HAL
open science

Rapport final du projet APPRODYN : APPROches de la fiabilité DYNamique pour modéliser des systèmes critiques

Jean-François Aubry, Génia Babykina, Anne Barros, Nicolae Brinzei, Gilles Deleuze, Benoîte de Saporta, François Dufour, Yves Langeron, Huilong Zhang

▶ **To cite this version:**

Jean-François Aubry, Génia Babykina, Anne Barros, Nicolae Brinzei, Gilles Deleuze, et al.. Rapport final du projet APPRODYN : APPROches de la fiabilité DYNamique pour modéliser des systèmes critiques. [Rapport de recherche] Surveillance, Sûreté et Sécurité des Grands Systèmes. 2012. hal-00740181

HAL Id: hal-00740181

https://hal.science/hal-00740181v1

Submitted on 9 Oct 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Projet APPRODYN :

APPROches de la fiabilité DYNamique

pour modéliser des systèmes critiques

Rapport Final - Mars 2012 V7

Auteurs :
Jean François Aubry[2], Genia Babykina[2], Anne Barros[1], Nicolae Brinzei[2], Gilles Deleuze[3], Benoîte de Saporta[4], François Dufour[4], Yves Langeron[1], Huilong Zhang[4]

[1]Université de Technologie de Troyes (UTT-ICD)
[2]Université de Lorraine (CRAN)
[3]EDF R&D
[4]Institut de Mathématiques de Bordeaux-INRIA (CQFD)

Coordination :
Gilles Deleuze EDF R&D
gilles.deleuze@edf.fr

Projet APPRODYN :
APPROches de la fiabilité DYNamique
pour modéliser des systèmes critiques

Rapport Final - Mars 2012

Sommaire

1 Bilan du projet 5
1.1 Rappel des objectifs et de l'objet du projet 5
1.2 Moyens engagés 5
1.3 Elaboration d'un cas test représentatif (chapitre 4) 6
1.4 Expérimentation d'approches (chapitres 5, 6, 7) 8
1.4.1 Apport d'un modèle hybride par rapport à un modèle à évènements discrets 10
1.4.2 Modélisation par Automates Stochastiques Hybrides (ASH) (chapitre 5) 10
1.4.3 Modélisation par Processus Markoviens Déterministes par Morceaux (PMDPM) (chapitre 6) 10
1.4.4 Modélisation par Réseaux de Petri Stochastiques (RdPS) (chapitre 7) 11
1.5 Comparaison détaillée des approches 12
1.5.1 Approches expérimentées dans le projet APPRODYN 12
1.5.2 Comparaison des résultats d'APPRODYN avec les résultats du « *Benchmark NUREG/CR-6942* » 16
1.6 Dissémination 18
1.6.1 Rapports et présentations 18
1.6.2 Publications 18
1.6.3 Contribution à ouvrage collectif 18
1.6.4 Identification des compétences sur les approches de modélisation de la SdF des systèmes hybrides 18
2 Contexte et objectif du projet 20
2.1 Contexte 20
2.2 Objectif 21
3 Glossaire 22
4 Présentation du cas test 23
4.1 Généralités 24
4.2 Eléments pour la modélisation du procédé 26
4.2.1 Modèle comportemental du GV 26
4.3 Description fonctionnelle simplifiée de l'installation 29
4.4 Fonctions des systèmes élémentaires 30
4.5 Profils de fonctionnement 30
4.5.1 Cycles normaux 30
4.5.2 Perturbations 32
4.5. Propriétés attendues du système 32
4.5.3 Niveaux d'eau dans le Générateur de Vapeur 32
4.5.4 Autres propriétés attendues du système étudié 32
4.6 Modélisation de la logique de commande 33
4.6.1 Fonction de commande 33
4.6.2 Capteurs 33
4.6.3 Autres automatismes 34
4.6.4 Mesures et logiques de vote 35
4.6.5 Essais périodiques 36
4.6.6 Actionneurs 36

4.7 Représentation des Automates Programmables Industriels (API) 37
4.8 Données de fiabilité et graphes d'états 38
4.8.1 Valeurs de Taux de défaillance, Pfd 38
4.8.2 Vieillissement 39
4.8.3 Graphes d'états et autres données de fiabilité – Barillet VVP (et parties passives) 40
4.8.4 Graphes d'états et autres données de fiabilité - Pompes électriques CEX 41
4.8.5 Constitution d'une pompe CEX 41
4.8.6 Modes de défaillance d'une pompe CEX 41
4.8.7 Indisponibilité de la partie instrumentation CEX 42
4.8.8 Graphe des états - Pompe électrique CEX en marche 43
4.8.9 Graphe des états - Pompe électrique CEX en attente 43
4.8.10 Automate de spécification des pompes électriques CEX en 2/3 44
4.9 Graphes d'états et autres données de fiabilité - TurboPompe Alimentaire (TPA)... 45
4.9.1 Constitution d'une TurboPompe Alimentaire TPA 45
4.9.2 Modes de défaillance d'une turbopompe TPA (hors turbine) 45
Tableau 4.8. Modes de défaillance d'une turbopompe TPA (hors turbine) 45
4.9.3 Indisponibilité de la partie instrumentation TPA 46
4.9.4 Graphe des états – Turbopompe TPA (hors turbine) 46
4.9.5 Modes de défaillance d'une turbopompe TPA (partie turbine) 47
4.9.6 Graphe des états – Turbopompe TPA (partie turbine, en fonctionnement) 48
4.9.7 Graphe des états – Turbopompe TPA (partie turbine, en attente) 48
4.9.8 Automate de spécification des turbopompes TPA redondées 49
4.9.9 Hypothèses pour la conduite en démarrage et montée en puissance des turbopompes TPA 49
4.9.10 Hypothèses pour la conduite en puissance des turbopompes TPA 50
4.9.11 Hypothèses pour la baisse de puissance des turbopompes TPA 50
4.10 Graphes d'états et autres données de fiabilité - Vanne pneumatique réglante ARE 51
4.10.1 Constitution d'une vanne pneumatique réglante ARE 51
4.10.2 Modes de défaillance d'une vanne ARE 51
4.10.3 Indisponibilité de la partie instrumentation ARE 53
4.10.4 Fonctionnement des turbopompes TPA redondées 54
4.10.5 Graphes des états d'une vanne ARE 56
4.11 Graphes d'états et autres données de fiabilité - Capteurs 60
4.11.1 Fonctionnement des capteurs 60
4.11.2 Modes de défaillance des capteurs 60
4.11.3 Rappel des logiques de vote 60
4.11.4 Essais Périodiques 60
4.12 Données pour l'optimisation des inspections 62
4.12.1 Optimisation des inspections des API de régulation et actionneurs CEX, TPA, ARE 62
4.12.2 Optimisation des inspections des capteurs 65
4.13 Données pour la représentation des erreurs de spécification, de conception logique, ou de paramétrage. 66
4.14 Simplifications du cas test et niveau de difficulté 66
5 Modélisation par Automates Stochastiques Hybrides (ASH) 67
5.1 Principes et références 67
5.2 Qu'est-ce qu'un automate stochastique hybride ? 67
5.2.1 Définition 67
5.2.2 Approche par structuration et synchronisation de manière générique 69

5.3 Modélisation du cas test 70
5.3.1 Exemple du Système Elémentaire CEX 71
5.3.2 Exemple du système élémentaire ARE et de son automate de commande. 72
5.4 Résultats qualitatifs et quantitatifs 78
5.4.1 Exemple 1 : AAR suite à défaillance VVP. 79
5.4.2 Exemple 2 : AAR suite à défaillance CEX 80
5.4.3 Exemple 3 : AAR suite à défaillance TPA 81
5.4.4 Exemple 4: Simulation d'histoires 85
5.4.5 Exemple 5: Recherche de séquences critiques 86
5.4.6 Exemple 6: Simulation d'histoires avec accélération 88
5.4.7 Exemple 7: Modélisation du comportement des capteurs 89
5.5 Conclusion et perspectives pour l'approche ASH 94
6 Simulation et Processus Markoviens Déterministes par Morceaux 95
6.1 Principes et références 95
6.1.1 Qu'est-ce qu'un processus markovien déterministe par morceaux ? 96
6.2 Modélisation du cas test 97
6.2.1 Modélisation des CEX 100
6.3 Résultats qualitatifs et quantitatifs 100
6.4 Conclusion et perspectives pour l'approche par PMDPM et simulation 102
7 Modélisation par Réseaux de Petri Stochastiques 103
7.1 Principes et références 103
7.2 Qu'est-ce qu'un Réseau de Petri stochastique (RdPS) ? 103
7.2.1 Exemple 103
7.3 Modélisation du cas test 104
7.4 Variables et paramètres du processus 105
7.4.1 Variables d'informations 107
7.5 L'outil MOCA-RP 107
7.6 Résultats qualitatifs et quantitatifs 108
7.6.1 Simulation avec profil par palier. 108
7.6.2 Essais avec profil de fonctionnement réaliste 110
8 Références 113

1 Bilan du projet

1.1 Rappel des objectifs et de l'objet du projet

Le projet avait pour but d'expérimenter des approches de la fiabilité dynamique afin de supporter l'étude probabiliste de la sûreté de fonctionnement des systèmes de contrôle-commande critiques utilisés dans les domaines de la production d'énergie et des industries de procédé.

La particularité d'un système hybride est de comporter des interactions entre :

- Des processus physiques, modélisés par des variables continues ;
- Des évènements « ponctuels »: ordres du contrôle-commande, changement du profil de mission, modélisés par des processus à évènements discrets) ;
- Des défaillances internes ou des changements de contexte imprévus, modélisés par des processus aléatoires (stochastiques) à évènements discrets.

La Fiabilité Dynamique s'intéresse aux interactions entre

- La fiabilité d'un constituant du système (stable, avec vieillissement, avec renouvellement…) ;
- L'historique du système (interventions, changements d'états, nombre de marches/arrêts, franchissement de seuils, nombre de déviations, d'arrêts automatiques, de chocs…).

L'enjeu concerné est la disponibilité ; il s'agit de simuler une exploitation sur une période de temps relativement longue et de rechercher une optimisation de divers éléments du système (stratégie suivie par la logique de commande, conditions d'exploitation et de maintenance…) en vue de diminuer les pertes de production et le vieillissement prématuré des composants matériels du système. Nous ne sommes donc pas pour ce projet dans le cadre des Etudes Probabilistes de Sûreté.

1.2 Moyens engagés

Entre le 15 septembre 2010 et le 31 mars 2012[1], le projet a impliqué, à des niveaux variés, 18 personnes issues de 5 organisations. Pour assurer la coordination des efforts et la transversalité, 7 réunions d'avancement ont été faites. Le suivi du projet pour le GIS a été assuré par Mme Nada Matta. Egalement, 2 journées de séminaires sur simulateur SIPACT ont été organisées, les 5-6 septembre 2011, dans les locaux d'EDF R&D à Clamart. Ces journées, ouvertes à tous les participants du projet, avaient pour but de simuler les interactions entre circuit primaire et circuit secondaire sur un outil thermofluidique employé par EDF.

Les financements demandés au GIS étaient les suivants :

Budget demandé au GIS (€ HT)							
Partenaires	Personnel	Consommables	Matériels	Frais de Déplacements	Frais de gestion	Autres Dépenses	Total
EDF R&D	0	0	0	0	0	0	0
CRAN	32 502	300	1 500	5 000	3 144	0	42 446
INRIA	5 000	0	15 000	18 000	0	5 000	43 000
UTT	4 500	0	0	7 500	0	0	12 000
Total	42 002	300	16 500	30 500	3 144	5 000	97 446

Tableau 1.1. Financement du projet par le GIS (budget initial)[2]

[1] Suite à décision du 29 septembre 2010, de prolonger le GIS 3SGS jusqu'à avril 2012.
[2] Le CRAN a reçu un complément de 10000 Euros pour prolonger un post doc de 9 à 12 mois.

1.3 Elaboration d'un cas test représentatif (chapitre 4)

Un cas test a été constitué, suffisamment documenté pour permettre des comparaisons ultérieures. Il s'agit d'une représentation simplifiée d'une partie du circuit secondaire d'un réacteur à eau pressurisée français de 900 MW, avec sa logique de commande. Le choix est motivé par les critères suivants :

- Cas test représentatif et généralisable à des domaines non nucléaires ;
- Etudes de référence aux USA ;
- Modèle simplifié disponible ;
- Retour d'expérience disponible.

L'interface entre l'eau et la vapeur dans le GV est un mélange diphasique eau-vapeur sous pression, de ce fait la loi de variation du niveau d'eau dans le GV suit un modèle non linéaire et présente des difficulties particlières de modélisation. Pour ce projet, qui s'intéresse à la modélisation hybride pour étudier la sûreté de fonctionnement d'une logique de commande, un modèle simplifié est suffisant.

Pour représenter la variation du niveau d'eau dans le générateur de vapeur, un modèle linéaire complet est fourni, à 4 variables continues. Le rapport en fournit le détail au chapitre 5 (Présentation du cas test). Le rapport fournit les informations sur les points suivants, nécessaires à l'étude de sûreté de fonctionnement :

Description fonctionnelle simplifiée de l'installation
Données de fiabilité
Exploitation et Maintenance

Il est important de noter que les données et modèles présentés dans ce chapitre sont représentatifs mais non réels. Des simplifications et approximations ont été faits, en particulier sur les points suivants:

- Fonctionnement de la regulation
- Comportement physique à l'intérieur du GV
- Modes de défaillance de la partie tuyauterie, robinetterie, vannes (VVP)
- Quantification des taux de défaillance, proportion entre modes de défaillance, défaillances de cause commune, des couts de maintenance

En conséquence, les difficulties méthodologiques constatées sont représentatives du cas réel, mais les résultats quantitatifs obtenus ne le sont pas. Ils ne doivent pas être employés ou repris à d'autres fins que le cas test. De même, la terminologie des descriptions fonctionnelles et dysfonctionnelles du cas test n'est pas représentative de son domaine d'origine (nucléaire), afion d'en faciliter la compréhension par d'autres domaines. Enfin, le cas test traite de situations relevant de la disponibilité d'un système qui n'est pas classé de sûreté.

Le cas test présente des « niveaux de difficulté » successifs. Le niveau « Extrême » représente ce qui pourrait être atteint par des approches qui sont du point de vue théorique, des résolutions de l'équation de Chapman-Kolmogorov. L'objectif visé est la simulation de plusieurs milliers d'histoires sur plus de 18 mois.

Les approches expérimentées dans ce projet et les ressources disponibles ont permis de montrer la faisabilité de modèles prenant en compte plusieurs profils de mission, des défaillances des capteurs présentant des aspects dynamiques, c'est-à-dire jusqu'au niveau de difficulté « Très élevé ».

Afin de rendre réalisable la simulation d'un nombre significatif d'histoires d'au moins 18 mois, une réduction de la taille de l'espace des états a conduit parfois à se ramener à un niveau « Elevé » ou « Moyen ».

Niveau de représentation d'un système hybride	Niveau de prise en compte des requis du cas test
Extreme : Modèle hybride à grand espace des états + fiabilité dynamique	Prise en compte de l'ensemble des requis du cas test, En particulier : • Injection d'erreurs dans la modélisation de la commande : erreurs de spécification, de conception logique, erreurs de paramétrage, • Représentation de phénomènes relevant de la fiabilité dynamique (usure, dérives, vieillissement..) • Etude des interactions potentielles entre systèmes (par exemple, interactions entre TPA et VVP, entre ARE et CEX…) • Histoires avec indisponibilités fortuites et redémarrages successifs
Très Elevé : Modèle hybride à grand espace des états	Idem niveau « Extreme » sauf : • Représentation de phénomènes relevant de la fiabilité dynamique • Injection d'erreurs dans la modélisation de la commande : erreurs de spécification, de conception logique, erreurs de paramétrage, • Etude des interactions potentielles entre systèmes
Elevé : Modèle hybride	Idem niveau « Très Elevé » moyennant des simplifications visant à réduire l'espace des états ou le temps de calcul. Par exemple : • Représentation des profils de mission les plus simples, ou de parties stationnaires des profils, • Echec de réparation intégré au MTTR à condition qu'il ne génère pas de séquence critique. • Pas d'évènements pendant une réparation lorsque le système est à l'arrêt • Pas d'évènements pendant un redémarrage • Pas de modélisation de certaines défaillances des capteurs • Histoires s'arrêtant à la première indisponibilité fortuite • Réduction du nombre et de la durée des histoires
Moyen: Modèle hybride partiel	Idem niveau « Elevé » avec en plus, réduction de la taille du modèle. Modélisation de certaines parties du système, en conservant leur aspect « hybride ».
Faible : Modèle dynamique partiel	Modélisation discrète et dynamique du système
Mauvais : Modèle discret statique	Modélisation discrète et statique

Tableau 1.2. Niveaux de représentation d'un système hybride

1.4 Expérimentation d'approches (chapitres 5, 6, 7)

Le projet APPRODYN a permis d'expérimenter des approches de la modélisation hybride dans le cadre de l'étude probabiliste de la sûreté de fonctionnement des systèmes de contrôle/commande critiques, notamment ceux utilisés dans le domaine de la production d'énergie et des industries des procédés. Nous avons pu explorer les possibilités offertes par des approches novatrices mais encore peu utilisées en milieu industriel. Il s'agit des automates stochastiques hybrides (ASH), et d'une simulation des Processus Markoviens Déterministes par Morceaux (PMDPM). Les deux approches sont comparées avec des approches de plus large diffusion et mieux outillées, telles que les réseaux de Petri Stochastiques (RdPS)..

Le tableau suivant résume les observations faites pour les trois approches, qui ont toutes visé le niveau « Très Elevé » de représentation d'un système hybride. Elles ont selon les critères, atteint des niveaux entre « Moyen » et « Très Elevé ». La proportion d'histoires avec Indisponibilité Fortuite (IF) est conhérente dans les deux approches, mais il existe un écart sur la proportion d'IF dûes aux systèmes TPA et ARE, dûes à une régle différente. La somme ARE + TPA est cohénrente.

Tableau 1.3.a. Comparaison qualitative pour les trois approches

	Approche RdPS	Approche par simulation du PMDPM	Approche par ASH
Résultats qualitatifs et quantitatifs obtenus	Partiel Pas de simulation d'histoires en nombre.	Distribution des causes d'Indisponibilité Fortuite	Distribution des causes d'Indisponibilité Fortuite Identification et évaluation des séquences menant à l'Indisponibilité Fortuite
Difficultés rencontrées	Représentation de la commande Temps d'exécution Raideur du modèle induite par la représentation des capteurs	Temps d'exécution Raideur du modèle induite par la représentation des capteurs	Mise en œuvre complexe des outils Temps d'exécution Raideur du modèle induite par la représentation des capteurs
Perspectives	Améliorer modélisation de la commande (problème de synchronisation)	Modélisation complète des capteurs Résolution des aspects optimisation Recherche de séquences critiques Parallélisation (capacité déjà apportée par l'outil) Synchronisation	Résolution des aspects optimisation Parallélisation des calculs Améliorations de l'outil Scilab/Scicos : parallélisation, synchronisation
Notes	Modèle global obtenu par composition Relativement aisé à mettre en œuvre Absence de modèle de commandes	Création d'un simulateur graphique interactif et évolutif Blocs PID et MPC Pas de limites au nombre de variables physiques	Modèle global obtenu par composition d'Automates à Etats Finis (vérification possible) Développements futurs sur Scicos Scilab indispensables

.

Tableau 1.3.b. Comparaison des résultats quantitatifs

	Approche par simulation du PMDPM	Approche par ASH
Nombre d'histoires	4000 (durée 18 mois)	200
Nombre d'Indisponibilités Fortuites (IF) observées au niveau système complet	2190 (55%)	118 (59%)
Repartition des causes d'IF par Système Elémentaire	VVP : 36% CEX : 2,3% TPA : 2,1% ARE : 59% (Les passages à 2% de puissance sont traités comme des IF)	VVP : 47% CEX : 0% TPA : 51% ARE : 2% (Les passages à 2% de puissance **ne sont pas** traités comme des IF)

1.4.1 Apport d'un modèle hybride par rapport à un modèle à évènements discrets

Nous savons qu'un modèle de Système à Evènements Discrets (SED) statique ne peut représenter directement la partie hybride du cas test et les aspects de reconfiguration ou de réparation des systèmes redondés.. Il n'est pas dans l'objectif d'APPRODYN de représenter le cas test par une telle approche. La validité de la comparaison ne tiendra qu'au poids relatif de la fiabilité des parties statiques du systèmes par rapport aux autres. Il est plus intéressant d'aborder ces modèles par l'intégration d'une modélisation hybride avec la démarche EPS.
Une approche par SED dynamique, de type BDMP, a plus de potentiel et peut représenter certains aspects de reconfiguration ou de réparation des systèmes redondés … Une telle comparaison pourrait être faite dans une suite d'APPRODYN.

1.4.2 Modélisation par Automates Stochastiques Hybrides (ASH) (chapitre 5)

La modélisation par Automates Stochastiques Hybrides a été réalisée au CRAN où ce concept a été défini formellement et appliqué à des cas tests académiques en fiabilité dynamique [PER 09, PER 11]. Ils ont permis la modélisation et l'étude probabiliste des systèmes présentant des conflits dans l'évolution de leur comportement [PER 10] et l'évaluation de l'intensité de défaillance des systèmes complexes en contexte dynamique [BAB 11].

La modélisation par ASH permet d'accéder à l'évaluation de la sûreté de fonctionnement d'un système complexe tel que celui du cas-test considéré. Outre l'accès aux probabilités des états dangereux, elle permet d'analyser exhaustivement l'ensemble des séquences qui y mènent et leurs probabilités respectives. Dans l'état actuel des outils utilisés, le travail de modélisation reste très conséquent et la dimension du modèle est importante. Cependant, cette expansion de la taille du modèle peut être relativisée par plusieurs considérations : les outils informatiques modernes s'en jouent de plus en plus facilement et de nombreuses approches de simplification ont vu le jour pour simplifier les Automates à Etats Finis (AEF), par exemple, les diagrammes de décision binaires exemple [HAM 05, POC 08]... Dans la perspective du développement de quelques modules à insérer dans la plateforme Scilab-Scicos, le travail de modélisation pourra être substantiellement simplifié. De plus, lorsque les outils de composition d'ASH seront développés formellement, à l'instar de ceux existant pour les AEF, seuls les automates embryons seront à saisir, le reste se fera automatiquement sans nécessiter la visualisation graphique de l'automate complet.

La modélisation par ASH a été implantée dans l'environnement de simulation et de calcul numérique Scilab-Scicos, plateforme logicielle libre ouverte. L'analyse structurelle du modèle permet d'obtenir l'ensemble des séquences d'évènements possibles et, en conséquence, les séquences critiques. La simulation du modèle sur un grand nombre d'histoires (méthode de Monte Carlo) permet l'accès à l'évaluation probabiliste (probabilité d'être dans un état, dans un groupe d'états, probabilité d'une séquence…). Des développements sont encore nécessaires pour disposer d'outils d'aide à la modélisation et d'accélération des simulations.

1.4.3 Modélisation par Processus Markoviens Déterministes par Morceaux (PMDPM) (chapitre 6)

Le travail présenté s'inscrit dans la continuité d'une série de travaux déjà réalisés au sein de l'équipe INRIA-CQFD. Ils ont pour objectif d'illustrer la mise en œuvre d'une méthode alliant la puissance de modélisation des processus markoviens déterministes par morceaux (PMDPM) et l'efficacité calculatoire de la simulation de Monte Carlo, pour traiter certains problèmes relevant du champ de fiabilité dynamique. Des systèmes de taille « académique » [ZHA 2009] et « industrielle » [ZHA 2008] ont déjà été modélisés et simulés, les implémentations ont été réalisées en C++ ou Matlab. Pour modéliser ce système, plus complexe, les logiciels Simulink et Stateflow de Mathwork, ont été choisis. Ils permettent de construire un simulateur interactif. L'approche par simulation offre des perspectives intéressantes à plusieurs points de vue :

- programmation graphique. Le code source ressemble à un diagramme de fiabilité. En mode débuggeur, les utilisateurs peuvent visualiser pas par pas les états et les transitions ;

- maintenance évolutive du simulateur. Les composants VVP, CEX, TPA, ARE ont été modélisés d'abord séparément (en supposant les autres composants 100 % fiables) et ensuite rassemblés par des simples copier-coller. Par la suite, d'autres composants pourront être ajoutés. De même, le problème de la redondance des composants multiples, pourra être traité assez simplement en pré-construisant une librairie de composants ;
- limitation du nombre de composants. Il n'y a pas de problème d'explosion combinatoire dans cette approche. En effet, les machines à états de stateflow sont orientées composant, c'est-à-dire qu'à chaque pas de temps, et pour chaque composant, le simulateur calcule l'état du composant. On peut alors considérer l'état du système comme un vecteur, dont la dimension est égale au nombre de composants.

L'inconvénient principal de cette approche est le temps d'exécution. Pour le cas test traité ici, une histoire est simulée en environ 30 secondes (sur un MAC portable), il faut donc 8 heures pour 1000 itérations de Monte Carlo. L'expérience [ZHA 2008] montre qu'un simulateur C++ dédié à un problème de cette taille peut sans doute s'exécuter dix fois voire cent fois plus rapidement, mais au prix d'un investissement lourd en programmation et d'un code généré difficile à faire évoluer. Nous avons partiellement résolu le problème en divisant le temps de calcul par 10 grâce à l'utilisation du « Parallel Computing Toolbox».

D'autres pistes peuvent également être explorées. L'équipe INRIA-CQFD propose des algorithmes numériques de contrôle optimal : arrêt optimal, contrôle impulsionnel, etc. [SDG2010, SAP2011, SD2011]. Dans toutes ces méthodes, le simulateur Monte Carlo est la brique élémentaire.

La modélisation par PMDPM s'applique très bien à ce problème de fiabilité dynamique et l'approche Simulink associé à Stateflow permet de construire un simulateur interactif, évolutif, sans problème d'explosion combinatoire.

1.4.4 Modélisation par Réseaux de Petri Stochastiques (RdPS) (chapitre 7)

Les premiers résultats dits en situation réelle ne sont pas satisfaisants. Le temps a manqué pour étudier complètement le cas test du projet APPRODYN. Malgré cela, ce que l'on peut retenir de l'approche par RdPS est sa facilité de mise en œuvre. Elle ne demande pas de connaissances particulières en informatique si ce n'est une programmation modulaire, hiérarchisée. C'est une technique empreinte de bon sens et couramment utilisée dans le monde industriel. Cette manière de programmer alliée à une représentation graphique de type automate explique que les RdPS sont souvent utilisés en sûreté de fonctionnement.

A ce stade du projet, le point bloquant est la gestion de la loi de contrôle/commande à tout instant qui se trouve ne pas être robuste. L'approche par RdPS a souhaité rester ancrée au plus près de la réalité du cas test ApproDyn. D'une part, le système n'est pas invariant dans le temps dans le sens où sa nature intrinsèque dépend de la puissance demandée. D'autre part, les actionneurs pilotés sont à commande bornée. Les indicateurs de fiabilité demandés sont corrélés à la grandeur commandée (le niveau d'eau dans le générateur de vapeur). Pour ces raisons, l'approche par RdPS ne peut actuellement fournir de résultats quantitatifs sur les différentes probabilités souhaitées comme celle d'un arrêt automatique du réacteur.

S'agit-il d'un verrou technique dans l'utilisation de l'outil (problème de priorisation des tirs de transition) et la programmation de la loi de commande (discrétisation de la loi PID) ? S'agit-il d'un verrou scientifique dans la manière d'effectuer les simulations de Monte Carlo (la gestion du temps n'étant pas la même pour les évènements stochastiques et les phénomènes continus) ? Autant de questions auxquelles l'approche RdPS n'a pu répondre mais qui sont autant de perspectives pour une suite à ce projet.

1.5 Comparaison détaillée des approches

1.5.1 Approches expérimentées dans le projet APPRODYN

Le projet a montré la possibilité de modéliser des systèmes hybrides d'assez grande taille, combinant une partie combinatoire à évènements discrets et une partie hybride proprement dite, par plusieurs approches.
Pour une comparaison générale des approches, nous avons défini un certain nombre de critères qualitatifs. L'annexe I présente la comparaison faite dans l'étude NUREG de référence, ainsi que des adaptations et améliorations de ses critères, que nous avons en partie réutilisées. Nous avons distingué les critères qui concernent la méthode, de ceux qui concernent l'outil informatique.

Le tableau suivant propose une comparaison les trois approches menées dans le projet APPRODYN selon ces critères.

Critère	RdPS	Simulation du PMDPM	ASH
Capacité à traiter les phénomènes stochastiques : limitée au cadre exponentiel, traite les lois usuelles de la fiabilité, non limité…(Méthode)	Lois exponentielle, Weibull, différents tirs à la sollicitation. Ouvert à la programmation d'autres lois	Tous types de phénomènes stochastiques, temporels on non	Non limitée, tous types de phénomènes stochastiques temporels ou non.
Capacité à traiter les variables continues (Méthode)	Critère vérifié en partie	Sans limite, traité par Simulink	Sans limite, pris en charge par Scicos Scilab
Taille du modèle : explosion combinatoire, de l'espace d'états (Méthode)	Pas d'explosion combinatoire de par la modélisation hiérarchisée.	Pas de problème d'explosion combinatoire	Très importante (nécessité de rechercher des moyens de simplification)
Nouveauté de la méthode, diffusion dans la communauté de la sûreté de fonctionnement et de l'analyse des risques (Méthode)	Les RdPs sont déjà couramment utilisés en SdF	Approche nouvelle dans la fiabilité dynamique (avec contrôleur)	Nouvelle méthode à diffuser dans la communauté
Critère n°5 étude NUREG : Facilité de programmation. (Outil) Accessibilité à un analyste et facilité de mise en ouvre (conception du modèle..), ressources nécessaires (puissance de calcul, hardware, connaissance en informatique). Documentation nécessaire pour réutilisation du modèle par un tiers.	Outil : Logiciel du commerce MOCA-RP Fonctionne sur PC standard sous Windows Très facile à appréhender. Langage graphique et non langage de scripts. Pas de connaissance informatique particulière.	Outil : Logiciel du commerce Simulink/Stateflow Fonctionne sur PC standard sous Windows Coût de licence de prix non négligeable Apprentissage aisé Modèle du système facile à employer Pris en main facile par un tiers. Facile à faire évoluer Possibilité de créer des bibliothèques de composants réutilisables	Outil : logiciel libre Scilab/Scicos Fonctionne sur PC standard sous Windows ou Linux Apprentissage moyennement aisé Facilité d'emploi à améliorer par des développements spécifiques Un minimum de documentation nécessaire
Facilité de vérification du modèle : facilité du deboguage (Outil)	Maintenabilité difficile Deboguage mode pas à pas	Mode deboguage déjà prévu en Simulink/Stateflow Simulateur interactif	Facilité du débogage à améliorer
Facilité de vérification du modèle : complétude et cohérence avec spécification (Méthode),	Modélisation hiérarchique depuis le composant vers le système complet	Bonne. Elle est héritée des modèles élémentaires Hiérarchisé, multiéchelle	Bonne. Il suffit de vérifier la conformité des modèles élémentaires aux spécifications
Facilité de vérification du modèle : cohérence du modèle (Méthode),	Point non étudié	-Point non étudié	Bonne. Elle est héritée des modèles élémentaires (composition parallèle)
Capacité de parallélisation (pour simulation d'histoires) (Outil)	Possibilité d'utiliser les multiples cœurs d'un même processeur.	Bonne. Très efficace pour simulation de Monte Carlo	A développer, en relation avec INRIA Scicos Scilab (proactive parallel suite)

Critère	RdPS	Simulation du PMDPM	ASH
Capacité de « desynchronisation »[3] , de traitement de systèmes à cinétiques très différentes (multiéchelle de temps) (Outil)	Point non étudié	Bonne	A voir par co-simulation (Parallel virtual machine)
Capacité à révéler les séquences d'états dangereux (effets domino), et à distinguer les états ou séquences affectant la fiabilité et ceux affectant la sureté (Méthode)	Point non étudié	Pas encore étudié	Elle est complète
Critère n°8 étude NUREG : Capacité à révéler les défaillances intermittentes, reversibles (Méthode)	Point non étudié	Pas encore étudié	Oui
Critère n°4 étude NUREG : Capacité à représenter quantitativement et avec précision les dépendances entre défaillances (Méthode)	Point non étudié	Possible, mais pas encore étudiée	Non testée mais possible
Capacité à estimer les incertitudes stochastiques (sur les paramètres) (Méthode)	Point non étudié	Possible, mais pas encore étudiée	Par multiplication des simulations donc encore difficile
Critère n°1 étude NUREG : Capacités *inductives* (retrouver des défaillances observées) et *déductives* (trouver des défaillances pas encore observées) (Méthode)	Point non étudié	Pas encore étudié	Oui, par analyse des langages d'automates

[3] et de ne modéliser la régulation et les évolutions continues qu'en cas de défaillance d'un élément du système.

Critère	RdPS	Simulation du PMDPM	ASH
Performance par rapport à des critères SdF d'interêt (Disponibilité, Fiabilité, Optimisation, identification de séquences critiques…) (Méthode)	Performant pour études de Disponibilité Fiabilité	Performant pour études de Disponibilité Fiabilité Identification et évaluation de séquences critiques : non performant Optimalisation : arrêt optimal, contrôle impulsionnel (mais pas encore développée)	Performant pour identification et évaluation de séquences critiques Moyennement performant (temps de calcul) pour étude de Disponibilité, Fiabilité Optimisation possible
Critère n°9 étude NUREG : Capacité à fournir des résultats pertinents pour des utilisateurs finaux (analyste EPS, expert Contrôle-Commande). Exemple: séquences minimales, probabilités de défaillance, incertitudes associées aux résultats.	Oui (probabilités de défaillance…)	Oui (valeurs probabilistes,…)	Séquences minimales oui, probabilités de séquences oui

1.5.2 Comparaison des résultats d'APPRODYN avec les résultats du « *Benchmark NUREG/CR-6942* »

Par rapports aux travaux conduits par la NRC [NUR 07a], à l'origine de la proposition du projet APPRODYN, nous considérons avoir apporté des compléments intéressants sur les points suivants :

APPRODYN ajoute aux deux approches de l'étude NUREG/CR-6942 , trois approches nouvelles, reproductibles ou réutilisables.

Après un recensement de plusieurs approches, l'étude avait écarté les Réseaux de Petri Stochastiques tout en mentionnant leur capacité à représenter des modèles hybrides (travaux de Trivedi et Kulkarni, 1993). L'étude NUREG avait recensé et évalué une approche particulière, multi états, à base de digraphes, nommée Dynamic Flowgraph Methodology (DFM). Nous avions expérimenté cette approche [CHA 10], en préparation au projet APPRODYN, sans la retenir, car elle était inaccessible, à l'état de « boîte noire » au sein d'un logiciel commercial dédié (DYMONDA).

Les approches Simulation et Processus Markoviens Déterministes par Morceaux et Automates Stochastiques Hybrides sont dans le groupe des approches basées sur l'équation généralisée de Chapman-Kolmogorov recensées par l'étude NUREG/CR-6942 (CET, CCCM, CCMT et ESD), qui ne les mentionnait pas. De ce groupe, seule l'approche Markov/Cell to Cell Mapping Technique (CCMT) [ALD 91] a été expérimentée par la NUREG/CR-6942 . Nous apportons donc deux expérimentation supplémentaires à ce groupe important pour la modélisation des systèmes hybrides.

Enfin, il est à noter que les modèles développés dans le projet APPRODYN, développés en Open Source (SCICOS/SCILAB) ou avec des logiciels courants (MATLAB, MOCA-RP), sont facilement reproductibles ou réutilisables.

APPRODYN propose une représentation simplifiée et réutilisable du comportement du Générateur de Vapeur.

Le rapport NUREG/CR-6942 [NUR 07a] présente un modèle simplifié de comportement du GV. Cependant, nous avons eu des difficultés à le reproduire, et il n'a pas été possible de disposer du code développé pour l'étude. Nous avons donc employé un modèle et des données publiées et complétées pour ce cas test, pour qu'il soit reproductible ou réutilisable pour d'autres expérimentations. Ainsi l'interopérabilité entre le modèle physique numérique et le modèle type EPS se fait par deux étapes intermédiaires : un modèle linéaire simplifié du phénomène physique puis un modèle hybride du système.

APPRODYN propose une autre approche pour représenter les automates et réseaux numériques.

A partir du même type de système, APPRODYN propose de mener la modélisation de façon différente.

L'étude NUREG/CR-6942 à consacré beaucoup d'efforts à la modélisation de la logique de commande, en essayant de modéliser dans une même approche différents problèmes d'interaction. Le cas test présente en effet potentiellement ce que le rapport NUREG appelle des interactions entre processus physiques et commandes (type I), et des interactions entre composants numériques (type II). Les auteurs n'ont finalement pas pu traiter l'ensemble du problème ainsi posé.

Dana le projet APPRODYN, la stratégie de modélisation est de considérer qu'il n'est pas nécessaire de développer un modèle qui représenterait à la fois les interactions de type I et de type II qui serait très complexe. Chaque type d'interaction est modélisé séparément, avec des approches différentes. Puis, on reprend des modèles du type I, les seuls effets au niveau de la régulation, qui sont en fait peu nombreux au niveau d'une fonction applicative telle qu'une commande PID (gel, intempestif, défaillance à la sollicitation). Cela peut en fait se faire par l'intermédiaire de quelques paramètres fiabilistes (taux de défaillance, défaillance à la sollicitation, et probabilité de Défaillance de Cause Commune, cf chapitre 4.7.), intégrés dans les données employées par la modélisation hybride qui permettent ainsi l'interopérabilité entre les modélisations.

La modélisation des interactions de type II entre constituants programmés ne requiert pas de modélisation hybride. Elle peut se faire par l'emploi d'arbres de défaillance dynamiques, d'automates à évènements discrets, ou par des améliorations d'arbres de défaillance statiques; par exemple, avec la recherche d'interactions par l'emploi de facteurs beta, représentant les probabilités de défaillances de cause communes. Plusieurs articles proposent des approches de ce type ([THUY 09], [EPRI 10], [JOU 10], [DEL 11]..).

Ainsi le projet APPRODYN s'est focalisé sur la modélisation des interactions de type I, processus/commande et en a montré la faisabilité.

Il est à noter, pour la partie commande, que les *erreurs de spécification, de conception logique, ou de paramétrage* relèvent d'erreurs systématiques, et pourraient être identifiées ou simulées par les approches d'APPRODYN, en injectant des erreurs dans les fonctions de commande ou les automates de spécification.

APPRODYN propose une grille améliorée pour comparer les approches de fiabilité dynamique

Nous avons défini un certain nombre de critères qualitatifs, à partir de l'étude NUREG de référence, avec des adaptations et améliorations de ses critères. Nous avons distingué les critères qui concernent la méthode, ceux qui concernent l'outil informatique.

APPRODYN n'a pas traité de l'intégration avec la démarche EPS.

Outre outre des développements techniques à apporter aux approches ; il reste à lever le verrou de la compatibilité ou de l'interopérabilité de ces approches avec les démarches actuelles d'estimation probabiliste de la sûreté des systèmes (selon les domaines, EPS, PSA, nœud papillon…). Ces démarches sont en effet fondées sur des modèles discrets et statiques (arbres de défaillances et des arbres d'évènements), avec une prise en compte indirecte du temps et des phénomènes physiques. Ce verrou, fait partie de la problématique générale, formulée sous le terme d'« *Intégration des Approches Déterministes et Probabilistes (IDPSA)* ».

L'étude NUREG/CR-6942 a abordé ce verrou, en définissant ce système comme étant de sûreté et nécessaire au refroidissement du fluide primaire après un Arrêt Automatique Réacteur. Ainsi, pour les deux approches expérimentées (DFM et Markov/CCMT, une traduction a du être faite, pour représenter la commande numérique du système d'alimentation dans les arbres d'évènements. Cela a ouvert des questions, complexes, qui n'ont pas pu été traitées dans le cadre l'étude NUREG/CR-6942 : étude de sensibilité, mesure d'importance, calcul d'incertitude. L'interopérabilité avec un outil EPS, SAPHIRE a également été étudiée dans l'étude NUREG/CR-6942 .

Nous n'avons pas abordé ce point, ce n'était pas un objectif abordable étant données les ressources du projet. De plus, nous l'aurions fait de façon artificielle, car, pour le réacteur considéré par le projet APPRODYN le système étudié n'est pas de sûreté ; d'autres systèmes, décrit plus en détail dans les EPS, assurent une circulation d'eau secondaire dans le GV en cas de besoin, en particulier après un Arrêt Automatique Réacteur.

1.6 Dissémination

1.6.1 Rapports et présentations

En plus de ce rapport final, et d'une présentation au Sénat le 4 avril 2012, quatre présentations de l'avancement du projet ont été faites :

- Conseil Scientifique du GIS le 13 janvier 2011,
- « Workshop GIS 3SGS » le 12 octobre 2011 à Valenciennes,
- Journée SEE/GT S3 du GDR MACS du 18 janvier 2012 à Paris et à la
- Journée du GT INCOS du GDR MACS du 29 mars 2012 à Paris.

Ces évènements ont tenu lieu de rapports d'avancement[4], de plus plusieurs articles ont été élaborés en fin de projet.

1.6.2 Publications

4 publications ont été acceptées en 2012 pour des congrès :

[ZHA 12] H. Zhang, B. de Saporta, F. Dufour, G. Deleuze, Dynamic reliability: towards efficient simulation of the availability of a feedwater control system, 8th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC-HMIT), San Diego, USA, 2012 (accepté)

[SAP 12a] B. de Saporta, F. Dufour, H. Zhang, Predictive maintenance for the heated hold-up tank, PSAM11 & ESREL12, Helsinki, Finland, 2012 (accepté)

[ZHA 12b] H. Zhang, B. de Saporta, F. Dufour, G. Deleuze. Fiabilité dynamique : simulation d'un système de régulation du niveau d'eau d'un générateur de vapeur. Congrès Lambda Mu 18 Maîtrise des Risques et Sûreté de Fonctionnement. Octobre 2012 (accepté)

[BAB 2012] G. Babykina, N. Brînzei, J-F. Aubry, G. Deleuze, Modélisation et évaluation des systèmes complexes critiques en fiabilité dynamique par automates stochastiques hybrides. Congrès Lambda Mu 18 Maîtrise des Risques et Sûreté de Fonctionnement. Octobre 2012 (accepté)

1.6.3 Contribution à ouvrage collectif

[GIS 12] Aubry J.F., Babykina G, Brinzei N., Medjaher S., Barros A., Bérenguer Ch, Grall A., Langeron Y., Nguyen D.N., Deleuze G., De Saporta B., Dufour F., Zhang H., " Projet APPRODYN : approches de la fiabilité dynamique pour modéliser des systèmes critiques " in *Supervision, surveillance et sûreté de fonctionnement des grands systèmes*, Matta N., Vandenboomgaerde Y., Arlat J. (Ed.), Hermes Sciences - Lavoisier, Chapter 8, (2012), 181-222.

