le module. L'insertion ou l'extraction d'un module ne nécessite pas la déconnexion ou la connexion d'un fil ou d'un câble.

Collectrons

Pour des raisons de disponibilité de la tranche, le remplacement d'un collectron indisponible nécessitant l'ouverture de la cuve n'est pas prévu au cours du cycle du combustible.

Lors de chaque arrêt normal de la tranche pour rechargement, les chaînes de mesure sont vérifiées de la même manière que lors de la mise en service. Ces tests comprennent :

- la mesure des résistances d'isolement,
- la mesure des signaux de bruit de fond dus à la décroissance ß du Co 60. Les valeurs mesurées servent de valeurs de base pour la correction du signal du Co 60,
- la vérification des modules électroniques à l'aide de générateurs de test (possible également pendant le fonctionnement de la centrale).

Lors du test des chaînes d'instrumentation, la transmission des signaux aux différents utilisateurs peut être vérifiée en même temps et la réponse des appareils de surveillance des valeurs limites peut être testée.

Thermocouples de sortie cœur

La maintenance est contraignante en ce qui concerne la disponibilité de la tranche ; elle sera donc effectuée autant que possible lors d'un arrêt programmé.

Lors de chaque arrêt normal de la tranche pour rechargement, les chaînes d'instrumentation sont vérifiées de la même manière que lors de la mise en service. Ces tests comprennent :

- la vérification des signaux de mesure par comparaison des mesures redondantes,
- la vérification des modules électroniques en cas de valeur lue anormale,
- la mesure des résistances d'isolement,
- la mesure des résistances de boucle.

Lors du test des chaînes d'instrumentation, la transmission des signaux aux différents utilisateurs peut être vérifiée en même temps.

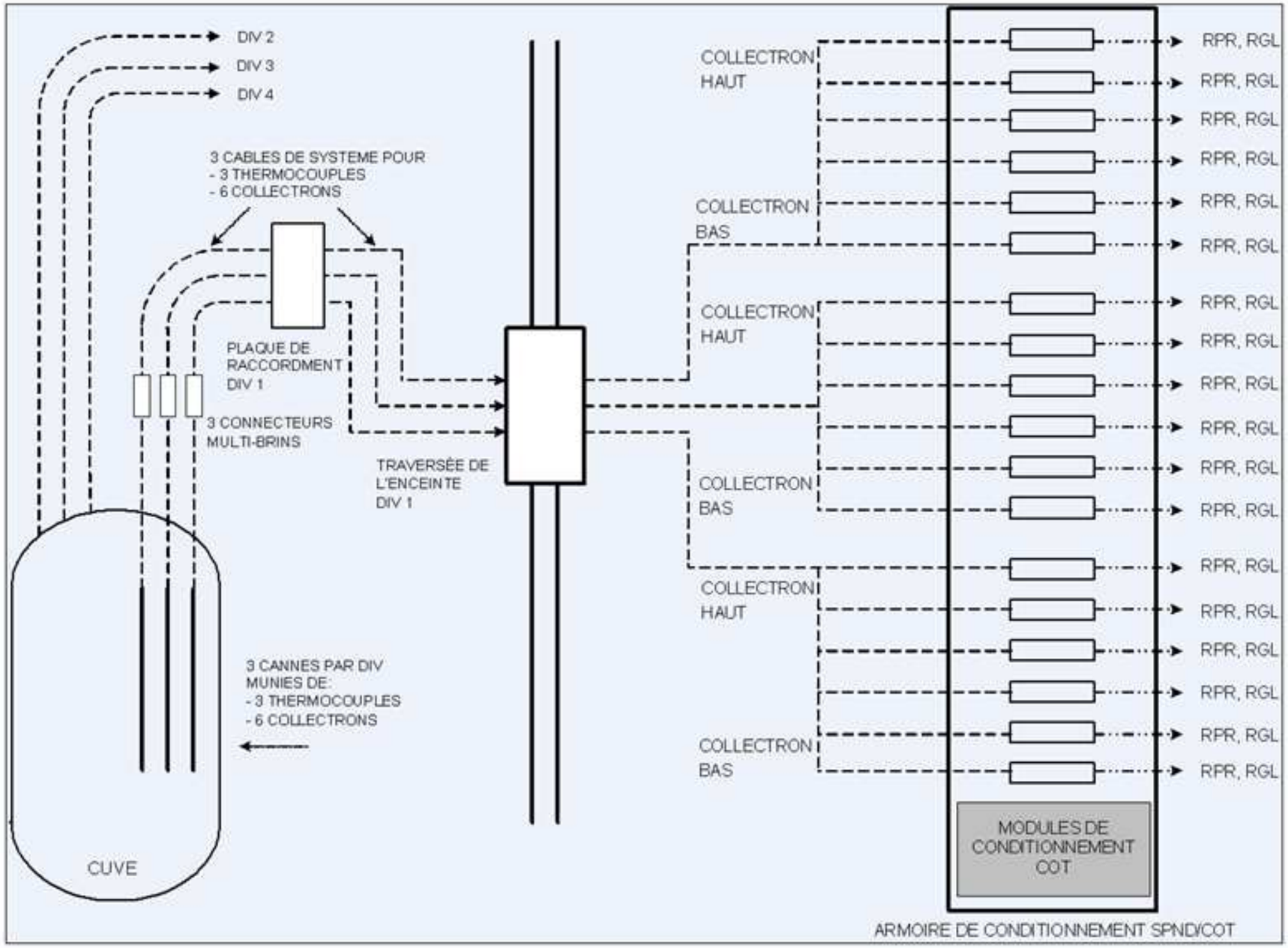
5. SCHÉMA DE PRINCIPE

Le schéma de principe de l'instrumentation interne fixe du cœur est présenté en figure **FIG–7.5.2.2.1**.

TAB–7.5.2.2.1 POSITION AXIALE DES COLLECTRONS

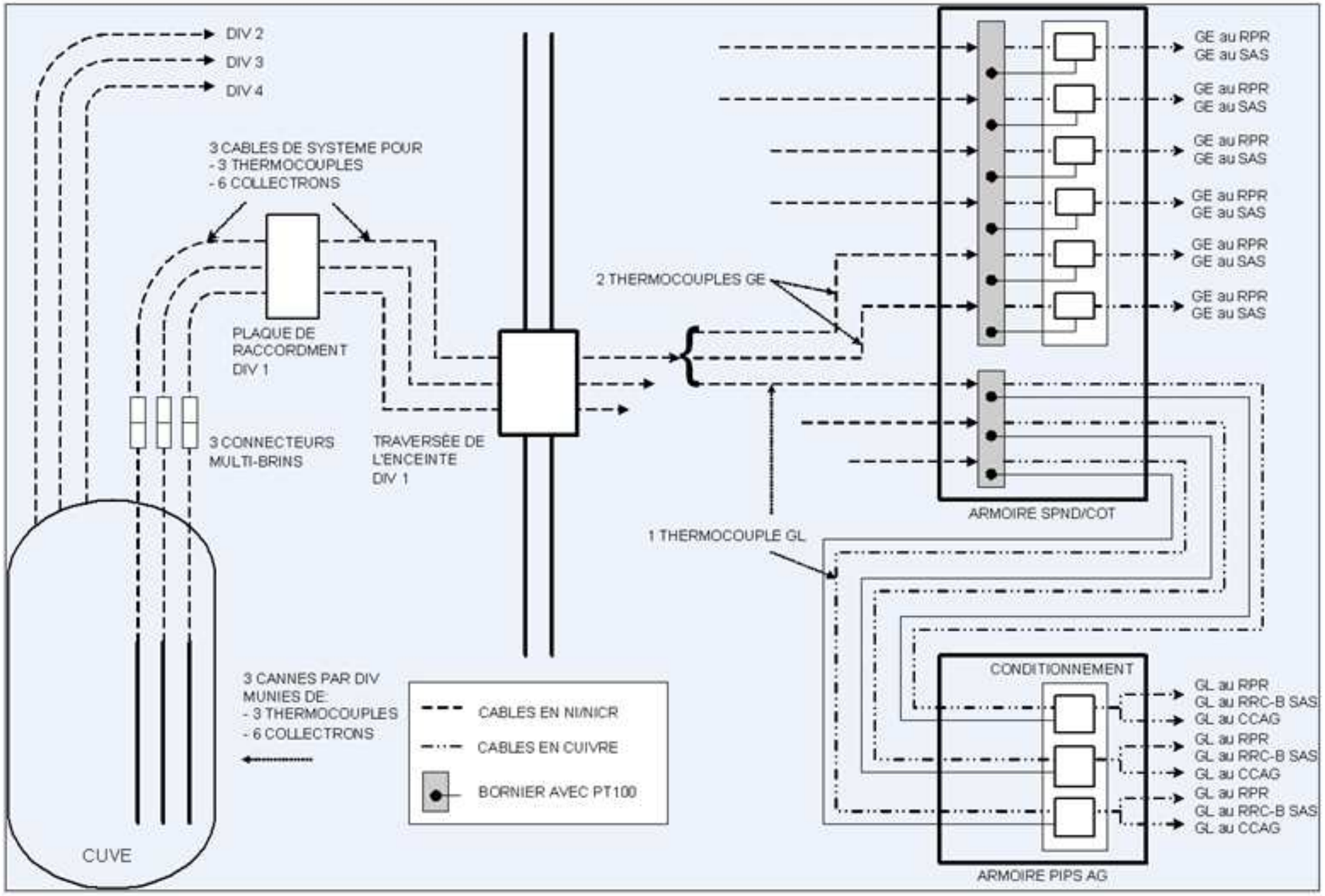
FIG–7.5.2.2.1 SCHÉMA DE PRINCIPE DU SYSTÈME D'INSTRUMENTATION INTERNE FIXE DU CŒUR

SPND



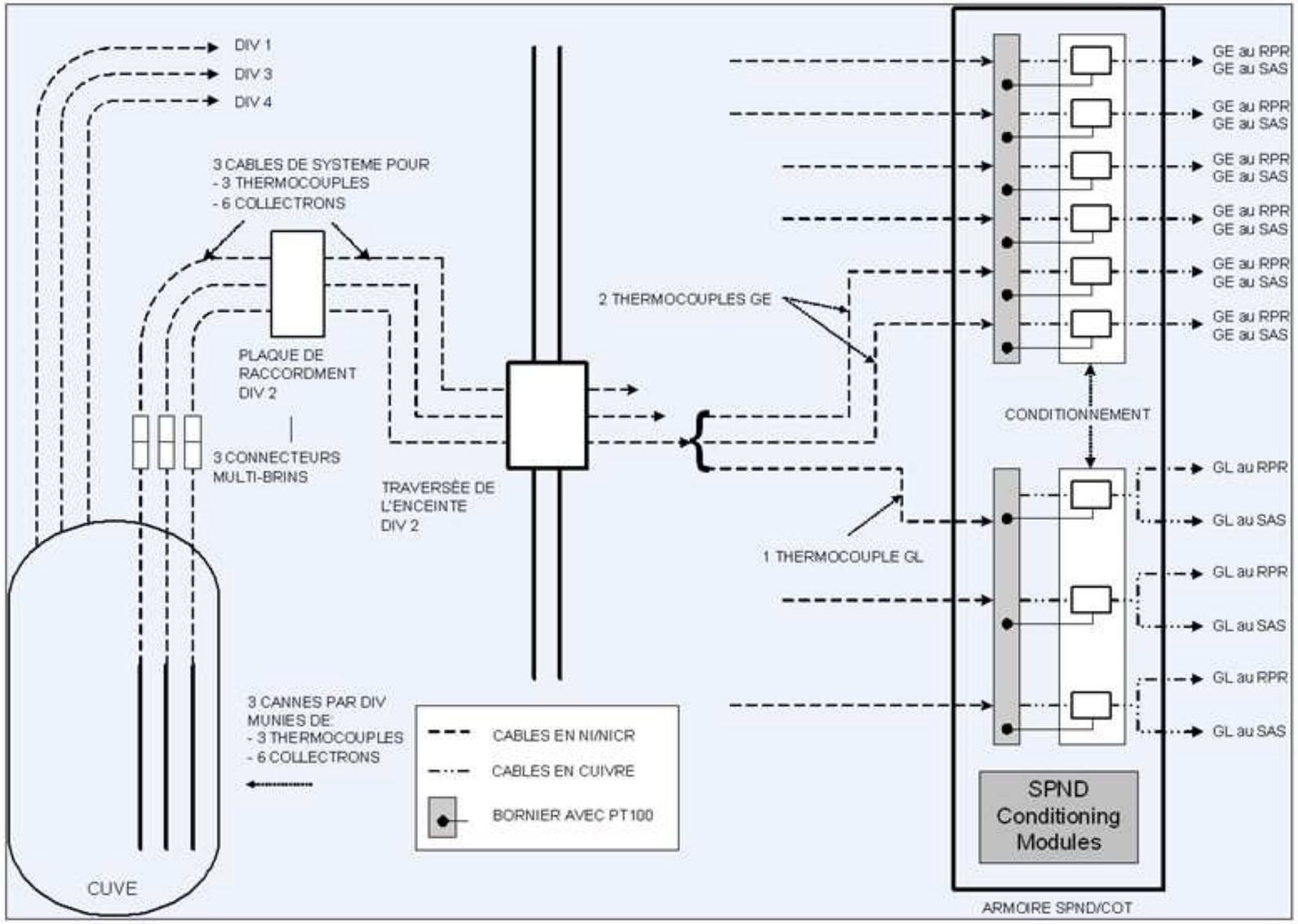
COT – DIVISIONS 1 ET 4

La figure ci-dessous représente la division 1.
La même disposition s'applique pour la division 4.



COT – DIVISIONS 2 ET 3

La figure ci-dessous représente la division 2.
La même disposition s'applique pour la division 3.



FIG–7.5.2.2.2 EMPLACEMENT DES THERMOCOUPLES DE SORTIE CŒUR

FIG–7.5.2.2.3 EMPLACEMENT RADIAL ET AXIAL DES COLLECTRONS

SOMMAIRE

FIGURES :

.7.5.3 INSTRUMENTATION EXTERNE DU CŒUR (RPN)

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

0.1.1. Contrôle de la réactivité

Les contributions du système au contrôle de la réactivité doivent être les suivantes :

- fournir des mesures permanentes du flux neutronique quel que soit le niveau de puissance du réacteur, dans certaines situations incidentelles ou accidentelles de catégorie PCC-2, PCC-3, PCC-4 ou RRC-A,
- élaborer le signal diversifié de « puissance nucléaire > Max1 » qui déclenche un arrêt automatique du réacteur en situation RRC-A d'ATWS par perte du système RPR et augmentation excessive du débit vapeur.

0.1.2. Évacuation de la puissance résiduelle

Le système RPN ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.1.3. Confinement des substances radioactives

Le système RPN ne contribue pas directement au confinement de substances radioactives.

0.1.4. Contributions indirectes aux fonctions de sûreté

Sans objet.

0.1.5. Contributions spécifiques à la protection contre les agressions

Le système RPN ne contribue pas spécifiquement à la protection contre les agressions.

0.1.6. Contributions à l'élimination pratique

Le système RPN ne contribue pas directement à l'élimination pratique.

0.2. CRITÈRES FONCTIONNELS

Au titre de ses contributions à l'accomplissement des fonctions de sûreté, le système doit satisfaire les critères fonctionnels suivants :

0.2.1. Contrôle de la réactivité

- mesures du flux neutronique :
  Le système RPN doit fournir, dans la plage de flux attendue de fonctionnement, dans les temps de réponse et de précisions requises, des mesures du flux neutronique, différentes du bruit de fond, dans l'ensemble des PCC et RRC-A afin de respecter les critères d'acceptabilité de ces études (cf. sous–chapitre 15.1 et section 19.1.1).

- ordre d'arrêt automatique du réacteur :
  Le système RPN partie SAS doit élaborer le signal diversifié de «puissance nucléaire > Max1» qui déclenche un arrêt automatique du réacteur en situation RRC-A d'ATWS par la perte du système RPR et l'augmentation excessive du débit vapeur, afin de respecter les critères d'acceptabilité de cette étude (cf. section 19.1.1).

0.2.2. Évacuation de la puissance résiduelle

Le système RPN ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.2.3. Confinement des substances radioactives

Le système RPN ne contribue pas directement au confinement de substances radioactives.

0.2.4. Contributions indirectes aux fonctions de sûreté

Sans objet.

0.3. EXIGENCES RELATIVES A LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Les parties du système RPN jouant un rôle vis-à-vis de la sûreté doivent faire l'objet d'un classement de sûreté conformément aux règles de classement indiquées à la section 3.2.1.

0.3.1.2. Critère de Défaillance Unique (active et passive)

Les fonctions du système RPN classées F1 doivent être robustes à l'application du critère de défaillance unique.

0.3.1.3. Alimentation électrique de secours

L'alimentation électrique des composants du système RPN nécessaire à l'accomplissement des fonctions classées F1 doit être secourue par les groupes diesels principaux.

0.3.1.4. Séparation physique / géographique

Les fonctions classées F1 du système RPN doivent être conçues conformément à l'exigence de séparation physique/géographique de leurs équipements redondants constitutifs :

- séparation physique et électrique des chaînes de mesure redondantes (fonction F1A).

0.3.1.5. Qualification aux conditions accidentelles

Les équipements classés du système RPN doivent être qualifiés en fonction des conditions de fonctionnement danslesquelles ils sont sollicités au titre de leur contribution à l'accomplissement des fonctions de sûreté, conformément aux règles du sous-chapitre 3.7.

0.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

Les équipements du système RPN redevables d'un classement mécanique, électrique, contrôle-commande et sismique doivent être classés conformément aux règles de classement présentées dans la section 3.2.1.

Le système RPN n'est pas concerné par le classement ESPN car le système n'est pas soumis à la pression.

0.3.2. Exigences réglementaires

0.3.2.1. Textes réglementaires

0.3.2.1.1. Textes officiels

Le système RPN est concerné spécifiquement par les textes officiels suivants :

- Décret 2007-534 du 10 avril 2007 autorisant la création de l'installation nucléaire de base dénommée Flamanville 3 :
  - Art. 2 – Section III-1.1.1. b : « Dès lors que le combustible nécessaire au fonctionnement normal du réacteur est chargé dans la cuve, la réaction nucléaire est surveillée en permanence. Les moyens de mesure en place permettent d'effectuer cette surveillance au-delà de la puissance thermique de dimensionnement du réacteur. »
  - Art. 2 – Section III-1.1.1.c : « Ces moyens de mesure et l'intensité des sources de comptage associées sont choisis et maintenus à un niveau de performances tel que l'exploitant n'ait jamais à faire démarrer la circulation de l'eau du circuit primaire principal ni à entreprendre la diminution de la concentration de cette eau en absorbant neutronique soluble sans disposer d'une mesure significative du flux neutronique. »
  - Art. 2 – Section III-1.1.1.d : « Le suivi de la distribution de puissance dans le cœur est assuré par différents systèmes de mesure neutronique répartis dans et en dehors du cœur. »

0.3.2.1.2. Prescriptions techniques

Le système RPN n'est pas concerné par une prescription technique spécifique.

0.3.2.1.3. Réglementations internationales

Le système RPN n'est pas concerné par une réglementation internationale spécifique.

0.3.2.2. Textes para-réglementaires

0.3.2.2.1. Règles fondamentales de sûreté

Le système RPN est concerné par la Règle Fondamentale de Sûreté suivante :

- RFS IV.2. b : « exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté ».

0.3.2.2.2. Directives techniques

Le système RPN est concerné par les sections suivantes des Directives Techniques (voir section 1.7.0) :

- section A.2.2 - redondance et diversification dans les systèmes de sûreté,
- section B.1.1 - le suivi de la distribution de puissance dans le cœur peut être assuré par une instrumentation neutronique fixe dans le cœur, un système de mesure mobile (« aéroball ») et une instrumentation neutronique à l'extérieur du cœur.
- section B.2.1 - classement des fonctions, barrières, structures et systèmes de sûreté,
- section G3 - conception du contrôle-commande.
  Cette section précise les exigences relatives à l'instrumentation et au contrôle-commande.
  Les exigences applicables à l'instrumentation concernent :
  - le classement fonctionnel de l'instrumentation,
  - la prise en compte du critère de défaillance unique, de la maintenance et de la séparation physique,
  - la prise en compte des conséquences des agressions internes et externes sur le contrôle-commande.

0.3.2.3. Textes EPR spécifiques

Le système RPN n'est pas concerné par un texte spécifique EPR.

0.3.3. Agressions

0.3.3.1. Agressions internes

Les fonctions du système RPN doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Les fonctions du système RPN doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3.4. Diversification

Le système ne fait pas l'objet d'une exigence de diversification.

0.3.5. Radioprotection

Le système RPN n'est pas concerné par une exigence de radioprotection.

0.3.6. Exigences liées au fonctionnement, à la maintenance et à l'accessibilité long terme

Le système RPN n'est pas concerné par une exigence liée au fonctionnement, à la maintenance et à l'accessibilité long terme dans la gestion long terme après accident.

0.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

0.4.1. Essais de démarrage

Le système RPN doit être conçu pour permettre la réalisation d'essais de démarrage permettant de s'assurer de sa conception adéquate et de ses performances, et notamment du respect des critères fonctionnels qui lui sont assignés au § 0.2.

0.4.2. Surveillance en exploitation

Le système RPN doit être conçu pour permettre une surveillance en exploitation normale des caractéristiques du système nécessaires à l'accomplissement de ses missions de sûreté afin d'assurer le bon comportement de ses composants et leur disponibilité en fonctionnement normal, incidentel et accidentel.

0.4.3. Essais périodiques

Les parties classées du système RPN doivent être conçues pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

0.4.4. Maintenance

Le système RPN doit être conçu pour permettre la mise en œuvre d'un programme de maintenance conformément au chapitre VIII des RGE.

1. RÔLE DU SYSTÈME

Le système RPN assure les fonctions opérationnelles suivantes dans les différentes conditions de fonctionnement de l'installation dans lesquelles il est sollicité :

1.1. RÔLE DU SYSTÈME PENDANT L'EXPLOITATION NORMALE DE LA TRANCHE

Le système RPN fournit quel que soit le niveau de puissance du réacteur, des signaux destinés aux fonctions de régulation, de contrôle, de surveillance, de limitation du cœur et d'affichage du cœur transmis par le système RPR dans la Salle de Commande principale (SdC, c'est-à-dire MCP+MCS) et sur le panneau de repli.

Pour cela, le système est conçu avec trois niveaux de mesure afin de couvrir la plage complète de flux neutronique : les niveaux source, intermédiaire et puissance.

Le système RPN fournit des signaux pour la surveillance des équipements internes de la cuve.

Le système RPN fournit aussi des signaux au dispositif d'analyse et de mesure de la réactivité (RMAD) pour les essais physiques du cœur.

1.2. RÔLE DU SYSTÈME DANS LES CONDITIONS DE FONCTIONNEMENT PCC–2 À PCC–4, RRC-A,EN ACCIDENT GRAVE ET SITUATIONS AGRESSIONS

Le système RPN fournit dans les conditions de fonctionnement PCC2 à PCC4 et en situation RRC-A, des signaux destinés aux fonctions de protection du cœur et aux fonctions de surveillance post-accidentelle.

Le système RPN partie SAS élabore le signal diversifié de « puissance nucléaire > Max1 » qui déclenche un arrêt automatique du réacteur en situation RRC-A d'ATWS par la perte du système RPR et l'augmentation excessive du débit vapeur, afin de limiter les conséquences d'une crise d'ébullition.

2. BASES DE CONCEPTION

2.1. HYPOTHÈSES GÉNÉRALES DE FONCTIONNEMENT

Les critères de dimensionnement du système RPN sont principalement les suivants :

- disponibilité des fonctions classées de sûreté lors d'une défaillance ou lors des opérations de maintenance,
- disponibilité du signal diversifié d'arrêt automatique du réacteur par « puissance nucléaire > Max1 » en cas de défaillance du système RPR,
- critère de défaut de mode commun au moment du basculement d'une chaîne de mesure vers une autre chaîne de mesure,
- mise à disposition d'une mesure précise du flux neutronique depuis l'arrêt à froid jusqu'à 120% de la puissance nominale, en fonctionnement normal et en situation dégradée.

Pour répondre à ces critères, le système RPN est dimensionné comme suit :

- indépendance électrique entre les quatre redondances (3 pour la chaîne de mesure de niveau source (CNS)) pour traiter les fonctions classées et maintenir ainsi une redondance en cas de défaillance unique cumulée avec la maintenance d'un équipement,
- indépendance entre le signal diversifié d'arrêt automatique du réacteur par « puissance nucléaire > Max1 » et le système RPR,
- trois chaînes de mesure neutroniques (Source, Intermédiaire et Puissance) pour permettre une mesure précise à tous les niveaux de puissance du réacteur ainsi qu'une redondance fonctionnelle prenant en compte le défaut de mode commun au moment du basculement d'une chaîne de mesure vers une autre chaîne de mesure par le recouvrement des gammes entre les trois chaînes de mesure,
- En situation incidentelle ou accidentelle, l'objectif de la conduite est de ramener la chaudière en état d'arrêt à froid, le réacteur étant maintenu sous-critique. Pour ce faire, l'opérateur dispose des informations à base des signaux des chaînes de mesures neutroniques.

Pour que cette mesure conserve une signification tout au long de l'accident malgré un taux de vide dans le cœur ou une chute de (N - 1) grappes (configuration dissymétrique) sur arrêt automatique du réacteur, il est nécessaire d'assurer :

- un recouvrement des échelles de mesure entre le niveau « INTERMÉDIAIRE » et le niveau « PUISSANCE »,
- un dimensionnement des chaînes intermédiaires pour fonctionner en situation dégradée (chaînes utilisées en conduite post-accidentelle) et ce, durant [] (voir § 0.3.1.5.).

2.2. HYPOTHÈSES DE DIMENSIONNEMENT

2.2.1. Contrôle de la réactivité

Mesures permanentes du flux neutronique

Chaînes de niveau source (CNS)

Taux de comptage minimal

Un taux de comptage minimal égal à 1 c/s est requis pour distinguer ce dernier du bruit de fond.

Plage de flux

Les CNS fournissent une mesure du flux neutronique à l'arrêt (depuis les conditions sous-critiques (dès le chargement du combustible)) et durant la phase initiale de démarrage (jusqu'aux conditions de niveau de flux faible critique de la « plage d'impulsions »)[].

Une discrimination électronique des impulsions des rayons γ est effectuée.

Chaînes de niveau intermédiaire (CNI)

Plage de flux

Les CNI fournissent une mesure du flux neutronique au démarrage et lors de la montée en puissance (environ 5 x 10^{-6} % PN à au moins 60 % PN, voir toute section traitant de PCC pour atteinte de l'état d'arrêt sûr).

Compensation de courant

Le détecteur est compensé ou est insensible aux rayons γ.

[]

Temps de réponse

Le temps de réponse des CNI est approprié pour l'activation de l'arrêt automatique du réacteur.

[]

Précision

La précision des CNI est appropriée pour l'activation de l'arrêt automatique du réacteur.

[]

Chaînes de niveau puissance (CNP)

Plage de flux

Les CNP fournissent une mesure du flux neutronique lors de la montée de puissance et en puissance (niveaux de puissance allant de 0,5 % PN jusqu'à 120 % PN, voir sections 15.2.2m, 15.2.4e, 15.2.3f et 19.1.3Fsb.6).

Temps de réponse

Le temps de réponse des CNP est approprié pour l'activation de l'arrêt automatique du réacteur.

[]

Précision

La précision des CNP est appropriée pour l'activation de l'arrêt automatique du réacteur.

[]

Recouvrement entre les trois chaines de mesures

Les recouvrements des gammes des trois niveaux de chaînes (CNS, CNI et CNP) assurent la continuité de la protection et du contrôle du réacteur de l'arrêt jusqu'à la pleine puissance.

Ordre d'arrêt automatique du réacteur

Chaînes de niveau puissance (CNP)

Temps de réponse

Le temps de réponse du conditionnement et du traitement par le système RPN partie SAS est approprié pour l'activation de l'arrêt automatique du réacteur.

[]

Précision

La précision des CNP est appropriée pour l'activation de l'arrêt automatique du réacteur.

[]

Seuil de fonction de sûreté

La valeur du seuil de fonction de sûreté élaboré par le système RPN partie SAS, est appropriée pour l'activation de l'arrêt automatique du réacteur.

