Nouvelle méthodologie de synthèse de lois de commande tolérante aux fautes garantissant la fiabilité des systèmes

Ahmed Khelassi

Nancy-Université

Ecole doctorale IAEM Lorraine
Faculté des Sciences et Technologies

CRAN

THÈSE

pour l'obtention du

Doctorat de l'Université Henri Poincaré, Nancy 1
Spécialité : Automatique, Traitement du Signal, des Images et Génie Informatique

présentée par

Ahmed KHELASSI

Nouvelle Méthodologie de Synthèse de Lois de Commande Tolérante aux Fautes Garantissant la Fiabilité des Systèmes

Soutenue publiquement le 11 Juillet 2011

Composition du jury :

Président	Mustapha OULADSINE	Professeur à l'Université Aix-Marseille 3
Rapporteurs	Christophe BERENGUER	Professeur à l'Université de Technologie de Troyes
	Vincent COCQUEMPOT	Professeur à l'Université Lille 1
Examinateurs	Youmin ZHANG	Professeur à Concordia University, Canada
	Jean Baptiste LEGER	Ingénieur de Recherche Société PREDICT
Directeurs de thèse	Didier THEILLIOL	Professeur à l'Université Henri Poincaré
	Philippe WEBER	Maître de Conférences à l'Université Henri Poincaré

Centre de Recherche en Automatique de Nancy UMR - 7039 - CNRS - UHP - INPL
Boulevard des Aiguillettes 54506 Vandœuvre-Les-Nancy
Tel. +33(0)3 83 68 44 61 - Fax +33(0)3 83 68 44 62

Cette thèse est dédiée à mes Parents.

Remerciements

Les travaux présentés dans ce mémoire ont été effectués au Centre de Recherche en Automatique de Nancy (CRAN), au sein du Groupe Sûreté de Fonctionnement et Diagnostic (SURFDIAG) de l'Université Henri Poincaré (UHP). En préambule de ce mémoire, je souhaite adresser ici tous mes remerciements aux personnes qui m'ont apporté leur aide et qui ont ainsi contribué à l'élaboration de ces travaux de recherche.

En premier lieu, ma reconnaissance s'adresse conjointement à Messieurs Didier Theilliol et Philippe Weber pour leur double encadrement particulièrement efficace dans la conduite de ces travaux.

Je tiens à remercier Monsieur Didier Theilliol, Professeur à l'Université Henri Poincaré, qui a encadré ma thèse. Sa confiance ne m'a jamais fait défaut et il a constamment porté un regard critique, ouvert et constructif sur ces travaux. En dépit d'un emploi du temps fort chargé, j'ai conscience des efforts qu'il a dû fournir pour se rendre disponible. Merci Didier pour ta disponibilité et pour tout ce que j'ai appris en travaillant avec toi.

Mes remerciements vont également à mon co-encadrant de thèse Monsieur Philippe Weber, Maître de Conférences à l'Université Henri Poincaré. A la fois pertinent et pédagogue, il a toujours su m'encourager. Ses compétences ont été un atout indéniable à la réussite de ces travaux. Merci Philippe pour ton soutien et pour les différents conseils et discussions constructives que nous avons eu.

J'exprime ma gratitude aux Professeurs Christophe Berenguer et Vincent Cocquempot pour avoir accepter de rapporter mon mémoire et pour l'intérêt qu'ils ont bien voulu porter à ce travail. Je remercie également Professeur Mustapha Ouladsine et Monsieur Jean Baptiste Leger d'avoir accepté d'examiner ce travail et de participer à ce jury de thèse.

I would like to address my thanks to Professor Youmin Zhang for the several remarks about my research works and for making me the great honor to be part of the jury.

Je remercie aussi l'ensemble des permanents du Groupe SURFDIAG pour leur accueil et un remerciement spécial à notre sympathique secrétaire Sabine Huraux, pour son assistance administrative, sa disponibilité et surtout son efficacité. Mes vifs remerciements s'adressent également aux membres du Département QLIO de l'IUT Nancy-Brabois, où j'ai passé des années de monitorat sympathiques.

Je remercie mes chers amis et collègues Kamel et Boumedyen (Bob) pour tous les moments de joie et de bonheur que nous avons passé ensemble. Je n'oublierai pas

les petites réunions nocturnes non scientifiques que nous avons passé. Merci surtout pour les conseils et les réconforts durant les moments difficiles.

Je pense aussi aux anciens collègues Brian, Abdou, Hossein pour la générosité et la bonne humeur quotidienne. Je remercie aussi mes collègues Tushar, Ghassan, Ahmed ainsi que mes compatriotes Souleymen et Amine (Cheikh Rasslen) pour les moments sympathiques que nous avons eu. Je vous souhaite la réussite personnelle et professionnelle.

Je tiens à dire toute ma sympathie aux personnes avec lesquelles j'ai passé des moments formidables à l'extérieur du Labo. Je pense particulièrement aux membres de "Football Club Nation " pour tous les matchs de foot que nous avons joué chaque Samedi, sous la neige, la pluie et le soleil fracassant de Juillet, grand respect à notre organisateur Salim pour son assistance durant cette période, ça va me manquer.

Je ne pourrais clore ces remerciements sans exprimer ma reconnaissance à ceux qui me sont chers. Mes parents, Merci pour les valeurs et les principes dans les quels vous m'avez élevé, Merci pour le soutien et les encouragements malgré la distance qui nous sépare physiquement. Ce travail de thèse est le vôtre avant qu'il soit le mien. Mes frères et sœurs, Merci pour tout, votre accueil de l'été me fait oublier tous les moments difficiles, je vous souhaite la réussite et le bonheur. Ma chère fiancée, Merci pour ta patience durant ces années, tes encouragements, ton soutien et ton amour m'ont permis d'achever cette étape de ma vie.

La liste des personnes à remercier est longue, je souhaite exprimer ma gratitude envers tous ceux qui m'ont apporté leur aide et leur soutien dans cette aventure.

Le 16 Mai 2011
Deux ans, 7 mois et 16 jours

"Quand tu ne sais pas où tu vas, Regarde d'où tu viens".

Proverbe Bèrbère

Références personnelles

Travaux en cours d'évaluation

- **A. Khelassi**, P. Weber, D. Theilliol, Y.M. Zhang. Reliable Fault-Tolerant Control Incorporating Actuator Criticality. *IEEE Transactions on Aerospace and Electronic Systems*. (Soumis en Juin 2011)

Revues Internationales avec comité de lecture

- **A. Khelassi**, D. Theilliol, P. Weber. Reconfigurability Analysis for Reliable Fault-tolerant Control Design. *International Journal of Applied Mathematics and Computer Science*, vol. 12, N 3, 2011.

- P. Weber, B. Boussaid, **A. Khelassi**, D. Theilliol, C. Aubrun. Reconfigurable control design with integration of reference governer and reliability indicators. *International Journal of Applied Mathematics and Computer Science- Special issue*, (En révision)

Conférences internationales avec comité de lecture

- **A. Khelassi**, D. Theilliol, P. Weber. A novel active fault tolerant control design with respect to actuators reliability. *50th IEEE Conference on Decision and Control and European Control Conference, IEEE CDC-ECC, 2011, Orlando, FL. USA.* (Article Accepté)

- **A. Khelassi**, D. Theilliol, P. Weber. Fault tolerant control design with respect to actuators health degradation : An LMI approach. *IEEE Multi-conference on Systems and Control, IEEE MSC-CCA, 2011, Denver, CO. USA.* (Article Accepté)

- **A. Khelassi**, P. Weber, D. Theilliol, C. Aubrun. Evaluation of Fault Tolerant System against Actuators Aging applied to Flotation Circuit. *18th IFAC World Congress, 2011, Milan. Italy.* (Article Accepté)

- **A. Khelassi**, J. Jiang, D. Theilliol, P. Weber, Y.M. Zhang. Reconfiguration of Control Inputs for overactuated Systems based on Actuators health. *18th IFAC World Congress, 2011, Milan. Italy.* (Article Accepté)

- **A. Khelassi**, P. Weber, D. Theilliol. Reconfigurable control design for overactuated systems based on reliability indicators. *IEEE Conference on Control and Fault-Tolerant Systems, IEEE SysTol, 2010, Nice. France.*

- **A. Khelassi**, D. Theilliol, P. Weber. Control design for over-actuated systems based on reliability indicators. *UKACC International Conference on CONTROL 2010, Coventry. United Kingdom.*

- **A. Khelassi**, D. Theilliol, P. Weber. On Reconfigurability for Actuator Faults under Reliability Constraints. *IFAC Workshop on Automation in Mining, Mineral and Metal Industry, IFAC-MMM 2009, Viña del Mar. Chile.*

- **A. Khelassi**, D. Theilliol, P. Weber. Reconfigurability analysis for reliable fault-tolerant control design. *7th Workshop on Advanced Control and Diagnosis, ACD'2009, Zielona Gora. Poland.*

- B.Tondu, R. Lezama-Morales, **A. Khelassi**. Robust control of a McKibben artificiel muscle actuator using a sliding mode control with a smith predictor. *In Proceeding of the 13th IASTED International Conference on Robotics and Applications, RA 2007, Germany.*

Conférences nationales avec comité de lecture

- **A. Khelassi**, D. Theilliol, P. Weber. Synthèse d'une loi de commande reconfigurable assurant la fiabilité des systèmes. *Sixième Conférence Internationale Francophone d'Automatique, CIFA 2010. France.*

Table des matières

Table des figures

Introduction générale

Au cours de ces dernières décennies, la complexité des installations industrielles a augmenté avec le développement technologique. La sûreté de fonctionnement des systèmes technologiques critiques constitue un enjeu important tant sur le plan économique que scientifique. Dans le cadre des systèmes à risques, la capacité à effectuer les tâches pour lesquelles le système a été conçu peut être entravée par l'apparition de phénomènes anormaux. Il peut alors s'en suivre des fonctionnements non désirés, catastrophiques notamment dans le domaine de l'aéronautique, du nucléaire, ou des sites industriels classés SEVESO... etc. Pour palier aux problèmes liés à l'apparition des défauts, les communautés scientifiques et industrielles, se sont tournées vers le développement de systèmes de commande tolérants aux défauts. En effet, un système tolérant aux fautes se caractérise par son aptitude à maintenir ou à retrouver des performances en fonctionnement dégradé, proches de celles qu'il possède en régime nominal.

Les travaux développés dans cette thèse visent à intégrer deux disciplines différentes liées à la sûreté de fonctionnement que sont la tolérance aux défauts et la fiabilité des systèmes. Les systèmes de commande tolérante aux fautes permettent de garantir des performances proches de celles désirées même après l'apparition d'un évènement indésirable ou d'une dérive. Cependant, cette propriété de tolérance aux fautes ne résout pas complètement le problème de la sûreté de fonctionnement du système et plusieurs questions restent ouvertes :

La disponibilité des actionneurs au moment de l'occurrence des défauts garantit-elle l'accommodation de ces derniers ? - Quelles sont les limites fonctionnelles du système a priori pour accommoder les éventuels défauts ? - Comment le système sera-t-il en mesure de faire face à l'apparition des défauts et à garantir les performances désirées jusqu'à la fin de la mission ? - Dans le cadre des systèmes sur-actionnés, comment gérer les efforts appliqués aux actionneurs afin d'améliorer la sûreté de fonctionnement du système ? - Comment équilibrer les charges appliquées sur les actionneurs en tenant compte de leur durée de vie et garantir en même temps les performances désirées ? - Existe-il une méthodologie pour estimer l'état de vieillissement des actionneurs afin de les intégrer comme information complémentaire dans la synthèse de la loi de commande ? - Pour le cas des systèmes dynamiques, comment synthétiser un système de commande tolérante aux fautes garantissant la fiabilité et une durée de vie résiduelle optimale ?

Synthétiser des systèmes de commande tolérante aux fautes avec des décisions et des actions de commande en tenant compte de la fiabilité des actionneurs constitue une approche innovante pour répondre aux nouveaux problèmes posés par les impératifs de la commande et de la sûreté de fonctionnement. Ce mémoire de thèse s'intéresse au développement d'une nouvelle méthodologie de synthèse de lois de commande tolérante aux fautes garantissant la fiabilité du système. Du point de vue

méthodologique, ces travaux consistent à proposer des solutions pour la synthèse des lois de commande tolérante aux fautes intégrant l'évaluation prévisionnelle de la fiabilité du système relevant classiquement de communautés disciplinaires distinctes. Ces nouvelles stratégies nécessitent l'adaptation des différents outils de caractérisation de la fiabilité avec la théorie de la commande, notamment avec l'intégration explicite de l'impact de la charge appliquée sur les lois modélisant la fiabilité des actionneurs.

Dans le premier chapitre de la thèse, les principaux concepts de la commande tolérante aux fautes ainsi que les outils fondamentaux d'analyse de la fiabilité des systèmes sont présentés. Dans une première partie, un état de l'art sur les différentes méthodes de commande tolérante aux fautes est présenté en se focalisant sur les approches dites actives. Dans la deuxième partie, les différentes définitions ainsi que les principaux concepts de l'étude de fiabilité des systèmes sont introduits. Les motivations de l'intégration des informations sur la fiabilité des composants dans la synthèse des lois de commande sont présentées. Dans ce contexte et malgré le peu de travaux existant sur cet aspect, un état de l'art sur les différents travaux de recherche existant dans la littérature est décrit. Chaque approche présentée fait l'objet d'une discussion critique afin de mettre en évidence ses avantages et ses inconvénients.

Le second chapitre est consacré à l'étude de reconfigurabilité des systèmes linéaires en tenant compte de la fiabilité des actionneurs. L'objectif est d'étudier les limites fonctionnelles des systèmes assurant la mission attribuée avec un niveau de probabilité désiré. En général, la capacité fonctionnelle du système à tolérer les défauts est mesurée par un indicateur énergétique de reconfigurabilité calculé pour des conditions de fonctionnements défaillants. Le niveau de l'énergie définissant les limites d'accommodation est imposé dans la phase de conception. Dans cette étude, la probabilité que, après accommodation des défauts, le système soit capable d'atteindre le temps de fin de mission est introduite sous forme d'une contrainte de fiabilité. La relation entre la fiabilité globale à respecter et la commandabilité du système évaluée en terme d'énergie est présentée. Un indice de reconfigurabilité basé sur l'énergie nécessaire pour accommoder les défauts tout en respectant un niveau de fiabilité satisfaisant est proposé.

Les travaux du troisième chapitre concernent la commande tolérante aux défauts des systèmes sur-actionnés en présence de défauts actionneur. Ainsi, le problème d'allocation et de ré-allocation de la commande est abordé en prenant en compte la dégradation et le vieillissement des actionneurs. Une méthodologie d'allocation et ré-allocation de la commande, avec comme objectif d'assurer d'une part les performances désirées et d'autre part de garantir la fiabilité des systèmes est proposée. Les deux approches développées requièrent l'adaptation des différents indicateurs de fiabilité afin d'intégrer ces derniers dans la synthèse de la loi de commande. Des exemples illustrant les performances et les limites de la méthodologie proposée sont donnés à la fin du chapitre.

Le quatrième chapitre est entièrement consacré à la synthèse d'une loi de commande tolérante aux fautes assurant la fiabilité globale du système. Une procédure d'analyse de fiabilité des systèmes commandés en ligne est proposée en se basant sur une étude de sensibilité. L'étude de sensibilité développée permet d'établir le diagramme de fiabilité du système modélisé par sa représentation d'état et de classer ainsi les actionneurs selon leur criticité. La synthèse d'un régulateur active tolérant aux fautes est proposée en tenant compte de l'étude de sensibilité de la fiabilité du système par rapport à la fiabilité des actionneurs. Le problème de synthèse de la loi de commande tolérante aux fautes garantissant la fiabilité du système est proposé sous une formulation LMI.

La conclusion et les perspectives des travaux proposés sont données à la fin de ce mémoire de thèse.

Chapitre 1

Commande tolérante aux fautes et fiabilité des systèmes

Dans ce chapitre introductif, nous allons présenter dans une première partie les principaux concepts de la commande tolérante aux fautes ainsi que les outils de base d'analyse de la fiabilité des systèmes. Une classification non-exhaustive des principales méthodes de commande tolérante aux fautes sera donnée. Cette classification permettra de se positionner parmi les grandes familles de méthodes existantes. En effet, chaque méthode présentée fera l'objet d'une discussion critique afin de mettre en évidence ses avantages et ses inconvénients. Dans une deuxième partie, les différentes définitions ainsi que les principaux concepts nécessaires pour évaluer la fiabilité des systèmes seront introduits. Ces deux premières parties nous permettront de parcourir les méthodes utilisées dans cette thèse et de justifier les orientations choisies. Le principe de base de la nouvelle méthodologie de commande tolérante aux fautes intégrant des informations sur la fiabilité des composants sera introduit à la fin de ce chapitre. Dans ce contexte et malgré le peu de travaux existant sur cet aspect, nous présentons un état de l'art sur les différents travaux de recherche proposés dans la littérature.

1.1 Systèmes tolérants aux fautes

Au cours des dernières décennies, les performances des équipements industriels ont été considérablement augmentées. Le gain en performances s'est accompagné d'un accroissement de la complexité des installations provoquant une demande plus forte de disponibilité et de sécurité. Cependant, la capacité à effectuer les tâches pour lesquelles le système a été conçu peut être entravée par l'apparition de phénomènes anormaux que sont les défauts.

Introduite dans les années 80, la commande tolérante aux fautes fut l'objet de plusieurs travaux de recherches dans le domaine de systèmes à risque. L'objectif principal est de pallier aux problèmes liés à l'apparition des défauts pouvant conduire à des fonctionnements non désirés, voire catastrophiques. En effet, ce type de problème a été souvent évité en se fondant sur la redondance matérielle à base d'actionneurs et de capteurs. Cette stratégie est non seulement onéreuse mais elle nécéssite aussi un important dispositif de maintenance.

Dans ce contexte et pour répondre aux nouveaux problèmes posés par les impératifs de tolérance aux défauts et au coût, de nombreuses méthodes et techniques fondées sur des modèles dynamiques ont été développées et traitées de manière analytique. L'objectif est de détecter les défauts, de les traiter et de prendre une décision

concernant la reconfiguration du système ou de ses objectifs. Cette problématique est abordée dans la littérature comme relevant du problème de la commande tolérante aux fautes et a fait l'objet de nombreux travaux de recherche comme présenté dans la récente synthèse bibliographique de Zhang et Jiang (2008).

1.1.1 Commande tolérante aux fautes

Un système de commande tolérante aux fautes se caractérise par son aptitude à maintenir ou retrouver des performances acceptables proches de celles désirées en régime nominal ainsi que dans un mode de fonctionnement dégradé. Une commande tolérante aux fautes possède la capacité de s'accommoder, de manière automatique, des défauts pouvant affecter ses différents composants. La tâche incombant les systèmes tolérants aux fautes est de synthétiser des lois de commande garantissant la stabilité et les performances dynamiques désirées, non seulement lorsque tous les composants sont opérationnels, mais aussi après l'apparition de défauts.

En effet, un défaut est défini comme étant une déviation, non souhaitée, d'au moins une propriété caractéristique ou d'un paramètre du système. Le défaut est une dérive pouvant conduire à des mauvais fonctionnements ainsi que la perte totale du composant. Les défauts sont des phénomènes qui apparaissent à différents endroits du système. Les défauts actionneurs agissent au niveau de la partie opérative du système en détériorant le signal d'entrée. Un défaut de type actionneur peut être une perte d'efficacité, un blocage ou une panne totale de l'actionneur.

En revanche, les défauts de type capteur sont la cause d'une mauvaise image de l'état physique du système. Un défaut capteur partiel produit un signal relativement différent de la vraie variable. Il peut se traduire par une réduction de la valeur affichée, de la présence d'un biais ou de bruit accru empêchant une bonne lecture.

1.1.2 Classification des méthodes de commande tolérante aux fautes

Les méthodes de synthèse des systèmes de commande tolérante aux fautes sont généralement classées et regroupées dans deux grandes familles : les approches passives (*Passive Fault Tolerant Control Systems*, PFTCS) et les approches dites actives (*Active Fault Tolerant Control systems*, AFTCS). Comme le montre la figure (1.1), la distinction entre les deux approches dépend de la méthode de synthèse, des défauts considérés, du type de redondance présent ainsi que du comportement du système dans le cas dégradé.

1.1.2.1 Approches passives

Une loi de commande tolérante aux fautes passive est synthétisée pour tolérer un nombre pré-défini de défauts supposés connus avant la phase de conception. La synthèse des méthodes PFTCS est basée sur les outils de la commande robuste afin d'assurer l'insensibilité du système en boucle fermée à certains défauts. La tolérance aux fautes est assurée sans changement de structure des régulateurs nominaux et

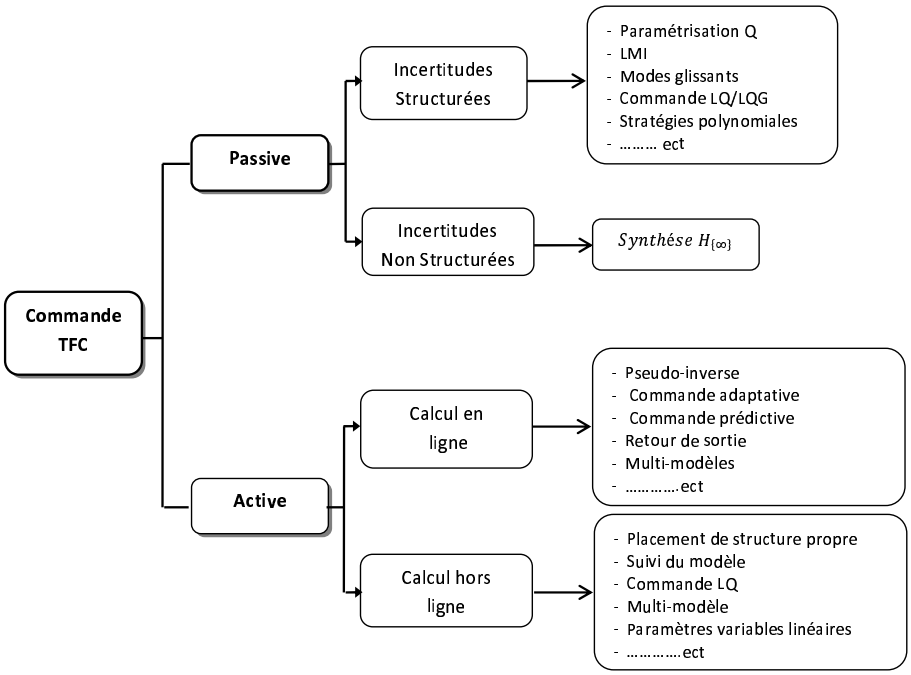

FIGURE 1.1 – Classification des méthodes tolérantes aux fautes

sans utilisation d'informations en ligne relatives aux différents défauts affectant le système. Généralement, dans les approches PFTCS (voir figure.1.2), les défauts sont considérés comme sources d'incertitudes de modèle (Patton, 1997). Un certain degré de *tolérance* aux défauts est garanti en se basant sur les techniques classiques de commande robuste (Zhou, 2000; Chen et Patton, 2001; Niemann et Stoustrup, 2003).

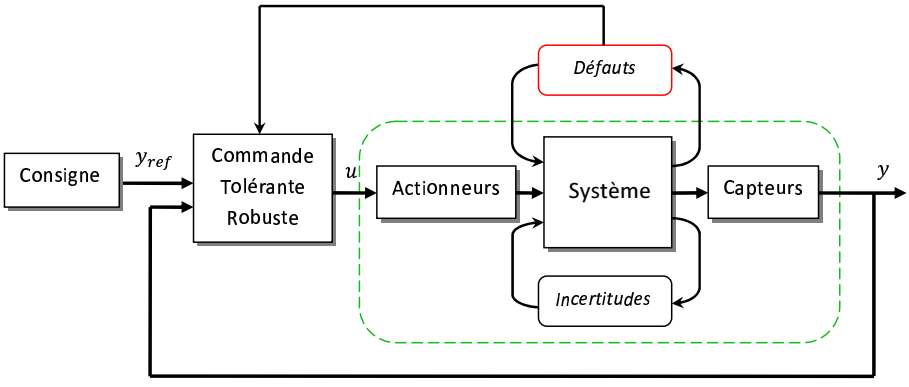

FIGURE 1.2 – Schéma de principe d'une loi de commande FTC passive

Ainsi, dans (Jamouli *et al.*, 2004), les auteurs proposent de modéliser l'effet des défauts sur le système par un processus aléatoire. Une méthodologie basée sur la minimisation d'un critère de type LQG permet alors de synthétiser la loi de commande FTC. (Niemann et Stoustrup, 2005) utilisent la paramétrisation de Youla comme degré de liberté pour atteindre les performances FTC requises. Le problème est résolu à l'aide de la technique *loop shaping* de la commande robuste H_∞. (Marcos *et al.*, 2005) proposent la synthèse d'un régulateur à quatre degrés de

liberté (*4-DOF controller*) impliquant la gestion d'un compromis entre les performances de la régulation et du diagnostic.

En revanche, même si l'idée des approches passives est séduisante d'un point de vue conceptuel, ce type de solution reste pour le moins discutable. La robustesse accrue vis-à-vis de certains défauts prédéfinis est obtenue au dépend d'un niveau de performance dégradé en mode de fonctionnement nominal. Cette approche présente donc un inconvénient majeur car en général, les défauts sont des événements qui ne se produisent que rarement, il n'est pas souhaitable de dégrader de manière significative et permanente les performances du système. De plus, il apparait évident que, plus l'ensemble des défauts prédéfinis sera important et l'impact de ces défauts sur le système jugé sévèrement, plus le comportement en situation normale sera dégradé. Ainsi, les lois de commande FTC passives garantissent de manière générale un faible niveau de performances. Cependant, dans certaines applications où la classe de défauts est connue et restreinte, ces techniques peuvent s'avérer suffisantes.

Pour plus de détails sur les méthodes de commande robuste, le lecteur pourra se référer aux travaux de (Zhao et Jiang, 1998; Suyama, 2002; Veillete, 2002).

1.1.2.2 Approches actives

Dans la plupart des systèmes de commande conventionnels, la loi de commande est synthétisée sans tenir compte d'éventuelles occurrences de défauts pouvant affecter le système. Dans d'autre cas, la redondance matérielle disponible dans le système à commander peut être très limitée. L'augmentation ou le changement de la configuration matérielle peut s'avérer onéreuse, voire impossible due aux limitations physiques.

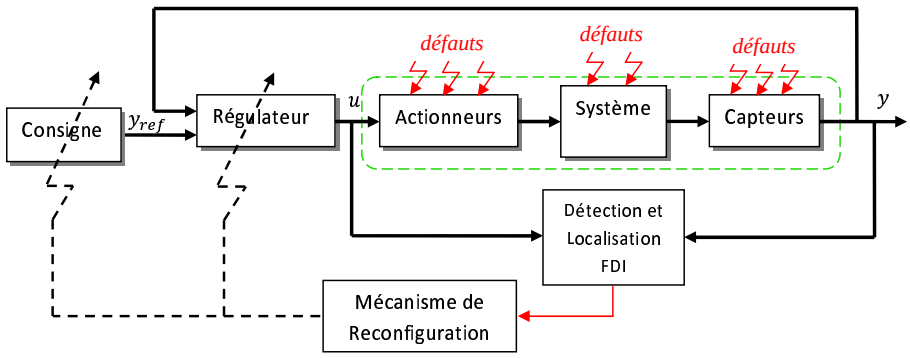

FIGURE 1.3 – Schéma de principe d'une loi de commande FTC active

Plus récemment, nous assistons de plus en plus au développement des approches tolérantes aux fautes dites *Actives*. Comme le montre la figure (1.3), celles-ci se caractérisent par la présence d'un module de diagnostic de défauts (FDD). Le principe consiste à détecter et localiser les défauts affectant le système en ligne. En fonction de la sévérité du défaut, une nouvelle stratégie de commande est appliquée via un mécanisme de reconfiguration en changeant un ensemble de paramètres de la loi de commande ou par la mise en place d'une nouvelle structure de commande.

Il existe plusieurs approches permettant de résoudre ce problème. Les méthodes dites de reconfiguration du système sont souvent fondées sur l'existence de redondance de chaines de mesure et/ou actionneurs. L'idée consiste à détecter et à localiser convenablement les défauts, et à commuter ensuite sur une nouvelle chaîne d'actionneurs et/ou capteurs redondante saine. Dans le cadre de ces méthodes, la véritable problématique de la commande tolérante aux fautes repose sur le diagnostic de défauts. Ce type de technique est utilisé par exemple dans le domaine spatial, où des mécanismes de redondance *hot* (functionnal redundancy) ou *cold* (full redundancy) sont mis en place.

Par ailleurs, lorsqu'un recours à des chaines redondantes d'actionneurs et/ou capteurs n'est pas possible, l'objectif est alors de concevoir des stratégies d'accommodation de défauts permettant de compenser complètement ou partiellement l'effet des défauts en utilisant les ressources disponibles. Pour plus de détails sur l'analyse de ces méthodes, le lecteur peut se référer aux travaux de recherches bibliographiques (Blanke *et al.*, 2001; Zhang et Jiang, 2008).

1.1.3 Commande active tolérante aux fautes

Les approches AFTC compensent les effets des défauts soit en sélectionnant des lois de commande pré-calculées soit en synthétisant une loi de commande en ligne et en temps réel. Avant de présenter les principales techniques et stratégies actives de reconfiguration, nous présentons brièvement le concept de base ainsi que les principales méthodes de diagnostic nécessaires pour la synthèse d'une approche AFTC.

1.1.3.1 Diagnostic des défauts

Le diagnostic est défini comme l'ensemble des actions mises en œuvre afin de détecter et localiser les défauts affectant le système. La détection concerne la mise en évidence d'événements qui affectent l'évolution d'un système. La détection consiste à comparer le fonctionnement réel du système avec ce qu'il devrait être sous l'hypothèse de fonctionnement nominal. La tâche de localisation consiste à analyser les événements de façon à pouvoir déterminer le type de défauts (capteur, actionneur, ..etc) ainsi que les composants défectueux du système, voir figure (1.3).

Pour répondre à cette démarche de diagnostic, de nombreuses approches ont été développées et proposées. Ces dernières peuvent être classées en deux catégories principales : méthodes basées sur le traitement du signal, et méthodes à base de modèle. Les techniques basées sur le traitement du signal sont fondées sur le test des propriétés spécifiques de différents signaux de mesure. Les filtres passe-bandes et l'analyse spectrale sont des exemples des différentes techniques utilisées dans cette catégorie de méthodes. Ces méthodes de diagnostic font appel à une connaissance du système constituée par la formulation explicite d'un modèle analytique. Les premiers travaux dans ce sens remontent au début des années soixante-dix (Mehra et Peshon (1971). Ces approches sont basées sur la comparaison du comportement réel du processus avec celui fourni par un modèle analytique. Le résultat de cette comparaison est contenu dans un ensemble de signaux indicateurs de défauts appelés

les résidus. Une stratégie permettant d'évaluer ces résidus et donc de détecter et localiser l'éventuel défaut succède généralement à la phase de génération.

Dans le cas de systèmes linéaires, la génération des résidus est formalisée par la recherche d'un vecteur $r(t) \in \mathbb{R}^{q_r}$ tel que

$$r(t) = H_u u(t) + H_y y(t) \tag{1.1}$$

de façon à satisfaire un cahier des charges donné. Ce cahier des charges est généralement formulé en terme de spécifications de robustesse vis-à-vis des perturbations internes (telles que les incertitudes paramétriques, les dynamiques mal connues, ... etc) et externes (perturbations exogènes) et de sensibilité vis-à-vis des défauts. Dans cette formulation, $y(t) \in \mathbb{R}^p$ et $u(t) \in \mathbb{R}^m$ représentent respectivement les vecteurs de mesure et de commande. H_u et H_y sont des filtres dynamiques stables. L'analyse du comportement temporel et/ou fréquentiel du vecteur $r(t)$ doit alors permettre de remplir complètement la tâche de diagnostic. Un état de l'art de ces méthodes peut être trouvé dans la liste non exhaustive des références suivantes : Chen et Patton (1999); Patton *et al.* (2000); Frank *et al.* (2000); Isermann (2005). Nous citons dans ce qui suit les principaux travaux :

• **L'approche à base de modèles paramétriques** (Isermann, 1984; Zolghadri, 1996) Dans cette approche, on ne génère pas réellement un vecteur de résidus, mais on estime un vecteur de paramètres dont la variation à l'extérieur d'une plage de référence représente l'apparition d'un défaut dans le système surveillé (ou plus exactement représente un changement dans les caractéristiques du procédé). Cette variation peut alors être détectée à l'aide d'un test de décision dans l'espace paramétrique.

• **L'approche par projection dans l'espace de parité** (Chow et Willsky, 1984; Gertler, 1997) La philosophie de l'approche par projection dans l'espace de parité est d'exploiter la redondance analytique existante dans les équations d'état lorsque celles-ci sont écrites sur un horizon d'observation. Le vecteur de résidus est alors généré en projetant les mesures observées sur cet horizon dans un espace appelé espace de parité à l'aide d'un vecteur appelé vecteur de parité. En fait, l'espace de parité est un espace que le vecteur d'état du système non perturbé ne peut atteindre.

• **Les approches à base d'observateurs** (Frank, 1990; Chen et Patton, 1999) L'idée principale des méthodes de génération du vecteur de résidus $r(t)$ à base d'observateurs est d'estimer une combinaison ou l'ensemble des mesures du système surveillé à partir des grandeurs mesurables. $r(t)$ est alors généré en formant la différence entre les sorties estimées et les sorties réelles. L'observateur peut être considéré comme un modèle placé en parallèle avec le système où l'écart en sortie est pondéré dans le but d'obtenir des résultats plus pertinents.

• **Les approches basées sur la synthèse directe de filtres de diagnostic** Ces approches sont basées sur la réalisation directe du filtre de diagnostic $H_u(s)$ et $H_y(s)$ satisfaisant aux propriétés spécifiques de robustesse et de stabilité. Deux techniques

sont distinguées, celles qui visent à estimer les défauts (Stroustrup et Niemann, 2002; Henry et Zolghadri, 2006) et celles qui visent à générer un vecteur de résidus au sens classique du terme (Ding *et al.*, 2000; Jaimoukha *et al.*, 2006).

1.1.3.2 Lois de commande tolérantes aux fautes actives

• **La méthode de la pseudo-inverse PIM** (Antsaklis et Gao, 1992; Staroswiecki, 2005a,b; Ciubotaru *et al.*, 2006) Cette méthode est l'une des méthodes les plus citées dans le domaine de la commande tolérante aux fautes par approches actives. Elle est caractérisée par sa simplicité de calcul et d'implantation et sa capacité à manipuler une large classe de défauts. Cette approche consiste à synthétiser le gain d'une loi de commande par retour d'état de telle sorte que la dynamique du système défaillant en boucle fermée s'approche de celle en fonctionnement nominal, au sens d'une norme. La norme la plus utilisée est la norme de Frobenius. Dans la version de base de la méthode pseudo-inverse PIM, un système linéaire nominal est considéré sous la forme :

$$\begin{cases} \dot{x}(t) = & Ax(t) + Bu(t) \\ y(t) = & Cx(t) \end{cases} \tag{1.2}$$

où $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $y(t) \in \mathbb{R}^p$. A, B et C sont des matrices de dimensions appropriées. La loi de commande considérée dans le cas nominal est un retour d'état défini par $u(t) = Kx(t)$, sous l'hypothèse d'accessibilité du vecteur d'état. Après l'apparition du défaut, le système (1.2) est modélisé par une représentation d'état de la forme :

$$\begin{cases} \dot{x}^f(t) = & A_f x^f(t) + B_f u^f(t) \\ y^f(t) = & C_f x^f(t) \end{cases} \tag{1.3}$$

où la nouvelle loi de commande tolérante aux fautes $u^f(t)$ est de structure équivalente, c'est à dire $u^f(t) = \mathcal{K}_f x^f(t)$. La méthode de pseudo-inverse consiste à calculer la matrice de gain de retour d'état $\mathcal{K}_f$ de telle sorte que la distance entre la dynamique en boucle fermée, du système nominal et celui défaillant, soit minimisée. Le problème est reformulé comme suit,

$$\begin{cases} K_f & = arg\min \|(A + BK) - (A_f + B_f K_f)\|_F \\ & = B_f^+(A + BK - A_f) \end{cases} \tag{1.4}$$

où B_f^+ est la matrice pseudo-inverse de B. $\|.\|_F$ représente la norme de Frobenius.

Caractérisée par sa simplicité, cette approche est très appropriée à une implémentation en ligne. En revanche l'inconvénient majeur de la méthode pseudo-inverse classique réside dans la stabilité du système en fonctionnement dégradé. En effet, le gain de retour K_f minimisant le critère (1.4) n'assure pas forcément la stabilité du système dégradé (1.3) en boucle fermée. Pour pallier ce problème, des extensions de la méthode ont été proposées dans (Gao et Antsaklis, 1991) et (Staroswiecki, 2005a). Ces extensions sont basées sur la recherche d'un ensemble de contrôleurs dits *admissibles*.

• **La méthode de placement de structure propre** (Wang et Lin, 1999; Tsui, 1999; Konstantopoulos et Antsaklis, 1996) La méthode proposée par les auteurs consiste à placer les valeurs et les vecteurs propres caractérisant la dynamique de la boucle fermée de façon à être robuste vis-à-vis des défauts. En effet, l'idée principale consiste à assigner exactement les plus importantes valeurs propres de la dynamique des systèmes nominaux et défaillants, et en même temps de minimiser la distance entre les vecteurs propres correspondants au sens de la norme l_2. Cette méthode a été développée aussi bien avec une loi de commande par retour d'état (Zhang et Jiang, 1999a) qu'avec une loi de commande par retour de sortie (Konstantopoulos et Antsaklis, 1996). Considérant le système nominal (1.2) et défaillant (1.3), la méthode de placement de structure propre calcule le gain de retour d'état K_f, solution du problème d'optimisation suivant (Zhang et Jiang, 2000).

$$\begin{cases} trouver & K_f \\ s.q. & (A_f + B_f K_f)v_i^f = \Lambda_i v_i^f,\ i = 1, \ldots, m \\ et & v_i^f = arg\min_{v_i^f} \|W_i(v_i - v_i^f)\|_2 \end{cases} \tag{1.5}$$

où Λ_i et Λ_i^f sont respectivement les valeurs propres de la matrice d'état du système nominal et défaillant en boucle fermée. v_i et v_i^f sont respectivement les vecteurs propres correspondants. $W_i > 0$ est une matrice de pondération à définir servant de degré de liberté supplémentaire.

Le nouveau gain K_f est synthétisé dans le but de faire coïncider les pôles du système nominal en boucle fermée avec les pôles du système défaillant. De même, les vecteurs propres correspondants doivent être les plus proches possibles. En effet, les valeurs propres déterminent la fréquence naturelle et l'amortissement des modes du système, alors que les vecteurs propres indiquent l'influence de chaque mode sur les différentes sorties du système. Cette approche ne présente pas de complexité de calcul du fait qu'une solution analytique du problème (1.5) est disponible (Zhang et Jiang, 2000). Cependant, les incertitudes de modèle ainsi que les incertitudes relatives au processus de détection et d'identification des défauts ne sont pas aisées à prendre en compte.

• **Les méthodes multi-modèles** (Theilliol *et al.*, 2003; Zhang et Jiang, 2001; Yang *et al.*, 2000; Noura *et al.*, 2000; Theilliol *et al.*, 1998) Ces méthodes sont basées sur un ensemble fini de modèles linéaires reliés par des fonctions d'activation. Cet ensemble décrit le système dans des conditions de fonctionnement nominales et défaillantes. L'objectif des méthodes multi-modèles de la commande tolérante aux fautes est de synthétiser en ligne une loi de commande à appliquer à travers une combinaison pondérée des différentes lois de commande issues des correcteurs précalculés (*belding control law*). Dans cette famille de méthodes AFTC, deux principales approches peuvent être distinguées : *Multiple Model Switching and Tuning* (MMST) et *Interacting Multiple Model* (IMM). Nous présentons dans ce qui suit ces deux principales approches.

a) Multiple Model Switching and Tuning **:** (Boskovic et Mehra, 1998) Dans l'approche MMST, la dynamique de chaque mode dégradé est décrite par

un modèle différent. Ces modèles sont implantés en parallèle et chacun possède un régulateur propre. La reconfiguration de la commande consiste à définir, à chaque instant, le couple *Modèle* (M_i)*/Régulateur*$(\mathcal{K}_i)$ le plus approprié à une situation dégradée particulière. En effet, en présence de défaut, le système est supposé passer d'un modèle nominal M_0 à un modèle défaillant M_f correspondant à un contrôleur pré-calculé $\mathcal{K}_f$.

Considérons les systèmes représentés sous la forme d'état suivante :

$$S : \begin{cases} \dot{x} &= A_0(p(t))x + B_0(p(t))u \\ y &= C_0(p(t))x \end{cases} \tag{1.6}$$

avec $x \in \mathbb{R}^n,\ u \in \mathbb{R}^m,\ y \in \mathbb{R}^p$ et $A_0 \in \mathbb{R}^{n\times n},\ B_0 \in \mathbb{R}^{n\times m}$ et $C_0 \in \mathbb{R}^{p\times n}$ ainsi que $p(t) \in S \subseteq \mathbb{R}^l$ définissent les paramètres du système. $p(t)$ varie dans le temps de manière abrupte et représente les différents défauts considérés.

Soit $\mathcal{M}$ l'ensemble de N modèles linéaires

$$\mathcal{M} : \{M_1, \ldots, M_N\} \tag{1.7}$$

tel que

$$M_i : \begin{cases} \dot{x}_i &= A_i x_i + B_i u_i \\ y_i &= C_i x_i \end{cases} \tag{1.8}$$

où le modèle M_i correspond à un ensemble de paramètres $p_j \in S$ donné. Un régulateur stabilisant $\mathcal{K}_i$ est synthétisé pour chaque modèle $M_i \in \mathcal{M}$.

La loi de commande tolérante aux fautes par MMST est obtenue en choisissant à chaque instant le contrôleur correspondant au modèle le plus proche du système nominal. Le choix du contrôleur est effectué en se basant sur un indice de performance à minimiser. L'indice de performance est proposé en fonction de l'erreur entre les sorties estimées du modèle M_i et les mesures. Un exemple d'indice de performance utilisé couramment est donné comme suit (Narendra et Balakrishnan, 1997) :

$$\mathcal{J}_i(t) = \alpha e_i^2(t) + \beta \int_0^t e^{-\lambda(t-\tau)} e_i^2(\tau) d\tau \tag{1.9}$$

avec $\alpha \geq 0,\ \beta > 0,\ \lambda > 0$. En fait, α et β sont respectivement des coefficients de pondération des termes d'erreurs instantanées et des termes d'erreurs à long terme. Le facteur d'oubli λ assure la bornitude de l'indice de performance $\mathcal{J}_i(t)$ pour une erreur e_i bornée. Ainsi, le couple *Modèle* (M_i)*/Régulateur*$(\mathcal{K}_i)$ possédant le plus petit indice de performance est alors choisi. Une période d'attente $T_{min} > 0$ est imposée afin d'éviter des commutations trop rapides.

b) Interacting Multiple Models **:** Dans la méthode d'Interaction de Modèles Multiples IMM, chaque mode de fonctionnement dégradé est modélisé par une combinaison convexe de modèles pré-définis dans un ensemble $\mathcal{M}$. Le système défaillant peut s'écrire sous la forme :

$$M_f = \sum_{i=1}^{N} \mu_i M_i = \mu_i^T \begin{bmatrix} M_1 \\ \vdots \\ M_N \end{bmatrix}, M_i \in \mathcal{M},\ \mu_i > 0 \in \mathbb{R},\ \sum_{i=1}^{N} \mu_i = 1, \tag{1.10}$$

Dans cette approche, le processus de détection de défauts consiste donc à identifier en ligne la valeur des variables μ_i. Pour répondre à ce problème, deux principales méthodes sont proposées dans la littérature. La première méthode appelée *Multiple Model Adaptive Estimation MMAE* est basée sur la synthèse d'un filtre de Kalman pour tout $M_i \in \mathcal{M}$ (Maybeck, 1999; Zhang et Jiang, 1999a). Dans la seconde méthode, l'estimation de l'erreur de sortie est calculée en fonction du vecteur μ. Ce dernier est donc choisi en minimisant cette erreur (Kanev et Verhaegen, 2000; Kanev *et al.*, 2001).

Après l'identification du modèle défaillant, une multitude de stratégies d'accommodation comme la commande prédictive (Kerrigan et Maciejowski, 1999), la stratégie EA (Zhang et Jiang, 1999b), ou un contrôleur fixe (Maybeck, 1999) peut être utilisée.

