

TP SCADE - Energie

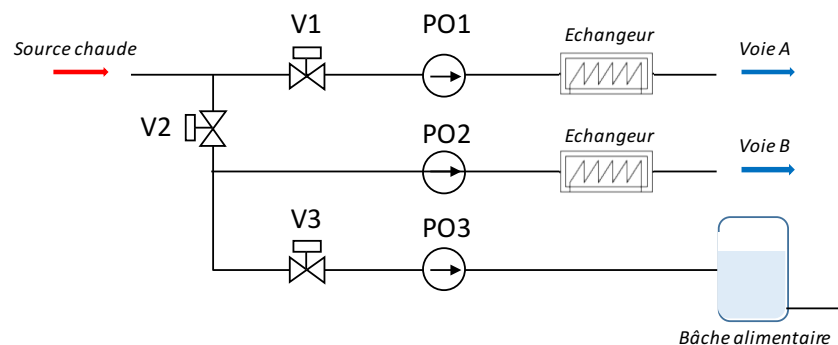
Exercice 1

L'objectif de ce premier exercice est de se familiariser avec l'utilisation de l'outil SCADE.

I. Cahier des charges

On considère un système hydraulique composé de vannes et de pompes. Le système possède trois modes de fonctionnement : à l'arrêt, refroidissement et remplissage en mode secours :

- dans le mode Arrêt, toutes les fonctions du système sont à l'arrêt,
- dans le mode Refroidissement, le refroidissement peut s'exécuter à l'aide de deux fonctions F1 et F2, au choix, selon que l'on effectue le refroidissement par la voie A (F1) ou par la voie B (F2),
- dans le mode Remplissage-secours, lorsque que le système est déjà en mode Refroidissement, le système peut également effectuer une mission de secours d'alimentation en eau d'un système hors du périmètre d'étude ; ce service est supporté par la fonction F3.



L'exécution d'une fonction F_i requiert une configuration particulière d'équipements (vannes et pompes). On considère que lorsque que les équipements sont dans la bonne configuration, alors la fonction est active et que, dans le cas contraire, la fonction est inactive. Les configurations sont les suivantes : F1 = V1 ouverte et PO1 enclenchée, F2 = V2 ouverte et PO2 enclenchée et F3 = V3 ouverte et PO3 enclenchée.

Pour des raisons de sécurité, les contraintes suivantes doivent être respectées :

- Une pompe ne doit jamais être enclenchée si la vanne située en amont n'est pas ouverte,
- Les fonctions F1 et F2 (redondantes) ne doivent jamais être activées simultanément.

Pour des raisons de disponibilité, on privilégiera une alternance entre F1 et F2 pour effectuer le refroidissement (lors de l'activation du mode Refroidissement, la fonction qui sera sollicitée devra être différente de celle qui l'avait été la fois d'avant).

Enfin, les entrées/sorties du système de commande sont les suivantes :

- Entrées (booléennes)
 - o V1_ouv, V2_ouv, V3_ouv : capteurs indiquant la position ouverte des vannes
 - o Dem_RF, Dem_Arret_RF, Dem_RP, Dem_Arret_RP : demande des opérateurs pour respectivement lancer et stopper les opérations de refroidissement et de remplissage.
- Sorties (booléennes)¹
 - o Commandes de pompes : PO1, PO2 et PO3
 - o Commandes de vannes : V1, V2 et V3

¹ On fait l'hypothèse qu'une valeur booléenne à vrai correspond à l'enclenchement des pompes et à l'ouverture des vannes et qu'une valeur booléenne à faux correspond à l'arrêt des pompes et la fermeture des vannes),