[]

2.2.2. Évacuation de la puissance résiduelle

Le système RPN ne contribue pas directement à l'évacuation de la puissance résiduelle.

2.2.3. Confinement des substances radioactives

Le système RPN ne contribue pas directement au confinement de substances radioactives.

2.2.4. Contributions indirectes aux fonctions de sûreté

Sans objet.

2.3. AUTRES HYPOTHÈSES

Le système RPN contribue à la mise en service du système RBS en cas de détection d'un taux de comptage CNS élevé. Cette contribution est réalisée uniquement au titre de la défense en profondeur et n'est donc pas valorisée dans les études d'accident.

3. DESCRIPTION - FONCTIONNEMENT

3.1. DESCRIPTION

3.1.1. Description générale du système

Les mesures des trois niveaux de flux (source, intermédiaire et puissance) sont réalisées à partir de :

- 3 chaînes composées chacune d'1 détecteur et d'1 chaîne de conditionnement pour le niveau source,
- 4 chaînes composées chacune d'1 détecteur et d'1 chaîne de conditionnement pour le niveau intermédiaire,
- 4 chaînes composées chacune de 2 détecteurs (1 détecteur en section basse et un détecteur en section haute par chaîne) et d'1 chaîne de conditionnement pour le niveau puissance. L'étendue totale de flux neutronique à acquérir est d'environ 10 à 11 décades jusqu'à environ 120% de la puissance nominale du réacteur.

Les signaux des détecteurs et les alimentations haute tension des détecteurs sont transmis par des câbles blindés reliant les boîtiers de distribution installés dans les boîtiers de connexion des traversées de l'enceinte de confinement et affectées aux détecteurs en fonction des exigences de séparation par division.

A l'extérieur de l'enceinte de confinement, les câbles sont connectés aux armoires d'instrumentation qui leur sont affectées dans les 4 divisions des bâtiments de sauvegarde.

Les signaux sont transmis aux fonctions de contrôle-commande chargées de leur exploitation ultérieure.

3.1.2. Description des matériels principaux

Le système RPN est constitué des matériels principaux suivants :

3.1.2.1. Détecteurs

Chaînes de niveau source (CNS)

Détecteurs de niveau source

Des tubes compteurs proportionnels à dépôt de bore sont utilisés comme détecteurs de niveau source. Dans un compteur à dépôt de bore, une fine couche de ^{10}B est déposée sur la surface intérieure de la cathode cylindrique. Ces tubes compteurs détectent les neutrons thermiques (exactement comme les chambres d'ionisation à dépôt de bore) à l'aide de la réaction nucléaire ^{10}B (n, α) → ^{7}Li. Les noyaux de ^{7}Li et les particules α qui sont générés ionisent le gaz du tube compteur et produisent des impulsions de charge. []

Outre les impulsions produites par les neutrons, les impulsions produites par le rayonnement gamma ainsi que par le bruit génèrent un signal de bruit de fond. Néanmoins, les impulsions des neutrons étant d'amplitude considérablement plus élevées, le bruit de fond est discriminé.

La sensibilité est suffisante pour couvrir toute la plage de flux prévue. []

Le temps de réponse des CNS est approprié pour l'activation de l'alarme et la mise en service du système RBS.

[]

La précision des CNS est appropriée pour l'activation de l'alarme et la mise en service du système RBS.

[]

Chaîne audio

Un signal audio est disponible dans la Salle de Commande principale (SdC) et un deuxième dans le bâtiment réacteur (BR)) pour informer les opérateurs d'une excursion de réactivité.

Chaînes de niveau intermédiaire (CNI)

Le rayonnement gamma retardé, qui n'est pas proportionnel à la puissance du réacteur, contribue de manière non négligeable au signal de mesure dans la gamme des flux neutroniques faibles. Des chambres d'ionisation à dépôt de bore avec compensation gamma sont donc utilisées comme détecteurs de niveau intermédiaire. La réaction nucléaire générant le signal de sortie des chambres est la même que pour les tubes compteurs à dépôt de bore.

La sensibilité est suffisante pour couvrir toute la plage de flux prévue.

[]

Chaînes de niveau puissance (CNP)

Les détecteurs de niveau puissance sont des chambres d'ionisation à dépôt de bore non compensées. Une compensation gamma n'est pas nécessaire, car le courant d'ionisation produit par le rayonnement gamma peut être négligé lors du fonctionnement en puissance par rapport au courant produit par le flux neutronique. Les deux chambres de chaque position de mesure azimutale du niveau puissance sont installées dans les chaînes de conteneurs de telle manière qu'il en résulte une affectation de la chambre inférieure à la moitié inférieure du cœur et de la chambre supérieure à la moitié supérieure du cœur. Les courants des chambres sont envoyés individuellement aux armoires de conditionnement.

La sensibilité est suffisante pour couvrir toute la plage de flux prévue.

[]

Réactimètre (RMAD)

L'exécution des essais physiques à puissance nulle après chaque rechargement requiert un RMAD dont le but principal est de calculer la valeur de la réactivité en se basant sur un signal représentant le niveau de flux neutronique.

Ce dernier équipement n'étant pas un système en ligne, il n'y a aucune exigence de classement spécifique.

Le signal utilisé pour représenter le niveau de flux neutronique est le signal fourni par une CNP, car ce type de détecteur est supposé être plus représentatif de la valeur moyenne axiale sur toute la hauteur du combustible que le détecteur de niveau intermédiaire se trouvant dans le plan médian du cœur.

Étant donné que le niveau de flux neutronique à l'endroit où sont effectuées les mesures de réactivité est très faible, le signal de sortie du détecteur ne peut pas être amplifié à l'aide du module de conditionnement normal.

Ce signal devant être amplifié par la carte de conditionnement interne du RMAD, ce dernier est donc directement connecté au détecteur avant l'entrée du module d'amplification.

Les CNI sont équipées de ce dispositif de connexion temporaire pour pallier à des besoins particuliers pendant les essais physiques.

Pour éviter toute difficulté due à un détecteur indisponible, les 4 CNP et les 4 CNI sont équipées de ce dispositif de connexion temporaire.

3.1.2.2. Structure mécanique du système

Les détecteurs de neutrons (tubes compteurs et chambres d'ionisation) sont montés dans des chaînes de conteneurs mobiles suspendues à des câbles en acier et sont descendus dans des tubes guides jusqu'à leurs positions de mesure.

Les extrémités supérieures de ces tubes guides aboutissent dans des boîtiers de raccordement accessibles de la salle au-dessus des plaques de blindage de la paroi du puits de cuve. []

Les tubes guides sont fermés à l'extrémité supérieure par le couvercle du boîtier de raccordement et à l'extrémité inférieure par des brides. A la hauteur du plan médian du cœur, les tubes guides des détecteurs niveau intermédiaire et niveau puissance sont entourés d'un blindage en plomb destiné à réduire l'impact du rayonnement γ sur les signaux de mesure des détecteurs niveau intermédiaire. La figure **FIG–7.5.3.1** montre le nombre de tubes guides, leur implantation [] et les détecteurs qui les équipent.

Les câbles de connexion de chaque détecteur sont amenés aux panneaux de raccordement se trouvant dans les boîtiers de raccordement. Ces câbles vont des panneaux de raccordement aux armoires de conditionnement en passant par les traversées étanches de l'enceinte menant aux armoires de conditionnement.

Les chaînes de mesure du système RPN sont affectées aux divisions redondantes des bâtiments de sauvegarde. Ceci est notamment valable pour les parcours de câbles, les traversées dans les parois de l'enceinte et l'hébergement des modules de conditionnement des signaux dans les divisions des bâtiments de sauvegarde. Les modules électroniques de l'instrumentation neutronique externe du cœur sont installés dans leurs propres armoires d'instrumentation, les armoires redondantes étant montées dans les différentes divisions.

Chaînes de conteneurs et emplacement des détecteurs

Chaque chaîne de conteneurs est constituée d'un ensemble de conteneurs individuels connectés les uns aux autres par des joints universels. Les chaînes de conteneurs peuvent donc facilement être installées et déplacées dans les tubes guides.

Chaînes de conteneurs du niveau source (CNS)

Chacune des trois CNS comporte un conteneur équipé d'un tube compteur à dépôt de bore. Le tube compteur se trouve dans le plan médian de la moitié inférieure de la zone active du cœur. La chaîne de conteneurs est fixée dans le tube guide à l'aide d'un câble. Pendant le fonctionnement, la position du détecteur reste inchangée.

Chaînes de conteneurs du niveau puissance (CNP) et du niveau intermédiaire (CNI)

Chacune des quatre chaînes de conteneurs comprend les deux chambres d'ionisation d'une CNP et la chambre d'ionisation avec compensation gamma d'une CNI. La chambre de niveau intermédiaire se trouve dans le plan médian de la zone active du cœur. Une chambre de niveau puissance est installée dans le plan médian de la moitié supérieure de la zone active du cœur et l'autre chambre est installée dans le plan médian de la moitié inférieure de la zone active du cœur.

3.1.2.3. Systèmes de contrôle commande en interface

Les CNS, CNI et CNP étant des systèmes d'instrumentation, les interfaces avec les autres systèmes sont des signaux (électriques).

Systèmes serveurs du système RPN

- système RPR pour les CNS.

Systèmes servis par le système RPN

- système RPR pour les CNS, CNI et CNP,
- système RCSL pour les CNP,
- chaîne audio pour les CNS,
- système KIR pour les CNP,
- système KDO pour les CNP,
- système RMAD pour les CNI et CNP.

3.1.3. Description des dispositions d'installations principales

Les CNS, CNI et CNP se trouvent dans le bâtiment réacteur (BR). Elles sont placées dans leurs tubes guides, dans le béton entourant la cuve.

Chaînes de niveau source (CNS)

Les CNS sont placées dans un endroit où elles peuvent recevoir la densité de flux maximale.

Pour ce faire, l'épaisseur de béton devant le détecteur est réduite. Pour s'assurer que les CNS puissent recevoir le maximum de densité de flux, la concentration en bore dans le béton est réduite tant que possible.

[]

Emplacement axial

Étant donné que des sources primaires peuvent être utilisées, la position axiale optimale des CNS est le plan médian de la moitié inférieure du cœur, devant la section du cœur où se trouvent les sources de neutrons.

Emplacement radial

Les CNS sont positionnées []de manière à obtenir le meilleur compromis entre la distance par rapport au cœur et les contraintes d'implantation.

Chaînes de niveau intermédiaire (CNI)

Les CNI sont placées à un endroit où elles sont le moins sensibles à la distribution axiale du flux, c'est-à-dire près du plan médian axial du cœur, pour éviter une modification de la réponse du détecteur avec des variations de déséquilibre axial, en particulier avec des oscillations de Xénon et lors de conditions accidentelles.

Le détecteur est protégé par un blindage de plomb pour réduire l'influence du flux gamma.

Chaînes de niveau puissance (CNP)

Les CNP sont placées à un endroit où leur efficacité est maximale compte tenu des contraintes d'installation et des contraintes mécaniques. Des détecteurs à deux sections axiales sont retenus. Les

sections supérieures et inférieures sont positionnées axialement à une hauteur qui correspond respectivement au centre des moitiés supérieure et inférieure du cœur (les moitiés du cœur se rapportent à la hauteur active du cœur (colonne de pastilles de combustible)).

3.2. FONCTIONNEMENT

3.2.1. Fonctionnement en régime normal de la tranche

En régime normal de la tranche, le système RPN est en service continu.

Au-delà d'un certain niveau de puissance du réacteur, les CNS sont coupées pour les protéger.

3.2.2. Fonctionnement en régime permanent du système

Les CNS fournissent des mesures permanentes du flux neutronique à l'arrêt et durant la phase initiale de démarrage[].

Les CNI fournissent des mesures permanentes du flux neutronique au démarrage et lors de la montée en puissance (de 5 x 10^{-6} % PN à au moins 60 % PN).

Les CNP fournissent des mesures permanentes du flux neutronique lors de la montée de puissance et en puissance (de 0,5 à 120 % PN).

Lorsque le système RPR est défaillant, le système RPN partie SAS élabore le signal diversifié de « puissance nucléaire > Max1 » qui déclenche un arrêt automatique du réacteur.

3.2.3. Fonctionnement en régime transitoire

Sans objet.

3.2.4. Autres régimes de fonctionnement du système

3.2.4.1. Fonctionnement dégradé du système

Défaillance de la totalité ou d'une partie du système

En règle générale, une défaillance totale ou partielle du système RPN a pour conséquence la perte d'une ou plusieurs mesures du flux à l'extérieur du cœur ; la perte simultanée de deux types de chaînes de mesure (ou plus) n'est pas envisagée.

Le signal diversifié de « puissance nucléaire > Max1 », élaboré par le système RPN partie SAS est traité en logique 2/4. En cas de défaillance d'une redondance, la logique de vote du système RPN partie SAS est automatiquement dégradée de manière à garantir la sûreté de la tranche.

Défaillance des systèmes en interface

Le système RPN n'est desservi que par les alimentations électriques. Les défaillances des alimentations ou d'une partie des alimentations électriques entraînent la perte consécutive d'une partie ou de la totalité du système RPN. Des actions spécifiques sont prévues pour assurer les fonctions de protection par le système RPR.

4. ANALYSE DE SÛRETÉ

4.1. CONFORMITÉ A LA RÉGLEMENTATION

Le système RPN est conforme à la réglementation générale en vigueur (voir le sous-chapitre 1.7) et ne fait pas l'objet de dérogations particulières.

4.2. RESPECT DES CRITÈRES FONCTIONNELS

4.2.1. Contrôle de la réactivité

Les études de transitoires incidentels/accidentels des sous-chapitres 15.2 et 19.1 faisant intervenir les fonctions du système RPN correspondant aux critères fonctionnels énoncés au § 0.2.1. sont réalisées en considérant, pour les paramètres suivants, des valeurs cohérentes avec les hypothèses de dimensionnement énoncées au § 2.2. (cf. sous-chapitre 15.1 et section 19.1.1) :

- plage de flux,
- recouvrement entre chaînes de mesure,
- temps de réponse,
- précision,
- seuil de fonction de sûreté (élaboré par le système RPN partie SAS),
- taux de comptage minimal pour les CNS.

Pour les transitoires concernés, ces études (cf. sous-chapitres 15.2 et 19.1) :

- présentent les effets de ces fonctions sur le déroulement des transitoires,
- montrent que le dimensionnement de ces fonctions est tel qu'il permet de contribuer au respect de leurs critères d'acceptabilité.

4.2.2. Evacuation de la puissance résiduelle

Sans objet

4.2.3. Confinement des substances radioactives

Sans objet

4.2.4. Contributions indirectes à l'accomplissement des fonctions de sûreté

Sans objet

4.3. CONFORMITÉ AUX EXIGENCES DE CONCEPTION

Le système RPN est conforme aux exigences de conception évoquées au § 0.3., notamment pour ce qui concerne :

4.3.1. Exigences issues du classement de sûreté

4.3.1.1. Classement de sûreté

Les classements des équipements du système RPN jouant un rôle vis-à-vis de la sûreté sont présentés dans la section 3.2.2.

4.3.1.2. Critère de défaillance unique (active et passive)

- défaillance unique active
  La conception du système RPN est conforme à l'exigence de robustesse au critère de défaillance unique active énoncée au § 0.3., notamment sur les points suivants :
  Le système RPN comporte :
  - 3 chaînes redondantes CNS comprenant chacune un détecteur, le système de conditionnement du signal et le matériel d'alimentation électrique,
  - 4 chaînes redondantes CNI comprenant chacune un détecteur, le système de conditionnement du signal et le matériel d'alimentation électrique,

- 4 chaînes redondantes CNP comprenant chacune deux détecteurs, le système de conditionnement du signal et le matériel d'alimentation électrique,
- 4 armoires électroniques redondantes d'alimentation électrique des détecteurs et de conditionnement des signaux.

Chaque redondance est installée dans une division redondante des bâtiments de sauvegarde, [].

- défaillance unique passive
  Sans objet.

4.3.1.3. Alimentation électriquede secours

Dans chaque division, l'alimentation électrique des équipements du contrôle-commande classé E1A est fournie par deux lignes 400V CA différentes (3 phases + neutre) provenant de tableaux de distribution différents. Cette alimentation est de type « sans coupure ». Des convertisseurs CA/CC redondants branchés à ces lignes d'alimentation fournissent aux équipements du contrôle-commande la tension appropriée. Les lignes d'alimentation en courant continu issues des convertisseurs sont isolées les unes des autres.

La conception du système RPN est conforme à l'exigence de secours électrique énoncée au **§ 0.3.**, notamment sur les points suivants :

- En cas de Perte Totale des Alimentations Electriques Externes (MDTE), les armoires électriques sont secourues par les diesels principaux et par des batteries [] permettant la continuité d'alimentation pendant les transitoires de basculement des sources externes ou internes.

4.3.1.4. Séparation physique/géographique

La conception du système RPN est conforme à l'exigence de séparation physique/géographique, notamment sur les points suivants :

- Chacune des redondances est séparée physiquement et électriquement depuis les détecteurs neutroniques situés dans le bâtiment réacteur (BR), jusqu'aux circuits électroniques de traitement des informations. Les 4 armoires électriques sont installées dans des bâtiments de sauvegarde distincts.

4.3.1.5. Qualification aux conditions accidentelles

Les équipements du système RPN relevant d'une quantification aux conditions accidentelles sont présentés dans la section 3.7.1.1.2.

4.3.1.6. Classement ESPN, mécanique, électrique, contrôle commande et sismique

La conformité des classements mécanique, électrique, contrôle-commande et sismique des équipements du système RPN jouant un rôle vis-à-vis de la sûreté aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

4.3.2. Exigences réglementaires

4.3.2.1. Textes réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.1.1. Textes officiels

La conformité aux textes officiels spécifiquement applicables au système, listées dans le **§ 0.3.2.**, est assurée par :

- la surveillance en permanence de la réaction nucléaire (cf. **§ 3.1.1.** et **§ 2.2.**),

- les opérations de maintenance réalisées afin de maintenir le niveau de performance (cf. § 4.4.4.). De plus, les RGE détaillent les exigences de disponibilités des chaînes (cf. chapitre VIII),
- le suivi de la distribution de puissance dans le cœur (cf. § 3.1. et § 3.2.).

4.3.2.1.2. Prescriptions techniques
Sans objet.

4.3.2.1.3. Réglementations internationales
Sans objet.

4.3.2.2. Textes para-réglementaires

La conformité aux textes para-réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.2.1. Règles fondamentales de sûreté
La justification du respect des exigences issues des Règles Fondamentales de Sûreté est présentée aux § 4.3. et § 4.4.(RFS IV.2.b).

4.3.2.2.2. Directives techniques
La conformité aux directives techniques spécifiquement applicables au système, listées dans le paragraphe 0.3.2, est assurée par :

- les § 2.1. et § 4.3.1.2. pour la directive A.2.2,
- le § 3.2.2. pour la directive B.1.1,
- les § 4.3.1.1. et § 4.3.1.6. pour la directive B.2.1,
- les § 4.3.1., § 2.1. et § 4.3.3. pour la directive G3.

4.3.2.3. Textes EPR spécifiques

Sans objet.

4.3.3. Agressions

4.3.3.1. Agressions internes

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

4.3.3.2. Agressions externes

La démonstration de la robustesse de l'installation aux agressions externes relève du sous-chapitre 3.3.

4.3.4. Diversification

Sans objet.

4.3.5. Radioprotection

Sans objet.

4.3.6. Fonctionnement, maintenance et accessibilité long terme

Sans objet.

4.3.7. Système tel que réalisé

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

4.4.1. Essais de démarrage

Le système RPN fait l'objet d'un programme d'essais de démarrage conformément aux modalités présentées au chapitre 14, permettant notamment de vérifier le respect des critères suivants :

- plage de flux,
- recouvrement entre chaînes de mesure,
- seuil de fonction de sûreté (élaboré par le système RPN partie SAS),
- taux de comptage minimal pour les CNS.

Il est à noter que la vérification du critère fonctionnel de plage de flux neutronique n'est pas possible de façon directe du fait qu'il n'existe pas d'instrumentation de référence neutronique qui permette de calibrer les chaînes du système RPN en flux neutronique. Ce critère est transformé en taux de comptage, courant ou puissance nucléaire (après calibrage par le bilan d'enthalpie) qui sont des critères testables.

Remarque : Le temps de réponse au niveau matériel est validé au cours des tests réalisés sur testbay. Sur site, il n'est pas possible de varier le flux neutronique d'une manière rapide pour solliciter la réponse de l'instrumentation.

Remarque : La précision au niveau matériel est validée au cours des tests réalisés sur testbay. Sur site, la précision des fonctions de sûreté est validée après calibrage dans le cadre des essais de physique du cœur.

4.4.2. Surveillance en exploitation

Le système RPN est sollicité en fonctionnement normal de la tranche, ce qui permet une surveillance fonctionnelle de ses caractéristiques sollicités dans ce cadre ; il s'agit notamment :

- d'une évaluation qualitative des valeurs de mesure des chaînes d'instrumentation et de leur comportement lors du fonctionnement en puissance. Les valeurs mesurées sont alors comparées à celles fournies par les chaînes redondantes.
- les équipements qui surveillent l'alimentation électrique des modules électroniques ainsi que l'alimentation haute tension des détecteurs et qui comparent les valeurs de mesure issues des positions de mesure redondantes génèrent des alarmes en réponse à toute défaillance et soutiennent ainsi ces vérifications.

4.4.3. Essais périodiques

Les parties classées du système RPN font l'objet d'essais périodiques conformément au chapitre IX des Règles Générales d'Exploitation, permettant notamment de vérifier le respect des critères suivants :

- bon fonctionnement de l'électronique du conditionnement des signaux de mesure du système RPN,
- bonne transmission des signaux de mesure du système RPN au système RPR,
- bonne transmission des signaux CNP aux systèmes RCSL et SAS/PAS.

4.4.4. Maintenance

Le système RPN fait l'objet d'un programme de maintenance conformément au chapitre VIII des RGE.

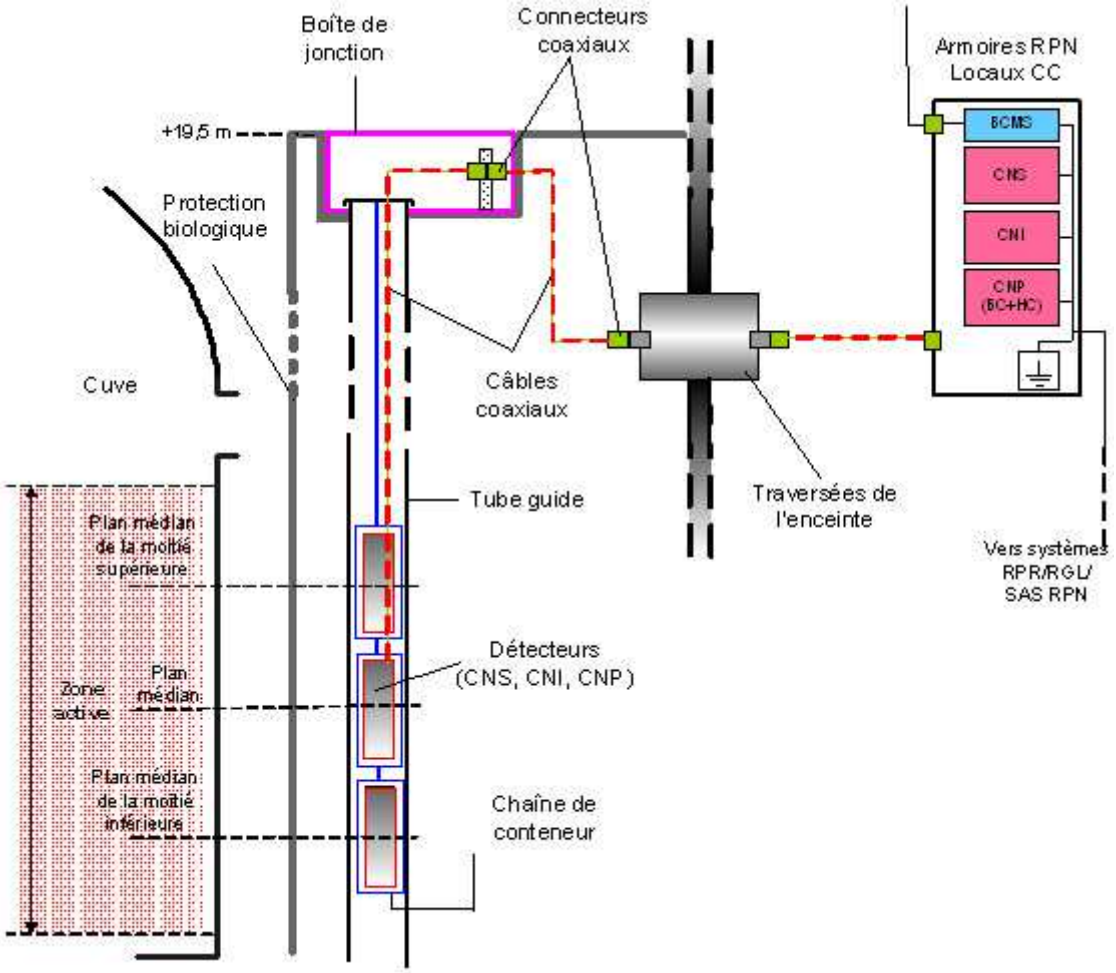
5. SCHÉMA DE PRINCIPE

Le schéma de principe du système RPN est présenté en figure FIG–7.5.3.2.

FIG–7.5.3.1 VUE D'ENSEMBLE DE L'EMPLACEMENT DES DÉTECTEURS []

[]

FIG–7.5.3.2 SCHÉMA DE PRINCIPE



SOMMAIRE

TABLEAUX :

FIGURES :

.7.5.4 MESURE DE LA POSITION DES GRAPPES

0. EXIGENCES DE SÛRETÉ

La conception mécanique de cette instrumentation relève de la section 5.3.2.

0.1. FONCTIONS DE SÛRETÉ

0.1.1. Contrôle de la réactivité

L'instrumentation de mesure de la position des grappes (RPI) ne contribue pas directement au contrôle de la réactivité.

0.1.2. Évacuation de la puissance résiduelle

L'instrumentation RPI ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.1.3. Confinement des substances radioactives

L'instrumentation RPI ne contribue pas directement au confinement des substances radioactives.

0.1.4. Contributions indirectes aux fonctions de sûreté

L'instrumentation RPI doit contribuer indirectement au contrôle de la réactivité :

- fournir la mesure de la position de chaque grappe dans les états standards A à C et dans les conditions de fonctionnement de catégorie PCC-2 à PCC-4 et RRC-A.

L'instrumentation RPI doit contribuer indirectement au confinement des substances radioactives :

- fournir la mesure de la position de chaque grappe dans les états standards A à C et dans certaines situations RCC-A, afin de maintenir l'intégrité de la seconde barrière en participant au signal d'arrêt des pompes primaires.

0.1.5. Contributions spécifiques à la protection contre les agressions

L'instrumentation RPI ne contribue pas spécifiquement à la protection contre les agressions.

0.1.6. Contributions à l'élimination pratique

L'instrumentation RPI ne contribue pas directement à l'élimination pratique.

0.2. CRITÈRES FONCTIONNELS

Au titre de ses contributions à l'accomplissement des fonctions de sûreté, l'instrumentation doit satisfaire les critères fonctionnels suivants :

0.2.1. Contrôle de la réactivité

L'instrumentation RPI ne contribue pas directement au contrôle de la réactivité.

0.2.2. Évacuation de la puissance résiduelle

L'instrumentation RPI ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.2.3. Confinement des substances radioactives

L'instrumentation RPI ne contribue pas directement au confinement des substances radioactives.

0.2.4. Contributions indirectes aux fonctions de sûreté

Au titre de sa contribution indirecte au contrôle de la réactivité, l'instrumentation RPI doit satisfaire les critères fonctionnels suivants :

- Mesure de la position des grappes : l'instrumentation RPI doit fournir, avec le temps de réponse et la précision requis, la mesure de la position des grappes lors d'évènements PCC-2 à PCC-4 et en situations RRC-A, afin de respecter les critères d'acceptabilité de ces études.