• **La commande prédictive à base de modèle** (Kerrigan et Maciejowski, 1999; Maciejowski et Jones, 2003) La commande prédictive consiste à résoudre un problème de commande optimale en ligne et à chaque pas de temps. Il s'agit de déterminer l'action de commande qui minimise un critère quadratique pondéré de l'erreur de consigne et de la commande. L'intérêt de cette méthode dans le contexte FTC est de pouvoir modifier en ligne les différentes contraintes de contrôle (comme la perte d'efficacité d'un actionneur) avec un nombre limité de paramètres, de façon à garantir un niveau de performance acceptable du système bouclé en fonctionnement défaillant. Par ailleurs, cette approche nécessite une optimisation en ligne exigeant ainsi une grande puissance de calcul. De plus, cette méthode est valable sous certaines hypothèses : le modèle d'un défaut et ses effets sur le système doivent être parfaitement connus, les défauts considérés doivent être de faible amplitude de telle sorte que les objectifs de commande puissent rester inchangés après l'apparition d'un défaut(Maciejowski, 2000).

• **La commande adaptative** (Bodson et Groszkiewicz, 1997; Zhang et Jiang, 2002b; Ye et Yang, 2006). De nombreuses méthodes actives utilisant un modèle analytique sont basées sur l'approche adaptative. Ces méthodes sont recommandées pour résoudre le problème d'accommodation aux défauts. Le principe de base est le suivant : L'apparition d'un défaut sur le système entraine une modification de ses paramètres. L'identification en ligne des nouveaux paramètres permet de déterminer les coefficients du nouveau correcteur.

La méthode par modèle de référence est une approche séduisante permettant de concevoir une nouvelle loi de commande telle que les performances du système défaillant s'approchent le plus possible de celles d'un modèle de référence, au sens d'un critère. Pour illustrer ce principe, considérons un système linéaire à temps

invariant,

$$\begin{cases} \dot{x}(t) = & Ax(t) + Bu(t) + d(t) \\ y(t) = & Cx(t) \end{cases} \tag{1.11}$$

où $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $y(t) \in \mathbb{R}^p$ représentent respectivement le vecteur d'état, des entrées de commande et de sortie. $d(t)$ modélise les perturbations. Pour cette approche, un modèle de référence est défini comme suit

$$\dot{y}_d(t) = A_d y_d(t) + B_d r(t) \tag{1.12}$$

où $y_d \in \mathbb{R}^k$ est le vecteur de sorties désirées. $r \in \mathbb{R}^k$ est la référence. A_d et B_d sont des matrices carrées données déterminant la dynamique du modèle de référence, avec A_d stable. Une loi de commande par retour d'état $u(t)$ est considérée,

$$u(t) = C_0 r(t) + G_0 x(t) + v(t) \tag{1.13}$$

où $C_0 \in \mathbb{R}^{k \times k}$, $G_0 \in \mathbb{R}^{k \times n}$ et $v \in \mathbb{R}^k$ sont les paramètres du contrôleur. La dynamique du système en boucle fermée est alors donnée comme suit,

$$\dot{y}(t) = (CA + CBG_0)x(t) + CBC_0 r(t) + CBv(t) + Cd(t) \tag{1.14}$$

Comme indiqué précédemment, l'objectif de la loi de commande (1.13) est de faire coïncider la dynamique en boucle fermée (1.14) avec la dynamique désirée (1.12). Pour résoudre ce problème, deux approximations peuvent être réalisées dont l'approche explicite qui consiste à minimiser, au sens des moindres carrés, l'erreur entre la sortie du modèle de référence et la sortie du système. Nous trouvons aussi l'approche implicite où le critère d'optimisation porte directement sur les trajectoires suivies par les variables du vecteur d'état et non sur les sorties. Un état de l'art sur les différents algorithmes proposés dans ce contexte peut être consulté dans (Morse et Ossman, 1990; Bodson et Groszkiewicz, 1997).

1.1.4 Discussion

Le principal objectif d'utiliser la commande tolérante aux fautes est d'améliorer la sûreté de fonctionnement des systèmes. En effet, la sûreté est définie comme l'aptitude d'une entité à satisfaire à une ou plusieurs fonctions requises dans des conditions données. Pour les systèmes non réparables, le principal indicateur de sûreté de fonctionnement d'un système est la fiabilité. Cependant, bien que les analyses de la fiabilité et de la tolérance aux fautes soient utilisées dans le même objectif : *assurer et améliorer la sécurité et la sûreté de fonctionnement des systèmes*, il est difficile d'établir un couplage entre ces deux outils dans le but de contribuer à des lois de commande garantissant la sûreté de fonctionnement des systèmes. Dans la partie suivante, les principaux concepts et éléments de base pour l'évaluation et l'analyse de fiabilité des systèmes sont présentés.

1.2 Fiabilité des Systèmes non réparables

Dans cette partie, les principaux outils et éléments nécessaires dans l'analyse de la fiabilité des système sont présentés. Cependant, beaucoup de notions comme '*défaut*', '*défaillance*', '*panne*' ou '*dégradation*' sont source d'ambiguïté entre la communauté 'Commande des systèmes' et 'sûreté de fonctionnement'. Afin d'unifier les notations et préciser les termes employés dans ce mémoire, nous considérons les définitions suivantes :

Définition 1.1 *La défaillance est un événement conduisant à un état dégradé ou de panne de l'entité.*

Définition 1.2 *La dégradation est présentée comme un état de fonctionnement non nominal qui peut conduire à l'apparition d'un défaut.*

Définition 1.3 *La panne est présentée comme l'état de l'entité après défaillance. Elle est caractérisée par l'inaptitude de l'entité à accomplir sa fonction requise.*

Définition 1.4 *Un défaut est un mode de défaillance conduisant l'entité à l'imperfection de ses fonctions. Il révèle un état de fonctionnement dégradé. L'occurrence d'un défaut n'interrompt pas forcément le fonctionnement de l'entité. Il est considéré comme une dérive, une faute ou une erreur affectant le fonctionnement de l'entité.*

1.2.1 Grandeurs caractéristiques de la fiabilité en temps continu

De nombreuses définitions de la fiabilité d'un système ou d'un composant sont présentées dans la littérature, toutes étant justifiées et relatives à un secteur d'activité donné. Au sens strict, la fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise, dans des conditions données, pendant une durée donnée (Villemeur, 1997). Le terme *dispositif* désigne une entité, c'est-à-dire tout composant, système ou équipement que nous pouvons considérer et utiliser individuellement. Au sens mathématique, la fiabilité est généralement caractérisée et mesurée par la probabilité que l'entité accomplisse une ou plusieurs fonctions requises dans des conditions données, pendant une durée bien déterminée (Pagés et Gondran, 1980; Villemeur, 1997).

Dans ce contexte, nous définissons aussi la disponibilité comme l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné. La disponibilité est généralement mesurée par la probabilité que l'entité soit en état d'accomplir une fonction requise à un instant t.

Afin de donner les expressions mathématiques des différents indicateurs de fiabilité, nous considérons T, une variable aléatoire continue dans $\mathbb{R}^+$, représentant la durée de vie en temps continu d'un système, de sa mise en service jusqu'à sa panne.

Définition 1.5

1. *La fonction de répartition de T appelée aussi la défiabilité donne la probabilité que le système tombe en panne avant l'instant t :*

$$\forall t \geq 0, F(t) = \mathbb{P}(T \leq t) \tag{1.15}$$

2. *La densité de T appelée la densité de probabilité de défaillance ou encore fonction de distribution est la probabilité que la défaillance intervienne dans l'intervalle de temps entre t et $t + dt$.*

$$\forall t \geq 0,\ V(t)dt = \mathbb{P}(t < T \leq t + dt) \tag{1.16}$$

En effet, la distribution $V(t)$ est définie, si elle existe, comme la dérivée de la fonction de répartition $F(t)$ par rapport à t comme suit,

$$F(t) = \int_0^t V(x)dx \tag{1.17}$$

3. *La fiabilité notée $R(t)$ donne la probabilité que le système soit toujours en fonctionnement à l'instant t :*

$$R(t) = \mathbb{P}[T > t] = 1 - F(t) \tag{1.18}$$

En se basant sur les définitions présentées précédemment, la relation suivante peut être obtenue :

$$V(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{1.19}$$

Contrairement à la densité de probabilité de défaillance (1.19) qui correspond à une probabilité à priori, le taux instantané de défaillance appelé aussi taux de défaillance s'apparente à, la probabilité conditionnelle de défaillance sur $]t, t + dt]$ sachant que l'entité n'a pas eu de défaillance sur $[0, t]$.

Définition 1.6 *Nous appelons taux instantané de défaillance la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T de défaillance d'une entité, soit compris dans l'intervalle de temps $[t, t + \Delta t]$, par la durée Δt de l'intervalle de temps lorsque celui-ci tend vers zéro, en supposant que l'entité n'as pas eu de défaillance sur $[0, t]$.*

$$\forall t \geq 0, \lambda(t) = \lim_{dt \to 0} \frac{\mathbb{P}[t < T \leq t + dt / T > t]}{dt} \tag{1.20}$$

La relation (1.20) signifie que $\lambda(t)dt$ tend vers la probabilité conditionnelle de défaillance sur $]t, t + dt]$ sachant que l'entité n'a pas eu de défaillance sur $[0, t]$ quand $dt \to 0$. Cependant, d'après le théorème des probabilités conditionnelles, la relation suivante est obtenue :

$$\lambda(t)dt = \frac{\mathbb{P}[t < T \leq t + dt]}{\mathbb{P}[T > t]} \tag{1.21}$$

En intégrant (1.15), (1.16) et (1.20) dans (1.21), la relation déterminant le taux de défaillance $\lambda(t)$ est obtenue comme suit :

$$\lambda(t) = \frac{V(t)}{R(t)} \tag{1.22}$$

Or, comme $V(t) = -\frac{dR(t)}{dt}$, les relations liant le taux de défaillance et la fiabilité peuvent être obtenues dans (1.23) et (1.24) comme suit :

$$\lambda(t) = -\frac{\frac{dR(t)}{dt}}{R(t)} = -\frac{d}{dt}(lnR(t)) \tag{1.23}$$

$$R(t) = e^{-\int_0^t \lambda(t)dt} \tag{1.24}$$

Généralement, la loi de variation du taux de défaillance $\lambda(t)$ évolue dans le temps en suivant une courbe dite "*en baignoire*" (voir Figure.1.4). Trois périodes sont ainsi définies :

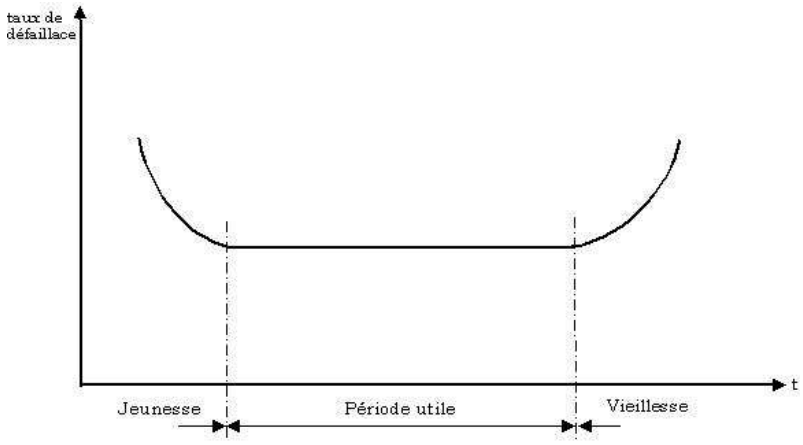

FIGURE 1.4 – Taux de défaillance en fonction du temps

- La période de jeunesse, commençant à un instant donné et pendant laquelle le taux de défaillance $\lambda(t)$ diminue très rapidement par rapport au temps t.

- La période utile où $\lambda(t)$ varie peu dans les conditions normales. Durant cette période appelée aussi durée de vie utile, les défaillances apparaissent avec un taux de défaillance sensiblement constant.

- La période de vieillissement où $\lambda(t)$ augmente de plus en plus vite dans le temps comparativement avec la période utile.

Le temps moyen de bon fonctionnement avant la première défaillance MTTF (Mean Time To Failure) est défini comme le temps moyen de $t = 0$ jusqu'à la première défaillance de l'entité. Le MTTF d'une entité est donc l'espérance mathématique de

sa durée de vie T évoluant selon une distribution bien déterminée. En général, le MTTF est défini comme suit :

$$MTTF = \int_0^\infty tV(t)dt = \int_0^\infty -t\frac{dR(t)}{dt}dt \tag{1.25}$$

que nous pouvons intégrer par parties :

$$MTTF = \int_0^\infty R(t)dt - [tR(t)]_0^\infty$$

L'expression du temps moyen avant la première défaillance MTTF peut être aussi obtenue en fonction de la fiabilité comme suit :

$$MTTF = \int_0^\infty R(t)dt \tag{1.26}$$

1.2.2 Principales lois de probabilité pour l'évaluation de la fiabilité

Généralement, pour modéliser le taux de défaillance $\lambda(t)$ et calculer le MTTF ainsi que la fiabilité $R(t)$, les lois discrètes et continues sont utilisées. Nous examinons rapidement dans ce qui suit les principales lois continues utilisées dans ce mémoire. Les principales distributions discrètes sont données dans l'Annexe.

1.2.2.1 La loi exponentielle

La loi exponentielle caractérise la période durant laquelle le taux de défaillance est constant. C'est le cas des composants électroniques et nombreux composants électriques en période utile.

Pour un taux de défaillance constant : $\lambda(t) = \lambda$, la fiabilité dans le cas continu définie dans (1.24) est évaluée comme suit :

$$R(t) = e^{-\lambda t} \tag{1.27}$$

La fonction de répartition $F(t)$ ainsi que la densité de probabilité sont définies :

$$F(t) = 1 - R(t) = 1 - e^{-\lambda t} \tag{1.28}$$

$$V(t) = -\frac{dR(t)}{dt} = \lambda e^{-\lambda t} \tag{1.29}$$

Le temps moyen de bon fonctionnement défini dans (1.26) est obtenu dans ce cas par :

$$MTTF = \int_0^\infty R(t)dt = \frac{1}{\lambda} \tag{1.30}$$

Ce modèle est le plus utilisé pour sa simplicité dans le calcul de la fiabilité des systèmes composés de plusieurs entités différentes. En outre, il est important de souligner que le passé de tels systèmes n'affecte pas leur évolution future (processus Markovien).

1.2.2.2 Distribution de Weibull

La distribution de Weibull convient pour modéliser la fiabilité des composants dans leur période de vieillissement caractérisée par un taux de défaillance variant dans le temps. La loi de Weibull est caractérisée par la densité de probabilité suivante :

$$v(t) = \frac{\beta(t-\eta)^{\beta-1}}{\alpha^{\beta}} \exp(-(\frac{t-\eta}{\alpha})^{\beta}) \tag{1.31}$$

avec

- η appelé le paramètre de position qui représente le décalage existant entre le début de l'observation et le début du processus examiné,
- α est le paramètre d'échelle lié au temps moyen de bon fonctionnement,
- β est le paramètre de forme associé à la cinétique du processus observé.

La distribution de Weibull s'ajuste en fonction de la valeur de ses paramètres :

- pour $\beta < 1$, le taux de défaillance est décroissant avec le temps, ce qui est représentatif de la période de jeunesse des composants.
- pour $\beta = 1$, le taux de défaillance est constant avec le temps, ceci correspond à la période de vie utile (loi exponentielle).
- pour $\beta > 1$, le taux de défaillance est croissant avec le temps. Ce cas correspond à la période de vieillissement ou d'usure.

Comme défini dans (1.17), la fonction de répartition dans le cas d'une loi de Weibull a pour expression :

$$F(t) = 1 - \exp(-\frac{t-\eta}{\alpha})^{\beta} \tag{1.32}$$

Par ailleurs, la fonction de défaillance $\lambda(t)$ ainsi que la fonction de fiabilité $R(t)$ sont données respectivement comme suit :

$$\lambda(t) = \frac{\beta}{\alpha}(\frac{t-\eta}{\alpha})^{\beta-1} \tag{1.33}$$

$$R(t) = \exp -(\frac{t-\eta}{\alpha})^{\beta} \tag{1.34}$$

1.2.3 Évaluation de la fiabilité des systèmes

Après avoir introduit les principales lois modélisant la fiabilité des composants, nous nous intéressons à l'évaluation de la fiabilité des systèmes comportant plusieurs composants. En effet, la fiabilité d'un système donné dépend de la manière dont les entités constituant le système sont inter-connectées. Dans ce cadre, deux types de systèmes sont à distinguer, les systèmes ayant une structure élémentaire et ceux ayant une structure complexe. Une structure élémentaire est composée d'un ensemble de composants indépendants placés en série, en parallèle ou toutes combinaisons possibles entre série et parallèle. En revanche, un système est dit de structure

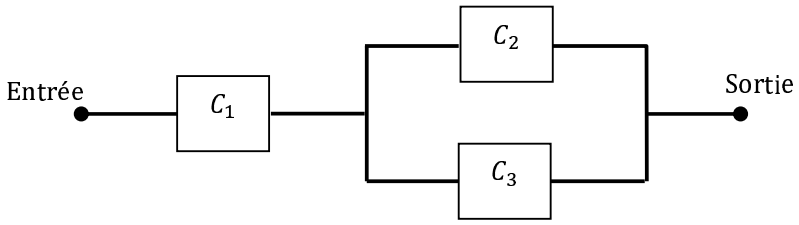

FIGURE 1.5 – Système à structure simple

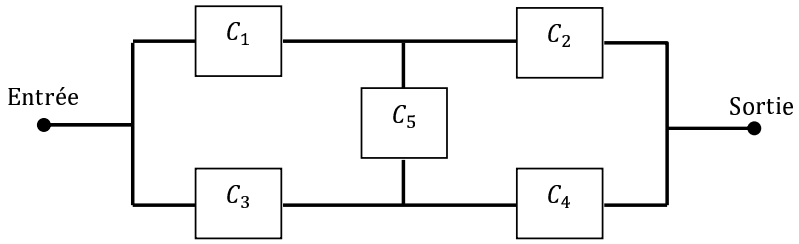

FIGURE 1.6 – Système à structure complexe

complexe si les composants constituant ce dernier ne peuvent pas être décomposés en structure élémentaire.

Les figures (1.5) et (1.6) illustrent respectivement un exemple de diagramme de fiabilité pour un système à structure élémentaire et à structure complexe.

1.2.3.1 Fiabilité des systèmes série

Considérons un système composé de m éléments. Celui-ci est dit de type série si la défaillance de l'un des m composants entraine la défaillance du système global. Le diagramme de fiabilité d'un tel système est représenté dans la Figure (1.7).

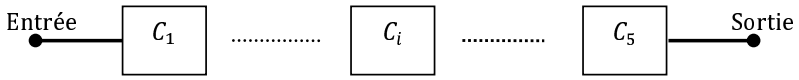

FIGURE 1.7 – Système avec m composants en série

Notons $M_i(t)$ l'événement suivant : "le *ième* élément fonctionne de $t = 0$ à l'instant t". Étant donnée $\mathbb{P}(M_i(t))$ la probabilité d'occurrence de cet évènement. La fiabilité $R(t)$ du système est donnée par,

$$R_{sys}(t) = \mathbb{P}(M_1(t) \cap M_2(t) \cap \dots M_m(t)) \tag{1.35}$$

Si les évènements $M_i(t)$ sont indépendants, la relation équivalente suivante est obtenue,

$$R_{sys}(t) = \prod_{i=1}^{m} R_i(t) \tag{1.36}$$

avec $R_i(t) = \mathbb{P}(M_i(t))$.

1.2.3.2 Fiabilité des systèmes parallèle

Le diagramme de fiabilité d'un système est parallèle (cas de la redondance active) si la panne des m composants est nécessaire pour entrainer la panne du système global, voir Figure (1.8).

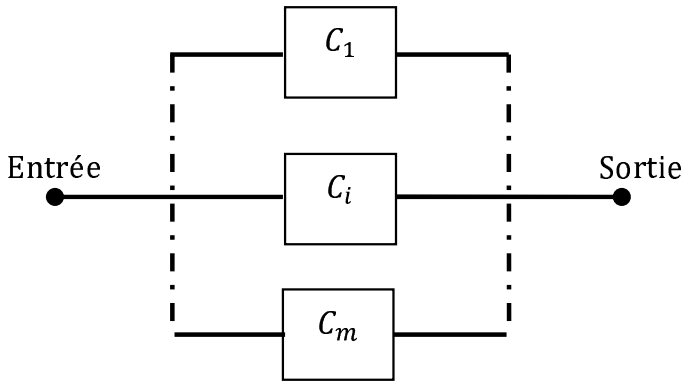

FIGURE 1.8 – Système avec m composants en parallèle

Avec les notations précédentes, la fiabilité du système s'exprime par :

$$R_{sys}(t) = \mathbb{P}(M_1(t) \cup M_2(t) \cup \ldots \cup M_m(t)) = 1 - \mathbb{P}(\bar{M}_1(t) \cap \ldots \cap \bar{M}_m(t)) \quad (1.37)$$

où $\mathbb{P}(\bar{M}_i(t)) = 1 - \mathbb{P}(M_i(t))$.

Ainsi, l'expression équivalente suivante est obtenue :

$$R_{sys}(t) = 1 - \prod_{i=1}^{m}(1 - R_i(t)) \quad (1.38)$$

1.3 Tolérance aux fautes et fiabilité

Afin de répondre aux différents besoins liés aux nouveaux impératifs de la commande (stabilité, précision,... etc) et de la sûreté de fonctionnement des systèmes (disponibilité, fiabilité,... etc), nous nous intéressons à la synthèse de nouvelles lois de commande tolérante aux fautes garantissant la fiabilité des systèmes.

1.3.1 Fondements et Motivations

La sûreté de fonctionnement a été et restera un objectif important dans beaucoup de domaines tels que l'aéronautique, l'automobile, et l'aérospatial. Le rapport annuel de l'Agence Européenne de la Sécurité Aérienne daté de 2007 (EASA, 2007) montre l'évolution des accidents mortels dans le transport aérien. En effet, la figure (1.9) présente le pourcentage d'accidents répartis dans plusieurs catégories. Parmi les catégories présentant un taux important, nous trouvons *la panne ou le dysfonctionnement d'un système ou d'un composant*. Des situations anormales et le vieillissement des matériaux peuvent provoquer des défauts au niveau des actionneurs. L'apparition du défaut peut produire des accidents catastrophiques comme

par exemple l'explosion de la navette américaine Columbia en Février 2003. En revanche, nous apprenons des incidents comme celui du vol 232 à Sioux City en 1989 de Kalita Air freighter à Detroit en 2004 ou aussi l'incident du DHL Freighter à Baghdad en Novembre 2003, que les pilotes peuvent réussir partiellement l'atterrissage lorsque la panne ou le dysfonctionnement n'empêche pas la commandabilité du système où un certain niveau de performance peut encore être atteint.

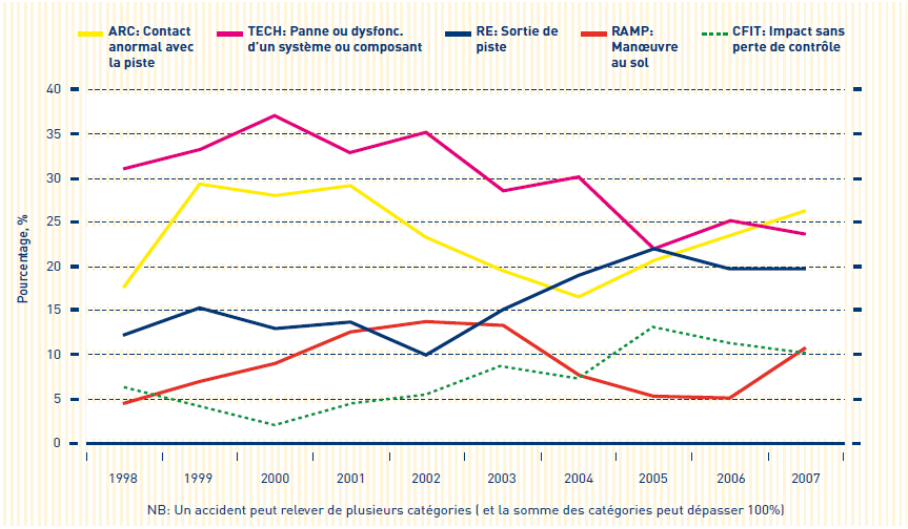

FIGURE 1.9 – Pourcentage et type d'accidents

Afin de réduire le niveau de risque et contribuer à la synthèse de systèmes tolérants aux fautes garantissant la fiabilité, il est intéressant de prendre en compte dans la synthèse des lois de commande, la dégradation, le vieillissement et l'état de santé des composants importants tels que les actionneurs. En effet, les indicateurs de fiabilité sont des outils utilisés pour évaluer les performances d'un système aux différentes étapes de sa vie. En phase de conception, les indicateurs de fiabilité sont utilisés pour répondre au cahier des charges. Au niveau de la fabrication des composants, ils consistent à s'assurer que les prescriptions du cahier des charges sont bien respectées. Au niveau de l'exploitation, et spécifiquement pour les systèmes commandés en ligne, les indicateurs de fiabilité peuvent fournir une estimation sur l'état de santé des composants et l'évolution de leur dégradation en fonction des paramètres extérieurs ou des contraintes d'utilisation.

Dans une boucle de contrôle, les efforts désirés sont calculés par des contrôleurs et appliqués sur le système par les actionneurs. La fiabilité des actionneurs et leur état de santé peuvent jouer un rôle crucial dans le choix de la stratégie de commande appliquée en ligne afin d'augmenter la durée de vie du système reconfigurable. En effet, les actionneurs sont les responsables de la liaison entre les lois de commande calculées et les actions physiques appliquées sur le processus. C'est pourquoi ils sont connus sous le nom d'éléments de contrôle final (Isermann, 2006). L'importance est telle, que les défauts sur les actionneurs ainsi que leur vieillissement sont souvent la cause majeure de la détérioration des performances d'un système de commande, voir même la panne du système global (Zhang et Jiang, 2003). Dans le contexte

de la tolérance aux fautes, les actionneurs représentent un élément principal et très sensible dans la quantification des capacités du système à tolérer des situations anormales. La relation coût/fiabilité des actionneurs sur les systèmes est inférieure à celle des capteurs, puisque les capteurs sont dans la plupart des cas moins chers et plus fiables (Zhao et Jiang, 1998; Zhang et Jiang, 2002a). A noter que les observateurs peuvent être utilisés pour mesurer les variables afin d'obtenir une redondance analytique fiable (Chen et Patton, 1999; Isermann, 2006), permettant aussi de remplacer la fonction des capteurs réels.

Les travaux proposés dans cette thèse consistent à utiliser des informations sur la fiabilité des actionneurs dans la synthèse de la loi de commande. L'objectif est de garantir un meilleur niveau de fiabilité du système global en régime nominal et dans un fonctionnement dégradé par une gestion optimale des actionneurs. Le schéma de principe est donné dans la figure (1.10).

Comme souligné par (Zhang et Jiang, 2008), cette problématique est parmi les sujets de recherche ouverts dans le domaine de la commande tolérante aux fautes. Peu de travaux ont été développés et proposés dans la littérature pour intégrer des informations sur la fiabilité des composants dans la synthèse de systèmes de commande. Afin d'appréhender les travaux existants, nous présentons les travaux effectués dans ce sens par les communautés scientifiques contrôle et fiabilité.

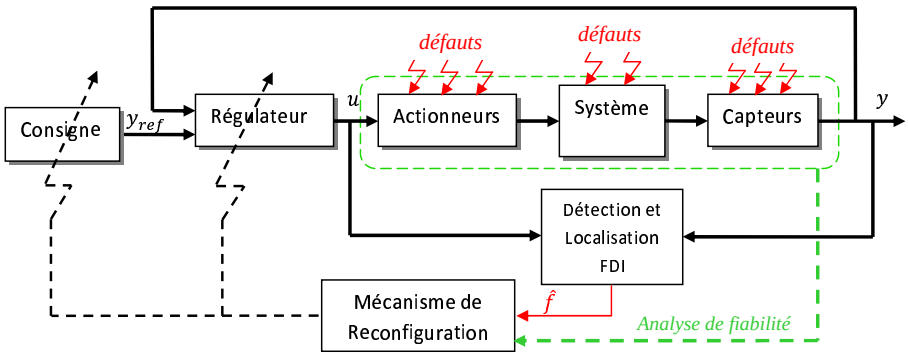

FIGURE 1.10 – Schéma de principe de la commande AFTC proposée

1.3.2 Approche pour la sélection d'une configuration optimale basée sur l'analyse de fiabilité

Dans le travail de (Wu *et al.*, 2002), un algorithme basé sur l'analyse hors ligne de fiabilité est proposé pour le choix d'une configuration optimale des systèmes reconfigurables (Wu *et al.*, 2002; Wu, 2002). Les systèmes sont composés de plusieurs sous-systèmes placés en série. Chaque sous-système est constitué de plusieurs composants et possède une multitude de configuration assurant un objectif ou une fonction locale. Une fiabilité $R_i(t)$ et un indice de coût financier $C_i(R_i(t))$ sont associés à chaque sous-système suivant le nombre de composants utilisés. L'objectif de l'approche est de sélectionner en ligne une configuration optimale maximisant la fiabilité globale du système sous contrainte d'un coût à respecter. Ce problème

est reformulé en un problème d'allocation de fiabilité où la solution est proposée en utilisant la programmation dynamique. La durée de vie de chaque configuration est évaluée en utilisant un processus Markovien.

La fiabilité du système global $R(t)$ est calculée comme suit :

$$R(t) = \prod_{i=1}^{n} R_{i,j}(t) \tag{1.39}$$

où $R_{i,j}(t)$ est la fiabilité du sous système i utilisé dans la configuration j. La fiabilité du sous système i suivant la configuration j est donnée par :

$$R_{i,j}(t) = \sum_{k=1}^{K} p_k^{i,j}(t) \tag{1.40}$$

où $p_k^{i,j}$ est la probabilité que le sous système i reste dans l'état de fonctionnement k du processus Markovien constitué de K états. Les états considérés sont des états absorbants où un seul défaut affectant le système conduit à la panne du système global.

Le coût associé de chaque sous système $C_{i,j}(t)$ est évalué en fonction du coût initial de ses composants $A^{i,j}$ et le coût de défaillance $F_k^{i,j}$ associé à un état k :

$$C_{i,j}(t) = A^{i,j} + \sum_{k=1}^{K} F_k^{i,j} p_k^{i,j}(t) \tag{1.41}$$

Ainsi, le coût de la j^{eme} configuration est donné par :

$$C_j(t) = \sum_{i=1}^{n} C_{i,j}(t) \tag{1.42}$$

La configuration optimale adoptée est celle ayant une fiabilité globale $R(T_d)$ maximale en respectant un coût C^* pour une durée de vie T_d.

Dans cette approche, les performances désirées du point de vue commande n'ont pas été considérées. Le nombre des sous systèmes est fixe. Les fonctions (objectifs) associées sont supposées atteignables quelque soit le nombre de composants utilisés. Ainsi, les états dégradés modélisant le fonctionnement du système affecté par un défaut (ne conduisant pas à la panne totale du système) ne sont pas considérés.

1.3.3 Méthode de reconfiguration basée sur la redondance matérielle et la fiabilité des composants

Ce travail a été proposé par (Staroswiecki et Hoblos, 2004). Dans cette stratégie, un système reconfigurable est considéré par sa présentation d'état comme suit :

$$\begin{array}{ll} \dot{x}(t) & = f(x(t), u(t)) \\ y(t) & = g(x(t)) \\ z(t) & = h(x(t)) \end{array} \tag{1.43}$$

où, $x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ le vecteur de commande, $y \in \mathbb{R}^p$ le vecteur de sorties mesurées et $z \in \mathbb{R}^q$ le vecteur des états à estimer. L'ensemble des capteurs disponibles dans le système est noté I. Soit $J \subseteq I$ un sous ensemble de capteurs, la relation suivante peut être introduite :

$$P(z/J) = \begin{cases} 1 & si\ z\ est\ observable\ utilisant\ J \\ 0 & ailleurs \end{cases}$$

où $P(z/J)$ est la probabilité d'observer les variables $z(t)$ en utilisant la configuration (ou le sous ensemble de capteurs) J.

Le principe consiste à chercher la meilleure configuration de capteurs J^* possédant une fiabilité $R(z/J_0, T) \geq R^*$, en temps moyen de non-observabilité $MTTFO(z/J_0) \geq MTTFO^*$ et permettant d'observer les variables $z(t)$. La fiabilité des capteurs est évaluée pour une durée de fonctionnement T en respectant des degrés de redondance donnés. En effet, $R(z/J_0, T)$ est la probabilité que les variables $z(t)$ soient observables à l'instant t, sachant qu'elles étaient observables à $t = t_0$ en utilisant la configuration J_0. Cette mesure est évaluée pour un ensemble donné $K \subseteq J_0$ comme suit :

$$R(z/K, t) = P(z/K).R(K, t)$$

où $R(K, t)$ est la probabilité qu'aucun capteur de K ait une défaillance à l'instant t. Pour des capteurs identiques, $R(K, t)$ peut être calculée comme suit,

$$R(K, t) = \prod_{k \in K} R_k(t) \prod_{k \notin K} (1 - R_k(t))$$

avec $R_k(t) = e^{-\lambda_k t}$ la fiabilité du k^{eme} capteur possédant un taux de défaillance constant λ_k.

Le temps moyen de non-observabilité est donné par :

$$MTTFO(z/J_0) = \int_0^\infty R(z/J_0, t)dt$$

avec

$$R(z/J_0, t) = \sum_{K \subseteq J_0} P(z/K).R(K, t)$$

est la fiabilité de l'ensemble J_0 contenant tous les sous-ensembles K possibles.

Cette approche est une étude hors ligne proposée sans tenir compte des conditions de fonctionnement dégradé des capteurs. Les états considérés sont : état de marche ou état de panne. Dans le même esprit, une méthode intégrant des approches FTC actives et passives a été récemment proposée afin de sélectionner une configuration optimale des actionneurs redondants en ligne (Staroswiecki et Berdjag, 2010).

1.3.4 Méthode de reconfiguration optimale vis-à-vis de la fiabilité du système global

Le travail proposé dans (Guenab, 2007) porte sur la synthèse d'une méthode de reconfiguration intégrant la fiabilité des composants. La tâche de reconfiguration

permet d'amener le système dans un état de fonctionnement assurant les performances désirées tout en préservant la stabilité. Sous l'hypothèse qu'il existe plusieurs structures de fonctionnement résultant de la déconnexion des sous systèmes défaillants, chaque structure impose des nouvelles conditions de fonctionnement et par conséquent une nouvelle valeur de la fiabilité et du coût. Le système global considéré est donné par :

$$\begin{cases} \dot{x}(t) & = Ax(t) + Bu(t) \\ y(t) & = Cx(t) \\ \gamma_g(t) & = h(y(t)) \end{cases}$$

où $x \in \mathbb{R}^n$, $u \in R^m$ et $y \in \mathbb{R}^p$ représentent respectivement le vecteur d'état, de la commande et de sortie du système global. γ_g est l'évolution des objectifs désirés globaux en fonction des sorties. Le système considéré est supposé être composé de n sous systèmes indépendants (au sens dynamique) ou inter-connectés, chacun décrit selon la représentation d'état suivante :

$$\begin{cases} \dot{x}_i(t) & = A_i x_i(t) + B_i u_i(t) \\ y_i(t) & = C_i x_i(t) \end{cases} \quad , i = 1 \ldots, n$$

Chaque sous système possède son propre régulateur utilisant une loi de commande donnée de retour d'état. Sous l'hypothèse qu'il existe M configurations (structures) possibles $S^m (m = 1, \ldots, M)$, et chaque configuration S^m contient n_m sous systèmes permettant d'assurer les objectifs globaux correspondants γ_g^m, l'approche proposée consiste à choisir la meilleure configuration optimale S^{opt} sous contrainte de fiabilité globale R_g^* et de coût financier C_g^*. La fiabilité d'une structure donnée $R_g^m(t)$ et le coût financier correspondant C_g^m sont calculés en fonction de la fiabilité $R_i(t)$ et le coût C_i des composants constituant S^m.

- La première approche proposée traite uniquement les performances statiques. La détermination de la structure optimale se fonde sur une estimation de la fiabilité et des coûts des composants. Le critère de choix adopté est donné par :

$$S^{opt} = arg \min_{S^m} \quad J_{Sta}^m, \quad m = 1, \ldots, M$$

avec $J_{Sta}^m = \left| \frac{\gamma_g^{nom} - \gamma_g^m}{\gamma_g^{nom}} \right|$. En fait, γ_g^{nom} représente l'objectif global du système nominal, sous sa structure nominale. γ_g^m est l'objectif global du système reconfiguré sous la structure m.

- Une seconde méthode utilisant les performances des régulateurs est développée. La méthode de la pseudo-inverse PIM est utilisée pour synthétiser les régulateurs. Des modifications de la méthode PIM ont été proposées afin d'assurer la stabilité du système et d'atteindre des objectifs dynamiques désirés. Dans ce cadre, un indice des performances dynamiques est intégré dans le critère de choix de la structure optimale. L'indice de performance adopté dans cette méthode est donné par :

$$J_{dyn}^m = \max_i \left(\max_j \left(\left| \frac{\tau_j^{nom} - \tau_j^m}{\tau_j^{nom}} \right| \right) \right), \quad i = 1 \ldots, n_m.$$

où $\tau_j^m (j = 1, \ldots, k_i)$ sont les k_i valeurs propres des sous systèmes i calculées en ligne pour une structure m.

- Les deux méthodes développées précédemment ont été intégrées afin de définir une stratégie tolérante aux défauts. Elle est appliquée sur un système hydraulique et thermique à 3 cuves. L'indice de choix de la configuration optimale dans ce cas est considéré comme suit :

$$S^{opt} = arg \min_{S^m} \quad J^m, \quad m = 1, \ldots, M$$

avec $J^m = \omega J_{sta}^m + (1 - \omega) J_{dyn}^m$. $\omega \in [0, 1]$ est un paramètre de pondération à choisir.

1.4 Conclusion

Afin de mettre en exergue l'intérêt de nos travaux, nous avons exposé les différents travaux de recherche effectués dans le domaine des systèmes tolérants aux défauts exploitant l'analyse de la fiabilité. Dans un premier temps, nous avons présenté les systèmes tolérants aux défauts, leurs objectifs, leurs structures ainsi que les types de systèmes tolérants aux défauts. Dans un second temps, nous avons rappelé les concepts de la fiabilité. Ensuite, nous avons présenté une synthèse bibliographique des travaux de recherche intégrant l'analyse de la fiabilité dans les systèmes tolérants aux défauts.

Bien que la commande tolérante aux fautes ait comme objectif d'améliorer la sûreté de fonctionnement des systèmes, peu de travaux intégrant les outils de la fiabilité dans la synthèse des lois de commande tolérante aux fautes existent. Nous avons constaté que la plupart des méthodes de synthèse des lois de commande pour les systèmes tolérants aux défauts ne prennent en compte que des objectifs à court terme, en particulier la stabilité et les performances dynamiques. Dans les chapitres suivants, nous allons apporter des solutions pour contribuer à la synthèse des lois de commande tolérante aux fautes garantissant la fiabilité des systèmes.

Chapitre 2

Analyse de la Reconfigurabilité des Systèmes Garantissant la Fiabilité

2.1 Introduction

Les systèmes tolérants aux fautes sont conçus pour tolérer des types de défauts bien déterminés et garantir les performances désirées même dans un fonctionnement dégradé. Dans le cas des approches actives, la stratégie appliquée après l'apparition du défaut dépend directement de la sévérité de ce dernier et de son impact sur les propriétés fonctionnelles du système, telles que la commandabilité, l'observabilité, l'énergie disponible,...etc. Dans ce cadre, l'accommodation du défaut est utilisée. Elle consiste à modifier en ligne les paramètres du contrôleur sans changer les relations entrées/sorties. En revanche, si l'effet du défaut n'est pas accommodable, la reconfiguration ou la restructuration du système de commande est nécessaire afin de récupérer les fonctionnalités du système et assurer les performances désirées. Dans le but de connaître a priori la limite pour laquelle le système peut assurer ses fonctionnalités et choisir ainsi la stratégie de tolérance à appliquer, la mesure des capacités de tolérance aux défauts du système est nécessaire. Nous parlons donc de la reconfigurabilité du système. Dans cette étude, la probabilité que, après accommodation des défauts, le système est capable d'assurer les performances désirées jusqu'à la fin de la mission est introduite sous forme d'une contrainte de fiabilité. L'étude de reconfigurabilité consiste donc à mesurer les capacités de tolérance aux défauts pour un scénario donné, tout en satisfaisant à une durée de mission bien déterminée.

2.2 Reconfigurabilité des systèmes linéaires

2.2.1 Concept de base et propriétés

Dans cette étude, les systèmes modélisés sous forme d'un modèle linéaire invariant dans le temps sont considérés comme suit,

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{2.1}$$

où $x(t) \in \mathbb{R}^n$ le vecteur d'état, $u(t) \in \mathbb{R}^m$ le vecteur des entrées de commande, $y(t) \in \mathbb{R}^p$ le vecteur de sortie et $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}, C \in \mathbb{R}^{p\times n}$ des matrices constantes caractérisant le système. Avant de présenter la modélisation du système en mode de fonctionnement dégradé et introduire l'étude de reconfigurabilité, nous rappelons quelques définitions et propriétés nécessaires pour l'étude proposée.

Définition 2.1 *Un système est dit entièrement commandable si par une action sur l'entrée, n'importe quel point de l'espace d'état peut être atteint en un temps fini.*

Pour un temps fini t_M, la commandabilité d'un système linéaire peut être étudiée grâce à la matrice *Grammien* donnée par :

$$W_c(t_M) = \int_0^{t_M} e^{At} B B^T e^{A^T t} dt \tag{2.2}$$

où t_M est l'horizon de commande pendant lequel la matrice $W_c(t_M)$ est mesurée. $W_c(t_M) > 0$ est une matrice symétrique positive. En effet, (2.2) est connue sous le nom de *Grammien partiel* ou aussi *Grammien transitoire de commandabilité.*

Ainsi, la commandabilité d'un système linéaire peut être évaluée par le théorème suivant :

Théorème 2.1 *Le système linéaire (2.1) est commandable si et seulement si la matrice (2.2) est inversible pour au moins un temps t_M donné : la paire (A, B) est dite commandable.*

Le théorème (2.1) permet d'étudier la commandabilité du système sans évaluer la stabilité. Or, si la matrice (2.2) existe pour $t_M \to \infty$, la stabilité du système peut être évaluée dans ce cas en fonction du *Grammien de commandabilité* défini comme suit :

$$W_c = \lim_{t_M \to \infty} W_c(t_M)$$

En effet, si la matrice A est asymptotiquement stable, le Grammien de commandabilité W_c est aussi solution de l'équation de Lyapunov suivante :

$$AW_c + W_c A^T + BB^T = 0 \tag{2.3}$$

Définition 2.2 *Une matrice carré est asymptotiquement stable, dite Hurwitz, si ses valeurs propres sont à partie réelle négative.*

De ce fait, si le système (2.1) est instable, la solution de (2.3) n'existe pas. De même il existe une description similaire dans le cas de l'observabilité du système. Par dualité, le théorème suivant est obtenu :

Théorème 2.2 *Le système linéaire (2.1) est observable si et seulement si la matrice symétrique positive*

$$W_o(t) = \int_0^{t_M} e^{A^t t} C^t C e^{At} dt \tag{2.4}$$

est inversible pour au moins un t_M donné. On dit alors que la paire (A, C) est observable.

De même, si le Grammien d'observabilité transitoire (2.4) existe pour $t_M \to \infty$, alors :

$$W_o = \lim_{t_M \to \infty} W_o(t_M)$$

et l'on appelle *Grammien d'observabilité* W_o. Cette matrice est la solution unique de l'équation de Lyapunov suivante :

$$A^T W_o + W_o A + C^T C = 0 \tag{2.5}$$

Remarque 2.1 *Les propriétés énoncées précédemment de commandabilité et d'observabilité sont aussi garanties dans le cas discret.*

En effet, la commandabilité des systèmes linéaires discrets est obtenue à partir de la résolution de l'équation de récurrence définie par :

$$\begin{cases} x_{k+1} = A_d x_k + B_d u_k \\ y_k = C_d x_k \end{cases} \tag{2.6}$$

où la période d'échantillonnage est considérée implicitement dans les vecteurs d'état $x_k \in \mathbb{R}^n$, de l'entrée de commande $u_k \in \mathbb{R}^m$ ainsi que du vecteur de sortie $y_k \in \mathbb{R}^p$. Les matrices caractérisant la dynamique du système (2.6) possèdent les mêmes dimensions que dans le cas continu (2.1).