1.6.4 Identification des compétences sur les approches de modélisation de la SdF des systèmes hybrides

Au niveau français, l'équipe de Marne La Vallée, maintenant dispersée avait joué en France un rôle fondateur (Christine Cocozza, Sophie Mercier…). Un cas test plus simple,le cas test du réservoir, a été aussi abordé parYves Dutuit (Bordeaux) et André Cabarbaye (Cab Innovation).

Au niveau européen, la participation d'EDF R&D au séminaire « Deterministic/probabilistic safety analysis workshop» organisé par VTT et Scandpower en Octobre 2011[5] a permis d'identifier un certain nombre de centres de recherche européens impliqués dans des développements sur la

[4] Iinitialement prévus le 24 avril 2011, le 15 septembre 2011.

[5] Yvonne Adolfsson, Jan-Erik Holmberg, Göran Hultqvist, Pavel Kudinov, Ilkka Männistö, Proceedings of the Deterministic/probabilistic safety analysis workshop October 2011. VTT Public draft report, 2011.

modélisation des systèmes hybrides dans le cadre d'études de sûreté nucléaires. En plus de ces partenaires, nous avons fait référence aux travaux menés à l'Université Libre de Bruxelles (Etienne Labeau) et Polimi (Enrico Zio). Hors d'Europe, nous avons surtout repris les travaux de l'Université de l'Ohio (Tunc Aldemir).

2 Contexte et objectif du projet

2.1 Contexte

La sûreté des systèmes industriels à haute criticité repose en grande partie sur des systèmes programmés relativement complexes intrinsèquement (en terme de taille de code, architecture, nombre de variables traitées…) et extrinsèquement (nombre et nature des interactions entre les processus et le contrôle-commande). En 1985, [PER 84] caractérise un système complexe par la combinaison de deux attributs : les «interactions complexes» (interactive complexity) et le «couplage étroit» (tight coupling).

- ✓ Les interactions complexes conduisent à la présence de séquences inattendues et de non-linéarités (processus dynamiques), et à une compréhension incomplète du système.
- ✓ Le couplage étroit est caractéristique de processus interdépendants, et conduit à une sensibilité aux défaillances de cause commune.

Cette distinction à été déclinée dans des travaux précédents du NUREG relatifs à la modélisation d'un générateur de vapeur ([KIR 05] et à sa commande. Ainsi [NUR 07a], [NUR 06]) proposent deux types d'interactions:

- Interactions de type I, entre un processus physique (pressurisation, chauffage, echange de chaleur..) et sa commande. Cette interaction correspond aux interactions complexes de Perrow. Les systèmes présentant ces interactions sont des « systèmes dynamiques hybrides » parfois « non cohérents », qui ne sont pas représentables par une fonction booléenne invariante dans le temps
- Interactions de type II, entre les composants logiciels, matériels et logiciel enfouis (firmware) d'un système numérique. Elles correspondent aux interactions par couplage étroit de Perrow.Ces interactions sont dues à la présence de réseaux de communication, de traitements de type multi-tâche, multiplexage au sein de la commande. Elles sont importantes à analyser pour des systèmes numériques.

Pour les interactions de type I, les méthodes « classiques » d'évaluation de la sûreté se trouvent à leurs limites. En effet, elles consistent toutes peu ou prou à construire une fonction de structure sous forme d'équation booléenne, invariante dans le temps, des variables représentatives des états des composants (approche combinatoire statique). Il faut employer un langage d'évènements pour représenter correctement le système.

Cela mène à l'utilisation d'un formalisme de représentation du comportement du système du type états–transitions permettant de mettre en évidence les séquences d'évènements plutôt que leurs combinaisons sous forme de coupes ou de liens. C'est pour nous le caractère premier du « dynamisme » de la fonction de structure d'un système.

Au delà de ce premier point, le concept de « fiabilité des systèmes dynamiques hybrides» regroupe un ensemble de propriétés mises en évidence dans les travaux des dernières décennies, que nous résumons ici :

- les états du système sont définis par un Automate à Etats Finis (AEF). Ces états correspondent à des combinaisons des états des composants. Le nombre d'états des composants pouvant être différent du nombre de combinaisons possibles des états des composants, le système pouvant être arrêté avant un certain niveau de dégradation, une même combinaison d'états des composants peut être obtenue par des séquences incompatibles d'évènements ;
- chaque état du système est caractérisé aussi par un ensemble de variables continues et d'équations intégro-différentielles décrivant la physique de son évolution dans le temps ;
- le vieillissement des composants est une fonction qui dépend généralement du temps mais qui peut aussi dépendre de certaines des variables continues précédentes (exemple : température, pression, vitesse, etc.). En outre, des lois de vieillissement non dépendantes du temps peuvent être à considérer (par exemple, l'accumulation d'évènements de sollicitation) ;

- les changements d'état des automates employés pour la modélisation sont provoqués par des évènements de natures différentes : la défaillance ou la réparation d'un composant, mais aussi le franchissement d'un seuil associé à une variable continue (par exemple, une alarme impliquant la mise en marche d'une boucle de sécurité) ou à une variable numérale (par exemple, une accumulation d'évènements) ;
- des lois de probabilité différentes peuvent être associées à la défaillance ou à la réparation d'un même composant selon l'état dans lequel se trouve le système (par exemple, le vieillissement d'un composant peut dépendre de son mode de sollicitation, de sa stratégie de réparation, du niveau de contraintes associées à l'état présent du système…). C'est aspect définit la « fiabilité dynamique ».

La prise en compte de l'ensemble de ces considérations dans une même approche de l'évaluation fiabiliste d'un système n'est possible que par la simulation, la complexité analytique étant actuellement insurmontable.

Pour les interactions de type II, les approches de modélisation de la « fiabilité des systèmes dynamiques discrets», sont en général les plus pertinentes. Elles peuvent se faire par l'emploi d'arbres de défaillance dynamiques, d'automates à évènements discrets, voire par des améliorations d'arbres de défaillance statiques (recherche d'interactions par l'emploi de facteurs beta, représentant les probabilités de défaillances de cause commune). Plusieurs articles proposent des approches de ce type ([THUY 09], [EPRI 10], [JOU 10], [DEL 11]..). Nous ne les traitons pas dans ce projet

Dans notre cas, il n'est pas nécessaire de développer un modèle, très complexe, qui représenterait à la fois les interactions de type I et de type II. Cela peut se faire par l'intermédiaire de quelques paramètres (cf chapitre 4.7.).

2.2 Objectif

Ainsi, le projet a pour objectif d'expérimenter des approches de la fiabilité dynamique afin de supporter l'étude probabiliste de la sûreté de fonctionnement des systèmes de contrôle-commande critiques utilisés dans les domaines de la production d'énergie et des industries de procédé. Il s'intéresse à des approches à fort potentiel parfois encore peu « industrialisées » (c'est-à-dire encore peu formalisées ou outillées pour un industriel concepteur ou exploitant), et tente d'en évaluer leur potentiel sur un cas représentatif, en les comparant avec des approches de plus large diffusion, telles que les Réseaux de Petri Stochastiques.

3 Glossaire

AAR : Arrêt Automatique Réacteur
ABP: Réchauffeurs Basse Pression
ADG: Bâche alimentaire et dégazeur
AEF : Automate à Etats Finis
AHP: Réchauffeurs Haute Pression
API: Automate Programmable Industriel (en anglais: PLC (Programmable Logical Controller))
ARE: Régulation Débit Eau Alimentaire (ANG pour le palier CP0)
ASH (ou AHS) : Automate Stochastique Hybride (ou Automate Hybride Stochastique)
CCMT : Celle To Cell Markov Technique
CEX: Pompes d'extraction
DFM : Dynamic Flowgraph Methodology
EP : Essais Périodiques (ou Essais Révélateurs)
GV : Générateur de Vapeur
IDPSA : Integrated Deterministic Probabilistic Approaches (en français : Intégration des Approches Déterministes et Probabilistes).
IF : Indisponibilité Fortuite
MTBF : Moyenne des Temps de Bon Fonctionnement (en anglais : Mean Time Between Failures)
MTTR: Mean Time To Repair
MooN : M out of N. Cractérise le niveau d'une stucture redondée. S'écrit aussi M/N.
NRC : Nuclear Regulatory Commission
NUREG :Nuclear Regulatory Guide
Pfd : Probabilité de défaillance à la sollicitation
PMDPM : Processus Markovien Déterministe par Morceaux (en anglais : PDMP : Piecewise Deterministic Markovian Processes)
RdPS : Réseau de Petri Stochastique
SdF : Sûreté de Fonctionnement
SE : Système Elementaire
SED : Système à Evènements Discrets
TIF : Test Independent Failures
TPA: Turbo Pompe Alimentaire
VVP : Circuit Vapeur Principal

4 Présentation du cas test

Avertissement

Les données et modèles présentés dans ce chapitre sont *représentatifs* mais non *réels*. Des simplifications, transformations et approximations ont été faites, en particulier sur les points suivants:

Fonctionnement de la regulation
Comportement physique à l'intérieur du GV
Modes de défaillance de la partie tuyauterie, robinetterie, vannes (VVP)
Quantification des taux de défaillance, proportion entre modes de défaillance, défaillances de cause commune, des couts de maintenance

En conséquence, les difficultés méthodologiques et de calcul constatées sont représentatives du cas réel, mais les résultats quantitatifs obtenus ne le sont pas. Ils ne doivent pas être employés ou repris à d'autres fins que le cas test.

De même, la terminologie des descriptions fonctionnelles et dysfonctionnelles du cas test n'est pas complétement représentative de son domaine d'origine (nucléaire), afin d'en faciliter la compréhension par d'autres domaines. Enfin, le cas test traite de situations relevant de la disponibilité d'un système qui n'est pas classé de sûreté.

4.1 Généralités

Le projet a retenu le cas d'un système de régulation du niveau d'eau dans un Générateur de Vapeur (GV) d'un Réacteur à Eau Pressurisée de puissance 900 MW. La mission du système est de maintenir le niveau d'eau dans le Générateur de Vapeur, autour d'une position de référence. La mission échoue si le niveau d'eau augmente ou diminue au-delà ou en deçà de seuils limites, ce qui mène à une Indisponibilité Fortuite (IF) par Arrêt Automatique du Réacteur (AAR). Par la suite nous employons indifférement les termes IF ou AAR pour indiquer que le système n'assure plus sa mission. En réalité, les IF ne mènent pas systématiquement à un AAR, car il existe d 'autres systèmes de secours et d'autres critères d'arrêt.

Le circuit primaire du réacteur comporte 3 boucles, chacune équipé d'un GV. Nous ne représentons dans ce modèle qu'une seule boucle.

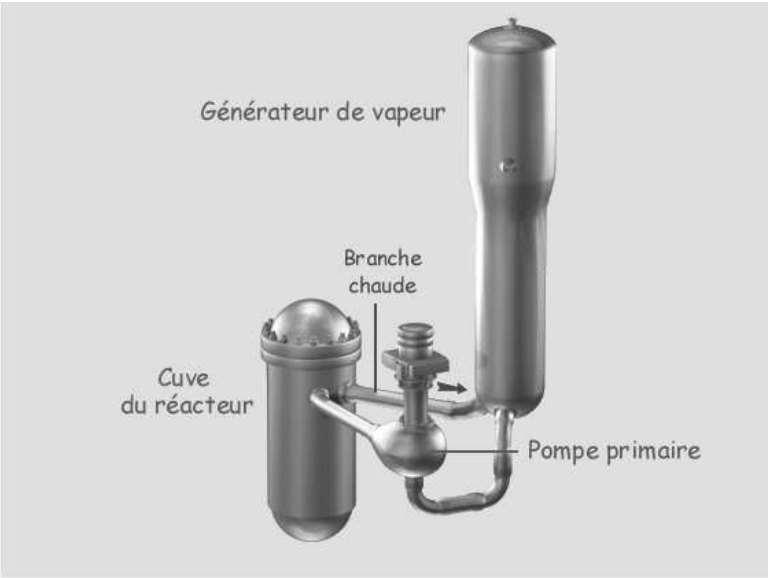


Figure 4.1. Représentation d'une boucle du circuit primaire d'un REP¨

Le générateur de vapeur est en pratique un échangeur thermique entre circuit primaire et circuit secondaire. Ses caractéristiques sont les suivantes

- Surface d'échange: 4746 m2
- Débit vapeur: 1820 t/hr
- Hauteur: 20,60 m
- Diamètre: 4,50 m
- Poids à vide: 300 t
- 3330 tubes assurent l'échange de chaleur entre eau du circuit primaire et eau du circuit secondaire.
- Durée de vie: environ 15 ans
- Soupapes tarées à 76,60 b

Ce cas test a pour intérêt d'être représentatif d'un système réel et d'englober des situations de cas test plus élémentaires employés dans la littérature de la fiabilité dynamique. Il peut être également assez facilement adapté à d'autres sources d'énergie ou d'autres situations rencontrées dans des industries de procédé.

Un cas test semblable a été proposé et décrit dans l'étude de référence NUREG/CR-6942 [MAN 08], [NUR 07] pour comparer des approches de fiabilité dynamique : la démarche DFM (Dynamic Flowgraph Methodology) et la démarche Markov/CCMT (Cell-to-Cell Mapping Technique). Cependant, les rapports rendus publics ne sont pas suffisants pour reconstituer un modèle reproductible. Nous avons donc développé un cas test complet.

Figure 4.2. Vue des parties internes du GV

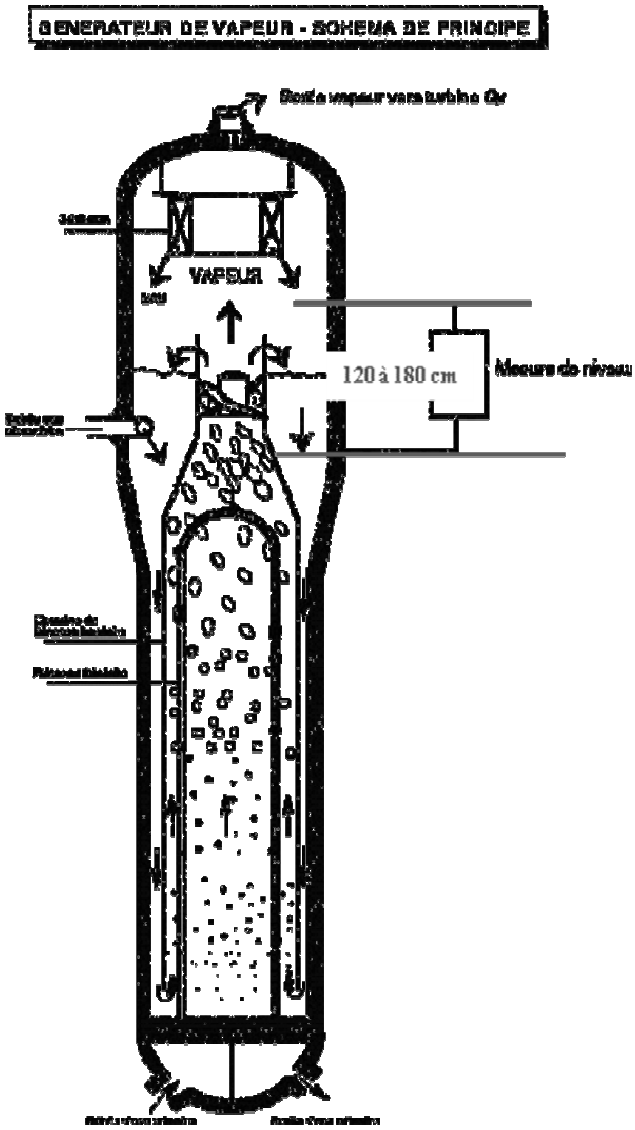


Figure 4.3. Schéma de principe du GV, avec la représentation de la plage de variation du niveau d'eau à surveiller.

P sortie vapeur GV: 55-58 b
T sortie vapeur GV: 270-273 °C
P eau alimentaire GV: 70 b
T eau alimentaire GV: 220°C (préchauffée)
T primaire entrée GV : 324°C
T primaire sortie GV: 280°C

Note : L'eau du primaire perd environ 40°C dans le GV, elle vaporise l'eau du secondaire, ne la réchauffe pas.

4.2 Eléments pour la modélisation du procédé

4.2.1 Modèle comportemental du GV

L'interface entre l'eau et la vapeur dans le GV est un mélange diphasique eau-vapeur sous pression, de ce fait la loi de variation du niveau d'eau dans le GV est difficile à modéliser. En particulier, on observe le phenomène de "swelling", gonflement du mélange diphasique causé par une variation de puissance thermique apportée au GV. Sous certaines conditions, il peut mener à une élévation du niveau de mélange dans le GV alors que la puissance diminue.

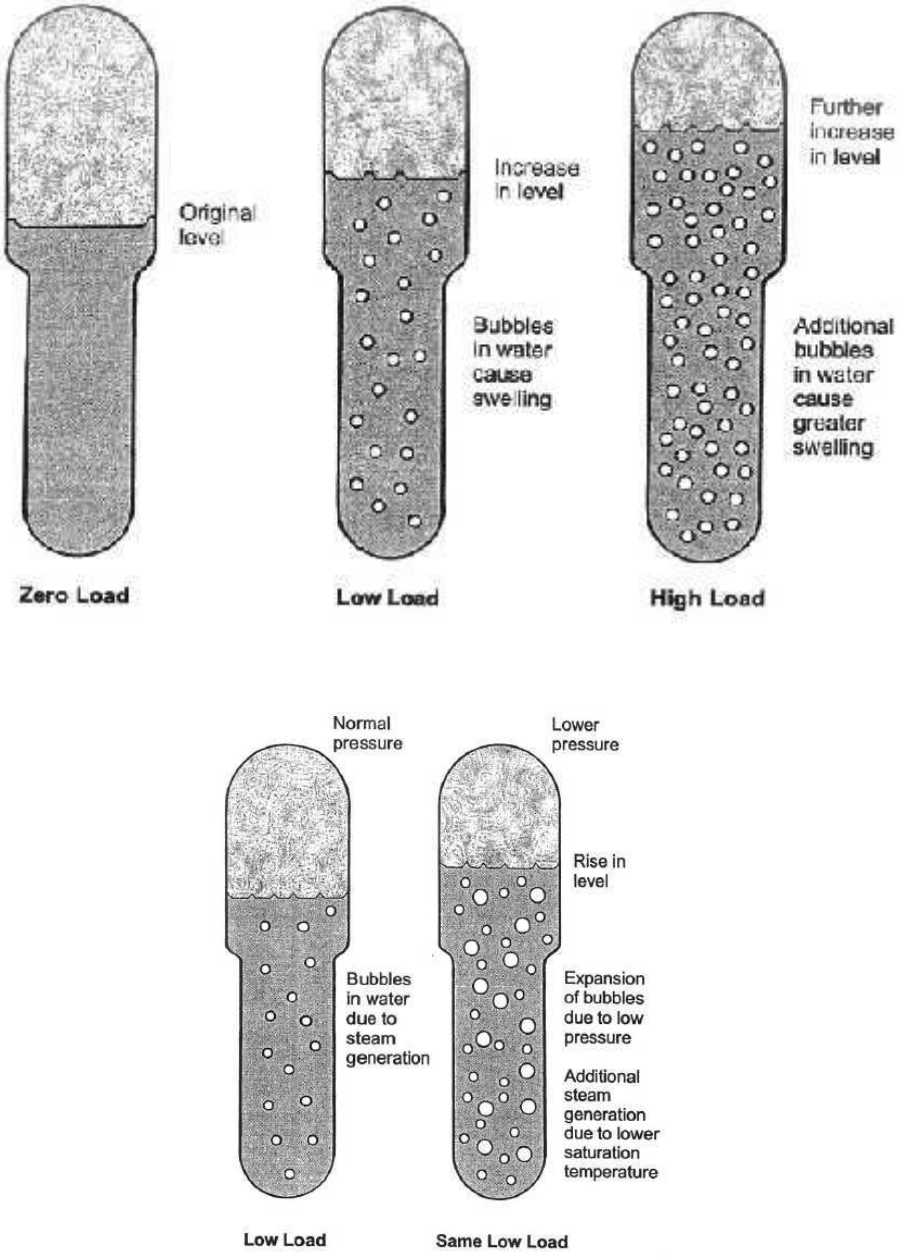


Figure 4.4. Illustration du phénomène de swelling[6]

[6] Doc. University Network of Excellence in Nuclear Engineering

Pour ce projet, qui s'intéresse à la modélisation hybride pour étudier la sûreté de fonctionnement d'une logique de commande, un modèle simplifié est suffisant.
Un modèle linéaire complet est employé, à 4 variables continues, avec une modification apportée dans [Kothare, 2000]. Il est obtenu à partir d'un modèle publié entre 1998 et 2000 par EDF pour une comparaison de fonctions de commande[7].
On considère deux niveaux, Nge, niveau du mélange diphasique, et Ngl niveau d'eau. On emploie un modèle simplifié linéaire, avec 4 variables d'état, et des coefficients qui dependent de la puissance apporté par le circuit primaire (P) et du débit d'eau alimentaire.

Le vecteur des variables d'état du système est **y**= [Nge, Ngl, Qv, Qe] avec:

Nge, niveau du mélange diphasique, c'est le niveau mesuré par les capteurs
Ngl, niveau d'eau,
Qe, debit d'eau alimentaire (regulé par la vanne ARE), Qe est une commande, notée conventionnellement u, du système de régulation
Qv, debit de vapeur (consommée par la turbine). Qv est une perturbation, , notée conventionnellement d, du système de régulation .

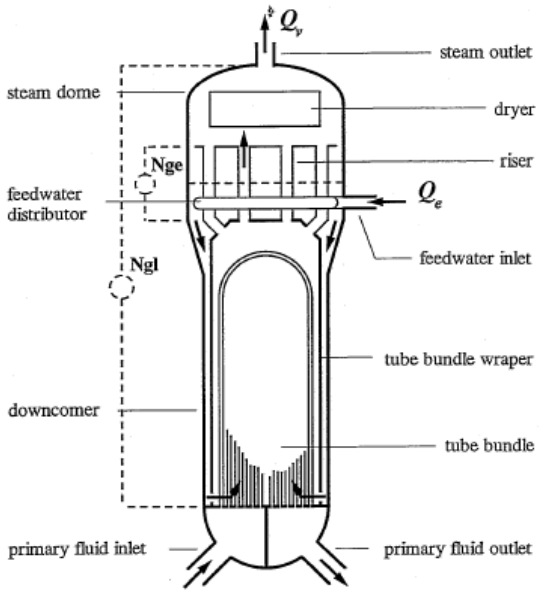


Figure 2: Schematic of a UTSG

Figure 4.5. Vue shématique du GV, et situation des variables continues modélisées

L'expression générale de la variation du niveau d'eau dans le GV est la suivante :

$$\boldsymbol{y}(t) = \boldsymbol{C}.\boldsymbol{x}(t) + \boldsymbol{D}.d(t)$$
$$\frac{\partial \boldsymbol{x}}{\partial t} = \boldsymbol{A}.\boldsymbol{x}(t) + \boldsymbol{B_u}.u(t) + \boldsymbol{B_d}.d(t)$$

[7] [EDF , 1998] HP-33/98/010/A Commande MPC pour contrôler le niveau d'eau de Générateur de vapeur REP P. BENDOTTI, C.M. FALINOWER

Il s'agit d'une système d'équations différentielles non linéaire (les coefficients dépendent d'une des variabbles, Qv). Les relations entre les grandeurs physiques (Qv, Qe, Nge, Ngl) peuvent être modélisées par deux fonctions de transfert.

$$N_{ge}(s) = \frac{1}{T_n s}\left(\frac{Q_e(s)}{(1+\tau s)(1+T_h s)} - \frac{1-F_g T_g s}{1+T_g s} Q_v(s)\right), \qquad N_{gl}(s) = \frac{1}{T_{\text{int}} s}\left(Q_e(s) - Q_v(s)\right),$$

où T_n, F_g, T_h, τ sont des paramètres qui dépendent uniquement de Pn.

$T_g = 10$ sec et $T_{\text{int}} = 140$ sec sont constants. $\frac{1}{T_n s}$ et $\frac{1}{T_{\text{int}} s}$ représentent l'effet de la capacité massique du GV. Ils permettent d'estimer la variation de niveau d'eau. Les effets de gonflement et de contraction de l'eau du GV sont représentés dans les coefficients de de $Q_e(s)$ et de $Q_e(s)$ (débit de vapeur)

Le terme $1 - F_g T_g s$ permet de prendre en compte le phénomène de gonflement

Avec $y_1 = N_{ge}, y_2 = N_{gl}$, $d = Q_v$ et $u = Q_e$, et **D**=0, nous obtenons le modèle linéaire suivant d'équations différentielles :

$$\dot{x}(t) = \begin{bmatrix} 0 & 0 & 0 & \frac{1}{T_n} \\ 0 & -\frac{1}{T_h} & 0 & -\frac{1}{T_n} \\ 0 & 0 & -\frac{1}{T_g} & 0 \\ 0 & 0 & 0 & -\frac{1}{\tau} \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix} u(t) + \begin{bmatrix} -\frac{1}{T_n} \\ 0 \\ \frac{1+F_g}{T_n} \\ 0 \end{bmatrix} d(t),$$

$$y(t) = \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ \frac{T_n}{T_{\text{int}}} & 0 & 0 & \frac{\tau}{T_{\text{int}}} \end{bmatrix} x(t).$$

Le tableau suivant fournit les valeurs des coefficients en fonction de la puissance P, exprimée comme un pourcentage de la puissance nominale Pn.

$P_n(\%)$	**3.2**	**4.1**	**9.5**	**24.2**	**30**	**50**	**100**
T_n	36	56	63	44	40	40	40
F_g	13	18	10	4	4	4	4
T_h	170	56	30	10	8	5	5
τ	10	10	10	30	30	30	30

Ces coefficients proviennent de simulations physiques numériques détaillées. Pour faire les calculs à des niveaux intermédiaires (2%, 60%..), des interpolations sont faites.

Ainsi l'interopérabilité entre le modèle physique numérique et le modèle type EPS se fait par deux étapes intermédiaires : un modèle linéaire simplifié du phénomène physique puis un modèle hybride du système.

4.3 Description fonctionnelle simplifiée de l'installation

Nous avons modélisé le Générateur et Vapeur et une partie du circuit secondaire d'un Réacteur à Eau Pressurisée (cf figure n°4.6.), constituée de trois systèmes en aval du condenseur, et le barillet VVP, pour l'amont, qui concentre la vapeur issue des Générateurs de Vapeur (GV). Le reste du circuit secondaire ne nous intéresse pas pour le cas test, il n'apporte pas de comportements différents, et est représenté sous forme de perturbations d(t).

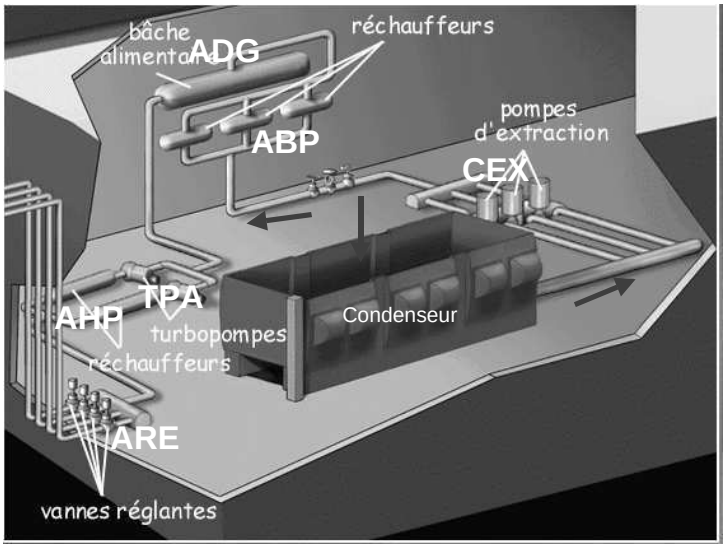


Figure n°4.6. Partie aval du circuit secondaire d'un Réacteur à Eau Pressurisée représentée dans APPRODYN

Un diagramme de fiabilité de l'ensemble du circuit secondaire, en simplifiant la partie amont au condenseur est donné en figure 4.7.:

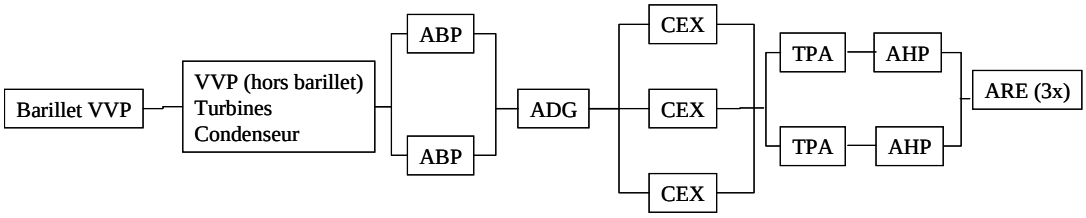


Figure n°4.7.

ADG: Bâche alimentaire et dégazeur
ABP: Réchauffeurs Basse Pression
AHP: Réchauffeurs Haute Pression
CEX: Pompes d'extraction. 2 pompes en service, 1 pompe en secours.
ARE: Régulation Débit Eau Alimentaire
TPA: Turbo Pompe Alimentaire.

De plus, les parties passives des systèmes élémentaires suivants ont été représentées en étant intégrées à VVP. Il s'agit de :

ADG: Bâche alimentaire et dégazeur
ABP: Réchauffeurs Basse Pression
AHP: Réchauffeurs Haute Pression
Le diagramme de fiabilité employé pour le projet ne conserve que les parties actives du circuit en aval du condenseur et le barillet VVP.

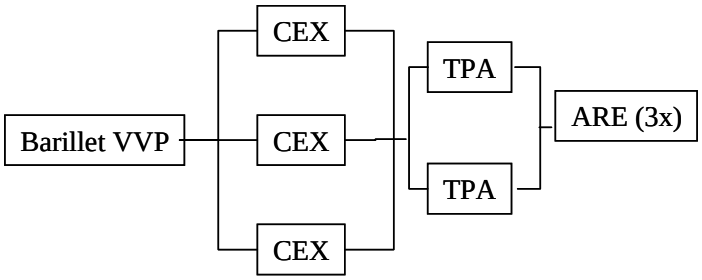


Figure n°4.8.

4.4 Fonctions des systèmes élémentaires

Le barillet VVP permet de maintenir le fonctionnement des turbopompes, sécheurs, etc…même en cas de perte d'un GV. Une rupture du barillet VVP est une défaillance de point unique ; elle représente un niveau minimal de fiabilité du système. Les défaillances du barillet VVP permettent aussi de représenter les défaillances des autres systèmes passifs (bâches, réchauffeurs, barillet en aval des vannes ARE).

Les trois pompes CEX maintiennent le vide au condenseur et permettent d'assurer un débit d'eau alimentaire. Elles sont redondées en 2/3, la troisième pompe est à l'arrêt, en attente. Elle est démarrée lorsqu'une des autres pompes tombe en défaut. La pompe en défaut, une fois réparée, reste en attente

Les deux turbopompes TPA assurent la pression commune aux trois GV, elles débitent dans un barillet commun modélisé dans la partie VVP. Elles fonctionnent en meme temps. En cas de défaillance d'une TPA, l'autre passe en survitesse et assure 60% de la charge. On considère dans ce modèle que la puissance de l'installation passe à 60% de son maximum (60% Pn) tant qu'une seule TPA fonctionne.

Enfin, un système de vannes réglantes ARE règle le débit pour chaque GV. Elle est formée de deux sous systèmes: une vanne petit débit (0 à 400 tonnes/h) et une vanne gros débit (0 à 1815 tonnes/h). La vanne petit débit, plus réactive, est employée de 2% Pn jusqu'à 15% Pn environ, sachant qu'elle peut fournir jusqu'à 23% Pn. La vanne gros débit est employée à partir de 15% Pn environ. Une régulation assure le basculement entre les deux vannes. Le temps de réponse de la vanne en ouverture/fermeture permet de suivre les variations de puissance de l'installation.

4.5 Profils de fonctionnement

4.5.1 Cycles normaux

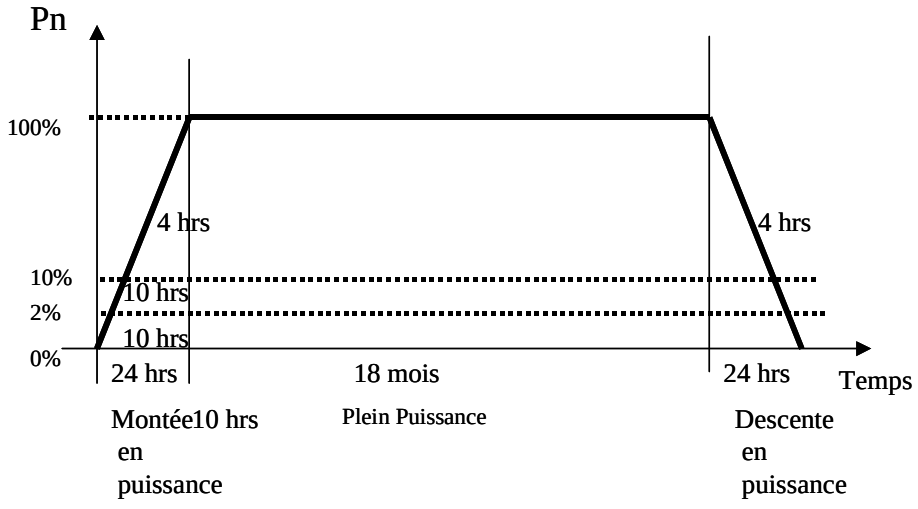
Deux scénarios peuvent être considérés. Ces scénarios peuvent subir des perturbations, en particulier des Arrêts de Production pour des causes diverses (arrêt turbine, arrêt du réacteur, etc.)., autres que celles imputables à la régulation des GV. Dans le cadre du projet, on ne considère que le scénario n°1.

En cas d'AAR, la tranche est à l'arrêt (0% Pn) pendant le temps nécessaire à l'identification et à la correction de la cause de l'AAR (de quelques heures à quelques jours, sauf aléa majeur), puis on redémarre depuis 0% Pn selon la rampe de montée en puissance. Pour les deux scénarios, elle dure 24 heures.

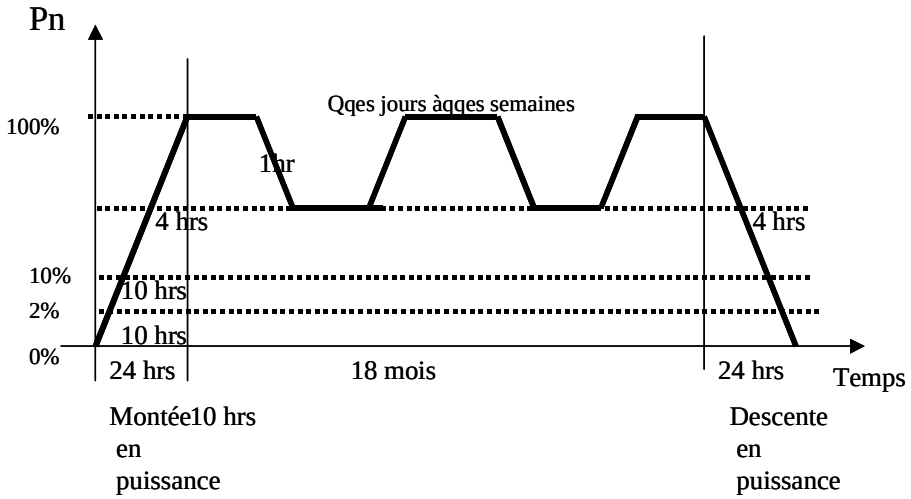
Sauf avarie grave, on considère que le temps mis pour revenir à pleine puissance après un AAR est de 8 heures (identification du problème, réparation, redémarrage).

Figure 4.9. Les scénarios de fonctionnement

Scénario n°1: fonctionnement en base, pleine puissance, sans aléas



Scénario n°2: fonctionnement à puissance variable



4.5.2 Perturbations

D'autres évènements peuvent causer un AAR et sont considérés comme des perturbations des cycles de fonctionnement:

- Arrêt du Groupe Turbalternateur (« trip turbine »), qui entraine la perte de demande en vapeur et l'ordre d'AAR. La perte de Groupe Turbalternateur est représentée dans le modèle APPRODYN comme un évènement perturbateur, par deux mécanismes :
  - Un evenement « Groupe Turboalternateur » de taux de défaillance 1.10-7/hr et de MTTR 2159 hrs
  - Un ensemble d'evenements « Mise en Sécurité Turbine » de taux de défaillance global 5,05.10-6/hr et de MTTR 8 heures.
- Perte du vide au condenseur. Cet évènement entraine une perte d'alimentation en eau de l'ARE, et l'ordre d'AAR, avec un taux de défaillance global 4,79.10-5/hr, et un MTTR = 8 hr (redémarrage).
- AAR pour raison autre:
  - perte de systèmes supports : fluides, air comprimé, alimentation électrique 48V, 220 V ou 6600 V….
  - cause liée au circuit primaire…

  Ces évènements ne sont pas modélisés dans le projet. Les fréquences varient de 1/an à 2.10-6/hr, avec des MTTR de 8 hr à 168 hr.

4.5. Propriétés attendues du système

Nous présentons ici les propriétés (ou exigences) que le système doit respecter pour ne pas causer d'Arrêt de Production. Comme elles concernent un évènement lié à la disponibilité, nous les appelons "Propriétés de Disponibilité".

4.5.3 Niveaux d'eau dans le Générateur de Vapeur

Plusieurs critères mènent à un Arrêt Automatique Réacteur (AAR), qui est l'évènement à éviter. Pour ce modèle qui porte sur des régulations, nous nous intéressons à la « gamme étroite », dans laquelle le niveau d'eau doit être maintenu.

Niveau (m)	Gamme (%)	Critère d'arrêt	Remarque
+2,6	100%		
+1,1	75%	NTH (Niveau Très Haut)	Arrêt
0	44%	NH (Niveau Haut)	Niveau atteint avec charge > 20% Pn. Consigne à tenir à +/-5%, sinon alarme (sans Arrêt Automatique)
-0,4	33%		Niveau à 0%Pn. Passe de 33 à 44% lorsque Pn passe de 0 à 20%.
-0,7	25%	NB (Niveau Bas)	Arrêt si coincidence avec déséquilibre entre débit Eau et débit Vapeur sur un GV (facteur 2)
-1	15%	NTB (Niveau Très Bas)	Arrêt par autre système
-1,6	0%		

Tableau n° 4.1.

4.5.4 Autres propriétés attendues du système étudié

La défaillance complète ou un défaut majeur détecté sur 2/3 pompes CEX, 2/2 TPA, une fuite détectée sur VVP causent directement un AAR du système.

4.6 Modélisation de la logique de commande

La logique de commande est constituée de trois types d'éléments: capteurs, actionneurs, automates. La fonction de commande est implémentée dans un automate.

4.6.1 Fonction de commande

Le procédé est représenté par la variable d'intérêt physique, Y, qui caractérise le niveau d'eau à l'intérieur du GV. La commande utilise sa mesure et régule le débit d'eau injecté dans le GV.

La fonction de commande comporte deux parties) :

- Régulateur : système de contrôle du procédé. Dans les modèles effectués dans le cadre d'APPRODYN, le contrôle est effectué par une régulation type PID.
- Installation : tuyauteries, pompes, vannes des circuits et le modèle du GV. La turbine et condenseur ne sont pas représentés explicitement, certains comportements sont inclus dans la perturbation d.

En pratique, le système est non linéaire, et plusieurs types de régulations peuvent être employés (MPC, PID non linéaire, PID linéaire…). Les approches retiendront le type de régulation qu'elles peuvent représenter, en l'occurrence une régulation PID non linéaire.

Avec les notations conventionnelles d'une fonction de commande, les variables sont les suivantes:

- Y = y(t) = [Nge, Ngl] sortie du modèle, variable d'intérêt physique, niveau d'eau à l'intérieur du GV
- d = Qv, perturbation,
- y_m : mesure de Y : contrainte (perturbation) définie par le mode de fonctionnement.
- u = Qe : commande du système de régulation (débit d'eau alimentaire dans le GV)
- Y- y_m : dérives et bruit sur les capteurs

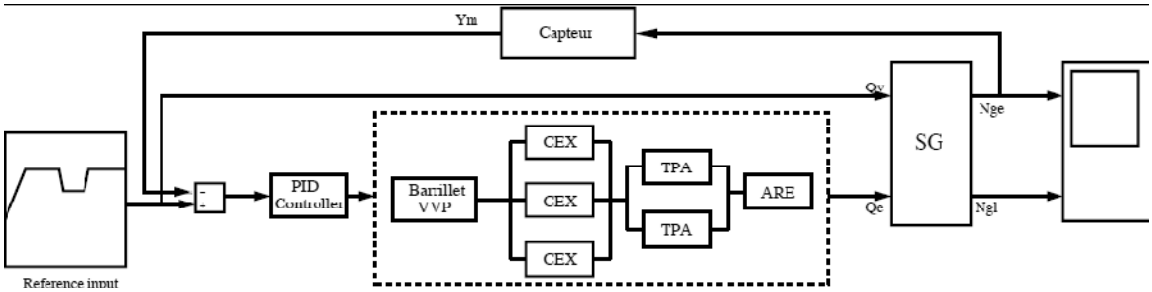


Figure 4.10. Représentation de la régulation du système d'alimentation en eau du GV

4.6.2 Capteurs

Deux technologies sont possibles : capteurs conventionnels ou « intelligents ». Pour le projet, nous représentons une technologie conventionnelle. Les données de fiabilité relatives aux capteurs sont exposées au chapitre 4.11.