Au titre de sa contribution indirecte au confinement des substances radioactives, l'instrumentation RPI doit satisfaire les critères fonctionnels suivants :

- Mesure de la position des grappes : l'instrumentation RPI doit fournir, avec le temps de réponse et la précision requis, la mesure de la position des grappes en situations RRC-A, afin de respecter les critères d'acceptabilité de ces études.

0.3. EXIGENCES RELATIVES À LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Les parties de l'instrumentation RPI jouant un rôle vis-à-vis de la sûreté doivent faire l'objet d'un classement de sûreté conformément aux règles de classement indiquées à la section 3.2.1.

0.3.1.2. Critère de Défaillance Unique (active et passive)

Les fonctions de l'instrumentation RPI classées F1 doivent être robustes à l'application du critère de défaillance unique.

0.3.1.3. Alimentation électrique de secours

L'alimentation électrique des composants de l'instrumentation RPI nécessaire à l'accomplissement des fonctions classées F1 doit être secourue par les groupes diesels principaux.

0.3.1.4. Séparation physique / géographique

Les fonctions classées F1 de l'instrumentation RPI doivent être conçues conformément à l'exigence de séparation physique/géographique de leurs équipements redondants constitutifs :

- séparation physique et électrique des armoires de contrôle-commande redondantes (fonctions F1A).

0.3.1.5. Qualification aux conditions accidentelles

Les équipements classés de l'instrumentation RPI doivent être qualifiés en fonction des conditions de fonctionnement dans lesquelles ils sont sollicités au titre de leur contribution à l'accomplissement des fonctions de sûreté, conformément aux règles du sous-chapitre 3.7.

0.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

Les équipements de l'instrumentation RPI redevables d'un classement mécanique, électrique, contrôle-commande et sismique doivent être classés conformément aux règles de classement présentées dans la section 3.2.1.

L'instrumentation RPI n'est pas concernée par le classement ESPN car l'instrumentation n'est pas soumise à la pression.

0.3.2. Exigences réglementaires

0.3.2.1. Textes réglementaires

0.3.2.1.1. Textes officiels

L'instrumentation RPI n'est pas concernée spécifiquement par un texte officiel.

0.3.2.1.2. Prescriptions techniques

L'instrumentation RPI n'est pas concernée par une prescription technique spécifique.

0.3.2.1.3. Réglementations internationales

L'instrumentation RPI n'est pas concernée par une réglementation internationale spécifique.

0.3.2.2. Textes para-réglementaires

0.3.2.2.1. Règles fondamentales de sûreté

L'instrumentation RPI n'est pas concernée par une règle fondamentale de sûreté spécifique.

0.3.2.2.2. Directives techniques

L'instrumentation RPI est concernée par les sections suivantes des Directives Techniques :

- Section G3 – Conception du contrôle-commande.

Cette section précise les exigences relatives à l'instrumentation et au contrôle-commande.

Les exigences applicables à l'instrumentation concernent :

- le classement fonctionnel de l'instrumentation,
- la prise en compte du critère de défaillance unique, de la maintenance et de la séparation physique,
- la prise en compte des conséquences des agressions internes et externes sur le contrôle-commande.

0.3.2.3. Textes EPR spécifiques

L'instrumentation RPI n'est pas concernée par un texte spécifique EPR.

0.3.3. Agressions

0.3.3.1. Agressions internes

Les fonctions de l'instrumentation RPI doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Les fonctions de l'instrumentation RPI doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3.4. Diversification

L'instrumentation RPI ne fait pas l'objet d'une exigence de diversification.

0.3.5. Radioprotection

L'instrumentation RPI n'est pas concernée par une exigence de radioprotection.

0.3.6. Exigences liées au fonctionnement, à la maintenance et à l'accessibilité long terme

L'instrumentation RPI n'est pas concernée par une exigence liée au fonctionnement, à la maintenance et à l'accessibilité long terme dans la gestion long terme après accident.

0.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

0.4.1. Essais de démarrage

L'instrumentation RPI doit être conçue pour permettre la réalisation d'essais de démarrage permettant de s'assurer de sa conception adéquate et de ses performances, et notamment du respect des critères fonctionnels qui lui sont assignés au § 0.2..

0.4.2. Surveillance en exploitation

L'instrumentation RPI doit être conçue pour permettre une surveillance en exploitation normale des caractéristiques du système nécessaires à l'accomplissement de ses missions de sûreté afin d'assurer le bon comportement de ses composants et leur disponibilité en fonctionnement normal, incidentel et accidentel.

0.4.3. Essais périodiques

Les parties classées de l'instrumentation RPI doivent être conçues pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

0.4.4. Maintenance

L'instrumentation RPI doit être conçue pour permettre la mise en œuvre d'un programme de maintenance conformément au chapitre VIII des RGE.

1. RÔLE DU SYSTÈME

L'instrumentation RPI assure les fonctions opérationnelles suivantes dans les différentes conditions de fonctionnement de l'installation dans lesquelles elle est sollicitée :

1.1. RÔLE DU SYSTÈME PENDANT L'EXPLOITATION NORMALE DE LA TRANCHE

En fonctionnement normal de la tranche, l'instrumentation RPI mesure, conditionne et calcule la position des 89 grappes.

Le matériel de mesure du temps de chute des grappes (RDTME) utilise les mesures analogiques de position des grappes (signaux de mesure brute provenant des bobines d'indication de position) pour effectuer les essais périodiques de la « détermination du temps de chute des grappes ». Ceci est généralement fait lors du démarrage de la centrale.

1.2. RÔLE DU SYSTÈME DANS DES CONDITIONS DE FONCTIONNEMENT PCC2 À PCC4, RRC-A, EN ACCIDENT GRAVE ET SITUATIONS AGRESSIONS

Lors des évènements PCC-2 à PCC-4 et en situations RRC-A, l'instrumentation RPI mesure, conditionne et calcule la position des 89 grappes.

Le RDTME n'est utilisé pour aucune fonction de sûreté.

2. BASES DE CONCEPTION

2.1. HYPOTHÈSES GÉNÉRALES DE FONCTIONNEMENT

Le critère de dimensionnement de l'instrumentation RPI est principalement le suivant :

- disponibilité des fonctions classées de sûreté lors d'une défaillance ou lors des opérations de maintenance.

Pour répondre à ce critère, l'instrumentation RPI est dimensionnée comme suit :

- indépendance électrique entre les redondances pour traiter les fonctions classées et maintenir ainsi une redondance en cas de défaillance cumulée avec la maintenance d'un équipement.

Le RDTME n'est utilisé pour aucune fonction de sûreté mais est conçu pour ne pas impacter les fonctions de sûreté de l'instrumentation RPI en cas d'interférence électromagnétique ou de séisme.

2.2. HYPOTHÈSES DE DIMENSIONNEMENT

2.2.1. Contrôle de la réactivité

L'instrumentation RPI ne contribue pas directement au contrôle de la réactivité.

2.2.2. Évacuation de la puissance résiduelle

L'instrumentation RPI ne contribue pas directement à l'évacuation de la puissance résiduelle.

2.2.3. Confinement des substances radioactives

L'instrumentation RPI ne contribue pas directement au confinement des substances radioactives.

2.2.4. Contributions indirectes aux fonctions de sûreté

- mesure de la position des grappes :
  Les exigences fonctionnelles liées au cœur pour le système RPR spécifient le degré de précision des positions des grappes. Le temps de réponse est déterminé par les exigences fonctionnelles relatives à l'ATWS causé par le blocage mécanique des grappes et celles relatives aux chaines de protection puissance linéique élevée IPG ou bas RFTC.
  []

  []

2.3. AUTRES HYPOTHÈSES

L'instrumentation RPI mesure la position des grappes[].

3. DESCRIPTION - FONCTIONNEMENT

3.1. DESCRIPTION

3.1.1. Description générale du système

L'instrumentation RPI appartient au système de contrôle et de mesure des grappes (RGL). Cependant, le logiciel utilisé pour le traitement fait partie du système de protection (PS). L'architecture du système de protection est décrite dans la spécification du système RPR (voir la section 7.3.1). La figure FIG–7.5.4.3 donne une vue d'ensemble de l'instrumentation RPI.

Il y a 22 grappes affectées aux divisions 1, 2, 3 et 23 grappes affectées à la division 4. L'affectation des capteurs aux divisions est indiquée sur la figure FIG–7.5.4.4. Une armoire de contrôle-commande (CC) est installée en conséquence dans chaque division du bâtiment de sauvegarde pour le conditionnement et le traitement numérique des signaux.

Le RDTME est partiellement inclus dans l'instrumentation RPI, mais possède aussi une partie en dehors de l'instrumentation RPI.

3.1.2. Description des matériels principaux

L'instrumentation RPI est constituée des matériels principaux suivants :

3.1.2.1. Structure

- capteurs :
  Le capteur de position des grappes (la bobine d'indication de position – PIC) est constitué d'une bobine primaire et de trois bobines secondaires. Deux des bobines secondaires (dites « auxiliaires ») indiquent que la grappe est dans la position haute ou basse. La bobine principale secondaire couvre la hauteur du doigt de gant. La mesure de position analogique de la grappe est dérivée du couplage magnétique entre la bobine primaire et les bobines secondaires, via la tige de commande.
  []
  []
  Les bobines secondaires auxiliaires fournissent les signaux qui indiquent lorsque la grappe est dans sa position haute ou basse.

- module de conditionnement :
  Le module de conditionnement assure l'alimentation auxiliaire de la bobine primaire et le conditionnement analogique (pré-amplification, génération d'un signal RMS) des signaux provenant des bobines secondaires et de la bobine primaire.
  La figure FIG–7.5.4.5 présente les tâches du module de conditionnement qui est spécialement conçu pour le conditionnement de la position analogique des grappes.

- système de traitement numérique (RPU) :
  [] L'unité RPU de l'instrumentation RPI calcule [] la position analogique des grappes qui sont envoyées aux unités du PS [] et aux unités du RCSL []. L'unité RPU comprend également la logique de calibrage de l'instrumentation RPI.
  La topologie mécanique des bobines de mesure et la ligne de connexion du système de mesure de position des grappes sont illustrées sur la figure FIG–7.5.4.6.

3.1.2.2. Signaux et commandes

Entrées (conversion analogique/numérique) :

Compte tenu des données susmentionnées relatives au module de conditionnement, le nombre minimum de signaux devant être traités avec les modules d'entrée analogiques et les modules d'entrée binaires sont listés ci-dessous :

Description	Objectif	Signaux
Signaux analogiques d'entrée 0…10 VCC	[] [] [] []	4 par grappe
Signaux binaires d'entrée 0/24 VCC	Alarme de synchronisation Alarme de surveillance de l'impulsion de synchronisation	1 par armoire 4 par armoire

Les tensions analogiques 0 – 10 V fournies par le module de conditionnement sont numérisées via les modules d'entrée analogiques.

Tous les signaux sont interconnectés sous forme de signaux analogiques référencés à la masse. Ceci est possible, car ces signaux restent dans la même armoire. Il est donc possible de traiter 16 signaux par module d'entrées analogiques. Un module d'entrée analogique est prévu pour les signaux de 4 grappes consécutives (selon la numérotation des grappes).

Sorties :

Le système de traitement numérique de l'instrumentation RPI calcule les données suivantes requises par d'autres systèmes :

- 'la mesure analogique de la position des grappes',
- 'la position haute de la grappe',
- 'la position basse de la grappe'.

Ces données sont transmises [] au système PS. De plus, ces données sont générées sous forme de signaux 0-20 mA et transmises [] depuis les sorties des modules de sortie analogiques jusqu'au système RCSL de la même division.

Le signal à destination du RCSL est conçu pour contenir la « mesure analogique de la position de grappe » ainsi que « la position de grappe basse ou haute ».

Des dispositifs de découplage spéciaux pour le transfert de données au sein de la même division ne sont pas nécessaires conformément au concept de séparation électrique. L'impact des risques électriques provenant du système RCSL ou du câblage correspondant vers le système PS est limité aux modules de sortie analogiques. Ils contiennent des optocoupleurs pour chaque chaîne qui empêchent la propagation des erreurs électriques aux autres modules installés dans la même armoire. Même si tout le module de sortie analogique est détérioré par l'erreur d'une de ses chaînes, cela n'affecte pas le système PS mais seulement le transfert de données de ce module au RCSL correspondant (une redondance dans la même division).

[]

3.1.2.3. Interfaces

Comme indiqué sur la figure **FIG–7.5.4.2** et la figure **FIG–7.5.4.3**, l'instrumentation de mesure de la position des grappes est en interface avec les systèmes suivants :

- PS : Le RPU calcule la position des grappes et transmet ces données au système PS[].

- RCSL : Les positions analogiques des grappes sont distribuées []au système RCSL.
- RDTME (la partie n'étant pas comprise dans l'instrumentation RPI).

3.1.3. Description des dispositions d'installations principales

Les armoires de CC du système de mesure de position des grappes sont installées dans les divisions correspondantes du bâtiment de sauvegarde.

La bobine d'indication de position (PIC) est installée au-dessus des mécanismes de commande des grappes, autour du doigt de gant sur toute sa hauteur, dans le bâtiment réacteur.

3.2. FONCTIONNEMENT

Les positions analogiques des grappes de l'instrumentation de mesure de position des grappes sont utilisées pour les conditions PCC-1, PCC-2, PCC-3, PCC-4 et les situations RRC-A.

3.2.1. Fonctionnement en régime normal de la tranche

L'instrumentation de mesure de position des grappes traite les positions analogiques des 89 grappes, y compris les positions haute et basse, lorsque le réacteur est dans les états standards A à C. Ces signaux sont utilisés dans des conditions de fonctionnement normales.

Dès que les liaisons avec la bobine d'indication de position (PIC) sont interrompues lors de l'arrêt, l'instrumentation de mesure de position des grappes n'est plus disponible. Pour l'arrêt à froid avec le cœur totalement déchargé, la fonction de mesure de la position des grappes n'est pas disponible et peut être désactivée. Le logiciel du système de mesure de la position des grappes permet aussi d'inhiber le traitement ultérieur des mesures en fixant le paramètre correspondant via l'unité de service PS.

Les équipements de mesure du temps de chute des grappes effectuent sur demande les tests périodiques de mesure du temps de chute des grappes, généralement réalisés lors du redémarrage de la centrale.

3.2.2. Fonctionnement en régime permanent du système

En situations PCC-1, PCC-2, PCC-3, PCC-4 et RRC-A, la principale tâche de l'instrumentation de mesure de position des grappes est l'acquisition des mesures analogiques de position des grappes et leur conditionnement analogique et numérique. Étant donné que la position analogique des grappes contribue à une fonction de sûreté, le logiciel de mesure de position des grappes fait partie de la base de données du RPR. Les armoires de CC de l'instrumentation de mesure de position des grappes peuvent être considérées comme des armoires de conditionnement.

L'instrumentation de mesure de position des grappes fournit les données d'entrée au système RPR et au système RGL. Par ailleurs, les signaux de mesure brute provenant des bobines d'indication de position PIC sont envoyés en continu à l'équipement de mesure du temps de chute des grappes (RDTME).

L'instrumentation de mesure de la position des grappes contribue à faire face à certaines conditions anormales de fonctionnement de la centrale (PCC-2, PCC-3, PCC-4 et RRC-A). L'instrumentation de mesure de position des grappes ne change pas de mode de fonctionnement pendant les conditions anormales de fonctionnement de la centrale PCC-2 à PCC-4 et RRC-A. L'instrumentation de mesure de position des grappes ne fait pas partie de l'instrumentation Accident Grave.

3.2.3. Fonctionnement en régime transitoire

Sans objet.

3.2.4. Autres régimes de fonctionnement du système

Les mesures de position des grappes sont distribuées dans chacune des 4 divisions, une défaillance dans une division pouvant donc mener à la perte d'une à 22 mesure(s) de position (23 pour la division 4, qui acquiert la position de la grappe centrale).

Due à la perte de la mesure de position d'une grappe, la comparaison entre la position mesurée et celle comptée ne peut plus se faire et un désalignement ne peut plus être détecté.

Dans le pire des cas, une défaillance électrique affecte l'armoire de CC d'une seule division de l'instrumentation de mesure de position des grappes. [] La perte des mesures affectées à la division concernée représente une défaillance unique tolérable dans le système RPR.

4. ANALYSE DE SÛRETÉ

4.1. CONFORMITÉ À LA RÉGLEMENTATION

L'instrumentation RPI est conforme à la réglementation générale en vigueur (voir le sous-chapitre 1.7) et ne fait pas l'objet de dérogations particulières.

4.2. RESPECT DES CRITÈRES FONCTIONNELS

4.2.1. Contrôle de la réactivité

L'instrumentation RPI ne contribue pas directement au contrôle de la réactivité.

4.2.2. Évacuation de la puissance résiduelle

L'instrumentation RPI ne contribue pas directement à l'évacuation de la puissance résiduelle.

4.2.3. Confinement des substances radioactives

L'instrumentation RPI ne contribue pas directement au confinement des substances radioactives.

4.2.4. Contributions indirectes à l'accomplissement des fonctions de sûreté

Les hypothèses de dimensionnement de l'instrumentation RPI énoncées au § 2.2. sont cohérentes avec les requis des systèmes/équipements servis.

4.3. CONFORMITÉ AUX EXIGENCES DE CONCEPTION

4.3.1. Exigences issues du classement de sûreté

4.3.1.1. Classement de sûreté

Les classements des équipements de l'instrumentation RPI jouant un rôle vis-à-vis de la sûreté sont présentés dans la section 3.2.2.

4.3.1.2. Critère de défaillance unique (active et passive)

Défaillance unique active

La conception de l'instrumentation RPI est conforme à l'exigence de robustesse au critère de défaillance unique active énoncée au § 0.3., notamment sur les points suivants :

- Le critère de défaillance unique est pris en compte pour la partie F1A du contrôle-commande de l'instrumentation RPI. Du fait qu'un seul capteur soit localisé sur chaque grappe, la mesure de position de chaque grappe n'est pas redondante. Cependant, chaque sous-groupe est constitué

de 4 grappes homologues localisées dans chacune des 4 sections du cœur et qui se déplacent ensemble, ce qui constitue une redondance pour la mesure de position d'un sous-groupe.

- Le critère de défaillance unique est respecté si, en cas de défaillance cumulée à un test ou une procédure de maintenance, le déroulement normal d'une action de protection n'est pas empêché.
- Il est pris en compte avec l'intégration de degrés de redondance suffisants, d'une structure et de dispositions adéquates (indépendance, séparation physique et électrique).

Défaillance unique passive

Sans objet.

4.3.1.3. Alimentation électrique de secours

La conception de l'instrumentation RPI est conforme à l'exigence de secours électrique énoncée au **§ 0.3.**, notamment sur les points suivants :

- En cas de Manque De Tension Externe (MDTE), les fonctions classées F1 sont secourues électriquement par les diesels principaux.
- Chaque armoire de contrôle-commande RPI est alimentée par deux convertisseurs [] indépendants (principe de la double alimentation) : une alimentation provient d'un convertisseur [] et l'autre d'un convertisseur []. Ils sont secourus par des batteries [].
- Les bobines d'indication de position PIC sont alimentés par la même alimentation électrique sans coupure. Ils sont secourus par des batteries [].

4.3.1.4. Séparation physique/géographique

La conception de l'instrumentation RPI est conforme à l'exigence de séparation physique/ géographique, notamment sur le point suivant :

- Les armoires de contrôle-commande RPI sont installées dans des divisions différentes afin de limiter les conséquences d'agressions internes et externes.

4.3.1.5. Qualification aux conditions accidentelles

Les équipements de l'instrumentation RPI relevant d'une qualification aux conditions accidentelles, sont présentés dans la section 3.7.1.1.2.

4.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

La conformité des classements mécanique, électrique, contrôle-commande et sismique des équipements de l'instrumentation RPI jouant un rôle vis-à-vis de la sûreté aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

4.3.2. Exigences réglementaires

4.3.2.1. Textes réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.1.1. Textes officiels

Sans objet.

4.3.2.1.2. Prescription techniques

Sans objet.

4.3.2.1.3. Réglementations internationales
Sans objet.

4.3.2.2. Textes para-réglementaires

La conformité aux textes para-réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.2.1. Règles fondamentales de sûreté
Sans objet.

4.3.2.2.2. Directives techniques
La conformité aux directives techniques spécifiquement applicables à l'instrumentation, listées au **§ 0.3.2.**, est présentée aux paragraphes **§ 4.3.1.**, **§ 4.3.3.** et **§ 4.4.4.** (G3).

4.3.2.3. Textes EPR spécifiques

Sans objet.

4.3.3. Agressions

4.3.3.1. Agressions internes

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

4.3.3.2. Agressions externes

La démonstration de la robustesse de l'installation aux agressions externes relève du sous-chapitre 3.3.

4.3.4. Diversification

Sans objet.

4.3.5. Radioprotection

Sans objet.

4.3.6. Fonctionnement, maintenance et accessibilité long terme

Sans objet.

4.3.7. Système tel que réalisé

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

4.4.1. Essais de démarrage

L'instrumentation RPI fait l'objet d'un programme d'essais de démarrage conformément aux modalités présentées au chapitre 14 permettant notamment de vérifier le respect du critère suivant :

- Précision.

Nota : Le temps de réponse est vérifié hors site sur une plateforme d'essai.

4.4.2. Surveillance en exploitation

La mesure de position des grappes par l'instrumentation RPI est une fonction sollicitée en exploitation normale de la tranche dans des conditions de fonctionnement incidentelles / accidentelles / d'agressions dans lesquelles elle est requise.

La surveillance de la disponibilité de ces fonctions est donc réalisée au titre de cette surveillance continue.

Auto surveillance :

Le traitement numérique et les modules participant à l'acquisition et au conditionnement des signaux des capteurs peuvent être considérés comme des systèmes d'auto-surveillance :

- Les unités de traitement et les modules de communication sont vérifiés par le logiciel système installé dessus, ce qui déclenche des alarmes et, au besoin, des actions automatiques lorsque des défaillances sont détectées.
- Tous les modules d'Entrée/Sortie (E/S) sont munis d'une surveillance d'insertion qui signale immédiatement l'absence d'un module ou d'un branchement.
- L'absence des signaux d'un capteur est signalée []. Cela permet de mettre en évidence la présence de fils coupés venant ou allant vers le module de conditionnement.
- Aussi, l'incohérence des signaux d'un capteur est signalée[].
- Les écarts entre la position analogique d'une grappe et la position stockée dans les compteurs numériques du système RCSL sont détectés et signalés par le système RCSL.
- Les signaux envoyés au système RCSL font également l'objet d'une vérification du « zéro flottant ».
- Le système de surveillance des armoires CC du RPI surveille et signale les alarmes standard des armoires, par exemple : porte ouverte, défaut d'insertion d'un module, panne d'alimentation (par exemple, défaut du coupe-circuit,) et aussi les deux alarmes de synchronisation.

4.4.3. Essais périodiques

Les parties classées de l'instrumentation RPI font l'objet d'essais périodiques conformément au chapitre IX des Règles Générales d'Exploitation permettant notamment de vérifier le respect du critère suivant :

- Précision de l'instrumentation RPI.

4.4.4. Maintenance

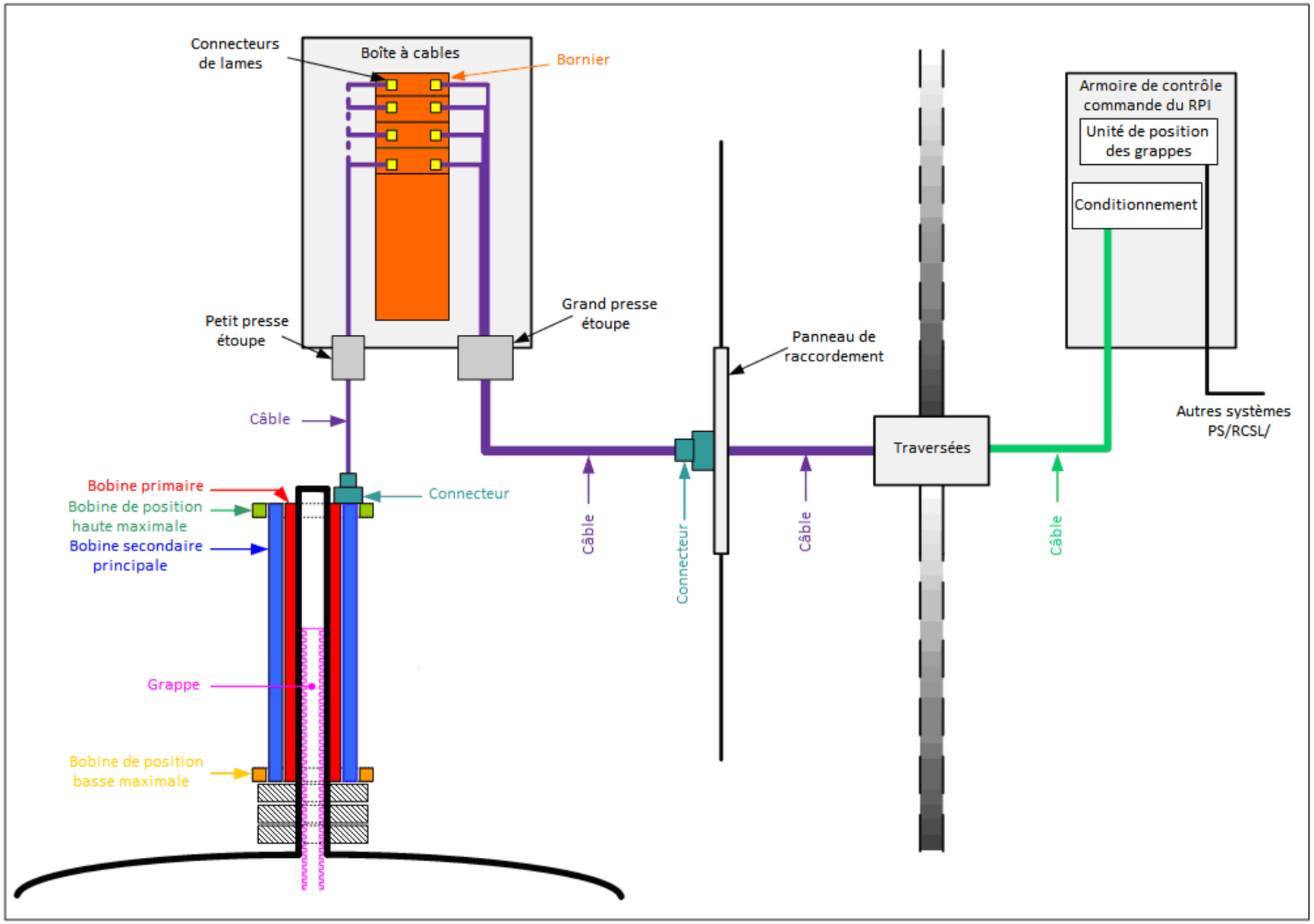
L'instrumentation RPI fait l'objet d'un programme de maintenance conformément au chapitre VIII des RGE.

5. SCHÉMA DE PRINCIPE

Le schéma de principe de l'instrumentation RPI est présenté en figure **FIG–7.5.4.1**.