Considérons l'état initial $x_0 = x(t_0)$, l'évolution de l'état x_k en fonction des entrées de commande $u_k,\ k = 0, 1, \ldots, q$ est donnée par :

$$\begin{array}{ll} x_1 & = A_d x_0 + B_d u_0 \\ x_2 & = A_d^2 x_0 + A_d B_d u_0 + B_d u_1 \\ \vdots & \quad \vdots \\ x_q & = A_d^q x_0 + A_d^{q-1} B_d u_0 + \ldots + B_d u_{q-1} \end{array} \tag{2.7}$$

qui peut s'écrire sous forme matricielle :

$$x_q - A_d^q x_0 = \sum_{i=0}^{q-1} A_d^{q-i-1} B_d u_i = [B_d \quad A_d B_d \quad \ldots \quad A_d^{q-1} B_d] \begin{bmatrix} u_{q-1} \\ u_{q-2} \\ \vdots \\ u_0 \end{bmatrix} \tag{2.8}$$

Propriété 2.1 *L'état final donné par x_q est obtenu pour une séquence de commande $u_i,\ \ i = 0, \ldots, q-1$, solution de l'équation (2.8) si la matrice*

$$\mathcal{C}_d = [B \quad AB \quad \ldots \quad A^{q-1} B] \tag{2.9}$$

est de rang n garantissant ainsi la commandabilité du système.

Comme dans le cas continu, le théorème suivant définissant la commandabilité des systèmes discrets est obtenu :

Théorème 2.3 *Le système linéaire discret (2.6) est commandable si et seulement si la matrice symétrique W_c^d existe, où*

$$W_c^d = \mathcal{C}_d \mathcal{C}_d^T = \sum_{i=0}^{\infty} A_d^i B_d B_d^T (A_d^i)^T \tag{2.10}$$

En effet, la matrice W_c^d appelée aussi *Grammien de commandabilité* dans le cas discret est la solution de l'équation de Lyapunov suivante :

$$W_c^d = A_d W_c^d A_d^T + B_d B_d^T \tag{2.11}$$

Par dualité, le Grammien d'observabilité dans le cas discret W_o^d est obtenu sous la forme suivante :

$$W_o^d = A^T W_o^d A + C^T C \tag{2.12}$$

2.2.2 Problématique

Dans un mode de fonctionnement donné, la vérification de la commandabilité permet le transfert de l'état du système $x(t)$ d'un état initial $x(0)$ vers un état désiré x_M par un signal de commande $u(t)$ d'énergie finie. Pour illustrer la relation entre la propriété de reconfigurabilité et l'énergie consommée dans un mode de fonctionnement défaillant, le théorème suivant est donné :

Théorème 2.4 *(Moore, 1981) L'énergie minimale $\mathcal{E}_{min}$ consommée par le système (2.1), nécessaire pour atteindre l'état final $x_M = x(t_M)$ depuis une condition initiale nulle $x(t_0) = 0$ est donnée par :*

$$\mathcal{E}_{min} = \min_{x(t_0)=0, x_M=x(t_M)} \left(\int_{t_0}^{\infty} u^T(t)u(t)dt \right) = x_M^T W_c^{-1}(t_M) x_M \tag{2.13}$$

où W_c est le Grammien de commandabilité calculé à partir de (2.3).

En effet, l'énergie $\int_{t_0}^{\infty} u^T(t)u(t)dt$ limite l'ensemble des états atteignables par le système. Dans le cas où la condition de stabilité est vérifiée, la quantité $x_M W_c^{-1} x_M$ représente une hyperellipsoïde qui englobe les états atteignables en utilisant l'entrée de commande $u(t)$. Ainsi, une valeur grande de $\mathcal{E}_{min}$ signifie qu'il existe des états difficiles à commander nécessitant une énergie importante pour les exciter. D'autre part, une plus petite valeur de $\mathcal{E}_{min}$ signifie que les états sont aisément commandables et par conséquent plus sensibles à l'excitation (Wicks et Decarlo, 1990).

En considérant le système (2.1) stable, les valeurs propres de la matrice W_c^{-1} peuvent être associées aux états du système. Les valeurs propres de grande amplitude correspondent bien aux états difficilement commandables. Ainsi, les états associés aux valeurs propres de petite amplitude correspondent aux états facilement commandables.

Par conséquent, les plus grands axes de l'hyperellipsoïde correspondent aux états facilement commandables. Ces derniers sont donnés par les plus petites valeurs propres de W_c^{-1}. De même, les plus petits axes de l'hyperellipsoïde correspondent aux états les moins sensibles à l'excitation et sont donnés par les plus grandes valeurs propres de W_c^{-1}.

Comme montré dans (Moore, 1981; Wicks et Decarlo, 1990), nous pouvons établir les limites énergétiques du système (2.1) sans considérer un type spécifique de $u(t)$, mais seulement son énergie décrite par l'équation (2.13). En présence d'un défaut, la propriété de commandabilité diminue et l'axe de l'hyperellipsoïde associé à l'état le plus excité décroit en amplitude en raison du défaut.

En effet, la valeur propre maximale de W_c^{-1} représente l'état le plus susceptible de se dégrader en présence d'un défaut. En se basant sur les limites énergétiques du système et comme montré dans (Staroswiecki, 2002), la reconfigurabilité peut être considérée comme la capabilité du système défaillant à préserver la propriété de commandabilité en tenant compte de l'occurrence du défaut.

Définition 2.3 *Le système (2.1) est dit (complètement) reconfigurable si la propriété de commandabilité du système nominal est préservée dans le cas défaillant en respectant un certain niveau d'énergie consommée.*

En fait, il s'agit de mesurer les limites de fonctionnement du système en état dégradé pour accommoder les défauts. Les défauts considérés sont les défauts de type actionneur. Afin de détailler l'effet des défauts actionneurs sur le système (2.1), nous considérons $u(t)$ la loi de commande calculée par le contrôleur et $u_m(t)$, la commande manipulée représentant les actions de commande appliquées réellement sur le système.

Propriété 2.2 *En fonctionnement nominal, sous l'hypothèse que la dynamique des actionneurs est négligée, les actionneurs reproduisent fidèlement les actions imposées par le contrôleur $u(t) = u_m(t)$. Les actionneurs sont, dans ce cas, considérés* 100% *effectifs. En revanche, après l'apparition d'un défaut, l'effet des actionneurs diminue et la relation entre la loi de commande $u(t)$ et les actions de commande $u_m(t)$ est partiellement interrompue (Zhang et Jiang, 2003).*

Ainsi, deux types de défaut actionneur peuvent être distingués indépendamment de la commande : perte d'efficacité et biais. Ces défauts sont représentés sous la forme générale suivante :

$$u_m(t) = u(t) + \Gamma(u_b - u(t)) \tag{2.14}$$

avec $\Gamma = diag(\gamma_1, \gamma_2, \ldots, \gamma_m)$ où $\gamma_i \in [0, 1]$ est appelé le facteur de perte d'efficacité du i^{eme} actionneur. u_b représente un biais de l'actionneur souvent dû à la calibration commande/actionneur.

La relation (2.14) modélisant les défauts multiplicatifs et additifs peut être reformulée comme suit :

$$u_m(t) = (I_m - \Gamma)u(t) + \Gamma u_b \tag{2.15}$$

En effet, pour $\gamma_i = 0$, $u_m(t) = u(t)$ et le i^{eme} actionneur fonctionne correctement. Si $0 < \gamma_i < 1$ et $u_b = 0$, une perte d'efficacité du i^{eme} actionneur est considérée. Cette dernière décrit une réaction partielle de l'actionneur au signal de commande, soit une certaine dégradation dans l'action appliquée réellement sur le système. D'autre part, si $0 < \gamma_i < 1$ et $u_b \neq 0$, un biais fixe est ajouté à la commande manipulée.

Par contre si $\gamma_i = 1$ et $u_b \neq 0$ un blocage physique de l'actionneur en une position fixe est considéré (actionneur bloqué). Ce défaut entraine une incapacité à commander l'actionneur en question à cause du biais fixe provoqué dés l'apparition du défaut. Autrement pour $\gamma_i = 1$ et $u_b = 0$, une panne totale de l'actionneur est considérée où ce dernier aura comme action $u_m(t) = 0$.

Dans ce travail, la perte d'efficacité des actionneurs provoquant une dégradation significative de la fiabilité du système est considérée. En effet, l'occurrence d'un défaut augmente la probabilité de perdre totalement l'actionneur dégradé et diminue sa durée de vie résiduelle de base. En se basant sur (2.15) et après l'apparition du défaut à l'instant $t = t_f$, le système (2.1) peut être modélisé par :

$$\begin{cases} \dot{x}(t) = Ax(t) + B_f u(t) \\ y(t) = Cx(t) \end{cases} \tag{2.16}$$

où B_f s'écrit en fonction de la matrice d'action de commande nominale B et les facteurs de perte d'efficacité Γ comme suit,

$$B_f = B(I_m - \Gamma), \quad \Gamma = \begin{pmatrix} \gamma_1 & & & 0 \\ & \gamma_2 & & \\ & & \ddots & \\ 0 & & & \gamma_m \end{pmatrix} \tag{2.17}$$

Pour les systèmes linéaires invariants dans le temps, l'évaluation de la reconfigurabilité est basée sur la limitation de l'énergie consommée dans des situations défaillantes (Staroswiecki, 2002). Cette dernière est mesurée par le Grammien de commandabilité. Cependant, pour estimer les capacités du système dégradé à assurer ses fonctionnalités jusqu'à la fin de la mission, il est nécessaire de prédire la fiabilité du système accommodé à la fin de la mission d'où la nécessité de définir la relation entre tolérance aux défauts et fiabilité des actionneurs. Dans ce contexte, étant donné un mode de fonctionnement nominal, les limites de reconfigurabilité peuvent être définies par le Grammien de commandabilité tout en respectant un niveau de fiabilité désiré.

2.2.3 Reconfigurabilité basée sur le Grammien de Commandabilité

Comme proposé dans (Staroswiecki, 2002), le Grammien de commandabilité est utilisé dans l'analyse de reconfigurabilité afin d'évaluer la capacité du système défaillant à transférer son état vers l'origine par accommodation avec une consommation d'énergie finie.

L'étude de reconfigurabilité est reformulée en un problème d'optimisation énergétique, minimisant un critère de performance comme suit (Staroswiecki, 2002) :

Critère 2.1 *Minimiser l'énergie*

$$\mathcal{J}(u, x_0) = \int_0^\infty \|u(t)\|^2 \, dt \tag{2.18}$$

transférant $x(0) = x_0$ *à* $x(\infty) = 0$, *où* $x_0 \in \mathbb{R}^n$, *et* $x(\infty) = \lim_{t\to\infty} x(t)$.

avec $\|.\|$ est la norme Euclidienne.

Remarque 2.2 *Un autre critère de performance basé sur une loi de commande spécifique pourra être utilisé (Staroswiecki, 2003). Étant donné que les résultats sont similaires, nous nous limitons au cas général annoncé dans le critère 2.1.*

Pour le système LTI (2.1), la solution de (2.18) est obtenue en se basant sur la théorie de la commande optimale en fonction de l'équation Hamiltonienne comme suit :

$$u(t) = B^T P x(t) \tag{2.19}$$

où P est la solution unique de l'équation de Lyapunov définie par :

$$A^T P + PA = -BB^T \tag{2.20}$$

Pour le critère (2.18), la matrice $P^{-1} = W_c$ représente le Grammien de commandabilité de la loi de commande $u(t)$. En fait, W_c détermine l'énergie nécessaire à consommer pour transférer l'état du système à son origine. La matrice W_c est inversible si la paire (A, B) est commandable. Elle peut être définie analytiquement comme suit :

$$W_c = \int_0^\infty e^{At} BB^T e^{A^T t} dt \tag{2.21}$$

Ainsi, la valeur optimale, solution du critère d'optimisation (2.18) est obtenue dans l'intervalle de temps $[0, \infty)$ comme suit :

$$\mathcal{J}(x_0) = x_0^T W_c^{-1} x_0 \tag{2.22}$$

D'aprés l'équation (2.22), les performances énergétiques du système dépendent de l'état initial x_0.

En effet, $\mathcal{J}(x_0)$ donne une image sur les performances des actionneurs où l'état du système $x(0) = x^*$ susceptible de consommer le plus d'énergie peut être défini comme suit :

$$x^* = \arg\max \mathcal{J}(x_0) \tag{2.23}$$

Propriété 2.3 *Les performances des actionneurs sont évaluées en fonction de la valeur propre maximale de la matrice W_c^{-1}. Cette valeur propre est interprétée comme l'énergie maximale consommée pour transférer l'état du système à l'origine.*

Ainsi, le coût minimum associé est défini comme suit :

$$\mathcal{J}^* = \mathcal{J}(x^*) = \max(\Lambda(W_c^{-1})) \tag{2.24}$$

où $\Lambda(W_c^{-1})$ est l'ensemble des valeurs propres de W_c^{-1}.

Remarque 2.3 *Considérons l'hyperellipsoïde obtenu à partir de W_c^{-1}, la plus grande valeur propre de W_c^{-1} représente l'état le moins excité et donc le plus susceptible de se dégrader en présence de défaut.*

Tenant compte de l'apparition du défaut, le système (2.1) s'écrit comme suit :

$$\begin{array}{ll} \dot{x}(t) = Ax(t) + Bu(t) & t \in [0, t_f) \\ \dot{x}(t) = Ax(t) + B_f u(t) & t \in [t_f, \infty) \end{array} \tag{2.25}$$

Considérons $\mathcal{J}_f(x_0)$ le coût minimum du critère 2.18 associé au système dégradé défini dans (2.16). L'état $x_f = x(t_f)$ est considéré dans ce cas comme l'état initial du système défaillant défini dans l'intervalle de temps $[t_f, \infty)$. En se basant sur le principe d'optimalité de Bellman, le coût minimum $\mathcal{J}_f(x_0)$ peut être obtenu dans un mode de fonctionnement dégradé en fonction de $\gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ par :

$$\mathcal{J}_f(x_0) = \mathcal{J}_{0f} + x_f^T W_c(\gamma)^{-1} x_f \tag{2.26}$$

où $\mathcal{J}_{0f}$ est le coût associé au système entre $t = 0$ et $t = t_f$. $W_c(\gamma)$ est la solution de la fonction de Riccati (2.27) définie pour le système défaillant $(A, B_f(\gamma))$:

$$AW_c(\gamma) + W_c(\gamma)A^T = -B_f(\gamma)B_f^T(\gamma) \tag{2.27}$$

D'autre part, la valeur du coût $\mathcal{J}_{0f}$ nécessaire pour transférer le système d'un état initial x_0 en x_f peut être exprimée par :

$$\mathcal{J}_{0f} = \mathcal{J}(x_0) - x_f^T W_c^{-1} x_f \tag{2.28}$$

Cependant, en intégrant (2.28) dans (2.26), le coût associé au système accommodé tenant compte des conditions initiales (2.22) est obtenu comme suit :

$$\mathcal{J}_f(x_0) = x_0^T W_c^{-1} x_0^T + x_f^T (W_c(\gamma)^{-1} - W_c^{-1}) x_f \tag{2.29}$$

Corollaire 2.2.1 *Pour $t_f = \infty$, le défaut n'est pas considéré, $W_c(\gamma) = W_c$ et le coût associé est celui du système nominal $x_0^T W_c^{-1} x_0$. Cependant, pour $t_f = 0$, l'occurrence du défaut est considérée au départ de fonctionnement. Le coût énergétique associé dans ce cas est $x_f^T W_c^{-1}(\gamma) x_f$.*

Comme prouvé dans (Staroswiecki, 2002), la tolérance aux défauts peut être évaluée suivant la définition suivante :

Définition 2.4 *(Staroswiecki, 2002) Un système est dit tolérant aux fautes pour un instant d'occurrence du défaut $t = t_f$ et un état initial x_0 si et seulement si le problème d'accommodation a une solution énergétique admissible.*

Définition 2.5 *Dans le cas défaillant, la solution de la commande tolérante aux fautes est admissible en terme d'énergie tenant compte de l'état initial x_0 si et seulement si :*

$$\mathcal{J}_f(x_0) \leq \mathcal{J}_{pth} \tag{2.30}$$

où $\mathcal{J}_{pth}$ est un coût énergétique prédéfini associé à l'état accommodable le plus dégradé.

Cependant, la tolérance aux défaut telle qu'elle est définie ici dépend d'une solution dite admissible en fonction de l'instant d'occurrence du défaut t_f (2.30). Par conséquent et comme l'instant de l'occurrence des défauts est inconnu a priori, il est nécessaire d'identifier cet instant en ligne par un module FDI.

En revanche, pour une étude de reconfigurabilité, il est plus intéressant de connaître les limites de fonctionnalité du système hors ligne. Une étude hors ligne permet de spécifier a priori la stratégie de tolérance aux défauts adaptée à chaque situation défaillante présumée et de l'appliquer en ligne.

Dans ce contexte, l'étude de reconfigurabilité pourra être effectuée hors ligne indépendamment de l'instant de l'apparition du défaut $t = t_f$ en considérant la

situation la plus dégradée en terme de temps. Cette dernière est définie pour $t_f = 0$ et $x_f = x_0$. La tolérance aux fautes dans ce cas peut être évaluée hors ligne par l'indicateur énergétique suivant :

$$\sigma(\gamma) = \max \Lambda(W_c^{-1}(\gamma)) \tag{2.31}$$

où $\Lambda(W_c^{-1}(\gamma))$ est l'ensemble des valeurs propres de $W_c^{-1}(\gamma)$ obtenues pour un mode de fonctionnement dégradé défini par $\gamma = (\gamma_1, \gamma_2 \ldots, \gamma_m)$.

Propriété 2.4 *Dans un mode de fonctionnement dégradé, les performances des actionneurs peuvent être caractérisées indépendamment de l'état par la valeur propre maximale de $W_c^{-1}(\gamma)$ interprétée comme l'énergie maximale nécessaire pour transférer les états du système à l'origine.*

Afin d'étudier la reconfigurabilité du système dans le cas défaillant et estimer l'ensemble des défauts qui pourront être accommodés par le système de commande, un indice énergétique de reconfigurabilité est proposé dans (Khelassi *et al.*, 2009b).

Proposition 2.1 *La tolérance aux défauts peut être évaluée en fonction du coût maximal correspondant à l'état admissible le plus dégradé pour lequel le système reste commandable par l'indice :*

$$\rho(\gamma) = \frac{\sigma(\gamma) - \sigma_{min}}{\sigma_{max} - \sigma_{min}} \tag{2.32}$$

où σ_{max} est l'énergie maximale nécessaire pour accommoder l'état le plus dégradé du système et le transférer a son origine. σ_{min} est l'énergie consommée dans le cas nominal $\gamma = 0$ nécessaire pour transférer l'ensemble des états à l'origine.

Par normalisation de l'indicateur énergétique (2.31), la valeur de l'indice (2.32) varie entre 0 et 100%. Ce dernier peut être considéré comme une image de la dégradation des performances du système en terme d'énergie ainsi que sa capacité à accommoder des situations défaillantes.

Lemme 2.1 *Dans un fonctionnement dégradé, la solution de la commande tolérante aux fautes par accommodation est admissible respectant les objectifs de commande si :*

$$\rho(\gamma) \leq \rho_{pth} \tag{2.33}$$

où ρ_{pth} est un seuil énergétique prédéfini qui représente le mode de fonctionnement le plus dégradé acceptable.

L'ensemble des solutions dites admissibles déterminant les modes dégradés accommodables est obtenu en fonction d'un certain niveau énergétique prédéfini. Or, il n'existe pas dans la littérature un indicateur ou un objectif définissant ce dernier. Souvent, la valeur de $\mathcal{J}_{pth}$ (en l'occurrence ρ_{pth}) est imposée dans la phase de conception. Dans la section suivante, la limite énergétique déterminant l'ensemble des défauts admissibles sera définie en fonction d'une durée de vie à assurer (Khelassi *et al.*, 2011d). Cette dernière sera exprimée en terme d'une fiabilité globale du système.

2.3 Reconfigurabilité basée sur l'analyse de fiabilité

L'étude de reconfigurabilité basée sur le Grammien de commandabilité est utilisée pour évaluer les performances du système et sa capacité à tolérer des situations défaillantes. Pour augmenter la sûreté de fonctionnement des systèmes tolérants aux fautes, il est judicieux de mesurer a priori la capacité du système à récupérer ces fonctionnalités jusqu'à la fin de la mission qui lui est assignée. Cet objectif peut être exprimé en fonction d'un critère énergétique respectant un niveau de fiabilité suffisant.

Proposition 2.2 *Le temps de bon fonctionnement d'un système peut être estimé par les lois de fiabilité. Pour contribuer aux systèmes tolérants aux fautes garantissant la fiabilité, le problème de reconfigurabilité est étudié en se basant sur un critère énergétique sous contrainte de fiabilité. L'indicateur énergétique déterminant les limites fonctionnelles du système accommodé (2.33) est obtenu en respectant un niveau de fiabilité désiré.*

$$\begin{array}{l} J(x_0) = \int_0^\infty \|u(t)\|^2 \ dt \\ s.t. \quad R(t) \geq R_{pth} \end{array} \tag{2.34}$$

où $R(t)$ est la fiabilité du système global. R_{pth} est un seuil de fiabilité déterminant la valeur minimale à respecter correspondant à une durée de vie spécifique.

L'objectif de cette partie est de définir le seuil énergétique d'admissibilité ρ_{pth} en se basant sur l'analyse de fiabilité du système pour chaque mode de fonctionnement défaillant. En fait, ρ_{pth} est la normalisation du seuil énergéti-que σ_{pth} nécessaire pour déterminer l'ensemble des modes dégradés admissibles.

2.3.1 Analyse de la fiabilité des systèmes commandables

Comme présenté dans le chapitre précédent, différentes lois peuvent être utilisées pour décrire la fiabilité d'une entité ou d'un système. Dans cette partie nous nous intéressons aux actionneurs dans leur période de vie utile. Cette période est caractérisée, par hypothèse, par une loi de distribution exponentielle ainsi qu'un taux de défaillance λ constant.

En effet, un taux de défaillance est estimé généralement dans un environnement et des conditions de fonctionnement fixes et bien déterminées. Lorsqu'un paramètre interne ou externe d'un composant varie, cela entraine la modification des caractéristiques de fiabilité tel que le taux de défaillance. C'est dans ce contexte que l'étude de reconfigurabilité proposée ici se positionne. En fait, dans une boucle de commande, l'efficacité des actionneurs dépend de l'intensité de la commande et de la sollicitation appliquée. Les caractéristiques de fiabilité de ces derniers varient d'un mode de fonctionnement à l'autre par rapport à la charge appliquée.

Dans ce qui suit, nous allons adapter la modélisation du taux de défaillance des composants ainsi que leurs fiabilités par rapport à la charge appliquée (Khelassi *et al.*,

2009a). En effet, plusieurs formules existent dans la littérature modélisant le taux de défaillance en fonction de la charge (Martorell *et al.*, 1999; Finkelstein, 1999; Toscano et Lyonnet, 2008). Dans ce travail, le modèle proportionnel de Cox introduit dans (Cox, 1972), appelé aussi *Proportional Hazards Model* (Martorell *et al.*, 1999) est adopté.

Hypothèse 2.1 *Le taux de défaillance d'une entité i peut être modélisé comme suit :*

$$\lambda_i = \lambda_i^0 \times g(\ell, \vartheta) \tag{2.35}$$

où λ_i^0 est le taux de défaillance de base du i^{eme} composant, obtenu sous des conditions de fonctionnement bien déterminées. $g(\ell, \vartheta)$ est une fonction modélisant l'effet et l'impact d'un facteur extérieur sur la fiabilité du composant. ℓ et ϑ sont respectivement le facteur considéré et un paramètre dépendant des caractéristiques du composant.

Dans cette étude, les composants concernés par une dégradation sont les actionneurs. Les facteurs considérés sont les lois de commande appliquées, en l'occurrence la charge appliquée sur les différents actionneurs.

Différentes définitions de la fonction $g(\ell, \vartheta)$ existent dans la littérature. La loi exponentielle est la plus utilisée. Cette fonction est liée directement au facteur de dégradation qui est dans notre cas la commande appliquée sur l'actionneur. Pour un fonctionnement nominal, le taux de défaillance intégrant l'effet de la charge sur la fiabilité peut être modélisé comme suit :

$$\lambda_i = \lambda_i^0 \times e^{\beta_i u_i^{moy}} \tag{2.36}$$

où β_i est un paramètre fixe qui dépend des caractéristiques de l'actionneur (Guenab, 2007). u_i^{moy} est un niveau moyen de la commande appliquée durant le fonctionnement de l'actionneur.

Cependant, la fiabilité des actionneurs peut être modélisée en fonction d'un niveau moyen de la commande appliquée comme suit :

$$R_i(t) = e^{-\lambda_i \times t} \tag{2.37}$$

Dans le cadre de l'étude de reconfigurabilité, u_i^{moy} est l'entrée de commande en régime permanent obtenue pour une mission donnée. L'impact de la commande délivrée durant la partie transitoire est négligé étant donné la durée de cette dernière.

2.3.2 Évaluation de la fiabilité en mode de fonctionnement défaillant

Comme illustré dans (Guenab *et al.*, 2006), la valeur estimée du taux de défaillance des actionneurs augmente en fonction de la charge appliquée. La fonction charge est considérée comme un facteur de stress diminuant la durée de vie de l'actionneur. Cependant, après l'apparition d'un défaut, l'actionneur est considéré en mode de fonctionnement dégradé où sa durée de vie et la probabilité que ce dernier reste

opérationnel diminuent. En effet, dans le cadre de la commande tolérante aux fautes, l'occurrence d'un défaut implique l'augmentation de la charge appliquée sur l'actionneur afin d'assurer les actions désirées. Ainsi, un nouveau taux de défaillance peut être estimé en tenant compte du coût énergétique nécessaire pour assurer les performances désirées malgré le défaut. Nous proposons une relation déterminant la fiabilité du composant dans un mode de fonctionnement dégradé obtenue en fonction de la charge nominale.

Considérons la dynamique d'un système nominal autour d'un point de fonctionnement bien déterminé donnée par (2.1). Dans un fonctionnement nominal, les actionneurs sont en état de bon fonctionnement et la commande délivrée par le système de commande est notée $u^{nom}(t)$. La dynamique de la sortie du système dans ce cas est modélisée par :

$$\dot{y}_{nom} = C\dot{x} = CAx + CBu^{nom} \tag{2.38}$$

De même, supposons qu'un ou plusieurs actionneurs soient défaillants (2.16). La dynamique de la sortie du système défaillant peut être exprimée par :

$$\dot{y} = C\dot{x} = CAx + CB_f u \tag{2.39}$$

Le système de commande tolérant aux fautes génère une commande u assurant que la dynamique (2.39) approxime aussi près que possible (2.38) sachant (2.17). Cet objectif est vérifié si la condition suivante est respectée :

$$Bu_{nom} = B_f u \tag{2.40}$$

où par conséquent :

$$u = (I - \Gamma)^{-1} u^{nom} \tag{2.41}$$

avec

$$B_f = B\Gamma$$

De ce fait, le taux de défaillance de l'actionneur en mode de fonctionnement dégradé peut être estimé en fonction d'un niveau de commande nominal comme suit :

$$\lambda_i(\gamma) = \lambda_i^0 \times e^{(1-\gamma_i)^{-1}\beta_i u_i^{nom}} \tag{2.42}$$

où la fonction charge introduite dans (2.36) modélise l'impact de la charge appliquée (nécessaire pour accommoder les défauts) sur la fiabilité de l'actionneur. En fait, la charge correspondante à la commande (2.41) est nécessaire pour assurer les fonctionnalités du système défaillant.

La fiabilité de l'actionneur dans un mode de fonctionnement dégradé peut être estimée en fonction de la charge appliquée dans le cas nominal ainsi que l'amplitude du défaut comme suit :

$$R_i(t, \gamma) = e^{-\lambda_i(\gamma)\times t} \tag{2.43}$$

Ainsi, la fiabilité du système global dépend de la manière dont les composants constituant le système sont inter-connectés. Dans ce contexte, une structure série ou parallèle peut être considérée respectivement par les relations (1.36) et (1.38) définies

dans le chapitre précédent. Dans le cadre de l'étude de reconfigurabilité, seuls les actionneurs sont considérés.

Corollaire 2.3.1 *Dans des conditions de fonctionnement dégradées, la fiabilité du système global peut être caractérisée par les taux de défaillances de bases des composants λ_i^0 ainsi que les facteurs de perte d'efficacités γ_i. Ces derniers offrent une image sur la consommation énergétique nécessaire (considérée comme un facteur de stress) affectant la durée de vie de l'actionneur après l'apparition d'un défaut.*

2.3.3 Indice de reconfigurabilité basée sur la fiabilité

Pour un système tolérant aux fautes garantissant la fiabilité, l'énergie maximale déterminant l'admissibilité des modes dégradés sera définie en fonction d'un niveau de fiabilité donné. En fait, le système accommodable dans ce cas doit achever la durée de sa mission avec une probabilité importante. Cette contrainte permet de garantir les fonctionnalités du système accommodé jusqu'à la fin de sa mission. Dans le cas où cette probabilité n'est pas respectée, la solution de tolérance consiste à planifier une reconfiguration du système de commande dès l'apparition du défaut en question.

Définition 2.6 *Un système est dit tolérant aux fautes et fiable pour un instant d'occurrence du défaut $t = t_f$ et un état initial x_0 si et seulement si le problème d'accommodation a une solution énergétique admissible respectant un niveau de fiabilité bien déterminé.*

Lemme 2.2 *Pour une distribution exponentielle, la contrainte de fiabilité $R(t) \geq R_{pth}$ est satisfaite $\forall t$ durant la mission $[t_0,\ t_M]$ si et seulement si cette dernière est respectée a priori pour l'instant de la fin de la mission $t = t_M$.*

Pour calculer la valeur de l'énergie admissible σ_{pth} déterminant l'ensemble des modes de fonctionnement dégradés accommodables, les modes dégradés dits acceptables sont définis comme suit :

$$\gamma^* = \{\gamma \in \Re^m,\quad R(t_M, \gamma) \geq R_{pth}\} \tag{2.44}$$

où, γ^* est l'ensemble des facteurs de perte d'efficacité correspondants aux modes dégradés respectant la contrainte de fiabilité. En se basant sur (2.44) et (2.33), le coût énergétique associé au mode acceptable le plus dégradé σ_{pth} sera défini en fonction de l'énergie maximale acceptable γ^* comme suit :

Définition 2.7 *Dans des conditions de fonctionnement dégradé, un système tolérant aux fautes est admissible en respectant les performances de commande désirées si :*

$$\rho(\gamma) \leq \rho_{pth} \tag{2.45}$$

où

$$\rho_{pth} = \frac{\sigma_{pth} - \sigma_{min}}{\sigma_{max} - \sigma_{min}} \tag{2.46}$$

avec

$$\sigma_{pth} = \max(\sigma(\gamma^*)) \tag{2.47}$$

En fait, le seuil de reconfigurabilité (2.47) est l'indice énergétique définissant les limites fonctionnelles des systèmes tolérants aux fautes garantissant la fiabilité désirée.

2.3.4 Mesures équivalentes de Reconfigurabilité

Comme indiqué dans la première partie de ce chapitre, d'autre indicateurs de reconfigurabilité existent dans la littérature. Dans cette partie nous présentons l'étude proposée par (Wu *et al.*, 2000) et nous définissons le lien existant avec celle que nous avons proposé, tout en intégrant la fiabilité. Dans les travaux de (Wu *et al.*, 2000), un indicateur de reconfigurabilité est déterminé en fonction du Grammien de commandabilité W_c et d'observabilité W_o. Ces derniers sont la solution des équations de Lyapunov suivantes :

$$\begin{aligned} AW_c + W_c A^T + BB^T &= 0 \\ A^T W_o + W_o A + C^T C &= 0 \end{aligned} \tag{2.48}$$

Chacune de ces équations est résolue afin de trouver une valeur minimale de W_c et de W_o. Une fois les deux valeurs obtenues, les modes de second ordre sont calculés. Pour le faire, la définition suivante est considérée :

Définition 2.8 *(Moore, 1981) Les modes de second ordre sont les éléments positifs* $\sigma_i^2, i = 1, \ldots, n$ *tels que :*

a) $\sigma_1^2 \geq \sigma_2^2 \geq \ldots \sigma_n^2$,

b) $\sigma_i^2 = \Lambda_i(W_c W_o)$

où Λ_i *représente la* i^{eme} *valeur propre de la matrice* $(.)$.

Les racines carrées des modes du second ordre sont connues comme les *valeurs singulières de Hankel* et elles restent inchangées par rapport à n'importe quelle transformation linéaire du système (Moore, 1981).

En se basant sur la définition (2.8), la reconfigurabilité du système est définie en fonction des facteurs de perte d'efficacité γ_i comme suit :

Définition 2.9 *(Wu* et al.*, 2000) Soit* γ *le vecteur des facteurs de perte d'efficacité représenté dans l'espace de défaillance tel que* $\gamma \in \omega$*, l'indicateur de reconfigurabilité* ∂ *est retenu :*

$$\partial = \min_{\gamma \in \omega} \sigma_i(\gamma) \tag{2.49}$$

pour $i = 1, \ldots, m$.

Cependant, si le système (2.1) est représenté sous forme équilibrée par transformation linéaire, les matrices caractérisant le fonctionnement (A_e, B_e, C_e) peuvent être données comme suit :

$$A_e = TAT^{-1}, \quad B_e = TB, \quad C_e = CT^{-1} \tag{2.50}$$

où la matrice régulière de transformation T est déterminée.

Cette forme dite équilibrée (Moore, 1981), permet d'évaluer les Grammiens de forme générale et elle montre l'influence des entrées sur les états et les états sur les sorties. De plus, sous cette représentation, la valeur du Grammien de commandabilité W_c^e est équivalente à celle d'observabilité W_o^e, d'où la relation suivante :

$$W_c^e = W_o^e = diag([\sigma_1, \sigma_2, \ldots, \sigma_m]) \tag{2.51}$$

où $\sigma_i = \sqrt{\Lambda_i(W_c W_o)}$. Ainsi,

$$TW_cT^T = T^{-T}W_oT^{-T} = diag([\sigma_1, \sigma_2, \ldots, \sigma_m]) \tag{2.52}$$

Dans cette forme, les Grammiens montrent la même relation énergétique entre excitations/états et états/sorties. Un indicateur de reconfigurabilité équivalent peut être défini comme suit :

$$\partial = \underline{\sigma}(W_c^b) \tag{2.53}$$

où, $\underline{\sigma}$ représente la plus petite valeur singulière de la matrice W_c^b. Par conséquent, dans les même cordonnées d'équilibre, la relation entre les indicateurs énergétiques de reconfigurabilité (2.31) et (2.54) est caractérisée comme suit :

$$\partial = \frac{1}{\sigma(\gamma)} \tag{2.54}$$

Un indice de reconfigurabilité pour les systèmes tolérants aux fautes garantissant la fiabilité peut être défini par normalisation comme dans (2.46) et (2.47).

En effet, l'indicateur de reconfigurabilité proposé par (Wu *et al.*, 2000) n'est que l'inverse de celui proposé par (Staroswiecki, 2002) et adopté dans ce travail.

2.4 Exemple d'illustration

Afin d'illustrer les différentes étapes de l'étude proposée, le modèle décrivant la dynamique d'un avion utilisé dans (Wu *et al.*, 2000) est retenu. Pour ce modèle, deux entrées de commande ainsi que trois sorties à contrôler sont définies. Le modèle est considéré avec deux entrées de commande pour simplifier la visualisation des résultats. Les valeurs des taux de défaillances associées aux actionneurs sont considérées dans la table (2.1).

Pour une dynamique de vol déterminée autour d'un point de fonctionnement spécifique, le modèle décrivant la dynamique du système (Wu *et al.*, 2000) est défini par la représentation d'état de la forme (2.1) avec les matrices suivantes :

$$A = \begin{bmatrix} -0.0226 & -36.6 & -18.9 & -32.1 \\ 0 & -1.9 & 0.983 & 0 \\ 0.0123 & -11.7 & -2.63 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 0 \\ -0.414 & 0 \\ -77.8 & 22.4 \\ 0 & 0 \end{bmatrix}, C = \begin{bmatrix} 0 & 5.73 & 0 & 0 \\ 0 & 0 & 0 & 5.73 \end{bmatrix}$$

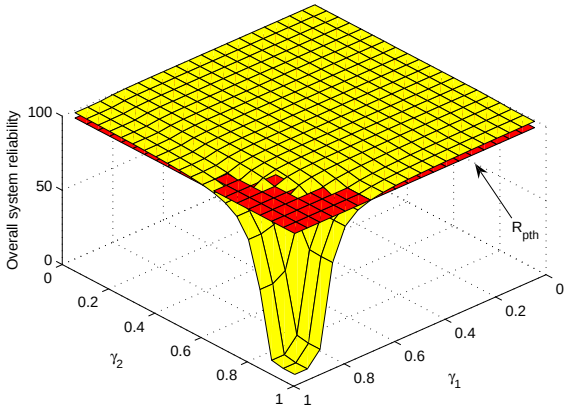

FIGURE 2.1 – Évaluation de la fiabilité du système à la fin de la mission ($t_M = 900\ min$)

Dans un mode dégradé, la dynamique du système peut être modélisée par la représentation d'état (2.16) en fonction des facteurs de perte d'efficacité γ_1 et γ_2. Chaque paire $\gamma = (\gamma_1, \gamma_2)$ considérée détermine un mode de fonctionnement dégradé donné. Dans cet exemple, la première entrée de commande est considérée comme une commande primaire. La deuxième entrée de commande assure aussi le fonctionnement du système pour un vol latéral.

Taux de défaillance de base	
λ_1^0	9e-6 h^{-1}
λ_2^0	5e-6 h^{-1}

TABLE 2.1 – Taux de défaillance des actionneurs

Pour chaque mode dégradé défini par γ où $0 \leq \gamma_i < 1$, le Grammien de commandabilité $W_c(\gamma)$ solution de l'équation de Lyapunov (2.27) est calculé. Afin d'étudier a priori la reconfigurabilité du système et de mesurer les limites d'accommodation, l'indice (2.32) basé sur la normalisation du coût maximal énergétique (2.31) est défini pour chaque paire (γ_1, γ_2).

L'indice (2.32) donne une image sur la capacité énergétique du système à accommoder la situation défaillante en fonction de la sévérité du défaut et de son impact sur les fonctionnalités du système. L'évaluation de la fiabilité globale du système (2.43) pour chaque mode dégradé permet de sélectionner l'ensemble des modes dégradés respectant (2.44). En fait, le mode défaillant le plus dégradé ayant un coût énergétique maximal (2.47) est considéré pour déterminer le seuil de reconfigurabilité pour lequel le système pourrait accommoder les défauts tout en respectant la contrainte de fiabilité. Ce dernier détermine le seuil énergétique d'un système tolérant aux fautes garantissant la fiabilité.

La valeur de la fiabilité globale R_{pth} retenue dans cette application est $R_{pth} = 0.90$. Les défauts sont donc accommodables pour n'importe quel instant t_f tout en assurant le fonctionnement jusqu'a la fin de la mission t_M avec une probabilité

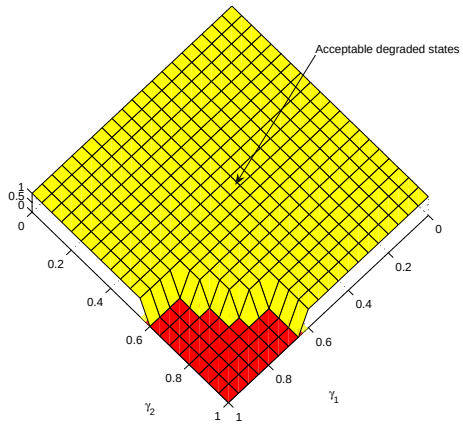

FIGURE 2.2 – Modes dégradés acceptables en terme de fiabilité ($t_M = 900\ min$)

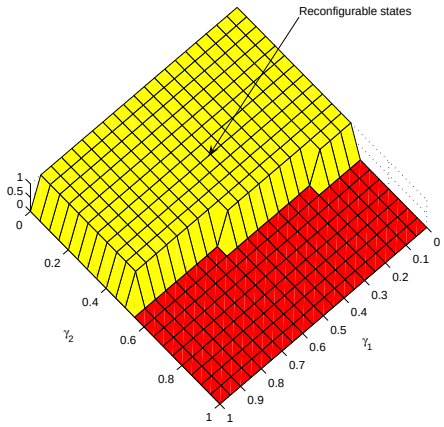

FIGURE 2.3 – Modes dégradés accommodables et fiables ($t_M = 900\ min$)

$\mathbb{P} \geq 0.90$. Comme une première application, la durée de la mission est supposée $t_M = 900\,\text{min}$.

La figure (2.1) présente l'évaluation de la fiabilité globale du système à la fin de la mission. Cette dernière est calculée pour chaque mode de fonctionnement défini par (γ_1, γ_2) et comparée à $\mathbb{R}_{pth} = 0.90$. A l'issue de cette comparaison, l'ensemble des modes de fonctionnement dégradés dits acceptables sont présentés dans la figure (2.2) où la valeur 1 est attribuée aux modes de fonctionnement acceptables. En effet, ces derniers sont les situations défaillantes dans lesquels les défauts sont accommodables avec une probabilité $\mathbb{P} \geq 0.90$ si le coût énergétique est admissible (2.45).

La valeur de l'énergie déterminant l'ensemble des modes dégradés accommodables est donnée par (2.47). Par normalisation, l'indice de reconfigurabilité ρ_{pth} des systèmes tolérants aux fautes garantissant la fiabilité est obtenu (2.46). La figure (2.3) présente les modes dégradés pouvant être accommodés tout en respectant la contrainte de fiabilité. La valeur 1 est attribuée à ces modes en fonction de (γ_1, γ_2).

Les résultats présentés dans les figures précédentes montrent l'avantage d'intégrer la fiabilité dans la détermination des limites de la tolérance aux défauts. Le coût énergétique nécessaire pour accommoder des situations défaillantes et assurer le fonctionnement jusqu'à la fin de la mission est calculé. Pour les systèmes tolérants aux fautes et fiables, les modes dégradés, considérés accommodables, minimisent la consommation de l'énergie et assure la fiabilité du système global.

Cependant, la fiabilité est une mesure définie en fonction du temps. La reconfigurabilité du système dans ce cas est évaluée en fonction d'une durée de mission à respecter. Afin d'évaluer l'influence du temps de la mission sur la capacité du système à tolérer des situations défaillantes, $t_M = 600\,\text{min}$ est considéré dans ce qui suit.

Dans la figure (2.4), sont présentés les modes dégradés acceptables respectant

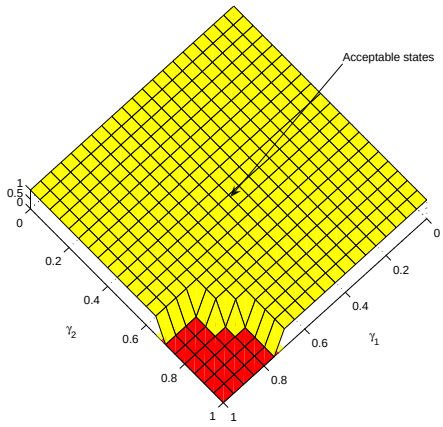

FIGURE 2.4 – Modes dégradés acceptables en terme de fiabilité pour $t_M = 600min$

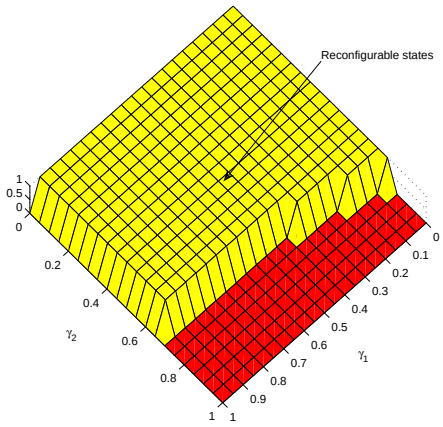

FIGURE 2.5 – Modes dégradés accommodables et fiables pour $t_M = 600min$

la contrainte de fiabilité pour $t_M = 600\,\text{min}$. En suivant la même démarche que précédemment, un indice de reconfigurabilité est obtenu et les modes dits accommodables dans ce cas sont présentés dans la figure (2.5). La valeur 1 est attribuée dans la figure à ces derniers.

