Institut Supérieur de l'Aéronautique et de l'Espace - TOULOUSE

ÉCOLE DOCTORALE MITT
MATHEMATIQUES INFORMATIQUE TELECOMMUNICATIONS de TOULOUSE

T H È S E

pour obtenir le titre de

Docteur en Sciences

de l'ISAÉ - Toulouse
Mention : Informatique

Présentée et soutenue par

Florian MANY

Combinaison des aspects sûreté de fonctionnement et temps réel pour la conception de plateformes avioniques

Thèse dirigée par David Doose

préparée à l'Office National des Études et Recherches Aérospatiales (ONERA)

soutenue le

Jury :

Rapporteurs :	-
	-
Directeur :	-
Président :	-
Examinateurs :	-
	-
	-
Invité :	-

Table des matières

I Introduction **1**

1 Introduction **3**

2 Contexte **5**
2.1 Systèmes critiques embarqués 5
2.1.1 Systèmes critiques 5
2.1.2 Systèmes embarqués 5
2.2 Une étude pluridisciplinaire 5
2.2.1 Problématique de l'approche multipoints de vue 5
2.2.2 Traitement des intéractions entre les vues 5

3 État de l'art **7**
3.1 Ordonnancement temps réel 7
3.2 Sûreté de fonctionnement 7

II Contribution **9**

4 Modéliser un environnement agressif **11**
4.1 Introduction 11
4.2 État de l'art 11
4.2.1 Des fautes aux erreurs 11
4.2.2 Modèle de fautes pseudo-périodiques 11
4.2.3 Approche par motifs de fautes 11
4.2.4 Commentaires 11
4.3 Rafales de fautes 11
4.3.1 Définition 11
4.3.2 Illustration 11

5 Se protéger des fautes et gérer les erreurs **13**
5.1 Introduction 13
5.2 État de l'art 13
5.2.1 Tolérer les fautes 13
5.2.2 Redondances spatiales et temporelles 13
5.2.3 Protections logicielles 13
5.3 Recouvrement des erreurs 13
5.3.1 Tactiques de recouvrement d'erreurs 13
5.3.2 Stratégies de recouvrement d'erreurs 13
5.3.3 Exemples de stratégie 13

6 Intégrer la tolérance aux fautes aux études d'ordonnancement 15
6.1 Introduction . . . 16
6.2 État de l'art . . . 16
6.2.1 Ordonnancement tolérant aux fautes . . . 16
6.2.2 Résilience aux fautes . . . 16
6.3 Équation de temps de réponse sous rafales de fautes . . . 16
6.3.1 Une équation conservative . . . 16
6.3.2 Evaluation de l'impact des stratégies de recouvrement . . . 16
6.4 Un premier bilan . . . 16
6.4.1 Un exemple . . . 16
6.4.2 une intuition . . . 16
6.5 Cas particulier des ordonnancements partitionnés . . . 16
6.5.1 Ordonnancement multi-niveaux . . . 16
6.5.2 Adaptation de l'équation . . . 16
6.6 Simulation . . . 16
6.6.1 TEARS . . . 16
6.6.2 Protocole de simulation . . . 16
6.6.3 Résultats . . . 16
6.6.4 Commentaires . . . 16
6.7 Evaluation de la résilience aux fautes . . . 16
6.7.1 Intérêt de la résilience aux fautes . . . 16
6.7.2 Evaluation pour des fautes pseudo-périodiques . . . 16
6.7.3 Evaluation pour des rafales de fautes . . . 16
6.7.4 Exemple . . . 16

7 Combiner les aspects sûreté de fonctionnement et temps réel 17
7.1 Introduction . . . 18
7.2 Propagation de fautes . . . 18
7.2.1 État de l'art . . . 18
7.2.2 Sensibilité d'un équipement à une perturbation . . . 18
7.2.3 Propagation des fautes . . . 18
7.3 Analyse de l'impact de la sûreté de fonctionnement sur l'ordonnancement temps réel . . . 18
7.3.1 Perturbation subie et perturbation ressentie par le système . . . 18
7.3.2 Méthodologie d'analyse . . . 18
7.3.3 Exemple . . . 18
7.4 Analyse de l'impact de l'ordonnancement temps réel sur la sûreté de fonctionnement . . . 18
7.4.1 La question de l'isolement . . . 18
7.4.2 Mise en oeuvre du partitionnement . . . 18

III Conclusion **19**

8 Bilan des travaux **21**

9 Discussion **23**
9.1 Conception et réalité des analyses combinées 23
9.2 Application au cas particulier de l'aéronautique 23
9.2.1 Aéronefs avec pilote(s) 23
9.2.2 Aéronefs sans pilote 23

10 Perspectives **25**

Première partie

Introduction

Chapitre 1

Introduction

Chapitre 2

Contexte

Sommaire

2.1 Systèmes critiques embarqués 5
2.1.1 Systèmes critiques 5
2.1.2 Systèmes embarqués 5
2.2 Une étude pluridisciplinaire 5
2.2.1 Problématique de l'approche multipoints de vue 5
2.2.2 Traitement des intéractions entre les vues 5

2.1 Systèmes critiques embarqués

2.1.1 Systèmes critiques

2.1.2 Systèmes embarqués

2.2 Une étude pluridisciplinaire

2.2.1 Problématique de l'approche multipoints de vue

2.2.2 Traitement des intéractions entre les vues

Chapitre 3

État de l'art

Sommaire

3.1 Ordonnancement temps réel 7
3.2 Sûreté de fonctionnement 7

3.1 Ordonnancement temps réel

3.2 Sûreté de fonctionnement

Deuxième partie

Contribution

Chapitre 4

Modéliser un environnement agressif

Sommaire

4.1 Introduction 11
4.2 État de l'art 11
4.2.1 Des fautes aux erreurs 11
4.2.2 Modèle de fautes pseudo-périodiques 11
4.2.3 Approche par motifs de fautes 11
4.2.4 Commentaires 11
4.3 Rafales de fautes 11
4.3.1 Définition 11
4.3.2 Illustration 11