TAB–7.5.4.1 CONSÉQUENCES DES DÉFAILLANCES DE MATÉRIEL

FIG–7.5.4.1 SCHÉMA DE PRINCIPE DE L'INSTRUMENTATION DE MESURE DE POSITION DES GRAPPES

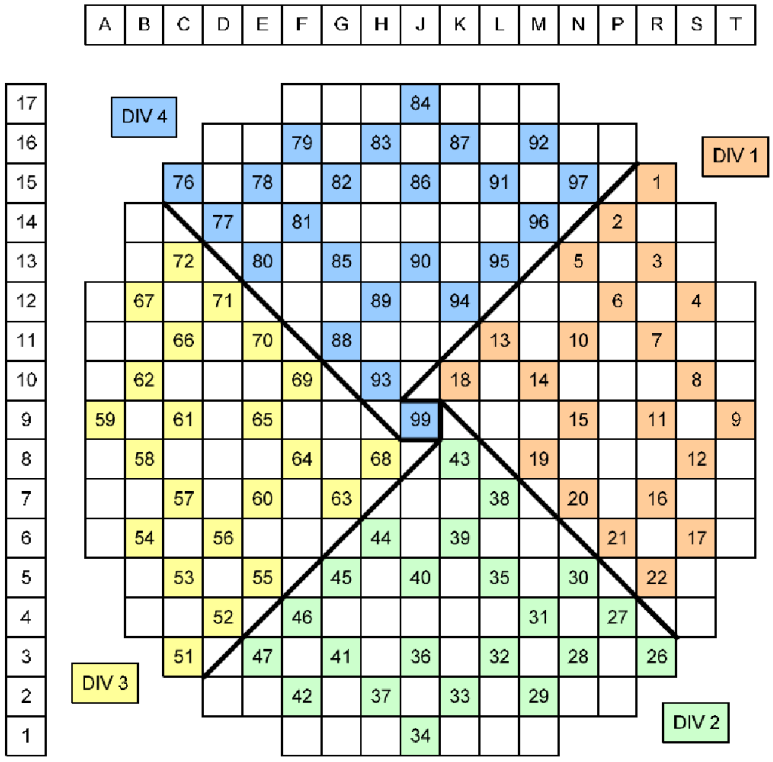


FIG–7.5.4.2 INTERFACES DE L'INSTRUMENTATION RPI

FIG–7.5.4.3 VUE D'ENSEMBLE DE L'INSTRUMENTATION RPI

[]

FIG–7.5.4.4 ATTRIBUTION DU NUMÉRO N3N4 (DU CODE ECS) À LA POSITION DES GRAPPES



FIG–7.5.4.5 TÂCHES DU MODULE DE CONDITIONNEMENT

[]

FIG–7.5.4.6 TOPOLOGIE D'UN CIRCUIT DE MESURE

[]

[]

SOMMAIRE

FIGURES :

.7.5.5 MESURES DU NIVEAU CUVE ET DE LA TEMPÉRATURE DÔME

0. EXIGENCES DE SÛRETÉ

La conception mécanique de cette instrumentation relève de la section 5.3.2.

L'instrumentation RPVDT n'est pas identifiée comme participant aux fonctions de sûreté et n'est pas mentionné dans ce paragraphe.

0.1. FONCTIONS DE SÛRETÉ

0.1.1. Contrôle de la réactivité

L'instrumentation de mesure du niveau cuve (RPVL) ne contribue pas directement au contrôle de la réactivité.

0.1.2. Évacuation de la puissance résiduelle

L'instrumentation RPVL ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.1.3. Confinement des substances radioactives

L'instrumentation RPVL ne contribue pas directement au confinement de substances radioactives.

0.1.4. Contributions indirectes aux fonctions de sûreté

L'instrumentation RPVL doit contribuer indirectement à l'évacuation de la puissance résiduelle :

- fournir une évaluation permanente du niveau de réfrigérant dans la cuve du réacteur dans certaines conditions de fonctionnement de catégorie PCC-2, PCC-3, PCC-4 et RRC-A.

0.1.5. Contributions spécifiques à la protection contre les agressions

L'instrumentation RPVL ne contribue pas spécifiquement à la protection contre les agressions.

0.1.6. Contributions à l'élimination pratique

L'instrumentation RPVL ne contribue pas directement à l'élimination pratique.

0.2. CRITÈRES FONCTIONNELS

Au titre de ses contributions à l'accomplissement des fonctions de sûreté, l'instrumentation RPVL doit satisfaire les critères fonctionnels suivants :

0.2.1. Contrôle de la réactivité

L'instrumentation RPVL ne contribue pas directement au contrôle de la réactivité.

0.2.2. Évacuation de la puissance résiduelle

L'instrumentation RPVL ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.2.3. Confinement des substances radioactives

L'instrumentation RPVL ne contribue pas directement au confinement de substances radioactives.

0.2.4. Contributions indirectes aux fonctions de sûreté

Au titre de sa contribution indirecte à l'évacuation de la puissance résiduelle, l'instrumentation RPVL doit satisfaire les critères fonctionnels suivants :

- mesure du niveau cuve : l'instrumentation RPVL doit fournir la mesure permanente du niveau de réfrigérant dans la cuve du réacteur, en PCC-2, PCC-3, PCC-4 et RRC-A afin de respecter les critères d'acceptabilité de ces études (sous–chapitre 15.1 et section 19.1.1).

0.3. EXIGENCES RELATIVES A LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Les parties de l'instrumentation RPVL jouant un rôle vis-à-vis de la sûreté doivent faire l'objet d'un classement de sûreté conformément aux règles de classement indiquées à la section 3.2.1.

0.3.1.2. Critère de Défaillance Unique (active et passive)

Les fonctions de l'instrumentation RPVL classées F1 doivent être robustes à l'application du critère de défaillance unique.

0.3.1.3. Alimentation électrique de secours

L'alimentation électrique des composants de l'instrumentation RPVL nécessaire à l'accomplissement des fonctions classées F1 doit être secourue par les groupes diesels principaux.

0.3.1.4. Séparation physique / géographique

Les fonctions classées F1 de l'instrumentation RPVL doivent être conçues conformément à l'exigence de séparation physique/géographique de leurs équipements redondants constitutifs :

- séparation physique et électrique des chaînes de mesure redondantes (fonctions F1B).

0.3.1.5. Qualification aux conditions accidentelles

Les équipements classés de l'instrumentation RPVL doivent être qualifiés en fonction des conditions de fonctionnement danslesquelles ils sont sollicités au titre de leur contribution à l'accomplissement des fonctions de sûreté, conformément aux règles du sous-chapitre 3.7.

0.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

Les équipements de l'instrumentation RPVL redevables d'un classement mécanique, électrique, contrôle-commande et sismique doivent être classés conformément aux règles de classement présentées dans la section 3.2.1.

Les équipements de l'instrumentation RPVL redevables d'un classement ESPN doivent être classés conformément à la réglementation applicable (cf. section 3.6.2).

0.3.2. Exigences réglementaires

0.3.2.1. Textes réglementaires

0.3.2.1.1. Textes officiels

L'instrumentation RPVL n'est pas concernée spécifiquement par un texte officiel.

0.3.2.1.2. Prescriptions techniques

L'instrumentation RPVL n'est pas concernée par une prescription technique spécifique.

0.3.2.1.3. Réglementations internationales

L'instrumentation RPVL n'est pas concernée par une réglementation internationale spécifique.

0.3.2.2. Textes para-réglementaires

0.3.2.2.1. Règles fondamentales de sûreté

L'instrumentation RPVL n'est pas concernée par une règle fondamentale de sûreté spécifique.

0.3.2.2.2. Directives techniques

L'instrumentation RPVL est concernée par les sections suivantes des Directives Techniques (voir les sections ci-dessous de la section 1.7.0) :

- section G3 – conception du contrôle-commande.
  Cette section précise les exigences relatives à l'instrumentation et au contrôle-commande.
  Les exigences applicables à l'instrumentation concernent :
  - le classement fonctionnel de l'instrumentation,
  - la prise en compte du critère de défaillance unique, de la maintenance et de la séparation physique,
  - la prise en compte des conséquences des agressions internes et externes sur le contrôle-commande.

0.3.2.3. Textes EPR spécifiques

L'instrumentation RPVL n'est pas concernée par un texte spécifique EPR.

0.3.3. Agressions

0.3.3.1. Agressions internes

Les fonctions de l'instrumentation RPVL doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Les fonctions de l'instrumentation RPVL doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3.4. Diversification

L'instrumentation RPVL ne fait pas l'objet d'une exigence de diversification.

0.3.5. Radioprotection

L'instrumentation RPVL n'est pas concernée par une exigence de radioprotection.

0.3.6. Exigences liées au fonctionnement, à la maintenance et à l'accessibilité long terme

L'instrumentation RPVL n'est pas concernée par une exigence liée au fonctionnement, à la maintenance et à l'accessibilité long terme dans la gestion long terme après accident.

0.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

0.4.1. Essais de démarrage

L'instrumentation RPVL doit être conçue pour permettre la réalisation d'essais de démarrage permettant de s'assurer, dans des conditions aussi représentatives que possible des différentes configurations de fonctionnement, de sa conception adéquate et de ses performances, et notamment du respect des critères fonctionnels qui lui sont assignés au § 0.2..

0.4.2. Surveillance en exploitation

L'instrumentation RPVL doit être conçue pour permettre une surveillance en exploitation normale des caractéristiques du système nécessaires à l'accomplissement de ses missions de sûreté afin d'assurer le bon comportement de ses composants et leur disponibilité en fonctionnement normal, incidentel et accidentel.

0.4.3. Essais périodiques

Les parties classées de l'instrumentation RPVL doivent être conçues pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

0.4.4. Maintenance

L'instrumentation RPVL doit être conçue pour permettre la mise en œuvre d'un programme de maintenance conformément au chapitre VIII des RGE.

1. RÔLE DU SYSTÈME

L'instrumentation RPVL/RPVDT assure les fonctions opérationnelles suivantes dans les différentes conditions de fonctionnement de l'installation dans lesquelles elle est sollicitée :

1.1. RÔLE DU SYSTÈME PENDANT L'EXPLOITATION NORMALE DE LA TRANCHE

Mesure du niveau de la cuve (RPVL)

En fonctionnement normal de la tranche, l'instrumentation RPVL fournit une évaluation permanente du niveau de réfrigérant dans la cuve.

Mesure de la température du dôme (RPVDT)

En fonctionnement normal de la tranche, l'instrumentation RPVDT fournit à l'opérateur la distribution de la température dans le dôme de la cuve.

1.2. RÔLE DU SYSTÈME DANS DES CONDITIONS DE FONCTIONNEMENT PCC–2 À PCC–4, RRC-A, EN ACCIDENT GRAVE ET SITUATIONS AGRESSIONS

L'instrumentation RPVL contribue à la fonction de sûreté d'évacuation de la puissance résiduelle. La mesure du niveau de réfrigérant dans la cuve ne participe pas au maintien de la sous-criticité. En effectuant une mesure du niveau à l'intérieur de la cuve, une partie de l'instrumentation participe à l'intégrité du circuit primaire.

Associée à la mesure de température à la sortie du cœur (servant à l'élaboration de la marge à la saturation à la sortie du cœur), la mesure du niveau de réfrigérant de la cuve fournit des informations permettant d'évaluer l'état de la tranche dans des conditions post-accidentelles et de surveiller le niveau de réfrigérant en situations post-accidentelles.

2. BASES DE CONCEPTION

2.1. HYPOTHÈSES GÉNÉRALES DE FONCTIONNEMENT

Les critères de dimensionnement de l'instrumentation RPVL sont principalement les suivants :

- disponibilité des fonctions classées de sûreté lors d'une défaillance ou lors des opérations de maintenance.

Pour répondre à ces critères, l'instrumentation RPVL est dimensionnée comme suit :

- indépendance électrique entre les quatre redondances pour traiter les fonctions classées et maintenir ainsi une redondance en cas de défaillance unique cumulée avec la maintenance d'un équipement.

2.2. HYPOTHÈSES DE DIMENSIONNEMENT

2.2.1. Contrôle de la réactivité

L'instrumentation RPVL ne contribue pas directement au contrôle de la réactivité.

2.2.2. Évacuation de la puissance résiduelle

L'instrumentation RPVL ne contribue pas directement à l'évacuation de la puissance résiduelle.

2.2.3. Confinement des substances radioactives

L'instrumentation RPVL ne contribue pas directement au confinement de substances radioactives.

2.2.4. Contributions indirectes aux fonctions de sûreté

Mesure du niveau cuve : Il n'y a pas de critère numériquement quantifiable associé au critère fonctionnel du **§ 0.2.**.

2.3. AUTRES HYPOTHÈSES

Mesure du niveau de la cuve (RPVL)

Précision :

Les trois seuils (haut des branches chaudes (HBC), milieu des branches chaudes (MBC) et bas des branches chaudes (BBC)) sont distingués sans ambiguïté. [] L'incertitude spatiale au cours de transitoires lents est donc liée à l'incertitude associée au positionnement des capteurs.

Temps de réponse :

Étant donné qu'aucune action automatique basée sur les informations RPVL n'est prévue, un temps de réponse court n'est pas requis. Néanmoins un temps de réponse []est pris en compte.

Dépressurisation rapide :

Afin d'être opérationnelle, l'instrumentation RPVL supporte, dans la cuve, une dépressurisation rapide et une diminution de la température associée (diminution de la température de saturation).

Mesure de la température du dôme (RPVDT)

Pour la chaîne d'instrumentation des thermocouples du dôme (capteur, électronique, connexions, convertisseur analogique / numérique), une exactitude globale est prise en compte[].

Un temps de réponse court n'est pas requis.

3. DESCRIPTION - FONCTIONNEMENT

3.1. DESCRIPTION

3.1.1. Description générale du système

Mesure du niveau de la cuve (RPVL)

La mesure de niveau de réfrigérant dans la cuve du réacteur est réalisée à partir de quatre sondes de mesure disposées dans chacun des quadrants du cœur. Chaque sonde contient trois capteurs, disposés à trois niveaux différents. Un tube guide entoure chacune des sondes.

A chaque sonde de mesure est associée une chaîne de traitement implantée dans une armoire de conditionnement.

Mesure de la température du dôme (RPVDT)

La mesure de la température du dôme du réacteur est réalisée à partir de cinq capteurs. L'un est disposé au centre du dôme, les quatre autres sont répartis dans deux sondes de mesure aussi utilisées par les thermocouples RPVL.

Systèmes en interface

Les signaux de sortie issus du matériel de conditionnement RPVL sont acquis et affichés dans le système d'automatisme de sûreté (SAS). En parallèle les 3 signaux de niveau de chaque division sont envoyés au système PS (faisant partie du système RPR). Les signaux de sortie du matériel de conditionnement RPVDT sont acquis et traités dans le système PAS. Le signal émis par le thermocouple situé au centre du dôme n'est pas conditionné dans les armoires RPVL/RPVDT, mais directement acquis par le système PAS.

Systèmes serveurs : Sans objet.

Systèmes servis : Les systèmes servis sont le PAS, le SAS, le PS, puis le MCP/MCS et la Salle de Commande (sous la forme d'informations adressées à l'opérateur).

3.1.2. Description des matériels principaux

Mesure du niveau de la cuve (RPVL)

Capteurs

Le capteur comprend un thermocouple chauffé et un thermocouple non chauffé qui se trouvent à la même hauteur mais qui sont logés dans des tubes séparés à l'intérieur du doigt de gant de la sonde. Les thermocouples [] ont un bon contact thermique avec la surface intérieure des tubes servant de logement (enveloppe). L'élément chauffé entre directement en contact thermique avec le thermocouple associé. [] (figure **FIG–7.5.5.5**).

Doigt de gant de la sonde

Les thermocouples, les éléments chauffants et leurs câbles sont insérés dans des tubes enveloppes qui sont installés dans un doigt de gant de sonde. Chaque doigt de gant de sonde comporte au total trois capteurs qui sont positionnés à trois niveaux (un capteur par niveau) afin de mesurer le niveau de réfrigérant : en haut de la branche chaude (HBC), en bas de la branche chaude (BBC) et au milieu de la branche chaude (MBC). Le doigt de gant de sonde est perforé d'un grand nombre de trous pour permettre une bonne circulation du réfrigérant et de la vapeur le long des tubes enveloppes (Figure **FIG–7.5.5.6**).

Tube guide

Chaque sonde est entourée d'un tube guide concentrique se trouvant dans la région du plénum supérieur et qui se prolonge dans la région du dôme de la cuve. Le tube guide dans la région du plénum supérieur est fixé en haut à la plaque support des tubes guides et en bas à la plaque supérieure de cœur (figure **FIG–7.5.5.7**). La partie supérieure du tube guide dans la région du dôme est fixée en bas à la plaque support des tubes guides. Le haut de la partie supérieure du tube guide est équipé d'un entonnoir pour guider le trajet de la sonde lors de l'assemblage. La zone entre le tube guide et le haut du tube de la sonde, où se trouve l'entonnoir, doit être aussi petite que possible pour limiter le débit de vapeur du dôme vers la sonde. De plus, il ne doit pas y avoir de circulation dans la sonde elle-même dans la zone de l'entonnoir.

Le tube guide a pour fonctions de :

- positionner les sondes à l'emplacement souhaité,
- protéger la sonde contre les forces induites par le débit dans le plénum supérieur.

Une autre fonction du tube guide est de garantir des conditions de fluidité définies autour des capteurs. En effet, dans de nombreuses situations accidentelles, le réfrigérant restant évolue en un mélange vapeur/réfrigérant fortement turbulent qui ne permet pas à un capteur directement en contact avec le mélange de fournir une indication significative. Par conséquent, la sonde est logée dans un tube de protection qui est fermé sur toute sa longueur, sauf en bas et en haut où se trouvent des ports de communication.

Câbles et connecteurs

A l'intérieur de la sonde, les fils provenant des éléments de détection (thermocouples et éléments chauffants) sont à gaine métallique []. Tous les fils d'une sonde aboutissent dans un connecteur électrique au niveau de la partie supérieure de la sonde située à l'extérieur du couvercle de cuve.

Les signaux des thermocouples cheminent par un système organique de câbles faits dans le matériau conducteur des thermocouples vers un boîtier de compensation se trouvant à l'extérieur de l'enceinte, dans la zone où la température est stable et homogène pour tous les thermocouples de la sonde où ils sont ensuite transmis par des fils []. Les traversées électriques, les connecteurs et les câbles sont par conséquent adaptés jusqu'au boîtier de compensation. La température du point de connexion (jonction froide) est mesurée []dans chaque division pour effectuer la compensation dans la chaîne de mesure.

Il est possible de déconnecter les câbles de la passerelle à câbles qui fait partie de l'équipement du couvercle de cuve (en haut des sondes et en amont de la piscine réacteur) à l'aide de plaques de raccordement, afin de permettre le retrait du couvercle de cuve sans avoir à retirer la sonde de la cuve.

Structure de support

La sonde est positionnée par la fermeture d'adaptateur sur le couvercle de cuve et le tube guide dans le plénum supérieur. Elle est suspendue à la tête de la fermeture d'adaptateur où l'obturateur du piquage permet de retenir la pression et d'assurer l'étanchéité (figure **FIG–7.5.5.3**).

Les câbles atteignent la passerelle à câbles au niveau de l'équipement du couvercle de cuve et sont acheminés jusqu'aux bâtiments de sauvegarde dans les chemins de câbles appropriés et par les traversées électriques du bâtiment réacteur. Le long du trajet, les câbles sont fixés du mieux possible, notamment afin d'éviter toute défaillance en cas d'événement sismique.

Matériel de conditionnement

Le matériel de conditionnement des quatre sondes est installé dans quatre divisions séparées situées dans les bâtiments de sauvegarde. Les équipements de conditionnement effectuent la compensation de température avant la comparaison des seuils. Ils assurent l'alimentation électrique des éléments

chauffants des capteurs et du thermomètre de la jonction froide []. De plus, ils convertissent et conditionnent les signaux envoyés par les thermocouples []. Les équipements de conditionnement sont logés dans une armoire par division. [] Les ruptures de fils sont détectées par une fonction de surveillance qui enclenche une alarme.

Mesure de la température du dôme (RPVDT)

Thermocouples logés dans les sondes RPVL

[] À l'intérieur de la sonde, les fils des thermocouples sont à gaine métallique []. Avec les fils de capteurs RPVL, ils cheminent jusqu'à un connecteur commun à chaque sonde RPVL/RPVDT.

Thermocouple pour la température centrale du dôme

Le thermocouple central est connecté en amont de la piscine du réacteur. Il possède sa propre traversée dans l'équipement du couvercle de cuve. La gaine du thermocouple central est en contact avec le réfrigérant. L'extrémité chaude du thermocouple est insérée dans la traversée du thermocouple du dôme, puis elle est placée dans le rétrécissement, à l'intérieur de la cuve. La géométrie de l'extrémité chaude du thermocouple correspond à l'extrémité de la traversée. [] Sa gaine est en acier inoxydable [].

Câbles et connecteurs du thermocouple pour la température centrale du dôme

A l'intérieur du bâtiment réacteur, le signal du thermocouple chemine du connecteur situé en amont de la piscine réacteur jusqu'à la traversée électrique via un câble de prolongation isolé. A l'extérieur du bâtiment réacteur, le signal du thermocouple chemine via un câble de compensation isolé jusqu'à l'armoire de conditionnement où s'effectue la compensation de température.

Matériel de conditionnement

Le signal du thermocouple central est conditionné par le système PAS de la division 1.

Les signaux des quatre autres thermocouples RPVDT sont conditionnés dans les mêmes armoires que les signaux RPVL.

3.1.3. Description des dispositions d'installations principales

La conception de la sonde RPVL/RPVDT (à l'exception de la température centrale du dôme) est telle que :

- Le retrait du couvercle de cuve peut se faire sans retirer les sondes.
- Le démontage des sondes peut se faire sans retirer le couvercle de cuve.
- Les connexions électriques, notamment celles situées dans l'enceinte, y compris les connexions électriques aux traversées électriques, sont complètement étanches et qualifiées pour résister aux conditions ambiantes spécifiées en cas d'APRP.
- Les connexions électriques à l'extérieur de l'enceinte sont de qualité suffisante pour éviter une atténuation du signal du capteur et tout bruit perturbateur jusqu'aux équipements de conditionnement.

Mesure du niveau de la cuve (RPVL)

Un ensemble d'indications de niveau est prévu pour chacune des quatre divisions (figure FIG–7.5.5.2). Chacun de ces ensembles surveille le niveau de réfrigérant en trois points de mesure axiaux : HBC (haut de la branche chaude), BBC (bas de la branche chaude), MBC (milieu de la branche chaude) (figure FIG–7.5.5.4). Les trois capteurs sont installés axialement l'un au-dessus de l'autre. Les ensembles d'indication de niveau sont installés dans la partie supérieure de la cuve. Le doigt de gant de la sonde est inséré dans la cuve à travers le couvercle de cuve via une fermeture d'adaptateur. Il s'étend de l'extérieur de la fermeture d'adaptateur du couvercle jusqu'à une zone située entre le bas

des lignes primaires et la plaque supérieure du cœur. Le doigt de gant de la sonde est logé dans un tube guide.

Mesure de la température du dôme (RPVDT)

Quatre des capteurs de mesure de la température du dôme se trouvent dans les mêmes sondes que les thermocouples RPVL. Ces capteurs sont répartis à deux niveaux différents au sein de deux sondes se situant à l'opposé l'une de l'autre.

Le dernier capteur se trouve dans une sonde qui lui est propre, au centre du dôme.

3.2. FONCTIONNEMENT

3.2.1. Fonctionnement en régime normal de la tranche

Mesure du niveau de la cuve (RPVL)

L'instrumentation RPVL mesure en permanence le niveau de réfrigérant dans la cuve du réacteur dès que la tranche est en fonctionnement.

Mesure de la température du dôme (RPVDT)

L'instrumentation RPVDT mesure en permanence la température à trois hauteurs différentes à l'intérieur de la cuve.

3.2.2. Fonctionnement en régime permanent du système

Mesure du niveau de la cuve (RPVL)

L'élément de détection se compose de thermocouples chauffés et non chauffés. L'échange thermique dans l'eau étant considérablement plus élevé que dans la vapeur, les thermocouples chauffés se trouvent à une température inférieure et génèrent une tension thermoélectrique plus faible lorsqu'ils sont plongés dans l'eau que lorsqu'ils sont entourés par la vapeur (figure **FIG–7.5.5.8**). Pour s'affranchir de l'influence de la température de l'eau ou de la vapeur, des thermocouples non chauffés sont utilisés en plus comme points de mesure de référence. La mesure du niveau de réfrigérant dans la cuve utilise les différences entre les signaux des thermocouples chauffés et non chauffés. Le niveau de réfrigérant est surveillé grâce à des seuils : si la différence de tension thermoélectrique entre les thermocouples chauffés et non chauffés dépasse un certain seuil, cela indique que le niveau de réfrigérant est passé en-dessous du niveau des thermocouples chauffés (figure **FIG–7.5.5.9**).

Lorsque le système de refroidissement est saturé ou sous-saturé, la mesure du niveau de réfrigérant de la cuve (RPVL) est prise en compte par les procédures de conduite accidentelle, à condition que les groupes motopompes primaires (GMPP) ne fonctionnent pas. En cas de perte d'inventaire primaire, le système de protection effectue automatiquement un arrêt des GMPP via un signal RCP-DP qui est représentatif de la saturation avec un rapport de vide important.

Mesure de la température du dôme (RPVDT)

Les éléments de détection sont des thermocouples.

3.2.3. Fonctionnement en régime transitoire

Sans objet.

3.2.4. Autres régimes de fonctionnement du système

3.2.4.1. Fonctionnement dégradé du système

La défaillance d'un composant ou des procédures de maintenance d'un composant de l'instrumentation RPVL induisent des conditions de fonctionnement anormales du système.

En cas de défaillance d'un composant et de maintenance simultanée d'un autre composant de l'instrumentation RPVL, les divisions de l'instrumentation RPVL disponibles permettent à l'opérateur d'être informé du niveau de réfrigérant dans la cuve.

4. ANALYSE DE SÛRETÉ

4.1. CONFORMITÉ A LA RÉGLEMENTATION

L'instrumentation RPVL est conforme à la réglementation générale en vigueur (voir le sous-chapitre 1.7) et ne fait pas l'objet de dérogations particulières.

4.2. RESPECT DES CRITÈRES FONCTIONNELS

4.2.1. Contrôle de la réactivité

L'instrumentation RPVL ne contribue pas directement au contrôle de la réactivité.

4.2.2. Évacuation de la puissance résiduelle

L'instrumentation RPVL ne contribue pas directement à l'évacuation de la puissance résiduelle.

4.2.3. Confinement des substances radioactives

L'instrumentation RPVL ne contribue pas directement au confinement de substances radioactives.

4.2.4. Contributions indirectes à l'accomplissement des fonctions de sûreté

L'instrumentation RPVL mesure le niveau cuve, ce qui contribue indirectement à l'évacuation de la puissance résiduelle.

4.3. CONFORMITÉ AUX EXIGENCES DE CONCEPTION

L'instrumentation RPVL est conforme aux exigences de conception évoquées au **§ 0.3.**, notamment pour ce qui concerne :

4.3.1. Exigences issues du classement de sûreté

4.3.1.1. Classement de sûreté

Les classements des équipements de l'instrumentation RPVL jouant un rôle vis-à-vis de la sûreté sont présentés dans la section 3.2.2.

4.3.1.2. Critère de défaillance unique (active et passive)

Défaillance unique active

La conception de l'instrumentation RPVL est conforme à l'exigence de robustesse au critère de défaillance unique active énoncée au paragraphe 0.3, notamment sur le point suivant :

- Les chaînes d'équipements de contrôle-commande classés F1B sont redondantes et installées dans des divisions séparées.

Défaillance unique passive

Sans objet.

4.3.1.3. Alimentations électriques de secours

La conception de l'instrumentation RPVL est conforme à l'exigence de secours électrique énoncée au **§ 0.3.**, notamment sur les points suivants :

Mesure du niveau de la cuve

Afin de respecter la séparation physique entre les divisions électriques et de répondre aux exigences d'indépendance, les 3 capteurs d'une sonde RPVL sont alimentés par la même division électrique. Les capteurs se trouvant au même niveau géométrique, appartenant à 4 sondes RPVL différentes, sont alimentés par 4 divisions électriques différentes.

Les armoires de CC de l'instrumentation de mesure du niveau de la cuve (RPVL) sont alimentées en []. Cette alimentation s'effectue via toutes les distributions secondaires qui sont alimentées par des distributions sans coupure provenant des divisions voisines. Les alimentations électriques sans coupure bénéficient de batteries d'une autonomie de [].

L'alimentation électrique des éléments chauffants se compose d'un rack pour chaque élément chauffant. Trois racks (correspondant aux trois niveaux mesurés) sont installés dans l'armoire de conditionnement de chaque division et alimentent les trois éléments chauffants de la division.

En cas de Manque De Tension Externe (MDTE), les armoires électriques sont secourues par les groupes diesels principaux.

Mesure de la température du dôme

Les thermocouples sont des éléments passifs qui ne nécessitent aucune alimentation électrique supplémentaire. Le conditionnement du signal de la mesure de la température du centre du dôme s'effectue dans le PAS (voir section 7.4.2). Les autres capteurs de température, qui sont logés dans les sondes RPVL, sont traités dans les armoires de conditionnement RPVL et sont donc soumis à la même conception électrique que celle indiquée ci-dessus.