Pour une mission de courte durée, la capacité du système à accommoder des situations défaillantes tout en assurant la fiabilité est relativement importante. La dégradation et le vieillissement des actionneurs dans le temps diminuent la probabilité d'assurer le fonctionnement du système après accommodation. Par conséquent, la stratégie de reconfiguration à appliquer sur le système dépend de la sévérité des défauts, du temps de la mission ainsi que des objectifs fixés en terme de fiabilité. Ces derniers varient suivant la nature et le rapport fonctionnement/risque du système. Pour des systèmes critiques comme les procédés nucléaires, les missions satellites, ..etc, la contrainte de fiabilité à respecter est relativement grande. Par ailleurs, pour des systèmes présentant moins de risque, le niveau de fiabilité à assurer après accommodation peut être relativement faible.

2.5 Conclusion

Dans ce chapitre, un indice énergétique de reconfigurabilité basé sur l'analyse de fiabilité du système est proposé. Les résultats obtenus montrent la relation entre l'admissibilité des systèmes tolérants aux fautes et la fiabilité globale. Dans l'approche proposée, l'étude a priori de la reconfigurabilité et la capacité du système à retrouver ses fonctionnalités dans un mode dégradé dépend d'un niveau de fiabilité à respecter. Cette étude est considérée pour un mode de fonctionnement nominal défini par un niveau de charge moyen connu. L'évaluation en ligne de la situation défaillante et de son impact sur les fonctionnalités du système ne sont pas nécessaires. Or, l'accommodation du système après l'occurrence du défaut peut être effectuée en ligne.

L'objectif de cette étude est de contribuer à la conception des systèmes de commande tolérante aux fautes garantissant la fiabilité et les objectifs désirés jusqu'à la fin de la mission. A l'issue des résultats obtenus, une étude de reconfigurabilité par rapport à différents modes de fonctionnement nominaux en tenant compte du niveau moyen de la charge peut être considérée.

Chapitre 3

Méthodologie d'allocation et ré-allocation de la commande garantissant la fiabilité

3.1 Introduction

Comme défini dans la section précédente, un système de commande tolérant aux défauts se caractérise par son aptitude à maintenir des performances proches de celles désirées, non seulement dans un fonctionnement nominal mais aussi lors d'un fonctionnement défaillant (Blanke *et al.*, 2006; Noura *et al.*, 2009). Ainsi, pour répondre aux différents besoins liés à la sûreté de fonctionnement des systèmes, la redondance des actionneurs et l'allocation de la commande sont utilisées. L'allocation de la commande a été largement étudiée dans la littérature, notamment par les travaux de (Durham, 1993). Un état de l'art sur les principales approches et méthodes existant dans la littérature est publié dans (Enns, 1998) et (Bodson, 2002). L'allocation de la commande est considérée spécifiquement dans le domaine de l'aéronautique et le spatial (Harkegard, 2002; Alwi et Edwards, 2008; Liu et Crespo, 2010), ainsi que pour les systèmes sous-marins (Sakar *et al.*, 2002; Merdic, 2004).

Un système de commande basée sur l'allocation permet de séparer l'aspect régulation de la tache de distribution des efforts aux actionneurs. Avec cette stratégie, la loi de commande spécifie uniquement l'ensemble des efforts à appliquer sur le système. La distribution de la commande est assurée séparément par un module appelé *Allocation*. Cette stratégie a pour avantage d'accommoder certaines classes de défauts sans modifier la synthèse de la loi de commande. Les défauts considérés dans ces travaux sont les pertes d'efficacité des actionneurs. Avec l'apparition de ces derniers, la ré-allocation de la commande est utilisée afin d'accommoder l'impact des défauts et de maintenir le fonctionnement du système (Zhang et Jiang, 2008). La ré-allocation de la commande nécessite l'intégration d'un module d'allocation reconfigurable en ligne dans la boucle de contrôle (Burken *et al.*, 2001; Alwi et Edwards, 2008). Ce module permet de redistribuer en présence de défauts, l'ensemble des efforts désirés sur les différents actionneurs. Dans ce cadre, plusieurs méthodes ont été proposées. Ces dernières peuvent être classées en deux catégories principales : les méthodes non optimales et les méthodes dites optimales (Durham, 1993). Pour les méthodes non optimales, la distribution de l'ensemble des efforts désirés est assurée directement sans passer par un critère d'optimisation. Dans ce cadre, le problème d'allocation directe ainsi que la méthode de la chaine bouclée sont utilisés (Bordignon, 1996). Dans ce travail, les méthodes dites optimales sont considérées (Bodson, 2002), où le problème d'allocation est reformulé en un problème d'optimisation.

Dans le but d'améliorer la sûreté de fonctionnement des systèmes sur-actionnés, nous proposons une méthodologie d'allocation et de ré-allocation de la commande en tenant compte de la fiabilité des actionneurs. En effet, les systèmes sur-actionnés présentent un avantage dans la synthèse des des systèmes de commande garantissant la fiabilité. Cet avantage se caractérise par l'existence de plusieurs choix possibles pour distribuer les efforts désirés. Dans ce travail, nous proposons d'intégrer des informations sur la fiabilité et les caractéristiques des actionneurs dans le système de commande assurant la distribution des efforts désirés.

Utiliser des indicateurs de fiabilité guidant la distribution des efforts au travers les actionneurs est une approche innovante, permettant de mieux gérer le vieillissement des actionneurs tout en assurant les performances désirées. Cette méthodologie nécessite l'adaptation des outils de fiabilité de base avec la théorie de la commande. Dans ce chapitre, deux indicateurs sont proposés avec comme objectif, calculer les entrées de commande garantissant les performances désirées en tenant compte des défauts et de la durée de vie résiduelle des actionneurs.

3.2 Modélisation et Commande des Systèmes Sur-actionnés

Soit un système décrit par sa représentation d'état :

$$\begin{cases} \dot{x}(t) = Ax(t) + B_u u(t) \\ y(t) = Cx(t) \end{cases} \tag{3.1}$$

où $A \in \mathbb{R}^{n\times n}$ et $B_u \in \mathbb{R}^{n\times m}$ représentent respectivement la matrice d'état et la matrice d'action de commande. $C \in \mathbb{R}^{p\times n}$ est la matrice de sortie. $x(t) \in \mathbb{R}^n$ et $u(t) \in \mathbb{R}^m$ sont respectivement, le vecteur d'état et le vecteur des entrées de commande. $y(t) \in \mathbb{R}^p$ représente le vecteur des sorties à contrôler.

Définition 3.1 (Harkegard (2002)) *Le système (3.1) est dit sur-actionné si la matrice B_u n'est pas de plein rang avec, $rang(B_u) = l < m$. Dans ce cas, la matrice B_u peut être décomposée comme suit :*

$$B_u = B_v B$$

où $B_v \in \mathbb{R}^{n\times l}$ et $B \in \mathbb{R}^{l\times m}$.

Pour résoudre le problème de la commande, un vecteur $v_d(t) = Bu(t)$ appelé vecteur de commande virtuelle est défini. $v_d(t) \in \mathbb{R}^l$ représente l'ensemble des efforts et moments produits et appliqués réellement sur le système. Ainsi, la loi de commande du système sur-actionné (3.1) est synthétisée en se basant sur la représentation d'état équivalente suivante :

$$\begin{cases} \dot{x}(t) = Ax(t) + B_v v_d(t) \\ v_d(t) = Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{3.2}$$

Dans ce chapitre, la redondance analytique est considérée où les efforts désirés peuvent être distribués au système en utilisant l'ensemble des actionneurs avec différents niveaux de sollicitation. Afin de faciliter la présentation de la méthode, le nombre des entrées de commande virtuelle choisies est considéré égal au nombre des variables à contrôler $l = p$. Dans le cas où $l > p$, une reformulation équivalente du problème d'allocation est possible comme démontré dans la propriété suivante :

Propriété 3.1 *Dans le cas où la matrice B_u n'est pas de rang plein, $rang(B_u) = l < n$, et $l > p$, la matrice B_u peut être décomposée en deux matrices : $B_u = B_v B$ avec $B_v \in \mathbb{R}^{n\times l}, B \in \mathbb{R}^{l\times m}$ et $rang(B) = l$. Le vecteur $v_d(t)$ déterminant la commande virtuelle sera défini sous la forme : $v_d(t) = Bu(t) \in \mathbb{R}^l$ avec $B = (B_v^T B_v)^{-1} B_v^T B_u$.*

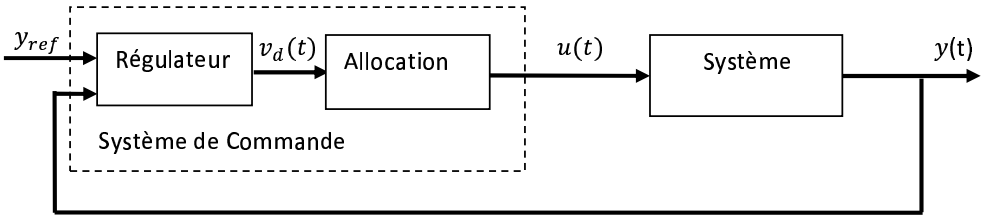

FIGURE 3.1 – Schéma de principe de la commande d'un système sur-actionné basée sur l'allocation

Dans le cadre de l'allocation de la commande et comme illustré par la figure (3.1), le régulateur détermine l'ensemble des efforts désirés à appliquer au système. Le bloc d'allocation est introduit dans la boucle de contrôle afin d'assurer la distribution des efforts désirés aux différents actionneurs. Cette configuration se caractérise par l'aptitude à accommoder certains défauts sans la modification des paramètres du régulateur.

Le problème de base de l'allocation de la commande peut être exprimé comme un problème d'optimisation linéaire avec contrainte. Il consiste à déterminer le vecteur des entrées de commande $u(t)$ satisfaisant :

$$v_d(t) = Bu(t) \tag{3.3}$$

avec

$$u_{min} \leq u \leq u_{max} \tag{3.4}$$

où (3.4) représente les limites physiques des actionneurs déterminant les saturations. Le problème d'allocation peut être interprété comme suit : *étant donné un vecteur désiré $v_d(t)$ synthétisé par le régulateur, comment allouer ou distribuer les efforts désirés à l'ensemble des actionneurs ?*

Pour répondre à cette problématique, plusieurs approches et méthodes ont été développées dans la littérature. Dans ce chapitre, nous nous intéressons aux approches dites optimales où la commande $u(t)$ assurant la distribution des efforts à

l'ensemble des actionneurs est généralement la solution d'un problème d'optimisation à deux étapes (3.5)-(3.6) :

$$\psi = \underset{u_{\min} \leq u \leq u_{\max}}{\arg\min} \quad \|Bu - v_d\|_2 \tag{3.5}$$

et

$$u^* = \arg\min_{u \in \psi} \|W_u u\|_2 \tag{3.6}$$

où W_u est une matrice de pondération utilisée pour donner un ordre de priorité aux actionneurs dans la distribution des efforts désirés. Le problème (3.5)-(3.6) peut être interprété comme suit : *étant donné ψ l'ensemble des entrées de commande dites admissibles minimisant $Bu - v_d$, trouver l'entrée de commande u minimisant l'énergie (pondérée par W_u).*

Dans (3.5) et (3.6), l'ensemble ψ détermine les différentes combinaisons des entrées de commande satisfaisant $Bu = v_d$ et assurant donc la distribution des efforts désirés sur les actionneurs. Ainsi, une seule combinaison $u(t)$ est retenue dans la solution en tenant compte du niveau de priorité attribué à chaque actionneur à partir de la matrice W_u.

Après l'apparition des défauts, la ré-allocation de la commande est utilisée. Cette dernière consiste à redistribuer les efforts désirés, déterminés par le régulateur sur l'ensemble des actionneurs tenant compte de la sévérité du défaut (figure (3.2)).

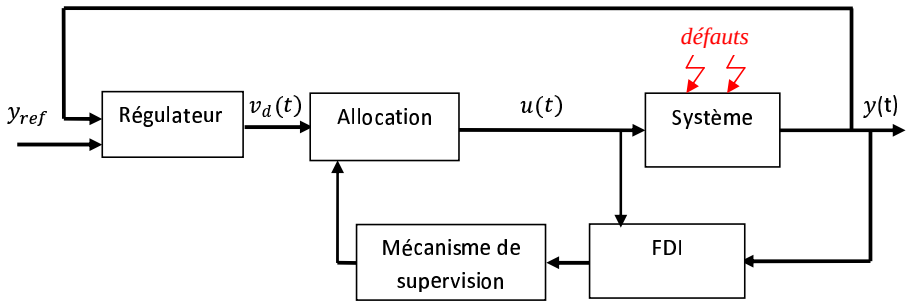

FIGURE 3.2 – Principe de la ré-allocation de la loi de commande par pondération

Dans ce travail, les pertes d'efficacité des actionneurs sont considérées où le système (3.2) peut s'écrire en fonctionnement dégradé sous la forme suivante :

$$\begin{cases} \dot{x}(t) &= Ax(t) + B_v v_d(t) \\ v_d(t) &= B_f u(t) \\ y(t) &= Cx(t) \end{cases} \tag{3.7}$$

Dans (3.7), la matrice B_f modélise l'impact des défauts sur le système. Cette représentation permet de rapporter l'image du défaut uniquement sur le bloc Allocation. B_f est définie en fonction des facteurs de perte d'efficacité γ_i comme suit :

$$B_f = B(I_m - \Gamma) \tag{3.8}$$

où

$$\Gamma = \begin{pmatrix} \gamma_1 & & & 0 \\ & \gamma_2 & & \\ & & \ddots & \\ 0 & & & \gamma_m \end{pmatrix}$$

avec $\gamma_i \in [0 \;\; 1]$. Pour $\gamma_i = 0$, le i^{eme} actionneur est considéré sain. Par contre, pour $\gamma_i = 1$, une défaillance est apparue et l'actionneur correspondant est hors service.

Afin de garantir les performances désirées, la valeur de la matrice de pondération W_u peut être modifiée en ligne dès l'identification des défauts (Alwi et Edwards, 2008). Cette technique permet de trouver une nouvelle distribution des efforts désirés où un vecteur de commande $u(t)$ est calculé afin d'assurer l'objectif (3.3).

Dans la stratégie d'allocation et ré-allocation, la matrice de pondération est utilisée pour solliciter ou pénaliser plus ou moins certains actionneurs. Or, il n'existe pas de critère bien déterminé pour choisir la valeur de la matrice de pondération. Une solution communément adoptée consiste à choisir une matrice $W_u = I_m$. Ce choix signifie que la distribution des efforts est effectuée au travers les actionneurs suivant les éléments de la matrice B et sans ordre de priorité. Ainsi, si les éléments de la matrice B sont identiques, les actionneurs sont sollicités avec le même niveau de charge. La section suivante sera consacrée à la définition des indicateurs contribuant à une nouvelle méthodologie de synthèse de lois de commande garantissant la sûreté de fonctionnement du système.

3.3 Analyse de la fiabilité pour une commande optimale tolérante aux fautes

En se fondant sur un choix adéquat de la matrice W_u, nous proposons de générer une commande optimale vis-à-vis de la fiabilité en imposant un ordre de sollicitation spécifique aux actionneurs. Cette méthodologie a pour but d'équilibrer les charges appliquées sur les actionneurs tout en respectant les performances de contrôle désirées. Cela permet de préserver et décélérer le vieillissement de l'ensemble des actionneurs. L'idée consiste à choisir la matrice de pondération W_u en se basant sur des indicateurs de fiabilité afin de redistribuer convenablement les efforts désirés sur les actionneurs et augmenter ainsi la probabilité de tolérer des éventuels défauts. Cet objectif permet également d'améliorer la sûreté de fonctionnement du système global.

3.3.1 Contribution à la ré-allocation de la commande en tenant compte des caractéristiques des actionneurs

Comme définie dans le premier chapitre, la fiabilité est l'aptitude d'une entité à accomplir une fonction requise, sous des conditions données pendant une durée bien déterminée (Gertsbakh, 2000). Dans cette partie, nous nous intéressons aux actionneurs dans leur période de vie utile. La fiabilité durant cette période est caractérisée

par une loi de distribution exponentielle ainsi qu'un taux de défaillance constant $\lambda(t) = \lambda^0$. Dans ce cadre, la fiabilité d'un composant est exprimée sous la forme suivante :

$$R(t) = e^{-\lambda^0 t} \tag{3.9}$$

Cette loi est caractérisée aussi par le temps moyen de bon fonctionnement avant la première défaillance noté $MTTF$ (Mean Time To Failure) :

$$MTTF = \int_0^\infty R(t)dt = \frac{1}{\lambda^0} \tag{3.10}$$

Généralement, le taux de défaillance d'un composant est obtenu a priori pour un niveau de sollicitation fixe. Cette caractéristique n'est plus valide si la variation de la charge (en cours de fonctionnement) est suffisamment importante pour avoir un impact non négligeable sur la fiabilité du composant. La variation de la charge induite par la sollicitation des actionneurs durant le fonctionnement influence alors la fiabilité du composant.

Pour modéliser cette dégradation des actionneurs soumis à des actions de commande variables dans leur période de vie utile, nous considérons l'hypothèse suivante :

Hypothèse 3.1 *Pour une période de fonctionnement donnée, le taux de défaillance d'un composant soumis à une commande variable peut être estimé par rapport à un niveau de charge donné, considéré comme la charge moyenne appliquée durant le fonctionnement.*

En tenant compte de l'hypothèse 3.1, un taux de défaillance $\lambda \geq \lambda^0$ est obtenu pour un niveau de charge donné où λ^0 est le taux de défaillance de base obtenu sous des conditions normales, voir figure (3.3).

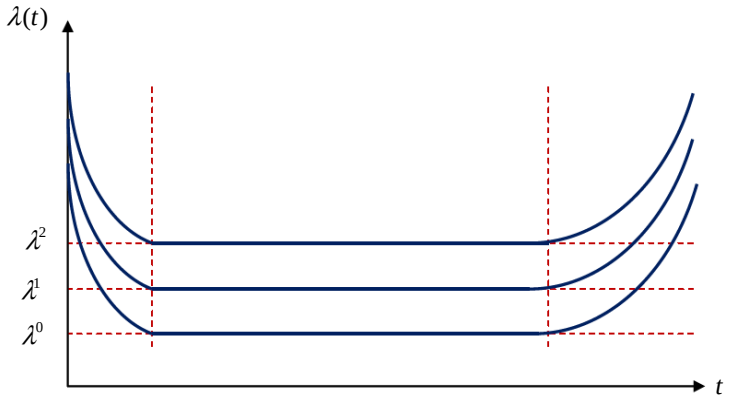

FIGURE 3.3 – Taux de défaillance

Plusieurs modèles mathématiques sont développés et proposés dans la littérature pour modéliser l'effet de la charge sur la fiabilité des composants (Martorell *et al.*, 1999; Finkelstein, 1999). Dans ce travail, nous avons retenu le modèle proportionnel de Cox (Cox, 1972; Dale, 1985).

Conformément à l'hypothèse 3.1, le taux de défaillance est considéré comme le produit d'un taux de défaillance nominal λ_i^0, et une fonction $g_i(\ell, \vartheta)$ modélisant la charge :

$$\lambda_i = \lambda_i^0 \times g_i(\ell, \vartheta) \tag{3.11}$$

Dans le cas de notre étude et afin d'adapter l'aspect charge avec la théorie de la commande, nous prenons pour hypothèse que $g_i(\ell, \vartheta)$ est une fonction liée directement à l'entrée de commande appliquée sur le i^{eme} actionneur. Différents modèles de la fonction charge $g_i(\ell, \vartheta)$ existent dans la littérature. Nous retenons dans ce travail le modèle exponentiel qui est souvent utilisé (Cox, 1972).

Définition 3.2 *Considérant le modèle exponentiel, le taux de défaillance peut être modélisé en fonction de la charge appliquée U_i^{moy} comme suit*

$$\lambda_i = \lambda_i^0 \times e^{\beta_i U_i^{moy}} \tag{3.12}$$

où β_i est un paramètre lié au composant. U_i^{moy} est la charge moyenne appliquée au i^{eme} actionneur durant le fonctionnement.

En fiabilité, la charge d'un composant peut être vue de plusieurs façons. La charge peut être liée à un régime de fonctionnement, à un nombre de sollicitations par unité de temps, ... etc. Lors de l'utilisation de l'actionneur dans une plage de fonctionnement parfaitement dimensionnée, le composant ne subit pas de détérioration plus grande selon le niveau de sollicitation s'il est inclus dans la plage de fonctionnement normale. Cependant la variation autour du point de fonctionnement peut entrainer une détérioration plus grande du composant. La charge peut alors être liée à la quantité variation ou à la dispersion autour du point de fonctionnement dans la zone utile.

Pour intégrer ce phénomène, nous proposons de calculer la charge moyenne U_i^{moy} pour une durée de fonctionnement de $t = 0$ jusqu'à t_M comme suit :

$$U_i^{moy} = \frac{1}{t_M} \int_0^{t_M} u_i(t)^2 dt \tag{3.13}$$

où $u_i(t)$ est l'entrée de commande associée au i^{eme} actionneur.

La détérioration et la durée de vie des actionneurs évolue proportionnellement à l'intensité de la charge appliquée. De plus, dans le contexte de la commande tolérante aux fautes des systèmes sur-actionnés, l'apparition d'un défaut nécessite la redistribution des charges sur les actionneurs. Cela implique le passage d'un mode de fonctionnement nominal à un mode de fonctionnement dégradé. Le mode de fonctionnement dégradé est caractérisé par des lois de commande différentes du cas nominal avec comme objectif, de compenser l'effet du défaut sur les performances du système. Pour les défauts de type perte d'efficacité des actionneurs, le mécanisme de tolérance aux défauts requiert l'augmentation de la charge appliquée sur l'ensemble des actionneurs afin de compenser l'effet des défauts et retrouver les performances nominales.

Afin de respecter les hypothèses de l'étude pour une distribution exponentielle, la charge appliquée aux actionneurs sera considérée pour un mode de fonctionnement

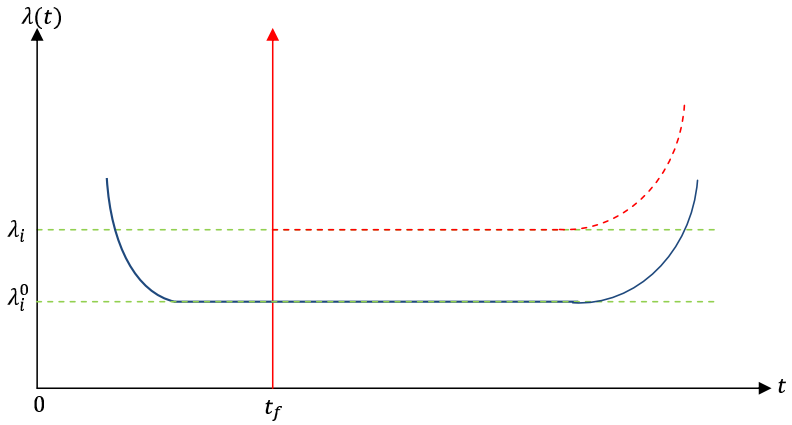

FIGURE 3.4 – Taux de défaillance en fonction de la charge

donné. La charge moyenne dans ce cas modélise le stress appliqué sur l'actionneur avant le passage à un mode de fonctionnement différent. Elle est considérée comme une caractéristique permettant l'estimation de la fiabilité et la durée de vie résiduelle d'un actionneur soumis à une commande évoluant dans le temps (Khelassi *et al.*, 2010b).

Considérons λ_i^0 comme le taux de défaillance d'un actionneur dans un fonctionnement nominal (supposé connu). Après l'apparition d'un défaut à l'instant $t = t_f$, le mode de fonctionnement du système change en un mode dégradé. Ainsi, un nouveau taux de défaillance λ_i modélisant les caractéristiques en fiabilité de l'actionneur peut être estimé en tenant compte de la charge appliquée comme suit,

$$\lambda_i = \lambda_i^0 \times e^{\beta_i U_i^{moy}} \tag{3.14}$$

avec

$$U_i^{moy} = \frac{1}{t_f} \int_0^{t_f} u_i(t)^2 dt \tag{3.15}$$

Dans ce cadre, un nouveau taux de défaillance estimé est attribué aux actionneurs dans chaque mode de fonctionnement en tenant compte du stress subit de $t = 0$ à t_f. La figure (3.4) illustre l'impact de la charge sur le taux de défaillance. En effet, le taux de défaillance estimé λ_i varie *par palier* suivant l'intensité de la charge appliquée. Cette dernière accélère la dégradation de l'actionneur et par conséquent diminue le temps de vie résiduelle de l'actionneur.

L'indicateur (3.14) peut être utilisé dans l'allocation et la ré-allocation de la commande afin de contribuer à une méthodologie de commande tolérante aux fautes garantissant la sûreté de fonctionnement du système. Dans le cas nominal, l'allocation de la commande sera réalisée en tenant compte des taux de défaillance de base λ_i^0 des actionneurs. Ces derniers donnent une image sur les caractéristiques de base des actionneurs en terme de fiabilité.

Après l'apparition d'un défaut, la redistribution des efforts désirés sera effectuée considérant (3.14). Ce dernier reflète une estimation sur l'état de dégradation et les caractéristiques des actionneurs à l'instant de l'occurrence des défauts en tenant compte du stress appliqué sur l'actionneur.

Dans ce qui suit, une nouvelle méthodologie de synthèse de lois de commande intégrant la dégradation des actionneurs est proposée dans le cas des systèmes sur-actionnés. En effet, la commande optimale $u(t)$ solution du problème (3.5)- (3.6) est obtenue en fonction de la matrice de pondération $W_u = diag\{w_1, w_2, \ldots, w_m\}$ choisie a priori. Dans cette partie, nous considérons la matrice de pondération W_u comme une clef permettant de bien gérer les charges attribuées aux actionneurs. L'idée consiste à choisir les éléments de la matrice de pondération W_u afin de solliciter d'une manière adéquate les actionneurs selon leur caractéristique de fiabilité ainsi que leur dégradation (Khelassi *et al.*, 2010a).

Dans un mode de fonctionnement nominal, nous proposons de choisir la matrice de pondération W_u en fonction des taux de défaillance de base λ_i^0 associés aux actionneurs comme suit :

$$W_u = \begin{pmatrix} \frac{\lambda_1^0}{\lambda_{max}^0} & & & 0 \\ & \frac{\lambda_2^0}{\lambda_{max}^0} & & \\ & & \ddots & \\ 0 & & & \frac{\lambda_m^0}{\lambda_{max}^0} \end{pmatrix} > 0 \tag{3.16}$$

où $\lambda_{max}^0 = \max(\lambda_i^0)$ est le taux de défaillance de l'actionneur le moins fiable.

En imposant ce choix a priori, les actionneurs seront sollicités dans la distribution des efforts désirés avec plus de priorité aux actionneurs les plus fiables. Les actionneurs les moins fiables seront préservés et moins sollicités tout en respectant le rapport commande/performance.

Cependant et comme indiqué précédemment, l'apparition des défauts provoque le passage d'un mode de fonctionnement nominal à un mode de fonctionnement dégradé. Ce dernier nécessite la re-distribution des efforts désirés sur les actionneurs afin de garantir les performances désirées en terme de commande. Dans ce cas, une nouvelle matrice de pondération W_u^f est calculée en ligne afin de prendre en considération l'état de dégradation des actionneurs dans la redistribution des efforts. Cela est réalisé par une estimation en ligne de l'état de dégradation des actionneurs considérant l'impact de la charge appliquée. Après l'identification des défauts, la ré-allocation de la commande peut être effectuée en fonction de la matrice de pondération W_u^f proposée comme suit (Khelassi *et al.*, 2010c) :

$$W_u^f = \begin{pmatrix} \frac{\lambda_1}{\lambda_{max}} & & & 0 \\ & \frac{\lambda_2}{\lambda_{max}} & & \\ & & \ddots & \\ 0 & & & \frac{\lambda_m}{\lambda_{max}} \end{pmatrix} > 0 \tag{3.17}$$

où λ_i est le taux de défaillance du i^{eme} actionneur estimé dans un état de fonctionnement dégradé. Ce dernier est calculé en tenant compte de la charge appliquée avant l'apparition du défaut par (3.14) et (3.15).

Par conséquent, pour $\lambda_i << \lambda_{max}$, $\omega_i \rightarrow 0$ et une forte priorité est donnée au i^{eme} actionneur dans la distribution des efforts désirés. Avec cette méthodologie, les actionneurs les moins fiables seront moins sollicités dans les limites imposées par le fait de garantir les performances désirées.

3.3.2 Contribution à la ré-allocation de la commande en tenant compte du vieillissement des actionneurs

Dans cette partie, le vieillissement des actionneurs par rapport au temps sera introduit dans la stratégie d'allocation et de ré-allocation de la commande. Les actionneurs dans ce cas sont considérés dans leur période de vieillissement. Les efforts désirés seront distribués au système en tenant compte des défauts et de l'état de vieillissement des actionneurs. Pour intégrer l'aspect vieillissement dans la commande des systèmes sur-actionnés, un indicateur basé sur les paramètres de fiabilité ainsi que sur les éventuels défauts identifiés est proposé.

Avant de développer l'indicateur proposé, la définition suivante est considérée.

Propriété 3.2 *L'état de dégradation des actionneurs est une mesure affectée par plusieurs facteurs. Dans cette étude, le vieillissement des actionneurs ainsi que la perte d'efficacité sont considérés pour quantifier la dégradation des actionneurs.*

Dans ce contexte, une estimation en ligne de l'état de dégradation des actionneurs pour un mode de fonctionnement donné est nécessaire (Khelassi *et al.*, 2011e). Dans ce travail nous proposons de considérer la distribution de Weibull à deux paramètres pour modéliser la dégradation et la détérioration des actionneurs par rapport au temps. Cette loi est adaptée au contexte de l'étude considérée où comme illustré dans (Toscano et Lyonnet, 2008), les conditions de fonctionnement dépendent aussi de l'intensité des charges appliquées. En effet, considérons la loi de Weibull, la distribution de défaillance des actionneurs notée $f(t)$ peut être modélisée par rapport au temps t comme suit :

$$f(t) = \frac{\beta t^{\beta-1}}{\alpha_0^{\beta}} \exp(-(\frac{t}{\alpha})^{\beta}) \tag{3.18}$$

où α^0 est le paramètre d'échelle. $\beta < 1$ est le paramètre de forme. En effet, β relève la tendance à la défaillance du composant dans le temps.

Dans le cas d'une loi de Weibull, la probabilité de défaillance cumulative peut être obtenue comme suit :

$$F(t) = 1 - \exp[-(\frac{t}{\alpha^0})^{\beta}] \tag{3.19}$$

Dans les formules classiques de la loi de Weibull, la dégradation de l'actionneur est considérée par rapport au temps. Cette loi telle qu'elle est proposée et utilisée dans le domaine de l'analyse de fiabilité, n'est pas adaptée à l'aspect commande car les actionneurs sont sollicités en permanence dans la boucle de contrôle avec une charge variable. Il est important donc de modéliser l'impact de la charge sur le vieillissement des actionneurs afin de le considérer dans la synthèse de la commande.

Dans ce contexte et pour contribuer à une nouvelle méthodologie d'allocation et ré-allocation en tenant compte du vieillissement des actionneurs, un nouvel indicateur basé sur les principaux paramètres de la loi de Weibull est développé. Comme illustré dans la section précédente, la charge appliquée sur l'actionneur accélère la

dégradation et le vieillissement des actionneurs par rapport au temps. Nous proposons dans ce qui suit, d'intégrer le modèle proportionnel de Cox (3.11) dans (3.19).

Un nouveau paramètre estimé α basé sur le paramètre de forme α^0 est proposé. En effet, α^0 accélérant ou ralentissant le vieillissement de l'actionneur par rapport au temps peut être évalué en tenant compte de la charge appliquée comme suit :

$$\alpha_i = \frac{\alpha_i^0}{g_i(\ell, \vartheta))}, \quad i = 1, \ldots, m \tag{3.20}$$

où α_i^0 est considéré comme le paramètre de forme de base du i^{eme} actionneur. $g_i(\ell, \vartheta)$ est la fonction charge définie dans ce cas comme suit :

$$g_i(\ell, \vartheta) = \exp(U_i^{moy}(t)), \quad i = 1, \ldots, m \tag{3.21}$$

avec U_i^{moy} la charge moyenne appliquée sur l'actionneur et définie à l'instant t comme suit,

$$U_i^{moy}(t) = \frac{1}{t}\int_0^t u_i(t)^2 dt \tag{3.22}$$

Le paramètre proposé dans (3.20) ainsi que la probabilité de défaillance classique de la loi de Weibull (3.19) contribuent à l'indicateur suivant :

$$F_i^c(t) = 1 - \exp[-(\frac{t}{\alpha_i(t)})^\beta] \tag{3.23}$$

L'indicateur (3.23) modélise la dégradation de l'actionneur par rapport au temps en intégrant la variation de charge appliquée à l'actionneur (Khelassi *et al.*, 2011a).

Propriété 3.3 *L'indicateur $F^c(t)$ proposé dans (3.23) permet l'intégration de l'impact de la charge dans la loi de Weibull. Cet impact est considéré comme un facteur supplémentaire pouvant accélérer le vieillissement des actionneurs par rapport au temps. L'indicateur (3.23) sera utilisé dans la gestion des actionneurs dans l'allocation et la ré-allocation de la commande.*

Dans le contexte de la commande des systèmes sur-actionnés, l'indicateur (3.23) peut être utilisé pour une gestion optimale des actionneurs. L'objectif est de préserver l'ensemble des actionneurs le plus longtemps possible durant la mission. Les efforts désirés $v_d(t)$ définis par le contrôleur sont distribués sur les actionneurs en tenant compte de l'état de dégradation des actionneurs estimé en ligne. Les entrées de commande optimales $u = (u_1, u_2, \ldots, u_m)$, solution du problème d'allocation (3.5) et (3.6) sont définies en fonction de la matrice de pondération $W_u = diag\{w_1, w_2, \ldots, w_m\}$. Afin de prendre en compte l'état de dégradation des actionneurs dans le calcul de la commande, une matrice de pondération variant dans le temps $W_u(t)$ est définie en fonction de l'indicateur (3.23) comme suit :

$$W_u(t) = \begin{pmatrix} \omega_2(t) & & & 0 \\ & \omega_2(t) & & \\ & & \ddots & \\ 0 & & & \omega_m(t) \end{pmatrix} \succ 0 \tag{3.24}$$

où,

$$\omega_i(t) = F_i^c(t) = 1 - \exp[-(\frac{t}{\alpha_i(t)})^{\beta_i}], \quad i = 1, \dots m \tag{3.25}$$

et $\omega_i(t) \leq 1, \ \forall i = 1, \dots, m$.

Par conséquent, pour $\omega_i(t) \to 0$ la valeur de l'entrée de commande associée au i^{eme} actionneur $u_i(t)$ est relativement importante. En effet, avec ce choix, les efforts désirés sont distribués sur les actionneurs en privilégiant plus les actionneurs les moins dégradés. Les actionneurs sont donc "stressés" inversement proportionnellement à leur état de dégradation dans la limite du possible. En effet, la commande tolérante aux fautes peut améliorer la fiabilité du système où, avec une gestion optimale des charges appliquées sur les actionneurs, l'ensemble des actionneurs reste opérationnel pour une durée plus importante tout en respectant les performances désirées de la boucle de contrôle.

La méthodologie d'allocation de la commande proposée ici distribue les efforts désirés sur le système en tenant compte du vieillissement des actionneurs par rapport à la charge. Cependant, si les conditions de fonctionnement changent à cause de l'occurrence d'un défaut, il est nécessaire de ré-estimer l'indicateur $\omega_i(t)$ afin de prendre en compte l'impact du défaut sur la dégradation des actionneurs. Dans la démarche que nous proposons, l'utilisation de l'actionneur en fonctionnement dégradé avec les mêmes objectifs de commande que ceux en régime nominal a pour effet une augmentation de la charge afin de compenser le défaut, ce qui se répercute sur la probabilité de défaillance de l'actionneur. Ainsi, le défaut accélère la vieillissement de l'actionneur lorsque la charge est utilisée dans la modélisation du vieillissement. En effet, le risque de perdre totalement l'actionneur affecté par le défaut est plus important. Cela diminue la capacité du système global à tolérer certaines classes de défauts surtout si la durée de vie résiduelle de l'actionneur en question est faible.

De ce fait et dans le but d'intégrer l'impact du défaut sur la fiabilité des actionneurs, la redistribution des efforts désirés au travers des actionneurs (Ré-allocation) peut être effectuée pour une matrice de pondération optimale $W_u(t)$ choisie comme suit :

$$W_u(t) = \begin{pmatrix} \omega_1(t) & & & 0 \\ & \omega_2(t) & & \\ & & \ddots & \\ 0 & & & \omega_m(t) \end{pmatrix} \tag{3.26}$$

avec

$$\omega_i(t) = 1 - \exp[-(\frac{t}{\alpha_i(t)(1-\gamma_i(t))})^{\beta_i}], \quad i = 1, \dots, m \tag{3.27}$$

où $\gamma_i(t)$ est le facteur de perte d'efficacité de l'actionneur estimée à l'instant t.

Nous proposons l'indicateur (3.27) qui intègre le vieillissement de l'actionneur par rapport au temps, à la charge appliquée ainsi que l'amplitude du défaut détecté. La relation suivante est vérifiée :

$$\left.\begin{array}{ll} g_i(t) \to g_{max} & : u_i^*(t) \to \epsilon \\ g_i(t) \to \epsilon & : u_i^*(t) \to u_{max} \end{array}\right\} \tag{3.28}$$

où g_{max} correspond au stress maximal pouvant être considéré. La sollicitation des actionneurs dans ce cas est inversement proportionnelle à l'amplitude du défaut.

Pour un défaut relativement sévère, l'actionneur défaillant est moins sollicité dans la ré-allocation de la commande respectant les limites imposées par la satisfaction des performances en terme de commande. Cela implique la redistribution des efforts sur les actionneurs les plus fiables en priorité.

3.4 Commande des systèmes sur-actionnés respectant la fiabilité

Garantir la fiabilité d'un système reconfigurable est un défi à résoudre pour répondre aux nouveaux problèmes liés à la commande et la sureté de fonctionnement. Dans cette partie, des solutions au problème de commande des systèmes sur-actionnés sont proposées intégrant la fiabilité des actionneurs.

3.4.1 Méthode de pseudo-inverse

Pour résoudre le problème de commande (3.5) et (3.6), plusieurs méthodes d'optimisation ont été proposées dans la littérature (Bodson, 2002). Dans cette partie, la méthode appelée *pseudo-inverse* basée sur la solution d'un critère de minimisation de la commande est retenue. Comme démontré dans (Bordignon, 1996) si les saturations physiques des actionneurs ne sont pas considérées, le problème (3.5) et (3.6) peut être reformulé tel un problème de minimisation d'énergie sous contrainte d'admissibilité comme suit :

$$\begin{array}{ll} \min\limits_{u} J = \|W_u u(t)\|_2 \\ s.q \quad Bu(t) = v_d(t) \end{array} \tag{3.29}$$

Une solution explicite à ce problème peut être obtenue en fonction de la pseudo-inverse de la matrice B et la matrice de pondération W_u.

Proposition 3.1 *Pour une loi de fiabilité suivant la distribution exponentielle, une stratégie d'allocation préservant les actionneurs et garantissant ainsi la sûreté de fonctionnement du système peut être mise en œuvre pour des entrées de commandes $u(t)$ obtenues comme suit :*

$$u(t) = W_u^{-1}(BW_u^{-1})^{+}v_d(t) \tag{3.30}$$

où $W_u > 0$ est définie par (3.16). $+$ est l'opérateur de pseudo-inverse.

Cependant, l'apparition d'un défaut actionneur nécessite la ré-allocation de la commande. Le problème de ré-allocation de la commande consiste à trouver le vecteur des entrées de commande $u(t)$ minimisant l'énergie et qui satisfait $B_f u(t) = v_d(t)$.

Dans le cas d'une loi de fiabilité suivant une distribution exponentielle, la commande optimale $u(t)$ peut être obtenue par la proposition suivante :

Proposition 3.2 *Après l'apparition des défauts, une méthodologie de ré-allocation de la commande optimale vis-à-vis de la fiabilité des actionneurs garantissant la*

sûreté de fonctionnement du système est proposée pour des entrées de commande calculées explicitement comme suit :

$$u(t) = W_u^{f\,-1}(B_f W_u^{f\,-1})^+ v_d(t) \tag{3.31}$$

où B_f est définie dans (3.8). La matrice de pondération W_u^f est donnée comme dans (3.17).

$$W_u^f = \begin{pmatrix} \frac{\lambda_1}{\lambda_{max}} & & & 0 \\ & \frac{\lambda_2}{\lambda_{max}} & & \\ & & \ddots & \\ 0 & & & \frac{\lambda_m}{\lambda_{max}} \end{pmatrix}$$

Par ailleurs, dans le cas où la loi de Weibull est retenue dans la modélisation de la fiabilité des actionneurs, une méthodologie d'allocation et ré-allocation de la commande optimale vis-à-vis de la fiabilité des actionneurs peut être appliquée comme suit,

Proposition 3.3 *Dans le cas où les saturations physiques des actionneurs ne sont pas considérées, une solution explicite au problème d'allocation et ré-allocation peut être obtenue en tenant compte de l'état de dégradation des actionneurs et de la sévérité du défaut identifié. La commande garantissant la sûreté de fonctionnement du système est calculée par la méthode de la pseudo-inverse comme suit :*

$$u(t) = {W_u}^{-1}(t)(B_f {W_u}^{-1}(t))^+ v_d(t) \tag{3.32}$$

pour une matrice de pondération $W_u(t) > 0$ définie en ligne par (3.26).

$$W_u(t) = \begin{pmatrix} \omega_2(t) & & & 0 \\ & \omega_2(t) & & \\ & & \ddots & \\ 0 & & & \omega_m(t) \end{pmatrix}$$

avec

$$\omega_i(t) = 1 - \exp[-(\frac{t}{\alpha_i(t)(1-\gamma_i(t))})^{\beta_i}], \quad i = 1, \ldots, m \tag{3.33}$$

3.4.2 Méthode de pseudo-inverse généralisée en cascade

Si les limites physiques des actionneurs (3.4) sont considérées dans le problème d'allocation de la commande, une solution admissible respectant les saturations des actionneurs n'existe pas toujours. (Virnig et Bodden, 1994) proposent la pseudo-inverse distribuée (RPI). Cette approche consiste dans une première étape à saturer toutes les entrées de commande qui dépassent théoriquement leurs limites. Puis, une nouvelle solution du problème d'optimisation basée sur les actionneurs non saturés est calculée dans la deuxième étape. D'autre part, (Bordignon, 1996) propose une autre version de la pseudo-inverse redistribuée appelée la pseudo-inverse généralisée en cascade (CGI). Pour cette dernière, la redistribution de la commande est retenue

jusqu'à ce qu'une solution acceptable soit obtenue, ou que toutes les entrées de commandes soient saturées. Toujours dans ce cadre, (Enns, 1998) suggère d'appliquer la technique CGI mais en saturant à chaque itération une seule entrée de commande et en redistribuant à chaque fois le reste des efforts désirés sur les autres actionneurs.

Afin d'intégrer l'estimation de la fiabilité des actionneurs comme indicateur supplémentaire guidant la distribution des efforts désirés, nous proposons une approche CGI modifiée. Le principe consiste à choisir dans la première étape la matrice de pondération en fonction des indicateurs de fiabilité. Les matrices (3.16) et (3.29) sont choisies respectivement dans le cas d'une loi exponentielle ainsi que dans la loi de Weibull. La commande correspondante à chaque actionneur est obtenue comme suit :

$$u_i^0(t) = {w_i}^{-1}(B_i {w_i}^{-1})^+ v_d(t)$$

avec

$$B = [B_1 \ B_2 \ \dots \ B_m], \quad B_i \in \mathbb{R}^{p\times 1}$$

et

$$W_u = \text{diag}\{w_1 \ w_2 \ \dots \ w_m\}, \quad w_i \in \mathbb{R}^1$$

Puis, si des entrées de commande atteignent théoriquement leurs saturations, l'actionneur le plus fiable est saturé :

$$\begin{cases} u_i^0(t) = u_i^{sat} & \text{si} \ \ w_i = w^{min} \\ u_i^0(t) = u_i(t) & \text{si} \ \ w_i \neq w^{min} \end{cases}$$

sachant que $w^{min} = \min(w_i), \quad i = 1, \dots, m$. u_i^{sat} représente la saturation du i^{eme} actionneur.