4.6.2.1 Capteurs conventionnels

Les capteurs conventionnels sont analogiques. La précision et la fiabilité des capteurs de niveau évolue en fonction du temps (par l'effet du vieillissement ou des arrêts répétés du système), et dépend des niveaux atteints par les paramètres physiques dans le GV. Cet aspect est de type « fiabilité dynamique »
Les capteurs conventionnels présentent trois mécanismes de dégradation : dérive continue à la hausse ou à la baisse d'une mesure ; dérivé par saut, mesure « collée » à une valeur. Ces mécanismes sont réduits par la redondance.
Les capteurs conventionnels ne sont pas capables d'autodiagnostic et de correction.

4.6.2.2 Capteurs « intelligents »

Les capteurs « intelligents » peuvent remplacer les capteurs conventionnels et mesurent les mêmes variables. Ils présentent une partie analogique et une partie numérique programmée. De ce fait, ils sont capables d'autotest, de correction de certaines erreurs et peuvent être paramétrés.

Les capteurs « intelligents » présentent des mécanismes de dégradation comparables aux capteurs conventionnels, qu'ils peuvent cependant, dans une certaine mesure, détecter et corriger: dérive continue à la hausse ou à la baisse d'une mesure ; dérivé par saut.

Les capteurs « intelligents » présentent des mécanismes de défaillance particuliers à leur technologie : erreur de paramétrage et erreur de codage/spécification pouvant mener à une perte de mesure ou une mesure « collée ». Ces mécanismes peuvent résulter d'erreurs systématiques et ne sont pas réduits par la redondance.

4.6.3 Autres automatismes

Les pompes CEX et TPA disposent également d'automatismes de commandes et de régulation. Ces automatismes présentent individuellement des difficultés de modélisation de niveau comparable ou plus faible que celui de l'ARE. Ils ne sont donc spécifiés dans le cas test.
Cependant, à un niveau de modélisation « Extrême » de système hybride, il pourrait être envisagé de les modéliser, avec la représentation des interactions logiques possibles entre CEX, ARE et TPA qui seraient dûes à des erreurs ou défaillances partagées entre les automatismes. Cependant, ce sont des interactions de type II, que l'on peut étudier par d'autres approches.

4.6.4 Mesures et logiques de vote

Les grandeurs physiques mesurées sont :
- le débit vapeur (Qv),
- le débit eau (Qe),
- le niveau Nge eau/vapeur « gamme étroite »
- le niveau Ngl eau « gamme large », que nous ne prenons pas en compte ici (Ngl est une grandeur dépendante de Nge et sa mesure n'est pas utile au système de régulation).

Les mesures sont effectuées par des capteurs, selon l'organisation donnée dans le tableau 4.2. :

Mesure	**Installation**	**Technologie**
Mesure Nge gamme étroite NTB (Niveau Très Bas) et NTH (Niveau Très Haut)	3 capteurs du système ARE/ANG par GV.	Mesure de pression. Précision 5% Eventuellement convertie en hauteur Tout Ou Rien en 2oo3
Mesure débit eau alimentaire (Qe)	2 capteurs du système ARE/ANG par ligne d'alimentation d'un GV 1 seul employé à la fois pour la régulation.	Mesure de débit (t/h) + Venturi Précision 2%
Mesure débit Vapeur (Qv)	2 capteurs du système VVP par ligne de sortie d'un GV	Mesure de pression convertie en débit Précision 5%
Mesure Nge gamme étroite NB (Niveau Bas)	Mesure de Niveau Bas : cf NTB et NTH Mesure déséquilibre eau vapeur , par GV : 2 comparaisons capteur débit eau (Qe) et capteur de débit vapeur (Qv) en ½	Arrêt si coincidence Niveau Bas avec déséquilibre entre débit Eau et débit Vapeur sur un GV (facteur 2)
Mesure Ngl gamme large (non modélisé)	1 capteur du système ARE/ANG par GV	Mesure de pression convertie en hauteur Tout Ou Rien Précision 2,5%

Tableau 4.2. Organisation des mesures

Des Essais Périodiques sont menés sur les capteurs pour assurer un écart <5% entre capteurs. La valeur mesurée du capteur est comparée avec la moyenne des deux autres. Si le capteur est en écart de plus de 5% avec la moyenne des deux autres capteurs, il est inhibé et déclaré défaillant. Il est ensuite remis en ligne, même si, après réparation, l'écart persiste.

4.6.4.1 Logiques de vote

Certains capteurs sont en redondance. Les mesures sont intégrées par des logiques de vote ou des moyennes, avec inhibition d'un capteur qui présente une anomalie détectée.

Mesures continues

Dans le cadre du projet, nous avons considéré ce cas pour la mesure Nge gamme étroite. Deux règles sont possibles:

Règle n°1 : Calcul de moyenne. La valeur mesurée est la moyenne des valeurs des trois capteurs. Les dérives de capteurs éventuelles sont détectées au mieux lors des Essais Périodiques.

Règle n°2 : Calcul de moyenne avec inhibition. On commence par comparer la valeur mesurée pae chaque capteur avec la moyenne des deux autres. Si le capteur est en écart de plus de 10% avec la moyenne des deux autres capteurs, il est inhibé et déclaré défaillant. Une action de réparation est lancée. Puis, la valeur mesurée est la moyenne des valeurs des capteurs non inhibés.

Mesures Tout Ou Rien

On suit une règle en 2oo3

4.6.5 Essais périodiques

Des Essais Périodiques sont menés sur les capteurs pour assurer un écart <5% entre capteurs. L'écart est mesuré par rapport à la moyenne des deux autres capteurs.

4.6.6 Actionneurs

Deux technologies sont possibles : actionneurs conventionnels ou « intelligents »
Les actionneurs (ou actuateurs) sont modélisés en étant intégrés aux vannes réglantes ARE et au pompes TPA à vitesse variables et à l'instrumentation de la pompe CEX. Ils ne sont pas plus détaillés dans le projet.

4.6.6.1 Actionneurs conventionnels

Les erreurs affectant l'instrumentation conventionnelle (défaillance à la sollicitation, blocage…) sont représentées dans les défaillances à la sollicitation et la proportion de défaillances non détectables de la partie « installation » du modèle.

4.6.6.2 Actionneurs intelligents

Les actionneurs « intelligents » présentent une partie analogique et une partie numérique programmée. De ce fait, ils sont capables d'autotest, de correction de certaines erreurs et peuvent être paramétrés.
Les actionneurs « intelligents » compensent en partie des défaillances affectant l'instrumentation conventionnelle (défaillance à la sollicitation, blocage…) et permettent de détecter des défaillances des instruments qu'ils pilotent (fuites..).
Les actionneurs « intelligents » présentent des mécanismes de défaillance particuliers à leur technologie : erreur de paramétrage et erreur de codage/spécification pouvant mener à une perte de mesure ou une commande « collée ». Ces mécanismes peuvent résulter d'erreurs systématiques et ne sont pas réduits par la redondance.

4.7 Représentation des Automates Programmables Industriels (API)

Nous pouvons représenter une architecture de Contrôle-Commande selon la hiérarchie suivante :

I. Système de Contrôle-Commande (I&C system level)
II. Division
III. Armoire
IV. Module
V. Composant de base (carte)

Le cas test APPRODYN détaille une fonction applicative spécifique (régulation par PID d'un niveau d'eau GV), qui est implémentée au niveau IV. Les erreurs et défaillances affectant les autres niveaux sont représentés uniquement par leurs effets sur l'application spécifique, à son niveau.

Trois grandes familles technologiques sont possibles (cf tableau 4.3.). Les technologies peuvent être combinées. Par exemple, une logique 100% conventionnelle, une logique programmée avec des capteurs conventionnels ou une logique 100% programmée, etc….

Niveau	Technologie conventionnelle	Technologie programmée	Technologie « émulée »
Capteur	Analogique	Capteur avec partie analogique et partie programmée (microprocesseurs et microcontroleurs)	Capteur avec partie analogique et partie programmée (FPGA…)
Actionneur	Relais et analogique	Actionneur avec partie analogique et partie programmée	Actionneur avec partie analogique et partie logique « cablée » (FPGA…)
API de régulation	Relais et analogique	Automate programmé (microprocesseurs)	Automate à logique « cablée » (FPGA…)
Point fort	Peu d'intempestifs	Autotest élevé Capacités de correction Pas de dérive des automates	Défaillances résiduelles systématiques limitées Capacités de correction Pas de dérive des automates
Point faible	Autotest limité Possibles dérives des automates, pas de correction	Défaillances résiduelles systématiques	Autotest moyen

Tableau 4.3. Comparaison de familles technologiques d'API, capteurs et actionneurs.

Nous avons vu au chapitre 2.1. que le cas test APPRODYN porte sur les interactions de type I, entre procédé et commande.

Nous considérons que la technologie de la commande n'a pas d'effet direct en terme de modélisation. Elle influe sur les valeurs de certaines données de fiabilité des Systèmes Elementaires (ordre intempestif, défaillance à la sollicitation, probabilité de Défaillance de Cause Commune), mais pas sur leur nature. Ces valeurs sont fournies par la suite, en tant que données de fiabilité.

Les taux de défaillance prennent principalement en compte les défaillances fonctionnelles d'origine *matérielles* des API, et des réseaux, et certains transitoires d'origine physique (Single Event Upset, SEU, causé par interaction silicium-rayonnement ionisant d'origine naturelle).

Les autres défaillances, d'origine *logicielles ou interaction logiciel/matériel,* concernent les technologies numériques, et sont issues des interactions de type II (cf chapitre 2.1.).

Les effets de ces interactions, issues des divers niveaux d'architecture d'un système de Contrôle-Commande, sont en fait peu nombreux au niveau d'une fonction applicative telle qu'une commande PID : gel, intempestif, défaillance à la sollicitation. Ils peuvent être représentés par quelques paramètres probabilistes : taux de défaillance, défaillance à la sollicitation (Pfd), et probabilité de Défaillance de Cause Commune. Ce nombre réduit de paramètres probabilistes intégrés dans les données employées par la modélisation hybride permet ainsi l'interopérabilité entre les modélisations.

La modélisation des interactions de type II entre constituants programmés ne requiert pas de modélisation hybride. Elle peut se faire par l'emploi d'arbres de défaillance dynamiques, d'automates à évènements discrets, ou par des améliorations d'arbres de défaillance statiques; par exemple, avec la recherche d'interactions par l'emploi de facteurs beta, représentant les probabilités de défaillances de cause communes. Plusieurs articles proposent des approches de ce type ([THUY 09], [EPRI 10], [JOU 10], [DEL 11]..). Enfin, pour les API , les *erreurs de spécification, de conception logique, ou de paramétrage* relèvent d'erreurs systématiques, d'origine humaine et organisationnelle, leurs causes profondes ne sont pas spécifiques à une technologie. Elles peuvent être identifiées ou simulées par les approches d'APPRODYN, en injectant des erreurs dans les fonctions de commande, dans les limites classiques de la testabilité[8]... L'injection de fautes n'a pas été faite dans ce projet.

4.8 Données de fiabilité et graphes d'états

Les données de fiabilité sont représentatives d'observations sur 34 tranches, exploitées depuis 1992, selon des cycles de 18 mois, interrompus d'arrêts techniques de 1 à 3 mois.

4.8.1 Valeurs de Taux de défaillance, Pfd

Les premières simulations ont fourni une hiérarchisation des systèmes un peu décalées par rapport aux observations. Les systèmes VVP, TPA et ARE sont, selon le REX, à peu près de même importance.
Les valeurs suivantes ont été révisées pour prendre en compte ce constat.

Tableau 4.4.

Composant	Taux de défaillance (par h)	Pfd (par sollicitation)
Barillet VVP	2,17.10-5	-
Pompe CEX	4,35.10-5	1,95.10-3
TPA hors turbine	1,46.10-4	5,45.10-4
Turbine des TPA	5,9.10-4	3,90.10-3
Vanne ARE	3,53.10-5	5,85.10-3
Capteur de mesure de niveau	5,2.10-6	-
Capteur de mesure de débit eau alimentaire	10-4	-
Capteur de mesure de débit vapeur	10-4	-
Capteur de mesure de niveau (gamme large)[9]	1,7.10-6	-
Instrumentation CEX[10]	6,5.10-6	1,95.10-3
Instrumentation TPA[11]	1,85.10-6	5,45.10-4
PID et instrumentation ARE[12]	2.10-5	5,85.10-3

Rappel : Pfd : Probabilité de défaillance à la sollicitation

[8] problème de l' «oracle »: il est difficile d'injecter des fautes auxquelles on a pas pensé dans les specifications).
[9] Non modélisé
[10] Avec périodicité d'inspection de 3 mois
[11] Avec périodicité d'inspection de 3 mois
[12] Avec périodicité d'inspection de 3 mois

4.8.2 Vieillissement

Nous avons considéré des taux de défaillance constants. En fait, certains phénomènes de vieillissement peuvent se produire sous l'effet du temps, ou de phénomènes physiques extrinsèques au procédé (par exemple, vieillissement de certains composants électroniques…). Ils peuvent, en absence de maintenance adaptée, aggraver la fréquence des défaillances unitaires des AAR, le risque d'échec en réparation ou d'échec à la sollicitation. L'amélioration du modèle peut être faite en employant des taux de défaillance non exponentiels, ou en approchant un vieillissement par une fonction en escaliers.

Dans le cadre du projet APPRODYN, nous n'avons pas représenté de taux de défaillance non constants.

De plus certains mécanismes présentent des rétroactions positives et peuvent requérir un aspect « fiabilité dynamique » de la modélisation. Plusieurs scénarios sont envisageables:

- Scénario 1 : Vieillissement de matériel par cumul d'évènements discrets dus à la défiabilité ou au vieillissement d'autres matériels (par exemple, vieillissement des parties mécaniques par cumul d'AAR). Par exemple:
    - Le vieillissement des matériels peut être dû à un effet cumulatif des arrêts/redémarrage sur les parties passives (barillet) et mécaniques de l'installation et augmenter les fréquences des arrêts/redémarrage, selon une relation logarithmique, linéaire ou puissance.
    - Le passage en survitesse ou en surrégime de certains matériels ou la sollicitation fréquente d'actionneurs pour compenser des dérives d'autres composants (capteurs, régulateurs..) peut causer une baisse de leur fiabilité, augmenter les fréquences des arrêts/redémarrage, et causer ensuite un scénario de type 1.
- Scénario 2 : Vieillissement de composants par effet continu d'un paramètre physique, sensible aux défaillances ou dérives d'autres composants. Par exemple:
    - Vieillissement de matériels par cumul de temps passé au dessus de certains seuils de certaines variables continues (par exemple, vieillissement de capteurs suite à une répétition d'excursions en température causée par le dérive d'un autre composant…)
    - Vieillissement continu sous l'effet d'un champ crée par le fonctionnement d'autres composants (par exemple, vieillissement de certains composants électroniques par la température d'un moteur proche dont ils régulent le fonctionnement…)
- Scénario 3 : Différentiel de vieillissement d'un matériel entre un matériel en fonctionnement et un matériel en attente (mode secours) ou en stockage (effet inverse).

Dans le cadre du projet APPRODYN, ces phénomènes ne sont pas représentés.

4.8.3 Graphes d'états et autres données de fiabilité – Barillet VVP (et parties passives)

4.8.3.1 Modes de défaillance du barillet VVP

Nous devons prendre en compte d'autres parties que le barillet du circuit VVP.
Cela mène aux valeurs révisées du tableau 4.5. en terme de répartition des modes de défaillances et de MTTR (Mean Time To Repair).

Tableau 4.5

Mode de défaillance	Contribution au taux de défaillance	Pfd	MTTR[13]	Effet	Mode de défaillance
Fuites	89%	na	12	AAR (supposé tjrs détecté)	Mode I Origine mécanique
Rupture Barillet	11%	na	168	AAR	Mode II Origine mécanique

Option: Il existe une proportion de fuites non détectées qui mène à une rupture selon une loi de vieillissement (en pointillé sur le graphe d'états)

4.8.3.2 Graphe des états du barillet VVP

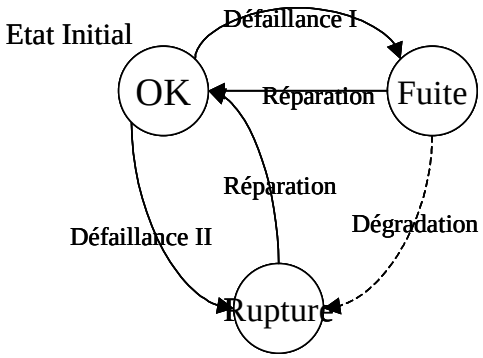


Figure 4.11

[13] Attention : valeurs de MTTR permutées dans la 1ere version

4.8.4 Graphes d'états et autres données de fiabilité - Pompes électriques CEX

4.8.5 Constitution d'une pompe CEX

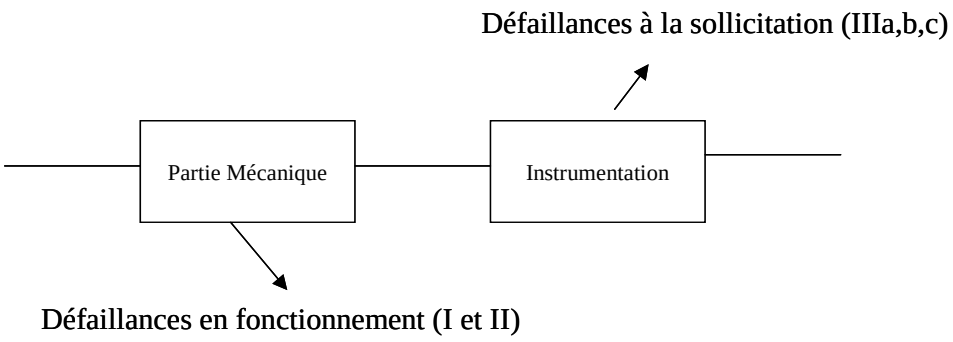


Figure 4.12. Pompe CEX : diagramme de fiabilité

4.8.6 Modes de défaillance d'une pompe CEX

Tableau 4.6. Pompe CEX : diagramme de fiabilité

	Contribution au taux de défaillance	Pfd	MTTR	Effet	Mode de défaillance
Refus de démarrage	na	100%	72	AAR si pompe de secours	Mode III ; Origine principale Instrumentation ou montage (FH). Trois situations de détection (a, b, c)
Défaillance en fonctionnement de la pompe (*)	99.9%	na	72	AAR si en 2/2	Mode I Origine mécanique ou électrique
Rupture ou fuite grave	0.1%	na	168	AAR si en 2/2	Mode II Origine mécanique
Démarrage intempestif	na	na	na	concerne 3e pompe, à l'arrêt, pas d'effet au niveau système	na

(*) vibrations importantes, fuites importantes, échauffement importants…

Démarrage intempestif non comptabilisé (pourrait concerner la 3e pompe, à l'arrêt, et n'a pas un effet au niveau système).

4.8.7 Indisponibilité de la partie instrumentation CEX

Le comportement dysfonctionnel de l'instrumentation est caractérisé par les paramètres suivants :

- Taux de défaillance
- MTTR
- Probabilité d'intempestif (Pspu)
- Probabilité de défaillance non révélée par autosurveillance ou par essai périodique (Ptif)
- Proportion de défaillances par cause commune (Facteur Beta)
- Proportion de défaillances (Blocage, Absence de réponse, Décalage de réponse)

L'indisponibilité d'un système programmé résulte de défaillances détectées par les autotests continus et immédiatement mises en réparation, de défaillances détectées seulement par des essais révélateurs, dits aussi Essais Périodiques (EP), et d'une proportion résiduelle de défaillances non détectables, liées en général à des erreurs de spécification ou aux incomplétudes des programmes de test.
La partie instrumentation est non redondée. L'indisponibilité moyenne d'un système 1oo1, notée $P_{fd(1001)}$ est :

$$P_{fd(1001)} = \lambda_{ND}.(T/2+MTTR) +\lambda_{D}.MTTR + Ptif$$

λ_D : taux de défaillances détectées par autotests.
λ_{ND} : taux de défaillances détectées par essais périodiques (dits aussi essais révélateurs)
Ptif: part de l'indisponibilité dûe aux défaillances non détectables (TIF : Test Independent Failures)[14]
$\lambda_{ND} + \lambda_D = \lambda$
MTTR : Temps moyen de réparation de l'instrumentation (après détection)
T : Périodicité des essais périodiques (L'indisponibilité dûe à l'essai périodique est négligée)
Valeurs par défaut (les valeurs précises dépendent des technologies d'automatismes employées) :
$\lambda_D / \lambda = 0,75$
$\lambda_{ND} / \lambda = 0,25$
MTTR = 8 heures
T révélateurs = 3 mois (systèmes testables « en Marche ») à 18 mois (systèmes testables uniquement est à l'arrêt).
L'indisponibilité dûe aux défaillances non détectables est donnée par une proportionnalité :
Ptif = 0,05.Pfd
Deux hypothèses à respecter :
Hypothèse de preuve limitée
Les valeurs de Pfd d'un « système programmé » ne peuvent être meilleures que 10-4/soll,
Hypothèse d'indépendance limitée
Les valeurs de Pfd de deux « systèmes programmés » mis en redondance doivent être supérieures à

Pfd	Pfd (détectées en EP)	Pfd (détectées en autotests)	Pfd (non détectables)	Proportion de défaillances non détectées	Proportion de défaillances détectées en EP	a = Proportion de défaillances détectées en autotests	MTTR = Tps moyen de réparation des défaillances détectées (hrs)	Lambda (en defaillances/heure)	T1 = période des essais révélateurs (mois)
1,93E-03	1,80E-03	3,90E-05	9,66E-05	0,05	0,25	0,75	8	6,50E-06	3
1,92E-03	1,81E-03	6,60E-06	9,58E-05	0,05	0,25	0,75	8	1,10E-06	18

10-6/soll.
Une Pfd proche de 1,95.10-3 / sollicitation est obtenue avec les valeurs suivantes :

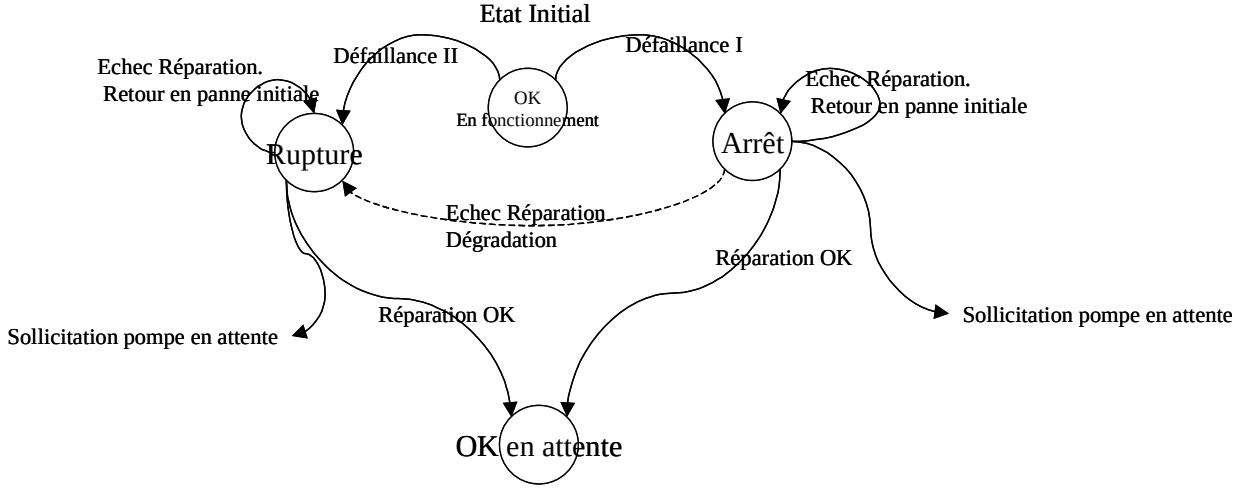
- λ = 6,5.10-6/hr, T = 3mois (cette paire de valeurs est retenue par défaut)
- λ = 1,1.10-6/hr, T = 18 mois

[14] cf SINTEF

4.8.8 Graphe des états - Pompe électrique CEX en marche

Option 1: Un échec de réparation est envisageable dans 10% des cas.
Option 2: Un échec de réparation a alors une probabilité de 0,25 de mener à une dégradation du composant (en pointillé sur le graphe d'états)

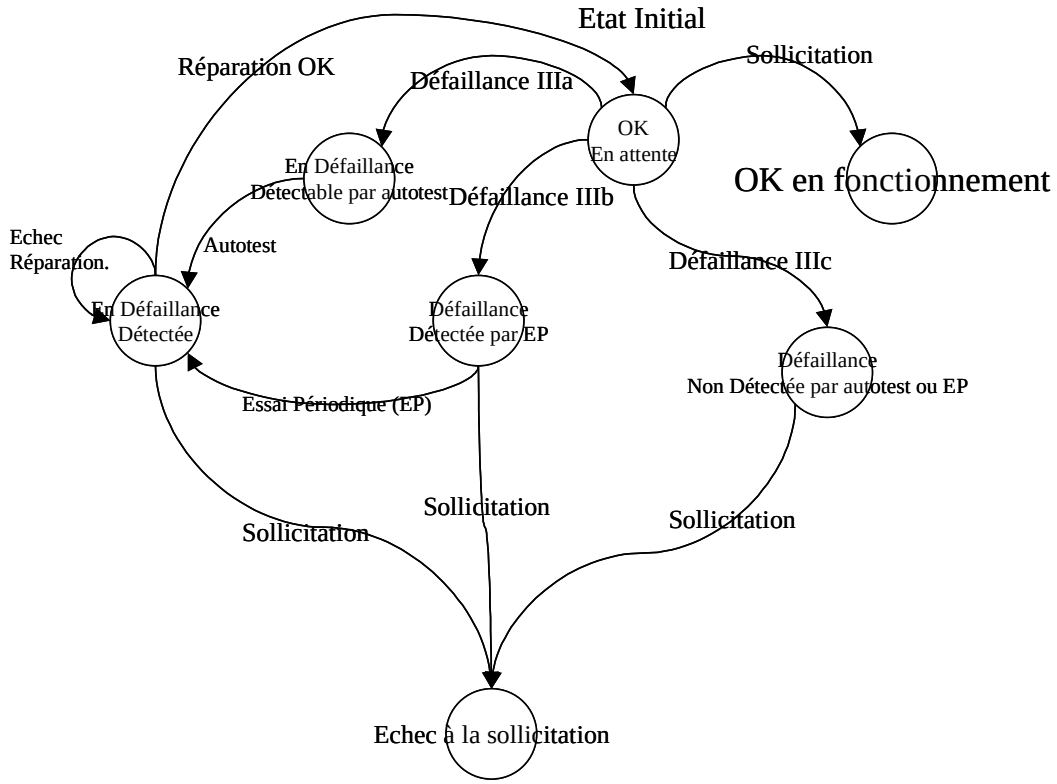
Figure 4.13.



4.8.9 Graphe des états - Pompe électrique CEX en attente

Le graphe concerne surtout les défaillances d'instrumentation ou les défauts de montage initiaux.
Une partie OK en fonctionnement mise à l'arrêt peut ne pas redémarrer, principalement à la cause de la partie instrumentation (défaillances IIIa,b,c)
La pompe en attente est soumise à des Essais Périodiques (1/mois par exemple)

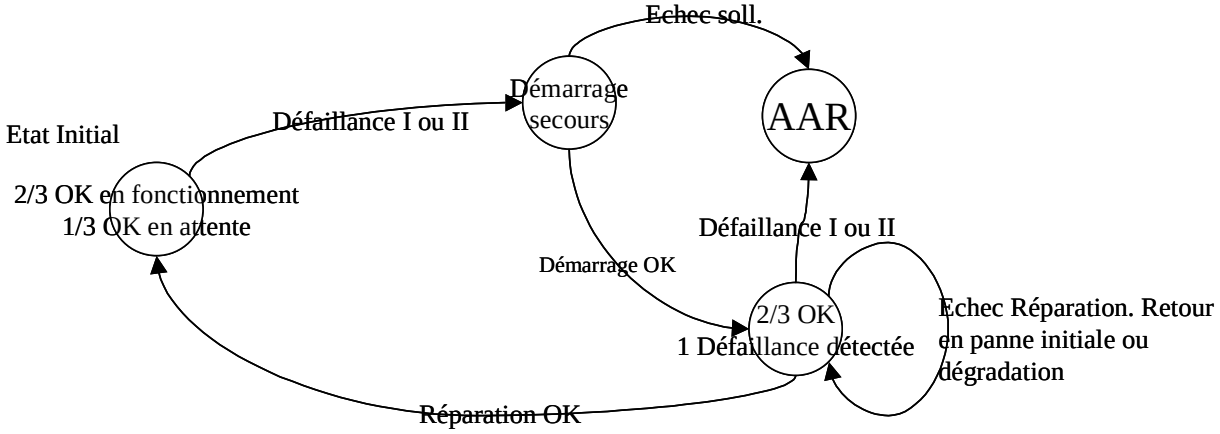
Figure 4.14.



4.8.10 Automate de spécification des pompes électriques CEX en 2/3

Redondance triple: deux en fonctionnement, une en secours

Figure 4.15.



Défaillances de cause commune : 5% des défaillances de Mode I ou II sont de cause commune. Dans ce cas, deux pompes sont défaillantes et conduit à l'AAR.

4.9 Graphes d'états et autres données de fiabilité - TurboPompe Alimentaire (TPA)

4.9.1 Constitution d'une TurboPompe Alimentaire TPA

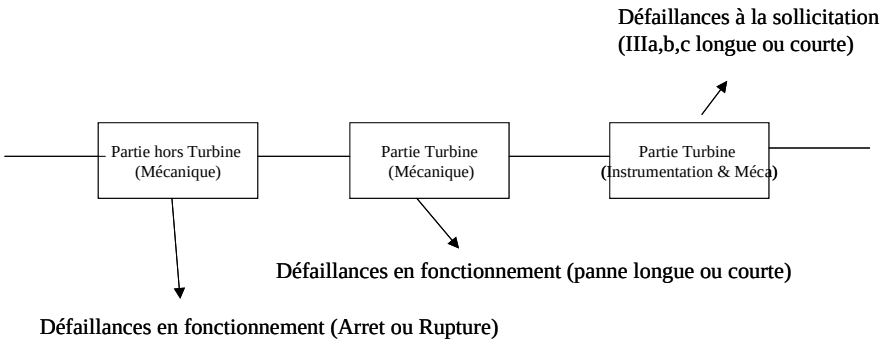


Figure 4.16. TPA : diagramme de fiabilité

Les parties turbine et hors turbine forment du point de vue fonctionnel un système série

4.9.2 Modes de défaillance d'une turbopompe TPA (hors turbine)

***Tableau 4.8**. Modes de défaillance d'une turbopompe TPA (hors turbine)*

	Contribution au taux de défaillance	Pfd	MTTR	Effet	Mode de défaillance
Défaillance à la sollicitation de la pompe	na	100%	28	AAR si pompe de secours	Mode III ; Origine principale montage (FH). Trois situations de détection (a, b, c)
Défaillance en fonctionnement de la pompe	99.9%	na	24	Arrêt. L'autre TPA passe en survitesse et assure 60% de la charge	Mode I Origine mécanique ou électrique
Rupture ou fuite grave	0.1%	na	144	Arrêt. L'autre TPA passe en survitesse et assure 60% de la charge	Mode II Origine mécanique

4.9.3 Indisponibilité de la partie instrumentation TPA

Les hypothèses et formules employées sont identiques à celles de la partie instrumentation CEX.
Une Pfd de 5,45.10-4 / sollicitation est obtenue avec les valeurs suivantes :

- λ = 1,85.10-6/hr,
- T = 1mois

ou

- λ = 3,1.10-7 /hr,
- T = 18 mois

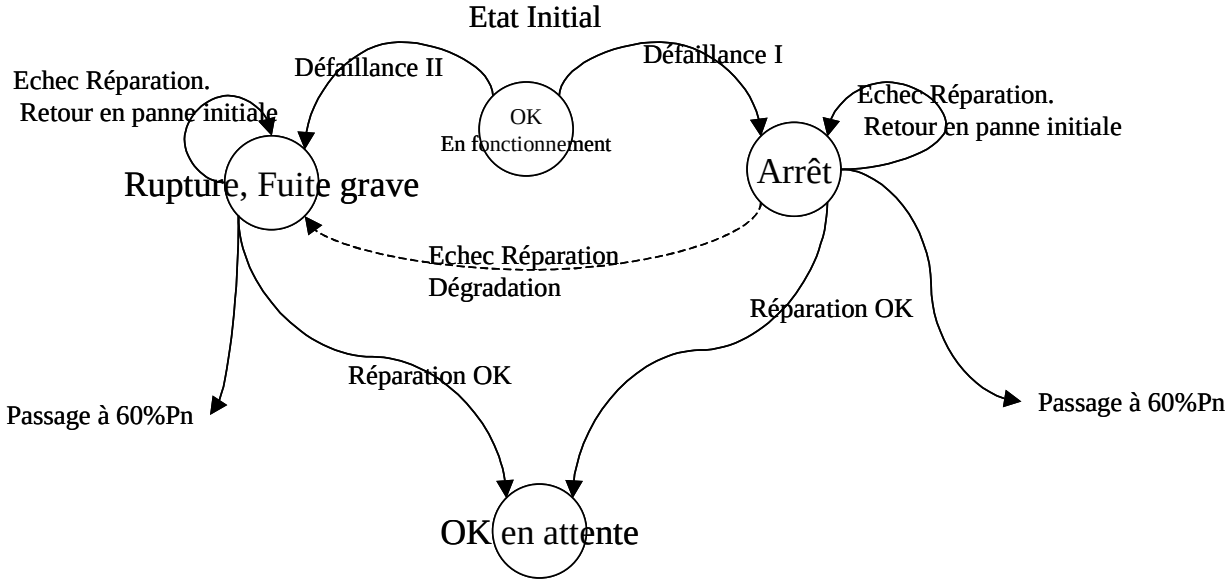
Tableau 4.9. Indisponibilité de la partie instrumentation TPA

Pfd	Pfd (détectées en EP)	Pfd (détectées en autotests)	Pfd (non détectables)	Proportion de défaillances non détectées	Proportion de défaillances détectées en EP	a = Proportion de défaillances détectées en autotests	MTTR = Tps moyen de réparation des défaillances détectées (hrs)	Lambda (en defaillances/heure)	T1 = période des essais révélateurs (mois)
5,50E-04	5,12E-04	1,11E-05	2,75E-05	0,05	0,25	0,75	8	1,85E-06	3
5,40E-04	5,11E-04	1,86E-06	2,70E-05	0,05	0,25	0,75	8	3,10E-07	18

4.9.4 Graphe des états – Turbopompe TPA (hors turbine)

Option : Un échec de réparation est envisageable dans 10% des cas. Il a alors une proba de 0,25 de mener à une dégradation du composant.

Figure 4.17. Graphe des états – Turbopompe TPA (hors turbine)



4.9.5 Modes de défaillance d'une turbopompe TPA (partie turbine)

Tableau 4.10. Modes de défaillance TPA (partie turbine)

Modes de défaillance	Contribution au taux de défaillance	Pfd	MTTR	Effet	Mode de défaillance
Défaillances à la sollicitation avec un temps de réparation court	na	99%	2	l'autre TPA reste en survitesse et assure 60% de la charge	Mode III ; Origine principale Intrumentation ou montage (FH). Trois situations de détection (a, b, c)
Défaillances à la sollicitation avec un temps de réparation long	na	1%	24	l'autre TPA reste en survitesse et assure 60% de la charge	Mode III ; Origine principale Intrumentation ou montage (FH). Trois situations de détection (a, b, c)
Défaillances en fonctionnement avec un temps de réparation court	25%	na	2	Arrêt. L'autre TPA passe en survitesse et assure 60% de la charge	Mode I Origine mécanique ou électrique
Défaillances en fonctionnement avec un temps de réparation long	75%	na	24	Arrêt. L'autre TPA passe en survitesse et assure 60% de la charge	Mode I Origine mécanique

4.9.6 Graphe des états – Turbopompe TPA (partie turbine, en fonctionnement)

Option : Un échec de réparation est envisageable dans 10% des cas. Il a alors une proba de 0,25 de mener à une dégradation du composant.

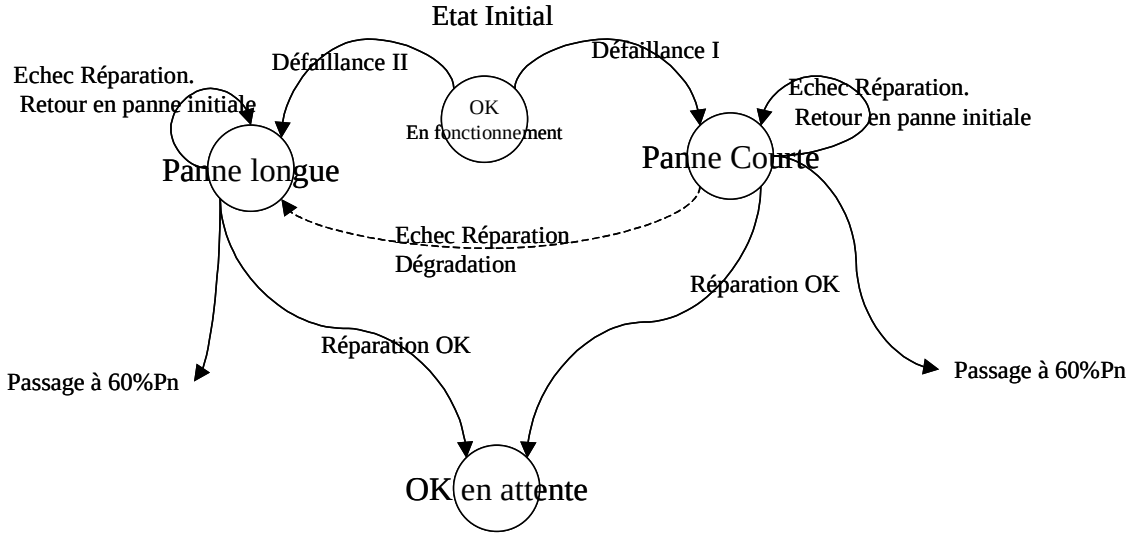


Figure 4.18. Graphe des états – Turbopompe TPA (partie turbine)

4.9.7 Graphe des états – Turbopompe TPA (partie turbine, en attente)

Une partie mise à l'arrêt peut ne pas redémarrer, principalement à la cause de la partie instrumentation (défaillances III a,b,c). La pompe à l'arrêt est testée par des Essais Périodiques

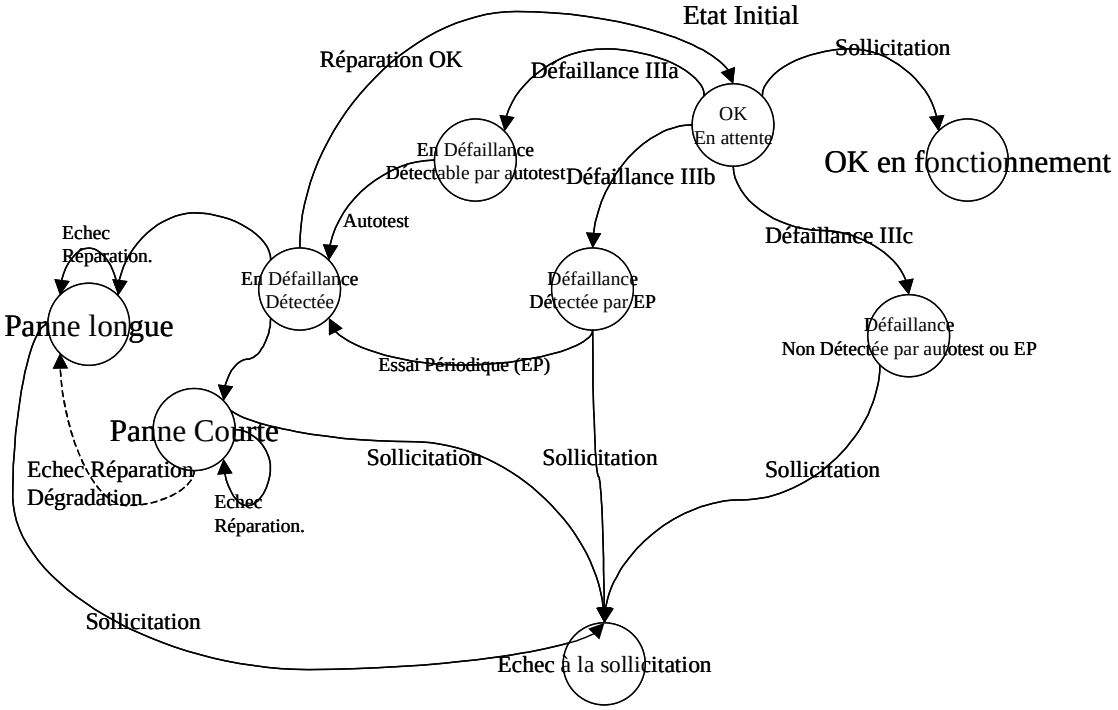


Figure 4.19. Graphe des états – Turbopompe TPA (partie turbine)

4.9.8 Automate de spécification des turbopompes TPA redondées

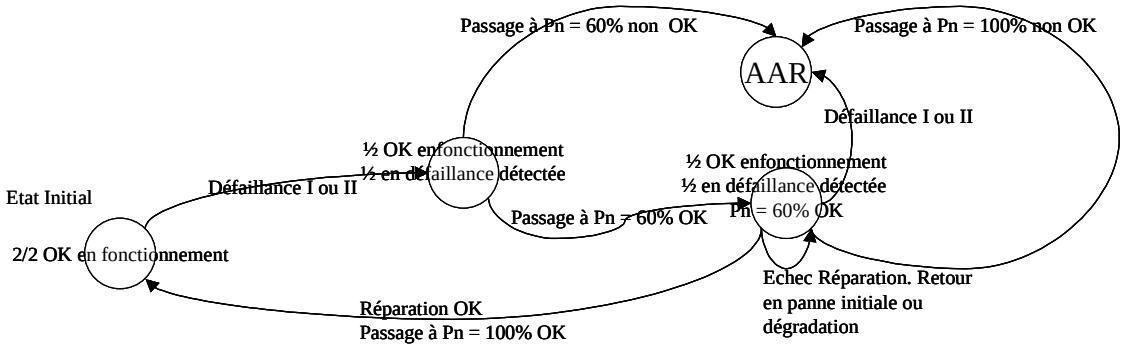


Figure 4.20. Automate de spécification des turbopompes TPA

Défaillances de cause commune : 5% des défaillances de Mode I ou II (Hors Turbine) ou de Mode I (Turbine) sont de cause commune. Dans ce cas, deux TPA sont défaillantes et conduit à l'AAR

Les explications nécessaires à cet automate sont fournies ci dessous.