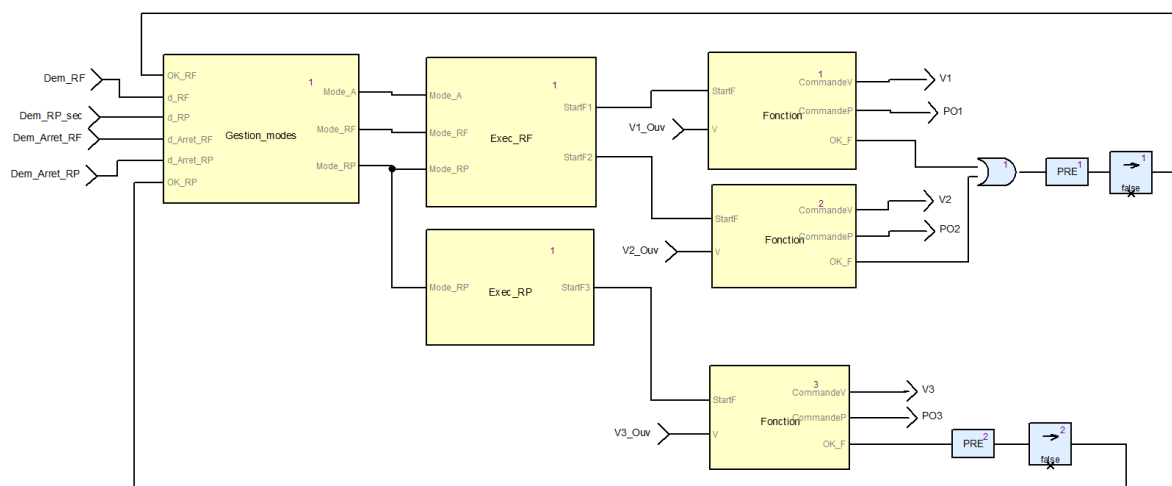
La commande est structurée autour de 4 modules principaux :

- **Gestion des modes** : automates à états finis décrivant les enchainements possibles entre les 3 modes Arrêt, Refroidissement et Remplissage ; on fera l'hypothèse que l'on ne peut quitter les modes Refroidissement et Remplissage que si la ou les fonctions sollicitées sont actives (en d'autres termes, lorsque l'on enclenche une opération, on attend que celle-ci soit active avant de quitter le mode).
- **Fonction** : les configurations des trois fonctions étant identiques, un seul module générique assurera les commandes nécessaires sur les vannes et les pompes ; ce module produit deux sorties (commandes V et PO) lorsqu'une fonction est sollicitée (StartF) et compte tenu de l'état de la vanne (V_ouv) ; il sera instancié pour les trois fonctions F1, F2 et F3.
- Le module **Exec_RF** détermine les fonctions de refroidissement à solliciter :
 - o sur entrée (front montant) dans le mode Refroidissement, une variable interne choix pourra être utilisée pour mémoriser la fonction préalablement activée et choisir la fonction à solliciter,
 - o sur entrée dans le mode Remplissage-secours, la fonction F1 doit être désactivée et la fonction F2 activée.

Dans ces 2 cas, il produira en sortie les sollicitations des fonctions F1 (StartF1) et F2 (StartF2).

- Le module **Exec_RP** produit la sollicitation de la fonction F3 (StartF3) sur entrée dans le mode Remplissage-secours. Il désactive la fonction F3 en sortie de ce mode.

Le schéma global de la commande est donné par la figure suivante :



Travail à réaliser

1. Réalisez les opérateurs *Gestion des modes*, *Fonction*, *Exec_RF* et *Exec_RP* en utilisant les modes de représentation les plus appropriés (diagrammes fonctionnels ou diagrammes d'états).
2. Assembler ces opérateurs au sein d'un opérateur global décrivant la commande du système.
3. Procédez à la simulation de votre application pour en valider le bon fonctionnement
4. Vérifier les propriétés suivantes :
 - a. il n'y a jamais de commande d'enclenchement de pompe PO1 si V1 n'est pas ouverte,
 - b. il n'y a jamais de commande d'enclenchement de pompe PO2 si V2 n'est pas ouverte,
 - c. il n'y a jamais de commande d'enclenchement de pompe PO3 si V3 n'est pas ouverte,
 - d. les fonctions F1 et F2 ne sont jamais actives simultanément,
 - e. il ne peut jamais y avoir deux front montants successifs de demande de démarrage de F1 (il n'y a jamais deux front montants successifs de StartF1),
 - f. il ne peut jamais y avoir deux front montants successifs de demande de démarrage de F2 (il n'y a jamais deux front montants successifs de StartF2).