4.3.1.4. Séparation physique/géographique

La conception de l'instrumentation RPVL est conforme à l'exigence de séparation physique/ géographique, notamment sur les points suivants :

- La protection des équipements de contrôle-commande classés F1B est obtenue grâce à la protection physique des divisions 2 et 3 et grâce à la séparation géographique des divisions 1 et 4 des bâtiments de sauvegarde.
- La séparation physique entre les divisions électriques et les exigences d'indépendance sont respectées. Chacune des 4 sondes RPVL est alimentée par une division électrique différente.

4.3.1.5. Qualification aux conditions accidentelles

Les équipements de l'instrumentation RPVL relevant d'une qualification aux conditions accidentelles, sont présentés dans la section 3.7.1.1.2.

4.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

La conformité des classements mécanique, électrique, contrôle-commande et sismique des équipements de l'instrumentation RPVL jouant un rôle vis-à-vis de la sûreté aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

La conformité du classement ESPN des équipements de l'instrumentation RPVL aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

4.3.2. Exigences réglementaires

4.3.2.1. Textes réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.1.1. Textes officiels
Sans objet.

4.3.2.1.2. Prescriptions techniques
Sans objet.

4.3.2.1.3. Réglementations internationales
Sans objet.

4.3.2.2. Textes para-réglementaires

La conformité aux textes para-réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.2.1. Règles fondamentales de sûreté
Sans objet.

4.3.2.2.2. Directives techniques
La conformité aux directives techniques spécifiquement applicables à l'instrumentation, listées au **§ 0.3.2.**, est présentée aux **§ 4.3.1.**, **§ 4.3.3.** et **§ 4.4.4.** (G3).

4.3.2.3. Textes EPR spécifiques

Sans objet.

4.3.3. Agressions

4.3.3.1. Agressions internes

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

4.3.3.2. Agressions externes

La démonstration de la robustesse de l'installation aux agressions externes relève du sous-chapitre 3.3.

4.3.4. Diversification

Sans objet.

4.3.5. Radioprotection

Sans objet.

4.3.6. Fonctionnement, maintenance et accessibilité long terme

Sans objet.

4.3.7. Système tel que réalisé

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

4.4.1. Essais de démarrage

L'instrumentation RPVL fait l'objet d'un programme d'essais de démarrage conformément aux modalités présentées au chapitre 14 permettant notamment de vérifier le respect des critères suivants :

- Les trois seuils (haut des branches chaudes (HBC), milieu des branches chaudes (MBC) et bas des branches chaudes (BBC)) sont distingués sans ambiguïté.

4.4.2. Surveillance en exploitation

Mesure du niveau de la cuve

La première approche concerne les défaillances du matériel de mesure du RPVL qui sont détectées et indiquées par le système d'auto-surveillance permanent.

Le système d'auto-surveillance permet de détecter des courts-circuits, des ruptures de fils[], une perte de la tension de sortie, un court circuit du système de chauffage et une perte d'alimentation électrique. L'ouverture d'une porte d'armoire peut également être détectée.

Si une défaillance ou une condition anormale est détectée, les alarmes sont transmises au système SAS. Une défaillance est signalée par une alarme sur le MCP.

4.4.3. Essais périodiques

Les parties classées de l'instrumentation RPVL font l'objet d'essais périodiques conformément au chapitre IX des Règles Générales d'Exploitation permettant notamment de vérifier le respect des critères suivants :

- bon fonctionnement de l'électronique de conditionnement RPVL,
- bonne transmission des signaux de mesure RPVL au système RPR et à l'automate SAS/PAS.

4.4.4. Maintenance

L'instrumentation RPVL fait l'objet d'un programme de maintenance conformément au chapitre VIII des RGE.

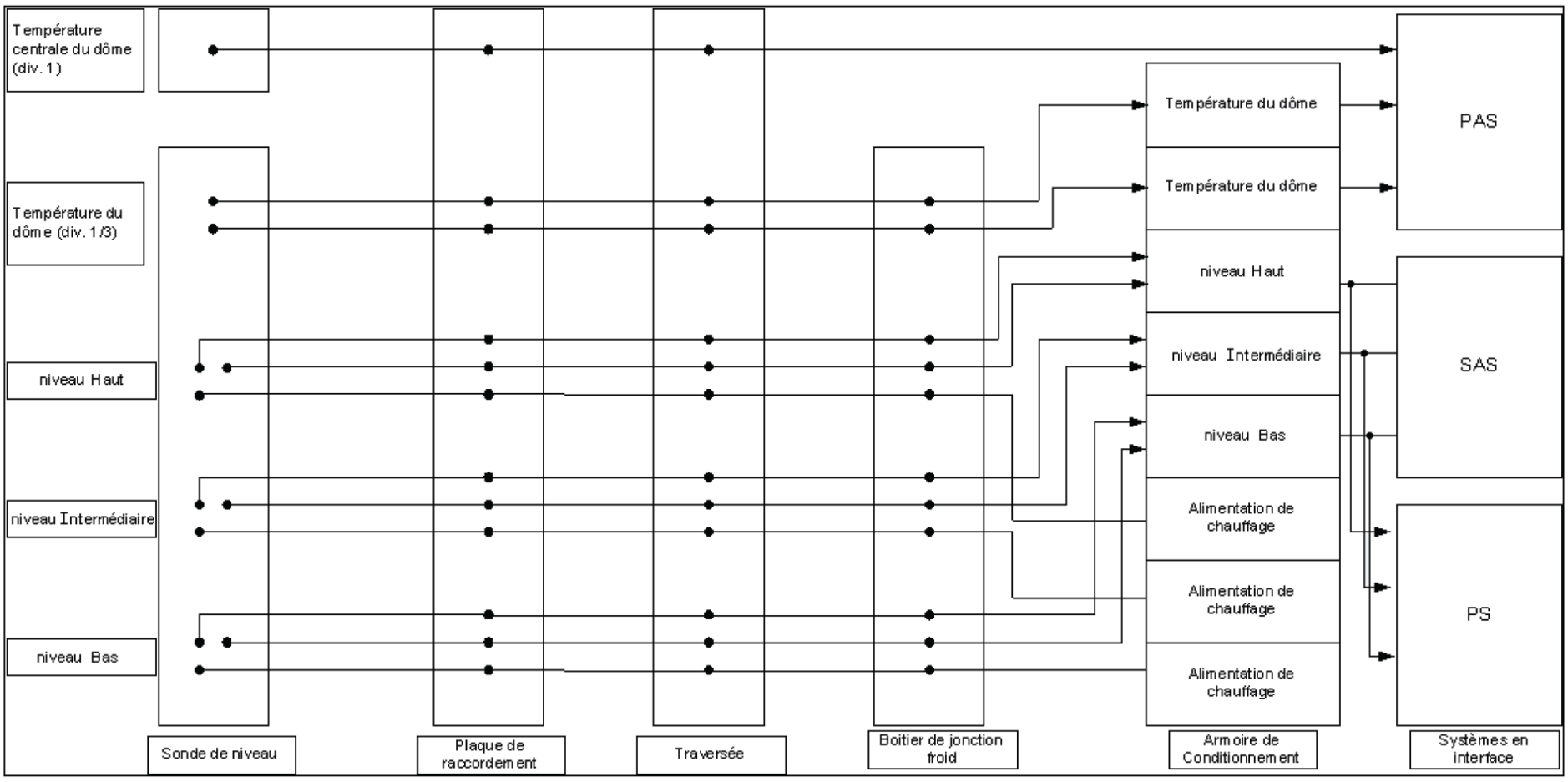
5. SCHÉMA DE PRINCIPE

Le schéma de principe de l'instrumentation RPVL/RPVDT est présenté en figure **FIG–7.5.5.1**.

FIG–7.5.5.1 SCHÉMA DE PRINCIPE POUR UNE DIVISION

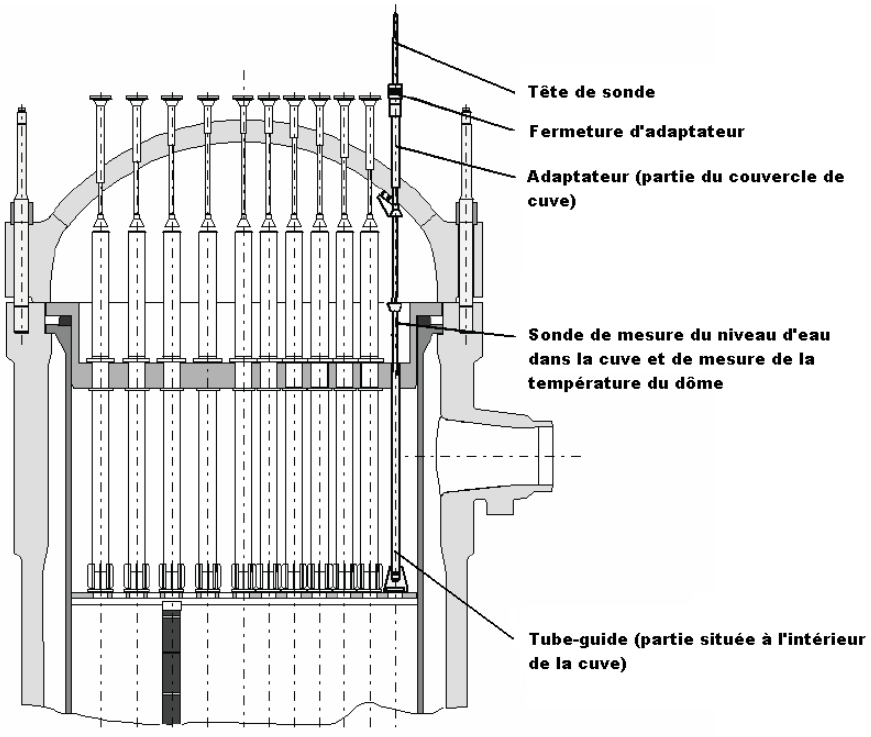
Voici le schéma de principe pour la division 1.

Le même schéma s'applique aux divisions 2, 3 et 4 pour l'instrumentation RPVL. La température centrale du dôme est acquise uniquement dans la division 1 et les mesures de température du dôme sont acquises uniquement dans les divisions 1 et 3



FIG–7.5.5.2 POSITION RADIALE DES SONDES DE MESURE RPVL ET RPVDT

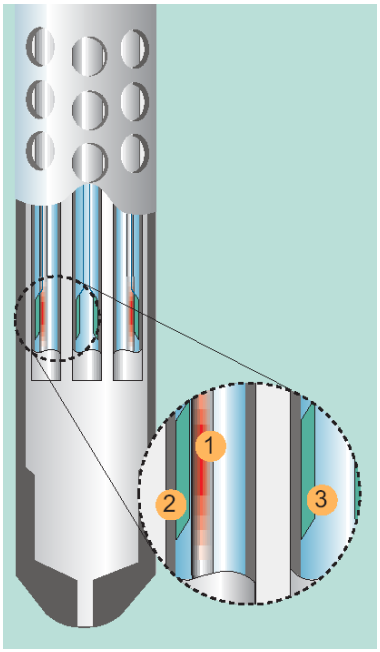
FIG–7.5.5.3 COMPOSANTS DES SONDES DE MESURE RPVL ET RPVDT



FIG–7.5.5.4 NIVEAUX AXIAUX DES THERMOCOUPLES RPVL

FIG–7.5.5.5 RPVL – POSITIONNEMENT DES THERMOCOUPLES ET DE L'ÉLÉMENT CHAUFFANT

FIG–7.5.5.6 RPVL ET RPVDT – CONCEPTION MÉCANIQUE DE LA SONDE



Trois petits tubes se trouvent à l'intérieur du doigt de gant de la sonde.

A une hauteur donnée, l'élément chauffant (1) et les thermocouples (2), (3) se trouvent dans deux de ces trois tubes.

Les thermocouples de l'instrumentation RPVDT se trouvent dans la partie supérieure de ces tubes.

FIG–7.5.5.7 VUE D'ENSEMBLE DU TUBE GUIDE

FIG–7.5.5.8 PRINCIPE DE FONCTIONNEMENT DE LA MESURE DU RPVL

FIG–7.5.5.9 RÉPONSE TEMPORELLE DE LA MESURE DU RPVL

SOMMAIRE

FIGURES :

.7.5.6 SURVEILLANCE DES CORPS MIGRANTS ET SURVEILLANCE VIBRATOIRE

1. INTRODUCTION

Ce paragraphe présente les trois principales fonctions de surveillance vibratoire du circuit primaire qui sont :

- La détection des corps migrants,
- Le suivi vibratoire des internes de cuve,
- Le suivi vibratoire des GMPP.

Ces 3 fonctions sont présentées dans les paragraphes ci-après. Aucune de ces fonctions ne constituent des fonctions de sûreté.

2. SURVEILLANCE DES CORPS MIGRANTS

2.1. PRESENTATION DE LA SURVEILLANCE DES CORPS MIGRANTS

Un corps migrant correspond à un corps étranger circulant dans le circuit primaire. Un corps migrant risque notamment d'engendrer un vieillissement prématuré de l'étanchéité du circuit primaire.

Le système de surveillance des corps migrants contrôle alors en continu le circuit primaire du réacteur via un dispositif de 11 capteurs vibratoires illustrés en fin de sous chapitre en figure FIG–7.5.6.1.

Le dispositif de détection de corps migrants du circuit primaire est composé de 11 capteurs accélérométriques :

- []
- []

Ces capteurs surveillent les zones du circuit primaire où la probabilité de présence de corps migrants est la plus forte.

2.2. METHODE DE DETECTION DES CORPS MIGRANTS

Les corps migrants entraînés par le fluide de refroidissement primaire provoquent un bruit spécifique généré par leur impact sur les parois et structures internes du circuit. Les capteurs détectent ce bruit provenant de la structure. Les signaux délivrés par les accéléromètres sont conditionnés par les convertisseurs de charge sous forme de signaux de courant. Les signaux vibratoires sont alors transmis à la baie de surveillance primaire qui réalise le traitement et le diagnostic.

Les corps migrants peuvent être identifiés par la valeur efficace des signaux de bruit provenant de la structure dans une gamme de fréquence acoustique prédéterminée (0-20kHz). Des niveaux seuil sont définis sur la base de mesures de référence et des alarmes se déclenchent en cas de dépassement. L'expérience de systèmes de surveillance entièrement automatisés a montré que les seuils doivent être définis à des niveaux relativement élevés afin d'éviter les déclenchements intempestifs d'alarmes du fait de la nature stochastique du bruit de fond. De faibles variations ne peuvent pas être automatiquement détectées suivant les modèles de bruit.

En revanche, l'oreille humaine permet d'identifier par sélectivité ces faibles variations. C'est pour cette raison qu'il est nécessaire de corréler le système de surveillance automatique à une surveillance subjective par écoute du bruit à intervalles réguliers. Cette possibilité est offerte par le tiroir de sonorisation disponible sur la baie de surveillance primaire. Ce tiroir récupère les signaux de vibrations brutes afin de pouvoir les écouter.

Chaque zone de détection est constituée de 2 ou 3 capteurs, cela permet d'améliorer la résilience de la détection de corps migrants face aux perturbations susceptibles d'impacter la chaine de mesure. Lorsqu'un corps migrant entre en collision avec les parois du circuit primaire dans une zone de détection, le choc sera détecté par l'ensemble des capteurs de la zone. Il est donc possible de faire la différence entre un signal du à un choc dans le circuit primaire et un signal du à une perturbation d'une des chaines de mesure.

Les fréquences et les niveaux de tensions des signaux vibratoires permettent d'en déduire l'énergie du choc. Le poids d'un corps migrant peut être alors estimé.

Suite à la détection d'un corps migrant, une analyse de risque est réalisée. L'analyse permet de statuer sur la nécessité d'extraction de ce corps.

2.3. ELEMENTS CONSTITUTIFS DU CIRCUIT DE DETECTION DES CORPS MIGRANTS

La chaine de détection des corps migrants est composée d'accéléromètres, de convertisseurs de charges, d'une armoire de conditionnement et d'une baie de surveillance primaire.

Les capteurs utilisés sont des accéléromètres piézoélectriques. Sous l'effet d'une accélération le capteur génère une charge proportionnelle à cette accélération. Cette charge est convertie en une variation de tension par le convertisseur de charge.

L'armoire de conditionnement est constituée d'un rack d'isolation et de conditionnement de signal. Ce rack permet d'alimenter les convertisseurs de charge ainsi que d'amplifier les signaux issus des accéléromètres. Ces signaux sont alors transmis à la baie de surveillance primaire.

La baie de surveillance primaire est constituée de cartes d'acquisitions et de traitements permettant la génération d'alarmes en salle de commande en cas de dépassement du niveau de seuil vibratoire préalablement défini. De plus, la baie de surveillance primaire possède un PC permettant de suivre les signaux issus des capteurs vibratoires dans les domaines temporels et fréquentiels. Enfin, le PC permet l'archivage de ces signaux dans l'objectif de permettre la vérification de l'existence d'un corps migrant en cas d'apparition d'alarme et, le cas échéant, d'en estimer son poids.

Caractéristiques techniques :

Les accéléromètres choisis possèdent les caractéristiques suivantes :

- Gamme de mesure ±5000g
- Bande passante : [1Hz ; 20kHz]
- Température maximum de fonctionnement : 380°C
- Tenue aux radiations : 850 kGy cumulé

Les convertisseurs de charges ainsi que leurs coffrets respectifs choisis possèdent les caractéristiques suivantes :

- Bande passante : [0,4Hz ; 50kHz]
- Plage de température de fonctionnement : -40°C et 100°C
- Tenue à l'irradiation : 10 kGy cumulé

L'armoire de conditionnement et la baie de surveillance primaire sont ventilées. Les armoires sont dimensionnées pour un fonctionnement à une température ambiante entre 5°C et 40°C.

3. SURVEILLANCE VIBRATOIRE DES STRUCTURES INTERNES (SSI)

3.1. PRESENTATION DE LA SURVEILLANCE VIBRATOIRE DES STRUCTURES INTERNES (SSI)

Afin de suivre l'état sur le long terme des internes de cuve, il existe une méthode non intrusive présentée dans la norme internationale CEI 61502 et reprise sur le site de Flamanville 3.

La surveillance utilise la composante basse fréquence des signaux issus des détecteurs CNP : Mesure de niveau puissance. Un comportement vibratoire anormal des éléments combustibles ou des internes inférieurs (réflecteur lourd, etc.) sera détecté par l'analyse fréquentielle de ces signaux, par comparaison avec les fréquences propres des matériels qui sont connues.

3.2. ELEMENTS CONSTITUTIFS DE LA CHAINE DE MESURE POUR LA SURVEILLANCE VIBRATOIRE DES INTERNES DE CUVE (SSI)

La chaine de mesure est constituée de capteurs à dépôt de bore, d'armoires d'isolations et de conditionnements ainsi que de la baie de surveillance primaire.

Les capteurs utilisés pour la surveillance des internes de cuve sont des chambres à ionisation à dépôt de bore. Les capteurs CNP sont au nombre de huit : quatre sont installés en partie basse de cuve et quatre sont installés en partie haute de cuve. Les capteurs CNP sont installés dans des tubes guides noyés dans le béton de la protection biologique et sont disposés en pourtour de la cuve. Ces capteurs font partie du système RPN (Réacteur Puissance Nucléaire) et sont présentés dans la section 7.5.3 du RDS. Ils sont polarisés en tension et fournissent un courant dépendant du nombre de neutron capturés.

Ces signaux sont alors conditionnés et isolés par les armoires RPN. Les signaux sont alors transmis à différents systèmes dont le système de détection des corps migrants (KIR). Les signaux sont filtrés, les parties variables de ces signaux sont ensuite amplifiées.

La baie de surveillance primaire réceptionne les signaux dans des cartes d'acquisitions. Ces cartes sont reliées au PC de la baie de surveillance primaire et permettent l'interprétation des composantes fréquentielles des signaux RPN en vibration des internes de cuve dans la bande de fréquence [1Hz ; 50Hz]. Ces données sont enregistrées et permettent un suivi de l'état des internes de cuve.

Les caractéristiques électriques de ces capteurs sont présentées en paragraphe 7.5.3 du RDS.

4. SURVEILLANCE VIBRATOIRE DES GROUPES MOTOPOMPES PRIMAIRES (SPP)

4.1. PRESENTATION DE LA SURVEILLANCE VIBRATOIRE DES GMPP

La prise en compte du retour d'expérience sur le parc et des études réalisées sur l'EPR ont conduit à la mise en place d'une surveillance vibratoire des Groupes Motopompes Primaires. Elle concerne la ligne d'arbre et la bride de support moteur.

Elle permet de disposer de bilans suffisamment complets. Les mesures relatives aux niveaux vibratoires, les températures des paliers, et dans certains cas des débits de fuite des joints, fournit une bonne connaissance qualitative de l'état de la ligne d'arbre et permet d'identifier les matériels sur lesquels intervenir prioritairement. En plus des moyens de détection spécifiques, une telle surveillance permet une détection précoce de certains types d'anomalies (détérioration des paliers et butées ou du palier hydrostatique, érosion de la roue par cavitation, détérioration des joints d'arbre, etc.) et une optimisation des périodicités de maintenance.

L'historique des paramètres des GMPP enregistré par la SPP et ses possibilités en matière d'analyse harmonique permet d'effectuer un diagnostic et d'identifier la cause d'une anomalie.

La SPP permet également de surveiller en continu le débit primaire, pendant les essais à chaud grâce à une mesure en absolu, puis pendant le fonctionnement de la tranche.

4.2. ELEMENTS CONSTITUTIFS DE LA CHAINE DE MESURE POUR LA SURVEILLANCE VIBRATOIRE DES GMPP

Les capteurs de vibration et de déplacement utilisés pour la surveillance vibratoire des GMPP permettent la surveillance du déplacement relatif de l'arbre par rapport à la carcasse et les vibrations de la carcasse elle-même. Ces données sont utilisées par la Baie de Surveillance Primaire afin de suivre l'état des GMPP sur le long terme.

Au total 10 capteurs de déplacements ou de vibrations sont utilisés :

- 2 capteurs de déplacement radial d'arbre côté accouplement moteur
- 2 capteurs de déplacement radial d'arbre manchon pompe
- 1 capteur de déplacement axial d'arbre côté capot volant moteur
- 1 capteur de phase côté accouplement moteur
- 2 capteurs de vibration carcasse palier inférieur moteur
- 2 capteurs de vibration carcasse palier supérieur moteur

Les capteurs de déplacements et le capteur de phase sont des capteurs à courant de Foucault. La mesure de l'impédance des capteurs varie en fonction de la distance d'entrefer : distance entre le capteur et l'arbre moteur.

Les capteurs de vibration sont des capteurs vélocimètres. Des vibrations dans l'axe longitudinal du capteur génèrent une tension induite en sortie du capteur. Les capteurs de vibration sont fixés sur la carcasse des GMPP.

Les capteurs de déplacement et de vibration utilisées pour la surveillance vibratoire des GMPP sont, par ailleurs, présentés dans le sous chapitre 5.4.1 du RDS.

Caractéristiques techniques :

- Gamme de mesure : 1500µm crête à crête
- Bande passante : [10Hz ; 1kHz]
- Tenue en température : [-30°C ; +200°C]
- Tenue aux radiations : 100kGy cumulé

Les caractéristiques techniques des capteurs à courant de Foucault choisis (capteur de déplacement) sont les suivantes.

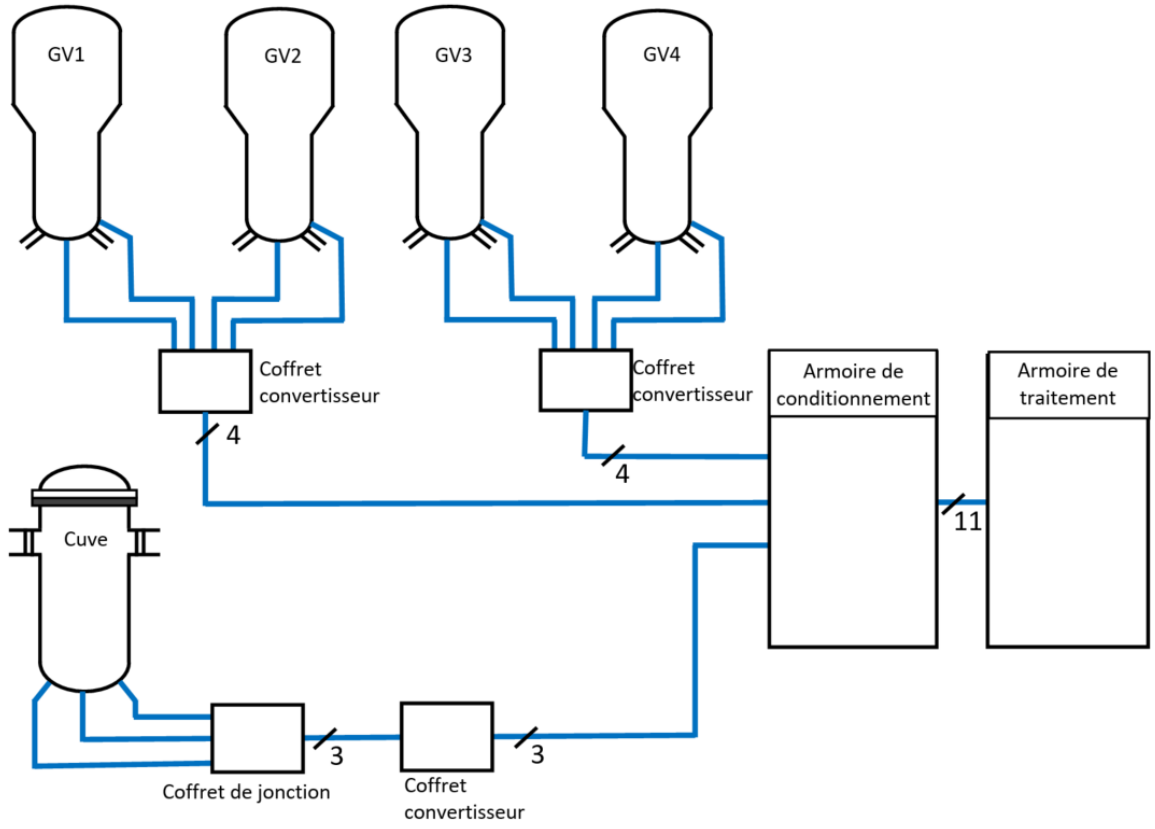
Pour le capteur de déplacement axial de l'arbre moteur :

- Gamme de mesure : [200µm ; 4000µm]
- Bande passante : [0Hz ; 10kHz]
- Tenue en température : [-30°C ; +170°C]
- Tenue aux radiations : 500kGy cumulé

Pour les capteurs de déplacement radial manchon pompe, accouplement moteur et capteur de phase :

- Gamme de mesure : [100µm ; 2000µm]
- Bande passante : [0Hz ; 10kHz]
- Tenue en température : [-30°C ; +170°C]
- Tenue aux radiations : 500kGy cumulé

FIG–7.5.6.1 PRÉSENTATION DE LA CHAINE DE MESURE DES SIGNAUX DE DÉTECTION DE CORPS MIGRANTS



SOMMAIRE

.7.5.7 SURVEILLANCE DES RAYONNEMENTS

1. MISSIONS DE SÛRETÉ

La conception du système KRT (système classé de sûreté) est traitée en section 9.5.7.1. La conception du système KRC (système non classé de sûreté) est traitée en paragraphe 4 du sous-chapitre 12.3.

La fonction de surveillance des rayonnements, hors radioprotection du personnel d'exploitation, étant supportée par le système KRT à l'intérieur de la centrale, toutes les missions de sûreté, les critères fonctionnels et les exigences de conception sont décrits précisément dans la section 9.5.7.1 "Surveillance de la tranche et du BTE" du rapport de sûreté pour la demande de mise en service.

2. FONCTIONS

L'instrumentation des rayonnements ionisants contribue :

- à la radioprotection du personnel d'exploitation et de la population environnante,
- au contrôle de la tranche en complément des mesures de contrôle conventionnelles, c'est-à-dire des mesures non radiologiques, pendant le fonctionnement autorisé (fonctionnement normal et transitoires courants prévus) et les situations accidentelles éventuelles.