4.9.9 Hypothèses pour la conduite en démarrage et montée en puissance des turbopompes TPA

Les TPA sont inactives à P<2%Pn.
Lorsque la puissance atteint 2%Pn et que le niveau des GV est à au moins 33% de la gamme étroite, une TPA est mise en marche, et ARE prend le relais de ASG pour l'alimentation en eau.

La montée en puissance requiert deux TPA en état, une en marche, une en attente.
Si lapremière TPA (TPA 1) ne démarre pas, on lance la seconde (TPA 2). Si elle démarre, on effectue des réparations sur la première et on reste à 2%Pn.
Si lTPA2 ne démarre pas, des réparations sont effectuée sur TPA2 puis TPA1 à 2%Pn.

Lorsque la puissance P < 60%Pn, une TPA est employée, éventuellement en survitesse, la seconde est en redondance.
Lorsque la puissance P atteint 60%Pn, on met la seconde TPA en marche. Si elle ne démarre pas, des réparations sont effectuée à 60%Pn.

La montée en puissance au delà de 60%Pn requiert donc deux TPA en marche.

Si une pompe TPA tombe en panne à plus de 60%Pn, l'autre passe en survitesse et assure 60% de la charge qui est donc réduite (« *forçage à 60%* »). La puissance reste à 60%Pn tant qu'une seule TPA fonctionne.

Des que la seconde TPA est réparée, elle est remise en charge et la puissance reprend sa montée jusqu'à 100% Pn.

Si la seconde TPA ne démarre pas ou tombe en panne, cela conduit à l'AAR. Une option est de passer dans cette situation en « *forçage à 2%* ».

4.9.10 Hypothèses pour la conduite en puissance des turbopompes TPA

Scénario n°1 :
Cas d'une puissance=100%Pn.
Lorsqu'une TPA tombe en panne à une puissance >60%P, la consigne est de ramener la puissance à 60%Pn par une action sur les fonctions de régulation (ce qui prend quelques minutes). On est alors à 60%Pn avec une TPA OK et une TPA en réparation (« *forçage à 60%* »).
Cette action peut échouer à la sollicitation ou ne pas être lancée si la défaillance de la TPA est non détectée. La probabilité de cet échec est de 10-3/d. Cette situation mène à un AAR.
Si la seconde TPA ne démarre pas ou tombe en panne, cette situation mène AAR.
La puissance est maintenue à 60%Pn (« *forçage à 60%* »).en attendant que la seconde TPA soit réparée, puis on remonte en charge. Le temps d'attente de la seconde TPA est trop court pour qu'un EP soit mené.

Scénario n°2 :
Cas d'une puissance=60%Pn avec une seule TPA.
Il faut alors prendre en compte les défaillances et les EP menés sur la TPA en attente. Ce scénario n'est pas modélisé pour l'instant.

4.9.11 Hypothèses pour la baisse de puissance des turbopompes TPA

1er cas : puissance > 60%Pn avec deux TPA en marche.
Les régulations de la source thermiquesont utilisées pour faire baisser la puissance.
Lorsque la puissance atteint 60%Pn, une TPA est arrêtée.
La baisse de puissance continue.
Si la TPA en fonctionnement tombe en panne, la seconde est démarée, la réduction de puissance continue. LA TPA en panne est mise en réparation.
Si la seconde TPA ne démarre pas, cela conduit à un AAR.
Lorsque la puissance atteint 2%Pn, la TPA encore en marche est arrêtée.

2e cas : puissance < 60%Pn avec une TPA en marche (scénario n°2 du 4.9.10).
Les régulations de la source thermiquesont utilisées pour faire baisser la puissance.

Si une TPA tombe en panne,
la seconde est démarée, la réduction de puissance continue. LA TPA en panne est mise en réparation.
Si la seconde TPA ne démarre pas, cela conduit à un AAR.
Lorsque la puissance atteint 2%Pn, la TPA encore en marche est arrêtée.

4.10 Graphes d'états et autres données de fiabilité - Vanne pneumatique réglante ARE

4.10.1 Constitution d'une vanne pneumatique réglante ARE

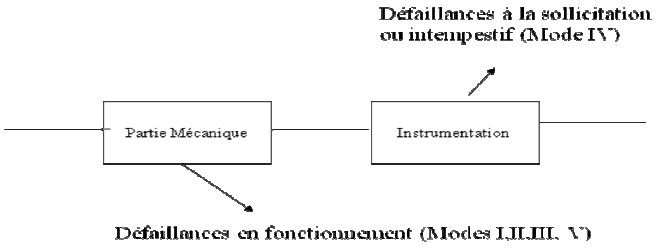


Figure 4.21. Vanne ARE

4.10.2 Modes de défaillance d'une vanne ARE

Ce matériel est en sollicitation au démarrage, puis en marche continue.

Tableau 4.11. Modes de défaillance vanne ARE

	Contribution au taux de défaillance	Pfd	MTTR	Effet	Mode de défaillance
Refus d'ouverture d'une vanne pneumatique VL	na	72%	12	La vanne reste collée à son ouverture actuelle Comptabilisé en Mode V.	Origine principale Intrumentation ou montage (FH)
Refus de fermeture d'une vanne pneumatique VL	na	28%	12	La vanne reste collée à son ouverture actuelle Comptabilisé en Mode V.	Origine principale Intrumentation ou montage (FH)
Rupture d'une vanne pneumatique VL ou fuite grave	0,10%	na	120	Fuite grave > 20% du débit	Mode I Origine mécanique
Fuite interne d'une vanne pneumatique VL	11%	na	12	Cause débit supérieur à la consigne de +0 à +20%	Mode II Origine mécanique
Fuite externe d'une vanne pneumatique VL	1,00%	na	12	Cause débit inférieur à la consigne de -0 à -20%	Mode III Origine mécanique
Manœuvre intempestive vanne pneumatique VL	25%	na	12	Ouverture ou fermeture, partielle ou complète (aléatoire). Inclut démarrage intempestif	Mode IV. Origine FH ou instrumentation. Sur matériel en sollicitation continue.
Blocage vanne pneumatique VL	63%	na	12	La vanne reste collée à son ouverture actuelle.	Mode V. Origine mécanique

Note. L'évènement de démarrage intempestif d'une vanne hors de son domaine d'emploi n'est pas représenté. Il a l'effet de l'évènement fuite grave ou rupture.

Les fuites ne sont pas détectées immédiatement. Elles sont détectées si la régulation a un comportement anormal observable par la conduite, qui envoie alors une personne sur place. Pour notre modélisation, nous proposons *un temps fixe de 30 mn sans détection possible* puis un taux de détection « forfaitaire ».

Tableau 4.12. Modes de défaillance vanne ARE

	Effet aléatoire ?	Taux de détection
Mode I	Oui. Débit varie entre 20 et 100% selon loi uniforme.	100%
Mode II	Oui. Débit varie entre +0% et +20% selon loi uniforme.	10%
Mode III	Oui. Débit varie entre -20% et -0% selon loi uniforme.	50%
Mode IV	Oui. 1 fois sur 3 : fermé, 1 fois sur 3 : ouvert, 1 fois sur 3: Débit entre 0 et 100% selon loi uniforme.	10%
Mode V	Non. Débit fixé à la dernière consigne	0%

Les défaillances modes I, II et III nécessitent un arrêt du système pour être réparées.
Si une défaillance de mode I ou III est détectée, la puissance est abaissée jusqu'à 2%, la réparationest effectuée, puis la puissance est augmentée.
Les défaillances modes IV et V peuvent être réparées sans arrêter le système. Une réparation sur une défaillance de mode V peut cependant échouer dans 10% des cas et requérir un arrêt pour être réparée.

Note : Les niveaux de fuite grave peuvent être à révisés après simulation.

4.10.3 Indisponibilité de la partie instrumentation ARE

La partie instrumentation de l'ARE inclut la régulation (PID). Le comportement dysfonctionnel des API est caractérisé par les paramètres suivants :

- Taux de défaillance
- MTTR
- Probabilité d'intempestif (Pspu)
- Probabilité de défaillance non révélée par autosurveillance ou par essai périodique (Ptif)
- Proportion de défaillances par cause commune (Facteur Beta)
- Proportion de défaillances (Absence de sortie, Dérive sur un paramètre)

Les autres hypothèses et formules employées sont identiques à celles de la partie instrumentation CEX.

Une Pfd de 5,85.10-3 / sollicitation est obtenue avec les valeurs suivantes :

- λ = 2.10-5/hr,
- T = 1mois

ou

- λ = 3,35.10-6/hr
- T = 18 mois

Tableau 4.13. Indisponibilité de la partie instrumentation ARE

Pfd	Pfd (détectées en EP)	Pfd (détectées en autotests)	Pfd (non détectables)	Proportion de défaillances non détectées	Proportion de défaillances détectées en EP	a = Proportion de défaillances détectées en autotests	MTTR = Tps moyen de réparation des défaillances détectées (hrs)	Lambda (en defaillances/heure)	T1 = période des essais révélateurs (mois)
5,95E-03	5,53E-03	1,20E-04	2,97E-04	0,05	0,25	0,75	8	2,00E-05	3
5,84E-03	5,52E-03	2,01E-05	2,92E-04	0,05	0,25	0,75	8	3,35E-06	18

Note : Modes de défaillance et données de fiabilité de la régulation PID de l'ARE.
Les caractéristiques de la PID proprement dite sont incluses dans la fiabilité de la partie instrumentation ARE globale. Elles sont forunies ici pour mémoire. Essais révélateurs : concernent la partie logique commune du système de régulation générale implantée sur des API.
Taux de défaillance (perte totale) : 7,93.10-7/hr, négligeable par rapport au taux de défaillance de la régulation estimé à 2.10-5/hr
Couverture des autotests : 75%
MTTR: 6 heures
Proportions de défaillances :
50% des cas : Absence de sortie. Idem Mode V.
25% des cas : Dérive sur un paramètre. Idem Mode III.
25% des cas : Dérive sur un paramètre. Idem Mode II

4.10.4 Fonctionnement des turbopompes TPA redondées

Description simplifiée du fonctionnement des vannes ARE

Cette description est employée pour la modélisation. Nous pourrons ultérieurement, en option, employer une description détaillée, avec un recouvrement des domaines de fonctionnement des parties petit débit et gros débit.
Au (re)démarrage, le circuit de sauvegarde ASG (non représenté) assure la circulation d'eau dans les GV. Puis lorsque la puissance dépasse 2% de Pn, avec une TPA en marche et le niveau des GV à au moins 33% de la gamme étroite, on bascule sur ARE.
La vanne petit débit, plus réactive, est employée de 2% Pn jusqu'à 15%Pn environ.
La vanne gros débit est employée à partir de 15% Pn environ.
Simplification : Les deux vannes sont exclusives, leurs temps d'ouverture/fermeture sont considérés comme presque nuls.

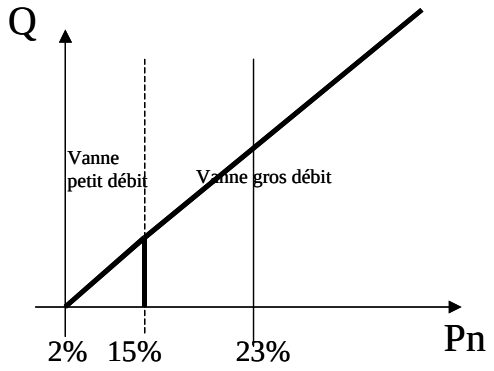


Figure 4.22. Domaines de fonctionnement vanne ARE

Chaque vanne réglante ARE, petit débit ou gros débit, peut être à un état initial ouvert ou fermé

Tableau 4.14. Modes de fonctionnement vanne ARE

	En Montée en Puissance	En Baisse de Puissance
Vanne Petit Débit	Etat Initial fermée à 2%Pn	Etat Initial fermée à 15%Pn
Vanne Gros Débit	Etat Initial fermée à 15%Pn	Etat Initial ouvert à Pn = 100%

Au (re)démarrage, le circuit de sauvegarde ASG (non représenté) assure la circulation d'eau dans les GV. *Cette étape* n'est pas *modélisée.*

Puis lorsque la puissance dépasse 2%Pn, avec une TPA en marche et le niveau des GV à au moins 33% de la gamme étroite, on bascule sur ARE.

La vanne petit débit, plus réactive, est employée de 2% Pn jusqu'à 15%Pn environ, sachant qu'elle peut fournir jusqu'à 23% Pn. La vanne gros débit est employée à partir de 15% Pn environ. Une régulation assure le basculement entre les deux vannes. Le temps de réponse de la vanne en ouverture/fermeture permet de suivre les variations de puissance de l'installation.

Trois domaines, et deux états de l'installation sont distingués : montée en puissance, baisse de puissance. Entre 15 et 23%Pn, la vanne gros débit est employée en priorité, mais peut être remplacée par la vanne petit débit en cas de besoin.

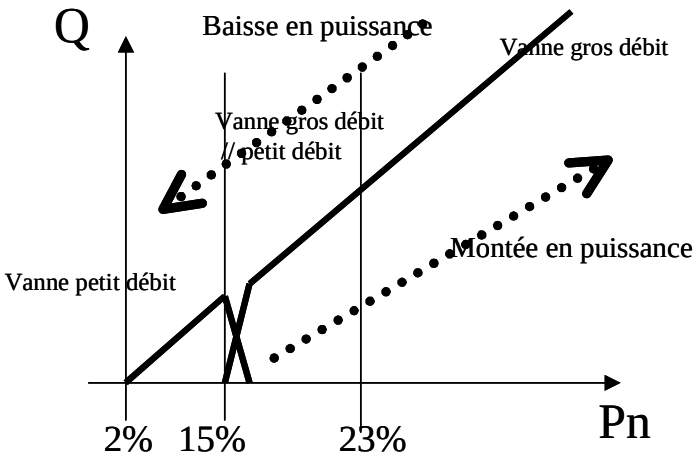


Figure 4.23. Domaines de fonctionnement vanne ARE (détail)

4.10.5 Graphes des états d'une vanne ARE

Vanne Petit Débit en Montée en Puissance.

L'état initial est Vanne fermée, la puissance est à 2%Pn.

Si la manœuvre se passe correctement (« Manoeuvre OK ») on atteint 15%Pn, avec une vanne petit débit en état

A 15%Pn, la régulation de l'ARE lance un ordre de fermeture de la vanne petit débit et d'ouverture de la vanne gros débit.
La vanne petit débit se ferme si elle est OK, passée manœuvre intempestive ou en fuite externe, en fuite grave, rupture. Ces modes de défaillance peuvent ensuite rester non détectés jusqu'à la prochaine sollicitation de la vanne.
Si elle est en fuite interne, la vanne petit débit est « *fuiteuse* », la fermeture de la vanne petit débit est partielle : un débit de 0 à 20% continue à passer, de façon détectée ou non.
Pour simplifier le modèle, cet effet n'est pas représenté dans les graphes des états vanne gros débit.
Il est donc considéré la aussi qu'elle se ferme correctement, et que sa défaillance est provisoirement masquée.

Le graphe indique par « AAR ou 15%Pn? » que le passage en AAR dépend de l'ampleur de la fuite de la vanne, et de la capacité de la régulation, ou de l'inertie du GV, à la compenser en attendant l'ouverture de la vanne gros débit. Si l'AAR n'est pas déclenché, la puissance 15%Pn est atteinte,, avec une vanne petit débit défectueuse.

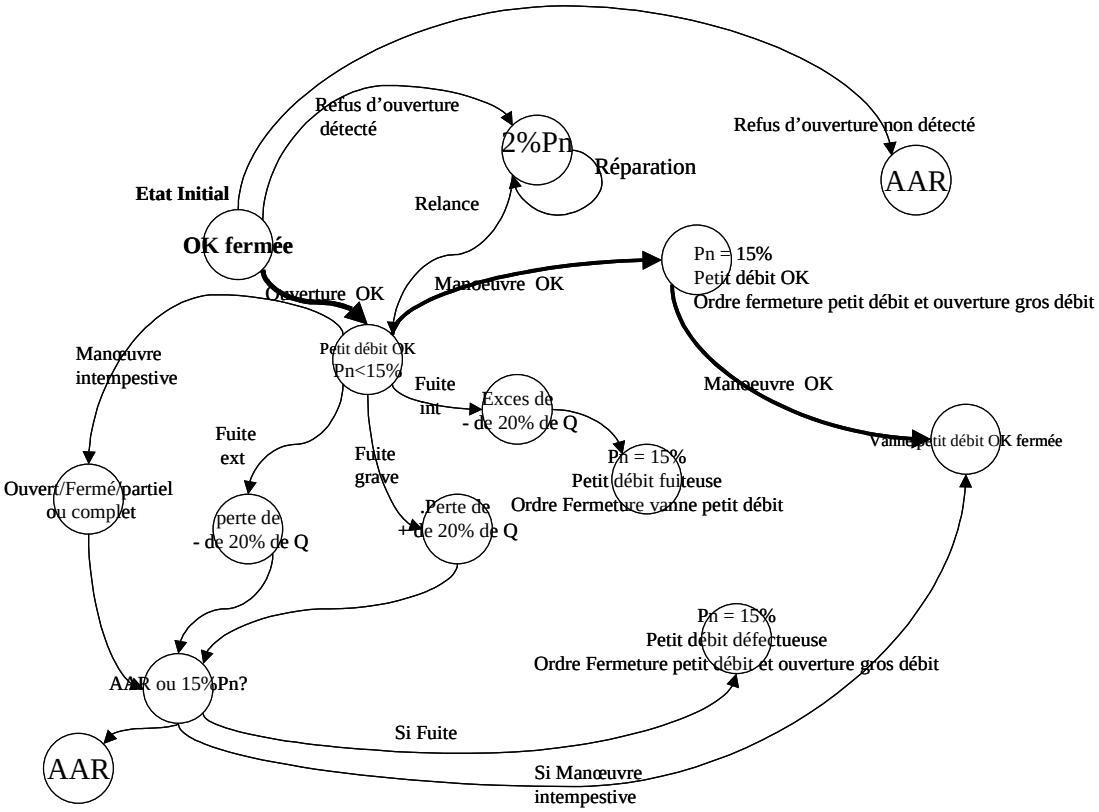


Figure 4.24. Vanne Petit Débit en Montée en Puissance
En gras : chemin suivi en situation normale

Vanne Petit Débit en Baisse de Puissance.

L'état initial est Vanne petit débit fermée, defectueuse ou non, la puissance est à 15%Pn

Note : La vanne gros débit peut être fuiteuse, sa fermeture est partielle : un débit de 0 à 20% continue à passer, de façon détectée ou non ; pour simplifier le modèle, cet effet n'est pas représenté dans les graphes des états vanne petit débit.

Le graphe indique par « AAR ou 2%Pn? » que le passage en AAR dépend de l'ampleur de la fuite de la vanne petit débit et de la capacité de la régulation ou de l'inertie du GV à la compenser. Si l'AAR n'est pas déclenché, on atteint 2%Pn, avec une vanne petit débit défectueuse.

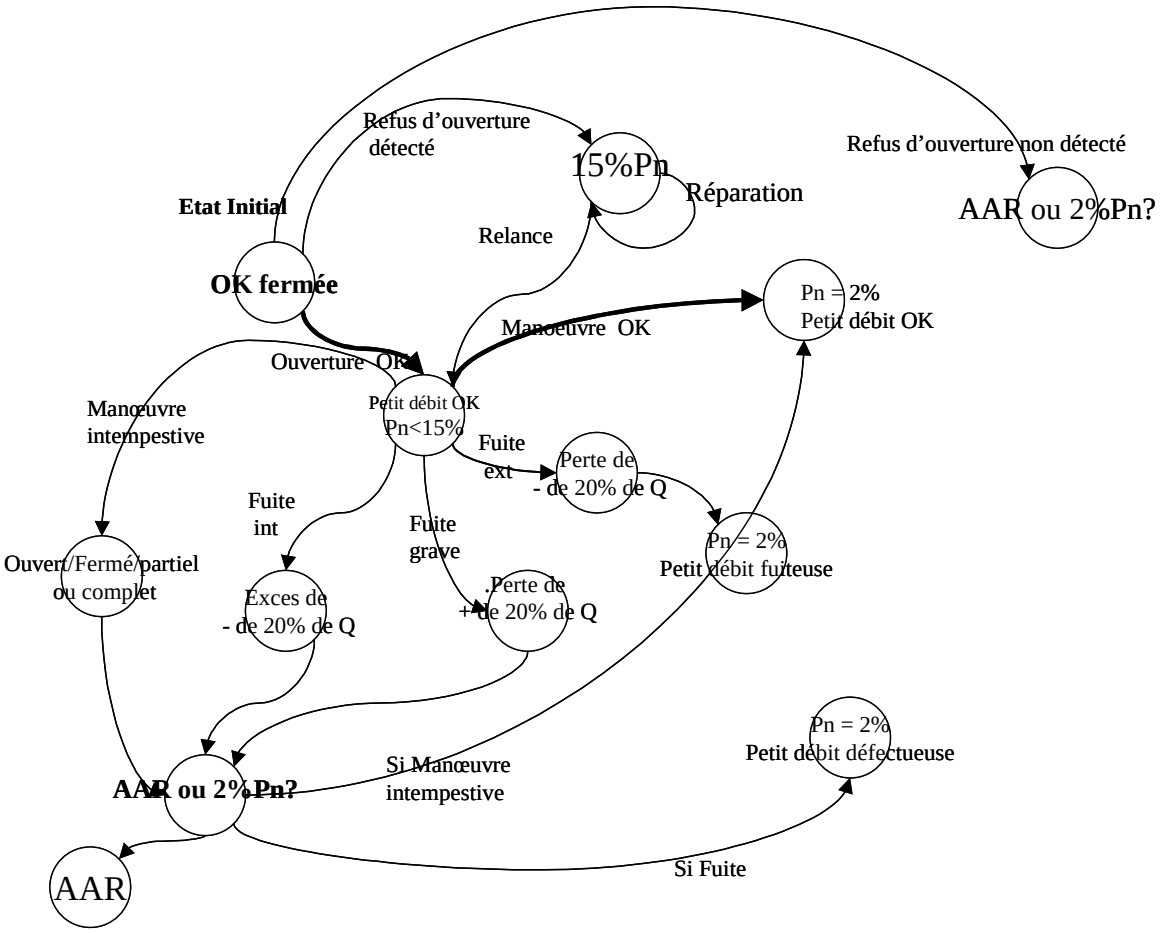


Figure 4.25. Vanne Petit Débit en Baisse de Puissance
En gras : chemin suivi en situation normale

Vanne Gros Débit en Baisse de Puissance.

L'état initial est Vanne gros débit ouverte, la puissance est à 100%Pn (scénario 1)

Note : La vanne petit débit peut être fuiteuse, la fermeture de la vanne petit débit est partielle : un débit de 0 à 20% continue à passer, de façon détectée ou non ; pour simplifier le modèle, cet effet n'est pas représenté dans les graphes des états vanne gros débit.

Le graphe indique par « AAR ou 15%Pn? » que le passage en AAR dépend de l'ampleur de la fuite de la vanne petit débit et de la capacité de la régulation ou de l'inertie du GV à la compenser. Si l'AAR n'est pas déclenché, la puissance 15%Pn est atteinte, avec une vanne gros débit défectueuse.

La vanne gros débit se ferme si elle est OK, passée par une manœuvre intempestive (qui est de ce fait effacée) ou en fuite externe, en fuite grave, rupture. Ces modes de défaillance peuvent ensuite restés non détectés jusqu'à la prochaine sollicitation de la vanne.

Si elle est en fuite interne, la vanne gros débit est fuiteuse, la fermeture de la vanne gros débit est partielle : un débit de 0 à 20% continue à passer, de façon détectée ou non.
Pour simplifier le modèle, cet effet n'est pas représenté dans les graphes des états vanne petit débit.
Elle est considére comme se fermer correctement, sa défaillance est provisoirement masquée.

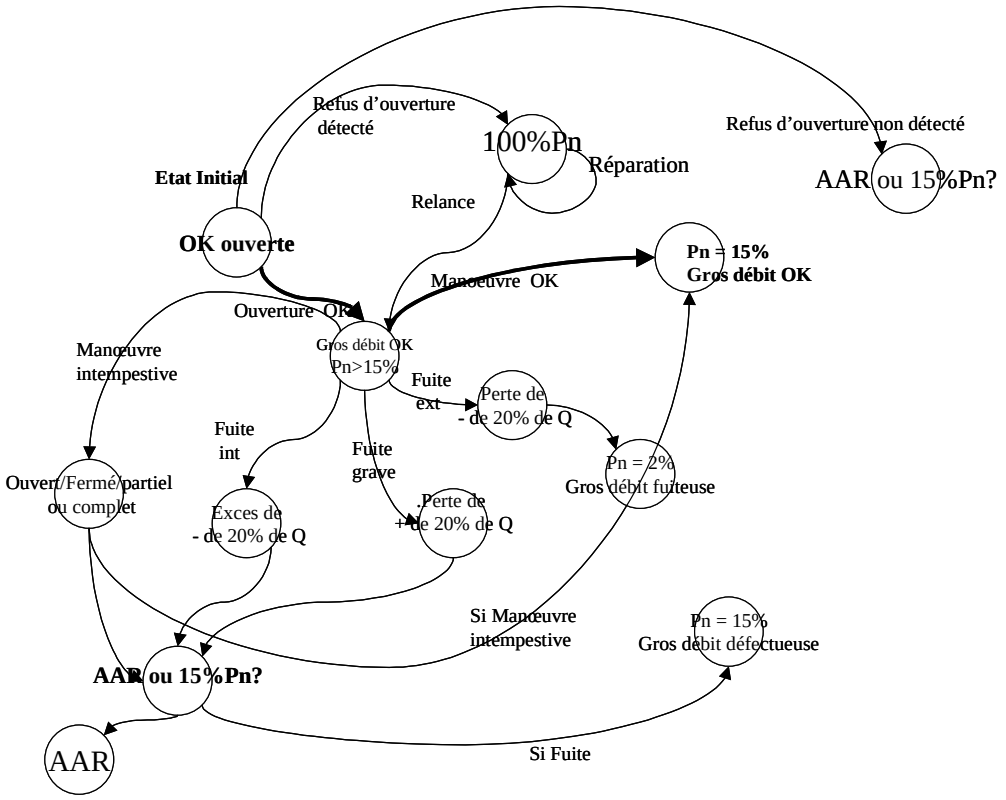


Figure 4.26. Vanne Gros Débit en Baisse de Puissance
En gras : chemin suivi en situation normale

Vanne Gros Débit en Montée en Puissance.

L'état initial est Vanne gros débit fermée, la puissance est à 15%Pn

Note : La vanne petit débit peut être fuiteuse, la fermeture de la vanne petit débit est partielle : un débit de 0 à 20% continue à passer, de façon détectée ou non ; pour simplifier le modèle, cet effet n'est pas représenté dans les graphes des états vanne gros débit.

Le graphe indique par « AAR ou 100%Pn? » que le passage en AAR dépend de l'ampleur de la fuite de la vanne petit débit et de la capacité de la régulation ou de l'inertie du GV à la compenser. Si l'AAR n'est pas déclenché, la puissance 100%Pn est atteinte, avec une vanne gros débit défectueuse.

Si elle est en fuite interne, la vanne gros débit est fuiteuse, la fermeture de la vanne gros débit est partielle : un débit de 0 à 20% continue à passer, de façon détectée ou non.
Pour simplifier le modèle, cet effet n'est pas représenté dans les graphes des états vanne petit débit.
Elle est considérée fermée correctement, et sa défaillance est provisoirement masquée.

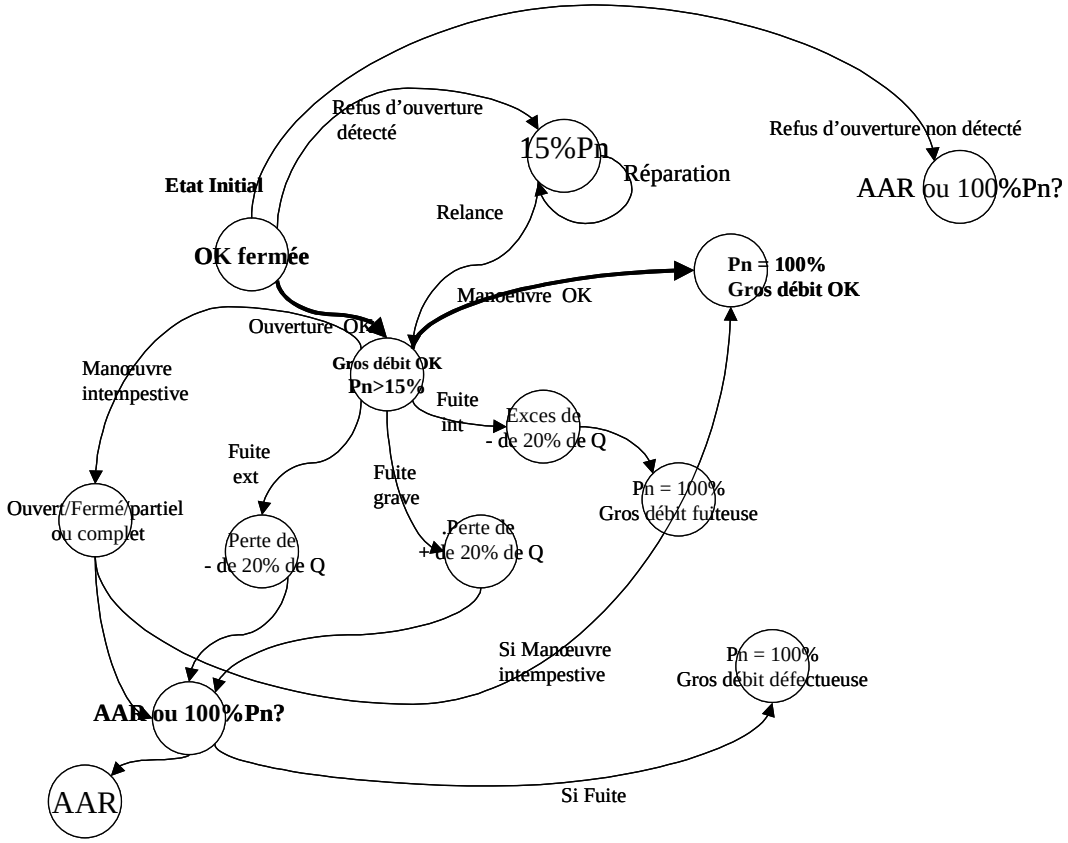


Figure 4.27. Vanne Gros Débit en Montée en Puissance
En gras : chemin suivi en situation normale

4.11 Graphes d'états et autres données de fiabilité - Capteurs

4.11.1 Fonctionnement des capteurs

Tableau 4.15. Installation des capteurs

Grandeur physique	Installation
Mesure Nge gamme étroite NTB (Niveau Très Bas) et NTH (Niveau Très Haut)	3 capteurs de niveau Tout Ou Rien par GV (dits ANG05x). Système en 2oo3, dégradé éventuellement en 1oo2.
Mesure débit eau alimentaire (Qe)	2 capteurs par ligne d'alimentation d'un GV (dits ANG04x). 1 seul employé à la fois pour la régulation.
Mesure débit Vapeur (Qv)	2 capteurs (dits VVP0x) par ligne de sortie d'un GV
Mesure Nge gamme étroite NB (Niveau Bas)	Mesure de Niveau Bas : cf NTB et NTH Mesure déséquilibre eau vapeur , par GV : deux comparaisons, chacune entre un capteur débit eau (Qe) Tout Ou Rien ANG04x et un capteur de débit vapeur (Qv) VVP0x
Mesure Ngl gamme large (non modélisé)	1 capteur Tout Ou Rien par GV (dit ANG06x).

4.11.2 Modes de défaillance des capteurs

Le comportement dysfonctionnel d'un capteur est caractérisé par les paramètres suivants :

- Taux de défaillance
- MTTR
- Proportion de défaillances par cause commune (Facteur Beta)
- Proportion de défaillances (Blocage, Absence de sortie, Dérive continue, Dérive par saut)
- Couverture de l'autosurveillance (technologie programmée), erreur en reconfiguration, reconfiguration intempestive (technologie programmée)

Le tableau n°XX détaille les modes de défaillance des capteurs.

4.11.3 Rappel des logiques de vote

Mesures continues

Dans le cadre du projet, nous avons considéré ce cas pour la mesure Nge gamme étroite. Deux règles sont possibles:

- Règle n°1 : Calcul de moyenne. La valeur mesurée est la moyenne des valeurs des trois capteurs. Les dérives de capteurs éventuelles sont détectées au mieux lors des Essais Périodiques.
- Règle n°2 : Calcul de moyenne avec inhibition. La valeur mesurée pae chaque capteur est comparée avec la moyenne des deux autres. Si le capteur est en écart de plus de 10% avec la moyenne des deux autres capteurs, il est inhibé et déclaré défaillant. Une action de réparation est lancée. Puis, la valeur mesurée est la moyenne des valeurs des capteurs non inhibés.

Mesures Tout Ou Rien

On suit une règle en 2oo3

4.11.4 Essais Périodiques

Des Essais Périodiques sont menés sur les capteurs pour assurer un écart <5% entre capteurs. L'écart est mesuré par rapport à la moyenne des deux autres capteurs. Ces essais peuvent cependant avoir des effets iatrogéniques, détaillés dans le tableau des modes de défaillance.

Tableau 4.16.: modes de défaillance des capteurs.

	Taux de défaillance unitaire d'un capteur (cf 5.1)	Stratégie de réparation	Modes de défaillance	Effets Iatrogéniques des essais périodiques	Risque de Défaillance de cause commune
Capteurs de niveau GV Nge (dits ANG05x).	5,2.10-6/hr	2oo3 : dégradation éventuelle en 1oo2 avec inhibition. Sinon, réparation	Dérive : 90% (de 5 à 20%, loi uniforme) Perte complète : 10% (fausse alarme)	Probabilité d'occurrence de 0,1 par essai. Conséquences : Essai fait par erreur sur chaîne fonctionnelle, dégrade système en 1oo1 temporairement (20% des cas). Défiabilisation. Fiabilité dégradée par facteur dix pour la suite de la mission (80% des cas).	Proportion de DCC sur les 3 capteurs : 5% Beta 2/3 = 3% Beta 3/3 = 2%
capteurs débit eau alimentaire Qe (dits ANG04x).	1,0.10-4/hr	Inhibition ou réparation, passage sur 1 capteur dispo en réserve	Dérive : 90% (de 2 à 20%, loi uniforme) Perte complète : 10% (mesure à 0)	Probabilité d'occurrence de 0,1 par essai. Conséquences : Fermeture intempestive et AAR (20% des cas).. Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).	
capteurs débit Vapeur Qv (dits VVP0x)	1,0.10-4/hr	réparation	Dérive : 90% (de 5 à 20%, loi uniforme) Perte complète : 10% (mesure à 0)	Probabilité d'occurrence de 0,1 par essai. Conséquences : Essai fait par erreur sur chaîne fonctionnelle et AAR (20% des cas). Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).	
capteurs gamme étroite	Combinent 1 capteur ANG04x et 1 capteur VVP0x	réparation	Selon capteurs	Probabilité d'occurrence de 0,1 par essai. Conséquences : Essai fait par erreur sur chaîne fonctionnelle et AAR (20% des cas). Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).	
capteurs gamme large (dit ANG06x) (non modélisé).	1,7.10-6/hr	réparation	Dérive : 90% (de 2,5 à 20%, loi uniforme) Perte complète : 10% (fausse alarme)	Probabilité d'occurrence de 0,1 par essai. Conséquences : AAR (20% des cas).. Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).	

4.12 Données pour l'optimisation des inspections

Note: Ces données n'ont pas été employés dans le cadre du projet APPRODYN.

4.12.1 <u>Optimisation des inspections des API de régulation et actionneurs CEX, TPA, ARE</u>

Seule la partie hors capteurs est considérée. Elle constitue un système 1oo1 associé à chaque pompe ou vanne.
Pour les systèmes élémentaires CEX, TPA, ARE, la relation entre indisponibilité et période des essais révélateurs est donnée par :

$$P_{fd(1001)} = \lambda_{ND}.(T/2+MTTR) +\lambda_{D}.MTTR + Ptif$$

Les inspections requièrent l'arrêt momentané du système inspecté pour effectuer des essais révélateurs.
Avec

- $Ptif$: partie de l'indisponibilité dûe aux défaillances non détectables (TIF : Test Independent Failures)
- $\lambda_{ND} + \lambda_{D} = \lambda$
- MTTR : Temps moyen de réparation de l'instrumentation (après détection) = 8 heures
- T : Périodicité des essais révélateurs = 3 mois (systèmes testables « Tranche en Marche ») à 18 mois (systèmes testables uniquement lorsque la Tranche est à l'arrêt).

La question est alors d'estimer les périodicités optimales Ti (i=1,2,3) des essais révélateurs pour chacun des sous systèmes CEX, TPA et ARE en prenant en compte :

- d'une part le cout des inspections, l'indisponibilité causée (la durée d'indisponibilité dûe à l'essai périodique n'est plus négligée) et la vulnérabilité qui en découle au niveau du système global par perte de redondance provisoire, le risque « iatrogénique » de défaillances causées par l'inspection,
- d'autre part le cout des pertes de production par indisponibilité du système global.

Hypothèses et contraintes pour les essais révélateurs
D'après les travaux de Zio et al.[15], les hypothèses et contraintes sont:

- Les inspections doivent laisser disponible au moins un « chemin » du système (il doit rester à tout moment pendant la durée de mission, e.g. 18 mois, au moins une CEX, une TPA et la vanne ARE non arrétée ou fermée pour inspection ou maintenance) ;
- Lorsqu'un système élementaire est réparé défaillant suite à un essai périodique, il est immédiatement mis en réparation et considéré comme « as good as new » (sauf si effet iatrogénique) ;
- Lorsqu'un système élementaire est identifié comme correct suite à un essai périodique, il est immédiatement remis en ligne (en attente ou en service, selon les cas) et considéré comme « as good as new » (sauf si effet iatrogénique) ;
- Les essais périodiques ont une durée ti. Le temps de remis en ligne est considéré comme négligeable ;
- Cout d'une heure de perte de production : C = 40000 Euros ;
- Cout d'un essai révélateur C = 100 Euros ;
- Durée d'un essai révélateur : t1 = t2 = t3 = 2 heures ;
- Cout d'une réparation C = 1000 Euros /hr ;

[15] Multiobjective optimization by genetic algorithms: application to safety systems P. Giuggioli Busacca, M. Marseguerra*, E. Zio. Reliability Engineering and System Safety 72 (2001)

- Durée d'une réparation (et durée d'indispo associée), MTTR selon mode de défaillance et systèmes élémentaire (cf 7.2, 6.5, 6.3 et 5.3).

Modes de défaillance :
Cf chapitres relatifs à la partie instrumentation des systèmes élémentaires CEX, TPA, ARE

Fiabilité
Cf chapitres relatifs à la partie instrumentation des systèmes élémentaires CEX, TPA, ARE

Effets Iatrogéniques :
Cf tableau n°4.16

Cas des actionneurs « intelligents».
A cette étape de l'étude, il n'y a pas de particularités pour l'instrumentation « intelligente ». (cf 4.1.5.).
Il n'y a pas non plus de différence entre les technologies d'API (cf 4.1.7).

Quantifications des paramètres caractéristiques (API et Actionneur)
Dans une première modélisation, sont considérées des technologies d'automates industriels programmés (API), des capteurs/actionneurs conventionnels .

Des défaillances de cause commune de Mode III ont été définies pour CEX, TPA, ainsi quedes modes de défaillances spécifiques aux effets iatrogéniques.

Tableau 4.17. Récapitulatif des données de fiabilité pour l'optimisation

	Regulation et actionneur CEX (1 pompe)	Regulation et actionneur TPA (1 pompe)	Actionneur ARE (1 vanne)
Périodicité des essais révélateurs	T1	T2	T3
Durée d'indispo associée	2 heures (1 pompe /3)	2 heures (1 pompe/2)	Baisse de débit de moitié pendant 2 heures
Pfd	A calculer	A calculer	A calculer
Couverture des autotests (λ_D / λ)	75% (cf 5.6)	75% (cf 6.8)	75% (cf 7.3)
Lambda total = λ_{ND} + λ_D = λ	6,5.10-6/hr (cf 5.6)	1,85.10-6/hr (cf 6.8)	2,5.10-5/hr (cf 7.3)
MTTR	selon mode de défaillance (cf 5.3)	selon mode de défaillance (cf 6.5, 6.3)	selon mode de défaillance (cf 7.2)
Beta (Causes commune entre 2 ou 3 vannes/pompes))	Beta 2/3 = 3% Bata 3/3 = 2%	Beta 2/2 = 5%	NA (système 1oo1)
Défaillances systématiques non détectées par autotest ou essais révélateurs	Ptif = 0,05.Pfd (cf 5.6)	Ptif = 0,05.Pfd (cf 6.8)	Ptif = 0,05.Pfd (cf 7.3)
Proportion de défaillances	(cf 5.3)	(cf 6.5, 6.3)	(cf 7.2)
Intempestifs (Pspu)	non comptabilisé (pourrait concerner la 3e pompe, à l'arrêt, et n'a pas un effet au niveau système).	non comptabilisé	Intégré dans manœuvre intempestive vanne pneumatique VL (cf 7.2)
Effets Iatrogéniques	Probabilité d'occurrence de 0,1 par essai. Conséquences : Essai fait par erreur sur un des sous-systèmes non arrêté, dégrade système en 1oo1 temporairement (20% des cas). Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).	Probabilité d'occurrence de 0,1 par essai. Conséquences : Essai fait par erreur sur un des sous-systèmes non arrêté et AAR (20% des cas). Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).	Probabilité d'occurrence de 0,1 par essai. Conséquences : Fermeture intempestive et AAR (20% des cas).. Défiabilisation. Fiabilité dégradée par facteur deux pour la suite de la mission (80% des cas).