1. Présentation du cas d'étude

1.1. Généralités

Une centrale nucléaire se compose essentiellement de trois circuits :

- le circuit primaire dont la mission principale est de produire de l'eau chaude pressurisée (la température aux environs de 320° , sa pressurisation permet de la maintenir à l'état liquide) ; le composant principal de ce circuit est le réacteur ;
- le circuit secondaire dont l'objectif est de produire de l'électricité à l'aide d'une turbine alimentée en vapeur d'eau pressurisée ;
- le circuit de refroidissement dont l'objectif est de transformer la vapeur du circuit secondaire en eau avant de sa réinjection dans les générateurs de vapeurs.

Des équipements à l'interface entre ces circuits assurent les échanges thermiques :

- entre les circuits primaires et secondaires, la vaporisation de l'eau est réalisée par les générateurs de vapeurs,
- entre les circuits secondaire et de refroidissement, le changement de phase vapeur vers eau est réalisé dans le condenseur à l'aide d'une source froide (une rivière par exemple).

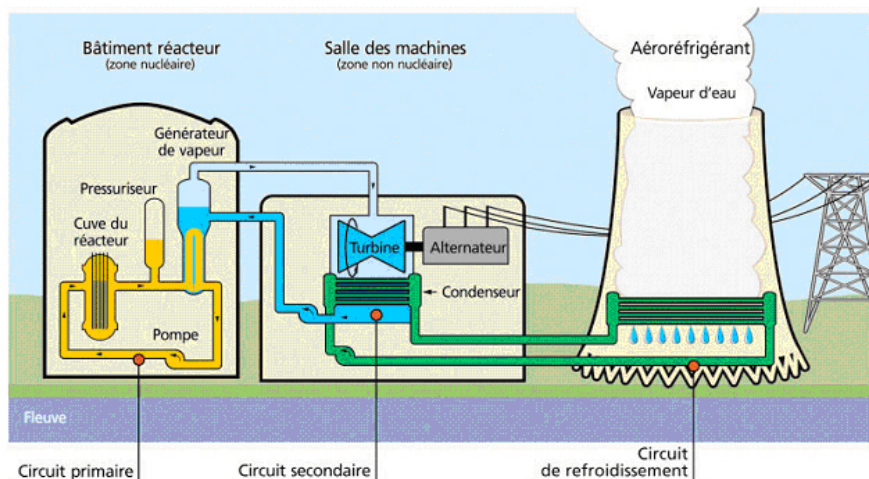


Schéma de principe

Une tranche nucléaire est décomposée en Systèmes Élémentaires, chacun d'entre eux assurant une mission spécifique (aux alentours de 250 SE par tranche).

Par ailleurs, une centrale nucléaire est un système multi-phases, les différentes phases de mission étant appelées **états de tranche**. Une équipe d'opérateurs a la charge de conduire la centrale, c'est à dire de déclencher les événements de changement d'état de tranche (en fonction des besoins et des contraintes de fonctionnement).

1.2. Périmètre fonctionnel du cas d'étude

Le cas d'étude proposé est extrait de la thèse de Pierre-Yves PIRIOU². Toute ressemblance avec des systèmes existants ou ayant existé serait purement fortuite.

² Piriou, Pierre-Yves, Contribution à l'analyse de sûreté de fonctionnement basée sur les modèles des systèmes dynamiques, réparables et reconfigurables, Thèse de doctorat de l'Université de Paris-Saclay, 27/09/2015.