Le concept de surveillance est basé sur :

- un contrôle continu au sein de la centrale par l'instrumentation de mesure installée de manière permanente, les capteurs fournissant des informations sur l'état de la centrale en conditions normales, incidentelles et accidentelles, avec enregistrement des données appropriées pour initier, en cas de besoin, des actions automatiques ou manuelles, lorsque des seuils sont dépassés,
- un contrôle périodique au sein de la centrale par prélèvement d'échantillons de mesure et leur analyse ultérieure en laboratoire,
- une surveillance générique réalisée par des équipements de mesure fixes ou mobiles.

Ces mesures sont complétées à l'aide de dispositifs de mesure fixes, portatifs ou mobiles pour la surveillance de la contamination du personnel et des zones de travail.

Ces fonctions sont réparties comme suit :

- la surveillance des circuits (surveillance de l'activité des liquides ou des gaz dans les systèmes),
- la surveillance des locaux (mesure de l'activité de l'air et surveillance du débit de dose local),
- la surveillance des effluents radioactifs (liquides ou gazeux),
- le contrôle du personnel,
- la surveillance de la contamination,
- la surveillance des déchets solides,
- la surveillance de l'environnement.

L'instrumentation de détection des rayonnements ionisants supporte des fonctions classées de sûreté jusqu'à F1A. (voir section 9.5.7.1 "KRT" et section 3.2.2 "Classement").

3. PRINCIPES DE MESURES ET DISPOSITIONS TYPES

Dans ce qui suit sont décrits les principes de mesure et les dispositions types applicables à l'instrumentation de détection des rayonnements ionisants installée de manière permanente pour la surveillance des systèmes et des effluents radioactifs.

Les dispositifs de mesures suivants liés à la gestion de la centrale ne sont pas traités ci-après :

- les appareils de mesure mobiles,
- le contrôle du personnel,
- la surveillance de la contamination,
- la surveillance des déchets solides,
- la surveillance de l'environnement et,
- les laboratoires radiologiques.

Les tâches requises pour le contrôle des rayonnements en continu dans une centrale nucléaire sont réalisées selon des méthodes comportant la mesure du rayonnement bêta ou gamma.

Les nucléides qui émettent des rayons alpha étant rares, comparés aux nucléides qui émettent des rayons bêta ou gamma, ne sont pas représentatifs de la radioactivité émise dans la centrale.

En outre, en raison de son extrême absorption, le rayonnement alpha ne conviendrait pas pour effectuer le contrôle continu de la radioactivité présente ou dégagée dans la centrale.

Un nombre réduit de dispositifs de mesures, basé autant que possible sur des composants standards, est utilisé. Chaque fois que cela est possible et adapté, des matériels standards sont privilégiés. Cette stratégie permet l'utilisation de technologies fiables et éprouvées et permet également d'optimiser l'entretien et le renouvellement progressif des matériels.

Les dispositifs installés de manière permanente pour la surveillance continue en centrale comprennent les composants suivants :

- un détecteur,
- un pot de mesure (si requis),
- une protection contre le rayonnement (si nécessaire),
- une structure de supportage,
- des câbles et des connecteurs,
- un transducteur,
- un module de traitement du signal,
- un système de test avec une source radioactive.

Ces points de mesure sont complétés par des dispositifs qui assurent un prélèvement permanent d'échantillons du milieu surveillé pour des analyses périodiques dans un laboratoire radiochimique.

Le choix des matériels prend en compte :

- les aspects radiologiques, par exemple : la mesure des activités (quantité ou concentration) ou du débit de dose,
- le milieu à surveiller (liquide ou gazeux),
- le type de rayonnement (bêta ou gamma),
- les conditions de la centrale (en fonctionnement, à l'arrêt, états perturbés, accidents).

En ce qui concerne les différents composants de la chaîne de mesure, le choix est déterminé sur la base des critères suivants :

- La précision requise des signaux de mesure selon les bandes de fonctionnement et les conditions ambiantes (ex : la température, l'humidité, la pression, le débit de dose local, les efforts dus au séisme) pendant le fonctionnement,
- le temps de réponse requis,
- la gamme de mesure requise,
- le seuil de détection requis,
- la gamme d'énergie spécifiée.

Une bonne pratique afin de réduire les défauts de mode commun, est le choix de composants diversifiés pour les chaînes de mesure redondantes (KRT APG-RES/KRT VVP) sauf quand le choix de la technologie ne le permet pas. Les critères de choix des composants de l'instrumentation de radioprotection prennent en compte le nécessaire respect des exigences d'assurance qualité. Les composants privilégiés sont ceux qui bénéficient d'un bon retour d'expérience en centrales nucléaires.

3.1. DÉTECTEURS

Les détecteurs généralement utilisés pour les mesures bêta et gamma sont les suivants :

- des chambres d'ionisation,
- des semi-conducteurs,
- des détecteurs à scintillation (peu utilisés pour les béta).

Si nécessaire, un préamplificateur pour la transmission des impulsions est incorporé ou situé à proximité du détecteur. Un étage de puissance est intégré, s'il ne fait pas déjà partie du transducteur.

Les détecteurs sont en général situés à côté ou à l'intérieur d'un pot de mesure ou d'une unité de filtration ou - en cas de mesure du débit de dose - installés sur le mur du bâtiment.

Les détecteurs sont montés de manière à ce qu'ils soient facilement accessibles pour les inspections périodiques en service. S'il n'existe pas de contraintes contraires plus importantes, la hauteur maximale d'installation est de [] m [].

Les détecteurs pour la mesure locale du débit de dose sont installés de façon qu'ils effectuent une surveillance représentative de la zone concernée.

Tous les autres détecteurs sont préférentiellement installés dans des pièces avec un très bas niveau de rayonnement (en général inférieur au seuil de [] Gy/h) afin de respecter les limites inférieures requises de détection.

3.1.1. Mesures de rayonnement bêta

Pour la surveillance des rayons bêta, on utilise des détecteurs qui ont une réponse spectrale faible vis-à-vis du rayonnement gamma par rapport au rayonnement bêta afin que cette influence soit négligeable dans la plupart des mesures. En outre, les détecteurs qui n'ont pas besoin pour leur fonctionnement de moyens auxiliaires tels que des gaz de comptage – comme, par exemple, pour les compteurs proportionnels de débit –, sont privilégiés.

3.1.2. Mesures de rayonnement gamma

Le contrôle des rayonnements gamma vis-à-vis de la surveillance en continu de la centrale revêt une importance particulière sur les sites nucléaires. En effet, il permet de surveiller les fluides radioactifs dans les tuyauteries et les réservoirs au moyen de détecteurs gamma installés à l'extérieur. Ainsi la contamination du détecteur ou son exposition à une pression élevée est évitée et son exposition à des températures élevées reste limitée :

- Les chambres d'ionisation sont principalement utilisées pour les mesures de débit de dose. Leur conception robuste capable de résister aux effets de l'environnement (ex: la température, l'humidité, les vibrations) et/ou leur large gamme de mesure permettent de les utiliser pour diverses applications.
- Les semi-conducteurs sont utilisés pour la surveillance spécifique de nucléides.
- Les compteurs à scintillation permettent de séparer l'énergie des particules incidentes selon un spectre correspondant à la sensibilité du photomultiplicateur associé. Ils sont employés pour la surveillance des liquides, des aérosols et de l'iode avec une limite basse de détection.

3.2. POTS DE MESURE

L'utilisation de pots de mesure dépend largement des conditions de mesure. Les raisons de l'utilisation d'un pot de mesure peuvent être :

- d'éviter la contamination du détecteur par le contact direct avec le milieu à surveiller (ex : l'eau),
- la nécessité d'un espacement entre le détecteur et le milieu surveillé, assurant de ce fait un calibrage constant de ce type d'appareil de mesure.

Les pots avec des détecteurs à l'extérieur et les dispositions de mesures où le détecteur est installé dans le milieu à contrôler sont deux solutions possibles.

La conception des pots de mesure prend en compte les critères suivants :

- la fabrication mécanique pour faciliter la manutention, l'installation et le remplacement,
- la compatibilité avec les matériaux et les conditions des systèmes à surveiller,
- la minimisation de l'absorption du rayonnement dans la direction du détecteur,
- les dispositions facilitant la décontamination, par exemple la non-rugosité des surfaces et l'utilisation de revêtement décontaminable,
- la minimisation des bras morts,
- la réduction des dépôts contaminés par une forme adéquate de l'intérieur du pot, par exemple en évitant les bavures et les cordons de soudure.

Les grands pots de mesure permettent d'améliorer la sensibilité globale de la mesure. Cependant les dimensions restent habituellement limitées, en raison :

- du coût croissant de la protection,
- de la dépendance croissante de la mesure à l'énergie, provoquée par l'absorption propre,
- de l'interaction avec le milieu, entraînant de ce fait un retard dans la mesure.

Pour la mesure du rayonnement bêta des gaz rares, le volume de mesure est fonction de l'absorption des rayonnements bêta de moyenne énergie dans l'air avec une épaisseur de saturation d'environ [] millimètres. L'enveloppe de protection a une épaisseur limitée afin de réduire l'absorption à un minimum.

Dans la plupart des cas, la limite de détection inférieure exigée pour les concentrations des aérosols radioactifs ou de l'iode ne peut pas être atteinte par la mesure directe. Dans ces cas, les pots de mesure contiennent une cartouche filtrante au travers de laquelle passe un échantillon d'air surveillé. Les dimensions et le matériau du filtre sont appropriés à cette tâche. L'activité sur le filtre est contrôlée par un détecteur à l'intérieur du pot à proximité ou à l'intérieur du filtre, ou en laboratoire (chaînes cheminée).

Des pots de mesure pour la surveillance des liquides sont conçus de telle sorte que les dépôts et la contamination sont réduits au minimum. Ils sont construits de façon à éviter la présence de bulles d'air dans le volume surveillé.

Des pots de mesure ne sont pas nécessaires dans des cas où la surveillance a pour unique but de détecter la présence de radioactivité, c'est-à-dire. s'il n'y a aucun besoin à traiter les données pour fournir l'activité spécifique en Bq/m ^{3}. Dans ces cas, le détecteur est monté à l'extérieur du système sans pot de mesure spécifique.

Aucun pot n'est également utilisé pour les mesures de débit de dose locales.

3.3. PROTECTION CONTRE LES RAYONNEMENTS

En fonction de la mesure effectuée, on emploie une protection de plomb qui entoure le détecteur avec uniquement une ouverture entre le détecteur et le volume à mesurer.

Des protections de plomb sont utilisées où cela est nécessaire pour respecter le seuil bas de détection exigée dans les situations de fonctionnement correspondantes. Une telle protection de plomb entoure à la fois le pot et le détecteur de mesure ou seulement le détecteur. L'épaisseur de la protection permet un faible niveau de détection compte tenu du bruit de fond local et sa variation et fait au moins [] centimètres.

La conception d'une protection de plomb doit prendre en compte :

- les contrôles en service et l'entretien de l'appareil de mesure qui doivent être exécutés,
- la décontamination qui doit être facile, en évitant des surfaces rugueuses et en utilisant un revêtement décontaminable.

3.4. TRANSDUCTEURS

Les signaux du détecteur (sous forme d'impulsions ou de courants) sont traités dans des transducteurs, de conception modulaire. Les transducteurs restituent les états réels et les valeurs mesurées.

Selon la mesure à effectuer et les longueurs de câbles nécessaires, les transducteurs sont soit montés dans des coffrets individuels soit regroupés ensemble dans des armoires en tenant compte des critères de redondance.

3.5. DISPOSITIFS PERMANENTS DE PRÉLÈVEMENT

Indépendamment des moyens de contrôle en continu décrits plus haut, les principes de surveillance de la radioactivité incluent une surveillance périodique basée sur la prise d'échantillons qui sont ensuite analysés en laboratoire radio-chimique. Sur demande, tout ou partie de ces échantillons peuvent être stockés comme élément de preuve. L'analyse par le laboratoire est exécutée de façon périodique ou sur demande.

Les échantillons sont prélevés de manière discontinue ou continue.

Dans la plupart des cas, des dispositifs de prélèvement en continu sont placés dans un circuit de by-pass du système surveillé. Les milieux contenant des nucléides à surveiller sont collectés dans un filtre adapté ([]) ou par un absorbant adapté (ex : Tritium et CO_2 dans l'air) ou dans des bouteilles ([]).

4. EXIGENCES COMMUNES AUX ZONES RADIOACTIVES

Les matériaux mis en œuvre doivent répondre aux exigences suivantes :

- la résistance au rayonnement,
- une finition extérieure adaptée pour réduire autant que possible les problèmes de contamination,
- les matériaux qui sont difficiles à décontaminer seront évités au maximum,
- le choix des matériaux pour les composants nécessitant un remplacement doit être fait afin de réduire le débit de dose pendant la maintenance,

- la résistance aux conditions ambiantes maximales durant le fonctionnement (humidité, température, vapeur, eau, etc.),
- les matériaux ferritiques non protégés (dans les systèmes de ventilation, les systèmes de mélange d'air, etc ...) seront évités dans les utilisations où un détachement et une dispersion d'oxydes peuvent se produire,
- les matériaux ou revêtements susceptibles d'être contaminés au cours des arrêts de tranche devront être facilement décontaminables.

SOMMAIRE

.7.5.8 INSTRUMENTATION ACCIDENTELLE

1. DÉFINITION

L'instrumentation accidentelle fournit des informations sur tous les systèmes de sauvegarde impliqués dans la sûreté de l'installation et sur les paramètres de l'environnement de l'installation afin de réaliser les actions requises et de maîtriser l'accident.

2. FONCTIONS

Le concept de surveillance distingue :

- le contrôle continu au sein de l'installation au moyen d'un équipement de mesure installé de manière permanente. Cet équipement fournit des informations pour :
  - la surveillance de l'installation en condition normale, incidentelle et accidentelle,
  - la documentation sur les informations appropriées et l'initiation des actions,
  - les alarmes pour le déclenchement des actions [], quand les valeurs seuils sont dépassées.
- la surveillance discontinue au sein de l'installation par échantillonnage et évaluation en laboratoire.

Les fonctions de surveillance conduisent aux tâches de mesure et de contrôle suivantes :

- fournir des informations sur les paramètres procédés nécessaires pour permettre au personnel de la salle de commande de réaliser les actions [] de protection spécifiées dans les procédures accidentelles,
- fournir des informations sur les paramètres procédés pour vérifier que les actions sûreté requises sont en cours,
- fournir des informations sur les paramètres procédés pour signaler le risque de perte d'intégrité ou la perte effective des barrières de confinement vis-à-vis des rejets radioactifs,
- fournir des informations sur les paramètres procédés pour indiquer les opérations en cours sur les systèmes de sauvegarde et les autres systèmes impliqués dans la sûreté de l'installation,
- fournir des informations sur les paramètres entraînant l'activation automatique des systèmes de protection et l'état des signaux de protection afin de permettre une activation [] de ces systèmes si l'activation automatique n'a pas fonctionné,
- fournir des informations sur la disponibilité des autres systèmes de sauvegarde, par exemple ceux qui pourraient être nécessaires ultérieurement lors de la mitigation de l'accident, afin de réaliser des actions adaptées en temps voulu.

Les équipements de mesure des rejets radioactifs et des conditions météorologiques fournissent des informations permettant une évaluation de l'état radiologique de l'installation en fonctionnement normal, pendant et après des situations accidentelles, et permettant d'aider à déterminer le niveau des rejets radioactifs.

3. PRINCIPES DE MESURE ET EXIGENCES

3.1. DISPOSITIONS TYPIQUES

Afin de satisfaire ces différentes tâches, les principes de mesure élémentaires et les dispositions typiques suivantes sont appliquées :

- une surveillance du procédé conçue pour résister aux conditions incidentelles et accidentelles dans les différentes zones affectées par l'accident (par exemple la température, la pression, le niveau, le débit ; analyse des gaz et des liquides, flux de neutron, position de vanne),
- une surveillance du procédé par l'instrumentation utilisée en fonctionnement normal qui n'est pas affectée par les conditions incidentelles ou accidentelles, et qui reste ainsi disponible pendant la séquence accidentelle,
- une surveillance des différentes zones intérieures et extérieures enceintes (par exemple la température, la pression, la radioactivité, l'analyse des gaz et liquides),
- une surveillance de la zone géographique proche de la centrale (par exemple l'émission des effluents liquides radioactifs, des gaz, du taux local de particules dans l'atmosphère, des paramètres météorologiques).

3.2. EXIGENCES SUR LES SONDES ET LES CAPTEURS

En plus des exigences de sûreté générales liées au classement, au critère de défaillance unique, aux essais périodiques, et aux conséquences des agressions internes et externes (section 7.5.0 et Directives Techniques G.3), des exigences spécifiques sur les sondes et les capteurs sont rappelées :

- Le temps de réponse et la précision des capteurs répondent aux exigences définies pour les conditions normales et accidentelles *ad hoc*.
- Les capteurs et les sondes sont montés de telle manière qu'ils sont facilement accessibles pour les inspections en service périodiques.
- Des prises de raccordement sont utilisées pour la connectique afin de faciliter l'entretien.

En outre, pour les sondes et les capteurs utilisés dans les zones où existent des conditions sévères en fonctionnement normal et/ou accidentel :

- Des sondes sans circuits électroniques sont privilégiées.
- Les conséquences de l'accident ne doivent pas impacter la précision exigée et le temps de réponse des sondes.
- Les capteurs sont utilisés si leurs composants électroniques répondent aux exigences sur les conditions d'environnement pendant et après un accident.
- Les positions des capteurs répondent aux exigences définies pour les conditions normales et accidentelles.

3.3. EXIGENCES LIÉES AUX PROCÉDURES ACCIDENTELLES

Les procédures accidentelles décrites dans le sous-chapitre 13.3 fournissent plusieurs stratégies opérationnelles dans le cadre de l'approche par état. En cohérence avec les fonctions de sûreté dans lesquelles l'instrumentation est directement impliquée (voir paragraphe 1 de la section 7.5.0), un diagnostic permanent des six fonctions d'état évalue l'état de l'installation afin de déterminer la stratégie de conduite appropriée à l'état de l'installation.

L'instrumentation nécessaire au diagnostic des fonctions d'état (décrite au sous-chapitre 13.3 du RDS) doit être classée au moins F1B.

SOMMAIRE

FIGURES :

.7.5.9 INSTRUMENTATION DU BORE

Sur l'EPR, la concentration en bore est mesurée dans le fluide primaire au niveau du circuit de contrôle volumétrique et chimique (RCV) et du circuit d'échantillonnage (REN).

Les paragraphes qui suivent présentent uniquement la station de boremètres (Boron Concentration Measurement System (BCMS)) qui permet de mesurer la concentration en bore dans le système RCV.

Le boremètre, utilisé sur le circuit d'échantillonnage du système REN pour mesurer la concentration en bore dans le circuit primaire est abordé dans la section 9.3.1.

Du fait de la conception du système, le système BCMS mesure directement la concentration en B-10 de la ligne de charge du système RCV et non sa concentration en bore totale. La concentration en bore totale est calculée par multiplication de la concentration en B-10 par le facteur de conversion d'enrichissement en B-10 du bore. Chaque fois que le terme « concentration en bore » est utilisé dans cette section, il s'agit de la concentration en B-10. Dans le cas contraire, cela sera explicitement mentionné.

0. EXIGENCES DE SÛRETÉ

0.1. FONCTIONS DE SÛRETÉ

0.1.1. Contrôle de la réactivité

La contribution du système au contrôle de la réactivité doit être la suivante :

- fournir des mesures de la concentration en bore dans la ligne de charge du système RCV, dans certaines conditions de fonctionnement de catégorie PCC-2.

0.1.2. Évacuation de la puissance résiduelle

Le système BCMS ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.1.3. Confinement des substances radioactives

Le système BCMS ne contribue pas directement au confinement des substances radioactives.

0.1.4. Contributions indirectes aux fonctions de sûreté

Sans objet.

0.1.5. Contributions spécifiques à la protection contre les agressions

Le système ne contribue pas spécifiquement à la protection contre les agressions.

0.1.6. Contributions à l'élimination pratique

La contribution du système BCMS à l'élimination pratique doit être la suivante :

- prévenir les dilutions hétérogènes en détectant les bouchons d'eau claire.

0.2. CRITÈRES FONCTIONNELS

Au titre de ses contributions à l'accomplissement des fonctions de sûreté, le système doit satisfaire les critères fonctionnels suivants :

0.2.1. Contrôle de la réactivité

- mesures de la concentration en bore :
  Le système BCMS doit fournir, dans la plage attendue, dans les temps de réponse et les précisions requises, des mesures de concentration en bore dans la ligne de charge du système RCV, en PCC-2 afin de respecter les critères d'acceptabilité de ces études (cf. sous-chapitre 15.1).

0.2.2. Évacuation de la puissance résiduelle

Le système BCMS ne contribue pas directement à l'évacuation de la puissance résiduelle.

0.2.3. Confinement des substances radioactives

Le système BCMS ne contribue pas directement au confinement des substances radioactives.

0.2.4. Contributions indirectes aux fonctions de sûreté

Sans objet.

0.2.5. Contributions à l'élimination pratique

Le système BCMS doit détecter, dans les temps de réponse et les précisions requises, les bouchons d'eau claire pouvant se former dans la ligne de charge du système RCV.

0.3. EXIGENCES RELATIVES A LA CONCEPTION

0.3.1. Exigences issues du classement de sûreté

0.3.1.1. Classement de sûreté

Les parties du système BCMS jouant un rôle vis-à-vis de la sûreté doivent faire l'objet d'un classement de sûreté conformément aux règles de classement indiquées en section 3.2.1.

0.3.1.2. Critère de Défaillance Unique (active et passive)

Les fonctions du système BCMS classées F1 doivent être robustes à l'application du critère de défaillance unique.

0.3.1.3. Alimentation électrique de secours

L'alimentation électrique des composants du système BCMS nécessaire à l'accomplissement des fonctions classées F1 doit être secourue par les groupes diesels principaux.

0.3.1.4. Séparation physique / géographique

Les fonctions classées F1 du système BCMS doivent être conçues conformément à l'exigence de séparation physique/géographique de leurs équipements redondants constitutifs :

- séparation physique et électrique des chaînes de mesure redondantes (fonction F1A).

0.3.1.5. Qualification aux conditions accidentelles

Les équipements classés du système BCMS doivent être qualifiés en fonction des conditions de fonctionnement danslesquelles ils sont sollicités au titre de leur contribution à l'accomplissement des fonctions de sûreté, conformément aux règles du sous-chapitre 3.7.

0.3.1.6. Classement ESPN, mécanique, électrique, Contrôle-Commande et sismique

Les équipements du système BCMS redevables d'un classement mécanique, électrique, contrôle-commande et sismique doivent être classés conformément aux règles de classement présentées dans la section 3.2.1.

Le système BCMS n'est pas concerné par le classement ESPN car le système n'est pas soumis à la pression.

0.3.2. Exigences réglementaires

0.3.2.1. Textes réglementaires

Parmi l'ensemble des exigences issues des textes réglementaires présentés dans la section 1.7.0 du Rapport de Sûreté,

0.3.2.1.1. Textes officiels

Le système BCMS est concerné spécifiquement par le texte officiel suivant :

- décret n° 2007-534 du 10 avril 2007 autorisant la création de l'installation nucléaire de base dénommée Flamanville 3, comportant un réacteur nucléaire de type EPR, sur le site de Flamanville (Manche)
  l'exigence applicable à l'instrumentation concerne l'index III.1.1.1a :
  Tant qu'un assemblage de combustible est présent dans la cuve, la concentration de l'eau du circuit primaire en absorbant neutronique soluble est surveillée en permanence.

0.3.2.1.2. Prescriptions techniques

Le système BCMS est concerné spécifiquement par la prescription technique suivante :

- prescription INB167-18 : « Une station de mesure de la concentration de l'eau en absorbant neutronique soluble, classée F1A, détecte les dilutions hétérogènes ou homogènes incontrôlées se produisant dans le circuit RCV de contrôle chimique et volumétrique de l'eau du circuit primaire ; cette station est installée au refoulement des pompes de charge, sur un tronçon commun de la ligne de charge et de la ligne d'injection aux premiers joints des groupes motopompes primaires. Cette station génère un signal également classé F1A qui déclenche automatiquement le basculement de l'aspiration des pompes de charge du circuit RCV sur le réservoir IRWST et l'isolement de la ligne d'aspiration du réservoir de contrôle volumétrique du circuit RCV. »

0.3.2.1.3. Réglementations internationales

Le système BCMS n'est pas concerné par une réglementation internationale spécifique.

0.3.2.2. Textes para-réglementaires

0.3.2.2.1. Règles fondamentales de sûreté

Le système BCMS n'est pas concerné par une règle fondamentale de sûreté spécifique.

0.3.2.2.2. Directives techniques

Le système BCMS est concerné par les sections suivantes des Directives Techniques (voir les sections ci-dessous extraites de la section 1.7.0 du Rapport De Sûreté) :

- section B.2.3.1 – fonction de contrôle de la réactivité :
  « Concernant les dilutions du bore homogènes, le concepteur doit étudier la mise en place de l'activation de l'arrêt d'urgence ou d'un système de borication au moins pour les transitoires de référence de dilution homogène »
  « En tout état de cause, la fiabilité de la fonction d'arrêt d'urgence doit être suffisamment élevée pour contribuer à « pratiquement éliminer » les séquences de fusion du cœur à haute pression. Nonobstant le rôle du système de borication supplémentaire, des moyens adéquats doivent être mis en œuvre dans cet objectif, tels qu'une diversification des composants principaux du système

d'arrêt d'urgence (mesures physiques, signaux et traitements associés, disjoncteurs d'arrêt d'urgence) ».

- section G3 – conception du contrôle-commande :
  Cette section précise les exigences relatives à l'instrumentation et au contrôle-commande.
  Les exigences applicables à l'instrumentation concernent :
  - le classement fonctionnel de l'instrumentation,
  - la prise en compte du critère de défaillance unique, de la maintenance et de la séparation physique,
  - la prise en compte des conséquences des agressions internes et externes sur le contrôle-commande.

- section E2.2.2 – prévention des accidents d'injection rapide de réactivité :
  « Il est souligné que la mise en place d'un basculement automatique classé F1A de l'aspiration des pompes de charge du système de contrôle volumétrique et chimique (RCV) au réservoir d'eau interne à l'enceinte de confinement en cas de détection d'un débit dilué par un boremètre unique F1A, composé d'une source de neutrons et de quatre détecteurs de flux, serait une mesure de conception positive pour limiter les conséquences des dilutions provenant des lignes RCV. Cependant, la possibilité de classer le boremètre F1A doit être établie. »

0.3.2.3. Textes EPR spécifiques

Le système BCMS n'est pas concerné par un texte spécifique EPR.

0.3.3. Agressions

0.3.3.1. Agressions internes

Les fonctions du système BCMS doivent être protégées vis-à-vis des conséquences des agressions internes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.4.

0.3.3.2. Agressions externes

Les fonctions du système BCMS doivent être protégées vis-à-vis des conséquences des agressions externes si leur perte remet en cause l'atteinte des objectifs de sûreté du sous-chapitre 3.3.

0.3.4. Diversification

Le système ne fait pas l'objet d'une exigence de diversification.

0.3.5. Radioprotection

Le système BCMS n'est pas concerné par une exigence de radioprotection.

0.3.6. Exigences liées au fonctionnement, à la maintenance et à l'accessibilité long terme

Le système BCMS n'est pas concerné par une exigence liée au fonctionnement, à la maintenance et à l'accessibilité long terme dans la gestion long terme après accident.

0.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

0.4.1. Essais de démarrage

Le système BCMS doit être conçu pour permettre la réalisation d'essais de démarrage permettant de s'assurer de sa conception adéquate et de ses performances, et notamment du respect des critères fonctionnels qui lui sont assignés au § 0.2..

0.4.2. Surveillance en exploitation

Le système BCMS doit être conçu pour permettre une surveillance en exploitation normale des caractéristiques du système nécessaires à l'accomplissement de ses missions de sûreté afin d'assurer le bon comportement de ses composants et leur disponibilité en fonctionnement normal, incidentel et accidentel.

0.4.3. Essais périodiques

Les parties classées du système BCMS doivent être conçues pour permettre la réalisation d'essais périodiques conformément aux règles définies dans le chapitre IX des Règles Générales d'Exploitation.