Ensuite, une nouvelle valeur des efforts désirés est calculée et distribuée aux actionneurs en excluant l'actionneur le plus fiable (saturé) :

$$v_d^1(t) = v_d(t) - B_s u_s(t)$$

avec

$$\begin{cases} u_s(t) = u_i^{sat} & \text{pour} \ \ W_{ui} = W_u^{min} \\ B_s = B_i & \text{pour} \ \ s = i \end{cases}$$

où $v_d(t)$ représente les efforts désirés à distribuer sur le reste des actionneurs en excluant l'actionneur le plus fiable. Cette procédure sera répétée en saturant à chaque itération l'actionneur le plus fiable de l'ensemble jusqu'à l'obtention d'une solution réalisable ou jusqu'à ce que tous les actionneurs soient saturés.

3.4.3 Méthode du point fixe

Par ailleurs, si les limites physiques des actionneurs sont considérées, le problème d'allocation à deux étapes (3.5)-(3.6) peut être reformulé en un problème de minimisation mixte. Dans ce cas, la commande optimale est l'objet du problème d'optimisation suivant :

$$u = \underset{u_{\min} \leq u \leq u_{\max}}{\arg\min} \quad (1-\epsilon)\|Bu - v_d\|_2 + \epsilon\|W_u u\|_2 \tag{3.34}$$

où $\epsilon \in [0,\ 1]$ est un scalaire à choisir.

Pour résoudre ce problème, l'algorithme de point fixe proposé par (Burken *et al.*, 2001) peut être utilisé. Une solution itérative est obtenue pour $u_d = 0$ comme suit,

$$u^k = \text{sat}[(1-\epsilon)\eta B^T v_d + (I_m - \eta H)u^{k-1}], \quad k = 1, \ldots, N \tag{3.35}$$

où N est le nombre maximum d'itérations considérées avec

$$\begin{aligned} H &= (1-\epsilon)B^T B + \epsilon Q_2 \\ Q_2 &= W_u^T W_u \\ \eta &= \|H\|_F^{-1} \end{aligned}$$

$\|H\|$ représente la norme de Frobenius de la matrice H. sat(.) désigne la fonction de saturation des actionneurs définie comme suit,

$$\text{sat}_i(u) = \begin{cases} \underline{u}_i, & u_i < \underline{u}_i \\ u_i, & \underline{u}_i \leq u_i \leq \bar{u}_i, \quad i = 1, \ldots, m \\ \bar{u}_i, & u_i > \bar{u}_i \end{cases}$$

où $\underline{u} = u_{min}$ et $\bar{u} = u_{max}$.

Dans le cas d'une distribution exponentielle, la matrice de pondération dans le cas nominal est choisie en fonction des taux de défaillances de base des actionneurs (3.16). Après l'apparition d'un défaut, la matrice B est remplacée par B_f dans (3.35). La ré-allocation est appliquée dans ce cas pour une nouvelle matrice de pondération W_u^f en tenant compte de la dégradation des actionneurs (3.17).

En revanche, pour une loi de Weibull, la matrice de pondération $W_u(t)$ définie dans (3.26) est choisie. La distribution des efforts désirés est assurée en tenant compte de l'état de dégradation des actionneurs tout en respectant les saturations physiques des actionneurs.

Remarque 3.1 *L'algorithme du point fixe présenté dans cette partie est interprété comme la recherche du gradient guidé par la valeur de η. Dans (Burken* et al., *2001), les auteurs recommandent de choisir à chaque instant t les entrées de commande obtenues $u(t-T)$ comme point initial $u^k(t)$, $k = 0$. Ainsi, la convergence de la solution u^N vers un unique optimum est assurée.*

3.4.4 La méthode de l'ensemble actif

L'algorithme de l'ensemble actif *(Active set Method)* proposé par (Harkegard, 2002) est utilisé également pour résoudre le problème d'allocation de la commande en tenant compte des saturations. Dans cette méthode, le problème d'optimisation mixte (3.34) est proposé comme suit :

$$u^* = \underset{u_{\min} \leq u \leq u_{\max}}{\arg\min} \quad \|Bu - v\|_2 + \rho\|W_u(u - u_d)\|_2 \tag{3.36}$$

où u_d est l'entrée de commande désirée avec $\rho >> 1$.

Le problème d'allocation (3.36) peut être reformulé sous la forme suivante :

$$\arg\min_{u_{\min}\leq u\leq u_{\max}} \|Bu - v_d\|_2 + \rho\|W_u(u-u_d)\|_2 = \arg\min_{u_{\min}\leq u\leq u_{\max}} \left\| \begin{pmatrix} \rho^{\frac{1}{2}}B \\ W_u \end{pmatrix} u - \begin{pmatrix} \rho^{\frac{1}{2}}v_d \\ W_u u_d \end{pmatrix} \right\|_2 \tag{3.37}$$

Avec la méthode de l'ensemble actif, la commande $u(t)$ solution du problème d'allocation est obtenue par la résolution d'une série de contraintes d'égalité.

L'algorithme des moindres carrés pondérés basé sur la méthode de l'ensemble actif (Harkegard et Glad, 2004) est utilisé pour trouver une meilleur approximation à l'entrée de commande virtuelle v_d. Dans ce contexte, le problème d'allocation (3.36) devient :

$$u = \arg\min_{u} \|\bar{A}u - \bar{b}\|_2 \tag{3.38}$$

$$\begin{matrix} Bu = v \\ \bar{C}u \geq U \end{matrix} \tag{3.39}$$

où

$$\bar{C} = \begin{bmatrix} I \\ -I \end{bmatrix} \quad \text{et} \quad U = \begin{bmatrix} u_{min} \\ -u_{max} \end{bmatrix} \tag{3.40}$$

Ce problème est équivalent à un problème des moindres carrés pondérés avec :

$$\bar{A} = \begin{pmatrix} \rho^{\frac{1}{2}}B \\ W_u \end{pmatrix} \tag{3.41}$$

$$\bar{b} = \begin{pmatrix} \rho^{\frac{1}{2}}v \\ W_u u_d \end{pmatrix} \tag{3.42}$$

Afin de contribuer à une méthode d'allocation effective garantissant la fiabilité du système, nous proposons de considérer un choix optimal de la matrice de pondération. Dans le cas d'une distribution exponentielle, la matrice de pondération dans le cas nominal est choisie en fonction des taux de défaillance de base des actionneurs (3.16). Après l'apparition du défaut, la matrice B est remplacée par B_f dans (3.39) et (3.41). La ré-allocation est appliquée dans ce cas pour une nouvelle matrice de pondération W_u^f (3.16) dans (3.41) et (3.42) en tenant compte de la dégradation des actionneurs.

En revanche, pour une loi de Weibull, nous choisissons la matrice de pondération $W_u(t)$ définie dans (3.26). La distribution des efforts désirés est assurée en tenant compte de l'état du vieillissement des actionneurs tout en respectant les saturations physiques.

3.5 Commande linéaire quadratique garantissant la fiabilité des systèmes sur-actionnés

Comme illustrée précédemment, la stratégie d'allocation est une alternative permettant de garantir les performances désirées des systèmes sur-actionnés en deux

étapes (figure 3.5). Il s'agit de calculer les efforts désirés par un contrôleur puis de distribuer ces derniers via un module d'allocation. En revanche, un contrôleur classique linéaire quadratique (figure 3.6) peut être aussi utilisé pour garantir la stabilité et distribuer les efforts désirés en une seule étape.

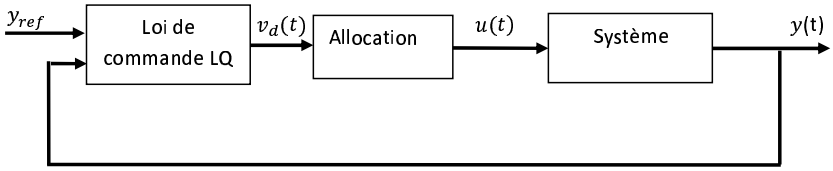

FIGURE 3.5 – Commande linéaire quadratique avec allocation

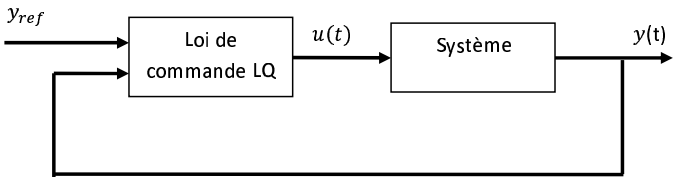

FIGURE 3.6 – Commande linéaire quadratique classique

Considérons le système sur-actionné représenté dans la figure (3.5). Pour une stratégie d'allocation, l'entrée de commande optimale $u(t)$ est obtenue en fonction des efforts désirés $v_d(t)$. La commande virtuelle $v_d(t)$ peut être calculée par une approche linéaire quadratique pour des matrices de pondération $Q_2 \geq 0, \quad R_2 > 0$ données comme suit :

$$v_d(t) = G_a y_{ref}(t) - K_a x(t) \tag{3.43}$$

avec

$$\begin{aligned} G_a &= R_2^{-\frac{1}{2}}(G_0 R_2^{-\frac{1}{2}})^+ \\ K_a &= R_2^{-1} B_u^T S_2 \\ G_0 &= C(B_u L - A)^{-1} B_u \end{aligned} \tag{3.44}$$

où S_2 est la seule matrice symétrique semi-définie positive, solution de l'équation algébrique de Riccati suivante :

$$A^T S_2 + S_2 A + Q_2 - S_2 B_u R_2^{-1} B_u^T S_2 = 0$$

Comme prouvé dans (Harkegard et Glad, 2004), une commande linéaire quadratique classique équivalente peut être obtenue dans le cas des systèmes sur-actionnés en respectant les égalités matricielles suivantes :

$$\begin{aligned} Q_1 &= Q_2 \\ R_1 &= W_u^2 + B^T(R_2 - (BW_u^{-2}B^T)^{-1})B \end{aligned} \tag{3.45}$$

où la commande $u(t)$ est obtenue par la théorie de la commande optimale comme suit :

$$\begin{array}{l} u(t) = Gy_{ref}(t) - Kx(t) \\ G = R_1^{-\frac{1}{2}}(G_0 R_1^{-\frac{1}{2}})^+ \\ K = R_1^{-1} B_u^T S_1 \end{array} \tag{3.46}$$

avec S_1, la seule matrice symétrique semi-définie positive, solution de l'équation algébrique de Riccati suivante :

$$A^T S_1 + S_1 A + Q_1 - S_1 B_u R_1^{-1} B_u^T S_1 = 0$$

Pour synthétiser une commande LQ équivalente garantissant la fiabilité des systèmes sur-actionnés, nous proposons de considérer la fiabilité des actionneurs dans le choix de la matrice W_u définissant R_1. En fonctionnement nominal, la matrice de pondération est choisie en fonction des indicateurs de fiabilité comme suit

$$W_u = \begin{pmatrix} \frac{\lambda_1^0}{\lambda_{max}^0} & & & 0 \\ & \frac{\lambda_2^0}{\lambda_{max}^0} & & \\ & & \ddots & \\ 0 & & & \frac{\lambda_m^0}{\lambda_{max}^0} \end{pmatrix} \tag{3.47}$$

Après l'apparition des défauts, une estimation de l'état de dégradation des actionneurs est possible. La stratégie de tolérance aux défauts est appliquée en fonction de la matrice de pondération W_u^f :

$$W_u^f = \begin{pmatrix} \frac{\lambda_1}{\lambda_{max}} & & & 0 \\ & \frac{\lambda_2}{\lambda_{max}} & & \\ & & \ddots & \\ 0 & & & \frac{\lambda_m}{\lambda_{max}} \end{pmatrix}$$

Dans le cas de défauts accommodables, la ré-estimation de la matrice de pondération est suffisante pour compenser les défauts et assurer la distribution des efforts désirés. Or, dans certains cas, la reconfiguration de la loi de commande est nécessaire. Un nouveau gain K_f garantissant la fiabilité peut être obtenu en fonction de la matrice de pondération W_u^f comme proposé dans (Sauter *et al.*, 2002).

3.6 Application

Pour illustrer la méthodologie proposée dans ce chapitre, nous considérons le simulateur ADMIRE développé par the Group of Aeronautical Research and Technology in Europe (GARTEUR). Un modèle linéarisé autour d'une vitesse de 0.22 $Mach$ et une altitude de $3000m$ est considéré.

Les états du système sont notés $x = [\alpha\ \beta\ p\ q\ r]^T$. Les sorties à contrôler $y = [\alpha\ \beta\ p]$ où, α est l'angle d'attaque (rad), β est l'angle d'assiette de l'avion (rad), p est la vitesse de roulis (rad/s), q est la vitesse de tangage (rad/s) et r la vitesse de lacet (rad/s). Les entrées de commande associées représentent respectivement le

détournement du canard, l'aile droit, l'aile gauche et la gouverne. Le modèle linéarisé est donné sous forme d'une représentation d'état linéaire (3.1) avec :

$$A = \begin{bmatrix} -0.5432 & 0.0137 & 0 & 0.9778 & 0 \\ 0 & -0.1179 & 0.2215 & 0 & -0.9661 \\ 0 & -10.5128 & -0.9967 & 0 & 0.6176 \\ 2.6221 & -0.0030 & 0 & -0.5057 & 0 \\ 0 & 0.7075 & -0.0939 & 0 & -0.2127 \end{bmatrix}$$

$$B_u = \begin{bmatrix} 0.0069 & -0.0866 & -0.0866 & 0.0004 \\ 0 & 0.0119 & -0.0119 & 0.0287 \\ 0 & -4.2423 & 4.2423 & 1.4871 \\ 1.6532 & -1.2735 & -1.2735 & 0.0024 \\ 0 & -0.2805 & 0.2805 & -0.8823 \end{bmatrix}$$

Dans cette application et pour simplifier l'illustration, la dynamique des actionneurs est négligée. Un modèle approximé est considéré avec :

$$B_u = B_v B$$

et

$$B_v = \begin{bmatrix} 0_{2\times 3} \\ I_{3\times 3} \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & -4.2423 & 4.2423 & 1.4871 \\ 1.6532 & -1.2735 & -1.2735 & 0.0024 \\ 0 & -0.2805 & 0.2805 & -0.8823 \end{bmatrix}$$

Le vecteur des entrées de commande virtuelle représentant l'ensemble des efforts désirés $v_d(t)$ contient l'accélération angulaire de roulis, le tangange et le lacet produits par la commande.

Dans ce qui suit, deux exemples sont présentés. Dans le premier exemple, la loi de distribution exponentielle est considérée pour modéliser la fiabilité des actionneurs. Un choix de la matrice de pondération est imposé considérant les caractéristiques des actionneurs. Les entrées de commande optimales ainsi que l'évaluation de la fiabilité des actionneurs seront comparées avec les résultats obtenus pour une matrice de pondération classique $W_u = I$. Dans le deuxième exemple, la loi de Weibull et la dégradation des actionneurs par rapport aux temps, à la charge et au défaut sont considérées dans l'allocation et la ré-allocation de la commande.

3.6.1 Approche basée sur la loi exponentielle

Dans cette partie et afin de présenter les résultats dans une fenêtre de temps relativement petite, les valeurs des taux de défaillance des actionneurs sont changées d'échelle. Ces dernières seront considérées avec des valeurs très grandes et présentées dans le tableau suivant :

Le changement d'échelle permet simplement de visualiser sur une même figure à la fois la variation des entrées de commande et son impact sur la fiabilité des

TABLE 3.1 – Taux de défaillance des actionneurs

Taux de défaillance de base	
λ_1^0	1e-3 h^{-1}
λ_2^0	5e-3 h^{-1}
λ_3^0	9e-3 h^{-1}
λ_4^0	4e-3 h^{-1}

actionneurs avec des horizons plus courts adaptés à la théorie de la commande. Dans un cas normal, il faudrait visualiser l'impact de la commande à travers des simulations ayant des horizons très longs. Pour simplifier le nombre de simulations, nous avons donc artificiellement rendu les phénomènes plus proches dynamiquement ce qui en réalité n'affecte pas le comportement des algorithmes proposés.

Dans cet exemple, une stratégie d'allocation et de ré-allocation préservant les actionneurs par une gestion optimale des charges attribuées est appliquée. Les efforts désirés sont distribués aux actionneurs pour une matrice de pondération W_u choisie selon la proposition 3.1.

La figure (3.7) montre l'évolution de la sortie contrôlée dans le cas nominal. Les entrées de commande associées sont présentées dans la figure (3.8).

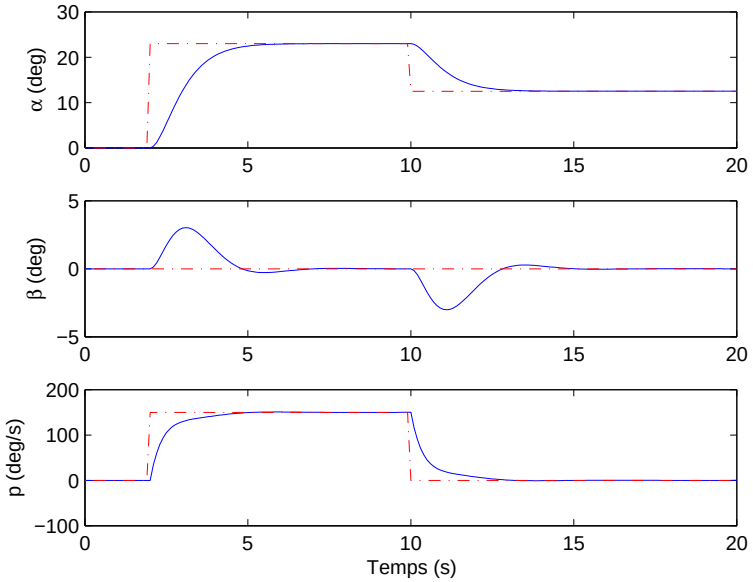

FIGURE 3.7 – Évolution de la sortie dans le cas nominal

L'actionneur 3, considéré comme l'actionneur le moins fiable est moins sollicité dans le cas d'une matrice optimale comparativement au choix classique. Cela nécessite la distribution des efforts sur les autres actionneurs. Cette distribution est réalisée tout en respectant la fiabilité des actionneurs.

Comme illustré à la figure (3.8), pour le choix d'une matrice W_u optimale,

les efforts désirés sont distribués différemment comparativement au choix classique $W_u = I_4$.

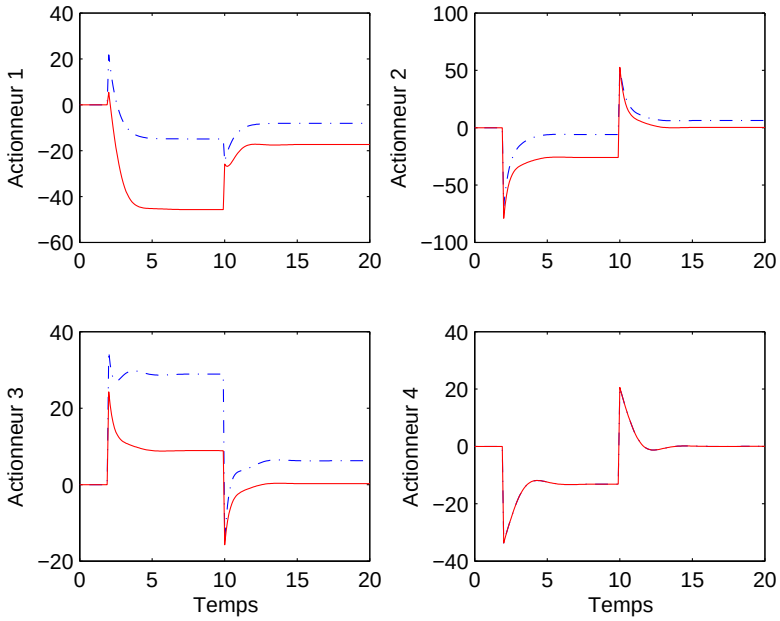

FIGURE 3.8 – Entrées de commande dans le cas nominal ($W_u = I_4$ en discontinu, W_u optimale en continu)

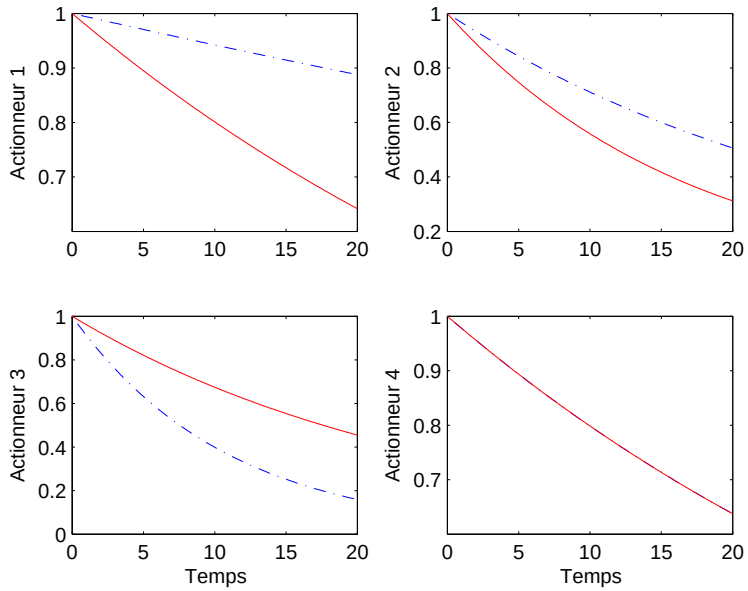

FIGURE 3.9 – Évolution de la fiabilité des actionneurs dans le cas nominal ($W_u = I_4$ en discontinu, W_u optimale en continu)

En effet, l'actionneur le plus fiable (caractérisé par le plus petit taux de défaillance) est plus sollicité comparativement au choix classique. Cette distribution permet d'équilibrer les charges appliquées sur les différents actionneurs et de préserver l'ensemble des actionneurs dans le temps. Ce résultat est illustré dans la figure (3.9). Pour une matrice de pondération optimale, la fiabilité des actionneurs évaluée a priori à la fin de la mission est supérieure à $R_i(t_m) > 0.38,\ \forall i \in [1,\ 4]$.

Or le risque de perdre l'actionneur le moins fiable est beaucoup plus important dans le choix classique où $R_3(t_M) = 0.18$. Ce résultat montre qu'avec une gestion optimale des charges appliquées sur les actionneurs, la sûreté de fonctionnement du système peut être améliorée.

Pour poursuivre notre illustration, nous allons considérer une perte d'efficacité du premier actionneur $\gamma_1 = 0.5$ à l'instant $t = 7s$. Après la détection et l'identification du défaut, une nouvelle matrice de pondération est calculée en ligne. La proposition (3.2) est appliquée afin de redistribuer l'ensemble des efforts désirés et obtenir ainsi, une nouvelle loi de commande respectant la dégradation des actionneurs par rapport à la charge appliquée. La figure (3.10) montre l'évolution des entrées de commande dans le cas dégradé pour un choix optimal de la matrice de pondération (en continu) ainsi que pour le choix classique (en discontinu).

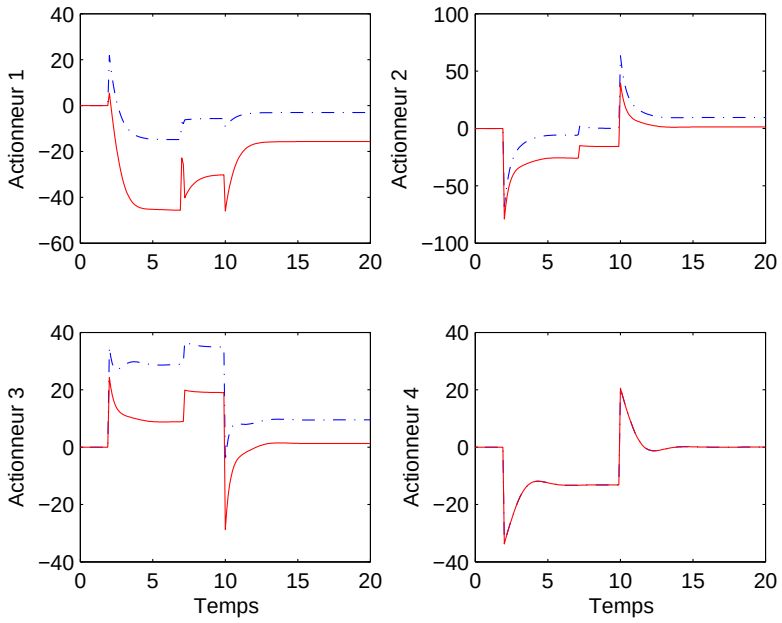

FIGURE 3.10 – Entrées de commande dans le cas dégradé

Comme le montre la figure (3.10), les efforts désirés sont distribués après l'apparition du défaut tenant compte de l'état de dégradation des actionneurs à l'instant t_f. Par exemple, le premier actionneur considéré comme le plus fiable, est plus stressé par rapport au cas classique et cela malgré la perte de son efficacité. Cela se traduit par le fait que son état de dégradation n'est pas critique par rapport aux autres actionneurs considérés sains. En revanche, l'actionneur 3 théoriquement sain reste

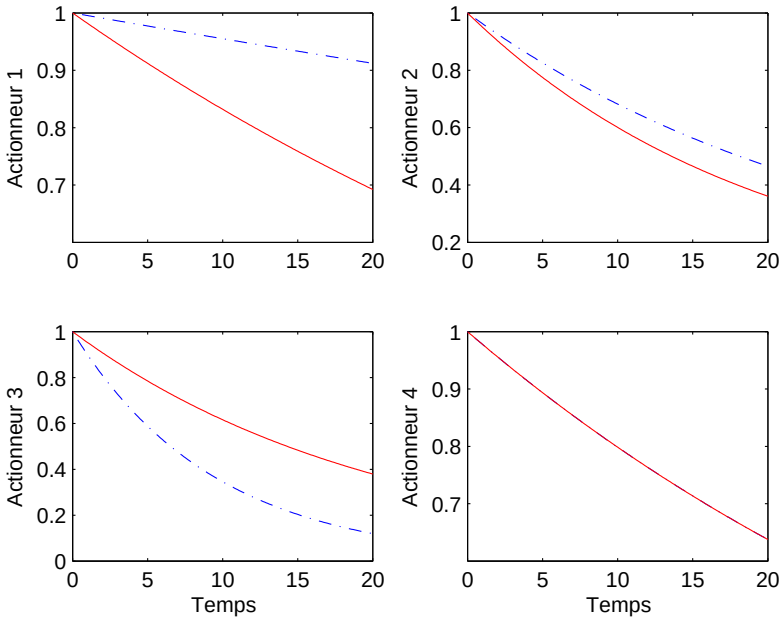

FIGURE 3.11 – Évolution de la fiabilité des actionneurs dans le cas dégradé

toujours moins stressé par rapport au cas classique.

Ce constat est confirmé par la figure (3.11). Nous remarquons que les actionneurs 3 et 4 sont les moins fiables. L'algorithme de ré-allocation sollicite ces derniers avec moins de priorité bien qu'ils ne soient pas affectés par le défaut. La fiabilité de l'actionneur dégradé est importante. Même avec l'apparition du défaut, la probabilité que l'actionneur défaillant tombe en panne est faible. Finalement nous constatons que la fiabilité des actionneurs pour un choix classique vérifie $\min(R_i(t)) = 0.15$. Or, dans le cas d'une matrice optimale, La fiabilité des actionneurs $R_i(t) > 0.38,\ \forall i \in [1,\ 4]$. Cela augmente la sûreté de fonctionnement du système et minimise le risque qu'un second actionneur tombe en panne durant la mission.

3.6.2 Approche basée sur la loi de Weibull

Dans cet exemple, le vieillissement des actionneurs est considéré dans l'allocation et la ré-allocation de la commande. Le tableau suivant présente les paramètres de la loi de Weibull modélisant la fiabilité de chaque actionneur.

Nous avons retenu des facteurs d'échelle anormalement faibles pour des raisons de présentation et d'adaptation avec les horizons de la commande. Ceci permet d'exagérer les phénomènes pour les rendre plus lisibles.

Les efforts désirés calculés par le régulateur sont distribués sur les actionneurs en tenant compte de l'état de dégradation des actionneurs estimé en ligne. La matrice de pondération $W_u(t)$ est choisie comme dans la proposition 3.3, où dans le cas nominal, $\gamma = I_4$. Les entrées de commande obtenues sont présentées dans la figure (3.12).

TABLE 3.2 – Modèle de vieillissement des actionneurs

Paramètres du modèle de vieillissement				
Act.1	α_1^0	26	β_1^0	3
Act.2	α_2^0	36	β_2^0	3
Act.3	α_3^0	50	β_3^0	3
Act.4	α_4^0	44	β_4^0	3

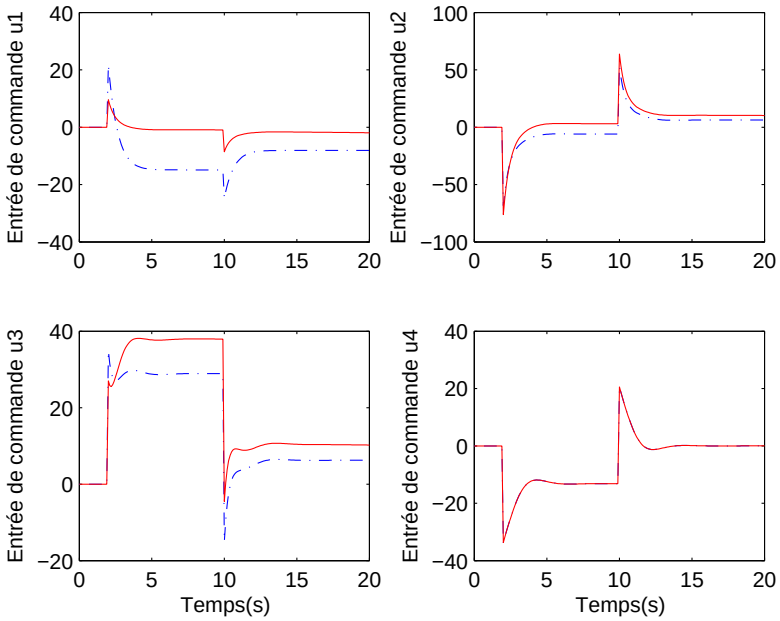

FIGURE 3.12 – Entrées de commande dans le cas nominal

Dans ce cas, les entrées de commande sont calculées en tenant compte du vieillissement des actionneurs. Le premier actionneur ayant le plus petit paramètre d'échelle est le moins fiable. La tendance du vieillissement avec le risque que cet actionneur tombe complètement en panne durant la mission est plus importante par rapport aux autres actionneurs. Ces caractéristiques expliquent le fait que le premier actionneur soit moins stressé dans le cas d'une matrice de pondération optimale. En contrepartie et afin d'assurer la distribution des efforts désirés, le troisième actionneur est stressé durant la mission en tenant compte de son vieillissement. Le quatrième actionneur est insensible au stress. Cela dépend de la modélisation et la conception du système.

La figure (3.13) montre l'évolution de la fiabilité des actionneurs, pour les paramètres de base (en tiret), avec charge pour un choix classique (discontinu) et avec charge pour un choix optimal de la matrice de pondération (continu). Pour le scénario considéré, la fiabilité des actionneurs évaluée suivant la proposition (3.3) est $R_i(t) > 0.23,\ i \in [1, \ldots, m]$. Or, pour le choix classique, $\min(R_i(t))\ \forall i \in [1,\ 4]$ est égal à 0.15.

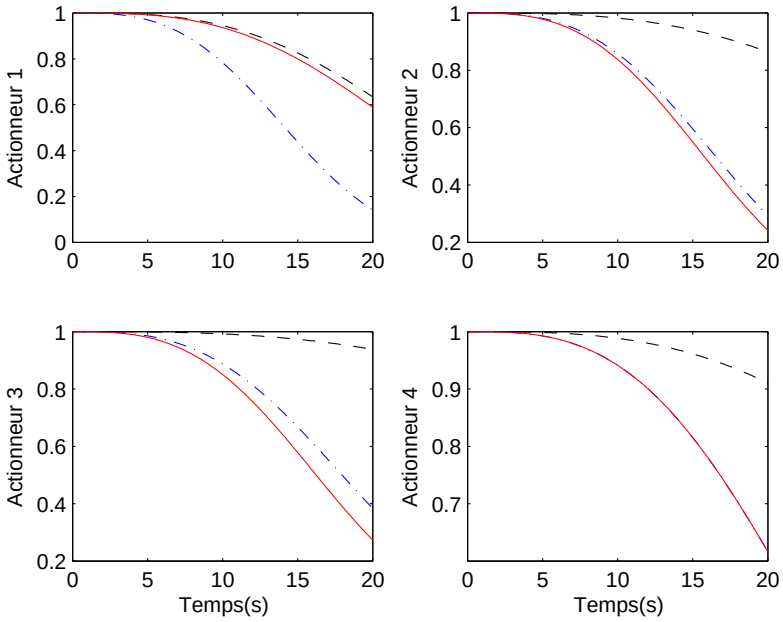

FIGURE 3.13 – Évaluation de la fiabilité sans défaut

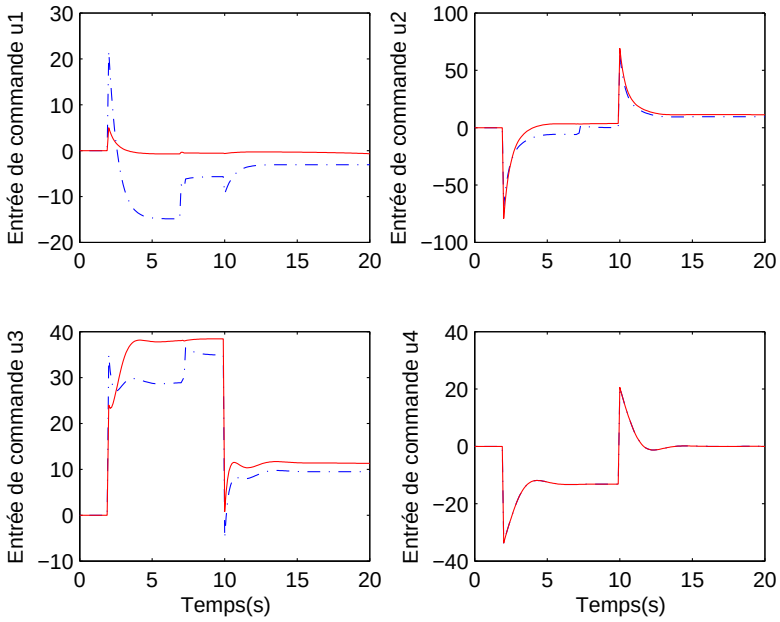

FIGURE 3.14 – Entrées de commande dans le cas dégradé

Ce résultat montre que le risque qu'un actionneur tombe en panne durant la mission est moins important pour la stratégie proposée. La capacité d'accommoder les défauts et satisfaire les performances désirées jusqu'à la fin de la mission est

significative comparativement à la stratégie classiquement utilisée.

Nous allons considérer maintenant une perte d'efficacité du premier actionneur à l'instant $t_f = 7sec$ d'une valeur $\gamma_1 = 0.50$. La figure (3.14) montre l'évolution des entrées de commande dans le cas dégradé.

Dans ce cas, l'impact du défaut sur la fiabilité de l'actionneur est considéré. Comme expliqué dans les sections précédentes, le défaut accélère le vieillissement de l'actionneur. Le premier actionneur est moins stressé dans la distribution des efforts désirés. Afin d'assurer les performances désirées, le troisième actionneur considéré comme l'actionneur le moins détérioré est plus sollicité comparativement au choix classique. La nouvelle commande est appliquée à chaque instant en tenant compte de la capacité des actionneurs à achever la mission avec une probabilité plus élevée.

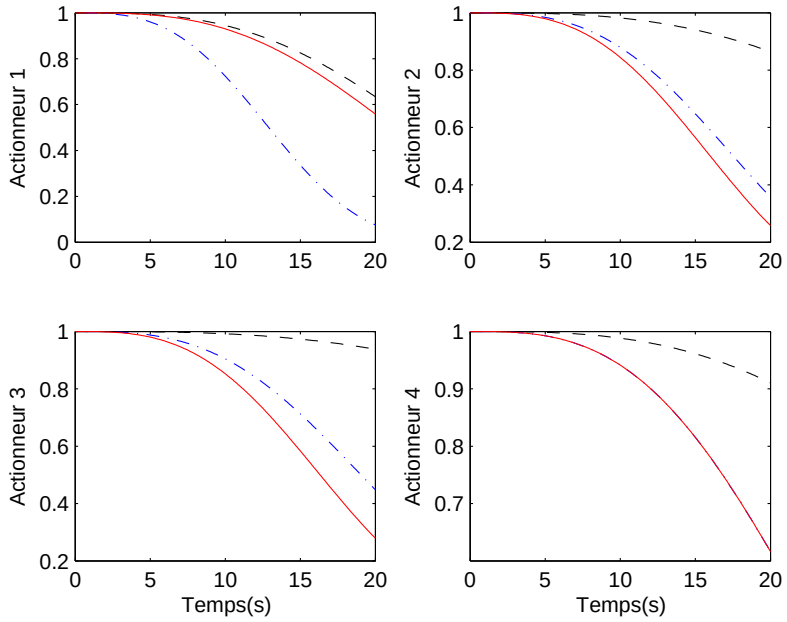

FIGURE 3.15 – Évaluation de la fiabilité avec défaut

La figure (3.15) montre l'évaluation du vieillissement des actionneurs (en tiret), avec charge pour un choix classique (discontinu) et avec charge pour un choix optimal de la matrice de pondération (continu).

Pour le scénario considéré, la fiabilité des actionneurs évaluée suivant la proposition (3.3) considérant le défaut est $R_i(t) > 0.23,\ i \in [1, \ldots, m]$. Or, pour le choix classique, $\min(R_i(t)) = 0.10$. Le résultat montre qu'il est possible d'augmenter la sûreté de fonctionnement du système en minimisant le risque qu'un actionneur tombe en panne avant la fin de la mission et de conserver ainsi l'avantage du suractionnement.

3.7 Conclusion

Dans ce chapitre, nous avons proposé une méthodologie de synthèse de lois de commande tolérante aux fautes garantissant la sûreté de fonctionnement des systèmes sur-actionnés. Une méthode effective d'allocation et de ré-allocation de la commande en tenant compte de la fiabilité des actionneurs est développée. La méthodologie proposée s'appuie sur l'idée d'imposer une matrice de pondération spécifique dans le problème d'allocation et ré-allocation de la commande. La matrice de pondération est choisie en se basant sur l'estimation de la fiabilité des actionneurs ainsi que leur vieillissement. Pour cela, nous avons retenu le modèle de Cox suivant une loi exponentielle ainsi qu'une distribution de Weibull pour modéliser la dégradation des actionneurs intégrant l'impact des charges appliquées. Sous les hypothèses considérées, des indicateurs basés sur les paramètres de fiabilité guidant la synthèse de la commande sont proposés et déclinés sur plusieurs méthodes d'allocation et ré-allocation. La méthodologie proposée est illustrée au travers d'un exemple aéronautique. Les résultats montrent une efficacité des solutions proposées. Ce travail est donc une première contribution avec des résultats encourageants.

Chapitre 4

Active fault tolerant controller synthesis with Respect to actuators criticality

In this chapter, actuator criticality analysis is integrated in the design of active fault-tolerant control systems. The main objective consists on the design of a fault-tolerant controller which guarantees a highest overall system reliability while still maintaining immediate stability and tracking performance of reconfigured system. Such an objective is achieved by incorporating an actuator criticality indicator in the fault-tolerant controller design, which is implemented by managing effectively the control inputs in order to improve the system dependability both in nominal operation and in the presence of faults. Actuator criticality analysis of systems modeled by a state space representation is proposed. A design of the fault-tolerant controller is reformulated as a linear matrix inequality problem.

4.1 Introduction

In the control design for safety-critical systems, reliability, dependability, and safety are the basic design requirements. Safety-critical systems should be able to maintain a satisfactory closed-loop performance in nominal cases and even more challenging and important to adapt with faulty situations. These types of adaptive systems are known as Fault-Tolerant Control Systems (FTCS). The aim of FTCS is to keep plant available by the ability to achieve the objectives assigned in the faulty cases and to accept reduced performance when critical faults occur Zhang et Jiang (2003). Currently, various approaches for FTCS design have been proposed and developed in the literature. Overviews on the development of FTCS have been provided in survey papers and books such as Blanke *et al.* (2001); Zhang et Jiang (2008) and Noura *et al.* (2009) for example. Among these approaches, some of them require an on-line Fault Detection and Isolation (FDI) or Fault Detection and Diagnosis (FDD) mechanism. These approaches are called Active Fault-Tolerant Control Systems (AFTCS) Zhang et Jiang (2008).

Therefore, it is important to enhance the system dependability not only by improving reliability of individual components, or by designing control systems which compensate the effect of faults but also by taking into consideration the degradation of actuators life time. One motivation to integrate information about actuators health level in the controller design is to improve the safety and the dependability of the reconfigurable system as an ultimate goal of introduction of a fault-tolerant control system, or in general, a fault-tolerant system. Indeed, overall system reliability can be improved by a fault-tolerant control system which uses effectively the

available actuation redundancy (hardware and analytical) both in nominal case and after fault occurrence. Consequently, the system can remain operational for a longer duration with respect to the acceptable control performance requirements.

Some research work have introduced reliability analysis with FTCS. Wu (2001a,b) and Wu et Patton (2003) have used Markov chain to model the system reliability where subsystems are supposed to reach two states : intact (available) or failed (unavailable) states. In Staroswiecki et Hoblos (2004) and Staroswiecki et Berdjag (2010), the authors proposed a sensor and actuator reconfiguration strategy based on physical redundancy. The reliability analysis provides some indicators to select the optimal set for reconfiguration strategy. In a similar way, He *et al.* (2009) has considered the reliability of sensor faults in the filtering design issue. A reconfiguration mechanism of FTC strategy incorporating reliability analysis under dynamic behavior constraints has been proposed in Guenab *et al.* (2010).

In this paper, on-line actuator criticality evaluation is integrated in the design of an active fault-tolerant controller. The novelty of the proposed approach is to synthesize a fault-tolerant controller which achieves the control objective with a highest overall system reliability level, therefore named as a reliable fault-tolerant controller. Such an objective is achieved/guaranteed by respecting the degradation and the criticality of each actuator in the desired control efforts distribution. Indeed, this objective improves the dependability of the reconfigurable system and keeps the set of actuators available as long as possible. The main idea consists on minimizing the solicitation of the critical actuators in the control efforts distribution to avoid potential overload/damage of the critical actuators and to maintain the overall handicapped system with longer safe operation, therefore a higher reliability level. To select the critical actuators, sensitivity analysis of the overall system reliability compared to the actuators degradation should be carried out *a priori*.

For achieving the above objective, the problem of fault-tolerant control design with incorporation of actuator criticality level is reformulated as a Linear Matrix Inequalities (LMIs) problem, making use of the power of such a constrained optimization tool.

Among various methods, the active fault tolerant controller synthesis guarantees the overall system reliability and safety is achieved through two approaches. The first method is based on the design of an optimal controller which improves the overall system reliability in the nominal case using LMI approach. In degraded mode, fault tolerant control by compensation is used where the control inputs in the faulty case are applied among to the system based on the nominal effective controller. The second method proposed in this chapter is based on Admissible Model Matching (AMM) approach using LMI regional pole placement. the main advantage of the AMM FTC is the ability to obtain admissible solutions compared to the classical Pseudo-Inverse Method (PIM) which leads to unstable behaviors Gao et Antsaklis (1991); Tornil-Sin *et al.* (2009). In the proposed method, effective admissible solution is proposed in nominal based on reliability analysis and actuators criticality. After fault occurrence, the LMI regional pole placement is used to reach the admissible behavior by considering the actuators aging. The actuators criticality is re-actived taking into account the actuators aging cased before fault occurrence.

4.2 Preliminaries and problem statement

Let us consider the linearized dynamic of the system given by :

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) \end{aligned} \tag{4.1}$$

where $A \in \mathbb{R}^{n\times n}$, $B_u \in \mathbb{R}^{n\times m}$ and $C \in \mathbb{R}^{p\times n}$ are respectively, the state, the control and the output matrices. $x \in \mathbb{R}^n$ is the system state, $u \in \mathbb{R}^m$ is the control input, $y \in \mathbb{R}^p$ is the system output and (A, B) is assumed to be stabilizable.

In nominal operation, the control law $u(t)$ is designed with the standard linear state feedback control law as follows :

$$u(t) = -Kx(t) \tag{4.2}$$

Indeed, several methods have been proposed to design a feedback controller K which satisfies the condition $A - BK \in \mathcal{M}_a$ where, $\mathcal{M}_a$ presents a family of acceptable closed-loop behaviors called *admissible behaviors* Staroswiecki (2005a).