Le cas d'étude se limite à deux Systèmes Élémentaires : **PTR** (Traitement et Refroidissement des Piscines) et **RRA** (Refroidissement du Réacteur à l'Arrêt, cuve fermée). Pour ce cas d'étude, nous n'observerons que trois états de tranche :

- Réacteur en Puissance (RP noté ETAT1) ; c'est la phase de production,
- Arrêt Pour Rechargement (APR noté ETAT3) ; lors de cette phase de mission, la cuve du réacteur est ouverte, afin de sortir le réactif consommé et de faire entrer le nouveau réactif,
- Transitoire entre RP et APR (noté ETAT2) ; c'est au cours de cette phase que la puissance du réacteur est augmentée (pour passer de APR à RP) ou abaissée (pour passer de RP à APR)

1.2.1. Système Élémentaire RRA

L'unique fonction réalisée par le système RRA est le **Refroidissement du Circuit Primaire (RCP) pendant les phases transitoires**. Lorsque le réacteur est arrêté pour rechargement, la cuve est ouverte, donc RRA ne doit pas être utilisé, et lorsqu'il est en puissance, c'est un autre SE (hors périmètre du cas d'étude) qui a la charge de le refroidir. **La fonction est activée par l'entrée logique RRA_OE³** (en provenance d'autres systèmes élémentaires).

Le système RRA est constitué de deux pompes (011PO et 012PO), de deux échangeurs thermiques (015RF et 016RF), et de quatre vannes (013VP, 014VP, 207VP et 211VP). La fonction de refroidissement peut être réalisée grâce à une pompe et un échangeur. Ainsi, quatre lignages permettent d'assurer cette fonction : (011PO - 013VP - 015RF), (011PO - 014VP - 016RF), (012PO - 013VP - 015RF) ou (012PO - 014VP - 016RF). En cas d'échec des quatre lignages, les vannes 207VP et 211VP permettent d'assurer la liaison avec le système élémentaire PTR (qui assure alors le refroidissement à la place de RRA).

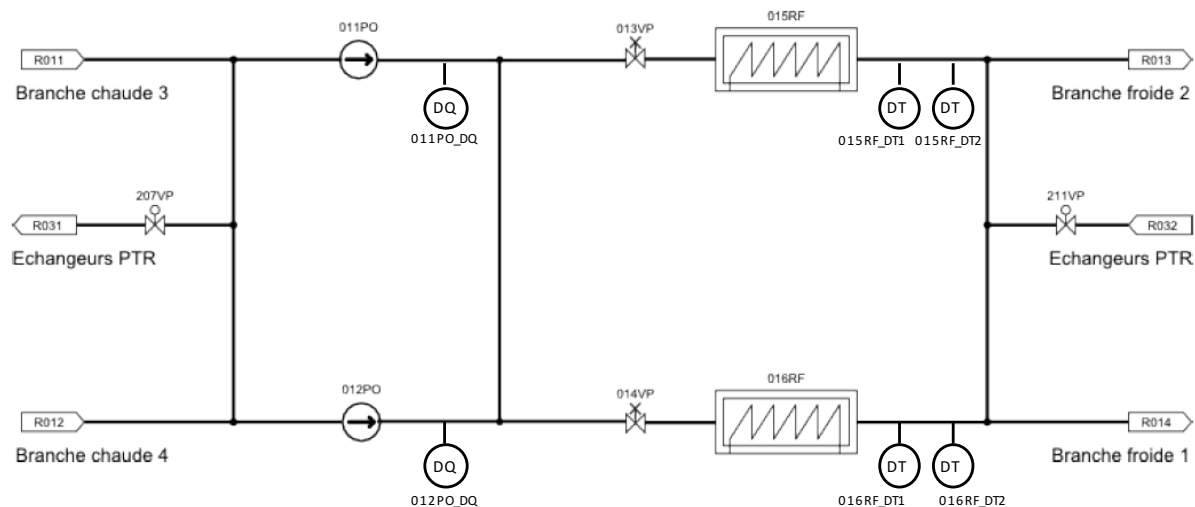


Schéma mécanique du système élémentaire RRA (version simplifiée)

Les pompes ont deux modes d'opération : actif et inactif. Le mode actif est commandé par une sortie logique maintenue (011PO_OE et 012PO_OE). Un transmetteur de débit placé en aval des pompes (011PO_DQ et 012PO_DQ) permet de vérifier le bon enclenchement des pompes. Attention, pour éviter les problèmes de cavitation⁴, les pompes ne doivent pas être enclenchées sans qu'au moins un circuit de circulation des fluides ne soit ouvert.