4.12.2 Optimisation des inspections des capteurs

Certains capteurs sont en redondance et testés périodiquement. Les mesures sont intégrées par des logiques de vote ou des moyennes, avec inhibition éventuelle d'un capteur qui présente une anomalie détectée.

La question est d'estimer les périodicités optimales T'i (i=1,2,3,4) des essais révélateurs pour chacune des chaînes de mesure.

Le chapitre 4.1.3 présente les capteurs employés. Une chaîne de mesure constitue un système 1oo1, 1oo2 ou 2oo3 selon les cas:

Tableau 4.18. Récapitulatif des données de fiabilité pour l'optimisation de l'inspection des capteurs

Grandeur physique	Architecture	Essais périodiques
Mesure Nge gamme étroite NTB (Niveau Très Bas) et NTH (Niveau Très Haut)	3 capteurs de niveau Tout Ou Rien par GV (dits ANG05x). Système en 2oo3 dégradé éventuellement en 1oo2.	Essais révélateurs de périodicité T'1
Mesure débit eau alimentaire (Qe)	2 capteurs par ligne d'alimentation d'un GV (dits ANG04x). 1 seul employé à la fois pour la régulation.	Essais révélateurs de périodicité T'2
Mesure débit Vapeur (Qv)	2 capteurs (dits VVP0x) par ligne de sortie d'un GV	Essais révélateurs de périodicité T'3
Mesure Nge gamme étroite NB (Niveau Bas)	Mesure de Niveau Bas : cf NTB et NTH Mesure déséquilibre eau vapeur, par GV : deux comparaisons, chacune entre un capteur débit eau (Qe) Tout Ou Rien ANG04x et un capteur de débit vapeur (Qv) VVP0x	-
Mesure Ngl gamme large (non modélisé)	1 capteur Tout Ou Rien par GV (dit ANG06x).	Essais révélateurs de périodicité T'4

Hypothèses et contraintes [ZIO, 2001]

- Un capteur est testé toutes les 6 semaines
- Les inspections doivent laisser fonctionnelle au moins une chaîne de mesure pour chaque grandeur.
- Lorsqu'un capteur est réparé défaillant suite à un essai périodique, il est immédiatement mis en réparation et considéré comme « as good as new » (sauf si effet iatrogénique).
- Lorsqu'un capteur est identifié comme correct suite à un essai périodique, il est immédiatement remis en ligne (en attente ou en service, selon les cas) et considéré comme « as good as new » (sauf si effet iatrogénique).
- Le temps de remise en ligne est considéré comme négligeable.
- Cout d'une heure de perte de production : C = 40000 Euros
- Cout d'un essai révélateur C = 100 Euros
- Durée d'un essai révélateur (et durée d'indispo associée), t = 2 heures pour tous les types de capteurs
- Cout d'une réparation C = 1000 Euros /hr
- Cout d'une inhibition : 0 Euros. Dans certains cas, l'inhibition est une alternative possible à la réparation.

- Durée d'une réparation (et durée d'indispo associée), MTTR = 8 heures

Cas des capteurs « intelligents ».
A cette étape de l'étude, il n'y a pas de particularités pour l'instrumentation « intelligente ». (cf 4.1.3.)

4.13 Données pour la représentation des erreurs de spécification, de conception logique, ou de paramétrage.

Le cas est concerné par ces erreurs, lorsqu'elles portent sur la fonction applicative spécifique (régulation par PID d'un niveau d'eau GV) ou dans le cas d'emploi de capteurs ou actionneurs « intelligents »..
Ces erreurs peuvent être identifiées ou simulées, dans les limites classiques de la testabilité, en injectant des « fautes » dans les règles logiques les valeurs de paramètres et les formules de calcul employées dans la régulation et la commande du système.
Ce point n'a pas été abordé plus en détail dans la projet APPRODYN.

4.14 Simplifications du cas test et niveau de difficulté

Des simplifications du modèle peuvent être faites, ce qui permet de définir des niveaux de difficulté ou de représentation d'un système hybride. Le tableau 1.2. « Niveaux de représentation d'un système hybride » propose des niveaux de difficulté et des simplifications.

5 Modélisation par Automates Stochastiques Hybrides (ASH)

5.1 Principes et références

De nombreuses approches sont possibles pour modéliser un système complexe. L'approche descendante (ou top down) considère le système dans sa globalité et le décompose progressivement en sous entités dans une structuration hiérarchisée. Elle s'arrête lorsque le niveau de détail obtenu permet de satisfaire au but de la modélisation. L'approche montante (ou bottom up) part de la description des composants élémentaires et construit progressivement le modèle du système en décrivant les interactions. Dans le cadre des études de sûreté, cette seconde approche nous a semblé plus à même de traquer toutes les séquences critiques d'évènements, outre bien sûr de permettre l'évaluation probabiliste. Nous avons choisi de mener l'étude sur la base de modèles de type Automates à Etats Finis (AEF). Les AEF ont été utilisés pour représenter le comportement des systèmes à évènements discrets, c'est-à-dire dont l'état (discret) évolue uniquement sur occurrence d'évènements On peut reprocher à cette approche sa tendance à l'explosion du nombre d'états, mais c'est sans doute le prix à payer pour des études plus exhaustives de la sûreté. Elle présente en effet des avantages :

- L'approche AEF permet une construction formelle du modèle du système en partant des « automates embryonnaires » des composants et systèmes élémentaires dont les propriétés sont facilement vérifiables (complétude, vivacité, atteinte en un temps borné, accessibilité, etc.). Par l'opération formelle de composition par synchronisation [CAS 08], l'automate résultat hérite des propriétés qui ne sont donc plus à vérifier. C'est un avantage par rapport à une approche type réseaux de Petri dans laquelle la construction du modèle est intuitive et doit être suivie, avant toute utilisation (en simulation en particulier), d'une étape de vérification de ses propriétés.
- Le second avantage, non moins important, est l'aptitude naturelle du modèle AEF à générer l'ensemble de séquences possibles d'évènements (son langage) incluant les séquences critiques.

La prise en compte du caractère stochastique des évènements tels que la défaillance d'un composant oblige à la définition du concept d'automate stochastique (un graphe de Markov en est un type particulier). De plus, la prise en compte de la dépendance de certains évènements (leur occurrence ou leur loi de probabilité d'occurrence) à l'évolution continue de la physique du système régie par des équations algébro-différentielles, oblige à la définition du concept d'automate stochastique hybride (ASH). Les automates stochastiques hybrides ont été définis formellement et appliqués à des cas tests académiques en fiabilité dynamique [PER 09, PER 11]. Ils ont permis la modélisation et l'étude probabiliste des systèmes présentant des conflits dans l'évolution de leur comportement [PER 10] et l'évaluation de l'intensité de défaillance des systèmes complexes en contexte dynamique [BAB 11].

5.2 Qu'est-ce qu'un automate stochastique hybride ?

5.2.1 Définition

Un automate stochastique hybride est un 11-tuple :

$$(X, E, A, \mathcal{X}, \mathcal{A}, H, F, \mathcal{P}, x_0, \mathcal{X}_0, \mathcal{P}_0)$$

dans lequel :

– X est un ensemble fini d'états discrets $\{x^1, x^2\ldots, x^m\}$;

– E est un ensemble fini d'évènements $\{e_1,\ldots,e_r\}$ déterministes ou stochastiques ;

– $\mathcal{X}$ est un ensemble fini de variables réelles évoluant dans le temps $\{x_1,\ldots,x_n\}$, on note par x le vecteur des variables x_i, $x = [x_1\ldots, x_m]^T$;

– A est un ensemble fini d'arcs de la forme (x, e_k, G_k, R_k, x') où x et x' sont les états origine et but de l'arc k, e_k est l'évènement associé à l'arc, G_k la condition de garde sur $\mathcal{X}$ dans l'état x et R_k est la fonction de réinitialisation de $\mathcal{X}$ dans l'état x' ;

– $A : X \times X \rightarrow (\Re^+ \rightarrow \Re)$ est une fonction des « activités », qui associe à un élément de X x X une fonction définie sur $\Re^+$ et à valeurs dans $\Re$;

– H est un ensemble fini d'horloges ;

– F : H→ ($\Re$ →[0,1]) est une application qui associe à chaque horloge une fonction de répartition ;

– $P = [p_i^l]$ est une matrice de distributions de probabilités où p_i^l est une distribution de probabilités de transition d'états $p\left(\chi^i \middle| \chi^l, e\right)$. Par exemple, si nous avons le même évènement e_q définissant les transitions de l'état discret x^l vers les états discrets x^1, x^2…, x^j (nous disons qu'il y a j transitions en conflit, l'automate à états finis sous-jacent ne serait alors pas déterministe), nous pouvons définir la probabilité p_1^l de passer de l'état x^l à l'état x^1, la probabilité p_2^l de passer de l'état x^l à l'état x^2 et la probabilité p_j^l de passer de l'état x^l à l'état x^j, avec $p_1^l + p_2^l + ... + p_j^l = 1$;

– x^0, x_0 et P_0 correspondent respectivement à l'état discret initial, à la valeur initiale du vecteur d'état continu dans l'état initial discret et à la distribution initiale de probabilités de transition.

Les éléments X, E et A de l'automate stochastique hybride correspondent à l'automate à états finis définissant sa partie évènementielle (discrète). *X, A, R* et *G* définissent sa partie continue. H correspond à son aspect temporisé et finalement F et *P* expriment son aspect stochastique.

Le fonctionnement de cet automate s'interprète de la manière suivante : si le système est dans l'état x^l, il est réceptif à un sous-ensemble des évènements de E associés aux différents arcs sortant de cet état. Sur occurrence d'un de ces évènements e_q associé à l'arc k, si la condition de garde G_k associée à cet arc est vérifiée, le système passe à l'état x^i but de l'arc. La fonction R_k également associée à cet arc définit les valeurs initiales des variables continues du système dans l'état x^i. Si e_q est associé à plusieurs arcs, l'état final résultera du tir de la distribution de probabilité p_i^l. Dans l'état i l'évolution des variables réelles x en fonction de temps est définie par une fonction $f_i(\cdot)$.

Un exemple d'un ASH à quatre états discrets est schématiquement présenté sur la figure 5.1 ($\dot{x}$ correspond à la dérivée de la variable x). L'automate se trouve initialement dans l'état discret 1 et l'évolution de la variable continue x est donnée par la fonction $f_1(\cdot)$. L'occurrence de l'évènement e_1 et la vérification de la condition de garde G_1 permettent d'effectuer la transition vers l'état discret 2. La condition de réinitialisation R_1 donne la valeur initiale pour la variable continue x dans cet état discret qui évolue suivant la fonction $f_2(\cdot)$ et ainsi de suite.

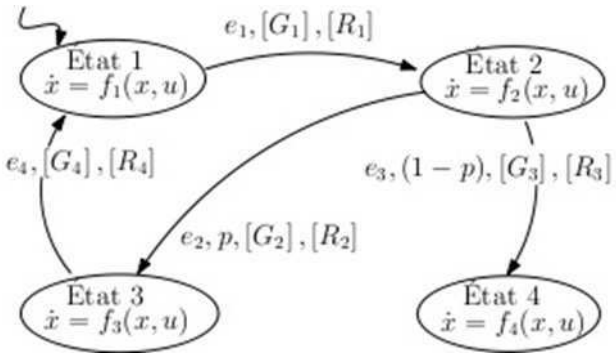


Figure 5.1. Exemple d'automate stochastique hybride

Les durées de bon fonctionnement et de réparation des composants sont matérialisées par les horloges H. Ces durées sont obtenues par tirage aléatoire à partir des fonctions de répartitions de probabilités..

Tous les facteurs contribuant à la complexité généralement associée au concept de fiabilité dynamique évoqués au § 2.1 sont donc pris en compte dans ce type de modèle qui ne permet certes pas d'accéder à des solutions analytiques mais qui est parfaitement adapté à la simulation.

L'outil informatique utilisé pour implémenter l'automate stochastique hybride afin d'évaluer la fiabilité d'un système dynamique hybride est la boîte à outils Scicos de Scilab. Nous avons implémenté l'automate stochastique hybride sur la base de l'automate hybride proposé par [NAJ 07]. L'automate dont la définition est donnée par [NAJ 07] est un bloc Scicos schématiquement présenté sur la figure 5.2 (un seul état discret est considéré dans le but de simplification). Il est constitué de *m* ports d'entrée, *m* correspondant au nombre d'états discrets de l'automate (à gauche du bloc) et de deux ports de sortie (à droite du bloc). La sortie en bas du bloc est une sortie composite *e* des évènements discrets. Celle-ci est activée quand une transition d'état se produit. Chaque entrée correspond à un vecteur qui contient la dynamique *A* du système dans l'était x^i (*c'est-à-dire* l'évolution des variables continues *X)*, les valeurs initiales de *X* dans l'état *(R)*, et les conditions de garde *G* associées aux transitions de sortie de l'état. Les deux sorties correspondent respectivement à un vecteur qui indique les numéros de l'état discret courant x^i et du précédent x^{i-1} et au vecteur des variables d'état continu *x* et de leurs dérivées $\dot{x}$.

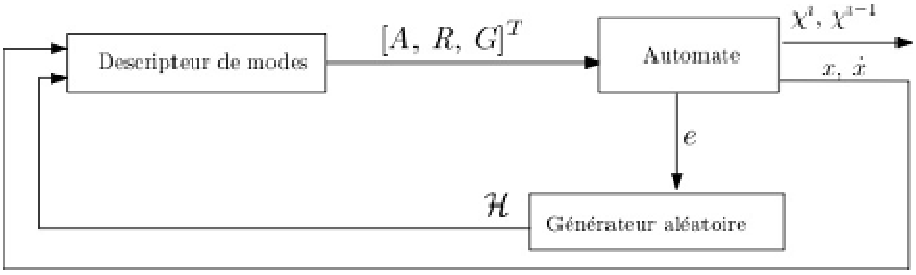


Figure 5.2. Implémentation d'un ASH sur Scicos/Scilab : schéma

Le générateur aléatoire de la figure 5.2 correspond à la structure temporisée stochastique H de la définition. Le générateur aléatoire réalise des tirages aléatoires correspondant aux transitions aléatoires et est activé chaque fois qu'il y a un changement d'état discret grâce à la sortie des évènements discrets de l'automate.

Le descripteur de modes correspond aux différentes dynamiques continues du système. Il y a autant de dynamiques continues que d'états discrets.

5.2.2 Approche par structuration et synchronisation de manière générique

Inspirée de l'approche développée pour les AEF [CAS 08], elle consiste à définir des AEF représentant le comportement de chacun des composants élémentaires et à les assembler à l'aide de l'opération de synchronisation d'AEF. On obtient ainsi un automate représentatif du système dont les propriétés ne sont pas à démontrer puisqu'il s'agit d'une opération formelle. L'intérêt de cette méthode est de délivrer un modèle formel du système dont on peut garantir la complétude vis-à-vis du cahier des charges dans la mesure de celle des automates élémentaires. Des erreurs dans la définition des automates élémentaires ou même dans la spécification peuvent être mises en évidence par certaines propriétés de l'automate global (accessibilité, blocage, réinitialisabilité, etc.). Pour les ASH, dans l'état actuel du développement des outils, on construit l' « *AEF sous-jacent* » avec cette méthode (dans ce projet on utilise les outils DESUMA développés par [CAS 08]) et on le complète avec le caractère stochastique associé aux évènements et les équations algébro-différentielles associées aux états.

Une autre approche structurée pour construire l'AEF sous-jacent serait possible en utilisant certaines classes de réseaux de Petri, tel que les réseaux de Petri colorés hiérarchiques définis par K. Jensen [JEN 09]. Ces réseaux de Petri permettent de générer le graphe de tous les marquages accessibles depuis l'état initial, graphe de marquage qui n'est rien d'autre que l'AEF global sous-jacent à l'ASH.

5.3 Modélisation du cas test

Dans le cadre du cas test les automates élémentaires et les automates globaux (résultats de synchronisation) suivants sont considérés :

1. Barillet VVP ;
2. Trois pompes CEX et l'automate de spécification pour leur fonctionnement commun donnant l'automate global CEX ;
3. Deux TPA partie turbine et deux TPA partie hors turbine avec deux automates de spécification, un automate de spécification pour le fonctionnement commun des deux TPA ;
4. Vanne ARE petit débit ;
5. Vanne ARE gros débit ;
6. Automate de commande. Il définit l'évolution de la puissance et donne les ordres de démarrage/arrêt, ouverture/fermeture aux composants, pilotant ainsi tous les autres sous-systèmes.

Le nombre d'états et des transitions pour chacun de ces automates élémentaires ainsi que pour les automates globaux est donné dans le tableau 5.1.

Du fait de la complexité du système considéré dans le cadre du cas test et du nombre élevé d'états de chaque sous-système qui en découle, la synchronisation a été faite au sein de chaque Système Elémentaire (CEX, TPA, etc.).

La représentation cohérente du fonctionnement simultané des sous-systèmes est atteinte à l'aide des variables de synchronisation qui sont communes aux sous-systèmes et qui assurent le lien entre ces derniers. Nous illustrons l'implémentation de cette approche par un exemple qui considère l'automate de l'ARE petit débit et l'automate de commande.

Sous-système	**Nombre d'états**	**Nombre de transitions**
Barillet VVP	**3**	**4**
CEX (1, 2, 3)	15 (x3)	26 (x3)
CEX spécification	46	114
CEX : automate global	**121**	**225**
TPA hors turbine (1, 2)	16 (x2)	27 (x2)
TPA turbine (1, 2)	13 (x2)	22 (x2)
TPA spécification turbine et hors turbine (1, 2)	*19 (x2)*	*30 (x2)*
TPA spécification globale	94	116
TPA : automate global	**1029**	**2655**
ARE petit débit	**49**	**93**
ARE gros débit	**49**	**93**
Automate de commande	**44**	**60**

Tableau 5.1. Automates élémentaires et automates globaux du cas test. Police standard : les automates élémentaires, en italique : les résultats de la synchronisation préliminaire, en gras : les automates globaux

5.3.1 Exemple du Système Elémentaire CEX

Le schéma de l'automate élémentaire d'une pompe CEX est présenté en figure 5.3 et l'automate de spécification du fonctionnement des trois CEX est en figure 5.4. L'automate élémentaire décrit le fonctionnement de la pompe indépendamment des autres pompes, l'automate de spécification définit le fonctionnement synchronisé des trois pompes.

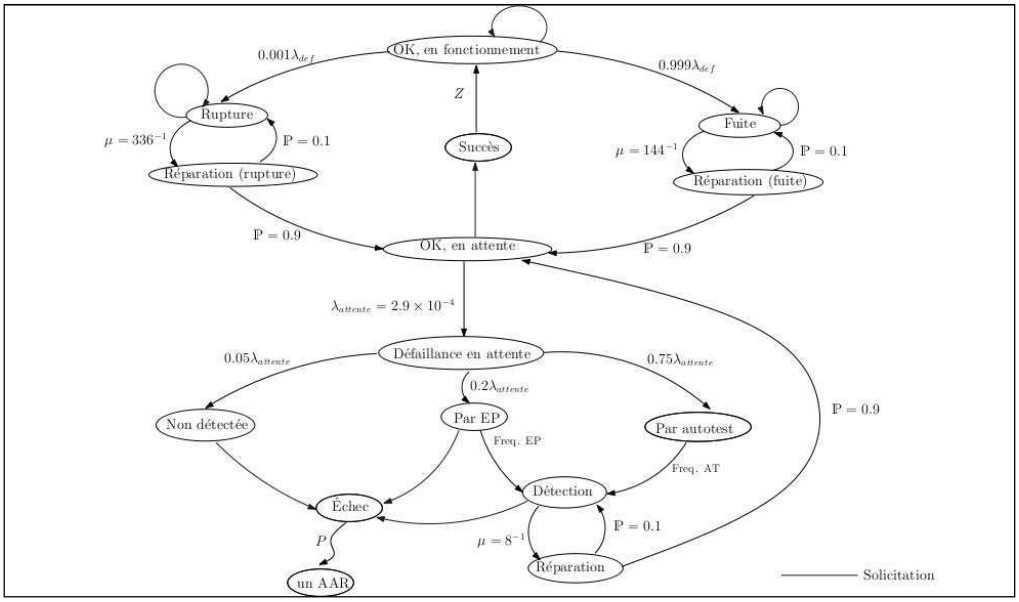


Figure 5.3. Automate élémentaire d'une pompe CEX.
$\lambda_{déf}$: taux de défaillance en fonctionnement, λ_{atente} : taux de défaillance en attente, μ : taux de réparation, Z : transition instantanée, en bleu : sollicitations.

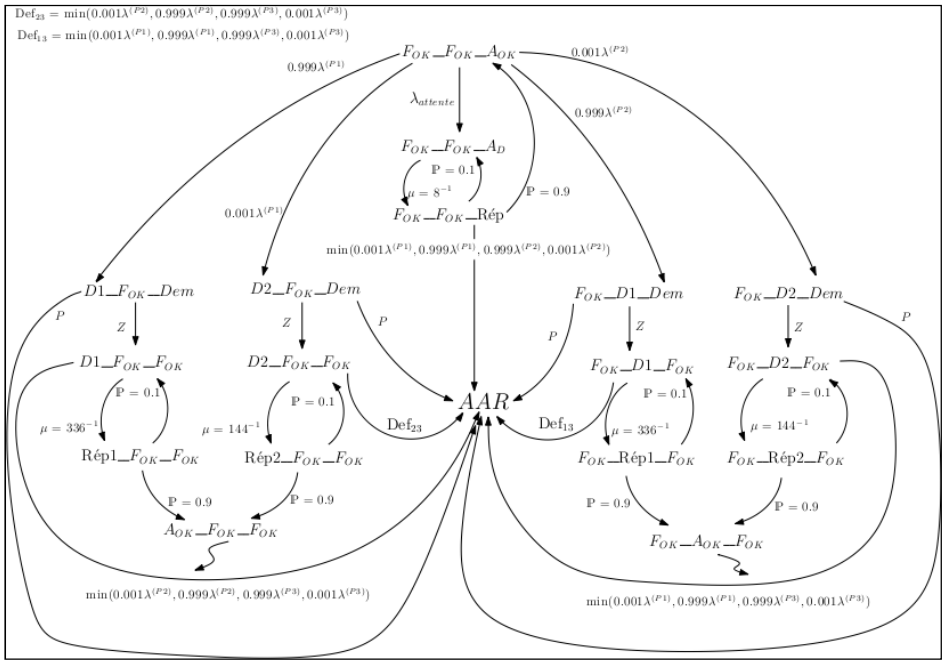


Figure 5.4. Automate de spécification d'une pompe CEX.

F_F_A : états des trois pompes, F : en fonctionnement, A : en attente, Rép1(2) : en réparation de défaillance de type 1(2), Z : succès de démarrage, P : échec de démarrage, $\lambda^{(Pi)}$: taux de défaillance en fonctionnement de pompe i, λ_{atente} : taux de défaillance en attente, μ : taux de réparation.

5.3.2 Exemple du système élémentaire ARE et de son automate de commande.

Le schéma simplifié (représentant une partie de la montée en puissance) de l'automate de commande est présenté sur la figure 5.5. Le lancement du système implique la montée en puissance (P) de 0 à 2 % au cours de temps t (l'échelle de temps considérée dans cet exemple est en heures) selon l'équation P = 0.2t. Cette montée est assurée par un autre système que l'ARE (l'ASG). Une fois la puissance de 2 % atteinte, l'automate de commande envoie l'ordre de démarrage à tous les sous-systèmes : CEX, TPA, ARE (dans le but de simplification les échecs de démarrage ne sont pas systématiquement présentés sur la figure 5.5). La puissance reste à 2 % tant que tous les sous-systèmes ne sont pas lancés correctement. Cette phase est suivie par la montée en puissance. L'évolution de la puissance n'est pas homogène pendant toute la période de montée, ce qui introduit le changement de l'équation d'état (ou encore l'équation qui définit l'évolution de la puissance, par exemple P = -6 + 0.8t ou P = -440 + 22.5t). Les transitions en gras (forçage de puissance à 2 %) représentent les évènements modélisés par variables de synchronisation, c'est-à-dire les évènements extérieurs et communs à plusieurs sous-systèmes (l'automate de commande, ARE et TPA dans l'exemple). Les transitions en pointillé représentent les évènements envoyés à l'automate de commande par l'automate de l'ARE petit débit.

Le schéma simplifié de la vanne ARE petit débit (un seul mode de défaillance est pris en compte dans la figure, pour simplification) est donné sur la figure 5.6. En phase de montée en puissance (ARE_{PD} ouverte), l'équation de puissance est donnée par l'automate de commande : P = 0.2t ou P = -6 + 0.8t (selon le temps global t). Dans ce cas, tous les sous-systèmes peuvent être forcés aux états correspondants à P = 2 % (fermeture des vannes, arrêt des pompes, etc.) dû aux évènements stochastiques (par exemple, défaillance en fonctionnement des TPA ou de l'ARE). Ces forçages sont exécutés à l'aide des variables de synchronisations. L'automate de l'ARE petit débit, à son tour, envoie les évènements d'échec/succès de l'ouverture à l'automate de commande.

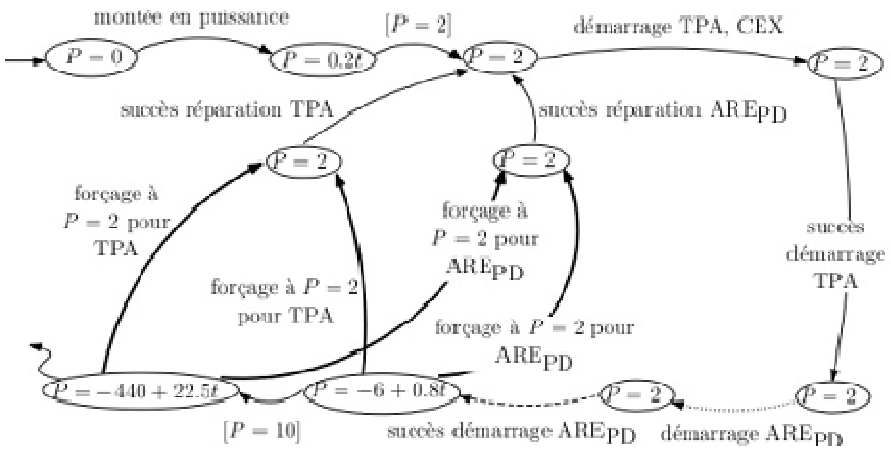


Figure 5.5. Automate de commande du cas test : schéma simplifié.

Les équations d'état sont indiquées. En gras : les transitions représentées par les variables de synchronisation, en pointillé large : les évènements envoyés à l'automate de puissance par l'automate de l'ARE petit débit, en pointillé étroit : les évènements envoyés par l'automate de l'ARE petit débit à l'automate de commande

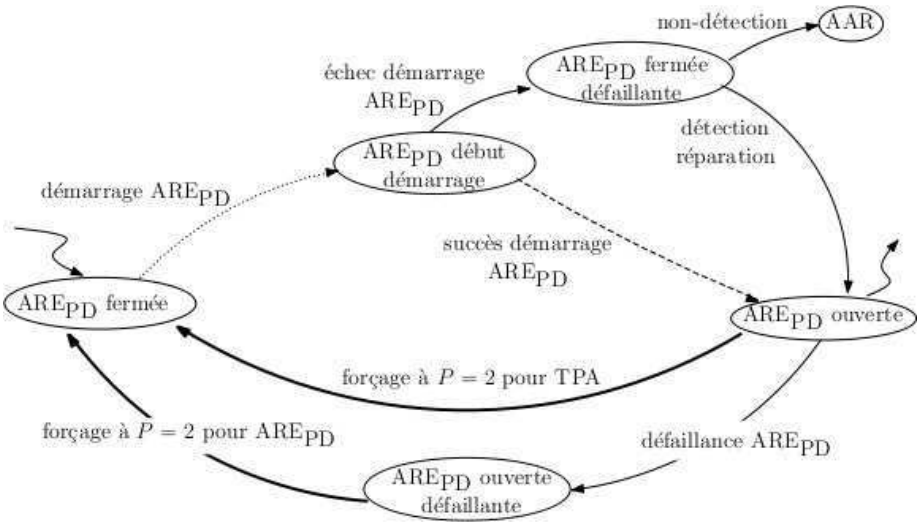


Figure 5.6. Automate de l'ARE petit débit du cas test : schéma simplifié.

En gras : les transitions représentées par les variables de synchronisation, en pointillé large : les évènements envoyés à l'automate de puissance par l'automate de l'ARE petit débit, en pointillé étroit : les évènements envoyés par l'automate de commande à l'automate de l'ARE petit débit

Une fois la puissance de 100 % atteinte, le système fonctionne pendant une certaine durée en régime stationnaire. En fin de cette période, la phase de descente en puissance est entamée. La descente en puissance est symétrique à la montée.
Les « fragments » de l'automate de puissance utilisé dans la modélisation et présentés dans le format DESUMA sont donnés sur les figures 5.7-5.10. Le tableau 5.2 fournit les éléments facilitant l'interprétation de ces figures : il contient les noms explicites des transitions et des variables de synchronisation qui y sont utilisées. Notons que dans l'approche ASH la cohérence générale et la complétude du modèle sont mis en avant. Cela explique en partie la grande taille du modèle.
Par exemple, au démarrage, l'ordre de démarrage des composants est respecté : CEX, TPA1, ARE PD, etc. En cas de refus de démarrage du TPA1, le système reste à 2% P_n (voir figure 5.7). Pendant la montée en puissance, les forçages à 2% pour cause de défaillances des vannes ARE ou pompes TPA et les forçages à 60% pour cause de défaillances des TPA sont prévus ; les forçages causés par les TPA influent sur l'état des ARE et inversement (voir figure 5.8). Lorsqu'une défaillance d'une des TPA survient pendant la période de puissance constante (100% P_n) ou pendant la descente en puissance, la descente en puissance est effectuée (continuée) sur la pompe en état de marche (voir figure 5.9). Il en est de même pour la descente en puissance de 60% à 0% : la descente commence par l'arrêt de TPA1, ouverture de ARE PD, suivie par la fermeture de ARE GD, etc. ; en cas de refus d'arrêt de TPA1, la descente est effectuée sur TPA2 (voir figure 5.10).
De la même manière il est prévu qu'au démarrage des TPA le démarrage de la partie hors turbine est suivi par le démarrage de la partie turbine de chaque TPA, et TPA1 est démarrée en premièr. Cces éléments sont pris en compte dans l'automate de spécification des TPA et dans les automates élémentaires de chacune des TPA.

Une telle approche permet la modélisation précise du phénomène, mais nécessite un grand nombre d'états des automates, augmentant ainsi la taille du modèle, ce qui rend les simulations couteuses en temps.

Nom de transition	Interprétation	Type de transition (variable de synchronisation)
d_cex	Démarrage de CEX	Envoyé à l'automate CEX
ok_d_CEX	Succès de démarrage de CEX	reçu de l'automate CEX
d1P	Démarrage de TPA1	Envoyé à l'automate TPA
d2P	Démarrage de TPA2	Envoyé à l'automate TPA
ok_d1P	Succès de démarrage de TPA1	reçu de l'automate TPA
ok_d2P	Succès de démarrage de TPA2	reçu de l'automate TPA
ouv_VPD	Ouverture de ARE PD	Envoyé à l'automate ARE PD
ok_ouv_VPD	Succès de l'ouverture de ARE PD	reçu de l'automate ARE PD
ferm_VPD	Fermeture de ARE PD	Envoyé à l'automate ARE PD
ok_ferm_VPD	Succès de fermeture de ARE PD	reçu de l'automate ARE PD
seuil_montee_2	Puissance atteint 2%	Variable continue d'état
seuil_montee_10	Puissance atteint 10%	Variable continue d'état
seuil_montee_15	Puissance atteint 15%	Variable continue d'état
seuil_montee_60	Puissance atteint 60%	Variable continue d'état
seuil_montee_100	Puissance atteint 100%	Variable continue d'état
fin_palier	Fin de palier de pleine puissance	Variable continue d'état : temps
seuil_Ngl=33	Le niveau de gamme large atteint 33%	Reçu de l'automate de régulation (PID)
for2%_VPD	Forçage à 2% pour cause de panne d'ARE PD	Reçu de l'automate de ARE PD et envoyé à l'automate de TPA
fin_for2%_VPD	Fin de forçage à 2% pour cause de panne d'ARE PD	Reçu de l'automate de ARE PD et envoyé à l'automate de TPA
for2%_VGD	Forçage à 2% pour cause de panne d'ARE GD	Reçu de l'automate de ARE GD et envoyé à l'automate de TPA
fin_for2%_VGD	Fin de forçage à 2% pour cause de panne d'ARE GD	Reçu de l'automate de ARE GD et envoyé à l'automate de TPA
for2	Forçage à 2% pour cause de panne de TPA	Reçu de l'automate de TPA
For60	Forçage à 60% pour cause de panne de TPA	Reçu de l'automate de TPA
P_TPA1	Panne de TPA 1	Reçu de l'automate de TPA
P_TPA2	Panne de TPA 2	Reçu de l'automate de TPA
a1P	Arrêt de TPA1	Envoyé à l'automate de TPA
ok_a1P	Succès d'arrêt de TPA1	Reçu de l'automate de TPA
a2P	Arrêt de TPA2	Envoyé à l'automate de TPA
ok_a2P	Succès d'arrêt de TPA2	Reçu de l'automate de TPA

Tableau 5.2. Les transitions et les variables de synchronisation utilisées dans l'automate de puissance.

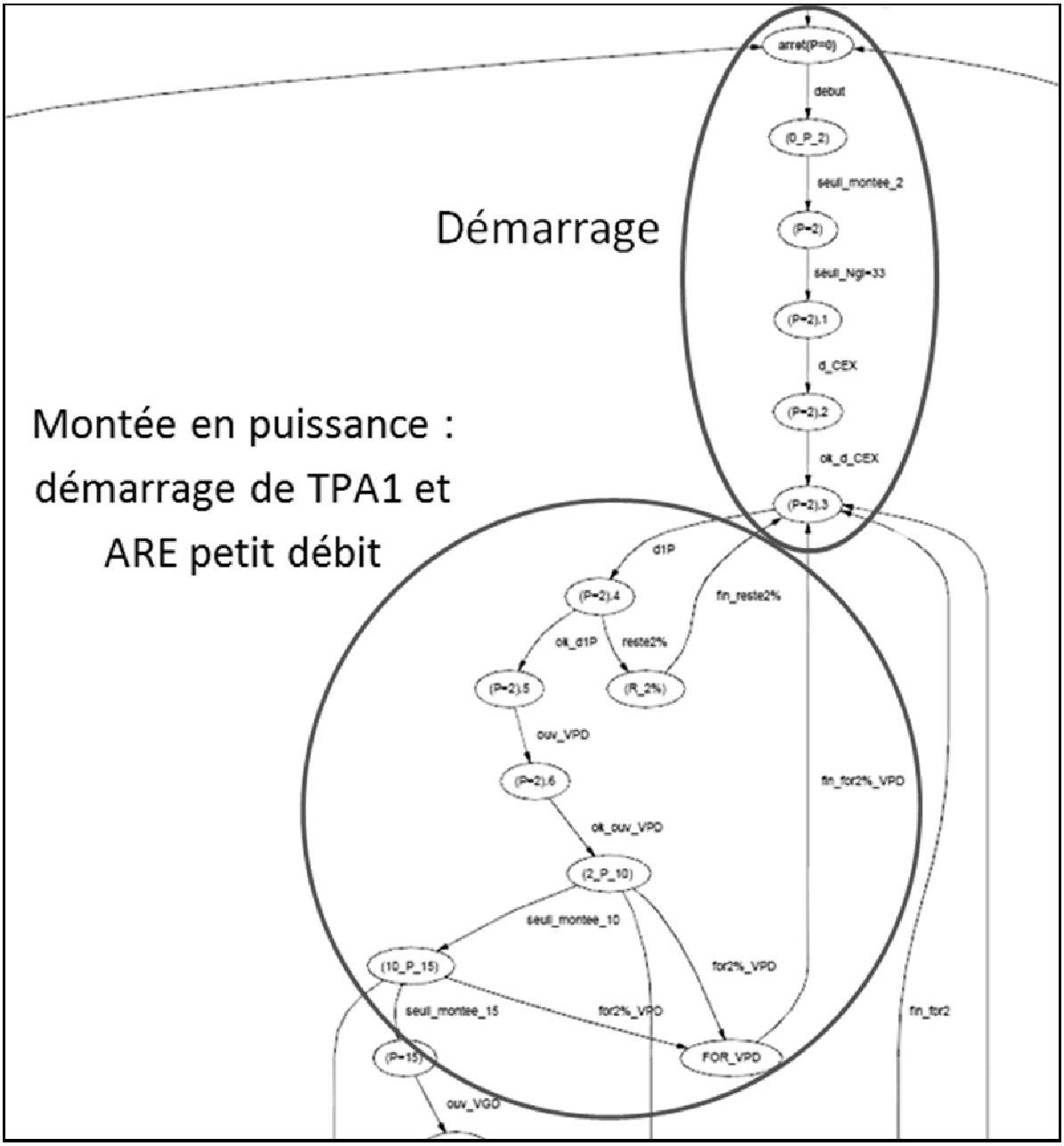


Figure 5.7. Automate de puissance : montée jusqu'à 15% de P_n.

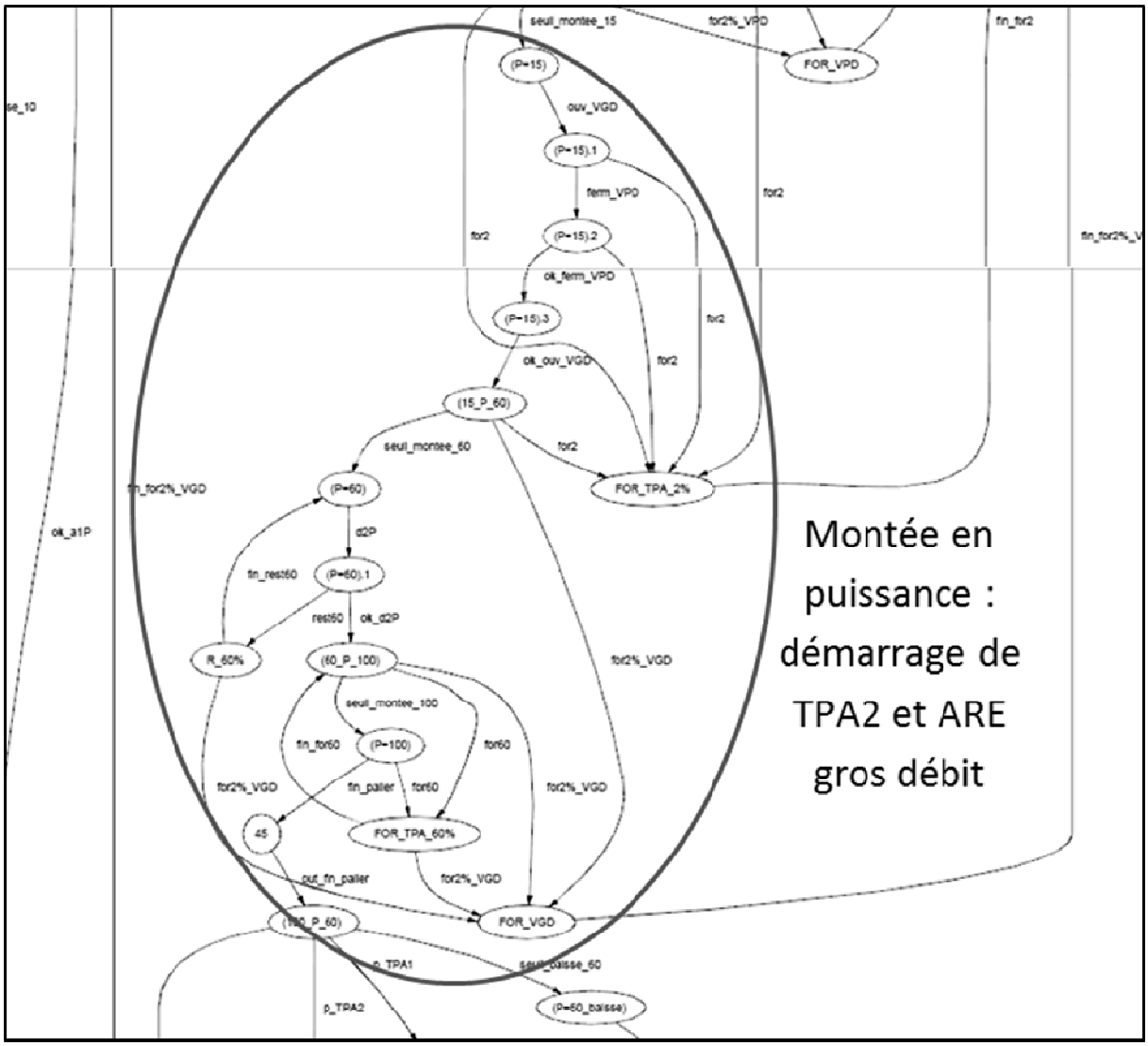


Figure 5.8. Automate de puissance : montée en puissance de 15% à 100% de P_n, palier 100% P_n.