0.4.4. Maintenance

Le système BCMS doit être conçu pour permettre la mise en œuvre d'un programme de maintenance conformément au chapitre VIII des RGE.

1. RÔLE DU SYSTÈME

Le système BCMS assure les fonctions opérationnelles suivantes dans les différentes conditions de fonctionnement de l'installation dans lesquelles il est sollicité :

1.1. RÔLE DU SYSTÈME PENDANT L'EXPLOITATION NORMALE DE LA TRANCHE

Le système BCMS n'a pas de rôle opérationnel en fonctionnement normal de la tranche.

1.2. RÔLE DU SYSTÈME DANS DES CONDITIONS DE FONCTIONNEMENT PCC2 A PCC4, RRC-A, EN ACCIDENT GRAVE ET SITUATIONS AGRESSIONS

Le système BCMS fournit dans les conditions de fonctionnement PCC2, des signaux destinés aux fonctions de protection du cœur.

2. BASES DE CONCEPTION

2.1. HYPOTHÈSES GÉNÉRALES DE FONCTIONNEMENT

Les critères de dimensionnement du système BCMS sont principalement les suivants :

- disponibilité des fonctions classées de sûreté lors d'une défaillance ou lors des opérations de maintenance.

Pour répondre à ces critères, le système BCMS est dimensionné comme suit :

- indépendance électrique entre les quatre redondances pour traiter les fonctions classées et maintenir ainsi une redondance en cas de défaillance unique cumulée avec la maintenance d'un équipement.

2.2. HYPOTHÈSES DE DIMENSIONNEMENT

2.2.1. Contrôle de la réactivité

Mesures de la concentration en bore :

Les mesures du boremètre sont requises pour les états de fonctionnement A à E de la tranche (états définis dans la section 15.0.1). Pendant ces états, le système RPR est en fonctionnement normal. L'état F (arrêt à froid avec le cœur totalement déchargé) n'est pas pris en compte pour l'analyse de sûreté.

Plage de concentration en bore

La plage de concentration en bore est appropriée pour prévenir les accidents de dilution homogène et hétérogène.

[]

Temps de réponse

Le temps de réponse du système BCMS est approprié pour prévenir les accidents de dilution homogène et hétérogène.

[]

Précision

La précision du système BCMS est appropriée pour prévenir les accidents de dilution homogène et hétérogène.

[]

2.2.2. Évacuation de la puissance résiduelle

Le système BCMS ne contribue pas directement à l'évacuation de la puissance résiduelle.

2.2.3. Confinement des substances radioactives

Le système BCMS ne contribue pas directement au confinement des substances radioactives.

2.2.4. Contributions indirectes aux fonctions de sûreté

Sans objet.

2.2.5. Contributions à l'élimination pratique

Seuil minimum de détection :

Le seuil minimum est approprié pour prévenir les accidents de dilution hétérogène.

Le système BCMS est capable de détecter des bouchons d'eau claire d'un volume supérieur ou égal à 2 m^3, qui est le volume retenu pour les études effectuées dans le cadre de l'élimination pratique (voir section 19.2.4).

[]

3. DESCRIPTION - FONCTIONNEMENT

3.1. DESCRIPTION

3.1.1. Description générale du système

Le système BCMS est conçu pour mesurer la concentration en bore dans le système RCV pour un traitement ultérieur par le système de protection (RPR). Les quatre appareils de mesure, de conception identique, sont installés sur la ligne de charge du système RCV tandis que les composants de contrôle commande sont séparés et répartis entre quatre divisions (voir figure FIG–7.5.9.2). La figure FIG–7.5.9.1 donne un aperçu des différents composants du système BCMS.

Les valeurs mesurées sont traitées par les fonctions « anti-dilution » du système RPR. Les valeurs mesurées et les informations d'état sont transférées par le système RPR pour un traitement ultérieur (affichage) au MCP et au MCS.

3.1.2. Description des matériels principaux

Le système BCMS est constitué des matériels principaux suivants :

3.1.2.1. Détecteurs

Le système BCMS est constitué de deux conteneurs comportant chacun deux détecteurs de neutrons. Le cadmium est utilisé pour le blindage neutronique à l'intérieur du conteneur et une source de neutrons est nécessaire pour la mesure. Les détecteurs de neutrons sont des tubes compteurs à dépôt de bore [].

3.1.2.2. Structure mécanique du système

Le système BCMS est constitué de plusieurs composants dans différentes salles et bâtiments. Le système BCMS comporte principalement les composants suivants :

- un dispositif de fixation des détecteurs (conteneur) dans le bâtiment combustible (BK) monté sur la ligne de charge du système RCV, en amont de la connexion de la ligne d'injection au jointn°1 des GMPP et en aval de la ligne de contournement des pompes du système,RCV,
- une source de neutrons et deux détecteurs de neutrons installés dans chacun des deux conteneurs,
- une unité de conditionnement des signaux des détecteurs (installé dans les armoires électroniques du système RPN),
- une unité de traitement des données (appartenant au système RPR).

3.1.2.3. Systèmes de Contrôle Commande en interface

Systèmes serveurs du système BCMS :

- le système RPN amène l'alimentation au BCMS,
- la mesure de température utilisée pour la compensation des effets de la température du fluide sur le taux de comptage fait partie du système RCV et est traitée par le système RPR.

Systèmes servis par le système BCMS :

- système RPR.

3.1.3. Description des dispositions d'installations principales

Les conteneurs du système BCMS se trouvent dans le bâtiment combustible (BK). Du fait de la conception du système RCV, tous les appareils de mesure BCMS sont installés sur le même tronçon de conduite. Les deux conteneurs sont installés sur la ligne de charge du système RCV en amont de la connexion de la ligne d'injection au jointn°1 des GMPP et en aval de la ligne de contournement des pompes du système RCV. La source de neutrons et les deux détecteurs sont fixés à des positions permettant d'obtenir une mesure optimisée (figure FIG–7.5.9.3).

L'électronique de conditionnement des impulsions est installée dans les armoires électroniques du système RPN dans les bâtiments de sauvegarde (BAS). Les signaux sont amplifiés et discriminés puis des impulsions standardisées sont transmises au module compteur de l'unité de traitement du système RPR.

3.2. FONCTIONNEMENT

3.2.1. Fonctionnement en régime normal de la tranche

En régime normal de la tranche, lorsque le système RCV est opérationnel, le système BCMS est en service continu.

Pour l'état F (arrêt à froid avec le cœur totalement déchargé) le système BCMS n'est pas requis. Il devient inopérant en mettant le point de consigne Haute Tension à 0 (en fixant le paramètre du logiciel) ou en coupant l'alimentation électrique. Il s'agit d'un arrêt se faisant division par division. Le logiciel du PS permet aussi d'inhiber le signal BCMS en fixant le paramètre correspondant.

3.2.2. Fonctionnement en régime permanent du système

Dans les conditions normales de fonctionnement, l'acquisition des données est effectuée périodiquement après le cycle de traitement du système RPR. Le réglage du cycle de traitement [] n'affecte ni la précision ni le temps de réponse du système BCMS.

[] Le calcul de la concentration en bore totale s'effectue en 4 étapes :

- compensation des effets de température,
- normalisation du taux de comptage,
- calcul de la concentration en bore 10 à partir du taux de comptage normalisé, pour envoi au RPR,
- conversion B-10/Bore enrichi, pour calcul de la concentration en bore totale et envoi au MCS.

Ainsi, le signal correspondant à la concentration en bore est donc mis à jour []. La valeur est ensuite traitée par le système RPR.

3.2.3. Fonctionnement en régime transitoire

Sans objet.

3.2.4. Autres régimes de fonctionnement du système

3.2.4.1. Fonctionnement dégradé du système

Défaillance de la totalité ou d'une partie du système

Une défaillance partielle ou totale du système BCMS est détectée à l'aide de fonction de surveillance de l'acquisition des signaux et en vérifiant que les signaux mesurés se trouvent dans la gamme attendue. En cas de défaillance détectée, une alarme est envoyée au MCP et au MCS. Ce message souligne que la concentration en bore calculée de la chaîne de mesure concernée n'est pas valide.

Les taux de comptage normalisé des quatre chaînes de mesure font l'objet d'une vérification de plausibilité vis-à-vis d'un seuil minimum et d'un seuil maximum. Si le taux de comptage est inférieur au seuil inférieur ou supérieur au seuil supérieur, une alarme est générée au niveau du système RPR et le signal de mesure est invalidé.

De même, la température fait l'objet d'une vérification de plausibilité vis-à-vis d'un seuil minimum et d'un seuil maximum, et le même type d'information est transmis au MCP et au MCS dans le cas où la température mesurée est inférieure au seuil inférieur ou supérieure au seuil supérieur. Le signal de mesure est aussi invalidé.

Une alarme est aussi générée et le signal de mesure est invalidé lorsque le signal « BCMS fault » venant des armoires de conditionnement est activé.

Par ailleurs, le signal est surveillé pendant le fonctionnement normal pour détecter les dégradations avant qu'elles ne provoquent de fausses valeurs de mesure. []

[]

Le signal BCMS est traité par le système RPR []. Dans le cas d'une défaillance de trois chaînes de mesure ou plus (ou si elles sont indiquées comme non valides), la fonction de protection anti dilution du système RPR est mise en œuvre.

Défaillance des systèmes en interface

Si l'alimentation électrique d'une division du système BCMS (c'est-à-dire celle du système RPN) tombe en panne, cette division cesse de fonctionner.

Si l'unité de traitement du système RPR tombe en panne, l'unité de conditionnement continue de fonctionner normalement. Néanmoins le calcul de la concentration en bore n'est alors plus possible.

Les dysfonctionnements du système RCV sont détectés par les mesures de débit. Si la ligne de charge du système RCV est vide, le système BCMS indique une erreur.

4. ANALYSE DE SÛRETÉ

4.1. CONFORMITÉ A LA RÉGLEMENTATION

Le système BCMS est conforme à la réglementation générale en vigueur (voir sous-chapitre 1.7) et ne fait pas l'objet de dérogations particulières.

4.2. RESPECT DES CRITÈRES FONCTIONNELS

4.2.1. Contrôle de la réactivité

Les études de transitoires incidentels/accidentels du sous-chapitre 15.2 faisant intervenir les fonctions du système BCMS correspondant aux critères fonctionnels énoncés au § 0.1.1. sont réalisées en considérant, pour les paramètres suivants, des valeurs cohérentes avec les hypothèses de dimensionnement énoncées au § 2.2. (cf. sous-chapitre 15.1) :

- plage de concentration en bore,
- temps de réponse,
- précision.

Pour les transitoires concernés, ces études (cf. section 15.2.2r) :

- présentent les effets de ces fonctions sur le déroulement du transitoire,
- montrent que le dimensionnement de ces fonctions est tel qu'il permet de contribuer au respect de leurs critères d'acceptabilité.

4.2.2. Evacuation de la puissance résiduelle

Sans objet.

4.2.3. Confinement des substances radioactives

Sans objet.

4.2.4. Contributions indirectes à l'accomplissement des fonctions de sûreté

Sans objet.

4.2.5. Contributions à l'élimination pratique

Les études d'élimination pratique de la section 19.2.4 faisant intervenir des fonctions du système BCMS sont réalisées en considérant, pour les paramètres suivants, des valeurs cohérentes avec les hypothèses de dimensionnement énoncées au **§ 2.2.** :

- seuil minimum de détection d'un bouchon d'eau claire
  Pour chaque transitoire concerné, ces études montrent que le dimensionnement de ces fonctions est tel qu'il permet d'éliminer pratiquement les situations concernées, à savoir la dilution hétérogène provenant du système RCV.
  Ces éléments permettent d'assurer le respect des critères fonctionnels énoncés au **§ 0.2.**.

4.3. CONFORMITÉ AUX EXIGENCES DE CONCEPTION

Le système BCMS est conforme aux exigences de conception évoquées au **§ 0.3.**, notamment pour ce qui concerne :

4.3.1. Exigences issues du classement de sûreté

4.3.1.1. Classement de sûreté

Les classements des équipements du système BCMS jouant un rôle vis-à-vis de la sûreté sont présentés dans la section 3.2.2.

4.3.1.2. Critère de défaillance unique (active et passive)

4.3.1.2.1. Défaillance unique active

La conception du système BCMS est conforme à l'exigence de robustesse au critère de défaillance unique active énoncée au **§ 0.3.**, notamment sur les points suivants :

- le câblage des détecteurs vers les bâtiments de sauvegarde (BAS) est réalisé en utilisant des chemins de câbles redondants,
- le dysfonctionnement d'un composant du système BCMS ne doit pas affecter le fonctionnement sûr de la tranche ou de tout système important pour la sûreté ; ceci est réalisé grâce à la séparation électrique et mécanique des quatre chaînes de mesure (la conception du système BCMS suit celle du système RPR). Chaque redondance est installée dans une division redondante des bâtiments de sauvegarde (BAS), [].

4.3.1.2.2. Défaillance unique passive

Sans objet.

4.3.1.3. Alimentation électriquede secours

L'électronique de conditionnement du système BCMS est installée dans les armoires du système RPN dont la conception est conforme à l'exigence de secours électrique énoncée au **§ 0.3.**, notamment sur les points suivants :

- En cas de Perte Totale des Alimentations Electriques Externes (MDTE), les armoires électriques sont secourues par les diesels principaux et par des batteries [] permettant la continuité d'alimentation pendant les transitoires de basculement des sources externes ou internes.

L'unité d'acquisition des impulsions est alimentée par du [].

Le traitement des signaux du BCMS est effectué dans le système RPR. L'unité de traitement des signaux (*"Signal processing"*) est installée dans une armoire [] et son alimentation respecte les normes applicables aux armoires [].

4.3.1.4. Séparation physique/géographique

La conception du système BCMS est conforme à l'exigence de séparation physique/géographique, notamment sur le point suivant :

- Les composants électroniques sont séparés géographiquement.
  []

4.3.1.5. Qualification aux conditions accidentelles

Les équipements du système BCMS à qualifier aux conditions accidentelles, sont présentés dans la section 3.7.1.1.2.

Remarque : la fonction du système BCMS est liée au circuit primaire, mais des conditions anormales dans le bâtiment réacteur (BR) ne conduisent pas à des conditions anormales dans le bâtiment combustible (BK).

4.3.1.6. Classement ESPN, mécanique, électrique, contrôle commande et sismique

La conformité des classements mécanique, électrique, contrôle-commande et sismique des équipements du système BCMS jouant un rôle vis-à-vis de la sûreté aux exigences énoncées au **§ 0.3.** est détaillée dans la section 3.2.2.

4.3.2. Exigences réglementaires

4.3.2.1. Textes réglementaires

La conformité aux textes réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.1.1. Textes officiels

Le système BCMS est en conformité avec les textes officiels spécifiques listés au **§ 0.3.2.**, comme spécifié dans le **§ 3.2.**.

4.3.2.1.2. Prescriptions techniques

La conformité aux prescriptions techniques spécifiquement applicables au système, listées au **§ 0.3.2.**, est présentée aux **§ 3.1.** et **§ 4.3.1.**. La conformité à la prescriptionINB167-18est également assurée par l'émission, en situations de dilutions homogènes ou hétérogènes dues à la défaillance du RCV, d'un signal F1A d' « anti-dilution » élaboré à partir des capteurs du système BCMS et après traitement des mesures au RPR. Ce signal isole, de manière F1A automatique, la ligne d'aspiration du réservoir de contrôle volumétrique du circuit RCV et initie le basculement automatique de l'aspiration des pompes de charge RCV vers l'IRWST.

4.3.2.1.3. RÉGLEMENTATIONS INTERNATIONALES

Sans objet.

4.3.2.2. Textes para-réglementaires

La conformité aux textes para-réglementaires est portée de manière générale par la section 1.7.1 du Rapport de Sûreté.

4.3.2.2.1. Règles fondamentales de sûreté

Sans objet.

4.3.2.2.2. Directives techniques

La conformité aux directives techniques spécifiquement applicables au système, listés dans le **§ 0.3.2.**, est assurée aux **§ 2.1.** et **§ 4.3.3.** (section G3) et aux **§ 3.1.2.** et **§ 4.3.1.** (section E2.2.2) et au **§ 2.2.5.** (section B2.3.1).

4.3.2.3. Textes EPR spécifiques

Sans objet.

4.3.3. Agressions

4.3.3.1. Agressions internes

La démonstration de la robustesse de l'installation aux agressions internes relève du sous-chapitre 3.4.

4.3.3.2. Agressions externes

La démonstration de la robustesse de l'installation aux agressions externes relève du sous-chapitre 3.3.

4.3.4. Diversification

Sans objet.

4.3.5. Radioprotection

Sans objet.

4.3.6. Fonctionnement, maintenance et accessibilité long terme

Sans objet.

4.3.7. Système tel que réalisé

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

4.4. ESSAIS, SURVEILLANCE EN EXPLOITATION ET MAINTENANCE

4.4.1. Essais de démarrage

Le système BCMS fait l'objet d'un programme d'essais de démarrage conformément aux modalités présentées au chapitre 14, permettant notamment de vérifier le respect des critères suivants :

- plage de concentration en bore,
- temps de réponse,
- précision.

Nota : Le temps de réponse au niveau matériel est défini par l'algorithme de traitement des taux de comptage implémenté au système RPR comme décrit dans le § 3.2.2.. Dans le cadre des essais au test bay du TXS le temps de réponse est validé en injectant des signaux de test et en observant la bonne réponse dynamique selon l'algorithme programmé. Sur site, il n'est pas possible de réaliser des injections de bore avec un profil rectangulaire et il ne peut pas non plus y avoir d'instrumentation de référence tournant en parallèle. Ainsi le temps de réponse ne peut pas être testé sur site.

4.4.2. Surveillance en exploitation

- Sans objet

4.4.3. Essais périodiques

Les parties classées du système BCMS font l'objet d'essais périodiques conformément au chapitre IX des Règles Générales d'Exploitation permettant notamment de vérifier le respect des critères suivants :

- plage de concentration en bore,
- précision.

Transmission :

Les essais périodiques consistent en une vérification de la bonne transmission des signaux de mesures entre l'unité de conditionnement du système BCMS (dans les armoires du système RPN) et l'unité de traitement du système RPR. Les essais peuvent être effectués indépendamment pour chaque chaîne de mesure.

Validation et calibrage :

Le BCMS est vérifié à intervalles réguliers [] en comparant la concentration en bore mesurée au résultat d'une mesure de référence (comme l'analyse chimique d'un échantillon ponctuel). Si la concentration en bore mesurée diffère sensiblement de la valeur de référence, le système BCMS doit être calibré. Le calibrage du système BCMS est pris en charge par l'unité de service TXS.

Le calibrage peut être effectué indépendamment pour chaque détecteur du système en réglant les deux paramètres – facteur de normalisation du taux de comptage et facteur de conversion B-10/Bore enrichi – dans le logiciel du BCMS.

4.4.4. Maintenance

Le système BCMS fait l'objet d'un programme de maintenance conformément au chapitre VIII des RGE.

L'accessibilité à tous les composants et aux salles est assurée en adéquation avec les besoins de maintenance. Pendant le fonctionnement normal du système BCMS, il n'y a pas besoin d'accéder aux composants du système BCMS. Tous les composants peuvent être commandés à l'aide d'un ordinateur de test directement connecté à l'électronique de conditionnement.

Des essais de maintenance périodiques (courbe de discrimination, linéarité de la réponse de la chaîne de mesure…) peuvent être effectués indépendamment pour chaque chaîne de mesure.

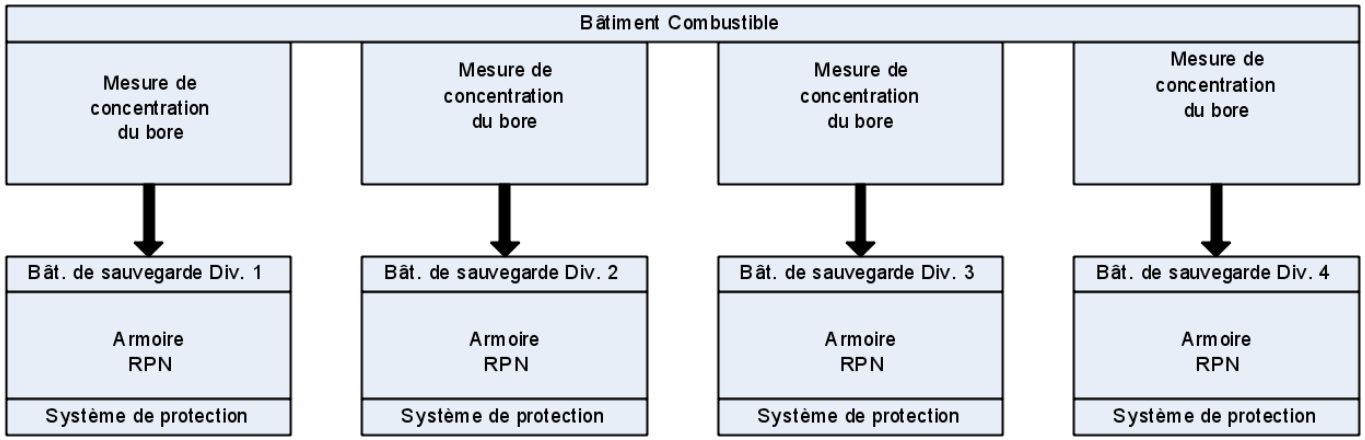
De plus, un calibrage du boremètre est obligatoirement réalisé[].

5. SCHÉMA DE PRINCIPE

Le schéma de principe du système BCMS est présenté en figure **FIG–7.5.9.1**.

FIG–7.5.9.1 SCHEMA DE PRINCIPE DU SYSTÈME D'INSTRUMENTATION DU BORE

FIG–7.5.9.2 VUE D'ENSEMBLE DU SYSTÈME D'INSTRUMENTATION DE MESURE DU BORE



FIG–7.5.9.3 IMPLANTATION DES CONTENEURS DU SYSTÈME D'INSTRUMENTATION DE MESURE DU BORE

A- -7.5.9.1 ANNEXE — []

[]

7.6 PROCÉDURES ET OUTILS DU SYSTÈME DE CONTRÔLE-COMMANDE

7.6.1 SYSTÈME DE CONTRÔLE- COMMANDE STANDARD

7.6.2 SYSTÈME DE PROTECTION DU RÉACTEUR, SYSTÈME DE LIMITATION, SURVEILLANCE ET CONTRÔLE DU REACTEUR, CONTRÔLE COMMANDE ACCIDENT GRAVE ET CONTRÔLE COMMANDE NOYAU DUR

SOMMAIRE

.7.6.1 SYSTÈME DE CONTRÔLE- COMMANDE STANDARD

Cette section traite des outils utilisés pour la programmation du PAS/SAS (données d'automatismes de niveau 1) et du MCP (IHM) du système de contrôle-commande standard. Ceci comprend la conception et le codage. Ces deux ensembles de données ainsi que la configuration du matériel, constituent le logiciel d'application du système de contrôle-commande standard. Des outils de même fonctionnalité sont dédiés pour le contrôle-commande au BTE.

Les outils de spécification fonctionnelle ne sont pas couverts par la présente section.

1. VUE D'ENSEMBLE

Des outils intégrés sont utilisés comme supports pour l'ensemble des activités d'ingénierie de contrôle-commande, de la conception à la mise en œuvre des systèmes de contrôle-commande PAS/ SAS et MCP et jusqu'à l'exploitation, la maintenance et les modifications futures. Ainsi ces outils couvrent la durée du cycle de vie des systèmes de contrôle-commande PAS/SAS et MCP.

Pour la partie du contrôle-commande du SAS/PAS et MCP supportée par un système d'outils intégrés, la gestion centralisée des données fonctionnant conformément aux principes de source unique et de documentation avale est appliquée. L'ensemble des données de conception (définissant la configuration matérielle et logicielle) sont stockées de manière centrale dans des bases de données accessibles par les outils adéquats pour :

- la gestion des données lors des études et pour les modifications ultérieures,
- la génération de la documentation de contrôle-commande,
- la génération du code du logiciel d'application,
- le support de la mise en oeuvre des contrôle-commande (intégration du système, installation sur site et mise en service),
- le support de la vérification et de la validation,
- les tests et diagnostics en exploitation.

Ce concept de gestion des données assure la cohérence entre les différentes étapes d'études ainsi qu'entre la mise en œuvre du contrôle-commande et la documentation associée.

Les activités d'étude du système de contrôle-commande sont planifiées, réalisées et documentées en prenant en compte les exigences exprimées au sous-chapitre 7.1. Parmi celles-ci, seule l'exigence d'assurance qualité s'applique aux outils de CAO pour le système de contrôle-commande standard. L'armoire contenant les serveurs des outils CAO est soumise au classement séisme SC2.

2. EXIGENCES RELATIVES À LA FIABILITÉ ET À LA DISPONIBILITÉ

La qualité de la conception et de la réalisation des outils de CAO doit assurer un haut niveau de disponibilité et de fiabilité aux utilisateurs.

Afin d'assurer un haut niveau de fiabilité et l'exactitude des résultats et des bases de données, les outils de CAO développés et/ou maintenus par le fournisseur doivent se conformer aux plans d'assurance qualité. Tout écart de ces plans d'assurance qualité en ce qui concerne les recommandations de la norme ISO 9000-3 doit être justifié.

Les outils de CAO qui ne sont pas développés et maintenus par le fournisseur sont soumis à un processus de sélection et répondent à des critères visant à assurer leur fiabilité et l'exactitude de leurs résultats.

3. CONCEPTION ET CODAGE

3.1. ACQUISITION DES DONNÉES D'ENTRÉE

Les exigences liées aux procédés concernant les fonctions de contrôle-commande (exigences fonctionnelles) sont établies par des ingénieurs procédé. Ces exigences fonctionnelles (diagrammes fonctionnels et imagerie) constituent les principales données d'entrée de l'étude du contrôle-commande du SAS/PAS et de MCP. Elles sont utilisées lors des différentes étapes de vérification et de validation pour apporter la preuve de la conformité du contrôle-commande aux exigences.

Afin d'éviter des erreurs de programmation, des spécifications claires, compréhensibles et sans ambiguïté des exigences fonctionnelles sont requises. Les exigences fonctionnelles sont documentées de manière uniforme.

3.2. CONCEPTION ET CODAGE LOGICIEL

Une méthode d'ingénierie du logiciel évitant la programmation manuelle d'un logiciel d'application spécifique est appliquée pour le système de contrôle-commande standard. Cette méthode est basée sur la réutilisation de logiciels qualifiés pré-existants ou développés spécifiquement.

Ainsi, la partie logicielle du système de contrôle-commande standard est construite sur la base des types suivants de logiciels préexistants :

- les parties du système d'exploitation qui peuvent être utilisées de manière identique dans chaque unité de traitement du même type,
- les parties du système d'exploitation dont la configuration dépend de l'application (c'est à dire pour gérer la communication au sein du système informatique distribué),
- les modules fonctionnels standardisés (bibliothèque), qui doivent être combinés et configurés pour réaliser des fonctions applicatives spécifiques.

En utilisant des modules fonctionnels standards, chacun possédant des caractéristiques d'entrée-sortie définies sur la base de paramètres, le logiciel est conçu dans son ensemble et sans ambiguïté en sélectionnant les modules fonctionnels requis, en effectuant leur paramétrage et en définissant les connexions entre les modules et avec les signaux externes.

Cette phase de conception est réalisée à l'aide d'un outil graphique [] qui fournit une représentation graphique du logiciel. La représentation graphique orientée-fonction est facile à comprendre aussi bien par l'ingénieur contrôle-commande qui peut concevoir le logiciel sans connaissances particulières de la programmation ou l'ingénieur procédé qui doit vérifier la conformité aux exigences fonctionnelles, que par l'utilisateur qui exploite le système de contrôle-commande.

En ce qui concerne l'IHM (MCP), l'imagerie est conçue et codée à l'aide de deux outils graphiques [] qui fournissent une mise en page standardisée de l'image et utilise des modules logiciels standards préexistants pour la conception et le codage du logiciel de l'IHM.

Les modes opératoires sont des images sans liens avec le procédé. Ils seront conçus et codés à l'aide d'un outil graphique [] qui fournit une mise en page standardisée de l'image et utilise des modules logiciels standards préexistants pour la conception et le codage des modes opératoires.