³ OE : ordre d'exécution, OA : ordre d'arrêt, OO : ordre d'ouverture, OF : ordre de fermeture, EO : état ouvert, EF : état fermé, DF : défaut.

⁴ La cavitation d'une pompe hydraulique se produit lorsque le fluide n'occupe pas entièrement l'espace disponible à l'intérieur de la pompe. La cavitation peut réduire le rendement de la pompe et si les phénomènes engendrant la cavitation se prolongent, elle peut engendrer la destruction de la pompe.

Les vannes sont de type TOR (Tout Ou Rien), on distinguera donc les modes ouvert et fermé. Ces modes sont commandés par deux sorties logiques (013VP_OO, 013VP_OF, 014VP_OO, 014VP_OF, 207VP_OO, 207VP_OF, 211VP_OO, 211VP_OF). Deux capteurs en positions ouverte et fermée permettent de s'assurer de la bonne exécution de la commande (013VP_EO, 013VP_EF, 014VP_EO et 014VP_EF, 207VP_EO, 207VP_EF, 211VP_EO et 211VP_EF).

Les échangeurs peuvent être activés ou désactivés à l'aide des commandes logiques (015RF_OE, 015RF_OA, 016RF_OE, 016RF_OA). Deux transmetteurs de température (015RF_DT1, 015RF_DT2, 016RF_DT1, 016RF_DT2) en aval des échangeurs permettent la régulation des échangeurs (hors périmètre d'étude).

1.2.2. Système Élémentaire PTR

Le système PTR réalise trois fonctions, qui seront requises ou non, selon l'état de tranche :

- **Refroidissement de la Piscine Combustible (RPC)** ; cette piscine contient les stocks de réactifs (neufs et usagés). Ces stocks doivent être immergés en permanence (pour l'étude considérée), donc cette fonction doit être assurée dans les trois états de tranche (ETAT1, ETAT2 et ETAT3) ;
- **Refroidissement de la Piscine Réacteur (RPR)** ; lorsque la cuve du réacteur est ouverte (pour le rechargement), celui-ci doit être immergé. Ainsi, la piscine du réacteur n'est remplie - et donc ne doit être refroidie - que dans l'état de tranche Arrêt Pour Rechargement (ETAT3).
- **Secours RRA (SRRRA)** : Secours de RRA; cette fonction est une redondance fonctionnelle passive de celle devant être réalisée par RRA. Aussi n'est elle requise que dans les phases transitoires (ETAT2), en cas d'échec de RRA.

PTR est constitué de deux pompes (021PO et 022PO), de deux échangeurs thermiques (025RF et 026RF) et deux vannes (022VP et 023VP). De même que pour RRA, quatre lignages permettent de réaliser chaque fonction de refroidissement : (021PO - 023VP - 025RF), (021PO - 024VP - 026RF), (022PO - 023VP - 025RF) ou (022PO - 024VP - 026RF).

De plus, ce système est dimensionné pour pouvoir réaliser deux fonctions de refroidissement simultanément, sur chaque lignage. Ainsi, à la différence des pompes de RRA, celles de PTR ont trois modes d'opération : désactivée (commandes 021PO_OA et 022PO_OA), activée en mode normal à 50% de leur charge (commandes 021PO_OEN et 022PO_OEN), activée en mode de report de charge à 100% (commandes 021PO_OER et 021PO_OER). Les transmetteurs de débit situés en aval de ces pompes mesurent trois niveaux de débit : nul, nominal, report de charge.