4.1 Introduction

4.2 État de l'art

4.2.1 Des fautes aux erreurs

4.2.2 Modèle de fautes pseudo-périodiques

4.2.3 Approche par motifs de fautes

4.2.4 Commentaires

4.3 Rafales de fautes

4.3.1 Définition

4.3.2 Illustration

Chapitre 5

Se protéger des fautes et gérer les erreurs

Sommaire

5.1 Introduction 13
5.2 État de l'art 13
5.2.1 Tolérer les fautes 13
5.2.2 Redondances spatiales et temporelles 13
5.2.3 Protections logicielles 13
5.3 Recouvrement des erreurs 13
5.3.1 Tactiques de recouvrement d'erreurs 13
5.3.2 Stratégies de recouvrement d'erreurs 13
5.3.3 Exemples de stratégie 13

5.1 Introduction

5.2 État de l'art

5.2.1 Tolérer les fautes

5.2.2 Redondances spatiales et temporelles

5.2.3 Protections logicielles

5.3 Recouvrement des erreurs

5.3.1 Tactiques de recouvrement d'erreurs

5.3.2 Stratégies de recouvrement d'erreurs

5.3.3 Exemples de stratégie

Chapitre 6

Intégrer la tolérance aux fautes aux études d'ordonnancement

Sommaire

6.1 Introduction 16
6.2 État de l'art 16
6.2.1 Ordonnancement tolérant aux fautes 16
6.2.2 Résilience aux fautes 16
6.3 Équation de temps de réponse sous rafales de fautes 16
6.3.1 Une équation conservative 16
6.3.2 Evaluation de l'impact des stratégies de recouvrement 16
6.4 Un premier bilan 16
6.4.1 Un exemple 16
6.4.2 une intuition 16
6.5 Cas particulier des ordonnancements partitionnés 16
6.5.1 Ordonnancement multi-niveaux 16
6.5.2 Adaptation de l'équation 16
6.6 Simulation 16
6.6.1 TEARS 16
6.6.2 Protocole de simulation 16
6.6.3 Résultats 16
6.6.4 Commentaires 16
6.7 Evaluation de la résilience aux fautes 16
6.7.1 Intérêt de la résilience aux fautes 16
6.7.2 Evaluation pour des fautes pseudo-périodiques 16
6.7.3 Evaluation pour des rafales de fautes 16
6.7.4 Exemple 16

6.1 Introduction

6.2 État de l'art

6.2.1 Ordonnancement tolérant aux fautes

6.2.2 Résilience aux fautes

6.3 Équation de temps de réponse sous rafales de fautes

6.3.1 Une équation conservative

6.3.2 Evaluation de l'impact des stratégies de recouvrement

6.4 Un premier bilan

6.4.1 Un exemple

6.4.2 une intuition

6.5 Cas particulier des ordonnancements partitionnés

6.5.1 Ordonnancement multi-niveaux

6.5.2 Adaptation de l'équation

6.6 Simulation

6.6.1 TEARS

6.6.2 Protocole de simulation

6.6.3 Résultats

6.6.4 Commentaires

6.7 Evaluation de la résilience aux fautes

6.7.1 Intérêt de la résilience aux fautes

6.7.2 Evaluation pour des fautes pseudo-périodiques

6.7.3 Evaluation pour des rafales de fautes

6.7.4 Exemple

Chapitre 7

Combiner les aspects sûreté de fonctionnement et temps réel

Sommaire

7.1 Introduction 18

7.2 Propagation de fautes 18

7.2.1 État de l'art 18

7.2.2 Sensibilité d'un équipement à une perturbation 18

7.2.3 Propagation des fautes 18

7.3 Analyse de l'impact de la sûreté de fonctionnement sur l'ordonnancement temps réel 18

7.3.1 Perturbation subie et perturbation ressentie par le système . 18

7.3.2 Méthodologie d'analyse 18

7.3.3 Exemple 18

7.4 Analyse de l'impact de l'ordonnancement temps réel sur la sûreté de fonctionnement 18

7.4.1 La question de l'isolement 18

7.4.2 Mise en oeuvre du partitionnement 18

7.1 Introduction

7.2 Propagation de fautes

7.2.1 État de l'art

7.2.2 Sensibilité d'un équipement à une perturbation

7.2.3 Propagation des fautes

7.3 Analyse de l'impact de la sûreté de fonctionnement sur l'ordonnancement temps réel

7.3.1 Perturbation subie et perturbation ressentie par le système

7.3.2 Méthodologie d'analyse

7.3.3 Exemple

7.4 Analyse de l'impact de l'ordonnancement temps réel sur la sûreté de fonctionnement

7.4.1 La question de l'isolement

7.4.2 Mise en oeuvre du partitionnement

Troisième partie

Conclusion

Chapitre 8

Bilan des travaux

Chapitre 9

Discussion

Sommaire

9.1 Conception et réalité des analyses combinées 23
9.2 Application au cas particulier de l'aéronautique 23
9.2.1 Aéronefs avec pilote(s) 23
9.2.2 Aéronefs sans pilote 23

9.1 Conception et réalité des analyses combinées

9.2 Application au cas particulier de l'aéronautique

9.2.1 Aéronefs avec pilote(s)

9.2.2 Aéronefs sans pilote

Chapitre 10

Perspectives