Définition 4.1 (Admissibility) *The triple $(A, B, K) \in \mathcal{M}_a$ is called admissible if and only if,*

$$\mathcal{M}_a = \{(A, B, K) : \Phi_{\mathcal{M}}(A, B, K) \leq 0\} \tag{4.3}$$

where $\Phi_{\mathcal{M}}(A, B, K)$ are the set of constraints that guarantee $(A - BK) \in \mathcal{M}_a$ can be achieved with the control law $u(t) = -Kx(t)$.

When this approach is applied to FTC, the nominal behavior is characterized by a given pair of matrices (A_n, B_n) while the post-fault behavior is characterized by a different pair (A_f, B_f). For the nominal system operation, a state feedback controller K_n that satisfies some nominal control specifications is available such that

$$\dot{x}(t) = (A_n - B_nK_n)x(t) = M^*x(t) \tag{4.4}$$

where M^* is known as the reference model.

Then, when actuator faults occur, the system (4.1) can be modeled in a degraded functional mode as follows :

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B_fu(t) \\ y(t) &= Cx(t) \end{aligned} \tag{4.5}$$

where the matrix B_f is written according to the nominal control input matrix B. In fact, B_f and B are linked by the control effectiveness factors $\gamma_i \in [0,\ 1]$, $i = 1, \ldots, m$, as follows Zhang et Jiang (2002b) :

$$B_f = B\Gamma, \quad \Gamma = \begin{pmatrix} \gamma_1 & & & 0 \\ & \gamma_2 & & \\ & & \ddots & \\ 0 & & & \gamma_m \end{pmatrix} \tag{4.6}$$

Indeed, if $\gamma_i = 1$, then the i^{th} actuator is considered to be fault-free. Nevertheless, when $0 < \gamma_i \leq 1$, the considered fault is a partial loss of control effectiveness. Moreover, when $\gamma_i = 0$ critical failure is considered and the actuator is out of order.

After fault occurrence, the system matrices change to (A, B_f) and the goal of the fault accommodation is to find the controller K_f that provides an exact (or best) matching to a nominal behavior where $(A - B_f K_f) \in \mathcal{M}_a$. In fact, while this study deals with the fault-tolerant controller design, it is assumed that fault is detected and isolated at time $t = t_f$ by using a FDI scheme.

Définition 4.2 *The faulty system (A, B_f) is fault-tolerant using active FTC if and only if the set :*

$$\mathcal{K}_f(A, B_f) = \{K_f : \Phi_{\mathcal{M}}(A, B_f, K_f) \leq 0\} \tag{4.7}$$

is not empty. Indeed, there exists a $K_f \in \mathcal{K}_f$: $A - B_f K_f \in \mathcal{M}_a$.

The set $\mathcal{K}_f(A, B_f)$ may contain more than one element and therefore a decision rule to select a unique feedback law in this set must be provided.

The main interest of this work is to design a fault-tolerant control law that maintains the dependability and the safety of the system. The main contribution is to consider the overall system reliability as a principle objective which guides the design of the fault-tolerant controller (Khelassi *et al.*, 2011b). Thus, to design a reliable fault-tolerant controller with a priority on the overall system reliability, the generated control inputs should be applied to the system by taking into account the criticality level of each individual actuator. The reliability can be considered with high priority for keeping longer remaining operation of the faulty system with the given faulty conditions, while the necessary stabilization and tracking performance can be achieved simultaneously. This objective leads to design a reliable fault-tolerant controller $K_f^* \in \mathcal{K}_f$ which guarantees an acceptable degraded performance and maximizes the overall system reliability $R_g(t_M)$ during the remaining mission before a safe landing of an aircraft or a safe shutdown of an industrial system such as nuclear power plant or a chemical plant etc. The problem of reliable fault-tolerant control design is defined as follows :

Définition 4.3 *The system (A, B_f) is fault-tolerant and reliable using an active fault-tolerant control of $K_f^* \in \mathcal{K}_f$ defined by :*

$$K_f^* = \{K_f : \Phi_{\mathcal{M}}(A, B_f, K_f) \leq 0,\ R_g(t_M) \longrightarrow R_g^{max}\} \tag{4.8}$$

where R_g^{max} is the maximum value of overall reliability that can be obtained using $\mathcal{K}(A, B_f)$. $R_g(t_M)$ is the overall system reliability estimated for $t = t_M$ and t_M is the predefined time of the end of mission.

Indeed, the fault-tolerant controller K_f^* determined by (4.8) guarantees the stability condition with an acceptable control performance requirement and improves the overall system reliability where K_f^* will be designed with an overall view on the criticality of each actuators.

Before presenting the main contribution on the reliable fault-tolerant controller design, let us consider the following lemma Boyd *et al.* (1994) :

Lemme 4.1 *The required energy associated to the control input* $u(t) = -Kx(t)$ *evaluated as the norm* $\|u(t)\|$ *can be enforced to respect an upper bound* $\|u(t)\| < \mu$ *at all times* $t \geq 0$ *if the LMI*

$$\begin{bmatrix} P & S^T \\ S & \mu^2 \end{bmatrix} \geq 0 \tag{4.9}$$

holds for a given $\mu > 0$, *where* $P > 0$, $x(0)^T P^{-1} x(0) \leq 1$ *and* $K = SP^{-1}$ *such that* S *satisfies the stabilizing condition,*

$$AP + PA^T + BS + S^T B^T < 0 \tag{4.10}$$

Proof 4.1 *When the initial condition is known, an upper bound on the norm of the control input* $u(t) = -Kx(t)$ *can be found for all* $t \geq 0$ *where,*

$$\begin{aligned} \max_{t\geq 0} \|u(t)\| &= \max_{t\geq 0} \|SP^{-1}x(t)\| \\ &\leq \max_{x\in\xi} \|SP^{-1}\| \\ &= \Lambda_{max}(P^{-1/2} S^T S P^{-1/2}) \end{aligned} \tag{4.11}$$

and

$$\xi = \{x \in I\!R^n, \quad x^n P^{-1} x \leq 1\} \tag{4.12}$$

with $\Lambda_{max}(.) = \max(\Lambda(.))$ *is the maximum eigenvalue of the matrix.*

Therefore, the constraint $\|u(t)\| < \mu$ *is enforced at all times if the following LMI condition is satisfied.*

$$P^{-1/2} S^T S P^{-1/2} \leq \mu^2 \tag{4.13}$$

or equivalent to

$$S^T S \leq \mu^2 P \tag{4.14}$$

where $P > 0$. *Then, the constraint (4.9) is obtained by using the Schur complement of the equivalent constraint*

$$P - \mu^{-2} S^T S \geq 0 \tag{4.15}$$

Remark 4.1 *As what presented earlier, no stochastic or deterministic uncertainties are introduced in the system model, since this would only complicate the presentation of main contribution of the paper without changing the basic fault-tolerant concept and the proposed design approach.*

The resolution of the reliable fault-tolerant controller design (4.8) requires the integration of the reliability analysis tools with the control theory (Khelassi *et al.*, 2011c). In the following section, we propose a reliability analysis procedure to select *a priori* the critical actuators in which their deterioration leads to a significant degradation of the overall reliability of the system (4.1).

4.3 Reliability analysis of closed-loop systems

In this section, overall reliability analysis procedure is proposed based on the dynamic model of the system. The proposed reliability analysis provides information on the Reliability Block Diagram (RBD) of the system and also on the actuators criticality levels. The obtained information will then be used for the controller design. The reliable fault-tolerant controller will be synthesized based on a proposed actuator criticality indicator.

4.3.1 Reliability computation

The life time of the system can be quantified by the overall system reliability estimation. Let us consider the following definitions :

Définition 4.4 *Reliability $R(t)$ is defined as the probability that units, components, equipments and systems will accomplish their intended function for a specified period of time under some operating conditions and specific environments Gertsbakh (2000).*

Définition 4.5 *A component is considered critical if its degradation and solicitation cause a significant degradation in the overall system reliability.*

In the useful period of life, the component can be characterized at a given time t by a baseline reliability measure $R^0(t)$. In the following, $R_i^0(t)$, associated to the reliability of the i^{th} actuator, is obtained under nominal conditions in the useful period of life defined such as :

$$R_i^0(t) = \exp(-\lambda_i^0 t), \quad i = 1, \ldots, m \tag{4.16}$$

where in the reliability engineering field, λ_i^0 is a baseline failure rate of the i^{th} actuator obtained under a nominal operating condition defined by a specific *stress level* called load level.

However, a realistic reliability measurement should also include the trend of actuator degradation according to the variation of the operating conditions. Indeed, in many situations and especially in the considered study, failure rates are obtained from actuators under different levels of stress depending on the applied control input and the corresponding expended energy. Several mathematical models have been developed to introduce the impact of the variable stress level in the reliability estimation. Proportional hazard model firstly proposed in Cox (1972) is adopted.

Définition 4.6 *The reliability component under a variable functional condition can be estimated according to the nominal failure rate as follows :*

$$\begin{aligned} R_i(t) &= \exp(-\lambda_i t) \\ \lambda_i &= \lambda_i^0 \times g_i(\ell, \vartheta) \end{aligned} \tag{4.17}$$

where λ_i^0 represents the baseline failure rate (nominal failure rate) for the i^{th} component and $g_i(\ell, \vartheta)$ is called a load function (independent of time) which represents the effects of stress on the component failure rate. ℓ represents an image of the applied load and ϑ is a component parameter.

Assumption 4.1 *In this study, the exponential distribution for reliability estimation is considered. The load function introduced in (4.17) will be defined according to the energy expended by the actuator until the end of the mission $t = t_M$. If the applied load is known, the actuator reliability measure can be evaluated for $t = t_M$ and noted as $R(t_M)$.*

Different definitions of the load function $g_i(\ell, \vartheta)$ exist in the literature, where the exponential form is commonly used. In this study, the load function is defined according to the root-mean-square of the applied control input as follows :

$$g_i(\ell, \vartheta) = \exp(\beta_i \int_0^{t_M} u_i^2(t)dt), \quad i = 1, \ldots, m \tag{4.18}$$

where β_i is an actuator parameter defined as follows :

$$\beta_i = (t_M(\overline{u}_i - \underline{u}_i))^{-1}, \quad i = 1, \ldots, m \tag{4.19}$$

where $\overline{u}_i$ and $\underline{u}_i$ are the upper and lower saturation bound of u_i respectively.

In fact, based on (4.17) and (4.18), the actuators degradation at a given time t_M is modeled as a function of the applied load related directly to the consumed expended.

4.3.2 Actuators criticality analysis : Special cases

Based on the definitions described previously, the actuator reliability $R_i(t_M)$ can be estimated depending on the baseline reliability $R_i^0(t_M)$ as follows :

$$\begin{array}{ll} R_i(t_M) & = \alpha_i(u) R_i^0(t_M), \quad i = 1, \ldots, m \\ \alpha_i(u) & = \exp(-\lambda_i^0 \beta_i \|u_i\|^2) \end{array} \tag{4.20}$$

where $\|.\|$ is the Euclidien norm. $\alpha_i(u_i) \leq 1$ represents the rate of reliability degradation due to the applied load during the mission. In fact, the following relation is satisfied : $if \quad \|u_i\|^2 \to 0 : R(t_M) \to R^0(t_M)$ where $\|u_i\|^2$ is the variation of the applied load compared to the nominal level of load. Thus, the component reliability decreases for a large variation of the applied load from the nominal load.

For a system composed by redundant actuators, the fault-tolerant controller can maximize the overall system reliability by considering the following lemma.

Lemma 4.1 *The overall system reliability $Rg(t_M, u)$ of a controlled system composed by m redundant actuators tends to Rg^{max} for a reliable control inputs $u^*(t) = -K^* x(t)$ that stress/solicit more the less reliable actuators (give the priority to demanding less from reliable actuators in the control efforts distribution) and satisfy the following condition as close as possible :*

$$K^* \mapsto \{u^*(t) \quad | \quad \min \frac{\alpha_i(u_i^*)}{\alpha_j(u_j^*)} \quad if \quad \frac{\lambda_i^0}{\lambda_j^0} < 1\},$$

where the nominal controller $K^* \in \mathcal{K}$. $i \in [1, \ldots, m]$, $j \in [1, \ldots, m]$ and $i \neq j$. Rg^{max} is the optimal value of overall system reliability that can be obtained at $t = t_M$.

Proof 4.2 *Systems composed by m redundant actuators can be presented by a parallel scheme of Reliability Block Diagram (RBD). The associated overall system reliability under nominal conditions $Rg^0(t_M)$ can be obtained as follows :*

$$Rg^0(t_M) = 1 - \prod_{k=1}^{m}(1 - R_k^0(t_M)) \tag{4.21}$$

The sensitivity of the overall system reliability s_i versus the i^{th} component can be evaluated as :

$$\begin{aligned} s_i &= \frac{\partial Rg^0(t_M)}{\partial R_i^0(t_M)} = \prod_{k=1;\ k\neq i}^{m}(1 - R_k^0(t_M)) \\ &= \prod_{k=1}^{m}(1 - R_k^0(t_M))(1 - R_i^0(t_M))^{-1} \end{aligned} \tag{4.22}$$

It can be shown that, if $R_i^0 > R_j^0$ (or $\lambda_i^0 < \lambda_j^0$) then $s_i < s_j$.

This result means that a small degradation $\alpha_i(u_i)$ of the i^{th} more critical actuator (for that the system reliability is more sensitive) causes a large degradation of the overall system reliability $R_g(t_M)$ and vice-versa for the j^{th} actuator.

However, a sensitivity of the overall system reliability compared to serial actuators is different. The reliable fault-tolerant controller can be synthesized with respect to the following lemma.

Lemma 4.2 *The overall system reliability $Rg(t_M, u)$ of a controlled system composed by m serial actuators tends to Rg^{max} for an reliable control inputs $u^*(t) = -K^*x(t)$ that give a priority to the more reliable actuators in the control efforts distribution and satisfy the following condition as close as possible :*

$$K^* \mapsto \{u^*(t) \ \mid \ \min \frac{\alpha_i(u_i)}{\alpha_j(u_j)} \ \ if \ \ \frac{\lambda_i^0}{\lambda_j^0} > 1\},$$

where $K^* \in \mathcal{K}$, $i \in [1, \ldots, m]$ and $j \in [1, \ldots, m]$. Rg^{max} is the optimal value of overall system reliability that can be obtained at $t = t_M$.

Proof 4.3 *For a serial actuators, the overall system reliability under nominal conditions $Rg^0(t_M)$ can be obtained as follows :*

$$Rg^0(t_M) = \prod_{k=1}^{m} R_k^0(t_M) \tag{4.23}$$

The sensitivity of the overall system versus the components s_i can be evaluated as :

$$s_i = \frac{\partial Rg^0(t_M)}{\partial R_i^0(t_M)} = \prod_{k=1;\ k\neq i}^{m}(R_k^0(t_M)) = \frac{R_g^0(t_M)}{R_i^0(t_M)} \tag{4.24}$$

It can be shown that, if $R_i^0 < R_j^0$ (or $\lambda_i^0 > \lambda_j^0$) then $s_i < s_j$.

This result means that a small degradation $\alpha_i(u_i)$ of the less sensitive actuator i causes a large degradation of the overall system reliability. So, the optimal value of the overall system reliability under a variable functional condition can be obtained for control inputs that minimize and limit the use of the less reliable actuators in the control efforts distribution.

4.3.3 Actuators criticality analysis : General case

In the more general case, a global reliability $R_g(t_M)$ is computed based on the reliabilities of elementary components or subsystems. In this context, $R_g(t_M)$ depends on the actuators's connection which can generally be decomposed on elementary combinations of serial and parallel components.

In the context of fault-tolerant control, it is crucial to know *a priori* how the actuators are connected in order to analyze the actuator's criticality. In fact, the variation of the overall system reliability when the applied load is considered depends on the structure of the system and the applied load corresponding to each actuator. The structure of the system can be modeled by the reliability block diagram. The design of an optimal controller which guarantees the overall system reliability implies the knowledge of the system structure where only existing information about the system is the state representation. The reliability analysis based on sensitivity can guide the design for a reliable fault-tolerant control strategy.

In fact, by considering the matrix $B = [b_1 b_2 \dots b_m], \quad b_i \in \mathbb{R}^{n\times 1}$, reliability block diagram of the actuators can be obtained by checking the controllability condition for the different combinations of b_i. For a control problem, the intended function for which the reliability block diagram will be established is to guarantee the system controllability. This condition makes the design of the control law possible. In order to obtain the relation $R_g(t) = f(R_1(t), R_2(t), \dots R_m(t))$ for the complex systems, the following subsets $\mathcal{L}_k, \quad k = 1, \dots, n_L$ are considered as follows :

$$\mathcal{L}_k = \{R_i, rank[Ctr(A, [\rho_1 b_1, \dots, \rho_m b_m])] = n\}, i \in [1, m] \tag{4.25}$$

where, $Ctr(A, B)$ is the controllability Grammian of the system defined by the matrices (A, B), and

$$\begin{cases} \rho_i = 0, & \text{the } i^{th} \text{ actuator is not considered in } \mathcal{L}_k \\ \rho_i = 1, & \text{the } i^{th} \text{ actuator is considered in } \mathcal{L}_k \end{cases} \tag{4.26}$$

In fact, $\mathcal{L}_k, k = 1, \dots, n_L$ are all the subset schemes of the actuators for which the controllability condition is satisfied and so a fault-tolerant controller can be calculated. $\mathcal{L}_k$ represents the successful solution of controllability similar to the success path defined in the standard reliability analysis.

Then, based on the *Poincare Theorem* Lyu (2005), the overall system reliability $R_g(t)$ can be expressed as a function of $R_i(t)$ as follows :

$$R_g(t) = \sum_{j=1}^{n_L} \prod_{i\in\mathcal{L}_j} R_i(t) - \sum_{j=2}^{n_L} \sum_{k=1}^{j-1} \mathcal{P}(\mathcal{L}_k \cap \mathcal{L}_j) + \dots + (-1)^m \mathcal{P}(\mathcal{L}_1 \cap \dots \cap \mathcal{L}_m) \tag{4.27}$$

where

$$\mathcal{P}(\mathcal{L}_k \cap \mathcal{L}_j) = \prod_{i\in\{\mathcal{L}_k, \mathcal{L}_j\}} R_i(t) \tag{4.28}$$

The *Poincare Theorem* is generally used to calculate the overall system reliability of complex systems. Hence, this theorem is adopted in this work to obtain the

relation of the overall system reliability for the controlled system defined by the matrices (A, B). The proposed evaluation is applied off-line where the reliability block diagram and the connection between the actuators is fixed in the system design stage and does not change.

Consequently, the actuators criticality can be evaluated by the following indicator obtained based on the sensitivity study such as :

$$s_i = \frac{\partial R_g^0(t_M)}{\partial R_i^0(t_M)}, \quad i = 1, \ldots, m \tag{4.29}$$

In order to maximize the overall system reliability, the applied loads depending on the reliable controller $K^* \in \mathcal{K}$ should guarantee the stability of the faulty closed-loop system with respect to the actuators criticality. The criticality indicator s_i can be obtained in the nominal case for a predefined t_M based on the baseline actuator failure rate $\lambda_i^0,\ i = 1, \ldots, m$. With the proposed indicator s_i the critical actuators can be known *a priori* before controller design.

Example

Let us consider the arbitrary system modeled by the following state space representation

$$A = \begin{bmatrix} -3 & 0.1 & 0.1 & 0 & -10 & 0 & 0 \\ 0 & -1 & 0 & -20 & 0 & 0 & 0 \\ 0.1 & 0.2 & -0.2 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0.02 & 0 & -1 & 0 & -1 & 0.3 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} -50 & 0 & 1 \\ 0 & -30 & 4 \\ -0.9 & 0 & 0 \\ 0 & -0.1 & 0 \\ 0.1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 1 \end{bmatrix}$$

By applied the relation (4.25) for the all combinations, the following subsets $\mathcal{L}_k$ that verify system controllability condition are obtained as follows :

$$\begin{aligned} \mathcal{L}_1 &= \{R_1, R_2, R_3\} \\ \mathcal{L}_2 &= \{R_1, R_2\} \\ \mathcal{L}_3 &= \{R_1, R_3\} \end{aligned}$$

where $n_L = 3$.

The relation of the overall system reliability $R_g(t)$ can be obtained by considering the Poincare theorem (4.27) as :

$$R_g(t) = R_1(t)R_3(t) + R_1(t)R_2(t) - R_1(t)R_2(t)R_3(t)$$

The criticality of the actuators can be measured by the sensitivity indicators s_i defined in (4.29), where :

$$\begin{aligned} s_1 = &\quad R_3(t_M) + R_2(t_M) - R_1(t_M)R_3(t_M) \\ s_2 = &\quad R_1(t_M) - R_1(t_M)R_2(t_M) \\ s_3 = &\quad R_1(t_M)(1 - R_2(t_M)) \end{aligned}$$

with $R(t_M) = \exp(-\lambda_i^0 t_M)$ and λ_i^0 are known for $i = 1, \ldots, m$. The corresponding system reliability bloc diagram is obtained as follows :

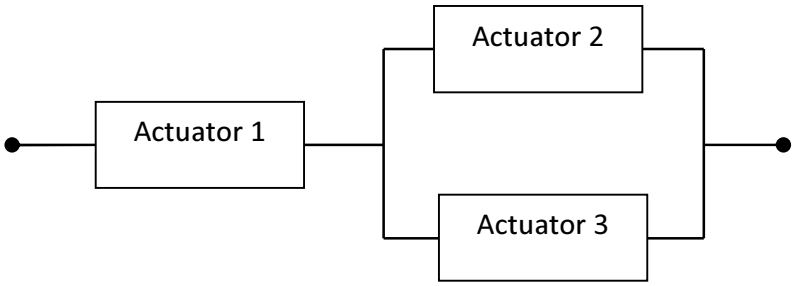

FIGURE 4.1 – Reliability block diagram of the example

4.4 Reliable Admissible Model Matching Fault Tolerant Control

Admissible model matching method proposed in Tornil-Sin *et al.* (2009) is considered to design a fault-tolerant controller such that the poles of the closed-loop system are inside a pre-established region. In this work, information about actuator criticality will be incorporated in the controller design in order to impose a priority level to the applied load corresponding to each actuator based on their criticality (Khelassi *et al.*, 2011c).

Generally, the set of admissible behaviors $\mathcal{M}_a$ can be proposed as :

$$\mathcal{M}_a = \{(A, B_f, \mathcal{K}_f) : \Lambda(A - B_f\mathcal{K}_f) \in \mathcal{D}_\alpha\} \tag{4.30}$$

where $\Lambda(.)$ is the set of the eigenvalues of the matrix $(.)$. $\mathcal{D}_\alpha$ is a desired region included in the unit circle with an affix $(-q, 0)$ and a radius r such that $(q + r) < 1$ is fixed. These two scalars q and r are used to determine a specific region included in the unit circle. According to Apkarian *et al.* (1995), (4.30) can be rewritten as follows :

$$\begin{bmatrix} -rP & qP + PM^T \\ qM + MP & -rM \end{bmatrix} < 0 \tag{4.31}$$

where $M = A - B_f K_f$ and $P > 0$.

In fact, $\mathcal{D}_a$ is the region encompassing the desired system poles Λ^d and the admissible ones. Before discussing the design of the fault-tolerant control in degraded functional mode, it is important to emphasize that an admissible controller K^* can be designed in the nominal case with respect to the actuator criticality level.

4.4.1 Controller design for normal cases

Actually, the existing methods of controller design are proposed in the literature without an overall view on the actuators characteristics or overall system reliability. In the following, we propose to design a reliable nominal controller K^* in order to maximize the overall system reliability and to improve the system dependability. The proposed controller K^* places the system eigenvalues $\Lambda(M)$ in the admissible region as close as possible to the desired eigenvalues Λ^d and manages effectively the actuators. In this case, acceptable degradation performance is tolerated against the system dependability. For that, an additional LMI constraint is considered in the controller design and the reliable controller K^* can be obtained in the nominal functional operation as follows :

Theorem 4.1 *Given a scalar μ and the criticality indicator s_i defined by (4.29), a reliable nominal controller $K^* = SP^{-1}$ can achieve $\Lambda(A-BK^*) \in \mathcal{D}_\alpha$ and $R_g(t_M) \rightarrow R_g^{max}$ by solving the following LMIs problem :*

$$\begin{bmatrix} -rP & qP + PA^T - S^T B^T \\ qP + AP - BS & -rP \end{bmatrix} < 0 \tag{4.32}$$

$$\begin{bmatrix} P & S^T \\ S & (\Omega^{-1}\mu)^2 \end{bmatrix} \geq 0 \tag{4.33}$$

where $P > 0 \in I\!R^{m\times m}$, $S \in I\!R^{n\times m}$ such that

$$\Omega = diag\ \{\Omega_1, \Omega_2, \ldots, \Omega_m\}$$

where Ω is a weighing matrix used to assign a priority level to the applied control efforts of the actuators based on their criticality with

$$\Omega_i = \frac{s_i}{s_{min}}, \quad s_{min} = \min(s_i) \tag{4.34}$$

Proof 4.4 *Based on Lemma 4.1, $\|u\| < \mu$ can be satisfied by considering a weighted norm $\|\Omega u\|$ where*

$$\|u\| \leq \|\Omega u\| < \mu \tag{4.35}$$

for $\Omega = diag\{\Omega_1, \Omega_2, \ldots, \Omega_m\} \geq 0$, and $\Omega_i \geq 1, \quad i \in [1, \ldots, m]$ where (4.35) is a constraint on the actuator applied load.

Based on the weighted norm $\|\Omega u\|$, the applied load constraint $\|u\| < \mu$ is satisfied by considering specified priority level to each actuator. In fact the applied load of each control input $u_i(t)$ can be enforced to respect a fixed upper bound for each actuator.

The values of Ω_i are chosen in order to manage the control inputs based on the criticality indicator (4.29) and contribute to a reliable controller as follows :

$$\Omega_i = \frac{s_i}{s_{min}}, \quad s_{min} = \min(s_i), \quad \forall i = 1, \ldots, m \tag{4.36}$$

where the required applied loads of the actuators are bounded by considering their criticality. The previous LMI constraint can be expressed as follows :

$$\begin{bmatrix} P & S^T \\ S & (\Omega^{-1}\mu)^2 \end{bmatrix} > 0 \tag{4.37}$$

The stability condition and the admissibility solution are both guaranteed by the LMI region constraint of poles placement (4.32).

The proposed reliable controller is designed by considering the actuator criticality level and required the control performance degradation. This acceptable degradation rate depends on the specifications of the designer and the considered application. It can be accepted against the improvement of the dependability and the overall system reliability.

4.4.2 Controller design for faulty cases

After faults occurrence, the active fault-tolerant controller K_f is required to guarantee the admissibility and the system stability in the degraded functional mode. As proposed in Tornil-Sin *et al.* (2009), admissible fault-tolerant controller can be calculated by solving the LMI problem (4.31) with $M = A - B_f K_f$. Generally, the unique objective design depends on the control specifications as stability, perturbations, etc. In order to improve the dependability of the faulty system in this work, we propose to design an admissible fault-tolerant controller K_f^* on-line with respect to the criticality level of the actuators. In fact, the fault-tolerant controller K_f^* is calculated on-line by considering the actuator criticality level which depend to the characteristics of the actuators and the corresponding applied load. The proposed idea requires the on-line estimation of the impact of the applied load on the criticality level of each actuator. A new criticality indicator is computed on-line for achieving an active fault-tolerant system with enhanced overall system reliability even in the presence of faults in the system.

In order to manage effectively the control inputs and the applied loads in the faulty case, we propose a reliable admissible model matching controller designed with respect to the criticality and reliability of the actuators by the following theorem.

Theorem 4.2 *Given a scalar μ, a fault-tolerant controller $K_f^* = SP^{-1}$ can be designed to achieve $\Lambda(A_f - B_f K_f^*) \in \mathcal{D}_\alpha$ and $R_g(t_M) \rightarrow R_g^{max}$ by solving the following LMIs problem :*

$$\begin{bmatrix} -rP & qP + PA^T - S^T B_f^T \\ qP + AP - B_f S & -rP \end{bmatrix} < 0 \tag{4.38}$$

$$\begin{bmatrix} P & S^T \\ S & (\Omega_f{}^{-1}\mu)^2 \end{bmatrix} \geq 0 \tag{4.39}$$

where $P > 0 \in I\!R^{m\times m}$, $S \in I\!R^{n\times m}$ *and* $B_f = B\Gamma$. $\Omega_f > 0$ *is a weighing matrix defined as :*

$$\Omega_f = diag\{\Omega_{f_1}, \Omega_{f_2}, \ldots, \Omega_{f_m}\}$$

where

$$\Omega_{f_i} = \frac{s_i^f}{s_{min}^f}, \quad s_{min}^f = \min(s_i^f), \ \forall i \in [1, \ldots, m] \tag{4.40}$$

and

$$s_i^f = \frac{R(t_M)}{R_i(t_M)} \tag{4.41}$$

is evaluated by taking into consideration the actuator's applied load function until $t_M = t_f$ *as,*

$$g_i(\ell, \vartheta) = \exp(\beta_i \int_0^{t_f} u_i^2(t)dt), \quad i = 1, \ldots, m \tag{4.42}$$

Proof 4.5 *After the fault occurrence at* $t = t_f$*, the criticality indicator* s_i *can be re-estimated on-line by considering the impact of the applied load on the actuators failure rates* λ_i *as defined in (4.17). The applied load in this case can be evaluated as :*

$$g_i(\ell, \vartheta) = \exp(\beta_i \int_0^{t_f} u_i^2(t)dt), \quad i = 1, \ldots, m$$

The stability and the admissibility of the closed-loop system in the faulty case can be guaranteed by considering $K_f^* = SP^{-1}$ *in the inequality (4.31) where* $M = A - B_f K_f^*$.

The proposed reliable admissible model matching approach can be also extended to the tracking problem by adding an integrator in order to eliminate steady-state errors as proposed in Guenab *et al.* (2010). The use of integral control eliminates the need to catalog nominal values or to reset the control. Rather, the integral term can be thought as constantly calculating the value of the control required at the set-point to force the error to go to zero. To accomplish the design of the feedback gains for the integral and the original state vector, an augmented model is proposed as follows :

$$\begin{bmatrix} \dot{\varepsilon}(t) \\ \dot{x}(t) \end{bmatrix} = \begin{bmatrix} 0 & -C_r C \\ 0 & A \end{bmatrix} \begin{bmatrix} \varepsilon(t) \\ x(t) \end{bmatrix} + \begin{bmatrix} 0 \\ B \end{bmatrix} \Gamma u(t) + \begin{bmatrix} I \\ 0 \end{bmatrix} y_r(t) \tag{4.43}$$

where $\varepsilon(t) = \int_0^t e(\tau)d\tau$ is the error integral state and :

$$z(t) = C_r y(t) \tag{4.44}$$

For the tracking problem, $C_r \in R^{l\times p}$ is a known constant matrix used to select the output required to track the reference signal. $z(t) \in I\!R^{l\times n}$ is the controlled outputs.

The corresponding control law is :

$$\begin{aligned} u^*(t) &= -\begin{bmatrix} K_e & K_x \end{bmatrix} \begin{bmatrix} \epsilon(t) \\ x(t) \end{bmatrix} + K_x N_x y_r(t) \\ &= -\bar{K}\bar{x} + \bar{G}y_r(t) \end{aligned} \tag{4.45}$$

Thus, the closed-loop system designed with the control law (4.68) is :

$$\dot{\bar{x}} = (\bar{A} - \bar{B}\bar{K})\bar{x}(t) + (\bar{B}\bar{G} - G)y_r(t) \tag{4.46}$$

such that the closed-loop behavior follows the reference model

$$\dot{\bar{x}}(t) = M^*\bar{x}(t) + N^*y_r(t) \tag{4.47}$$

where M^* is the desired system dynamic chosen to be stable. To satisfy the tracking specification, N^* is calculated as :

$$N^* = \bar{B}\bar{G} - G \tag{4.48}$$

where

$$N_x = C^T(C^TC)^{-1} \tag{4.49}$$

and the following rank condition is satisfied :

$$rank(C) = p. \tag{4.50}$$

Thus, the design of reliable admissible fault-tolerant controller with tracking specification can be solved using the separation principle : first, design of a reliable feedback control M^* is obtained using Theorem 4.6 in the nominal case (Theorem 4.2 for after fault occurrence). Then, the reference input $y_r(t)$ is introduced through the control input law (4.68) with respect to (4.48) and (4.49).

Propriété 4.1 *In Tornil-Sin et al. (2009), the authors propose a set of admissible behaviors $\mathcal{M}_a$ using LMI-based regional pole placement technique. This method locates the poles in particular convex regions called $\mathcal{D}$-regions. The fault accommodation is formulated in terms of several LMI problems. Using this approach, the admissibility condition could also be defined using the set admissible behaviors $\mathcal{M}_a$ proposed in Tornil-Sin et al. (2009) and the LMI regional pole placement approach.*

4.5 Active Fault Tolerant Compensation Control against Actuators Reliability

In this section, we propose to design an effective fault tolerant controller based on compensation principle. For this strategy, only effective nominal controller is designed in the normal functional. After faults occurrence, an additional control input is generated based on the nominal control in order to guarantee the required control performance.

Let us consider the linear time-invariant model given by (4.44) where (A, B) is stabilizable. By considering the actuator faults, the system can be written in degraded functional operation as follows :

$$\begin{array}{l} \dot{x}(t) = Ax(t) + B_f u(t) \\ y(t) = Cx(t) \\ z(t) = C_r y(t) \end{array} \tag{4.51}$$

where the matrix B_f is defined according to loss of effectiveness factors γ_i (4.6).

Assumption 4.2 *Du to the limitation of the fault tolerant compensation control, the considered degraded situation not interrupts the component operating. The faulty actuator can achieve its functional objectives under more severe operating conditions characterized by a heavy applied load.*

For the faulty system described by (4.51), the problem of fault tolerant control design is to determine a controller such that :

i) During normal operating mode, the closed-loop system is stable, and the output $z(t)$ tracks the reference signal $y_r(t)$ without steady-state error :

$$\lim_{t \longrightarrow \infty} e(t) = 0, \qquad e(t) = y_r(t) - C_r y(t) \tag{4.52}$$

ii) After faults diagnosis, the closed-loop system is still stable and the required output $z(t)$ tracks the reference signal $y_r(t)$ with an acceptable lower level of tracking performance.

It is well known that the tracking error integral action of a controller can effectively eliminate the steady-state tracking error. In order to obtain an active fault tolerant controller with tracking error integral, the following augmented state-space system is introduced by combined (4.51) and (4.52) as follows :

$$\begin{bmatrix} \dot{\varepsilon}(t) \\ \dot{x}(t) \end{bmatrix} = \begin{bmatrix} 0 & -C_r C \\ 0 & A \end{bmatrix} \begin{bmatrix} \varepsilon(t) \\ x(t) \end{bmatrix} + \begin{bmatrix} 0 \\ B \end{bmatrix} \Gamma u(t) + \begin{bmatrix} I \\ 0 \end{bmatrix} y_r(t) \tag{4.53}$$

where $\varepsilon(t) = \int_0^t e(\tau) d\tau$ is the error integral state.

By considering $\bar{x}(t) = [\varepsilon^T(t) \quad x^T(t)]^T$, the augmented system (4.53) can be described as follows :

$$\bar{x}(t) = \bar{A}\bar{x}(t) + \bar{B}\Gamma u(t) + G y_r(t) \tag{4.54}$$

where, $\bar{A} = \begin{bmatrix} 0 & -C_r C \\ 0 & A \end{bmatrix}$, $\bar{B} = \begin{bmatrix} 0 \\ B \end{bmatrix}$, $G = \begin{bmatrix} I \\ 0 \end{bmatrix}$

Indeed, the performance index that the designed controller should minimize is written as :

$$\mathcal{J}_t = \int_0^t [\varepsilon(t)^T Q_1 \varepsilon(t) + x(t)^T Q_2 x(t) + u(t)^T \Gamma R \Gamma u(t)] dt \tag{4.55}$$

where $Q_1 \in \mathbb{R}^{l \times l}$, $Q_2 \in \mathbb{R}^{n \times n}$ are positive semidefinite matrices and $R \in \mathbb{R}^{m \times m}$ is a positive definite matrix.

Based on the compensation control principal (Noura *et al.*, 2000) and the robust fault tolerant control method (Ye et Yang, 2006), the active fault tolerant controller which holds the tracking problem and minimizes the performance index (4.55) can be obtained by the following theorem :

Theorem 4.3 *Consider the closed-loop augmented faulty system (4.53) and the performance index (4.55). The following controller K_f stabilizes the faulty closed-loop augmented system for a given positive constant η :*

$$\begin{aligned} K_f = [K_e, K_x] &= \bar{B}_f^+ \bar{B} K \\ &= (\bar{B}_f)^+ \bar{B} S P^{-1} \end{aligned} \tag{4.56}$$

where $K = SP^{-1}$ is the nominal controller gain obtained by solving the following LMI optimization problem which minimizes the upper bound of the performance index :

$$\min \mathit{Trace}(T) \tag{4.57}$$

such that

$$\begin{bmatrix} \bar{A}P + \bar{B}S + (\bar{A}P + \bar{B}S)^T & G & S^T R^{1/2} & PQ^{1/2} \\ * & -\eta I & 0 & 0 \\ * & * & -I & 0 \\ * & * & * & -I \end{bmatrix} < 0 \tag{4.58}$$

and

$$\begin{bmatrix} T & I \\ I & Z \end{bmatrix} > 0 \tag{4.59}$$

with $P \in I\!R^{(n+l)\times(n+l)}$, $S \in I\!R^{m\times(n+l)}$, $Q = diag[Q_1, Q_2] \geq 0$ and $R > 0$.

Proof 4.6 *By the Schur complement formula, (4.58) can be written as :*

$$\bar{A}P + \bar{B}KP + (\bar{A}P + \bar{B}KP)^T + \frac{1}{\eta} GG^T + ZQZ + ZK^T RKZ < 0 \tag{4.60}$$

which is equivalent to :

$$X(\bar{A} + \bar{B}K) + (\bar{A} + \bar{B}K)^T X + \frac{1}{\eta} XGG^T X + Q + K^T RK < 0 \tag{4.61}$$

where $X = P^{-1}$.

Since $\eta > 0$, $Q = Q^T \geq 0$ and $R > 0$, $R = R^T$, then

$$X(\bar{A} + \bar{B}K) + (\bar{A} + \bar{B}K)^T X < 0 \tag{4.62}$$

Furthermore, an upper bound of the performance index (4.55) can be given by :

$$\mathcal{J}_t \leq \eta \int_0^t y_r^T(t) y_r(t) dt + \bar{x}^T(0) T \bar{x}(0) dt. \tag{4.63}$$

where η is the H_∞ norm $\|T_{zy_r}\|$ of the transfer function from the input $y_r(t)$ to the performance output $z(t)$:

$$z(t) = [Q^{1/2}, 0]^T \bar{x}(t) + [0, R^{1/2}]^T u(t) \tag{4.64}$$

Then, the upper bound of the performance index $\mathcal{J}_t$ can be minimized by solving the optimization problem (4.57), (Ye et Yang, 2006).

According to stability theorem, the control law $u(t) = Kx(t)$ with $K = SP^{-1}$ stabilizes the augmented system (4.54) for the fault free case described by $\Gamma = I_m$. After fault occurrence, the fault tolerant compensation control aims to find a control input

$$u(t) = Kx(t) + u_{ad}(t) \tag{4.65}$$

that stabilizes the faulty system and guarantees the nominal behavior. This objective can be guaranteed by the following condition :

$$\bar{B}u_N(t) = \bar{B}\omega(u_N(t) + u_{ad}(t)) \tag{4.66}$$

where $u_N(t) = -Kx(t)$.

By identification, the added control input $u_{ad}(t)$ is obtained according to the nominal control input $u_N(t)$ as follows :

$$u_{ad}(t) = ((B\Gamma)^+ B - I_m)u_N \tag{4.67}$$

By replacing (4.67) in (4.65), the fault tolerant controller gain (4.56) is obtained.

Thus, to design an effective fault tolerant compensation control law, we propose to introduce the actuator criticality indicator in the control design problem. The control inputs will be applied to the system by taking into account the criticality of the actuators. The aim is to design a fault tolerant controller gain that maximizes the overall system reliability and so improves the dependability of the system.

The stability and the tracking problem will be solved both in the nominal case by using an LMI approach. After fault occurrence, the control inputs in this case are calculated according to the fault severity and the nominal control inputs taken into account actuator criticality.

The proposed effective fault tolerant controller K^* based on the compensation principle holds the tracking problem, minimizes the performance index and manages effectively the actuators in order to guarantee a high level of overall system reliability. The following proposition is considered :

Proposition 4.1 *Consider the closed-loop augmented system (4.54) and the performance index (4.55). The following controller K_f^* stabilizes the closed-loop system for a given positive constant η and a sensibility matrix $\Omega \in \mathbb{R}^{m\times m} > 0$, where :*

$$K_f^* = [K_e^*, K_x^*] \quad = (\bar{B}_f)^+ \bar{B} K^* \tag{4.68}$$

The nominal controller gain $K^* = SP^{-1}$ is obtained by solving the following LMIs optimization problem :

$$\begin{bmatrix} \bar{A}P + \bar{B}S + (\bar{A}P + \bar{B}S)^T & G & S^T R^{1/2} & PQ^{1/2} \\ * & -\eta I & 0 & 0 \\ * & * & -I & 0 \\ * & * & * & -I \end{bmatrix} < 0 \tag{4.69}$$

$$\begin{bmatrix} P & S^T \\ S & (\Omega^{-1}\mu)^2 \end{bmatrix} \geq 0 \tag{4.70}$$

where $P \in I\!R^{(n+l)\times(n+l)}$, $S \in I\!R^{m\times(n+l)}$ *and* $Q = diag[Q_1, Q_2] \geq 0$ *and* $R > 0$.

$$\Omega = diag([\Omega_1, \Omega_2, \ldots, \Omega_m]) \tag{4.71}$$

with

$$\Omega_i = \frac{s_i}{s_{max}}, \quad s_{min} = \min(s_i), \ \forall i \in [1 \quad m] \tag{4.72}$$

Proof 4.7 *In fact, based on lemma.4.1,* $\|u\| < \mu$ *can be satisfied by considering the weighing norm* $\|\Omega u\|$ *where*

$$\|u\| \leq \|\Omega u\| < \mu \tag{4.73}$$

for $\Omega = diag\{\Omega_1, \Omega_2 \ldots, \Omega_m\} \geq 0$ *and* $\Omega_i \geq 1, \quad i \in [1 \ldots m]$.

By considering the weighting norm $\|\Omega u\|$, *the applied load of each control input* $u_i(t)$ *can be enforced to respect a fixed upper bound for each actuator. The values of* Ω_i *are chosen in order to manage the control inputs based on the actuator criticality :*

$$\Omega_i = \frac{s_i}{s_{min}}, \quad s_{min} = \min(s_i), \quad \forall i = 1 \ldots m \tag{4.74}$$

where the required applied loads of the actuators are bounded by considering their criticality level. Thus, the LMI constraint (4.73) can be expressed as follows :

$$\begin{bmatrix} P & S^T \\ S & (\Omega^{-1}\mu)^2 \end{bmatrix} > 0 \tag{4.75}$$

Indeed, in the nominal case, the problem is solved for $\Gamma = I_m$ *and* $B_f = B$ *where* $K_f^* = K^*$.

After faults occurrence, the controller gain K_f^* *is calculated based on the compensation principle for the considering faulty situation* $\gamma_i \neq 1$. *Stability and required control performance are guaranteed by considering the proof lemma (4.3).*

Property 4.1 *The proposed effective method is presented based on the control compensation strategy and fault diagnosis scheme. This method can be applied for the accommodated systems without need to fault diagnosis by using the adaptive fault tolerant control algorithms. The adaptive FTC methods aim to find an additive control inputs based on the nominal controller* K^* *in order to compensate the occurred faults by using a followed model reference. More details on the adaptive algorithms that can be combined with the proposed approach can be found in (Bodson et Groszkiewicz, 1997; Ye et Yang, 2006; Jin et Yang, 2009).*

In this section, effective active fault tolerant control method is proposed based on the control compensation principal. In the proposed method, a unique effective fault tolerant controller is designed with respect the baseline actuator criticality. The fault tolerant compensation control don't required the reconfiguration of the nominal control system. This strategy is easy and beneficial from the calculation point of view. However, this method presents a limitations. A specific condition should be verified in order to guarantee the existence of control compensation solution, see Noura *et al.* (2000).