Les échangeurs et vannes (ainsi que les capteurs et transmetteurs de température associés) sont, quant à eux, identiques à ceux de RRA.

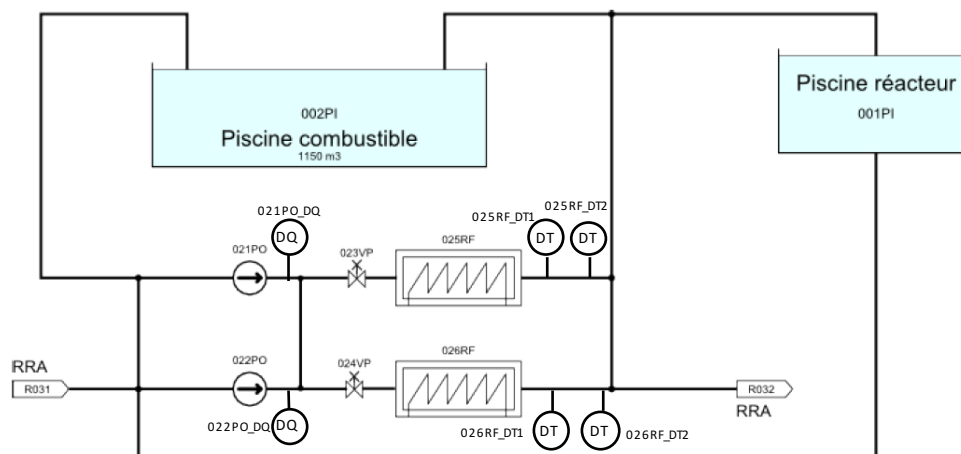


Schéma mécanique du système élémentaire PTR (version simplifiée)

2. Spécification du contrôle-commande du cas d'étude

2.1. Spécifications fonctionnelles

2.1.1. Commande RRA

La système RRA est activé par la demande RRA_OE sous réserve que l'état de tranche soit ETAT2. La commande RRA sera structurée autour de 2 grandes fonctions :

- *Commande du refroidissement en mode normal*
- *Demande de refroidissement en mode secours PTR*

2.1.1.a. Commande du refroidissement en mode normal

Gestion des configurations de pompes 011PO et 012PO

Cette sous-fonction de sélection permet de déterminer laquelle des deux pompes doit être activée en fonction de leurs états dysfonctionnels ; cette sous-fonction décrit une redondance passive entre les deux pompes, conformément à la stratégie de reconfiguration suivante :

- A l'état initial, seule la pompe 011PO est démarrée (par défaut, à l'enclenchement de RRA)
- Si aucune pompe n'est défaillante, ne rien changer
- Si une pompe est défaillante, elle doit être inactive et la pompe non défaillante doit être active.
- Si les deux pompes sont défaillantes, elles doivent être inactives et une alarme de défaillance RRA_PO_DF est générée.

Gestion des configurations de vannes 013VP et 014VP

Choix des vannes à ouvrir (ou fermer) en fonction de leurs états de défaillance ; cette sous-fonction décrit une redondance passive entre les deux vannes dont la gestion est identique à celle des pompes. Par défaut, à l'enclenchement de RRA, c'est la vanne 013VP qui est sélectionnée. Si aucune configuration n'est réalisable, cette fonction émettra une information de défaut RRA_VP_DF.

Commande des échangeurs 015RF et 016RF

Commande d'enclenchement et d'arrêt de chaque échangeur ; cette fonction a également pour entrée les informations délivrées par les deux transmetteurs de température : elle en établit une moyenne et génère une information de défaut (RRA_RF_DF) en cas d'écart supérieur à 10%. En cas de défaut sur un échangeur actif, la configuration bascule sur l'autre échangeur (fermeture de la vanne d'alimentation de l'échangeur en défaut, ouverture de la vanne d'alimentation de l'autre échangeur).