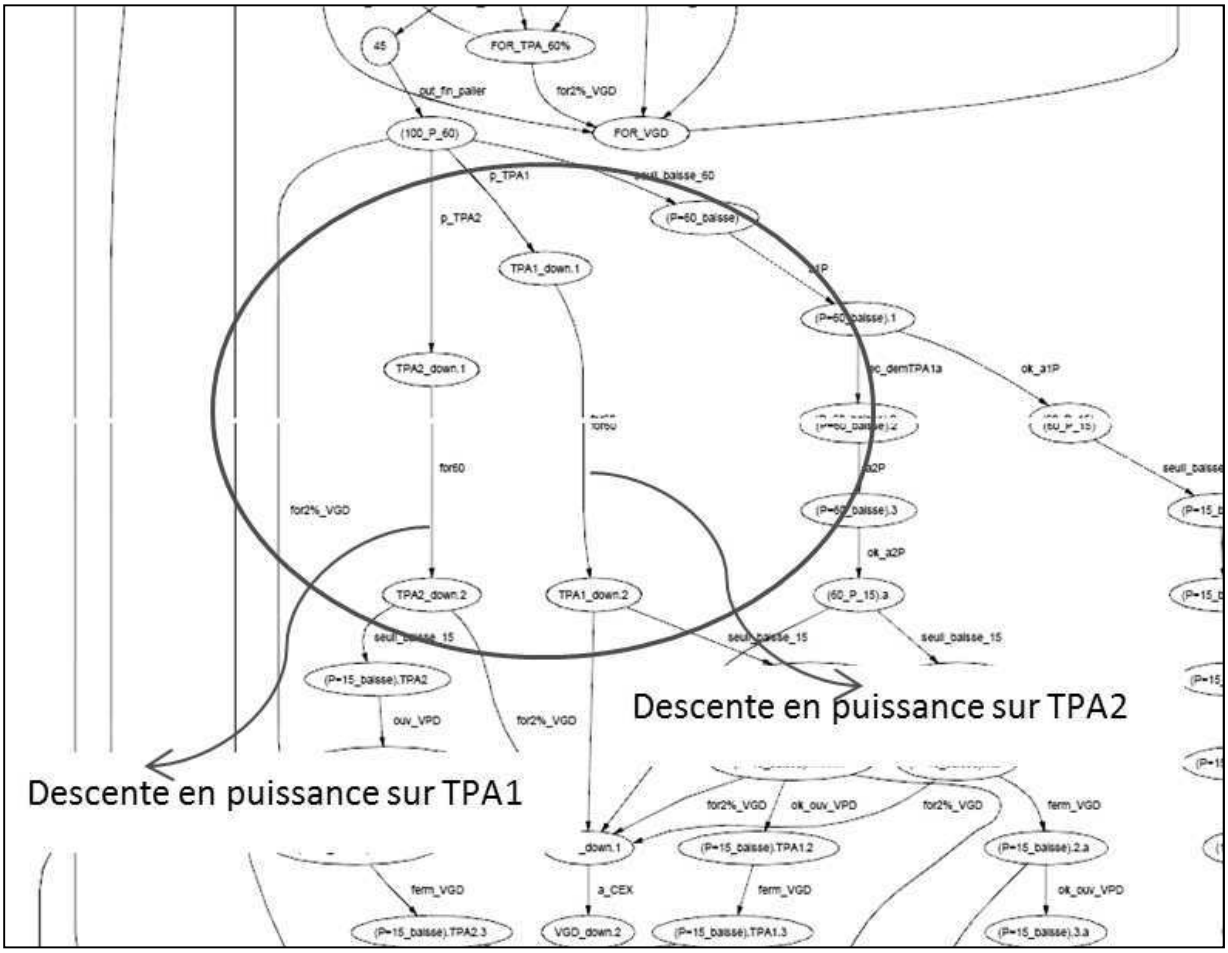


Figure 5.9. Automate de puissance : défaillance d'une des TPA pendant le palier de 100% P_n, suivie par le forçage à 60% et descente en puissance sur la TPA non-défaillant.

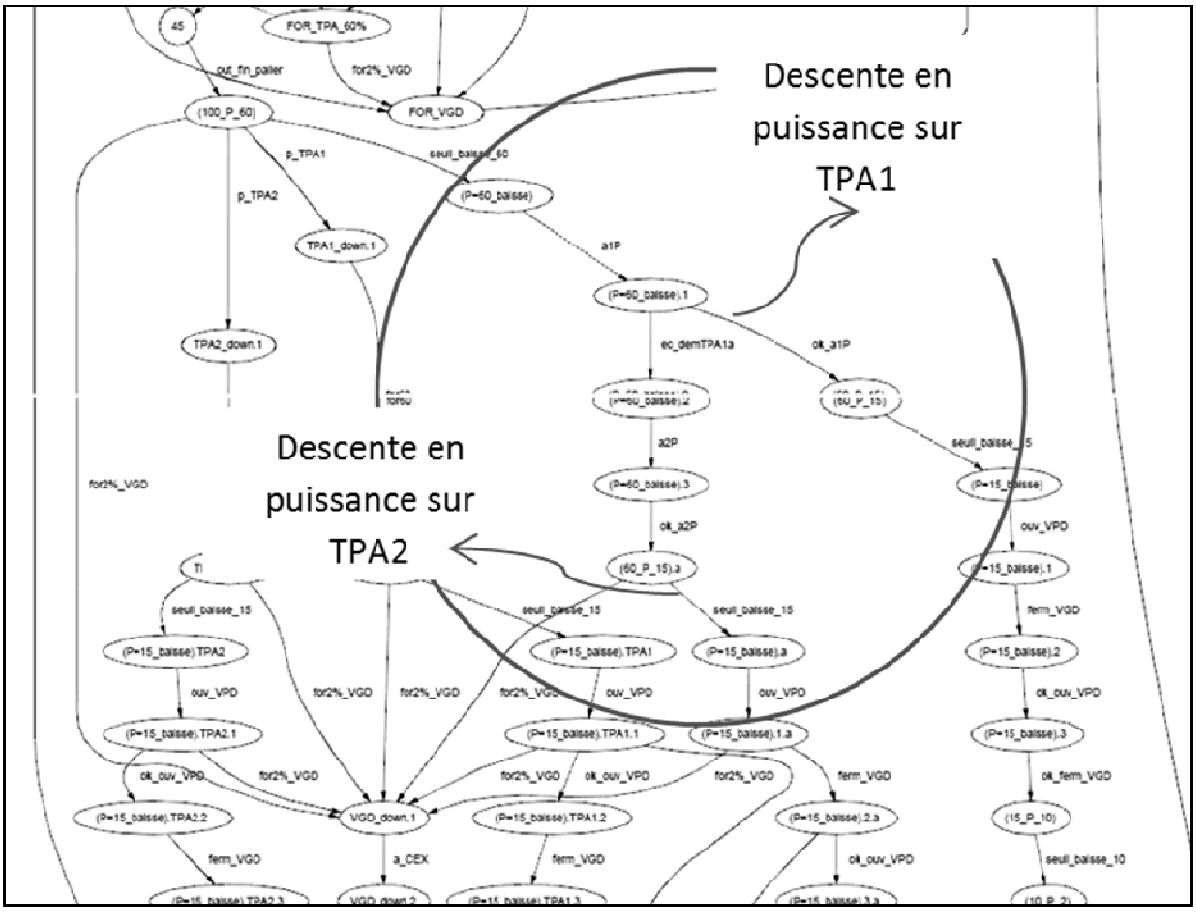


Figure 5.10. Automate de puissance : fin de la durée de palier de 100% Pn, descente en puissance.

La descente en puissance commence par l'arrêt de TPA1 et descente sur la TPA2, ou directement sur la TPA2 en cas de refus d'arrêt de TPA1.

5.4 Résultats qualitatifs et quantitatifs

L'approche ASH permet d'identifier toutes les séquences critiques et en calculer les probabilités d'occurrence. En fonction de la question posée, différents calculs peuvent être effectués. Nous présentons ici quelques exemples.

5.4.1 Exemple 1 : AAR suite à défaillance VVP.

La probabilité d'AAR causé par la défaillance de VVP peut facilement être calculée de la manière suivante (nous nous référons à la figure 5.11 pour illustration). Soit λ le taux de défaillance de VVP, alors λ^{-1} est la durée moyenne entre les défaillances (MTBF), qui est égale à 2560h dans notre exemple. La durée entre les défaillances est supposée suivre la loi exponentielle de paramètre λ. Afin d'estimer la probabilité d'occurrence d'AAR cause par le VVP durant 1 mois (la durée d'une simulation), il suffit ainsi de calculer la probabilité que la variable aléatoire X suivant la loi exponentielle de paramètre λ, soit inférieure à 1 mois. Dans notre cas, cette probabilité est de 25%.

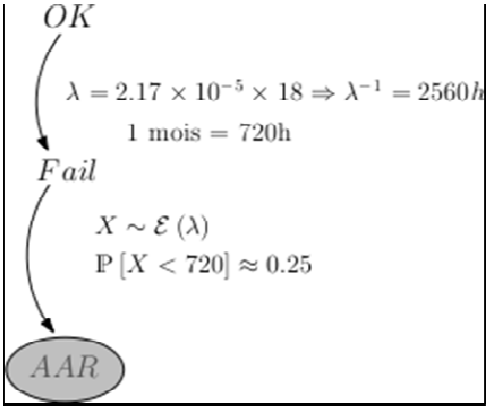


Figure 5.11. Probabilité d'AAR causé par la défaillance de VVP : illustration.

5.4.2 Exemple 2 : AAR suite à défaillance CEX

Nous présentons ici le calcul de la probabilité d'un AAR, causé par les défaillances des CEX, sachant que , plusieurs scénarios d'AAR sont possibles (par exemple: à cause de la défaillance en attente non-détectée ou non-réparée avant la demande de démarrage, à cause de la défaillance en fonctionnement de types différents, etc.) Notre exemple concerne la défaillance en fonctionnement de CEX 3 de type II,défaillance qui arrive le plus souvent.

La probabilité d'AAR causé par la défaillance des CEX est calculée de la manière suivante (nous nous référons à la figure 5.12 pour illustration). Soit λ le taux de défaillance de CEX, alors λ^{-1} est la durée moyenne entre les défaillances (MTBF), qui est égal à 2,6 ans dans notre exemple. En d'autres termes, une défaillance en fonctionnement de CEX arrive tous les 2,6 ans. Dans ce cas le CEX de secours est démarré, la probabilité de non-démarrage peut être considérée négligeable (0.00195/démarrage). Une fois la pompe de secours en marche, la pompe défaillante est mise en réparation. Il faut alors chercher la probabilité pour que la durée de réparation de la pompe de secours soit assez longue pour qu'une défaillance d'une des deux autres pompes puisse arriver avant la fin de la réparation de la pompe de secours. Nous prenons le pire cas , avec la durée de réparation le plus long (72h) et le temps de défaillance le plus court. Soit X la variable aléatoire caractérisant la durée jusqu'à la défaillance en fonctionnement d'une des CEX fonctionnelles, alors X suit une loi exponentielle de paramètre λ. La probabilité que X soit inférieure à la durée de réparation de la pompe de secours (72h) est alors égale à 0.3%. En conclusion, la probabilité d'un AAR du type considéré est de 0.3% en 2.6 ans.

La faible probabilité d'AAR des CEX est cohérente avec les faibles taux de défaillance des pompes, ainsi qu'avec le plus grand niveau de redondance (3 pompes), comparativement plus élevé que celui d'autres composants.

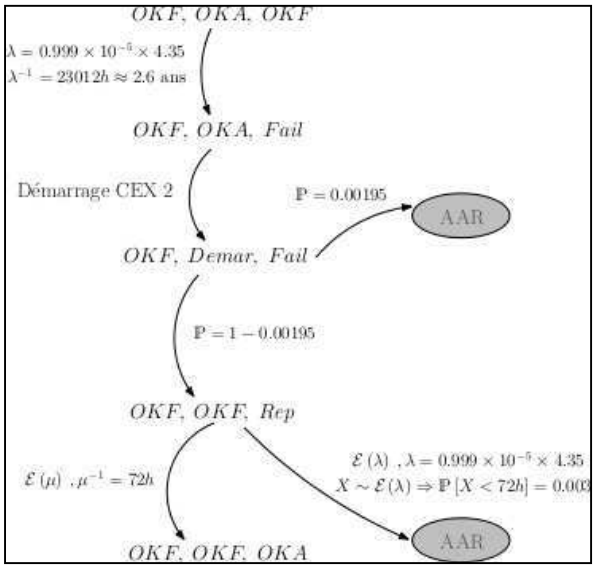


Figure 5.12. Probabilité d'AAR causé par les défaillances des CEX : illustration

5.4.3 Exemple 3 : AAR suite à défaillance TPA

Nous présentons ici le calcul de la probabilité d'AAR causé par le système élémentaire TPA lorsque la puissance est entre 0% et 60% Pn (un seul AAR à cause de TPA est possible dans ce cas). Nous nous appuyons sur la figure 5.13 pour illustration, les détails de calculs sont donnés dans l'encadré qui suit.

L'AAR résulte de la trajectoire suivante : le TPA1 démarre, la montée en puissance est effectuée, lorsque la puissance atteint 60% la TPA2 est démarrée, si elle ne démarre pas la puissance reste à 60% assurée par la TPA1 jusqu'à ce que la TPA2 ne soit pas réparée, si la défaillance en fonctionnement de TPA1 arrive avant la fin de réparation de TPA2, le système est arrêté (AAR).

Lorsque le TPA1 ne répond pas à la sollicitation, la puissance reste à 2% tant qu'elle n'est pas réparée. La probabilité de démarrage de la TPA1 est de 96% (démarrage de turbine et démarrage de partie hors turbine). Si la TPA1 tombe en panne pendant la montée en puissance jusqu'à 60%, le système est forcé à 2%, cela ne provoque pas d'AAR. Une fois la puissance à 60%, la TPA2 est démarrée avec la probabilité d'échec de démarrage de $9{,}3.10^{-4}$ (soit la partie hors turbine ne démarre pas, soit la partie hors turbine démarre et la partie turbine ne démarre pas).Dans le cas de non-démarrage de TPA2, la puissance est fixée à 60% et la réparation de TPA2 est effectuée.

Dans notre exemple nous considérons le pire cas : la durée de réparation la plus longue est prise en compte (parmi toutes les durées possibles dans ce cas : non-démarrage de partie turbine avec réparation courte/longue, etc.) et la durée jusqu'à la défaillance en fonctionnement de la TPA1 la plus courte est prise. La durée de réparation la plus longue est de 28h et la durée jusqu'à la défaillance la plus courte est de 2260h. Nous supposons que la durée entre les défaillances est une variable aléatoire X qui suit la loi exponentielle de paramètre λ (le taux de défaillance maximum). Il suffit alors de calculer la probabilité que cette durée soit inférieure à 28h. Selon les calculs la probabilité d'un AAR causé par les TPA dans le domaine de puissance [0% – 60%] P_n est de 1.2%.

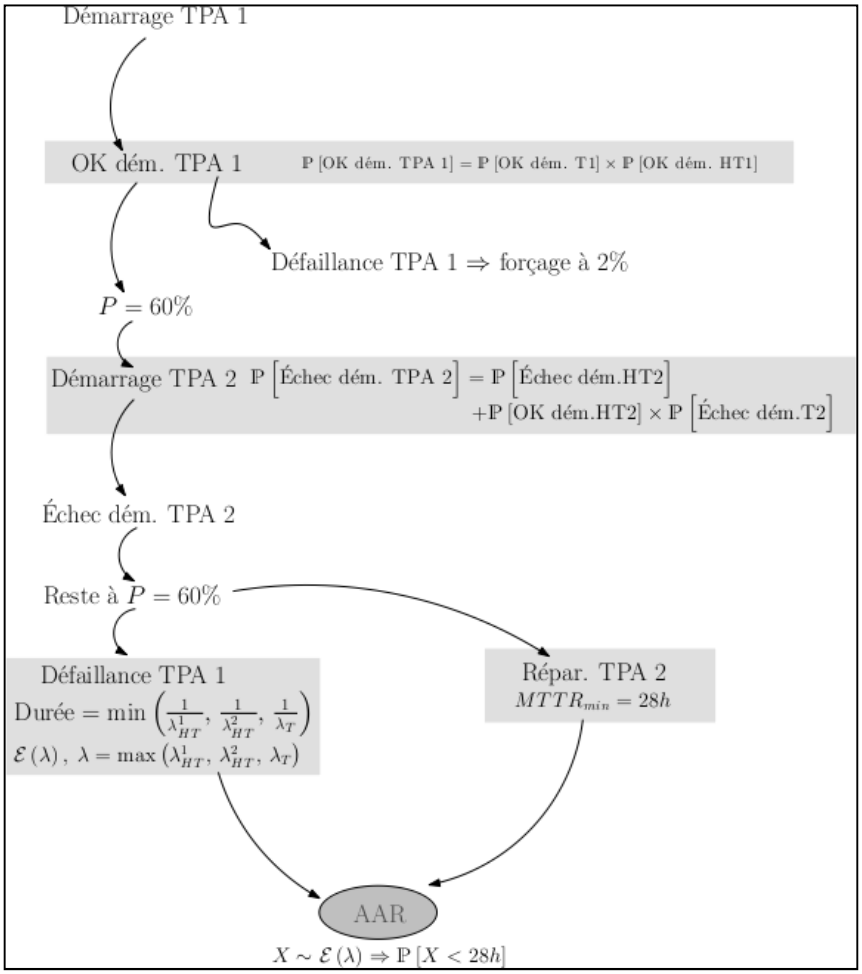


Figure 5.13. Probabilité d'AAR à cause de la défaillance des TPA : illustration

Encadré : Calcul de la probabilité d'un dype d'AAR, causé par les TPA

$$\begin{aligned}\mathbb{P}\left[\text{AAR}|P <= 60\%\right] &= \mathbb{P}\left[\text{Démarrage TPA1 : OK}\right] \\ &\times \mathbb{P}\left[\text{Démarrage TPA2 : échec}\right] \\ &\times \mathbb{P}\left[\frac{1}{\lambda_{TPA1}} < \frac{1}{\mu_{TPA2}}\right] \\ &= 1.07 \times 10^{-5}\end{aligned}$$

- Démarrage de TPA 1 :

$$\begin{aligned}\mathbb{P}\left[\text{Démarrage TPA1 : OK}\right] &= \mathbb{P}\left[\text{Démarrage T1 : OK}\right] \times \mathbb{P}\left[\text{Démarrage HT1 : OK}\right] \\ &= \left(1 - 3.9 \times 10^{-2}\right) \times \left(1 - 0.01 \times 5.45 \times 10^{-4}\right) \\ &= 0.96\end{aligned}$$

- Échec de démarrage TPA 2 :

$$\begin{aligned}\mathbb{P}\left[\text{Démarrage TPA2 : échec}\right] &= \mathbb{P}\left[\text{HT1 : échec}\right] + \mathbb{P}\left[\text{HT1 : OK}\right] \times \mathbb{P}\left[\text{ T2 : échec}\right] \\ &= \left(5.45 \times 10^{-4}\right) + \left(1 - 5.45 \times 10^{-4}\right) \times \left(0.01 \times 3.9 \times 10^{-2}\right) \\ &= 9.3 \times 10^{-4}\end{aligned}$$

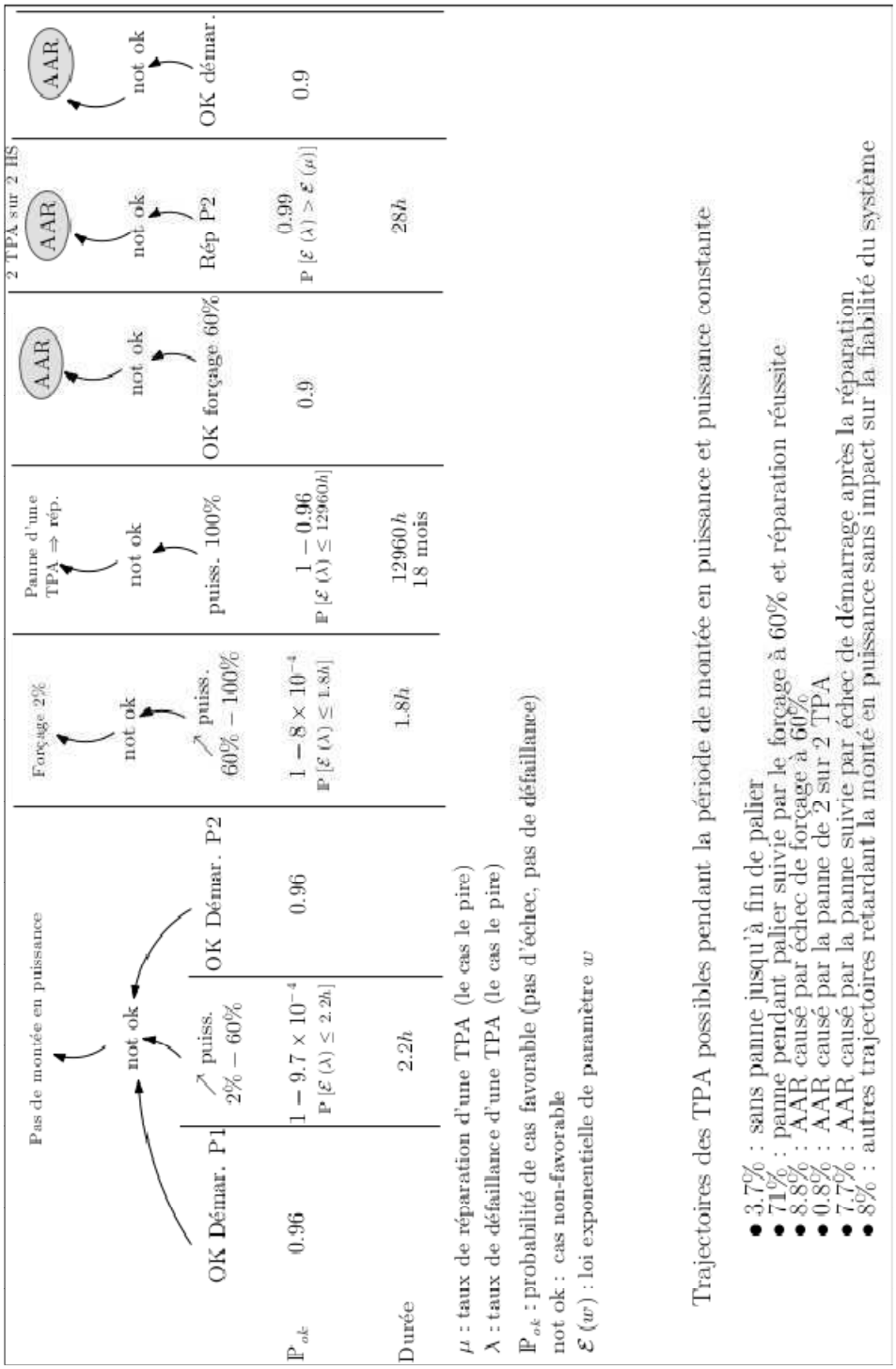
- Durée minimale jusqu'à la défallance de TPA 1 (le cas le pire) :

$$\begin{aligned}\frac{1}{\lambda_{TPA1}} &= \min\left(\frac{1}{\lambda_{HT}^1}, \frac{1}{\lambda_{HT}^2}, \frac{1}{\lambda_T}\right) \\ &= 1/\max\left(0.999 \times 1.46 \times 10^4, 0.001 \times 1.46 \times 10^4, 0.75 \times 5.9 \times 10^4\right) \\ &= \frac{1}{\lambda_T} = 1/4.425 \times 10^{-4} = 2260h\end{aligned}$$

- Probabilité que la durée minimale jusqu'à défaillance de TPA 1 dépasse la durée maximale de la réparation du TPA 2 :

$$\begin{aligned}\mathbb{P}\left[\frac{1}{\lambda_{TPA1}} < \frac{1}{\mu_{TPA2}}\right] &= \mathbb{P}\left[X < 28 \,|\, X \sim \mathcal{E}\left(\lambda_T\right)\right] \\ &= 0.012\end{aligned}$$

Plus généralement, la fréquence d'occurrence d'un sous-ensemble des séquences d'intérêt peut être calculée théoriquement à partir des automates construits.
Le calcul des fréquences des trajectoires possibles des TPA pendant la montée en puissance et pendant le palier de la puissance constante est donné est illustré dans l'encadré ci-dessous en tant qu'exemple. Le choix de domaine (composant, domaine de puissance, etc.) dépend de la question posée.



5.4.4

Exemple 4: Simulation d'histoires

Un exemple d' histoire simulée est présenté sur la figure 5.14. Il s'agit d'une trajectoire normale (sans défaillance, sans descente de puissance forcée), avec la durée du régime stationnaire (pleine puissance) d'un mois. Le niveau d'eau (N_{ge}) et le débit entrant (Q_e) pour cette histoire sont également donnés. Nous observons les grandes fluctuations de N_{ge} et de Q_e en phase de la montée et de la descente en puissance. Ces fluctuations sont dues au système de régulation. En phase stationnaire, le niveau d'eau et le débit restent stables.

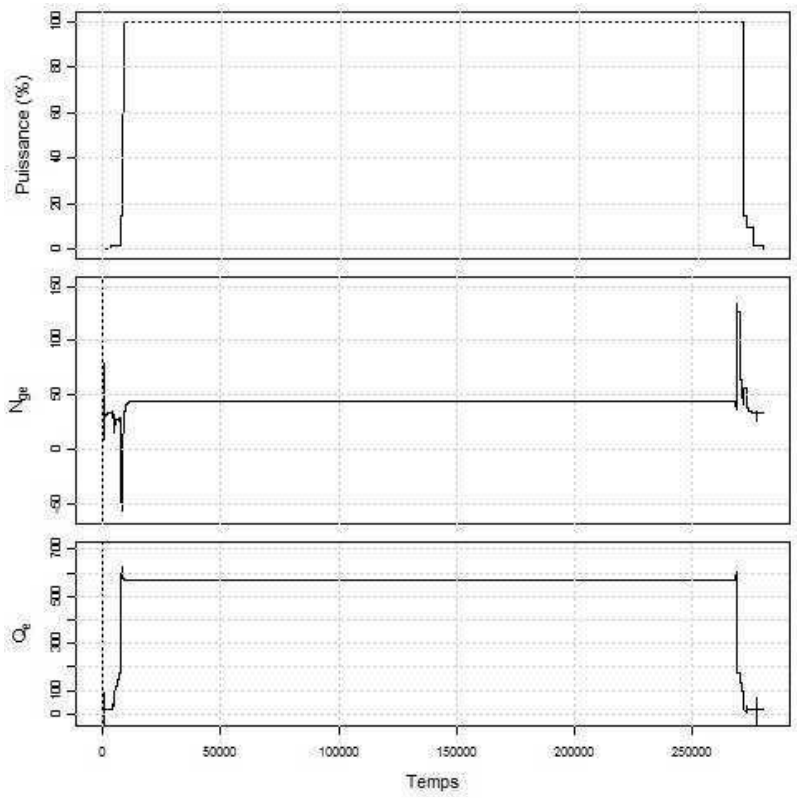


Figure 5.14. Exemple d'une trajectoire normale (sans défaillance, sans descente de puissance forcée) : évolution de la puissance (durée de l'état stationnaire : 1 mois), évolution du niveau d'eau (N_{ge}) et du débit entrant (Q_e).

5.4.5 Exemple 5: Recherche de séquences critiques

Nous nous sommes également intéressés à l'étude détaillée des séquences d'évènements. Les séquences susceptibles de se produire ont été identifiées et leur fréquence d'apparition a été évaluée empiriquement, sur la base de 111 histoires indépendantes simulées. Les résultats sont donnés dans le tableau 5.3. Seule une histoire s'est terminée par un arrêt automatique du réacteur (AAR). Ce résultat est logique, car un AAR est un évènement rare sur l'échelle de la durée de fonctionnement considérée (un mois). Nous constatons que dans la grande majorité des cas, les composants fonctionnent sans panne, à l'exception des pompes TPA. Seulement dans approximativement 20% des cas (en moyenne pour TPA1 et TPA2) leurs trajectoires sont normales, presque la moitié des histoires contiennent la défaillance en fonctionnement de la partie turbine des TPA, entre 10% et 15% (pour TPA1 et TPA2) des histoires contiennent la défaillance en fonctionnement de la partie hors turbine des TPA. Les défaillances en fonctionnement sont réparées avec succès dans la majorité des cas.

Les fréquences d'apparition des défaillances de la partie turbine et de la partie hors turbine des TPA, comparées entre elles, sont cohérentes avec les paramètres des simulations : le taux de défaillance de la partie turbine est quatre fois plus élevé.

Nombre (%) des trajectoires		Type de trajectoire	Description détaillée de trajectoire
Barillet VVP			
110 (99.1%)		Trajectoire normale	Fonctionnement
1 (0.9%)		Fuite	Fonctionnement → fuite → AAR du système
CEX			
109 (98.2%)		Trajectoire normale	Ouverture → fonctionnement → fermeture
2 (1.8%)		Défaillance en fonctionnement	Ouverture → fonctionnement → défaillance d'une CEX sur deux → démarrage de la 3ème CEX → fonctionnement → fermeture
TPA			
TPA 1	TPA 2		
31 (17.9%)	28 (25.2%)	Trajectoire normale	Ouverture → fonctionnement → fermeture
56 (50.5%)	49 (44.2%)	Défaillance en fonctionnement (partie Turbine)	Ouverture → fonctionnement → défaillance partie Turbine → réparation avec succès → redémarrage
12 (10.8%)	17 (15.3%)	Défaillance en fonctionnement (partie Hors Turbine)	Ouverture → fonctionnement → défaillance partie Hors Turbine → réparation avec succès → redémarrage
8 (7.2%)	9 (8.1%)	Echec de réparation partie Turbine	Ouverture → fonctionnement → défaillance partie Turbine → réparation → échec de réparation → réparation avec succès → redémarrage
3 (2.7%)	8 (7.2%)	Echec de réparation partie Hors Turbine	Ouverture → fonctionnement → défaillance partie Hors Turbine → réparation → échec de réparation → réparation avec succès → redémarrage
1 (0.9%)		Echec de démarrage partie Hors Turbine	Ouverture → échec d'ouverture de partie Hors Turbine → réparation → redémarrage
ARE			
Petit débit	Gros débit		
106 (95.5%)	109 (98.2%)	Trajectoire normale	Ouverture → fonctionnement → fermeture
4 (3.6%)		Blocage	Ouverture → fonctionnement → blocage → réparation → redémarrage
1 (0.9%)	2 (1.8%)	Echec d'ouverture	Ouverture → échec d'ouverture → réparation avec succès → redémarrage

Tableau 5.3. Fréquence d'occurrence des séquences d'évènements par composant

5.4.6 Exemple 6: Simulation d'histoires avec accélération

Le modèle global obtenu avec la synchronisation parallèle des modèles des composants a l'avantage d'être complet. Cependant, sa complexité en termes du nombre d'états et de transitions rend les simulations coûteuses en temps. L'optimisation du temps de calcul est nécessaire afin de simuler plus d'histoires avec une durée de fonctionnement plus longue, d'évaluer la fréquence d'apparition des arrêts automatiques du système et d'étudier en détail les séquences qui y mènent.

Le deuxième cas de figure considéré pour les simulations est le suivant. Dans les simulations nous supposons que le palier de pleine puissance constante dure 1 mois et nous adaptons les taux de défaillance et de réparation à cette durée. C'est-à-dire, les taux des défaillances et des réparations donnés initialement pour le palier de la durée de 18 mois sont multipliés par 18, la période d'essais périodique pour les pompes CEX est également modifiée de cette manière.

En terme d'occurrence d'AAR, les résultats suivants sont obtenus (tableau 5.4).

Sous-système	**Pourcentage d'AAR**
VVP	28%
CEX	0
TPA	30%
ARE PD	1%

Tableau 5.4. Résultats des simulations pour la durée du palier de la puissance constante d'un mois et les taux de défaillance/réparation adaptés. Les pourcentages sont calculés sur la base de 200 trajectoires simulées (y compris les trajectoires sans AAR).

L'absence d'arrêt causé par les CEX est vraisemblablement due aux longues durées inter-défaillances données, ainsi que la forte redondance de ces composants. Les forçages à 2% de puissance ne sont pas considérés comme les arrêts du système, ce qui explique le faible pourcentage des AAR causés par les ARE. Finalement, les taux de défaillance des TPA étant les plus élevés, les arrêts fréquents causés par ce composant sont cohérents.

5.4.7 Exemple 7: Modélisation du comportement des capteurs

Les capteurs sont modélisés séparément. Chaque capteur peut être en état de marche, en essai périodique (EP), en panne non-détectée ou en dérive ; avant l'essai périodique correspondant, la dérive peut être positive ou négative, en réparation et en essai périodique avec effet iatrogénique. L'automate élémentaire d'un capteur est représenté sur la figure 5.15 Dans le but de simplification et de réduction du nombre d'état, l'hypothèse de l'impossibilité d'EP par erreur pendant la dérive est faite.

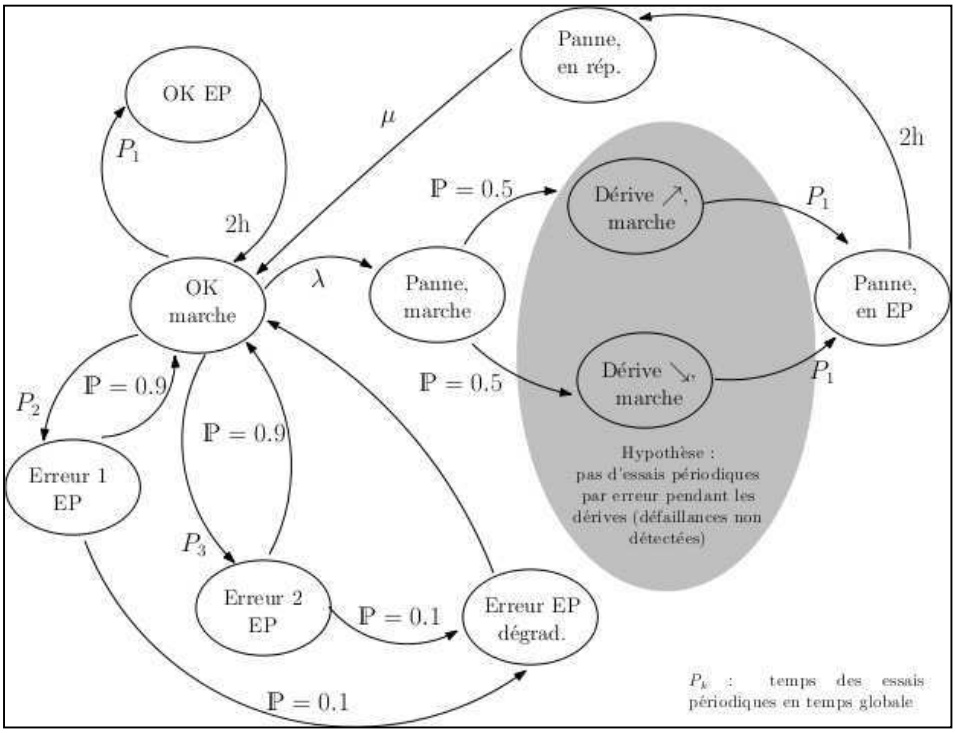


Figure 5.15. Automate élémentaire du fonctionnement d'un capteur.

EP : essai périodique, P_1, P_2, P_3 les dates d'EP pour chaque capteur, Erreur 1 (Erreur 2) : essai périodique (avec effets iatrogéniques). Hypothèse simplificatrice : impossibilité d'un essai périodique par erreur pendant la période de la dérive.

Le schéma général de la modélisation de fonctionnement synchronisé des trois capteurs est présenté sur la figure 5.16. L'algorithme utilisé pour le calcul du niveau d'eau est donné dans l'encadré qui suit. Il prévoit l'arrêt du système lorsque deux capteurs sur 3 sont en panne détectée.

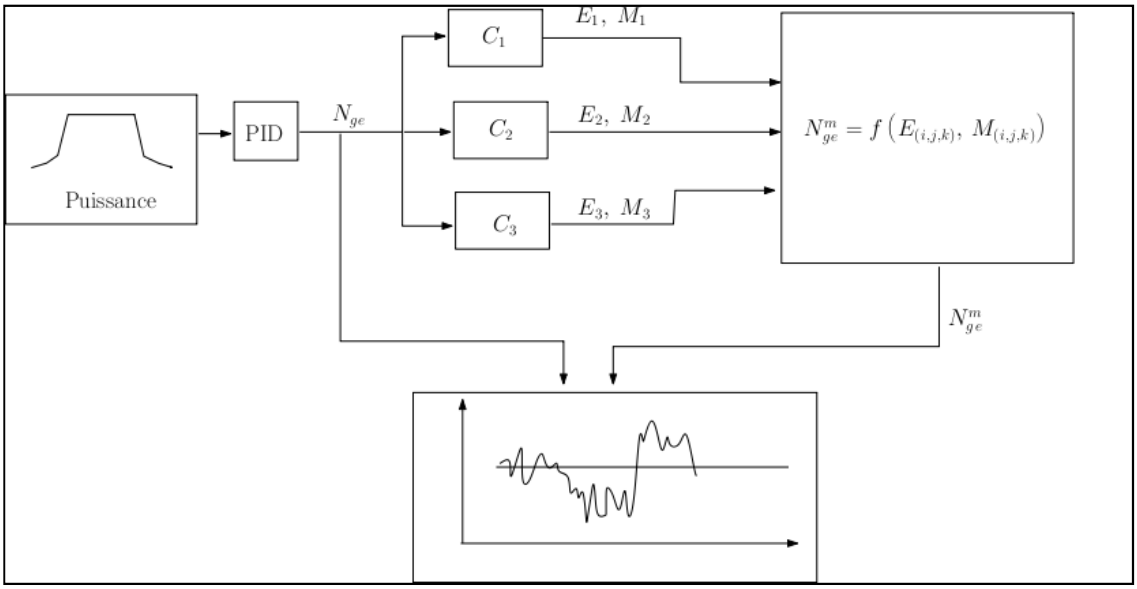


Figure 5.16. Fonctionnement synchronisé des trois capteurs.

L'entrée du système est le niveau de gamme étroite donné par le PID en fonction de la puissance. La sortie de l'automate de chaque capteur est son état (E_k) et sa mesure du niveau d'eau (M_k). La sortie du système est le niveau d'eau calculé à partir de données des trois capteurs (N_{ge}^m) est calculé selon la fonction f.

Algorithme 1: Décision sur la mesure de N_{ge} par les capteurs.

Entrée : Puissance, N_{ge}
Sortie : États des capteurs (E), mesures données par les capteurs (M)

```
for chaque pas de temps do
    M_{i,j,k}                                  /* mesures données par les 3 capteurs */
    E_{(i,j,k)} = {E^m_(·), E^p_(·)} = {marche, arrêt}      /* états des 3 capteurs */
            /* En fonction des états des capteurs leurs mesures sont
    prises ou non en compte */
    if E_i ∈ {E^m_i} & E_j ∈ {E^m_j} & E_k ∈ {E^m_k} then
                                                /* tous les capteurs en marche */
        if min |M_i − mean (M_j, M_k)| < 0.1 × mean (M_j, M_k) then
            N^m_ge = mean (M_i, M_j, M_k)    /* toutes les mesures considérées
            */
        else
            N^m_ge = mean (M_j, M_k)                              /* C_i inhibié */

    if E_i ∈ {E^p_i} & E_j ∈ {E^m_j} & E_k ∈ {E^m_k} then
                                              /* un des capteurs en panne ou EP */
        N^m_ge = mean (M_j, M_k)                          /* pas de comparaison */

    if E_i ∈ {E^p_i} & E_j ∈ {E^p_j} & E_k ∈ {E^m_k} then
                                                 /* 2 sur 3 capteurs en panne */
        STOP                                /* arrêt automatique du système */
```

L'algorithme utilisé pour le calcul du niveau d'eau est donné dans l'encadré ci-dessus. Le schéma général de la modélisation de fonctionnement synchronisé des trois capteurs est présenté sur la figure 5.16.

Afin de réduire les temps de calcul des simulations, le fonctionnement des capteurs est testé sur une durée d'un mois. Le profil de puissance correspond au scénario classique (montée, palier d'un mois de pleine puissance et descente). Tous les paramètres (périodes d'essais, taux de défaillance, durées des EP, etc.) ont été modifiés de la manière suivante :

- Nous considérons que les données sont fournies pour le fonctionnement pendant 18 mois, ce qui suppose *n* EP, *k* défaillances en moyenne, etc. pendant la période du fonctionnement. Les paramètres en question sont modifiés en sorte à garder ces propriétés (même nombre d'EP, de défaillances, etc. pendant la période du fonctionnement).

Le Tableau 5.5 fournit les paramètres donnés initialement et utilisés pour les simulations.

Paramètre	**Donnée 18 mois**	**Donnée 1 mois**
Période d'EP	6 semaines	60 heures
Décalage d'EP des 3 capteurs	2 semaines	20 heures
Taux de défaillance	10-3/h (en moyenne 12 fois en 18 mois)	1,6.10-2
MTTR	2 heures	0,5 heures
Dérive	10%/semaine	10% /10 heures
ρ	Dans 10% de d'EP sur capteur fonctionnel	10 (le taux de défaillance est multiplié par 10 dans 10% des EP faits par erreur sur capteur fonctionnel)

Tableau 5.5. Données utilisées pour simuler le fonctionnement des capteurs.

Le résultat d'une des simulations du fonctionnement des capteurs est donné sur la figure 5.17. Nous constatons qu'avec le temps la fréquence des dérives augmente, ce qui est lié aux effets iatrogéniques des EP par erreur, qui augmentent le taux de défaillance d'un capteur dans 10% de cas.

La figure 5.18 illustre la mesure donnée par les capteurs pendant la période ou 2 ou 3 capteurs dérivent en même temps dans le même sens (dérive négative dans l'exemple). Nous constatons qu'avec les paramètres utilisés pour les simulations, il est possible pendant une période assez longue d'avoir une situation de mesure fondée sur les capteurs défaillants. En effet, lorsque les capteurs dérivent dans le même sens, l'écart entre leurs mesures sera assez petit et leurs mesures seront prises en compte. Afin d'éviter une telle simulation, les fréquences d'EP pourront être augmentées.