4.6 Application 1 : Effective admissible FTC

In order to illustrate the novel fault tolerant controller design, a linearized flight control problem considered in (Benvenuti et Benedetto, 1994) is adopted where $x(t) = [\tilde{p}, \tilde{q}, \tilde{r}, \Delta_\alpha, \beta, \phi, \theta]^T$ is the state vector. $u(t) = [\delta_a, \delta_r, \delta_e]^T$ is the control input vector, with δ_a is the aileron deflection angle, δ_r is the rudder deflection angle and δ_e is the elevator deflection angle. The controlled outputs $y(t) = [\beta, \phi, \theta]^T$ are respectively, sideslip angle, bank angle and pitch angle.

$$A = \begin{bmatrix} -3.9 & 0.10 & 0.12 & 0 & -9.89 & 0 & 0 \\ 0 & -0.98 & 0 & -22.95 & 0 & 0 & 0 \\ 0.002 & 0.22 & -0.23 & 0 & 5.67 & 0 & 0 \\ 0 & 1 & 0 & -1.32 & 0 & 0 & \\ 0.026 & 0 & -0.99 & 0 & -0.19 & 0.03 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} -45.83 & -7.64 & 0 \\ 0 & 0 & -28.3409 \\ -0.921 & -6.51 & 0 \\ 0 & 0 & -0.168 \\ 0.0071 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$C_r = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and $C = I_7$.

To demonstrate the proposed approach in a short time window, the baseline actuators failure rates λ_i^0 are considered with a very huge values as given in the Table 4.1.

The requirement in nominal operating conditions is assumed for the following closed-loop desired poles :

$$\Lambda = \{-4, -4, -4.2, -2.7, -2.7, -2.7 + 0.2i, -2.7 - 0.2i\}$$

TABLE 4.1 – Failure rates of elementary components

Failure rates	
λ_1^0	$0.001\ min^{-1}$
λ_2^0	$0.0001\ min^{-1}$
λ_3^0	$0.09\ min^{-1}$

Nominal functional condition

First, the nominal controller K_n is designed using standard pole placement. The classical nominal feedback gain is obtained as follows :

$$K_n = \begin{bmatrix} -0.0653 & -0.0205 & 0.1606 & 0.0877 & 0.1229 & -0.2474 & -0.2199 \\ 0.0077 & 0.0580 & -0.9868 & -0.3178 & 0.5751 & 0.0110 & 0.8129 \\ 0.0010 & -0.2567 & -0.0002 & 1.0027 & 0.0012 & 0.0025 & -0.8711 \end{bmatrix}$$

In order the illustrate the effectiveness of the proposed approach, a nominal effective controller gain K^* is designed by based on theorem ().

By considering the actuator criticality analysis in (4.29) and the baseline failure rates $\lambda_i^0, \quad i = 1, 2, 3$, the reliability block diagram of the nominal system can be obtained by checking the controllability condition as in (4.25), see figure (4.2).

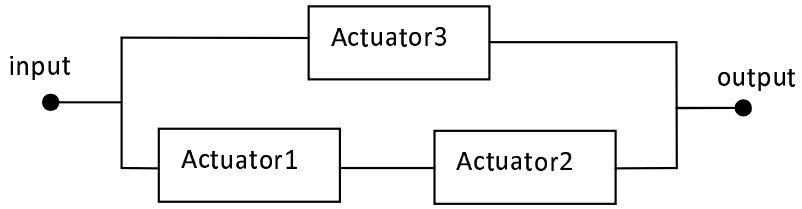

FIGURE 4.2 – Reliability block diagram of the actuators

For simplicity, complete failure of actuator 1 is not considered and the overall system reliability $R_g^0(t)$ can be expressed as :

$$R_g^0(t) = R_3^0(t) + R_1^0(t)R_2^0(t)(1 - R_3^0(t))$$

The criticality indicator of the actuators is obtained for $t_M = 20\ sec$ as follows :

$$s = [0.833,\ 0.818,\ 0.0218]^T \tag{4.76}$$

It can be seen that the actuator 1 is the most critical actuator where $\max(s_i) = s_1, \quad i \in [1, 2, 3]$. In the design of the reliable nominal controller K^*, the overall system reliability is considered as an objective to maximize. The most critical actuators will be less solicited in the design of closed-loop control signal of the fault-tolerant controller given in Theorem 1 with respect to the concern of overall reliability of the system. Since such a strategy will not push the critical actuator to its physical limit (with a risk of potential total failure/damage of the critical actuator) by using

the backup from less critical actuators with an optimum use of inherent redundancy existed in the actuators of the whole system. On the other side, the less critical actuators will be more solicited with respect to the admissibility condition and the overall reliability.

Based on (4.35) and (4.30), the corresponding weighting matrix Ω can be obtained as follows :

$$\Omega = \begin{pmatrix} 38.28 & 0 & 0 \\ 0 & 37.60 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Then, by applying the Theorem 1, the reliable admissible controller K^* is obtained with respect to the criticality level of each actuator as follows :

$$K^* = \begin{bmatrix} -0.0596 & -0.0032 & -0.0342 & 0.0102 & 0.5873 & -0.2408 & -0.0343 \\ 0.0117 & -0.0159 & -0.8797 & -0.0552 & 0.3773 & 0.0246 & 0.1445 \\ 0.0035 & -0.2824 & -0.2715 & 1.0757 & 0.6887 & -0.0005 & -1.0669 \end{bmatrix}$$

In fact, for the reliable controller K^*, the admissible behavior in the nominal functional mode is characterized by the eigenvalues of the system dynamic matrix $\Lambda(A - BK^*)$ obtained as :

$$\Lambda(A-BK^*) = \{-3.8,\ -3.4+0.3i,\ -3.4-0.3i,\ -3.1+0.4i,\ -3.1-0.4i,\ -2.7,\ -2.9\ \}$$

where as it can be verified, $\Lambda(A - BK^*) \in \mathcal{D}_\alpha$.

Figure 4.3 shows the evolution of the controlled outputs in the nominal case obtained for proposed nominal controller K^*. The result is compared with the controlled outputs obtained for the classical controller K_n designed without assigning a priority to the actuators where $\Omega = I_3$. The corresponding control inputs are presented in Figure 4.4.

In fact, for the proposed controller gain K^*, the control inputs are generated taken into account the criticality of the actuators. The more critical actuators are less stressed in the efforts distribution compared to K_n. As explained previously, a significant load applied on the critical actuators accelerates the degradation of the overall system reliability. To guarantee a satisfactory level of the overall system reliability, the critical actuators should be preserved from stress as possible.

The proposed approach obtained a slight degradation of the tracking control performance where the controlled outputs are a little more sensitive versus the evolution of the desired trajectory due to less aggressive demand putting on actuator(s) with higher criticality level(s) when generating control signals to be sent to each actuators. We consider that this degradation is acceptable against the main objective of dependability and overall system reliability aiming to ensure and acceptable tracking performance. The system remains stable and guarantees the required tracking control performance in the steady state.

However, it can be verified that the overall system reliability evaluated for the proposed controller K^* is greater compared to K_n. Figure 4.5 shows the comparison between the overall system reliability obtained with K^* and that obtained with K_n.

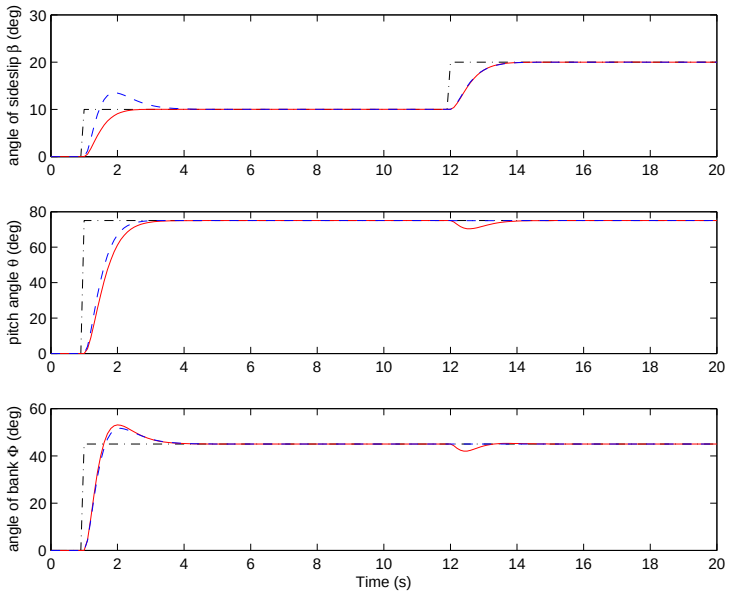

FIGURE 4.3 – Controlled outputs responses in the nominal case with K_n (dashed line) and K^* (solid line).

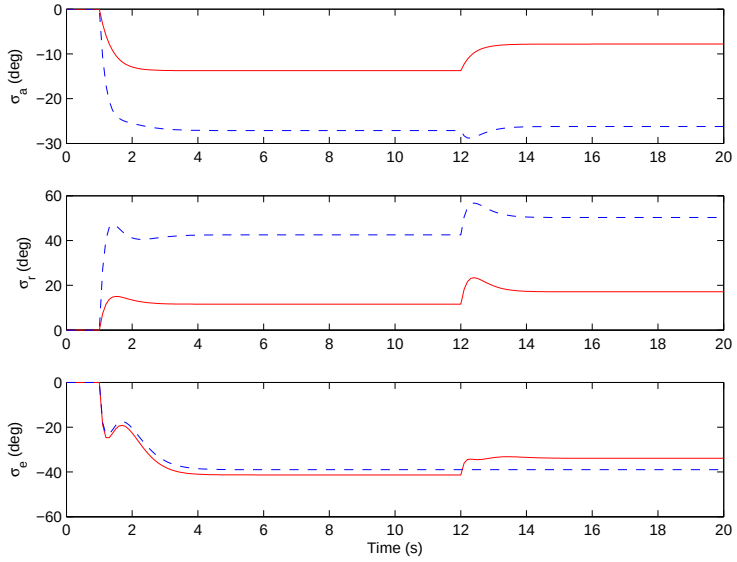

FIGURE 4.4 – Control inputs in the nominal case with K_n (dashed line) and K^* (solid line).

As demonstrated, the illustrated results show that with an optimal choice of the closed-loop system behavior and by an optimal applied load management, the overall system reliability can be guaranteed with same or close control performance. In fact, the system dependability can be improved in the nominal functional mode.

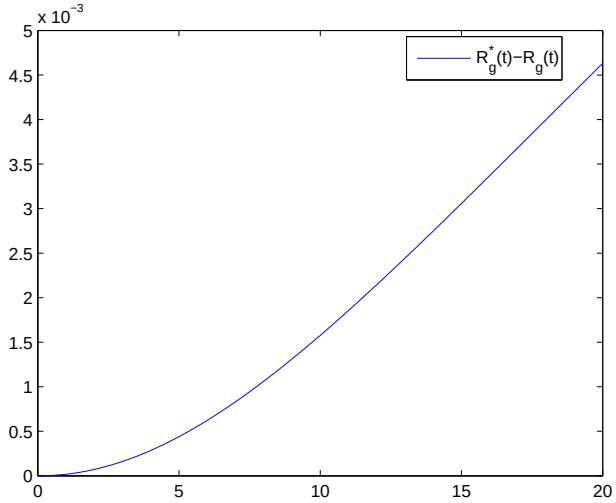

FIGURE 4.5 – Evaluation of the difference between the reliabilities.

Degraded functional conditions : First scenario

In the following, partial loss of the second actuator effectiveness is considered from $t_f = 7sec$. The faulty system can be modeled as in (4.5) where $B_f = B\Gamma$, with $\Gamma = \{1,\ 0.5,\ 1\}$. The figure (4.6) presents the behavior of the controlled outputs without accommodation.

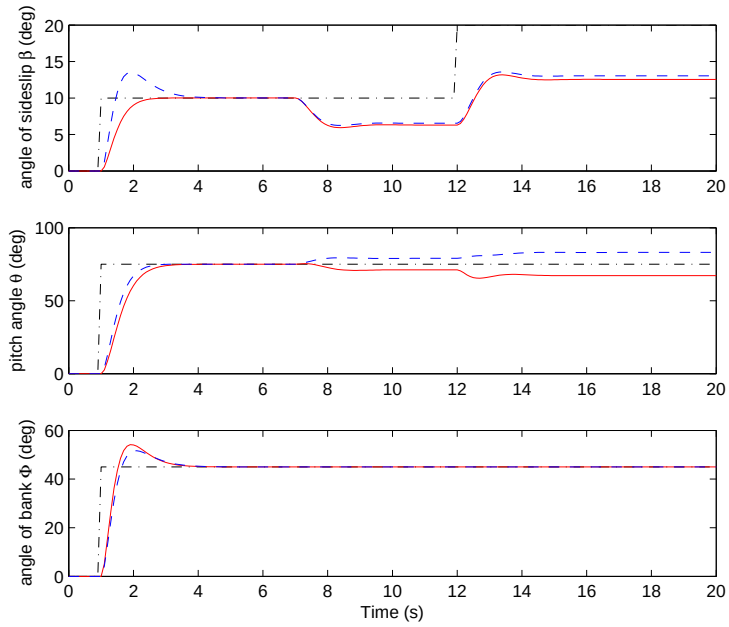

FIGURE 4.6 – Controlled outputs responses in the faulty case without accommodation for K_n (dashed line), K^* (solid line)and y_{ref} (dot-dashed line)

The aim of the proposed approach is to find a fault-tolerant controller K_f^* that guarantees the admissibility and the respect criticality of the actuators. Indeed, the criticality of the actuators is affected by the applied load before the occurrence of fault. Theorem 4.2 is used to design on-line the reliable admissible fault-tolerant controller K_f^* where the actuators reliability and the criticality indicators are estimated.

The effective controller gain K_f^* is obtained as follows :

$$K_f^* = \begin{bmatrix} -0.0595 & -0.0031 & -0.0456 & 0.0089 & 0.5606 & -0.2402 & -0.0292 \\ 0.0220 & -0.0279 & -1.6336 & -0.1044 & 0.4435 & 0.0499 & 0.2889 \\ 0.0096 & -0.2970 & -0.7304 & 1.0536 & 1.8179 & -0.0002 & -1.0668 \end{bmatrix}$$

The corresponding closed-loop eigenvalues $\Lambda(A - B_f K_f^*)$ are :

$$\Lambda(A-B_f K_f^*) = \{-3.8,\ -3.4+0.36i,\ -3.4-0.36i,\ -3.1+0.35i,\ -3.1-0.35i,\ -2.7,\ -2.9\}$$

The evolution of the controlled outputs and the control inputs are compared with the classical admissible fault tolerant controller K_f respectively in figure (4.7) and (4.8).

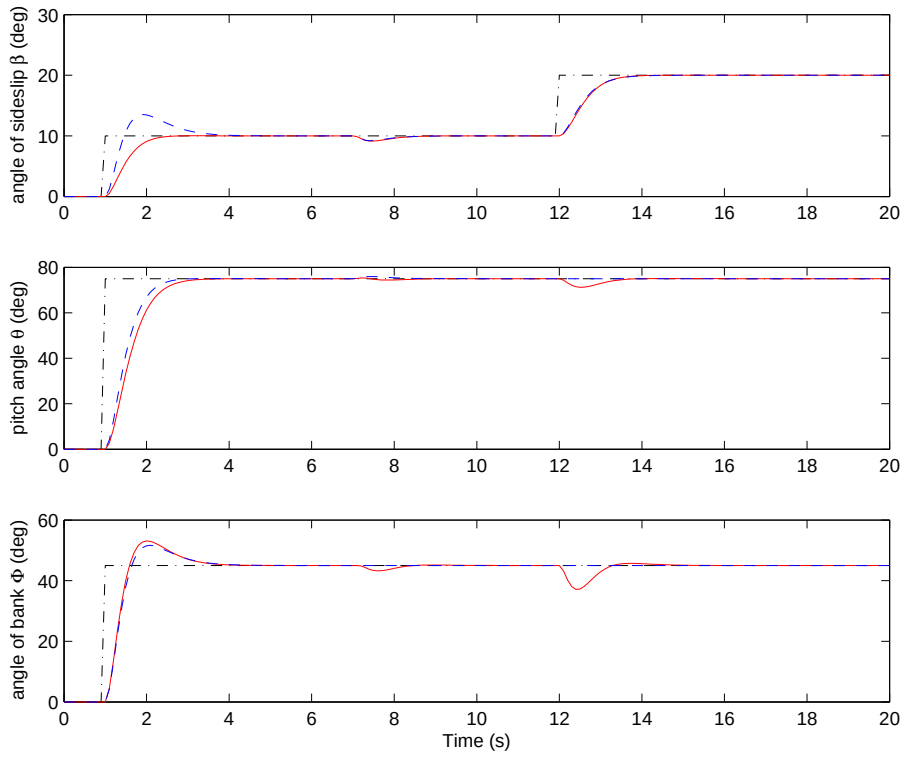

FIGURE 4.7 – Controlled outputs responses in the first faulty case with accommodation for K_f (dashed line), K_f^* (solid line)and y_{ref} (dot-dashed line)

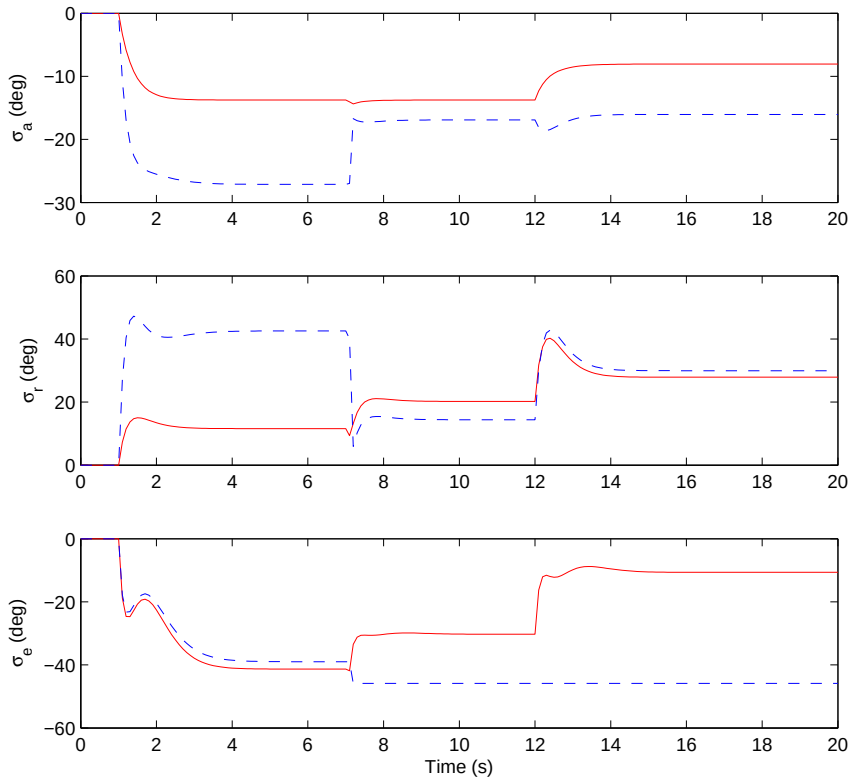

FIGURE 4.8 – Controlled inputs in the first faulty case with accommodation for K_f (dashed line) and K_f^* (solid line)

In fact, for the considered degraded scenario, the classical admissible fault tolerant controller K_f is obtained by solving the LMI problem (4.31), where

$$K_f = \begin{bmatrix} -0.0608 & 0.0035 & 0.1591 & 0.0000 & 0.1180 & -0.2425 & -0.0000 \\ 0.0262 & -0.0695 & -1.9406 & -0.0000 & 1.1703 & 0.0513 & 0.0001 \\ -0.0000 & -0.2696 & 0.0000 & 1.0680 & -0.0000 & 0.0000 & -1.0189 \end{bmatrix}$$

and the corresponding closed-loop eigenvalues $\Lambda(A - B_f K_f)$ are :

$$\Lambda(A-B_fK_f) = \{-3.49,\ -3.49,\ -3.11,\ -3.10,\ -3.11+0.11i,\ -3.11-0.11i,\ -3.55\ \}$$

As illustrated in figure (4.7), the system stability and the requirement control performance are guaranteed both for the classical admissible model matching fault tolerant control and for the proposed effective admissible fault tolerant control. In figure (4.7), the load applied to the most critical actuator (*Actuator 1*) is minimized and the corresponding stress is lower compared to K_f. The developed method preserves the critical actuators which causes a large degradation of the residual system life time and the overall system reliability. A solution to guarantee the distribution of the desired efforts and the control performance are obtained taken into account

the impact of fault and the actuators reliability. The increasing of the overall system reliability improves the dependability of the reconfigurable system where it can be operate until the end of the mission with a hight reliability.

In fact, as expected in figure (4.9) the probability that the system remains operational with K_f^* is larger compared to K_f.

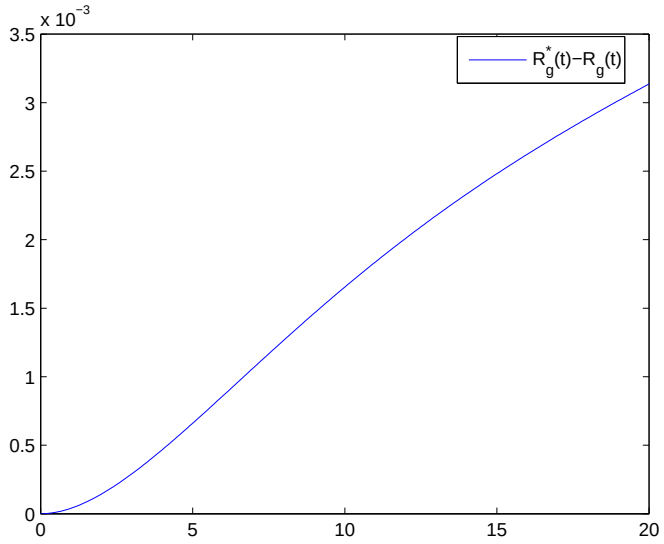

FIGURE 4.9 – Evaluation of the difference between the reliabilities in the first faulty case

Degraded functional conditions : Second scenario

In following, partial loss of the first actuators effectiveness is considered from $t_f = 7sec$. The degraded system can be modeled by (4.5) where in this case

$$B_f = B\Gamma, \quad \Gamma = \begin{pmatrix} 0.6 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The figure (4.10) shows the evolution of the controlled outputs both for the classical fault tolerant controller K_f and for the proposed effective controller gain K_f^*. As it can be verified, the obtained controller gains guarantee the system stability and the control performance with an approximate behaviors. However, the critical actuators are less stressed in the proposed approach compared to the classical one. The control inputs after fault occurrences are not calculated based on the magnitude of fault only, but for the effective controller gain K_f^*, the control inputs are applied to system taken into consideration the severity of fault and the actuators reliability degradation. In fact, the criticality order of the actuators is affected by the impact of load on the actuators reliability. The new estimation of the actuators criticality

indicators are considered on-line in order to guarantee an optimal actuators management. The proposed approach preserves the critical actuators from stress as possible which improves the overall system reliability and dependability.

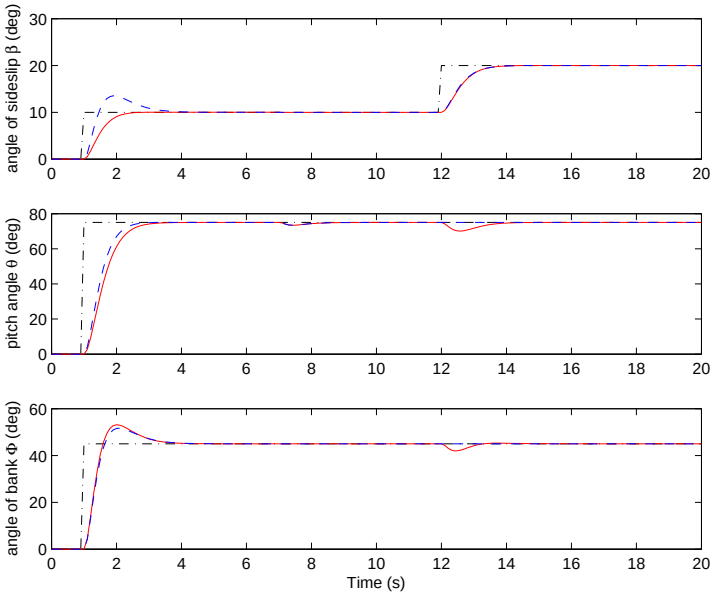

FIGURE 4.10 – Controlled outputs responses in the second faulty case with accommodation for K_f (dashed line), K_f^* (solid line) and y_{ref} (dot-dashed line)

The evaluation of the difference between the overall system reliability for the classical FTC controller and the effective FTC controller gain is presented in figure (4.12). It can be shown that the optimal management of the critical actuators maximizes the overall system reliability. As it can be expected, the probability that the system accomplishes the mission and the ability to tolerate an additional faults until the and of the mission are higher.

4.7 Application 2 : Effective compensation FTC

In this section, an example of tracking control for a linear F-16 aircraft model is given to demonstrate the proposed approach. The linearized aircraft model is described as in (4.44), where, $x(t) = [u_x, u_z, q, u_y, p, r]^T$ is the state, $u(t) = [\delta_{hr}, \delta_{hl}, \delta_{ar}, \delta_{al}, \delta_r]^T$ is the control input, and $y(t) = [a, \dot{\mu}, r_s, \alpha, \bar{\beta}]^T$ is the measured output, respectively. u_x, u_y and u_z are components of aircraft velocity along X, Y and Z body axes respectively. p, q and r are the roll rate about X body axis, the pitch rate about the Y body axis, and the yaw rate about Z body axis, respectively. $\delta_{hr}, \delta_{hl}, \delta_{ar}, \delta_{al}, \delta_r$ are right horizontal stabilator, left horizontal stabilator, right aileron, left aileron, and rudder, respectively. $\dot{\mu}$ is the stability-axis roll rate and r is the stability-axis yaw rate. α is angle of attack and $\bar{\beta}$ is angle of sideslip.

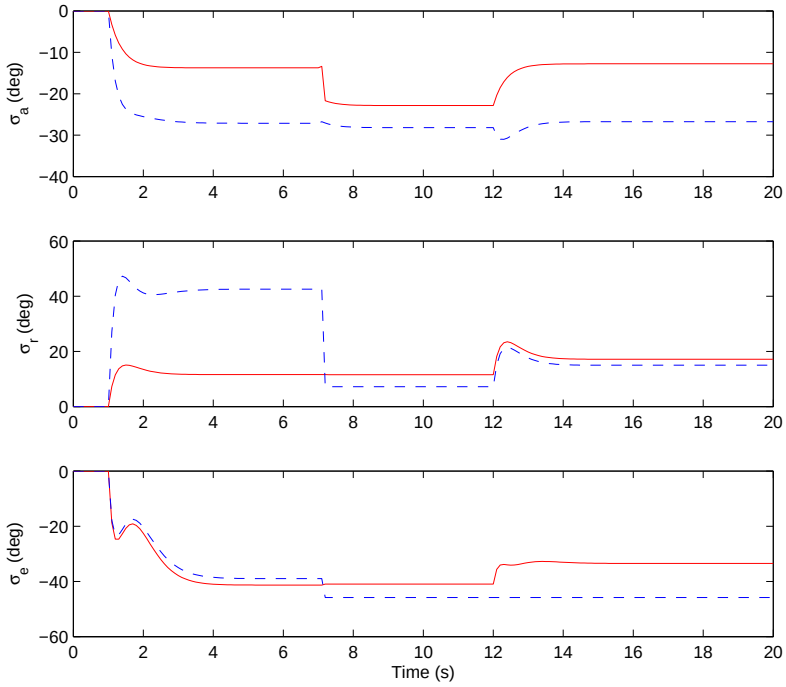

FIGURE 4.11 – Controlled inputs in the second faulty case with accommodation for K_f (dashed line) and K_f^* (solid line)

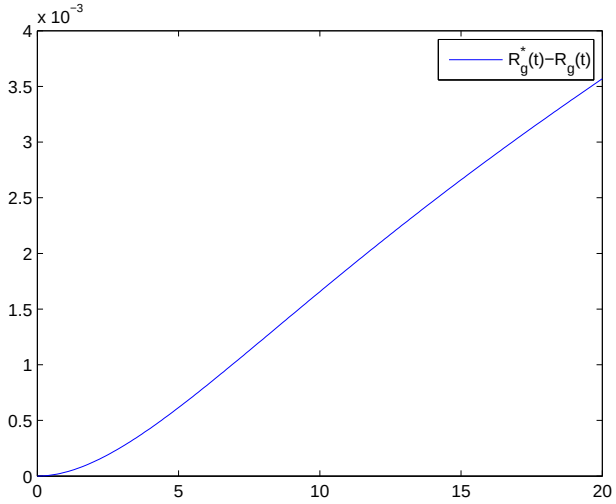

FIGURE 4.12 – Evaluation of the difference between the reliabilities in the second faulty case

The augmented nominal system is modeled as in (4.43) where $\Gamma = I_5$. To illustrate the proposed approach in the short time window, the values of the actuators failure rates are adapted with the time of the considered scenario. The failure rates

are considered with a very huge values and given in the table (4.2). The matrices, A, B and C are given as (Liao et Wang, 2002).

TABLE 4.2 – Failure rates of elementary components

Failure rates	
λ_1^0	$0.08\ min^{-1}$
λ_2^0	$0.04\ min^{-1}$
λ_3^0	$0.01 min^{-1}$
λ_4^0	$0.008\ min^{-1}$
λ_5^0	$0.004\ min^{-1}$

$$A = \begin{bmatrix} -0.0153 & 0.0481 & -5.9420 & 0.0021 & 0 & 0 \\ -0.091 & -0.9568 & 138.3608 & 0.0163 & 0 & 0 \\ 0.0002 & 0.0046 & -1.022 & -0.0005 & 0 & -0.0029 \\ 0 & 0 & 0 & -0.2804 & 6.2667 & -151.1435 \\ 0 & 0 & 0.0003 & -0.1821 & -3.4192 & 0.6401 \\ 0 & 0 & 0.0025 & 0.0454 & -0.0304 & -0.4535 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.239 & .0239 & 0.0250 & 0.0250 & 0 \\ -0.1722 & -0.1722 & -0.1799 & -0.1799 & 0 \\ -0.0873 & -0.0873 & -0.0076 & -0.0076 & 0 \\ -0.3149 & 0.3149 & 0.0233 & -0.0233 & 0.1205 \\ -0.1892 & 0.1892 & -0.3464 & 0.3464 & 0.1237 \\ -0.1678 & 0.1678 & -0.0147 & 0.0147 & -0.0587 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 57.2958 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 57.2468 & 2.3696 \\ 0 & 0 & 0 & 0 & -2.3696 & 57.2468 \\ -0.0155 & 0.3756 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.376 & 0 & 0 \end{bmatrix}$$

For the desired system dynamic and as chosen in (Ye et Yang, 2006), we consider $\eta = 2$ and

$$\mathrm{C_r} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where the matrix C_r determines the output required to track $\dot{\mu}, \alpha$ and β. $Q_1 = diag\ [0.09, 1, 0.36]$, and $Q_2 = diag\ [0.01, 0.2, 0.01, 0, 0, 0]$ are considered.

Nominal functional operating

As it can be expected and by testing the controllability condition (4.25), all the actuators are connected as a parallel scheme. The most critical actuator in this case is the actuators 5. In fact, a significant stress on the critical actuators implies a significant degradation in the overall system reliability. In this example, the proposed effective compensation fault tolerant control is considered. First, an effective controller gain K^* is designed in the nominal functional mode based on proposition (4.1) where $\Gamma = I_5$. On the other side, a classical nominal controller K is synthesis based on (theorem (4.3)). The figure(4.13) shows the trajectory aircraft in the nominal case for both, the proposed controller gain K^* and for the classical controller gain K.

It can be seen that the desired control performance and the tracking problem are guaranteed in the both cases. A slight degradation performance is expected on the first output obtained by the proposed approach. We consider that this degradation is acceptable against the main objective of dependability and overall system reliability aiming to ensure.

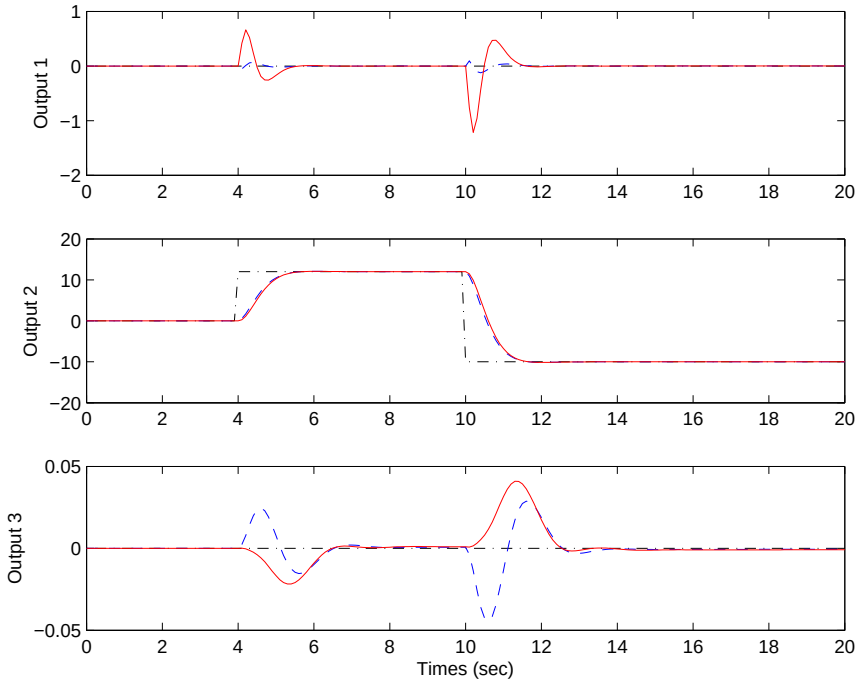

FIGURE 4.13 – Controlled outputs responses in nominal case with K (dashed line), K^* (solid line) and y_{ref} (dot-dashed line)

In figure(4.14) the generated control inputs are presented in the nominal functional mode. It can be seen clearly that the most critical actuator is less stressed and the corresponding applied load is lower compared to the classical approach.

As consequence and to ensure the distribution of the desired efforts, the remaining actuators are more stressed taken into account the system design specification.

In fact, with the proposed approach, the control system preserves the critical actuators from degradation as possible. This strategy minimizes the deterioration of the overall system and keeps the system operational longer.

The evaluation of the overall system reliability for the classical compensation controller and the effective compensation controller gain is presented in figure (4.15).

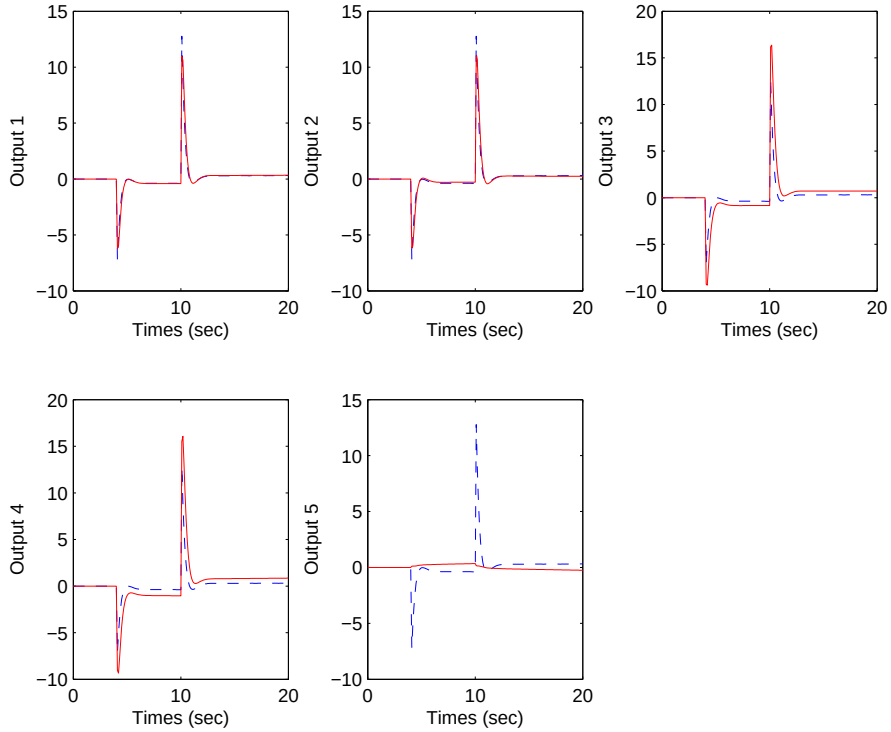

FIGURE 4.14 – Control inputs in the nominal case K (dashed line), K^* (solid line)

It can be shown that the preservation of the critical actuators from a large stress maximizes the overall system reliability. The probability that the system accomplishes the mission and the ability to tolerate an eventual faults are higher for the proposed approach. This strategy improves the dependability of the system.

Degraded functional operating

In following, a partial loss of the actuators 2 effectiveness is considered. For the degraded situation, the augmented system can be modeled by (4.43) where

$$\Gamma = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

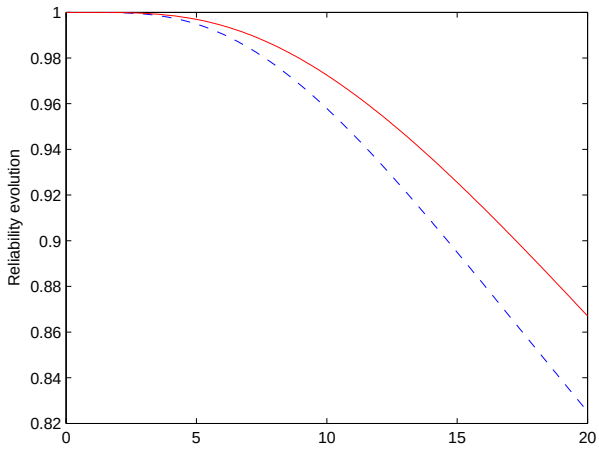

FIGURE 4.15 – Overall system reliability evolution $R_g(t)$ (dashed line), $R_g^*(t)$ (solid line)

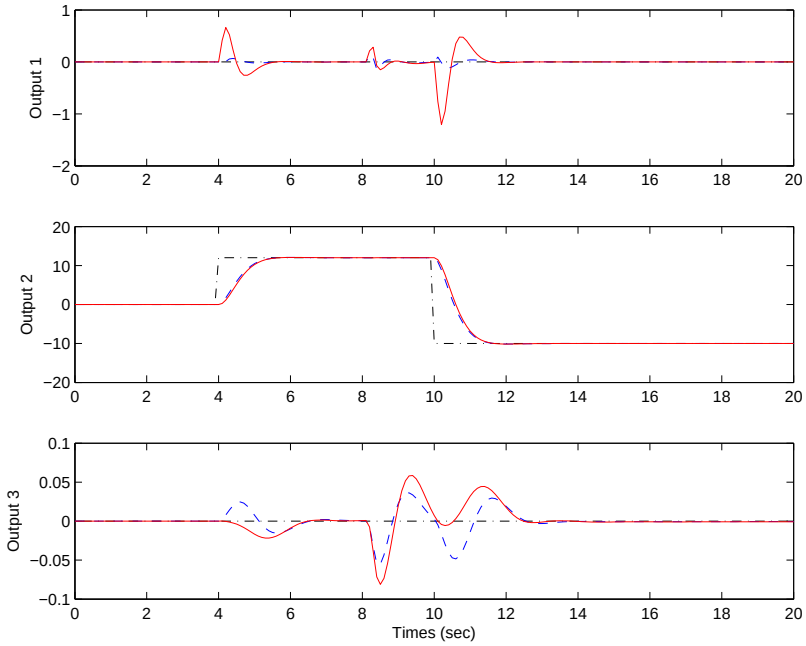

FIGURE 4.16 – Controlled outputs responses in degraded functional mode with K (dashed line), K^* (solid line) and y_{ref} (dot-dashed line)

The figure (4.16) shows the controlled outputs evolution in degraded functional mode. The actuator fault is considered from $t_f = 8sec$. The system stability and the tracking trajectory are guaranteed. The aim of the compensation FTC is to find as close as possible the nominal controller inputs by an the generation of the additional control inputs u_{ad}. In fact, after fault detection and isolation ans as

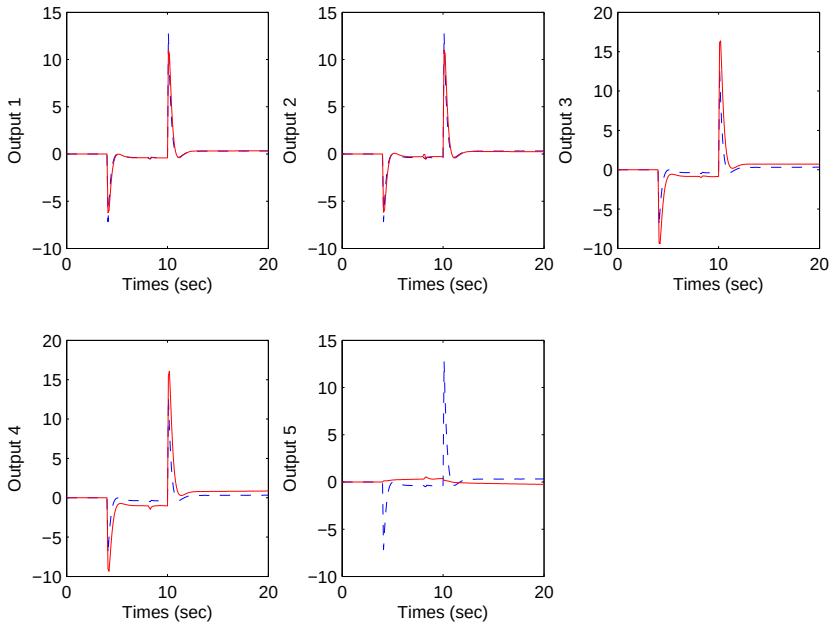

FIGURE 4.17 – Control inputs in degraded functional mode with K (dashed line), K^* (solid line)

presented in proposition (4.3) the controller gain K_f^* can be calculated in order to obtain the same control inputs generated by K^* in the normal functional operating. The overall system reliability for this scenario is approximatively the same obtained in the nominal functional mode where the impact of the fault on the control inputs is insignificant.

4.8 Conclusion

In this chapter, a novel active fault-tolerant controller design approach is proposed by considering the criticality of the actuators. The aim is to synthesize an effective fault-tolerant controller where the corresponding desired control efforts are applied to the system taken into consideration of the overall system reliability. The solution is performed by considering the sensitivity of the overall system reliability regarding the degradation of the actuators due to the applied load and faults. A procedure of reliability sensitivity analysis for controlled systems is proposed based on the state space representation. Actuator criticality indicator is proposed to guide the control law synthesis. The solution of reliable fault-tolerant controller design is obtained through a linear matrix inequality technique. The proposed reliable fault-tolerant control system is illustrated by a flight control application. The proposed approach is a new but preliminary work on the design of a new fault-tolerant control systems where the overall system reliability and dependability have been incorporated in the design for achieving acceptable performance with highest reliability of

the reconfigured system.

Conclusion Générale et Perspectives

Les méthodes de synthèse de la commande tolérante aux fautes sont classées en deux grandes familles avec d'une part les approches passives et d'autre part les méthodes actives. La majorité des méthodes développées sont issues de la théorie de la commande avec comme objectif d'améliorer la sûreté de fonctionnement du système. Dans ce mémoire, nous proposons une nouvelle méthodologie de synthèse des lois de commande tolérante aux fautes avec comme objectif supplémentaire, de garantir la fiabilité du système. Cette nouvelle méthodologie contribue à l'amélioration de la sûreté de fonction des systèmes reconfigurables.

Les outils de fiabilité sont utilisés principalement par la communauté 'Sûreté de fonctionnement' dans le but d'améliorer la fiabilité et la sécurité des systèmes. Bien que ces objectifs soient très proches de celui de la commande tolérante aux fautes, les travaux développés par la communauté 'Commande' n'intègrent pas ces outils. Dans les travaux de cette thèse, nous avons intégré les outils de l'analyse de fiabilité dans la synthèse des lois de commande tolérante aux fautes afin d'augmenter la durée de vie du système. Nous considérons que la fiabilité des actionneurs et leur état de dégradation peuvent jouer un rôle crucial dans le choix de la stratégie de commande appliquée au système. Les lois de commande ont été synthétisées et appliquées sur le système en tenant compte de la fiabilité et de l'état de dégradation des actionneurs. Des indicateurs de fiabilités ont été considérés dans la synthèse des régulateurs. Cette nouvelle méthodologie contribue à des systèmes de commande tolérante aux fautes garantissant la fiabilité.