Commandes des actionneurs

La commande des pompes 011PO et 012PO et des vannes 013VP et 014VP est réalisée dans un bloc de commande spécifique à chaque équipement. Ces blocs de commande prennent en compte les caractéristiques technologiques des équipements (par exemple commande maintenue pour les pompes) et réalisent une surveillance de leur fonctionnement (adéquation demande / état) qui peut conduire à l'émission d'une alarme de défaut.

2.1.1.b. Commande du refroidissement en mode secours PTR

Demande de secours

En cas de défaillance sur les deux voies RRA (pompes, vannes ou échangeurs) entraînant l'impossibilité d'effectuer le refroidissement via RRA, une demande de secours vers PTR doit être émise (SRRA_OE).

Commande des vannes 207VP et 211VP

Cette fonction gère la commutation de secours vers PTR en cas d'échec de la fonction de refroidissement. Dans ce cas, les vannes 207VP et 211VP doivent être ouvertes afin de reporter la charge du système RRA sur le système PTR. Dès que la fonction peut être rétablie sur RRA, ces vannes doivent être refermées.

2.1.2. Système Élémentaire PTR

La commande PTR est structurée autour des grandes fonctions suivantes.

Gestion de la configuration de la pompe 021PO

En l'absence de défaillance, la pompe 021PO est dédiée à la réalisation de la fonction RPC (qui doit être assurée dans tous les états de tranche considérés). La stratégie de reconfiguration est la suivante:

- si la pompe 021PO est défaillante, elle doit être inactive,
- sinon, elle doit être active tant que la fonction RPC est requise (toujours vrai dans notre cas),
- de plus, si la pompe 022PO est défaillante, alors que les fonctions RPR ou SRRA sont requises, la pompe 021PO doit être commutée sur le mode Report de Charge, pour assumer la charge de 022PO.

Gestion de la configuration de la pompe 022PO

La pompe 022PO est dédiée à la réalisation des fonctions RPR (qui ne doit être assurée que dans l'état de tranche ETAT3) et SRRA (qui ne doit être assurée que dans l'état de tranche ETAT2, si le système RRA est indisponible). La stratégie de reconfiguration est la suivante :

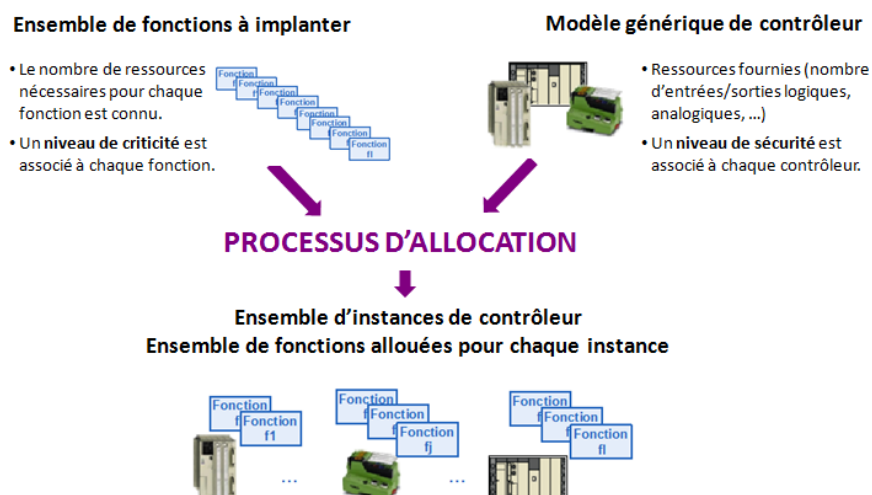
- si la pompe 022PO est défaillante, elle doit être inactive,
- sinon, elle doit être active tant que l'une des fonctions RPR ou SRRA est requise,
- de plus, si la pompe 021PO est défaillante alors que la fonction RPC est requise, la pompe 022PO doit être activée pour assumer la charge de 021PO : en mode normal si les fonctions RPR ou SRRA ne sont pas requises, en mode Report de Charge dans le cas contraire.