Cette méthode permet le stockage des données de conception du logiciel d'application du système de contrôle-commande dans des bases de données. Ainsi, le concept de gestion centralisée des données sur le cycle de vie du système de contrôle-commande, expliqué au paragraphe 1, s'applique également au logiciel.

Ceci permet :

- de vérifier la cohérence des données de conception du système de contrôle-commande par les outils de programmation,

- de générer automatiquement la documentation (schémas de réalisation, imagerie) assurant ainsi la cohérence entre le logiciel d'application du contrôle-commande et la documentation produite.

Puisque la méthode de conception du système de contrôle-commande définit de manière non ambiguë le logiciel, le codage peut être réalisé par un outil automatique qui combine et configure les modules logiciels préexistants comme spécifié.

L'outil de conception du logiciel de contrôle-commande est associé à un outil graphique [] de conception de la partie matériel du système numérique de contrôle-commande. Le matériel concerné est défini en sélectionnant et en configurant des modules matériel standards pour le traitement et la communication entre les unités de traitement et les périphériques. Après l'allocation du logiciel aux unités de traitement sur lesquelles il sera exécuté et une fois que l'affectation des signaux externes sur les cartes d'Entrées/Sorties est définie, toutes les informations nécessaires sont disponibles pour configurer la partie du logiciel d'exploitation qui dépend de l'application. Cette tâche peut donc être réalisée par un outil automatique.

La méthode de conception et de codage du logiciel donne un processus d'ingénierie logicielle très efficace qui évite la programmation classique sujette aux erreurs. Pour les applications liées à la sûreté, cette méthode constitue un moyen efficace de répondre aux exigences de haute fiabilité car :

- Le développement et la vérification du logiciel d'application bénéficie du haut niveau de fiabilité des modules logiciels et des outils d'ingénierie qui sont validés à l'avance,
- Les modules fonctionnels standardisés sont compacts et simples permettant une forte couverture par les tests.
- L'utilisation répétée des modules logiciels dans chaque application permet un retour d'expérience très rapide.
- La représentation du logiciel sous la forme d'un schéma de réalisation limite les erreurs lors de la conception du logiciel et lors de la vérification de la conformité vis à vis des exigences fonctionnelles.
- Le codage automatique du logiciel réduit considérablement la probabilité d'erreurs.

3.3. CONCEPTION ET CONFIGURATION MATÉRIEL

Le système matériel est conçu et configuré à partir d'équipements catalogues standards pour ce qui concerne les unités de traitement, de communication et les cartes d'entrée/sortie.

Les outils permettent :

- la conception du matériel, en format adéquat, de préférence graphique, structurée suivant la documentation de conception requise,
- la gestion centralisée des données de conception,
- la génération de la documentation.

Les outils d'aide à la conception participent aux activités de conception du système matériel pour les niveaux 1 et 2 dans :

- le choix des équipements sur la base de catalogues standards, l'interconnexion entre ceux-ci,
- la disposition en baies, racks,
- l'affectation des entrées/sorties à partir de/vers le niveau 0.

3.4. INTÉGRATION, INSTALLATION ET MISE EN SERVICE

Lors de l'intégration du système, les composants matériels et logiciels sont associés et configurés tel que spécifié. L'exécution correcte des fonctions systèmes est vérifiée par des tests. Des tests

complets des fonctions du logiciel d'application dans leur environnement matériel dédié contribuent à la validation du système (cf. section 1.6.2).

L'intégration des systèmes de contrôle-commande de niveau 1 et 2 est réalisée hors site (en usine, sur plate-forme de test). Au besoin, les systèmes de contrôle-commande interconnectés sont intégrés et testés ensemble avant leur installation sur site.

L'équipement de niveau 0 est généralement indisponible pour les tests d'intégration système. Afin de permettre un test complet des systèmes hors site, des dispositifs pour la simulation de signaux E/S (si nécessaire, des simulateurs du procédé de la centrale) sont utilisés.

L'installation et la mise en service comprennent les activités suivantes :

[]

Les activités d'intégration, d'installation et de mise en service bénéficient du concept de gestion centralisée des données. Les données de conception sont accessibles à l'aide des mêmes outils que ceux utilisés pour la conception. Des programmes automatiques vérifient et documentent la configuration réelle en ce qui concerne la cohérence, les versions utilisées, l'état de la vérification et des mises à jour. Des outils efficaces de liaison et de chargement du logiciel, de débogage et de diagnostic sont utilisés. Un mécanisme de comparaison du code chargé par rapport à la référence est en place afin de garantir le chargement de la version attendue du logiciel.

Des moyens de protection ont été mis en place afin que seule une division du contrôle-commande standard puisse être affectée en cas de défaillance des outils CAO.

Un outil de diagnostic [] permet de connaître en temps réel l'état du système de contrôle-commande standard. Cet outil a pour but de localiser précisément le matériel ou la partie du système de contrôle-commande en panne afin d'engager le plus rapidement possible l'action corrective.

4. VÉRIFICATION ET VALIDATION

Les activités de vérification et de validation pour les systèmes de contrôle-commande concernés sont planifiées, réalisées et documentées conformément aux exigences de sûreté liées au classement des systèmes et équipements de contrôle-commande et prennent en compte les procédures et outils d'ingénierie utilisés.

Ci-dessous figure une description du concept de vérification et de validation pour les systèmes PAS/ SAS et MCP.

4.1. VÉRIFICATION

La stratégie de vérification de la conception mise en oeuvre bénéficie fortement de la méthode d'ingénierie (cf. paragraphe 4) utilisée, du concept de gestion centralisée des données et de la documentation pour l'ensemble des données de conception (cf. paragraphe 1).

Le logiciel est construit à partir de modules préexistants ou développés spécifiquement. Ceux-ci, ainsi que les outils associés, sont fournis dans leur état validé avant le début du processus d'ingénierie spécifique aux applications. Ainsi, aucune vérification ultérieure des modules logiciels n'est nécessaire.

Les études sont facilitées par les outils de conception des systèmes de contrôle-commande qui intègrent une interface utilisateur graphique et des vérifications automatiques.

Un grand nombre de sources d'erreurs est supprimé par :

- des vérifications efficaces des saisies de données,

- des contrôles de cohérence, de complétude et de conformité aux règles formelles et aux conventions,
- des contrôles des performances du matériel.

Le principal effort humain de vérification concerne la vérification de la bonne prise en compte des exigences fonctionnelles dans la conception du logiciel d'application du système de contrôle-commande. Cette vérification est réalisée à l'aide de deux méthodes complémentaires :

- Vérification de documents de conception de contrôle-commande :
  Les fonctions d'application conçues sont décrites de manière cohérente et complète par des moyens graphiques (c'est à dire des schémas de réalisation), ce qui permet la compréhension aisée par les ingénieurs contrôle-commande et procédé. Les exigences fonctionnelles sont également documentées de manière uniforme et cohérente (cf. paragraphe 3). Ceci procure ainsi des conditions optimales pour une vérification efficace des documents.
- test du logiciel d'application :
  La méthode d'ingénierie logicielle permet le codage automatique du logiciel d'application dans un langage de programmation, c'est-à-dire sous une forme exécutable sur une plate-forme matérielle de test représentative du système cible. Le logiciel d'application sera automatiquement intégré dans un environnement de test ce qui permet une animation facile de l'objet du test et procure une aide graphique pour le suivi des signaux.

4.2. VALIDATION

La validation permet de démontrer que le système de contrôle-commande du PAS/SAS et MCP relié aux autres systèmes et au procédé de la centrale répond aux exigences fonctionnelles.

La validation comporte les étapes suivantes :

- validation des systèmes :
  validation (hors site) de toutes les fonctions de contrôle-commande sur plate-forme sans interaction avec le procédé de la centrale qui est simulé par des logiciels adéquats. Cette validation permet de s'assurer de la conformité entre la programmation et la spécification des points suivants : l'allocation des fonctions, le traitement des fonctions, les liaisons entre les cartes Entrée/Sortie et l'unité de traitement, l'imagerie du niveau 2 et son animation.
- validation globale :
  validation (sur site) des systèmes de contrôle-commande installés et électriquement mis en service, reliés au procédé de la centrale. Cette validation permet de faire une vérification systématique sur les interfaces entre les équipements de commandes et les matériels sur site mais également entre différents systèmes de contrôle-commande.

Afin de faciliter les étapes de validation sur plate-forme et sur site, et en particulier le débogage en cas de comportements non attendus, les diagrammes fonctionnels programmés peuvent afficher en temps réel les valeurs de certaines variables internes à l'automate.

5. GESTION DE CONFIGURATION

- Un outil de gestion de configuration [] a été développé afin d'assurer la traçabilité des différentes versions des données programmées. Différentes versions des données peuvent être sauvegardées, archivées ou restaurées via le disque dur des serveurs ou via des supports externes.
- L'outil de gestion de configuration remplit un historique de modification dans la partie documentaire de chaque diagramme ou image, contenant les indications suivantes :
  - indice de modification,
  - nom de l'utilisateur ayant réalisé la modification,
  - date de modification.

6. FONCTIONNEMENT, MAINTENANCE ET MODIFICATION

Pour l'exploitation, la maintenance et les modifications du système de contrôle-commande, une documentation complète et cohérente décrivant l'état actuel des systèmes et équipements de contrôle-commande est primordiale.

Les méthodes de conception appliquées permettent la gestion centralisée de l'ensemble des données nécessaires décrivant aussi bien la configuration matérielle que les fonctions d'application mises en oeuvre.

Ces données sont accessibles (au besoin en association avec les informations acquises sur l'état du contrôle-commande) pour :

- un contrôle en ligne de la documentation de contrôle-commande ou la génération d'une documentation papier cohérente,
- la supervision et le diagnostic,
- les tests,
- la modification.

La modification du système de contrôle-commande suit les mêmes procédures et utilise les mêmes outils que ceux mis en œuvre lors de la conception initiale et de la mise en œuvre du système de contrôle-commande y compris les étapes de vérification et validation.

En appliquant le principe de documentation aval, la modification débute avec la modification des données de conception du système de contrôle-commande (copie des bases de données à jour et valables) décrivant la configuration résultante du système de contrôle-commande modifié.

C'est à partir de ces bases de données que le système de contrôle-commande modifié et sa documentation sont générés. Les bases de données sont simultanément mises à jour avec l'intégration du système de contrôle-commande modifié dans la centrale.

7. SYSTÈME TEL QUE RÉALISÉ

A ce stade de la fabrication, de l'installation et du déroulement des essais, aucun écart n'impacte les requis de sûreté spécifiés dans le Rapport de Sûreté.

SOMMAIRE

.7.6.2 SYSTÈME DE PROTECTION DU RÉACTEUR, SYSTÈME DE LIMITATION, SURVEILLANCE ET CONTRÔLE DU REACTEUR, CONTRÔLE COMMANDE ACCIDENT GRAVE ET CONTRÔLE COMMANDE NOYAU DUR

La qualité d'un système de contrôle commande (CC) classé sûreté ne peut être assurée uniquement à partir de preuves établies sur le produit final. Elle nécessite la mise en œuvre d'un processus d'ingénierie adapté pour élaborer le système de CC, avec des mesures de vérification et de validation appropriées à des étapes intermédiaires du cycle de développement.

Cette section décrit le processus d'ingénierie du système de protection (PS), du système de limitation, surveillance et contrôle du réacteur (RCSL), du contrôle commande accident grave (CCAG) et du contrôle commande noyau dur (CC-ND). Ces systèmes se basent sur la technologie TELEPERM XS, qui est élaborée de manière générique, indépendamment de son application à une centrale particulière. Cette élaboration est présentée au § 1.. Le processus d'ingénierie suivi dans le cadre du projet Flamanville 3, pour la partie du développement spécifique à la centrale, est traité dans les sous-chapitres restants.

Remarque : le processus d'ingénierie du RCSL, du CCAG et du CC-ND est similaire à celui du PS en termes de structure. Cependant, certaines activités ne sont réalisées que pour le PS, car le RCSL et le CCAG sont classés F2 et le CC-ND est NC.

1. PLATEFORME TELEPERM XS

Le développement de la plateforme TELEPERM XS, y compris de ses outils d'ingénierie, est réalisé selon les procédures de l'organisation Produits et Technologies de FRAMATOME. Ces procédures sont établies sur la base des normes :

- CEI 61513 (§ 6) pour le cycle de vie du système,
- CEI 60880 pour le logiciel classé F1A,
- CEI 62138 pour le logiciel classé F1B ou F2.

Elles sont donc en conformité avec les exigences de RCC-E.

En ce qui concerne les tâches du logiciel, une distinction est faite entre :

- le logiciel en ligne – il est exécuté dans les modules de traitement du système TELEPERM XS et met en œuvre directement les fonctions de CC, les fonctions de communication ou les tâches d'auto-surveillance en ligne pendant le fonctionnement normal. Le logiciel en ligne comprend le logiciel système inclus dans l'étendue de la fourniture de la plateforme du système TXS, qui a été développé et qualifié indépendamment de la centrale, ainsi que le logiciel applicatif qui est créé au moyen d'une ingénierie spécifique au projet.
- le logiciel de service – pour la configuration, les essais périodiques et la maintenance. Ce logiciel, qui est créé au moyen d'une ingénierie spécifique au projet, est exécuté sur des ordinateurs d'exploitation et de maintenance indépendamment du fonctionnement de la centrale et ne contribue pas directement en lui-même à la réalisation des fonctions de CC.
- les logiciels outil – ils sont utilisés pour l'ingénierie du logiciel applicatif et du logiciel de service et sont exécutés sur des ordinateurs d'ingénierie.

2. PRÉSENTATION GÉNÉRALE DU PROCESSUS D'INGÉNIERIE

Dans le cadre du projet Flamanville 3, le développement de systèmes de CC basés sur la technologie TELEPERM XS suit un processus d'ingénierie bien établi, qui est défini dans :

- un plan de qualité du système,

- un plan de vérification et de validation du système.

Ces plans sont complétés par des procédures internes.

Le processus d'ingénierie est organisé en plusieurs phases :

- acquisition des données amont et planification,
- spécification du système,
- conception et mise en œuvre,
- intégration et validation,
- mise en service.

Le processus d'ingénierie est défini sur la base :

- du RCC-E, et
- des normes CEI applicables : CEI 61513 (§ 6) pour le cycle de vie du système, CEI 60880 pour le logiciel F1A et CEI 62138 pour les logiciels F1B et F2.

3. PHASES DU PROCESSUS D'INGÉNIERIE

3.1. PHASE « ACQUISITION ET PLANIFICATION »

Cette phase se compose de :

- l'élaboration des plans qui régiront le processus d'ingénierie pour les systèmes de CC basés sur la technologie TELEPERM XS,
- l'acquisition des données amont nécessaires au développement des systèmes de CC basés sur la technologie TELEPERM XS.

Les systèmes de CC basés sur la technologie TELEPERM XS sont développés sur la base :

- des prescriptions de sûreté établies par les ingénieurs de sûreté et de radioprotection, y compris celles venant du PSAR,
- des exigences fonctionnelles établies par les ingénieurs procédé,
- de la conception de l'architecture de CC, c'est-à-dire la décomposition de l'architecture de CC en systèmes de CC, la définition des interfaces entre les systèmes de CC et l'attribution de fonctions aux systèmes de CC.

3.2. PHASE « SPÉCIFICATION DE SYSTÈME »

Au cours de cette phase, les systèmes de CC basés sur la technologie TELEPERM XS sont conçus. Cela inclut en particulier :

- la définition de l'architecture des systèmes, mise en œuvre pour répondre aux exigences, et la subdivision du système en sous-systèmes physiques et sous-modules logiques,
- l'affectation des fonctions aux sous-systèmes ou sous-modules,
- la définition des concepts tels que le concept d'essai périodique, de présentation d'alarme ou de gestion des défaillances.

Les principaux documents d'ingénierie produits lors de cette phase sont :

- les spécifications du système,
- les schémas fonctionnels,

- les concepts qui définissent les principes généraux à employer dans le développement du matériel et du logiciel, conformément à la spécification du système.

Ces documents sont vérifiés au regard des données d'entrée.

3.3. PHASE « CONCEPTION ET MISE EN ŒUVRE »

Cette phase consiste à concevoir le matériel et le logiciel.

Pour le matériel, les étapes suivantes se succèdent :

- conception du matériel : schémas d'implantation préliminaires, schéma des réseaux, types de câblage et listes des entrées/sorties.
- conception détaillée du matériel : schémas d'implantation, schéma des bornes, schéma des circuits, listes des câblages et schémas des cavaliers.
- fabrication du matériel (c'est-à-dire assemblage des armoires) et essais de base du matériel (c'est-à-dire essais des armoires assemblées).

En parallèle, les étapes suivantes se succèdent pour le logiciel applicatif :

- conception du logiciel applicatif : sur la base des exigences fonctionnelles et des résultats de la phase de spécification du système. Cette conception utilise l'outil FunBase (voir **§ 6.1.**).
- Mise en œuvre du logiciel applicatif : la conception du logiciel applicatif est traduite en schémas fonctionnels à l'aide de l'outil FDE de SPACE (voir **§ 6.2.**). Le code source du logiciel applicatif est ensuite automatiquement généré à l'aide des générateurs de code TELEPERM XS et compilé à l'aide des compilateurs TELEPERM XS.
- tests de validation du logiciel applicatif : le logiciel applicatif est validé à l'aide d'un outil de simulation (SIVAT, voir **§ 6.4.**) dont les résultats sont comparés à ceux obtenus sur un modèle "oracle" du logiciel. La validation est effectuée de manière progressive : sous-modules puis fonctions de CC.

Enfin, le logiciel de service des unités TELEPERM XS (spécifique à la centrale) est développé (non classé sûreté).

3.4. PHASE « INTÉGRATION ET VALIDATION »

Dans cette phase, les armoires TELEPERM XS (matériel) sont installées sur une plateforme de test. Le logiciel système et le logiciel applicatif sont chargés sur les unités programmées. Après cette intégration, des tests de validation du système sont réalisés. Ils comportent :

- **tests préalables :** ces tests visent à assurer l'intégration correcte du système, ainsi que la mise en œuvre correcte de la configuration d'essai. Ils sont une condition préalable à la réalisation des essais suivants.
- **tests technologiques :** ces tests visent à valider les fonctionnalités liées au CC du système de CC : charge du système, détection et présentation des pannes, comportement en cas de défaillance, interfaces avec les systèmes IHM, performances, maintenance, fonctionnalités spécifiques au CC, etc.
- **tests fonctionnels :** ces tests visent à valider la mise en œuvre des exigences fonctionnelles pour le système de CC. Ils peuvent se concentrer sur des sous-modules logiciels particuliers ou sur les fonctions de CC complètes.

Voir le **§ 4.2.** pour plus de détails sur la validation.

3.5. PHASE « MISE EN SERVICE »

Au cours de cette phase, les systèmes de CC basés sur la technologie TELEPERM XS sont installés dans la centrale et mis en service. Les essais de mise en service sont spécifiés par :

- un plan de mise en service du système, et
- des instructions de mise en service du système.

L'installation et la mise en service comprend les activités suivantes :

- installation sur place de chaque système de CC dans un ordre défini :
  - montage mécanique de l'équipement,
  - interconnexion avec d'autres systèmes et/ou avec les éléments de la centrale (câblage),
  - vérification du concept de mise à la terre,
  - vérification des activités d'installation ci-dessus.
- mise en service de chaque système de CC sans le procédé de la centrale :
  - connexion à l'alimentation électrique,
  - configuration et test de l'équipement du système,
  - configuration et test des interconnexions avec les autres systèmes (y compris les liaisons assurées par les réseaux et la vérification câblée des entrées/sorties).
- mise en service des systèmes de CC raccordés au processus de la centrale :
  - configuration et test des paramètres basés sur le procédé (par exemple, régulations en boucle fermée) qui doivent être réglés et/ou vérifiés en lien avec le processus de la centrale,
  - test de fonctions particulières avec les éléments de la centrale,
  - tests requis pour la validation.

4. VÉRIFICATION ET VALIDATION

Tout au long du processus d'ingénierie décrit au **§ 3.**, des activités de vérification et de validation sont effectuées afin d'assurer l'exactitude, l'exhaustivité et la cohérence des travaux d'ingénierie. Pour le logiciel F1A, les activités de vérification et de validation sont réalisées par une équipe indépendante de l'équipe de conception.

4.1. VÉRIFICATION

La vérification est la « *confirmation par l'examen et par la fourniture d'une preuve objective que les résultats d'une activité répondent aux objectifs et exigences définis pour cette activité* ». De plus, « *en conception et développement, la vérification consiste à examiner le résultat d'une activité donnée pour déterminer la conformité avec l'exigence énoncée pour cette activité* ».

Dans la conception des systèmes de CC basés sur la technologie TELEPERM XS :

- Chaque document d'ingénierie doit être vérifié par une personne indépendante de l'auteur avant sa publication.
- La vérification couvre le contenu du fichier de conception, la forme du document et son contenu technique.

La vérification est complétée par des réunions d'examen technique qui se tiennent à la fin de chaque phase du processus d'ingénierie.

4.2. VALIDATION

La validation est « *la confirmation par l'examen et d'autres preuves qu'un système répond entièrement à la spécification d'exigence de la manière prévue (fonctionnalité, temps de réponse, tolérance aux pannes, robustesse*) ».

La validation d'un système de CC TELEPERM XS est assurée par des tests et par des analyses spécifiques.

Comme l'indiquent les **§ 3.3.** et **§ 3.4.**, les tests de validation incluent les tests de base du matériel, les tests préalables, les tests technologiques et les tests fonctionnels. Les essais de validation sont effectués :

- dans les locaux des fabricants d'armoires, pour les tests de base du matériel,
- à l'aide d'environnements de simulation (SIVAT, RTSIM), pour les tests technologiques et fonctionnels du logiciel applicatif et pour les tests technologiques du logiciel de service,
- sur une plateforme de test, pour les tests préalables, technologiques et fonctionnels des systèmes intégrés (matériel et logiciel).

Les tests de validation sont complétés par des analyses spécifiques, pour justifier le respect d'exigences particulières, par exemple :

- analyse des modes de défaillance et de leurs effets,
- analyse de la fiabilité et de la disponibilité,
- analyse du temps de réponse et de la précision.

5. GESTION DE LA CONFIGURATION

Au cours de l'ingénierie des systèmes de CC basés sur la technologie TELEPERM XS et pendant leur maintenance, un système de gestion de la configuration dédié est mis en place. Il s'occupe des actions suivantes :

- identification de la configuration : comment les systèmes de CC (et leurs sous-parties) et leurs versions successives, sont identifiés.
- contrôle de la configuration : comment les changements des systèmes de CC sont effectués.
- compte rendu de l'état de configuration : comment l'état des systèmes de CC (et leurs sous-parties) est enregistré et communiqué.
- audits et examens de la configuration.
- contrôle de l'interface : comment les changements des produits interfacés sont gérés.
- gestion et livraison des éditions.

6. OUTILS D'INGÉNIERIE

Les principaux outils d'ingénierie spécifiques employés pour la conception et la validation des systèmes de CC basés sur la technologie TELEPERM XS sont les outils d'ingénierie TELEPERM XS :

- FunBase, pour la conception du logiciel applicatif,
- SPACE, pour la mise en œuvre du logiciel applicatif,
- SINTEC et SIKON, pour la conception matérielle détaillée,
- SIVAT, CASSIS, RTSIM et ERBUS, pour les tests de validation.

6.1. FUNBASE

FunBase est un outil d'ingénierie qui prend en charge la préparation de la spécification de la fonction de CC. Il se compose d'une base de données stockant les informations importantes sur les fonctions de CC (entrées/sorties, signaux internes, description des tâches, etc.), ainsi que d'un éditeur graphique pour spécifier les algorithmes à mettre en œuvre.

6.2. SPACE

SPACE est le système d'ingénierie de la plateforme TELEPERM XS. Il inclut les outils utilisés pour l'ingénierie et la maintenance des systèmes de CC TELEPERM XS :

- ingénierie des schémas de réseau, schémas d'implantation et schémas fonctionnels,
- production de la documentation du système,
- production automatique du code,
- contrôle de cohérence des schémas conçus et du code généré,
- compilation et liaison du logiciel applicatif pour le système cible,
- chargement du logiciel applicatif sur le système cible.

SPACE inclut également quelques outils pour analyser les performances du système de CC conçu (par exemple, charge de la CPU et charge du réseau).

6.3. SINTEC ET SIKON

SINTEC et SIKON sont des outils d'ingénierie qui prennent en charge les spécifications matérielles détaillées des systèmes de CC. Ils se composent de bases de données stockant les informations relatives au matériel et au câblage ainsi que d'un éditeur graphique pour spécifier les plans d'armoires de CC.

6.4. SIVAT

SIVAT est un outil supplémentaire pour l'environnement d'ingénierie TELEPERM XS (SPACE). Il permet de tester par simulation la fonctionnalité du système de CC conçu à l'aide de SPACE. La simulation se base sur le code généré par les générateurs de code TXS. Elle permet de réaliser des tests du logiciel applicatif sur l'ordinateur d'ingénierie et sans le matériel cible.

6.5. CASSIS

CASSIS est un outil s'interfaçant avec SIVAT, RTSIM et ERBUS. Il permet d'automatiser les tâches de V&V telles que la génération de la documentation de tests, l'exécution des tests et l'analyse de couverture des tests.

6.6. RTSIM

RTSIM est utilisé pour valider le logiciel de service qui fonctionne sur l'unité de service (décrite au § 7.). RTSIM fournit un environnement de simulation dans lequel le logiciel de CC dans son ensemble (applicatif et système) peut être exécuté en temps réel.

6.7. ERBUS

ERBUS TXS est utilisé sur la plateforme de test pour tester le système de CC. ERBUS TXS permet de simuler les signaux entrants du système et de surveiller les signaux sortants. Il se compose :

- de machines de test, équipées de modules entrée/sortie, qui sont reliées aux modules d'entrée/ sortie du système testé,

- d'une unité de commande du simulateur, qui est un PC standard et qui est raccordé aux machines de test par un réseau. L'unité de commande du simulateur permet d'utiliser des scripts de test et d'enregistrer la valeur des sorties surveillées. L'unité de commande du simulateur peut également être reliée à l'unité de service du système testé. Dans ce cas, les scripts d'essai peuvent être utilisés sur l'unité de service.

7. OUTILS D'EXPLOITATION ET DE MAINTENANCE

Pendant le fonctionnement des systèmes basés sur la technologie TELEPERM XS, la plupart des tâches de diagnostic et de maintenance sont effectuées depuis l'unité de service. L'unité de service est un ordinateur industriel, relié par réseau aux MSI des systèmes de CC de TELEPERM XS (voir sections 7.3.1 et 7.4.3).

Le logiciel de service qui fonctionne sur l'unité de service est organisé en trois couches :

- le système d'exploitation (Linux),
- le serveur DIMAS, qui gère la communication avec les ordinateurs TELEPERM XS, à l'aide des messages de service et de surveillance provenant du protocole de communication TELEPERM XS,
- les clients DIMAS, qui sont interfacés avec le serveur DIMAS et fournissent les interfaces utilisateurs pour interagir avec le système de CC basé sur la technologie TELEPERM XS.

Les deux premières couches sont génériques et font partie de la plateforme TELEPERM XS. Les clients DIMAS de la troisième couche sont soit des clients génériques, appartenant à la plateforme TELEPERM XS, soit des clients spécifiquement développés pour Flamanville 3.

Les clients DIMAS servent en particulier à effectuer les opérations suivantes :

- chargement du logiciel applicatif à distance,
- modifications des paramètres, et suivi de l'historique,
- inhibition des unités programmées,
- verrouillage des chaînes d'acquisition,
- reconfiguration des mémoires,
- essais périodiques,
- diagnostic de l'état du système (alarmes, état des CPUs, état des signaux logiciel, etc.).

Ces opérations ne sont possibles que si le mode de fonctionnement des unités de traitement TELEPERM XS les autorise (voir paragraphe 6 de la section 7.3.1).

Par ailleurs, certaines opérations de maintenance sur certains modules de conditionnement du PIPS (par exemple, modules de conditionnement des mesures de température STT1) sont réalisées à partir d'un ordinateur de diagnostic sur lequel sont installés des logiciels spécifiques nécessaires (fournis avec les modules).