L'intégration des indicateurs de fiabilité dans la synthèse des lois de commande nécessite l'adaptation des outils de la fiabilité en adéquation avec la théorie de la commande. Ainsi, l'impact de la charge sur l'état de dégradation et le vieillissement des actionneurs ont été considérés. La loi exponentielle a été retenue en premier lieu, pour modéliser l'évaluation de la fiabilité des actionneurs dans le temps. Sous cette hypothèse, un indicateur de fiabilité estimant la dégradation des actionneurs par rapport à la charge est développé. Cet indicateur est utilisé dans l'analyse de reconfigurabilité des systèmes en présence de défauts. En général, la reconfigurabilité des systèmes est évaluée comme la capacité du système à conserver ses fonctionnalités en présence de défauts. Les limites de fonctionnalité sont testées par rapport à un seuil énergétique donné. Considérant l'indicateur de fiabilité proposé, le seuil énergétique indiquant les limites fonctionnelles du système est défini en fonction de l'état de dégradation des actionneurs. La procédure est proposée hors ligne et contribue aux choix de la stratégie employée pour accommoder les défauts. Afin d'appliquer l'étude proposée en ligne et contourner ses limites, la ré-adaptation des hypothèses considérées est nécessaire.

Puis, la commande tolérante aux fautes des systèmes sur-actionnés a été considérée. L'objectif est de proposer une méthodologie d'allocation et de ré-allocation de la

commande garantissant la fiabilité du système. Dans ce contexte, la matrice de pondération utilisée dans le problème d'allocation de la commande a été considérée comme une clef pour améliorer la sûreté de fonctionnement du système. La méthodologie proposée consiste à appliquer les efforts désirés sur le système en tenant compte de la fiabilité des actionneurs. La matrice de pondération est choisie en fonction des indicateurs de fiabilité afin de gérer d'une façon optimale les charges appliquées sur les actionneurs. Dans le cas nominal, la matrice de pondération est choisie en fonction des taux de défaillance des actionneurs. Après l'apparition des défauts, une nouvelle matrice de pondération est obtenue en se basant sur l'estimation de nouveaux taux de défaillance. Ces derniers donnent une image de la dégradation des actionneurs par rapport aux charges appliquées. Dans une seconde approche, le vieillissement des actionneurs est considéré. Un indicateur de fiabilité a été proposé estimant la dégradation de la fiabilité des actionneurs par rapport au temps, à la charge ainsi que la sévérité du défaut. Une matrice de pondération évoluant dans le temps est proposée en fonction de l'indicateur développé. La ré-allocation de la commande ne permet pas d'accommoder tous les défauts affectant le système. Parfois, il est nécessaire de reconfigurer le régulateur définissant les efforts désirés suivant le degré de redondance existant. Une méthodologie garantissant la fiabilité pour tous les modes de fonctionnent dégradés nécessite l'intégration des outils de fiabilité dans la synthèse du régulateur.

Afin de généraliser la méthodologie proposée, la synthèse d'un régulateur tolérant aux fautes garantissant la fiabilité du système est considérée. Nous proposons une procédure d'analyse de fiabilité des systèmes en se basant sur une étude de sensibilité de cette dernière au regard des actionneurs. Cette procédure permet de déterminer le diagramme de fiabilité d'un système modélisé par sa représentation d'état. En se basant sur cette analyse, les actionneurs jugés critiques sont sélectionnés en tenant compte de la structure du système. Ainsi, les gains de la loi de commande garantissant la fiabilité du système sont synthétisés sous une formulation LMI. Deux approches sont considérées : l'approche par compensation et l'approche appelée Admissible Model Matching. La méthodologie proposée est basée sur le taux de défaillances ainsi que l'amplitude des défauts. Des outils de la commande robuste peuvent être utilisés afin de considérer des incertitudes sur le diagnostic de défauts ainsi que les taux de défaillances des actionneurs.

Perspectives

Les travaux proposés sont développés dans le cadre de la commande active tolérante aux fautes. Il serait intéressant de synthétiser des lois de commande tolérante aux fautes garantissant la fiabilité du système selon des approches passives. Cela permet d'améliorer la robustesse du système par rapport aux incertitudes, aux perturbations ainsi qu'à la dégradation des actionneurs. Une étude de sensibilité des actionneurs par rapport aux entrées de commande est nécessaire. Les outils de la maintenance prévisionnelle peuvent être adaptés avec la théorie de la commande robuste H_2/H_∞ ou aussi par les techniques basées sur les chaines de Markov dans

le cas stochastique .

La loi de commande tolérante aux fautes garantissant la fiabilité est synthétisée en fonction des taux de défaillance de base des actionneurs. Nous avons supposé que les taux de défaillance de base des actionneurs sont connus a priori. Dans certains cas, les taux de défaillance sont partiellement connus. Il est intéressant d'intégrer les incertitudes sur les taux de défaillance dans les calculs. Cela implique l'adaptation des hypothèses considérées. Les approches stochastiques peuvent être une solution à cette problématique.

Par rapport aux systèmes sur-actionnés, la ré-allocation de la commande est une solution pour accommoder certaines classes de défauts suivant le degré de redondance existant. Il sera intéressant d'approfondir l'étude et envisager une analyse hors ligne de la structure du système. Cette étude permet de synthétiser un système de commande tolérante aux fautes dans le cas de défauts sévères non accommodables par la ré-allocation.

Annexe A : Fiabilité en discret

Grandeurs caractéristiques de la fiabilité en temps discret

Nous considérons que la durée de vie d'un système en temps discret est le nombre k de sollicitations nécessaire pour que le système tombe en panne. D'une autre manière, k représente le *rang* de la première sollicitation pour laquelle le système ne fonctionne plus. Les définitions des principales grandeurs de la fiabilité en temps discret, analogue à celles présentées précédemment en temps continu sont données comme suit :

Définition .7

1. *La probabilité que le système soit défaillant à la $k^{ème}$ sollicitation est :*

$$\forall k \in \mathbb{N}^*, \quad p(k) = \mathbb{P}(K = k) \tag{1}$$

   avec K l'état de défaillance du composant.

2. *La fonction de répartition, qui traduit la probabilité que le système soit défaillant entre la première et la $k^{ème}$ sollicitation est :*

$$\forall k \in \mathbb{N}^*, \quad F(k) = \mathbb{P}(K \leq k) = \sum_{i=1}^{k} p(i) \tag{2}$$

3. *La fiabilité, qui traduit la probabilité que le système fonctionne encore à la $k^{ème}$ sollicitation est :*

$$\forall k \in \mathbb{N}^*, \quad R(k) = \mathbb{P}(K > k) = 1 - F(k) = 1 - \sum_{i=1}^{k} p(i) \tag{3}$$

4. *Le temps moyen jusqu'à la première défaillance (Mean Time to failure) représente dans ce cas le nombre moyen de sollicitations. Il est défini comme suit :*

$$\forall k \in \mathbb{N}^*, \quad MTTF = \mathbb{E}(K) = \sum_{i=1}^{\infty} ip(i) \tag{4}$$

5. *Le taux de défaillance dans le cas discret donne la probabilité conditionnelle de défaillance de l'entité à la k^{eme} sollicitation, sachant que le fonctionnement du système est assuré jusqu'à $(k-1)$ sollicitation.*

$$\forall k \in \mathbb{N}^*, \quad \lambda(k) = \mathbb{P}(K = k | K \geq k) = \frac{\mathbb{P}(K = k)}{\mathbb{P}(K \geq k)} = \frac{p(k)}{R(k-1)} \tag{5}$$

En effet, la première notion d'un taux de défaillance appelé aussi taux de hasard en temps discret apparait dans le travail de (Barlow *et al.*, 1963). Dans le cas discret $\lambda(k)$ est inférieur ou égal à 1. Puis, le taux de défaillance dans le cas discret est présenté dans les travaux de (Barlow et Proschan, 1965; Cox, 1972). Il est important de noter que, contrairement au cas continu, le taux de défaillance en discret est une probabilité conditionnelle comprise donc entre 0 et 1. Comme dans le cas continu, toutes les grandeurs de la fiabilité peuvent s'exprimer à l'aide du taux de défaillance.

$$\lambda(k) = \mathbb{P}(K = k | K \geq k) = \frac{p(k)}{R(k-1)} = 1 - \frac{R(k)}{R(k-1)} \tag{6}$$

La formule de récurrence est alors déduite :

$$R(k) = R(k-1)(1 - \lambda(k))$$

Enfin, la fiabilité d'une entité dans le cas discret peut être évaluée en fonction de son taux de défaillance comme suit :

$$R(k) = \prod_{i=1}^{k} (1 - \lambda(i)) \tag{7}$$

Tenant compte de ce résultat, le MTTF défini dans (3) est exprimé en fonction de la fiabilité comme suit :

$$\begin{array}{l} MTTF = \mathbb{E}(K) = \sum_{k=1}^{\infty} k\mathbb{P}(K = k) \\ \quad = \sum_{k=1}^{\infty} k(R(k-1) - R(k)) = \sum_{k=0}^{\infty} (k+1)R(k) - \sum_{k=1}^{\infty} kR(k) \\ \quad = \sum_{k=0}^{\infty} R(k) \end{array} \tag{8}$$

En intégrant la relation (7) dans (8), l'expression du MTTF en fonction du taux de défaillance est obtenue :

$$MTTF = 1 + \sum_{k=0}^{\infty} \prod_{j=1}^{k} (1 - \lambda(j)) \tag{9}$$

D'après les travaux de (Padgett et Spurrier, 1985), le MTTF d'une entité existe dans le cas discret si le théorème suivant est vérifié :

Théorème .1 *Le MTTF existe si et seulement si il existe* $\epsilon > 0$ *et* $m \in \mathbb{N}$ *tels que tout* $k > m$, $\frac{k\lambda(k)}{1-\lambda(k)} > 1 + \epsilon$

Ainsi, les résultats suivants sont obtenus :

1. Si le taux de défaillance est croissant, $MTTF \leq \frac{1}{\lambda(1)}$
2. Si le taux de défaillance est décroissant, $MTTF \geq \frac{1}{\lambda(1)}$
3. Si le taux de défaillance est constant, $MTTF = \frac{1}{\lambda}$

lois discrètes de probabilité pour l'évaluation de la fiabilité

a) Loi binomiale

Soit X une variable aléatoire discrète qui représente le nombre de réalisation d'un événement A. Cette dernière est distribuée au cours de n expériences suivant une loi binomiale de paramètres (p, n) où p est la probabilité de réalisation de A :

$$P(X = k) = C_n^k p^k (1-p)^{n-k} \tag{10}$$

où :

$$C_n^k = \frac{n!}{k!(n-k)!} \tag{11}$$

avec $0 \leq k \leq n$ et $0 \leq p \leq 1$.

La fonction de répartition de la loi binomiale peut être obtenue comme suit :

$$F(k) = \mathbb{P}(X \leq k) = \sum_{i=0}^{k} C_n^i \mathbb{P}^i (1-p)^{n-i} \tag{12}$$

De plus :

$$E(X) = np$$

Cette distribution est utilisée dans le cas d'une entité ayant une probabilité de défaillance P à la sollicitation. Pour n sollicitations, le nombre de défaillances peut être représenté suivant une loi binomiale(P, n). Comme cas particulier, nous distinguons :

- Pour $n \to \infty$ et np constant, la loi binomiale tend vers une loi de Poisson.
- Pour $n \to \infty$ la loi tend vers une loi normale de moyenne np et de variance $\sigma^2 = np(1-p)$.

b) Loi de poisson

La loi de poisson est une loi à un paramètre positif μ définie par :

$$\mathbb{P}(X = k) = \frac{\mu^k}{k!} e^{-\mu} \tag{13}$$

Cette loi exprime la probabilité d'apparition d'un nombre k d'événements en un temps donné, lorsqu'à tout instant la probabilité d'occurrence d'un événement est la même. La fonction de répartition obtenue est donnée par :

$$F(k) = \sum_{i=0}^{k} \frac{\mu^i}{i!} e^{-\mu} \tag{14}$$

Annexe B : Stabilité

Nous allons rappeler ici quelques notions sur la stabilité dynamique des systèmes à temps continu ainsi que quelques théorèmes et transformations de la théorie des matrices.

Stabilité au sens de Lyapunov

La stabilité au sens de Lyapunov est une théorie mathématique générale applicable à toute équation différentielle. Ce principe signifie qu'une équation différentielle autonome avec une condition initiale suffisamment proche de la trajectoire d'équilibre a une solution qui reste arbitrairement proche de la trajectoire d'équilibre.

La méthode directe de Lyapunov nous permet de regarder la stabilité asymptotique comme l'existence d'une fonction de Lyapunov propre définie positive telle que sa dérivée soit strictement négative. Une classe de fonctions de Lyapunov jouant un rôle important dans l'analyse de stabilité des systèmes dynamiques est la classe des fonctions quadratiques. Ces fonctions s'écrivent sous la forme :

$$\begin{aligned} V(x,t) &= x^T(t)Px(t) \\ \dot{V}(x,t) &= \partial V(x,t)/(\partial V(x,t)/\partial t)^T < 0 \end{aligned} \tag{1}$$

Cette fonction est définie positive si P est une matrice symétrique définie positive. Dans le cas des systèmes autonomes LTI,

$$\dot{x} = Ax$$

Une condition nécessaire et suffisante pour que la dérivée $\dot{V}(x,t)$ soit négative et implicitement pour que le système autonome LTI soit asymptotiquement stable, consiste à trouver une matrice P symétrique définie positive telle que l'inégalité matricielle suivante soit vérifiée :

$$A^TP + PA < 0 \tag{2}$$

Stabilité en LMI

La stabilité du système peut être reformulée en un problème d'Inégalité Matricielle Linéaires comme suit (Boyd *et al.*, 1994) :

Si $P = P^T > 0$ et $Q = P^{-1}$, alors :

$$P - A^TPA > 0 \Leftrightarrow \begin{pmatrix} P & A^TP \\ PA & P \end{pmatrix} > 0 \tag{3}$$

$$Q - AQA^T > 0 \Leftrightarrow \begin{pmatrix} Q & AQ \\ QA^T & Q \end{pmatrix} > 0 \tag{4}$$

Théorie des matrices

Une matrice $P \in \mathbb{R}^{n \times n}$ est définie positive si et seulement si pour tout x non nul, la relation $x^T P x > 0$ est vérifiée.

Les valeurs propres d'une matrice symétrique définie positive sont réelles, positives et $det(P) > 0$.

Une matrice est définie non négative lorsque pour tout vecteur x non nul, la condition $x^T P x \geq 0$.

Si l'opposé de la matrice P noté $-P$ est non négative, alors P est définie négative. De même, lorsque $-P$ est définie non négative, alors P est définie non positive. Ces notions sont à distinguer de la définition d'une matrice positive qui est une matrice dont tous les coefficients sont positifs.

Complément de Schur

Soit les matrices $Q \in S_n$ (ensemble des matrices symétriques dans $\mathbb{R}^n$, $R \in S_m$ et la matrice M définie comme suit (Boyd *et al.*, 1994) :

$$M = \begin{pmatrix} Q & S \\ S^T & R \end{pmatrix} < 0 \tag{5}$$

Les relation suivantes sont équivalentes :

- M est définie négative
- $R < 0$ et $Q - SR^{-1}S^T < 0$
- $Q < 0$ et $R - S^T Q^{-1} S < 0$

Annexe C : Région LMI

Définition .8 (Les régions LMI) *Un sous ensemble $\mathcal{D}$ du plan complexe est dit une région LMI s'il existe une matrice symétrique $\alpha \in I\!R^{m\times m}$ et une matrice $\mathcal{B} \in I\!R^{m\times m}$ telle que*

$$\mathcal{D} = z \in \mathbb{C} : f_{\mathcal{D}}(z) < 0 \tag{1}$$

avec $f_{\mathcal{D}}(z) = \alpha + z\mathcal{B} + \bar{z}\mathcal{B}^T$. La notation $\bar{z}$ désigne le conjugué de z et $f_{\mathcal{D}}(z)$ est appelée la fonction caractéristique de $\mathcal{D}$.

Les valeurs propres d'une matrice A sont placées dans une région LMI $\mathcal{D}$ définie dans (1) du plan complexe, si et seulement si, il existe une matrice symétrique $P > 0$ telle que :

$$M_{\mathcal{D}}(A, P) = \alpha \otimes P + \mathcal{B} \otimes (AP) + \mathcal{B}^T \otimes (AP)^T \tag{2}$$

où $\otimes$ représente le produit de Kronecker. Considérons deux régions LMI $\mathcal{D}_1$ et D_2 du plan complexe. Les valeurs propres de la matrice A appartiennent à la région LMI $D_1 \cap D_2$ avec des fonctions caractéristiques $f_{D_1}(z)$ et f_{D_2} respectivement si et seulement si il existe une matrice symétrique $P > 0$, solution des inégalités suivantes :

$$\begin{array}{c} M_{D_1}(A, P) < 0 \\ M_{D_2}(A, P) < 0 \end{array} \tag{3}$$

que $z \in \mathcal{D}$.

Soit D_i une région résultante de l'intersection de N sous-régions LMI. Les valeurs propres d'une matrice réelle appartiennent à $\mathcal{D}$ si et seulement si il existe une matrice $P \in \mathbb{R}^{n\times n}$, symétrique définie positive, telle que :

$$M_{D_i}(A, P) = \alpha_i \otimes P + \beta_i \otimes (AP) + \beta_i^T \otimes (AP^T) < 0, \quad \forall i \in [1, 2, \ldots, N] \tag{4}$$

ce qui est équivalent à :

$$M_D(A, P) = \alpha \otimes P + \beta \otimes (AP) + \beta^T \otimes (AP)^T = Diag(M_D(A, P)) < 0, \quad \forall i \in [1, \ldots N] \tag{5}$$

où $\alpha = diag(\alpha_1, \ldots, \alpha_N)$ et $\beta = diag(\beta_1, \ldots, \beta_N)$. Cette inégalité montre alors que D peut elle même être formulée comme une région LMI. Ceci montre que l'approche LMI permet de considérer la même matrice P pour toutes les sous-régions de l'intersection tout en préservant la nécessité de la condition de $D-$ stabilité.

L'utilisation du domaine d'application de la fonction $f_D(z)$ permet de considérer un cercle de rayon r de centre $(-q, 0)$. La fonction caractéristique associée est alors :

$$\begin{pmatrix} -r & q + \bar{z} \\ q + z & -r \end{pmatrix} < 0 \tag{6}$$

La LMI garantissant que les pôles de la matrice A appartiennent à la région D est alors :

$$\begin{pmatrix} -rP & qP + PA^T \\ qP + AP & -rP \end{pmatrix} < 0 \tag{7}$$

avec $P > 0$.

Les coefficients sont alors réglés comme suit : $\alpha = \begin{pmatrix} -r & q \\ q & -r \end{pmatrix}$ et $\beta = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

Si l'on pose $q = 0$ et $r = 1$ (ce qui correspond au cercle unité en discret), alors cela revient à vérifier la contrainte suivante :

$$\begin{pmatrix} -P & A^T \\ AP & -P \end{pmatrix} < 0 \tag{8}$$

qui est équivalente à $A^T PA - P < 0$ avec P symétrique définie positive exprimant la stabilité quadratique d'un système de la forme $\dot{x} = Ax$.

La fonction (7) permet de définir une région bien précise du plan complexe et permet d'assurer un taux de décroissance sur la fonction de Lyapunov. En effet, la région circulaire complexe assure une borne minimale du taux de décroissance mais aussi un taux d'amortissement minimal en boucle fermée. Il est possible de cette manière de contraindre les pôles d'un observateur à appartenir à une région bien localisée du plan complexe et d'assurer en même temps la stabilité quadratique de l'ensemble.

Bibliographie

Alwi, H. et Edwards, C. (2008). Fault tolerant control using sliding modes with on-line control allocation. *Automatica*, 44:1859–1866. 3.1, 3.2

Antsaklis, Z. et Gao, P. (1992). Reconfigurable control system design via perfect model-following. *International Journal of Control*, 56:783–798. 1.1.3.2

Apkarian, A., Ghahinet, P. et Becker, G. (1995). Self-scheduled h_∞ control of linear parameter-varying systems. a design example. *Automatica*, 31(9):1251–1261. 4.4

Barlow, E., Marshall, A. et Proschan, F. (1963). Properties of probability distributions with monotone hazard rate. *Annals of Statistics*, 34:375–389. 4.8

Barlow, E. et Proschan, F. (1965). Mathematical theory of reliability. *In Jhon Wiley and Sons, Inc, New York*. 4.8

Benvenuti, L. et Benedetto, D. D. (1994). Approximate output tracking for nonlinear non-minimum phase systems with an application to flight control. *International Journal of Robust and Nonlinear Control*, 4:397–414. 4.6

Blanke, M., Kinnaert, M., Lunze, J. et Staroswiecki, M. (2006). *Diagnosis and fault tolerant control*. Control Systems Series, Springer-Verlag London. 3.1

Blanke, M., Staroswiecki, M. et Wu, E. (2001). Concepts and methode in fault-tolerant control. *In American control conference*, volume 4, pages 2606–2620, Arlington, VA, USA. 1.1.2.2, 4.1

Bodson, M. (2002). Evaluation of optimization methods for control allocation. *Journal of Guidance, Control, and Dynamics*, 25:703–711. 3.1, 3.4.1

Bodson, M. et Groszkiewicz, J. (1997). Multivariable adaptive algorithms for reconfigurable flight control. *IEEE Control Systems Magazine*, 5:217–229. 1.1.3.2, 1.1.3.2, 4.1

Bordignon, K. (1996). *Constrained control allocation for systems with redundant control effector*. Thèse de doctorat, vergenia Polytechnic Institute and State University. 3.1, 3.4.1, 3.4.2

Boskovic, J. D. et Mehra, R. K. (1998). A multiple model-based reconfigurable flight control system design. *In Proceedings of the 37th IEEE Conference on Decision and Control*, pages 4503 – 4508, Tampa, FL , USA. 1.1.3.2

Boyd, S., Ghaoui, L. E., Feron, E. et Balakrishnan, V. (1994). *Linear matrix inequalities in system and control theory*, volume 15. Society for Industrial and Applied Mathematics SIAM, Philadeplhia, PA. 4.2, 4.8, 4.8

Burken, J., Lu, P., Wu, Z. et Bahm, C. (2001). Two reconfigurable flight control design methods : Robust servomechanism and control allocation. *Journal of Guidance, Control, and Dynamics*, 24:482–493. 3.1, 3.4.3, 3.1

Chen, J. et Patton, R. J. (1999). *Robust model based fault diagnosis dor dynamic systems*. Kluwer Academic Publishers. 1.1.3.1, 1.1.3.1, 1.3.1

Chen, J. et Patton, R. J. (2001). Fault tolerant control systems design using linear matrix inequalities. *In Proceedings of the 6th European Control Conference, ECC'01*. 1.1.2.1

Chow, E. et Willsky, A. (1984). Analytical redundancy and the design of robust failure detection systems. *IEEE Transactions on Automatic Control*, 29:603–614. 1.1.3.1

Ciubotaru, B., Staroswiecki, M. et Christophe, C. (2006). Fault tolerant control of the boeing 747 short-period mode using the admissible model matching technique. *In IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes 06*, Beijing, China. 1.1.3.2

Cox, D. (1972). Regression models and life tables. *Journal of the Royal Statistical Society*, 34:187–220. 2.3.1, 3.3.1, 3.3.1, 4.3.1, 4.8

Dale, J. (1985). Application of the proportional hazards model in the reliability field. *Reliability Engineering*, 10:1–14. 3.3.1

Ding, S., Jeinsch, P. et Ding, E. (2000). A unifief approach to the optimization of fault detection systems. *International Journal of Adaptive Control and Signal Processing*, 14:725–745. 1.1.3.1

Durham, W. (1993). Constrained control allocation. *Journal of Guidance, Control, and Dynamics*, 16:717–125. 3.1

EASA (2007). Annual safety review 2007. *Agence Européenne de la Sécurité Aérienne*. 1.3.1

Enns, D. (1998). Control allocation approachs. *AIAA Guidance, Navigation, and Control Conference*, pages 98–108. 3.1, 3.4.2

Finkelstein, M. S. (1999). A note on some aging properties of the accelerated life model. *Reliability Engineering et System Safety*, 71(1):109–112. 2.3.1, 3.3.1

Frank, P. (1990). Fault diagnosis in dynamic system using analytical and knowledge based redundancy - a survey. *Automatica*, 26:459–474. 1.1.3.1

Frank, P., Ding, S. et , B. S. (2000). Current developments in the theory of fdi. *In Proceedings of IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes 2000*, pages 16–27, Budapest. 1.1.3.1

Gao, Z. et Antsaklis, P. (1991). Stability of the pseudo inverse method for reconfigurable control. *International Journal of Control*, 53:717–729. 1.1.3.2, 4.1

Gertler, J. (1997). detection and isolation using parity relations. *Control Engneering Practice*, 5:653–661. 1.1.3.1

Gertsbakh, I. (2000). *Reliability theory with applications to preventive maintenance*. Springer. 3.3.1, 4.4

Guenab, F. (2007). *Contribution aux systèmes tolérants aux défauts : Synthèse d'une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants*. Thèse de doctorat, Université Henri Poincaré, Nancy 1. 1.3.4, 2.3.1

Guenab, F., Theilliol, D., Weber, P., Zhang, Y. et Sauter, D. (2006). Fault tolerant control desing : A reconfiguration strategy based on reliability analysis under dynamic behaviour constraints. *In 6th IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes 06*, Beijing, RP China. 2.3.2

Guenab, F., Weber, P., Theilliol, D. et Zhang, Y. (2010). Design of a fault tolerant control system incorporating reliability analysis under dynamic behaviour constraints. *International Journal of Systems Science*, 42:219–223. 4.1, 4.4.2

Harkegard, O. (2002). Efficient active set algorithms for solving constrained least squares problems in aircraft control allocation. Las Vegas, Nevada. 3.1, 3.1, 3.4.4

Harkegard, O. et Glad, S. (2004). Resolving actuator redundancy-optimal control vs. control allocation. *Automatica*, 41:137–144. 3.4.4, 3.5

He, X., Wang, Z. et Zhou, D. (2009). Robust h_∞ filtering for time delay systems with probabilistic sensor faults. *IEEE Signal Processing Letters*, 16:442–445. 4.1

Henry, D. et Zolghadri, A. (2006). Norm based design of robust fdi schemes for uncertain systems under feedback control : comparaison of two approaches. *Control Engineering Practice*, 14:1081–1097. 1.1.3.1

Isermann, R. (1984). Process fault detection based on modeling ans estimation methods-survey. *Automatica*, 20(4):387–404. 1.1.3.1

Isermann, R. (2005). Model-based fault detection ans diagnosis - status and applications. *Annual Reviews in Control*, 29:71–85. 1.1.3.1

Isermann, R. (2006). *Fault-diagnosis systems : An introduction from fault detection to fault tolerance*. Springer Berlin, Germany. 1.3.1

Jaimoukha, I., Li, Z. et Papakos, V. (2006). matrix factorization solution to the h_-/h_∞ fault detection problem. *Automatica*, 42:1907–1912. 1.1.3.1

Jamouli, H., Sauter, D. et Keller, J. Y. (2004). Fault tolerant control using augmented fault detection filter. *In International Symposium on Industrial Electronics*, France. 1.1.2.1

Jin, X. et Yang, G. H. (2009). Robust adaptive fault tolerant compensation control with actuator failures and bounded distrurbances. *Acta Automatica Sinica*, 35: 305–309. 4.1

Kanev, S. et Verhaegen, M. (2000). Controller reconfiguration for non-linear systems. *Control Engineering Practice*, 8:1223–1235. 1.1.3.2

Kanev, S., Verhaegen, M. et Nijsse, G. (2001). A method for the design of fault-tolerant systems in case of sensor and actuator faults. *In In European Control Conference ECC'01*. 1.1.3.2

Kerrigan, E. et Maciejowski, J. (1999). Fault-tolerant control of a ship propulsion system using model predictive control. *In Proceedings of European Control Conference*, Karlsruhe, Germany. 1.1.3.2, 1.1.3.2

Khelassi, A., Jiang, J., Theilliol, D., Weber, P. et Zhang, Y. (2011a). Reconfiguration of control inputs for overactuated systems based on actuators health. *In Proceedings of 18th IFAC World Congress*, Milan, Italy. 3.3.2

Khelassi, A., Theilliol, D. et Weber, P. (2009a). On reconfigurability for actuator faults under reliability constraints. *In IFAC Workshop on Automation in Mining, Mineral and Metal Industry, IFAC-MMM*, Viña del Mar. Chile. 2.3.1

Khelassi, A., Theilliol, D. et Weber, P. (2009b). Reconfigurability for reliable fault-tolerant control design. *In* 7^{th} *Workshop on Advanced Control and Diagnosis*, Zielon Gora, Poland. 2.2.3

Khelassi, A., Theilliol, D. et Weber, P. (2010a). Control design for overactuated systems based on reliability indicators. *In UKACC International Conference on Control, CONTROL 2010*, Coventry. United Kingdom. 3.3.1

Khelassi, A., Theilliol, D. et Weber, P. (2010b). Synthèse d'une loi de commande reconfigurable assurant la fiabilité des systèmes. *In Sixième Conférence Internationale Francophone d'Automatique, CIFA 2010*, France. 3.3.1

Khelassi, A., Theilliol, D. et Weber, P. (2011b). Fault tolerant control design with respect to actuators health degradation : An lmi approach. *In Proceedings of IEEE Multi-conference on Systems and Control, MSC-CCA'11*, Denver, CO, USA. 4.2

Khelassi, A., Theilliol, D. et Weber, P. (2011c). A novel active fault tolerant control design with respect to actuators reliability. *In Proceedings of 50th IEEE Conference on Decision and Control and European Control Conference, IEEE CDC-ECC*, Orlando, FL, USA. 4.2, 4.4

Khelassi, A., Theilliol, D. et Weber, P. (2011d). Reconfigurability analysis for reliable fault-tolerant control design. *International Journal of Applied Mathematics and Computer Science*, 3. 2.2.3

Khelassi, A., Weber, P. et Theilliol, D. (2010c). Reconfigurable control design for over-actuated systems based on reliability indicators. *In Proceedings of IEEE SyStol'10, Conference on Control and Fault Tolerant Systems*, Nice, France. 3.3.1

Khelassi, A., Weber, P., Theilliol, D. et Aubrun, C. (2011e). Evaluation of fault tolerant system against actuators aging applied to flotation circuit. *In Proceedings of 18th IFAC World Congress*, Milan, Italy. 3.3.2

Konstantopoulos, L. et Antsaklis, P. (1996). An eigenstructure asignement approach to control reconfiguration. *In Proceedings of IEEE Mediterranean Symposium on Control and Automation*, Greece. 1.1.3.2

Liao, F. et Wang, J. L. (2002). Reliable robust flight tracking control : An lmi approach. *IEEE Transactions on Control Systems Technology*, 10:76–89. 4.7

Liu, Y. et Crespo, L. G. (2010). Adaptive control allocation in the presence of actuator failures. *In AIAA Guidance, Navigation, and Control Conference*. 3.1

Lyu, M. (2005). *Handbook of software reliability engineering*. IEEE Computer Society Press and McGraw-Hill Book Company. 4.3.3

Maciejowski, J. et Jones, C. (2003). Mpc fault-tolerant flight control case study : flight 1862. *In IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes 03*, pages 2317–2322, Washington D.C, USA. 1.1.3.2

Maciejowski, J. M. (2000). Fault-tolerant aspects of mpc. *In Proceedings of the IEEE Seminar on Practical Experiences with Predictive Control*. 1.1.3.2

Marcos, A., Balas, G. et Bokor (2005). Integrated fdi and control for transport aircraft. *AIAA Guidance, Navigation, and Control Conference*. 1.1.2.1

Martorell, S., Sanchez, A. et V.Serradell (1999). Age-dependent reliability model considering effects of maintenance and working conditions. *Reliability Engineering and System Safety*, 64:19–31. 2.3.1, 3.3.1

Maybeck, P. (1999). Multiple model adaptive algorithms for detecting and compensating sensor and actuator/surface failures in aircraft flight control systems. *International Journal of Robust and Nonlinear Control*, 9:1051–1070. 1.1.3.2

Mehra, R. K. et Peshon, L. (1971). An innovation appraoch to fault detection and diagnosis systems. *Automatica*, 7:637–640. 1.1.3.1

Merdic, E. (2004). *Thruster fault diagnosis and accomodation for overactuated open-frame underwater vehicles*. Thèse de doctorat, Mechatronics Research Centre-University of Wales College, Newport. 3.1

Moore, B. (1981). Principal component analysis in linear systems : controllability observability and momdel reduction. *IEEE Transactions on Automatic control*, 26:17–32. 2.4, 2.2.2, 2.8, 2.3.4, 2.3.4

Morse, W. D. et Ossman, K. A. (1990). Model following reconfigurable flight control systems of the $afti/f-16$. *Journal of Guidance, Dynamics and Control*, 13:969–976. 1.1.3.2

Narendra, K. S. et Balakrishnan, J. (1997). Adaptive control using multiple models. *IEEE Transactions on Automatic Control*, 42. 1.1.3.2

Niemann, H. et Stoustrup, J. (2003). Passive fault tolerant control of double inverted pendulum - a case study example. *In the 5th IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes 03*. 1.1.2.1

Niemann, H. et Stoustrup, J. (2005). Passive fault tolerant control of a double inverted pendulum-a case study. *Control Engineering practice*, 13:1047–1059. 1.1.2.1

Noura, H., Sauter, D., Hamelin, F. et Theilliol, D. (2000). Fault tolerant control in dynamic systems : Application to a winding machine. *IEEE Control system Magazine*, 20:33–49. 1.1.3.2, 4.5, 4.5

Noura, H., Theilliol, D., Ponsart, J. et Chamssedine, A. (2009). *Fault tolerant control systems : Design and practical application*. Springer Dordrecht Heidelberg London. 3.1, 4.1

Padgett, W. et Spurrier, J. (1985). Discrete failure model. *IEEE Transactions on Reliability*, 3:253–256. 4.8

Pagés, A. et Gondran, M. (1980). *Fiabilité des systèmes*. Editions Eyrolles. 1.2.1

Patton, R. (1997). Fault-tolerant control ; the 1997 situation. *IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes 97*, pages 1033–1055. 1.1.2.1

Patton, R. J., Frank, P. et Clark, R. (2000). *Issues of fault diagnosis for dynamic systems*. Springer, London. 1.1.3.1

Sakar, N., Podder, T. et Antonelli, G. (2002). Fault accomodation thruster force allocation of an auv considering thruster redundancy and saturation. *IEEE Transactions on Robotics and Automation*, 18:526–531. 3.1

Sauter, D., Hamelin, F., Noura, H. et Theilliol, D. (2002). Fault tolerant control in dynamic systems. *In Proceedings of 15th IFAC World Congress*, Barcelona, Spain. 3.5

Staroswiecki, M. (2002). On reconfigurability with respect to actuator failures. *15th Terminal word congress of IFAC2002*. Barcelona, Spain. 2.2.2, 2.2.2, 2.2.3, 2.2.3, 2.4, 2.3.4

Staroswiecki, M. (2003). Actuator faults and the linear quadratic control problem. *Proceedings of the 42nd IEEE Conference on Decision and control*. Maui, Hawwaii, USA. 2.2

Staroswiecki, M. (2005a). Fault tolerant control : The pseudo-inverse method revisited. *Proceedings of the 16th Triennal IFAC World Congress*. 1.1.3.2, 1.1.3.2, 4.2

Staroswiecki, M. (2005b). Fault tolerant control using an admissible model matching approach. *Proceeding of IEEE Conference on Decision and Control and the European Control Conference*. 1.1.3.2

Staroswiecki, M. et Berdjag, D. (2010). A general fault tolerant linear quadratic control strategy under actuator outages. *International Journal of Systems Science*, 41(8):971–985. 1.3.3, 4.1

Staroswiecki, M. et Hoblos, G. (2004). Sensor network design for fault tolerant estimation. *In. J. Adapt. Control Signal Precess*, 18:55–72. 1.3.3, 4.1

Stroustrup, J. et Niemann, H. (2002). Fault estimation- a standard problem approach. *International Journal of Robust and Nonlinear Control*, 12:649–673. 1.1.3.1

Suyama, K. (2002). What is reliable control. *In proceedings of the 15th Triennal IFAC World Congress*. 1.1.2.1

Theilliol, D., Sauter, D. et Ponsart, J. (1998). Fault tolerant control method for actuator and component faults. *Proceedings of IEEE Conference on Decesion and Control, CDC'98*. 1.1.3.2

Theilliol, D., Sauter, D. et Ponsart, J. (2003). A multiple model base approach for fault tolerant control in nonlinear systems. *IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes 2003*, pages 151–156. 1.1.3.2

Tornil-Sin, S., Theilliol, D., Ponsart, J. et Puig, V. (2009). Admissible model matching using d_r-regions : fault accomodation and robustness against fdd inaccuracies. *International Journal of Adaptive Control and Signal Processing*, 24(11):927–943. 4.1, 4.4, 4.4.2, 4.1

Toscano, R. et Lyonnet, P. (2008). On-line reliability prediction via dynamic failure rate model. *IEEE Transactions On Reliability*, 57:452–457. 2.3.1, 3.3.2

Tsui, C. (1999). A design example with eigenstructure assignment control whose loop transfer is fully realized. *Journal of Franklin Institute*, 336:1049–1053. 1.1.3.2

Veillete, R. (2002). Design of reliable control systems. *IEEE Transactions on Automatic Control*, 37:290–304. 1.1.2.1

Villemeur, A. (1997). *Sûreté de fonctionnement des systèmes industriels : fiabilité, facteurs humains, informatisation*. Editions Eyrolles. 1.2.1

Virnig, J. et Bodden, D. (1994). Multivariable control allocation and control law conditioning when control effectors limits. *AIAA Guidance, Navigation, and Control Conference*, pages 572–582. 3.4.2

Wang, A. P. et Lin, S. (1999). The parametric solutions of eigenstructure assignement for controllable and uncontrollable singular systems. *Journal of Mathematical Analysis and Applications*, 248:549–571. 1.1.3.2

Wicks, M. et Decarlo, R. (1990). Gramian assignment based on the lyapunov equation. *IEEE Transactions on Automatic Control*, 35(4):465–468. 2.2.2

Wu, E. (2001a). Reliability and fault tolerant control system part i. *In IEEE Conference on Decision and Control*, pages 1460–1465, Orlando, Florida, USA. 4.1

Wu, E. (2001b). Reliability and fault tolerant control system part ii. *In IEEE Conference on Decision and control*, pages 1466–1471, Orlando, Florida, USA. 4.1

Wu, E. et Patton, R. J. (2003). Reliability and supervisory control. *In 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes'03*, pages 139–144, Washington DC USA. 4.1

Wu, N. (2002). Reliability analysis for afti-f16 srfcs using assist and sure1. *Proceedings of American control conference, ACC'02*. 1.3.2

Wu, N., Wang, X., Sampath, M. et Kott, G. (2002). An operational approach to budget constrained reliability allocation. 15*th IFAC World Cogresse*. 1.3.2

Wu, N., Zhou, K. et Salmon, G. (2000). Control reconfigurability of linear time-invariant systems. *Automatica*, 36(11):1767–1771. 2.3.4, 2.9, 2.3.4, 2.4

Yang, Z., Izadi-Zamanabadi, R. et Blanke, M. (2000). On-line multiple model based adaptive control reconfiguration for a class of nonlinear control systems. *Proceedings of IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes'2000*, pages 745–750. 1.1.3.2

Ye, D. et Yang, G. H. (2006). Adaptive fault-tolerant tracking control against actuator faults with application to flight control. *IEEE Transactions on Control Systems Technology*, 14(6):1088–1096. 1.1.3.2, 4.5, 4.6, 4.1, 4.7

Zhang, Y. et Jiang, J. (1999a). Design on integrated fault detection, diagnosis and reconfigurable control systems. *Proceedings of the* 38*th IEEE Conference on decision and control, IEEE CDC'99*. 1.1.3.2, 1.1.3.2

Zhang, Y. et Jiang, J. (1999b). An interacting multiple-model based fault detection, diagnosis and fault-tolerant control approach. *Proceedings of the* 38*th IEEE Conference on Decision and Control, IEEE CDC'99*. 1.1.3.2

Zhang, Y. et Jiang, J. (2000). Design of proportional integral reconfigurable control systems via eigenstructure assignement. *Proceedings of the American Control Conference, ACC'00*. 1.1.3.2, 1.1.3.2

Zhang, Y. et Jiang, J. (2001). Active fault tolerant control using imm approach. *IEEE Transactions on Aerospace and Electronic systems*, 37:1221–1235. 1.1.3.2

Zhang, Y. et Jiang, J. (2002a). Active fault-tolerant control system against actuator failures. *In IEEE Proceedings Control Theory Applications*, volume 149, pages 95–104. 1.3.1

Zhang, Y. et Jiang, J. (2002b). Design of restructurable active fault-tolerant control systems. *In Proceedings of IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes'2003*, Barcelona, Spain. 1.1.3.2, 4.2

Zhang, Y. et Jiang, J. (2003). Fault tolerance control system design with explicit consideration of performance degradation. *IEEE Transactions on Aerospace and Electronic Systems*, 39(3):838–848. 1.3.1, 2.2, 4.1

Zhang, Y. et Jiang, J. (2008). Bibliographical review on reconfigurable tolerant-control system. *Annual Reviews in Control*, 32:229–252. 1.1, 1.1.2.2, 1.3.1, 3.1, 4.1

Zhao, Q. et Jiang, J. (1998). Reliable state feedback control system design against actuator failures. *Automotica*, 34:1267–1998. 1.1.2.1, 1.3.1

Zhou, K. (2000). A new controller architecture for high performance, robust and fault tolerant control. *In proceedings of the 39th IEEE Conference on Decision and Control*. 1.1.2.1

Zolghadri, A. (1996). An algorithm for real-time failure detection in kalman filter. *IEEE Transactions on Automatic Control*, 41:1537–1539. 1.1.3.1

Résumé

Les travaux développés dans ce mémoire de thèse portent sur la contribution à une méthodologie de synthèse de lois de commande tolérante aux fautes garantissant la fiabilité des systèmes. Cette nouvelle méthodologie nécessite l'adaptation des différents outils de caractérisation de la fiabilité avec la théorie de la commande. L'intégration explicite de l'aspect charge dans les lois modélisant la fiabilité en ligne est considérée. Une première partie des travaux est consacrée à la reconfigurabilité des systèmes tolérants aux fautes. Une analyse de reconfigurabilité en présence de défauts basée sur la consommation d'énergie ainsi que des objectifs liés à la fiabilité globale du système sont proposés. Un indice de reconfigurabilité est proposé définissant les limites fonctionnelles d'un système commandé en ligne en fonction de la sévérité des défauts et de la dégradation des actionneurs en terme de fiabilité. Dans la deuxième partie, le problème d'allocation et ré-allocation de la commande est considéré. Des solutions sont développées tenant compte de l'état de dégradation et du vieillissement des actionneurs. Les entrées de commande sont attribuées au système en tenant compte de la fiabilité des actionneurs ainsi que les éventuels défauts. Des indicateurs de fiabilité sont proposés et intégrés dans la solution du problème d'allocation et ré-allocation de la commande. La dernière partie est entièrement consacrée à la synthèse d'une loi de commande tolérante aux fautes garantissant la fiabilité globale du système. Une procédure d'analyse de fiabilité des systèmes commandés en ligne est proposée en se basant sur une étude de sensibilité et de criticité des actionneurs. Ainsi, une méthode de commande tolérante aux fautes en tenant compte de la criticité des actionneurs est synthétisée sous une formulation LMI.

Mots-clés : Commande tolérante aux fautes, Allocation et Rè-allocation de la commande, Sûreté de fonctionnement, Fiabilité, Défauts actionneurs.

Abstract

The works developed in this thesis deal with the active fault tolerant control design incorporating actuators reliability. This new methodology requires the adaptation of the reliability analysis tools with the system control field. The explicit integration of load in the actuators reliability models is considered. First, the reconfigurability analysis of fault tolerant control systems is treated. A reliable reconfigurability analysis based on the energy consumption with respect to overall system reliability is presented. A reconfigurability index which defines the functional limitation of the system is proposed based on fault severity and actuators reliability degradation. The second part of the developed works is devoted to control allocation and re-allocation. Two approaches of control re-allocation are proposed by taking into consideration actuator degradation health. The control inputs are applied to the system with respect to actuators reliability and faults. The third part contributes to a fault tolerant controller design incorporating actuator criticality. A sensitivity analysis of the overall system reliability and criticality indicator are proposed. A new method of active fault tolerant control is developed with Linear Matrix Inequality (LMI) formulation based on actuator criticality.

Keywords : Fault tolerant control, Control allocation and reallocation, Dependability, Reliability, Actuators faults,