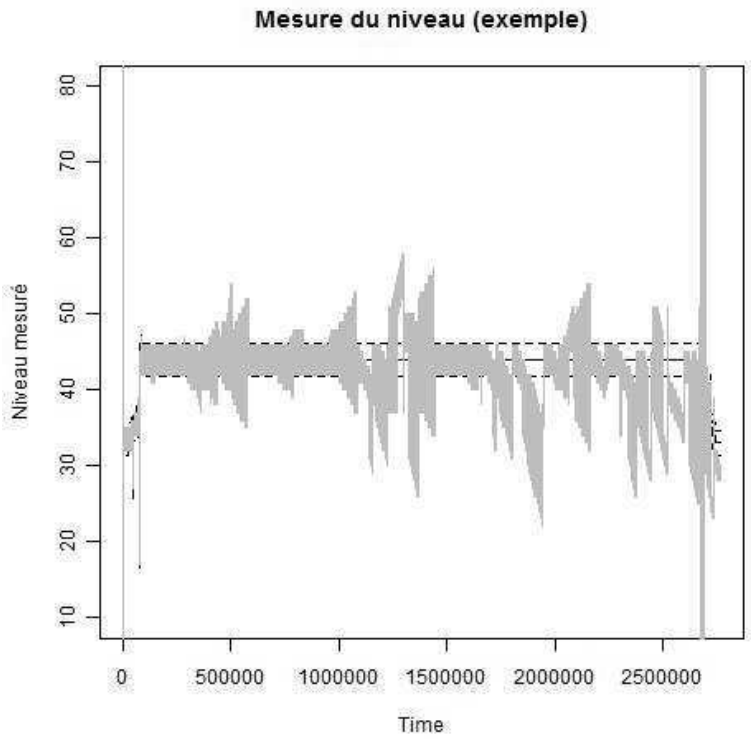


Figure 5.17. La mesure du niveau d'eau N_{ge}^{m} donné par les capteurs durant 1 mois du fonctionnement simulé : un exemple. En noire : le vrai niveau d'eau, en noir pointillé : le vrai niveau d'eau ±5%, en gris, la mesure donnée par les capteurs.

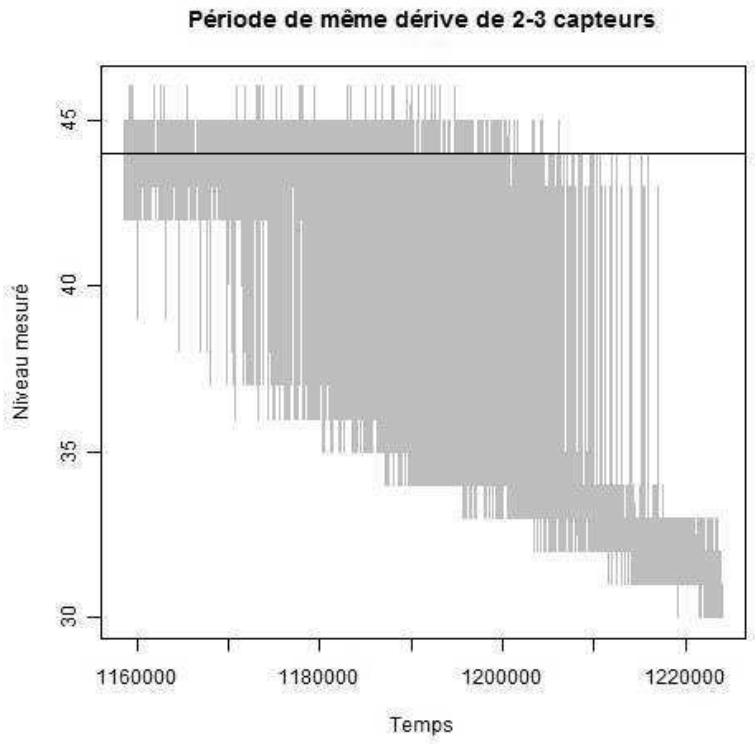


Figure 5.18. La mesure du niveau d'eau N_{ge}^{m} donné par les capteurs lorsque plus d'un capteur dérivent dans le même sens pendant une certaine période sans que la dérive soit détectée.

Finalement, dans nos simulations la mesure du niveau d'eau dépasse les bornes de ±5% du vrai niveau dans 46% de temps de fonctionnement simulé, dont 48% en dérivant vers le bas (ce qui correspond à l'hypothèse qu'une fois sur deux la dérive est positive). Les résultats quantitatifs sont fondés sur 100 histoires simulées.

5.5 Conclusion et perspectives pour l'approche ASH

La modélisation par ASH permet donc d'accéder à l'évaluation de la sûreté de fonctionnement d'un système complexe tel que celui du cas test considéré. Outre l'accès aux probabilités des états dangereux elle permet d'analyser exhaustivement l'ensemble des séquences qui y mènent et d'évaluer leurs probabilités respectives. Dans l'état actuel des outils utilisés, le travail de modélisation reste très conséquent et la dimension du modèle est importante. Cependant, cette expansion de la taille du modèle peut être relativisée par plusieurs considérations : les outils informatiques modernes s'en jouent de plus en plus facilement et de nombreuses approches de simplification ont vu le jour pour simplifier les AEF (par les diagrammes de décision binaires, voir par exemple [HAM 05, POC 08]). Dans la perspective du développement de quelques modules à insérer dans la plateforme Scilab-Scicos, le travail de modélisation pourra être substantiellement simplifié. De plus, lorsque les outils de composition d'ASH seront développés formellement, à l'instar de ceux existant pour les AEF, seuls les automates embryons seront à saisir, le reste se fera automatiquement sans nécessiter la visualisation graphique de l'automate complet. L'extraction des séquences critiques de ce modèle reste également à automatiser avec un outil de recherche de chemin dans le graphe sous jacent à l'ASH.

La simulation de Monte Carlo étant le moyen de l'évaluation probabiliste, tout développement visant à l'accélérer est bien entendu souhaitable. Le caractère ouvert de la plateforme Scicos Scilab devrait permettre aussi bien l'accélération de la simulation numérique de la dynamique continue (méthodes à pas variable…) que l'efficience de la méthode de Monte Carlo (distribution sur calculateur parallèle…). La recherche de critères de simplification du modèle est également une voie intéressante pour y parvenir.

6 Simulation et Processus Markoviens Déterministes par Morceaux

6.1 Principes et références

Dans le domaine de la sûreté de fonctionnement, la modélisation est une étape cruciale pour analyser la sûreté de fonctionnement d'un procédé. Lorsque les enjeux de disponibilité ou de sûreté le justifient, il est nécessaire de prendre en compte, de manière effective et réaliste, les divers types d'interactions pouvant exister entre les différentes grandeurs physiques du système, et son comportement global. Sur le plan de la fiabilité dynamique, une tendance qui semble émerger dans la littérature est une approche de type multi modèle. Le fonctionnement du processus physique étudié peut être alors décrit par différents régimes depuis le nominal jusqu'à la panne complète, en passant par divers comportements dysfonctionnels. La configuration des séquences opératoires ou accidentelles résulte essentiellement de l'occurrence de deux types d'évènements ponctuels :

- le premier type d'évènements est directement lié à une évolution déterministe des grandeurs physiques du système, comme par exemple le franchissement d'un seuil ;
- le second type d'évènements est de nature stochastique et va correspondre à des défaillances de certains composants ou à des sollicitations externes.

Dans ce contexte, les grandeurs physiques continues du système (par exemple la pression dans un actionneur pneumatique, la température d'un composant électronique, etc.) définissent des variables d'état et l'évolution de ces grandeurs est régie par les lois de la physique comme par exemple les lois de la mécanique, de la thermodynamique ou de l'électromagnétisme.

Le travail présenté s'inscrit dans la continuité d'une série de travaux déjà réalisés au sein de l'équipe INRIA-CQFD. Ils ont pour objectif d'illustrer la mise en œuvre d'une méthode alliant la puissance de modélisation des processus markoviens déterministes par morceaux (PMDPM) et l'efficacité calculatoire de la simulation de Monte Carlo, pour traiter certains problèmes relevant du champ de la fiabilité dynamique. La raison qui nous incite à choisir la modélisation PMDPM est double, d'abord, elle donne un cadre de modélisation à la fois générale et précise du problème. En suite cette modélisation nous offre la perspective dans le futur de faire du contrôle optimal : arrêt optimal, maintenance préventive [SAP 2011], etc.

Nous avons dans le passé modélisé et simulé des systèmes de taille « académique » [ZHA 2009] et « industrielle » [ZHA 2008], les implémentations ont été réalisées en C++ ou Matlab. Mais pour modéliser ce système de régulation du niveau d'eau, nous avons choisi les logiciels Simulink et Stateflow de Mathwork, pour trois raisons :

1) Plusieurs variables physiques (Nge, Ngl, Qe, Qv, etc) doivent être calculées à chaque pas de temps. Ces variables évoluent suivant des équations différentielles non linéaires. Un outil comme Simulink se prête parfaitement à ce type de problème. De plus des contrôleurs du type PID et MPC sont déjà implémentés dans Simulink sous forme de bloc système.

2) Le nombre de composants qu'on doit modéliser ainsi que leurs comportements spécifiques rendent le système très complexe. Chaque composant peut se trouver dans de nombreux états, nominaux ou dégradés. Le nombre total des combinaisons possibles pour l'ensemble des composants est gigantesque. Un langage de programmation comme C++ (ou Matlab) peut traiter ce problème mais il sera alors très difficile de faire évoluer le code. Ajouter ou supprimer un composant ou changer la configuration du système serait alors très fastidieux.

3) Stateflow étend les possibilités de Simulink avec un environnement de conception pour le développement de machines à états et de diagrammes de flux. Il fournit les éléments du langage nécessaires à la description d'une logique complexe sous une forme naturelle, lisible et compréhensible. Il est orienté objet, ce qui permet de modéliser les composants VVP, CEX, TPA, ARE séparément, et traiter la redondance avec un simple copier-coller.

6.1.1 Qu'est-ce qu'un processus markovien déterministe par morceaux ?

Les processus markoviens déterministes par morceaux (PMDPM ou PDMP en anglais) offrent un cadre de modélisation très général pour traiter des problèmes de sûreté de fonctionnement attachés à des systèmes physiques.

Soit M l'ensemble fini des régimes possibles du système.

Pour tout m dans M, soit E_m un ouvert de R^d.

Un processus markovien déterministe par morceaux est défini à partir de ses trois caractéristiques locales (Φ, λ, Q) où :

- le flot $\Phi : M\times R^d\times R\rightarrow R^d$ est continu et pour tous $s,t \geq 0$, $\Phi(\bullet,t + s)= \Phi(\Phi(\bullet,s),t)$.
  Il décrit la trajectoire déterministe du processus entre les sauts.
- Pour tout (m,x) dans $M\times E_m$, on définit le temps d'atteinte du bord du domaine ;
- :

$$t^*(m,x)=\inf \{ t>0 : \Phi(m,x,t) \in \partial E_m\}$$

- l'intensité de saut λ caractérise la fréquence des sauts. Pour tout (m,x) dans $M\times E_m$, et $t \leq t^*(m,x)$, on pose :

$$\Lambda(m,x,t) = \int_0^t \lambda(\phi(m,x,s))ds$$

- le noyau markovien Q représente la mesure de transition du processus et permet de sélectionner la nouvelle position après chaque saut.

La trajectoire $X_t=(m_t, x_t)$ du processus peut alors être définie de façon itérative. On part d'un point initial $X_0=(k_0, y_0)$ avec $k_0\in M$ et $y_0\in E_{k0}$. Le premier instant de saut T_1 est déterminé par :

$$P_{(k0,y0)}(T_1 > t) = \begin{cases} e^{-\Lambda(k0,y0,t)}, & t < t^*(k_0, y_0) \\ 0, & t \geq t^*(k_0, y_0) \end{cases}$$

Sur l'intervalle de temps $[0, T_1[$, le processus suit alors la trajectoire déterministe $m_t=k_0$ et $x_t=(\Phi(k_0, y_0,t)$. A l'instant aléatoire T_1, le processus subit un saut. Il change donc de régime et il est alors réinitialisé en X_{T1}, variable aléatoire qui suit la loi donnée par $Q_{k0}(\Phi(k_0, y_0, T_1),\bullet)$. On tire alors de façon analogue un nouveau temps de saut $T_2 - T_1$, et sur l'intervalle $[T_1,T_2[$le processus suit la trajectoire $m_t=k_1$ et $x_t=(\Phi(k_1, y_1,t - T_1)$. On construit ainsi de façon itérative le PMDPM.

La particularité du système GV est d'être un système régulé. Le flot Φ est la solution d'une équation différentielle contrôlée par un contrôleur PID. Il n'admet pas de solution analytique et sera calculé à chaque pas de temps par Simulink.

6.2 Modélisation du cas test

Nous considérons le scenario 1, représenté par la figure 6.1. Après une montée linéaire par morceaux d'une durée de 24 heures, le système atteint son régime stationnaire, 100 %Pn et il y reste pendant 18 mois, suivis par une descente de 24 heures. L'objectif est de simuler le comportement du système, soumis à des pannes aléatoires ou des erreurs de commande. La simulation est arrêtée dès qu'un arrêt automatique du réacteur (AAR) est constaté.

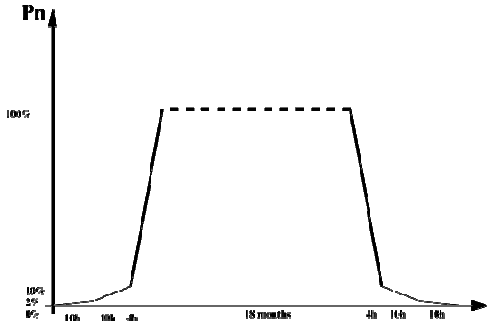


Figure 6.1. Scénario n°1

Le schéma global du simulateur est présenté par la figure 6.2. L'élément nommé « Scenario» permet de générer une rampe de monteé ou descente de la variable *Pn* qui est une donnée d'entrée du système. Cette rampe est saturée entre [0,100] par le bloc « Saturation ». On s'intéresse aux quatre signaux de sortie : Pn, Nge (niveau d'eau et consigne), Ngl (niveau eau large) et AAR (signal qui arrête la simulation).

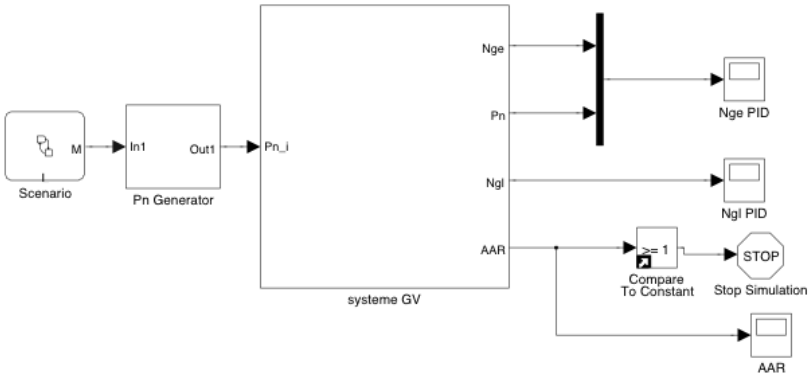


Figure 6.2: Schéma global du simulateur

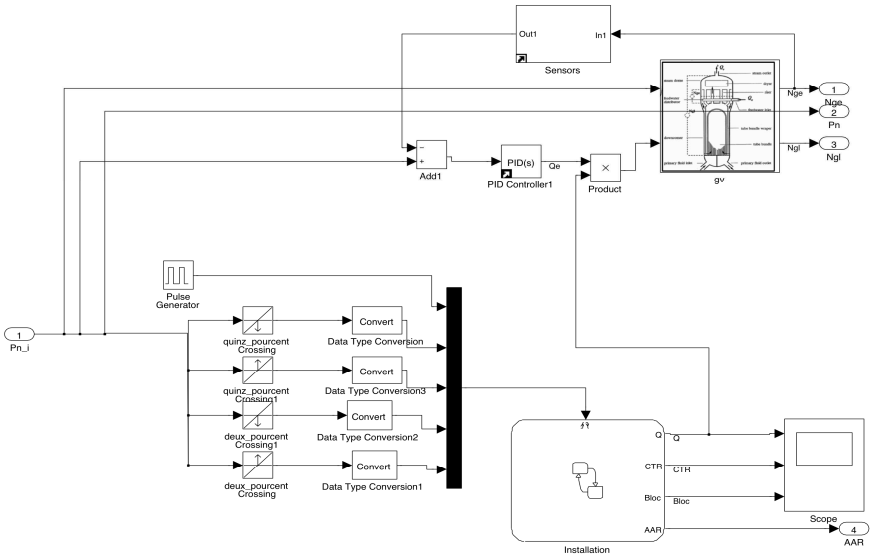


Figure 6.3. Schéma global du sous système GV

Le générateur GV est entièrement modélisé par le Sous Bloc « System GV », figure 6.3. On y trouve :

- Un Bloc Stateflow « Installation », qui regroupe les systèmes élémentaires VVP, les trois CEX, les deux TPA et ARE. Nous nous présentons en 6.3.1.les modèles de VVP et de CEX. Ce bloc est activé à chaque pas de temps, et également à chaque fois que la puissance Pn franchit les seuils 2 %, 15 % ;
- Le générateur GV, modélisé par le sous système « gv », avec deux entrées (Qv, Qe) et deux sorties (Nge, Ngl). Ce système obéit à un système d'équations différentielles non linéaires puisque ses coefficients dépendent de Qv. Voir [KOT 00] pour les descriptions détaillées de ce système ;
- Le contrôleur PID, qui a pour entrée la différence entre le consigne Pn et Nge, et pour sortie la variable Qe, le débit d'eau injecté dans le GV. La variable Qv représente les perturbations du système élémentaire ARE.

Un intérêt principal de la modélisation par Simulink et Stateflow est qu'elle se fait sous forme d'un graphe interactif, ce qui facilite la compréhension du modèle : si le système fonctionne en mode nominal, (par exemple montée, descente, régime puissance 100 %) et qu'aucun composant n'est en panne, le niveau d'eau est régulé par le contrôleur PID ; si un composant tombe en panne, il peut provoquer soit un AAR, soit une panne mineure. Dans le premier cas on arrête la simulation, dans le deuxième cas la simulation continue, on procède aux réparations, une descente en rampe et une remontée seront programmées le cas échéant.

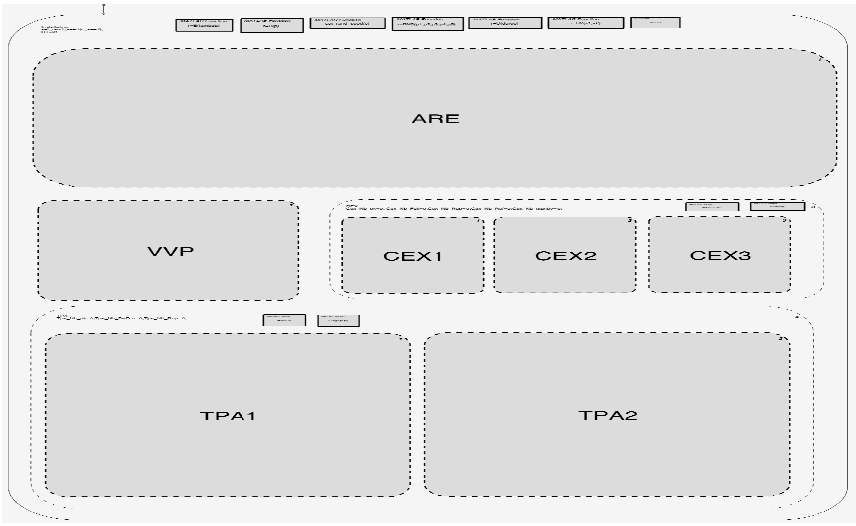


Figure 6.4. Bloc Stateflow « Installation »

8.5.4. Modélisation du VVP

Ce composant possède trois états (OK, Fuite, Rupture). La durée de séjour de chaque état suit une loi exponentielle. Lorsque ce composant est activé, il est par défaut dans l'état OK. Un tirage *x* de loi exponentielle est effectué (paramètre 2,17.10-5/h), on tire aussi une variable p de Bernoulli (B(0,89)). Lorsque la durée de séjour dans cet état dépasse x, la transition after(x,sec) est réalisée. Le composant passe à l'état Fuite si p=1 et à l'état Rupture si p=0. On envoie dans ce cas un signal AAR qui arrête la simulation. Des numéros de code du simulateurpermettent d'enregistrer le numéro de composant en panne et le type de panne.

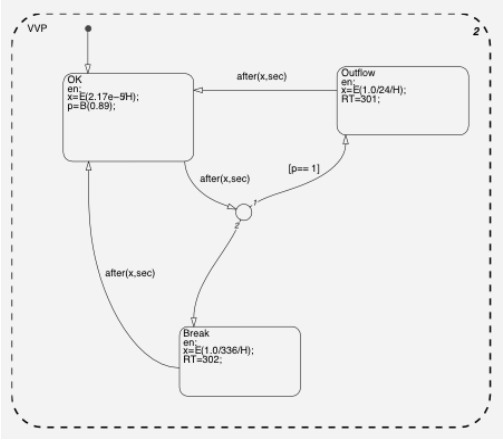


Figure 6.5.. Modélisation du VVP

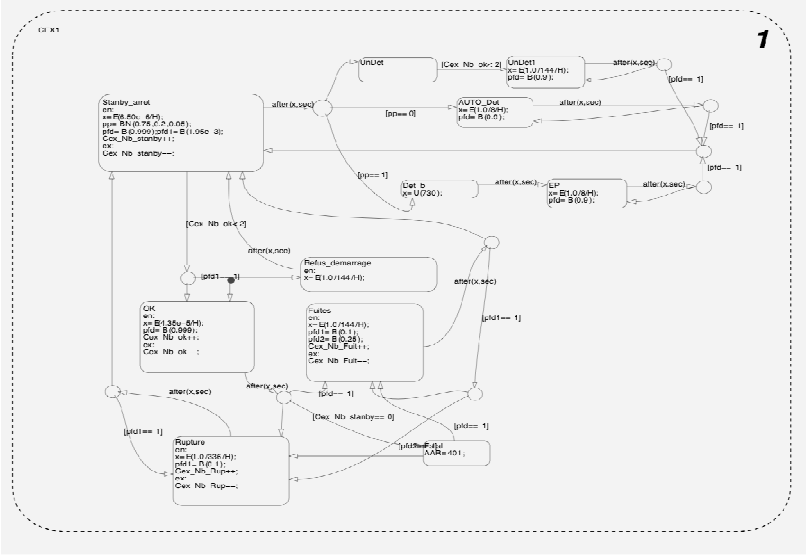


Figure 6.6. Modélisation d'une pompe CEX

6.2.1 Modélisation des CEX

La modélisation des CEX est similaire à celle du VVP, mais elle est beaucoup plus complexe à cause du fonctionnement en redondance. On remarque que les deux premiers CEX sont identiques (copier-coller), le troisième CEX est différent par son état initial. En effet, à l'état initial, deux CEX sont en fonctionnement, le troisième est en arrêt (*stanby)*. La figure 6.6 montre le détail d'un des trois CEX.

6.3 Résultats qualitatifs et quantitatifs

L'approche par simulation est particulièrment efficace pour générer des histoires. La durée totale du scenario (cas n°1 présenté plus haut) est de 18 mois. On distingue deux types de régimes : transitoire et stationnaire. Lorsque le système se trouve dans le régime transitoire, le niveau d'eau *Nge* et la puissance *Pn* varient rapidement. Pour suivre cette commande, on doit choisir un pas de temps suffisamment petit (0.6 seconde) pour que le contrôleur PID puisse fonctionner. Dans le régime stationnaire, toutes les variables physiques restent constantes, seules les pannes des composants modifient l'état du système. Mais comme le système est très fiable, la durée nominale est souvent très longue et un pas de temps très fin n'est pas pertinent car il ralentit énormément le simulateur. Nous proposons donc une technique particulière pour résoudre ce problème de pas de temps non homogène. Pour cela, deux modèles Simulink distincts ont été créés, le premier avec le bloc « PID », et le deuxième sans bloc « PID ». Ceci permet de choisir deux pas de discrétisation différents. Pendant le régime transitoire, on utilise un pas de 0.6 seconde, et pendant la période stationnaire, un pas de 60 minutes est suffisant pour simuler les pannes des composants. Un script Matlab pilote la simulation.

Pour illustrer les résultats et valider le modèle, nous avons pris une histoire sans panne, avec un régime de pleine puissance sur 10 jours (au lieu de 18 mois, pour raison illustrative). La figure 6.7 montre que le contrôleur PID a bien joué son rôle de régulateur, le niveau d'eau *Nge* coïncide avec la consigne *Pn*.

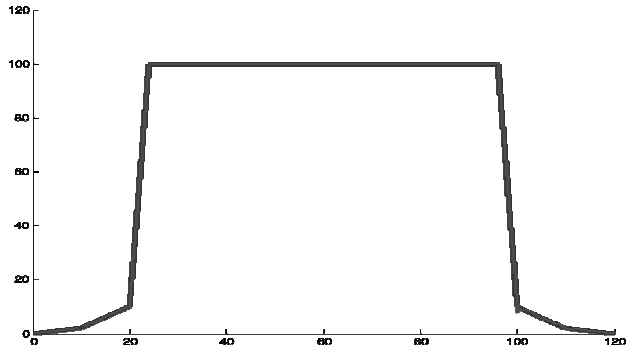


Figure 6.7. Comparaison entre Nge et Pn, en mode nominal

Sur nombre total de 4 000 histoires simulées, 2190 AAR ont été observés, soit une probabilité de 54.75 % : le système a environ une chance sur deux de subir un AAR, pour un horizon de 18 mois. Le tableau 6.1 récapitule le nombre d'AAR provoqués par chaque composant du système. On donne aussi leur pourcentage d'occurrence parmi les 2190 AAR.

Sous système	**Nombre d'AAR provoqués**	**Pourcentage**
VVP	792	36 %
ARE	1301	59 %
CEX	50	2,28 %
TPA	47	2,1 %
TOTAL AAR	2190	100 %

Tableau 6.1. *Nombre d'AAR constatés sur 4000 histoires*

La figure 6.8 illustre la probabilité cumulée des AAR au cours du temps.

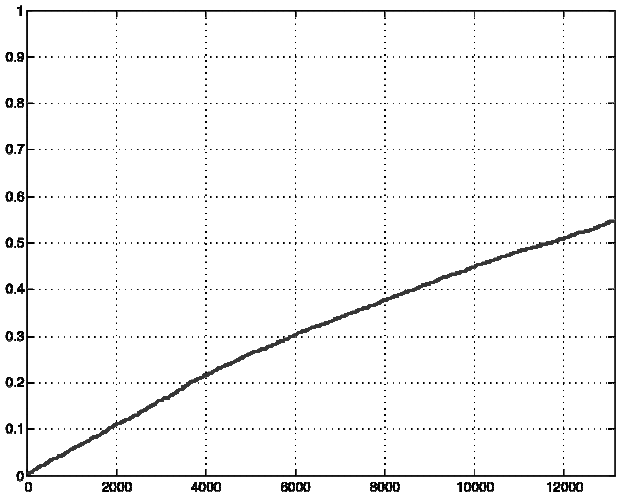


Figure 6.8. Probabilité cumulée des AAR

On n'a constaté aucun AAR provoqué par la vanne ARE petit débit. Ceci peut s'expliquer par le fait que la durée de séjour dans le régime transitoire est trop faible (48 heures) par rapport à la durée totale (18 mois), cette panne devient un évènement rare. On remarque également que beaucoup d'AAR sont causés par le barillet VVP (36 %). Son taux de défaillance (2,17e-5) est comparable à ceux des CEX (4,35e-5) et TPA (5,9e-4), mais ces derniers composants sont en redondance, ce qui permet de minimiser les AAR.

6.4 Conclusion et perspectives pour l'approche par PMDPM et simulation

La modélisation par PMDPM s'applique très bien à ce problème de fiabilité dynamique et l'approche Simulink associé à Stateflow permet de construire un simulateur interactif. Elle offre donc des perspectives intéressantes à plusieurs points de vue.

- Programmation graphique. Le code source ressemble à un diagramme de fiabilité. En mode débuggeur, les utilisateurs peuvent visualiser pas par pas les états et les transitions ;
- Maintenance évolutive du simulateur. Les composants VVP, CEX, TPA, ARE ont été modélisés d'abord séparément (en supposant les autres composants 100 % fiables) et ensuite rassemblés par des simples copier-coller. On peut donc ajouter aisément dans le futur d'autres composants. De même, on peut traiter facilement le problème de la redondance des composants en pré-construisant une librairie de composants ;
- Limitation du nombre de composants. Il n'y a pas de problème d'explosion combinatoire dans cette approche. En effet, les machines à états de Stateflow sont orientées composant, c'est-à-dire qu'à chaque pas de temps, et pour chaque composant, le simulateur calcule l'état du composant. On peut alors considérer l'état du système comme un vecteur, dont la dimension est égale au nombre de composants.

L'inconvénient principal de cette approche est le temps d'exécution. Pour le cas test que nous avons traité, une histoire est simulée en environ 30 secondes (sur un MAC portable), il faut donc 8 heures pour 1000 itérations de Monte Carlo. L'expérience [ZHA 2008] nous montre qu'un simulateur C++ dédié à un problème de cette taille peut sans doute s'exécuter dix fois voire cent fois plus rapidement, mais au prix d'un investissement lourd en programmation et d'un code généré difficile à faire évoluer. Pour accélérer la simulation, deux solutions existent : le calcul parallèle et la génération automatique d'un code C. Cela offre des perspectives intéressantes pour de futurs développements.

Pour accélérer la simulation, nous utilisons la boîte à outils "Parallel Computing" qui s'avere très efficace pour ce type de problème car les tirages de Monte Carlo sont indépendants. Nous avons reussi à diviser par 10 le temps de simulation sur un ordinateur équipé de 12 coeurs. Cela offre des perspectives intéressantes pour de futurs développements.

D'autres pistes peuvent également être explorées. L'équipe INRIA-CQFD propose des algorithmes numériques de contrôle optimal : arrêt optimal, contrôle impulsionnel [SDG2010, SAP2011, SD2011]. Dans toutes ces méthodes, le simulateur Monte Carlo est un support indispensable.

7 Modélisation par Réseaux de Petri Stochastiques

7.1 Principes et références

Plusieurs classes de réseaux de Petri (RdP) ont été élaborées pour répondre à la modélisation de problèmes spécifiques [DAV 94, MUR 89]. A l'origine, les RdP étaient utilisés dans le cadre de processus déterministes, notamment ceux rencontrés dans l'industrie et ses nombreux problèmes d'automatisation, de gestion de production et de flux. Ces dernières décennies, les évolutions technologiques sont telles que ces mêmes processus deviennent de plus en plus complexes, permettant des gains de productivité et de performance, mais souvent au détriment d'une maintenance couteuse. L'objectif alors est d'élaborer des politiques de maintenance qui tiennent compte de la sûreté de fonctionnement du système et de ses composants ceci afin de déclencher à temps toute action de maintenance ; c'est-à-dire ni trop tôt et ni trop tard. Parmi les méthodes possibles permettant de combiner un comportement déterministe d'un système et un comportement stochastique dû à des pannes éventuelles et/ou à des modes de dégradation ; la classe des RdP stochastiques permet la mise en place d'un cadre de modélisation hiérarchisée depuis un niveau élémentaire (le composant) jusqu'au niveau du système [ZIL 08].

7.2 Qu'est-ce qu'un Réseau de Petri stochastique (RdPS) ?

Un réseau de Petri Stochastique (RdPS) est un automate défini par le classique 5-tuple (P, T, F, W, M_0) dans lequel :

$P = \{p1, p2, ..., pm\}$ est un ensemble fini de places ;
$T = \{t1, t2, ..., tn\}$ est un ensemble fini de transitions ;
$F = (P \times T) \cup (T \times P)$ est un ensemble fini d'arcs reliant les places via les transitions ;
$W : F = \{1, 2, 3...\}$ est une fonction de pondération de chaque arc ;
$M_0 : P \rightarrow \{0, 1, 2, 3...\}$ est le marquage initial du réseau c'est-à-dire le nombre de jetons dans chaque place.

Le tir d'une transition est, ans la cas de RdP Stochastiques, conditionnée par une loi de probabilité (exponentielle, Weibull, etc.), image de la panne d'un composant, de sa durée de réparation, de la disponibilité d'une pièce de rechange. La liste des lois est non exhaustive. Il est à noter que le tir d'une transition déterministe est toujours faisable dans le cadre des RdPS (par la loi de Dirac). Pour un système complexe comme le cas d'étude ApproDyn, les composants doivent interagir de manière conjointe par l'échange de messages [DUT 97], évalués lors des tirs des différentes transitions. Ce flot de messages qui assure la cohésion, la synchronisation des RdPS peut aussi porter une information quantitative tel qu'un niveau d'eau dans le générateur de vapeur à l'instar des réseaux de Petri colorés où là l'information est portée par le jeton lui-même.

7.2.1 <u>Exemple</u>

A titre illustratif et afin de mieux saisir le principe des RdPS, on considère l'exemple simple d'un système mono-composant. Celui-ci est soumis à des maintenances préventives de durée fixe égale à 2 heures et de période fixe de 1 000 heures. Ces actions de maintenance rendent le système indisponible. Le taux de défaillance du composant est supposé suivre une loi exponentielle de paramètre $\lambda = 10^{-5}\ h^{-1}$. Le RdPS associé à cet exemple est décrit à la figure 7.1..

Deux RdPS sont utilisés pour modéliser ce système. Le premier pour le fonctionnement/dysfonctionnement du composant et le second pour sa maintenance. L'ensemble étant synchronisé uniquement par un message booléen symbolisant le passage ou non du système en maintenance.

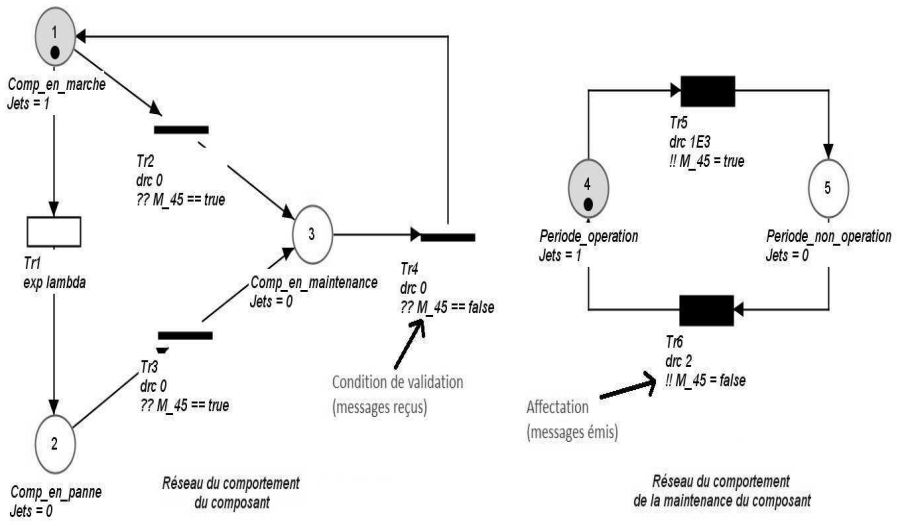


Figure 7.1. Réseau de Petri Stochastique : exemple introductif

Pour des grands systèmes, l'obtention de solutions analytiques des principales mesures de la sûreté de fonctionnement peut devenir très vite compliquée. C'est la raison pour laquelle les RdPS sont animés à l'aide de simulations de Monte Carlo. Pour mémoire, cette méthode consiste à simuler un nombre important d'histoires indépendantes décrivant chacune le comportement dans le temps du système et ceci pour un temps de mission fixé. Pour chaque histoire, on identifie les dates d'occurrence des différents évènements possibles comme l'apparition d'un mode de défaillance en effectuant un tirage aléatoire. Chaque histoire reproduit ainsi une des évolutions possibles du système, c'est à dire la séquence d'évènements décrivant son comportement et les actions de maintenance effectuées. Au cours de la simulation d'une histoire, on peut comptabiliser le nombre d'occurrences des différents évènements et le temps passé dans les différents états possibles à l'aide de compteurs dédiés. A la fin de la simulation de toutes les histoires, ces compteurs fournissent l'estimation statistique des quantités d'intérêt en établissant la moyenne sur le nombre total de simulations effectuées.

7.3 Modélisation du cas test

Afin de décrire complètement le système étudié, trois types de variables sont utilisées :

1) *les variables du processus* qui décrivent les variables physiques impliquées dans la dynamique du système,

2) *les variables d'information*, qui décrivent les données ou informations calculées, stockées et échangées entre les composants du système.

3) *les variables d'état des composants*, qui décrivent la structure (configuration) du système selon les modes de fonctionnement/dysfonctionnement de ses composants.

Le modèle général du système avec sa boucle de contrôle PID est illustré à la figure 7.2. . Le débit d'eau souhaité Q_{ec} est calculé à l'aide d'un correcteur PID sous sa forme discrétisée en utilisant la valeur de consigne de niveau d'eau *SetNge* et la valeur mesurée de niveau d'eau *Ngem*. Selon le point de fonctionnement (c'est à dire la valeur de la puissance *P*), la logique de commande de la vanne réglante ARE bascule entre deux vannes petit débit et gros débit. Le niveau d'eau *Nge* est donné par un système d'équations provenant d'une représentation dans un espace d'états non détaillée ici. Dans ce chapitre, nous supposons que le capteur de niveau d'eau ne présente aucun dysfonctionnement,

aucune dégradation, aucune déviation, telle que la valeur mesurée du niveau d'eau *Ngem* soit toujours égale à *Nge*. Pour chaque intervalle de temps [t,t + Δt), toutes les variables sont mises à jour à l'aide de réseaux de Petri dédiés. Cette mise à jour se fait suivant un ordre spécifique respectant la dynamique de fonctionnement du système. Cet ordonnancement est rendu possible par l'affectation d'une priorité de tir à chaque transition.

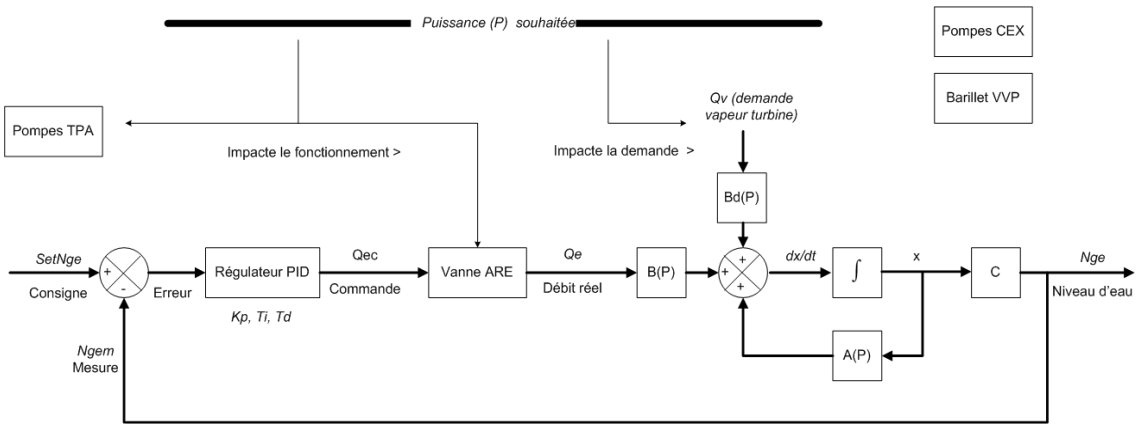


Figure 7.2. Vue synthétique du modèle

7.4 Variables et paramètres du processus

Les variables du processus correspondent aux variables de l'espace d'état (non détaillé ici) ainsi qu'au débit d'eau entrant *Qe*, au débit de vapeur *Qv*, au niveau d'eau *Nge*. Les paramètres du processus *Tm*, *Tint*, *Tn*, *Fg*, *Th*, τ correspondent aux différentes constantes de temps du système et doivent être mis à jour en fonction du point de fonctionnement (la puissance *P*) désiré. Comme première approche, cette mise à jour est obtenue à l'aide d'une simple interpolation linéaire basée sur des points caractéristiques propres au générateur de vapeur étudié. Un descriptif complet sur ces points caractéristiques ainsi que sur la représentation dans l'espace d'états est donné dans [KOT 00].

8.11.3.2 Variables d'état des composants

L'état de chaque composant est représenté à l'aide d'une variable entière. Le tableau 7.1. résume l'ensemble des variables utilisées pour chaque composant et chaque mode de fonctionnement.

Composant	Variable d'état	Valeur	Description
Barillet VVP	Barillet_VVP_Etat	=0 =1 =2	En marche OK En panne mode I (fuite) En panne mode II (rupture)
CEX_i=1,2,3	CEX_i_état	=0 =1 =2 =3 =4 =5 =6	En marche OK En panne mode I (défaillance en fonctionnement) En panne mode II (rupture ou fuite grave) En attente OK En attente (défaillance IIIa détectée par autotest) En attente (défaillance IIIb par les EP) Refus de démarrage (défaillance IIIc non détctable)
TPA_i=1,2	TPA_i_Etat	=0 =1 =2	En marche OK (partie hors turbine et partie turbine en marche OK) En attente OK (partie hors turbine et partie turbine en attente OK) Non OK (autre cas)
Hors_turbine_TPA_i=1,2	Hors_turbine_TPA_i_ Etat	=0 =1 =2 =3 =4	En marche OK En panne mode I (défaillance en fonctionnement) En panne mode II (rupture ou fuite grave) En attente OK Refus de démarrage
Turbine_TPA_i=1,2	Turbine_TPA_i_Etat	=0 =1 =2 =3 =4 =5 =6	En marche OK En panne mode I (défaillance en fonctionnement tps réparation court) En panne mode II (défaillance en fonctionnement tps réparation longt) En attente OK En attente (défaillance IIIa détectée par autotest) En attente (défaillance IIIb par les EP) Refus de démarrage (défaillance IIIc non détctable)
ARE_petit_débit	ARE_pD_Etat	=0 =1 =2 =3 =41 =42 =43 =5	En marche OK En panne mode I (rupture vanne VL ou fuite grave) En panne mode II (fuite interne vanne VL) En panne mode III (fuite externe VL) En panne mode IV (manœuvre intempestive vanne VL type I (fermée) En panne mode IV (manœuvre intempestive vanne VL type II (ouverte) En panne mode IV (manœuvre intempestive vanne VL type III En panne mode V (blocage vanne VL)

Tableau 7.1 Variables d'état des composants

7.4.1 Variables d'informations

La puissance *P*est une information partagée par les composants du système. C'est elle qui dicte leur conduite, leur mode opératoire. Suivant la valeur prise par cette variable, des ordres de démarrage/d'arrêt des TPA sont engendrés de même que des ordres d'ouverture/fermeture de vannes petit/gros débit. Pour finir, la consigne de niveau d'eau *setNge* dépend elle-aussi de *P*suivant la relation :

$$setNge = \begin{Bmatrix} 0.55\,P + 33\ si\ P \leq 20 \\ sinon \end{Bmatrix} = \begin{Bmatrix} 0.55\,P + 33\ si\ P \leq 20 \\ sinon \end{Bmatrix}$$

7.5 L'outil MOCA-RP

L'outil utilisé pour la modélisation à l'aide des RdPS est MOCA-RP (acronyme de « MOnte CArlo basé sur les Réseaux de Petri »[16]). Ce logiciel est destiné à la simulation du comportement de systèmes dynamiques complexes permettant d'obtenir – après traitement statistique – des résultats concernant leur fiabilité, disponibilité, productivité ainsi que tout autre paramètre probabiliste. MOCA-RP permet de décomposer un cas d'étude en sous-problèmes de manière hiérarchique ainsi que la création de bibliothèques de composants réutilisables. Cet outil semble donc parfaitement convenir au système du génération de vapeur étudié. A titre indicatif, le RdPS du barillet VVP est donné en figure 7.3.