Les fonctions **Commandes des actionneurs** et **Commande des échangeurs** suivent les mêmes principes que celles mises en œuvre sur RRA. Attention les blocs de commande des pompes 021PO et 022PO devront tenir compte de trois modes de sollicitation : demande d'arrêt, demande d'activation en mode normal, demande d'activation en mode report de charge.

En cas de d'impossibilité d'assurer le refroidissement pour les fonctions RPC, RPR ou SRRA (défaillances pompes, vanne, échangeurs de PTR), une alarme doit être émise (PTR_DF) et dans le cas où la fonction SRRA est requise, cette alarme doit être complétée par une seconde alarme (SRRA_DF).

2.2. Contraintes d'implantation

Dans le cadre du processus de conception d'architectures de contrôle-commande, une des activités d'ingénierie traite de l'allocation des fonctions de contrôle-commande sur des contrôleurs numériques. Elle obéit à des contraintes principalement relatives aux capacités d'accueil des fonctions dans les contrôleurs et à la sûreté notamment dans le cas de fonctions en redondance fonctionnelle.



Les fonctions de contrôles-commande considérées lors de la conception détaillée des architectures de contrôle-commande sont décomposées en unités élémentaires insécables que nous appelons Unité d'Allocation (UA). Ces UA possèdent des caractéristiques fonctionnelles telles que leur nombre d'entrées/sorties et des caractéristiques de sûreté telles que les contraintes d'exclusion répondant à des objectifs de redondances fonctionnelles.

Les contrôleurs numériques pressentis pour accueillir les UA sont composés d'unités de calcul et de cartes d'entrées/sorties standard ou dédiés qui possèdent également un ensemble de caractéristiques matérielles (nombre d'entrées/sorties autorisés par rack ou par carte, charge CPU admissible, ...) que l'on supposera connues et non modifiables par l'activité d'allocation.

L'architecture opérationnelle de contrôle-commande est définie comme l'allocation d'un ensemble d'UA requises pour supporter les services de contrôle-commande d'une installation sur une architecture matérielle. Le problème posé consiste alors à chercher une ou plusieurs solutions d'allocation garantissant le respect de contraintes (figure 1) :

- de dimensionnement qui traduisent l'adéquation entre les capacités des matériels (nombres d'entrées/sorties, charge CPU, ...) et les ressources requises par les UA,
- de sûreté qui imposent des exigences de séparation, afin de ne pas allouer deux UA en redondance fonctionnelle sur une même CA.

Nous considérons que les Automates Programmables Industriels utilisés pour implanter la commande RRA et PTR disposent de cartes d'entrées/sorties ayant les caractéristiques suivantes :

- carte d'entrées : 5 entrées logiques + 3 entrées analogiques
- carte de sorties : 5 sorties logiques + 3 sorties analogiques

Travail à réaliser

Conception du contrôle-commande

Question 1. A l'aide de l'atelier SCADE, concevoir la commande permettant de répondre aux spécifications présentée à la section précédente.

Vérification du contrôle-commande

Question 2. A l'aide de SCADE *verifier*, formaliser puis vérifier les propriétés suivantes :

- P1 : les pompes 011PO et 012PO ne sont jamais activées si la tranche n'est pas dans un état transitoire entre RP et APR.
- P2 : les pompes 011PO et 012PO ne doivent pas être activées si les deux vannes 013VP ou 014VP sont fermées ou défaillantes.
- P3 : une défaillance de la pompe 021PO lorsque la fonction SRRA est requise doit provoquer le passage en mode report de charge de la pompe 022PO.

Implémentation du contrôle-commande

Question 3. Proposer une architecture opérationnelle susceptible de servir de support d'implantation aux commandes RRA et PTR : proposer une structuration en unités d'allocation (UA) qui tiennent compte des exclusions entre UA imposée par les contraintes de sûreté de fonctionnement (redondance fonctionnelle).