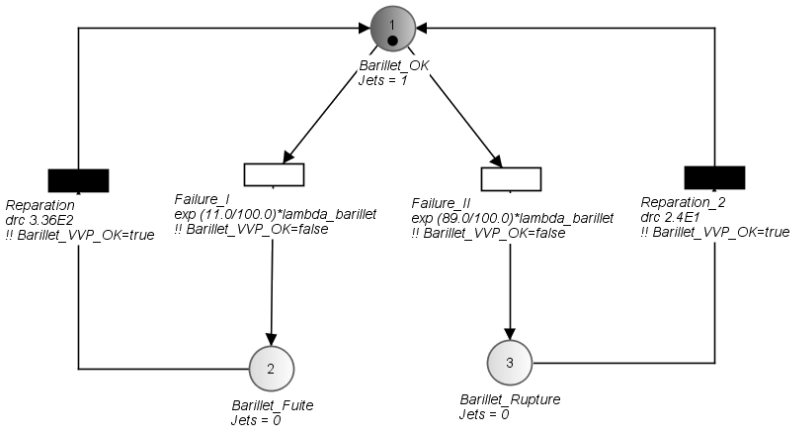


Figure 7.3. Barillet VVP

A ce stade du projet ApproDyn, 45 RdPS ont été générés correspondant à 228 places, 281 transitions, 664 arcs et 81 variables.

[16] actuellement maintenu par la société SatoDev (www.satodev.fr)

7.6 Résultats qualitatifs et quantitatifs

7.6.1 Simulation avec profil par palier.

Dans un premier temps, seule la boucle de régulation est testée avec un profil de fonctionnement par palier donné en figure 7.4.. Le premier objectif est de vérifier l'implantation discrétisée de la loi de commande PID au sein d'un réseau de Petri. Le second objectif est de tester la robustesse de cette même loi pour des variations de consigne de puissance allant de 5 % à 65 % ceci en dehors de tout dysfonctionnement de composant.

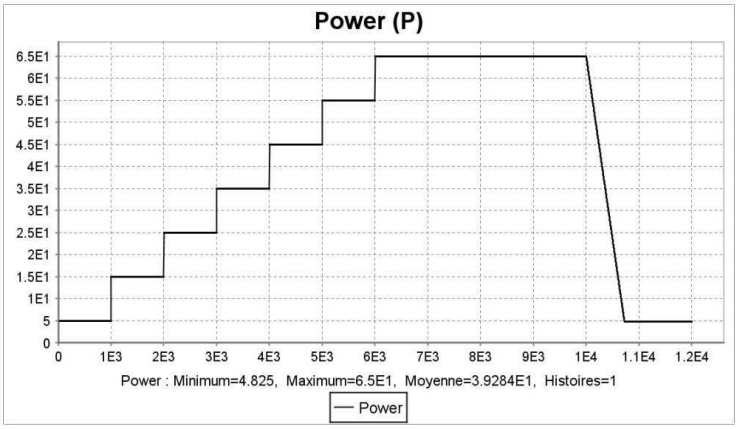


Figure 7.4. Profil de fonctionnement (test PID)

Le réglage de la loi de commande est obtenu à l'aide de la méthode de Ziegler-Nichols. Ce réglage a été fait en amont de la modélisation. Au regard des résultats décrits par la figure 7.5. (le débit d'eau) et par la figure 7.6. (le niveau d'eau), ce réglage unique peut convenir dans un premier temps même si les fortes oscillations montrent qu'il n'est pas optimal et qu'il mérite un *affinage* manuel de ses différents gains.

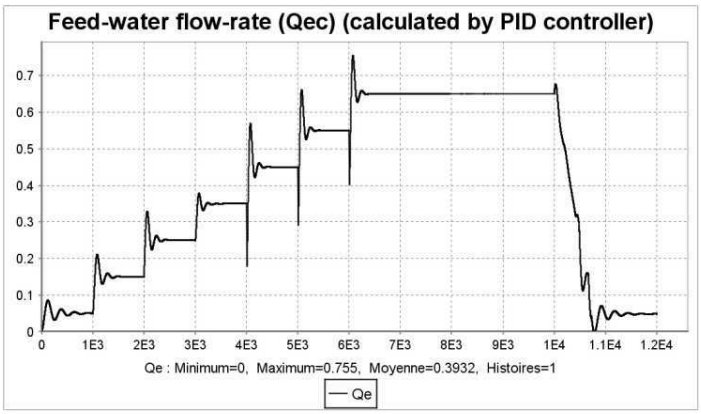


Figure 7.5. Débit d'eau Qe

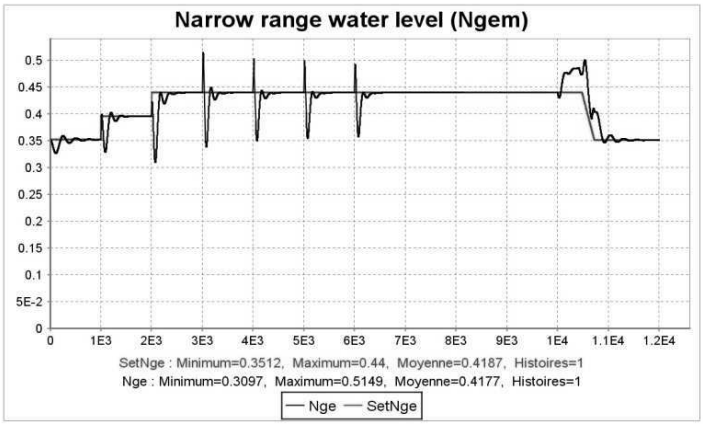


Figure 7.6. Niveau d'eau Nge

7.6.2 Essais avec profil de fonctionnement réaliste

L'objectif ici est de tester le modèle basé sur les RdPS avec un profil de fonctionnement réaliste décrit par la figure 7.7. L'histoire simulée est de 18 mois avec un pas de 0,1h.

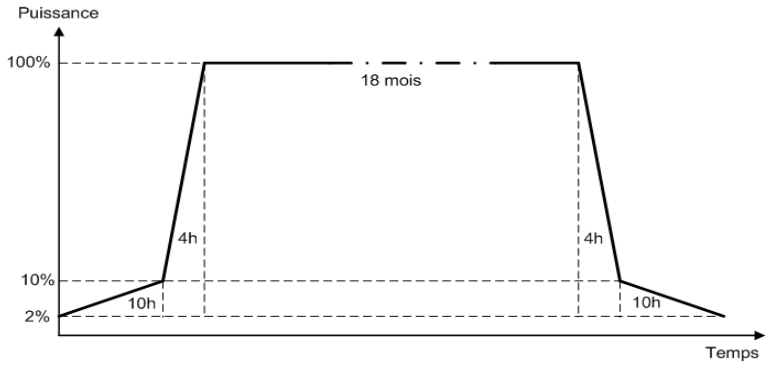


Figure 7.7. Profil de fonctionnement réaliste (consigne)

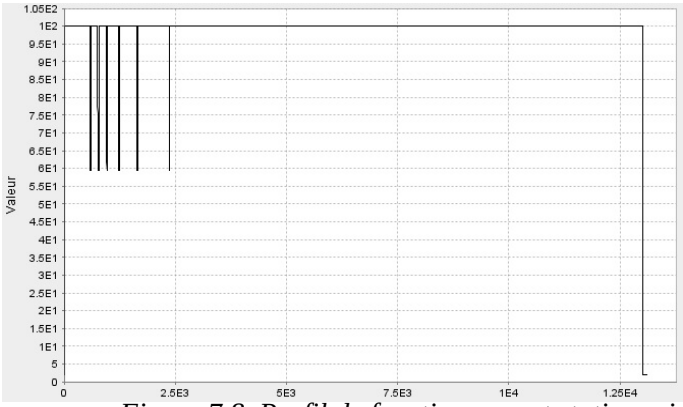


Figure 7.8. Profil de fonctionnement stationnaire (durée simulée de 18 mois)

La figure 7.8. illustre un profil de fonctionnement, en phasestationnaire, sur une histoire unique de la puissance P pendant la période des 18 mois. Les défaillances éventuelles des composants sont pris en compte dans la simulation, et se manifestent par des « glitches ». On peut voir que le barillet VVP et le groupe des trois pompes CEX ne tombent pas en panne pendant cette histoire, sinon au regard des modes opératoires du GV donnés au chapitre 1, un tel cas causerait un AAR. De même, il n'y a pas de défaillance type I, II et III des vannes ARE car cela provoquerait une chute de la puissance P à 2 % ; le temps d'effectuer leur maintenance.

Les figures 7.9 7.10 illustrent pour ce même profil de fonctionnement la variation du débit d'eau Qe ainsi que du niveau d'eau Nge.

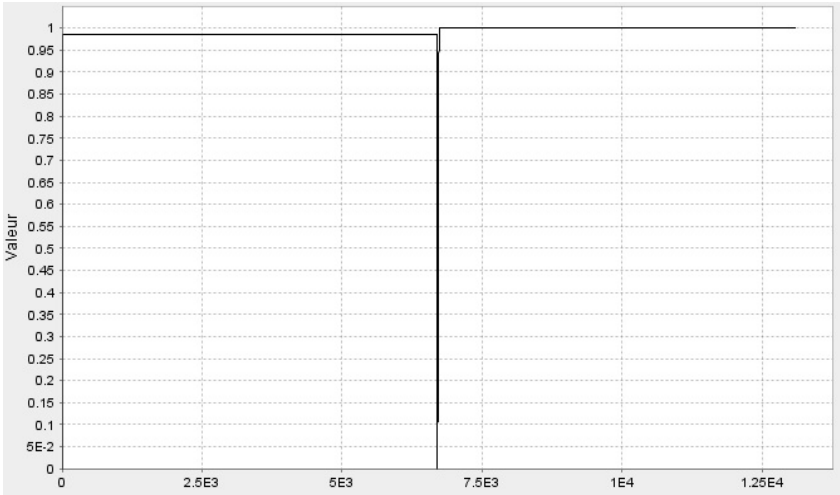


Figure 7.9.Débit d'eau réel Qe

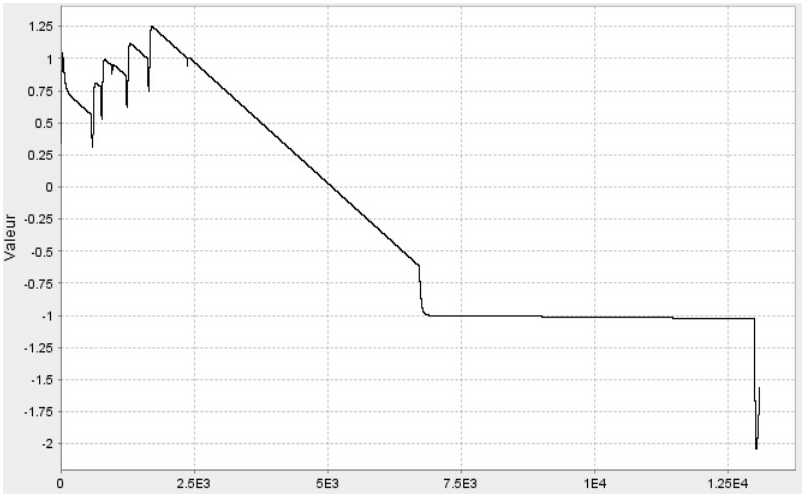


Figure 7.10.Niveau d'eau mesuré Nge

Ces deux profils, en particulier celui de Nge, indiquent clairement un problème de régulation. La loi de commande ne tient pas la consigne souhaitée. Tout ce passe comme si le débit d'eau n'était pas suffisant pour maintenir la hauteur d'eau Nge.

Conclusions et perspectives pour l'approche RdPS

Les premiers résultats dits en situation réelle ne sont pas satisfaisants. Le temps a malheureusement manqué pour étudier complètement le cas test du projet ApproDyn. Malgré cela, ce que l'on peut retenir de l'approche par RdPS est sa facilité de mise en œuvre. Elle ne demande pas de connaissances particulières en informatique si ce n'est une programmation modulaire, hiérarchisée ; technique empreint de bon sens et couramment utilisée dans le monde industriel. Cette manière de programmer alliée à une représentation graphique de type automate fait que les RdPS sont souvent utilisés en sûreté de fonctionnement.

A ce stade du projet, le point bloquant est la gestion de la loi de contrôle/commande à tout instant qui se trouve ne pas être robuste. L'approche par RdPS a souhaité rester ancrée au plus près de la réalité du cas test ApproDyn. D'une part, le système n'est pas invariant dans le temps dans le sens où sa nature intrinsèque dépend de la puissance demandée. D'autre part, les actionneurs pilotés sont à commande bornée. Les indicateurs de fiabilité demandés sont corrélés à la grandeur commandée (le niveau d'eau dans le générateur de vapeur). Pour ces raisons, l'approche par RdPS ne peut actuellement fournir de résultats quantitatifs sur les différentes probabilités souhaitées comme celle d'un arrêt automatique du réacteur.

S'agit-il d'un verrou technique dans l'utilisation de l'outil (problème de priorisation des tirs de transition) et la programmation de la loi de commande (discrétisation de la loi PID) ou scientifique dans la manière d'effectuer les simulations de Monte Carlo (la gestion du temps n'étant pas la même pour les évènements stochastiques et les phénomènes continus)? Autant de questions auxquelles l'approche RdPS n'a pu répondre mais qui sont autant de perspectives pour une suite à ce projet.

8 Références

Modélisations du GV

[IRV 80] IRVING E., MIOSSEC C., TASSART J., « Towards efficient full automatic operation of the PWR steam generator with water level adaptive control », *Proceedings of the International Conference on Boiler Dynamics and Control in Nuclear Power Stations*, p. 309-329, British Nuclear Energy Society, London, 1980.

[AST 00] ASTROM K.-J., BELL R.-D., « Drum Boiler dynamics », *Automatica 36)*, p. 363-378, 2000.

[PAR 85] PARRY A., PETRETOT J.F., VIVIER M.J., Recent progress in SG level control in French PWR plants. *Proceedings of the International Conference on Boiler Dynamics and Control in Nuclear Power Stations*

[FAL 99] BENDOTTI P., FALINOWER C.M., EDF Benchmark for robust control techniques evaluations of proposed solutions 14th world congress IFAC, Beijing, 1999

[KOT 96] KOTHARE M.V., METTLER B., MORARI M., BENDOTTI P., FALINOWER C.M.,, Level control in the steam generator of a nuclear power plant. Decision and control, 1996. Proceedings of the 35th IEEE (pp 4851-4856), December 1996.

[KOT 00] KOTHARE M.V., METTLER B., MORARI M., BENDOTTI P., FALINOWER C.M., Level Control in the Steam Generator of a Nuclear Power Plant, M.V. Kothare *et al.* 35th IEEE transactions in Decision and Control, January 2000.

[RAM 99] AIT RAMI M.; FOLCHERF J.P., EL GHAOUI L., BENDOTTI P., FALINOWER C.M.. Control of jump linear systems : Application to the steam generator water level. Proceedings of the 38" Conference on Decision & Control Phoenix, Arizona USA December 1999

[AST 00] ASTROM K.-J., BELL R.-D., « Drum Boiler dynamics », *Automatica 36)*, p. 363-378, 2000.

[BEM 99] A.Bemporad and M.Moari Control of systems integrating logical, dynamics and constraints. Automatica, 35(3):407-427, March, 1999.

Régulations

[BRA 99] Branicky, Borkar, Mitter A unified framework for hybrid control: model and optimal control theory. IEEE transactions on automatic control, 43(1), pp 31-45, January 1998

Modélisation des parties actionneurs, capteurs, automates

[BRI 11a] BRISSAUD F., SMIDTS C., BARROS A., BÉRENGUER C., Dynamic Reliability of digital-based transmitters , *RESS*, n° 96, 2011.

[BRI 11b] BRISSAUD F., CHARPENTIER D., BARROS A., BÉRENGUER C.,, Reliability analysis for new technology-based transmitters, in Reliability Engineering and System Safety, vol. 96(2), february 2011, pages 299-313

[THO 03] Thomas J, Dumur D., Buisson J., BENDOTTI P., FALINOWER C.M. Moving horizon sate estimation of hybrid systems. Application to faut detection of sensors of a steam generator. CCA, Istanbul, Juin 2003

Optimisation

[GIU 01] Giuggioli Busacca P., Marseguerra M., Zio E..Multiobjective optimization by genetic algorithms: application to safety systems. Reliability Engineering and System Safety 72 (2001) 59-74

Cas test NUREG/CR-6942

[PER 85] PERROW C.. Normal accidents: Living with high risk technologies. New York Basic Books, 1985.

[KIR 05] Kirschenbaum J., Stovsky M., Bucci P., Aldemir T., Arndt S.A. Benchmark development for comparing digital instrumentation and control system reliability modeling approaches. American Nuclea Society, LaGrange Pak, IL (2005).

[MAN 08] Mandelli D., Aldemir T., Kirschenbaum J., Bucci P., Miller D.W., Stovsky M., Ekici E., Arndt S.A., A benchmark system for the reliability modeling of digital instrumentation and control systems , *International Probabilistic Safety Assessment and management Conference PSAM 9*, Hong Kong, 2008.

[NUR 07a] NUREG/CR-6942, Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, US Nuclear Regulatory Commission, Washington DC, 2007.

[NUR 06] NUREG/CR-6901, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, US Nuclear Regulatory Commission, Washington DC, 2006.

[IRV 80] IRVING E., MIOSSEC C., TASSART J., « Towards efficient full automatic operation of the PWR steam generator with water level adaptive control », *Proceedings of the International Conference on Boiler Dynamics and Control in Nuclear Power Stations*, p. 309-329, British Nuclear Energy Society, London, 1980.

Modélisation des interactions type II

[EPRI 10] Thuy, Torok R., EPRI Report 1019182 Protecting Against Digital Common-Cause Failure-Combining Defensive Measures and Diversity Attributes, December 2010.

[THUY 09] A Mixed Approach to Assess the Impact of I&C in PSA. N.Thuy, G.Deleuze. Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009, Knoxville, Tennessee.

[JOU 10] G. Deleuze, R.Quatrain, F.Jouanet, N. Thuy. Experimentation of sensitivity study based on Beta Factors to assess the impact of I&C in PSA. PSAM 2010, Seattle, June 2010.

[DEL 11] G. Deleuze, R.Quatrain, F.Jouanet, N. Thuy. Assessment of common cause failures and defensive measures for the representation of I&C in probabilistic models. ESREL 2011, October 2011, Troyes, France.

[DEL 12] G. Deleuze, R.Quatrain, F.Jouanet,. D. Talbourdet, F. Lucet. A Method for the Assessment of Common Cause Failures of Digital I&C Hardware. ESREL 2012 (A paraître).

[CHA 11] CHAUX P.Y., ROUSSEL J.M., LESAGE J.J., DELEUZE G., BOUISSOU M.. *Qualitative analysis of a BDMP by Finite Automaton. ESREL 2011*

[CHA 12] CHAUX P.Y., ROUSSEL J.M., LESAGE J.J., DELEUZE G., BOUISSOU M.. Towards a unified definition of Minimal Cut Sequences for dynamic repairable systems . SAFECOMP 2012 (A paraître).

Cell to Cell Mapping Technique (CCMT)

[ALD 91] T. ALDEMIR, "Utilization of the Cell-To-Cell Mapping Technique to Construct MarkovFailure Models for Process Control Systems", G. APOSTOLAKIS (Ed.), *Probabilistic Safety Assessment and Management: PSAM1*, 1431-1436, Elsevier, New York (1991).

Dynamic FLowgraph Methodology (DFM)

[GAR 95] Garrett, C., Guarro, S., & Apostolakis, G. (1995). The dynamic flowgraph methodology for assessing the dependability ofembedded software systems. *IEEE Transactions on Systems, Man and Cybernetics* , Volume 25-5 824--840.

[YAU 95] Yau, M., Guarro, S., & Apostolakis, G. (1995). Demonstration of the dynamic flowgraph methodology using the Titan II space launch vehicle digital flight control system. *Reliability Engineering & System Safety* , Volume 43-3 335--353.

[CHA 10] Chaux P.Y., Deleuze G.. Comparaison de deux méthodes dynamiques d'évaluation de la sureté de fonctionnement :BDMP et DFM. Congrès Lambda Mu, La Rochelle, 2010.

Modélisation par Réseaux de Petri Stochastiques

[DAV 94] DAVID R., ALLA H., « Petri nets for modeling of dynamic systems », *A survey Automatica*, vol. 30, Issue 2, p. 175-202, 1994.
[MUR 89] Murata T., « Petri nets : Properties, Analysis and Applications », *Proceedings of the IEEE*, vol. 77, n° 4, p. 541-580, 1989.
[DUT 97] DUTUIT Y., CHÂTELET E., SIGNORET J.P., THOMAS P., « Dependability modelling and evaluation using stochastic Petri nets : application to two test cases », *Reliability Engineering & System Safety*, vol. 55, issue 2, 117-124, 1997.
[ZIL 08] ZILLE V., BÉRENGUER C., GRALL A., DESPUJOLS A., LONCHAMPT J., « Multi-component systems modeling for quantifying complex maintenance strategies », *Proc. Of European Safety & Reliability Conference '08, Valencia-Spain*, p. 3586-3591, 2008.

Modélisation par Automates Stochastiques Hybrides

[BAB 11] BABYKINA G., BRÎNZEI N., AUBRY J.F., PÉREZ CASTAÑEDA G.-A., « Reliability assessment for complex systems operating in dynamic environment », *Annual Conference of the European Safety and Reliability Association, ESREL 2011*, Troyes, France, septembre 2011.

[CAS 08] CASSANDRAS C.G., LAFORTUNE S., *Introduction to discrete event systems*, Springer Science, New York, USA, 2008.

[HAM 05] HAMIDI K., Contribution à un modèle d'évaluation quantitative des performances fiabilistes de fonctions électroniques et programmables dédiées à la sécurité, Thèse de doctorat de l'Institut National Polytechnique de Lorraine, Nancy, 27 octobre 2005.

[JEN 09] JENSEN K., KRISTENSEN L.M., *Coloured Petri Nets: modeling and validation of concurrent systems*, Springer-Verlag, Berlin Heidelberg, 2009.

[NAJ 07] NAJAFI M., NIKOUKHAH R., « Modeling Hybrid Automata in Scicos », *Multi-conference on Systems and Control (MSC)*, Singapore, 1-3 octobre, 2007.

[PER 09] PEREZ CASTAÑEDA G.A., Évaluation par simulation de la sûreté de fonctionnement de systèmes en contexte dynamique hybride, Thèse de doctorat de l'Institut National Polytechnique de Lorraine, Nancy, 30 mars 2009.

[PER 10] PÉREZ CASTAÑEDA G.A., AUBRY J.F., BRÎNZEI N., « Performance assessment of systems including conflict in the context of dynamic reliability », *International Journal of Adaptive and Innovative Systems*, Inderscience Publishers, 1(3-4), p. 233-247, 2010.

[PER 11] PÉREZ CASTAÑEDA G.A., AUBRY J.F., BRÎNZEI N., « Stochastic Hybrid Automata Model for Dynamic Reliability Assessment », *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 225(1), p. 28-41, 2011.

[POC 08] POCK M., BELHADAOUI H., MALASSÉ O., WALTER W., « Efficient generation and representation of failure lists out of an information flow model for modelling safety critical systems », *Annual Conference of the European Safety and Reliability Association, ESREL 2008*, Valencia, Espagne, 2008.

[PER11] Pérez Castañeda G.A., Aubry J.F., Brinzei N., Stochastic hybrid automata model for dynamic reliability assessment, *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 225 (1), 28-41, 2011
[CAS 10b] Perez Castaneda G.A., Aubry J.F., Brinzei N., « DyRelA (Dynamic Reliability andAssessment) », International Workshop on Dynamic Aspects in Dependability Models for Fault-Tolerant Systems, DYADEM-FTS 2010 in conjunction with European Dependable Computing Conference EDCC 2010, Valence (Espagne), 27-30 avril 2010

Modélisation par Processus Markoviens Déterministes par Morceaux

[DAV 93] DAVIS M.H.A., *Markov models and optimization*, Chapman and Hall, London, 1993.
[DUF 2002] DUFOUR F., DUTUIT Y., « Dynamic Reliability : a new model », *$\lambda\mu$-13 et ESREL02*, vol. 1, p. 350-353, 2002.
[ZHA 06] H. Zhang, F. Dufour, I. Fares, Y. Dutuit. Fiabilité dynamique: Outils analytiques et numériques, in: Proceedings of Lambda Mu , Lille, France, October, 2006
[ZHA 07] H. Zhang, K. Gonzalez, F. Dufour, Y. Dutuit. Piecewise Deterministic Markov Processes and Dynamic Reliability, in: Proceedings of Mathematical Methods in Reliability, Glasgow, Ecosse, July, 2007
[ZHA 08] ZHANG H., DUFOUR F., DUTUIT Y., ELEGBEDE C., « Application des processus déterministes par morceaux à un système de production pétrolière offshore », *Proceedings of $\lambda\mu$-16*, Avignon, France, 2008.
[ZHA 09] ZHANG H., DUFOUR F., DUTUITET Y., GONZALEZ K., « Piecewise deterministic Markov processes and dynamic reliability », *Journal of Risk and Reliability*, 222(4), p. 545-551, 2009
[SAP 09] B. de Saporta, F. Dufour, K. Gonzalez, Numerical method for optimal stopping of hybrid processes, 3rd IFAC Conference on Analysis and Design of Hybrid Systems, Zarragoza, Spain, 2009
[SDG 10] DE SAPORTA B., DUFOUR F., GONZALEZ K., « Numerical method for optimal stopping of piecewise deterministic Markov processes », *Annals of Applied Probability*, n° 20(5), p.1607-1637, 2010.
[SAP 11] DE SAPORTA B., DUFOUR F., ZHANG H., ELEGBEDE C., « Optimal stopping for the predictive maintenance of a structure subject to corrosion », *Journal of Risk and Reliability*, à paraître.
[SD 11] DE SAPORTA B., DUFOUR F., *Numerical method for impulse control of Piecewise Deterministic Markov Processes*, Automatica, à paraître.
[BRA 11] A. Brandejsky, B. de Saporta, F. Dufour, C. Elegbede, Numerical method for the distribution of a service time, ESREL 2011, Troyes, France, 2011
[SAP 11] B. de Saporta, F. Dufour, H. Zhang, Approximation of the value function of an impulse control problem of Piecewise deterministic Markov process, IFAC 18th world congress, Milano, Italy, 2011
[ZHA 12] H. Zhang, B. de Saporta, F. Dufour, G. Deleuze, Dynamic reliability: towards efficient simulation of the availability of a feedwater control system, 8th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC-HMIT), San Diego, USA, 2012
[SAP 12a] B. de Saporta, F. Dufour, H. Zhang, Predictive maintenance for the heated hold-up tank, PSAM11 & ESREL12, Helsinki, Finland
[BRA 12a] A. Brandejsky, B. de Saporta, F. Dufour, Numerical method for expectations of piecewise-determistic Markov processes, CAMCoS, 2012, *to appear*
[SAP 12b] B. de Saporta, F. Dufour, Numerical method for impulse control of Piecewise Deterministic Markov Processes, Automatica, 2012, to appear
[BRA 12b] A. Brandejsky, B. de Saporta, F. Dufour, Numerical methods for the exit time of a piecewise-deterministic Markov process, Advances in Applied Probability 44(1), 2012
[SAP 12c] B. de Saporta, F. Dufour, H. Zhang, C. Elegbede, Optimal stopping for the predictive maintenance of a structure subject to corrosion, avec F. Dufour, H. Zhang et C. Elegbede, Journal of Risk and Reliability, 2012, to appear

Autres publications

P. Broy, R. Donat, H. Chraibi, Y. Dijoux, C. Bérenguer, Dynamic Bayesian Networks for Assessing Reliability of Hybrid Systems, in Proceedings of the 7th International Conference on Mathematical Methods in Reliability : Theory, Methods, Applications - MMR2011 - 20-24 June 2011 - Beijing, China - Lirong Cui & Xian Zhao (eds) - Beijing : Beijing Institute of Technology Press, 2011 - ISBN : 978-7-5640-3983-7, pages 252-257
T.-D. Le Duy, D. Vasseur, M. Couplet L. Dieulle, C. Bérenguer, Parameter and Model Uncertainty Analysis using Dempster-Shafer Theory in Nuclear Probabilistic Risk Assessment, in Proceedings of the International Topical Meeting on Probabilistic Safety Assessment and Analysis - PSA 2011 -

March 13-17, 2011 - Wilmington, NC, USA - American Nuclear Society, 2011 - ISBN :978-0-89448-089-8, [14 pages]
F. Brissaud, C. Smidts, A. Barros, C. Bérenguer, Dynamic Reliability Modeling of Cooperating Digital-Based Systems, in Reliability, Risk and Safety - Back to the future - Proc. of the European Safety and Reliability Conference - ESREL 2010 - 5-9 september 2010 - Rhodes, Greece - B.J.M. Ale, I.A. Papazoglou & E. Zio (eds) - London : Taylor & Francis (CRC Press/Balkema), 2010 - ISBN : 978-0-415-60427-7, pages 1051-1060
N. Duflot, C. Bérenguer, L. Dieulle, D. Vasseur, On the independence of defense lines of a new nuclear power plant, in Risk, reliability and Societal Safety - Proc. of European Safety and Reliability Conference - ESREL 2007 - 25-27 June 2007 - Stavanger, Norway - T. Aven & J.E. Vinnem (eds) - Taylor & Francis (Balkema) - ISBN : 978-0-415-44783-7, vol. 2, pages 1005-1013
N. Duflot, C. Bérenguer, L. Dieulle, D. Vasseur, A min cut set-wise truncation procedure for importance measures computation in probabilistic safety assessment, in Reliability Engineering and System Safety, vol. 94(11), november 2009, pages 1827-1837
Y. Langeron, A. Barros, A. Grall, C. Bérenguer, Dependability assessment of networkbased safety-related system, Journal of Loss Prevention in the Process Industries, 24(5), 2011, pages 622-631
V. Zille, C. Bérenguer, A. Grall, A. Despujols, Modelling multi-component systems to quantify RCM maintenance strategies, in Journal of Risk and Reliability - Proceedings of the Institution of Mechanical Engineers, Part O, 225(2), 2011, pages 141-160
Ghostine R., Thiriet J.M., Aubry J.F. “Variable delays and message losses: influence on the reliability of a control loop”, *International journal on Reliability Engineering and System Safety*, 96 (1), (2011), 160-171.
Morel G., Pétin J.F., Johnson T., “Reliability, maintenance, and safety” in Springer Handbook of Automation, S.Y. Nof Editor, Chapter 42, pages 535-547, Springer Verlag, (2009).
Sallak M., Simon C., Aubry J.F. “A fuzzy probabilistic approach for determining Safety Integrity Level”, *IEEE transactions on Fuzzy System*, 16 (1), (2008), 239-248.
Pétin J.F., Gouyon D., Morel G., “Supervisory synthesis for product-driven automation and its application to a flexible assembly cell”, *Control Engineering Practice*, 15 (5), (2007), 595-614.
Schoenig R., Aubry J.F., Cambois T., Hutinet T. “An aggregation method of Markov graphs for the reliability analysis of hybrid systems”, *International Journal on Reliability Engineering and System Safety RESS*, 91 (2), (2006), 137-148.
Pétin J.- F., Morel G., Panetto H., Formal specification method for systems automation. European Journal of Control 12 (2), (2006), 115-130.
Babykina G, Brinzei N., Aubry J.F., Perez Castaneda G.A., “Reliability assessment for complex systems operating in dynamic environment”, *Annual Conference of the European Safety and Reliability Association, ESREL 2011*, Troyes, France, September 2011.
Lemattre T., Denis B., Faure J.M., Pétin J.F., Salaün P., “Designing operational control architectures of critical systems by reachability analysis”, *Proceedings of 7th IEEE Conference on Automation Science and Engineering (IEEE CASE 2011)*, Trieste, Italy, August 24-27, 2011.
Habib G., Pétin J.F., Divoux T., “Dynamic adaptation of IEEE 802.11e priorities for improving temporal performance and safety of a Wireless Networked Discrete Control System”, *IEEE Workshop on Dependable Control of Discrete Systems DCDS’11*, Saarbrucken, Germany, June 15-17 2011.
Pétin J.F., Evrot D., Morel G., Lamy P., “Combining SysML and formal methods for safety requirements verification”, *22nd International Conference on Software & Systems Engineering and their Applications*, Paris, France, December 7-9, 2010.
Belhadaoui H., Jallouli M., Diou C., Monteiro F., Malassé O., Aubry J.F., Dandache A., Buchheit G., Medromi H., “Evaluation of important reliability parameters using VHDL-RTL modelling and information flow approach”, *European Safety and Reliability Conference ESREL 2008*, Valencia, Spain, September 22-25 2008, 2549-2557.

Annexe.

Pour mener une comparaison générale des approches, nous avons défini un certain nombre de critères qualitatifs. Nous les avons élaborés à partir la comparaison faite dans les études NUREG de référence ([NUR 07a], [NUR 06]), moyennant des adaptations et améliorations de ses critères. En effet, nous les avons trouvés améliorables sur plusieurs points :Les évaluations proposées par les auteurs sont assez imprécises et discutables. Certaines, fournies dans ce tableau dans le rapport NUREG, semblent contradictoires avec les descriptifs des méthodes fournis dans le rapport par ailleurs.

- Les critères parlent de modèle et une fois de méthodologie, ne distinguent pas l'outil et la méthode mathématiques.
- Les évaluations du tableau sont peu justifiées et documentées
- Les exigences n°2 et n°3 nous semblent des questions de qualité de modélisation générales ou peu pertinentes dans le cadre d'APPRODYN, puisque, à la différence du rapport NUREG, nous avons un cas test applicatif précis, et les approches ont été choisies pour tenter de répondre à ses caractéristiques.
- L'évaluation NUREG porte en plus sur l'aspect « modélisation des systèmes numériques», qui n'est pas la question d'APPRODYN (cf aussi exigences n°6 et n°10).

Nous recensons ci-dessous les critères employés et leur description en anglais, ainsi que nos commentaires.

Exigence n°1 (prioritaire pour APPRODYN et [NUR 06]).
L'approche doit etre *inductive* (retrouver des défaillances observées) et *déductive* (trouver des défaillances pas encore observées)
The model must be able to predict encountered and future failures well and cannot be purely based on previous experience.

Exigence n°2 (non retenu par APPRODYN)
L'approche doit tenir compte de façon pertinente des particularités du système étudié
The model must account for the relevant features of the system under consideration.

Exigence n°3 (prioritaire pour [NUR 06], non retenu par APPRODYN).
L'approche doit être fondée sur des hypothèses valides et plausibles. Les effets des écarts et des simplifications doivent être connus.
The model must make valid and plausible assumptions, and the consequences of violating these assumptions need to be identified.

Exigence n°4 (prioritaire pour APPRODYN).
L'approche doit etre capable de représenter quantitativement et avec précision les dépendances entre défaillances
The model must quantitatively be able to represent dependencies between failure events accurately.

Exigence n°5 (prioritaire pour APPRODYN).
L'approche doit être conçue de manière à être accessible à un analyste et mise en ouvre (conception du modèle, implémentation dans un outil) sans besoin de ressources importantes. L'enjeu est la possibilité de vérification et de réutilisation du modèle par un tiers.
The model must be designed so it is not hard for an analyst to learn the concepts and it is not be hard to implement.

Exigence n°6 (prioritaire pour [NUR 06], non retenu par APPRODYN).
Les données employées pour la quantification doivent être crédibles auprès des communautés techniques de la Sûreté de Fonctionnement et du Contrôle-Commande
The data used in the quantification process must be credible to a significant portion of the technical community.

Sur le fond, il n'y a pas aujourd'hui de consensus dans la communauté de la SdF pour reconnaître des approches comme répondant à un problème quelconque de modélisation d'un système numérique, et ce n'est pas la question abordée par APPRODYN.

Exigence n°7 (prioritaire pour APPRODYN et [NUR 06]).
Cette exigence est assez peu explicite.
Nous l'avons reformulé et interprétée comme étant la capacité à révéler les séquences d'états dangereux (effets domino), et à distinguer les états ou séquences affectant la fiabilité et ceux affectant la sureté
(Méthode) *The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.*

Exigence n°8 (prioritaire pour APPRODYN et [NUR 06]).
Le modèle doit être capable de distinguer entre des fautes qui causent des défaillances fonctionnelles et celles qui causent des défaillances intermittentes
The model must be able to differentiate between faults that cause function failures and intermittent failures.

Exigence n°9 (prioritaire pour APPRODYN).
Le modèle doit être capable de fournir des résultats pertinents pour les utilisateurs (analyste EPS, expert I&C) dont les séquences minimales, les probabilités de défaillance et les incertitudes associées aux résultats.
The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.

Exigence n°10 (prioritaire pour étude [NUR 06], non retenu par APPRODYN, car en écart avec la stratégie de modélisation.).
Le modèle doit être capable de représenter l'interaction entre les parties numériques du système de Contrôle-Commande et et les parties non numériques dans les scenarios accidentels. La méthodologie doit prendre en compte à la fois les interactions de Type I et de Type II.
The methodology must be able to model the interaction of the digital I&C system portions of accident scenarios with non-digital I&C system portions of the scenarios. The methodology should account for both Type I and Type II interactions.

Exigence n°11 (prioritaire pour [NUR 06], retenu par APPRODYN).
Cette exigence est assez peu explicite et a du etre réécrite. Elle exprime le besoin de fournir des résultats sous forme discrete, afin d'être compatible avec l'approche EPS, sachant que l'intégration de modèle hybrides avec les EPS est une question qui n'est traitée dans APPRODYN.
Compatibilité avec les EPS. Le modèle ne doit pas nécessiter de variables continues pour décrie l'état de l'installation (données de surveillance, temps réel…) et doit pouvoir générer des états discrets.
The model should not require highly time-dependent or continuous plant state information.
Avec ces critères, la comparaison des approches de modélisation est résumée dans le tableau suivant. En grisé, evaluations du rapport [NUR 06]

Approche. Cf [NUR 06] et APPRODYN	Ex. n°1	Ex. n°2	Ex. n°3	Ex. n°4	Ex. n°5	Ex. n°6	Ex. n°7	Ex. n°8	Ex. n°9	Ex. n°10	Ex. n°11
Priorité pour NUREG	+		+			+	+	+		+	+
Priorité pour APPRODYN	+	Non Pert.	Non Pert.	+	+	Non Pert	+	+	+	Non Pert.	+
Arbres d'évènements continus	OK	OK	OK	OK	Non	?	?	OK	?	?	Non
Arbres d'évènements dynamiques	OK	OK	OK	?	OK	?	?	?	OK	OK	Non
Modèles Markoviens (CCMT)	OK	OK	OK	OK	Non	?	OK	OK	?	?	Non
Simulations de Monte Carlo	OK	OK	OK	OK	?	?	?	?	?	?	Non
PMDPM /Simulation	Cf 1.5.	Non Pert.	Non Pert.	Cf 1.5.	Cf 1.5.	Non Pert.	Cf 1.5.	Cf 1.5.	Cf 1.5.	Non Pert.	Cf 1.5.
Réseaux de Petri (yc RdPS)	OK	OK	OK	OK	Non	?	?	?	?	?	Non
RdPS	Cf 1.5.	Non Pert.	Non Pert.	Cf 1.5.	Cf 1.5.	Non Pert.	Cf 1.5.	Cf 1.5.	Cf 1.5.	Non Pert.	Cf 1.5.
DFM	OK	OK	OK	?	OK	?	?	?	OK	OK	OK
Automates Stochastiques Hybrides	Cf 1.5.	Non Pert.	Non Pert.	Cf 1.5.	Cf 1.5.	Non Pert.	Cf 1.5.	Cf 1.5.	Cf 1.5.	Non Pert.	Cf 1.5.
Arbres de défaillance dynamique	OK	?	?	?	OK	?	OK	?	OK	?	OK
Event Sequence Diagram	OK	OK	OK	OK	Non	?	?	?	OK	OK	Non
Go Flow	OK	?	OK	?	Non	?	?	?	OK	OK	OK
Approches Bayésiennes d'estimation de la fiabilité	OK	?	?	?	Non	Non	?	?	?	?	OK
Approches par Tests	?	?	OK	Non	OK	?	OK	OK	?	Non	OK
Approches basées sur les métriques logicielles	Non	?	Non	Non	?	?	OK	OK	Non	Non	OK
Modèle de Schneidewind	OK	?	?	?	?	?	?	?	Non	Non	OK