

# Assistance à la conception de plateformes avioniques – combinaison des aspects temps réel et sûreté de fonctionnement

---

**Florian Many**

2ème Année

Thèse encadrée par Frédéric Boniol et David Doose (ONERA-DTIM)



---

27 Janvier 2010

# Introduction

## Contraintes d'un système temps réel

- Respect des échéances temporelles (**Ordonnement**)
- Tolérance aux fautes (**Sûreté de fonctionnement**)

## Tolérance aux fautes

- Redondance spatiale
  - Duplication et triplication d'équipements
- Redondance temporelle
  - Modèle de données robuste
  - Réexécution de code

## Problématique

- **Etude d'ordonnançabilité de systèmes TR tolérant aux fautes**

# Démarche appliquée

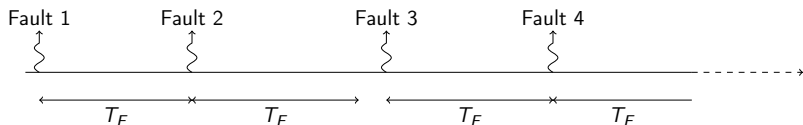
## Différentes études menées

- Modélisation de distribution de fautes
  - Phénomènes qui perturbent durablement un système temps réel
- Définition de stratégies
  - Comportement de l'odonnanceur à la détection d'une faute
  - Efficacité des stratégies par rapport à la "menace"
- Analyse d'ordonnançabilité

## Exemple de phénomène

- Passage dans un champ électromagnétique

# Distribution pseudo-périodique (1/2)



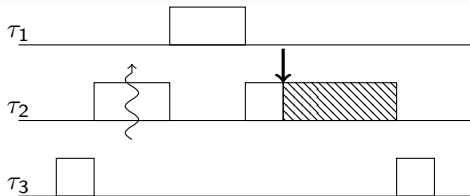
## Définition

- Fautes espacées par un intervalle de temps minimum  $T_F$

## Exemple

- Compatibilité électromagnétique alimentation et ordinateur

## Distribution pseudo-périodique (2/2)



### Calcul du pire temps de réponse $\Theta$

$$\Theta_i = C_i + I_i + F_i \quad (1)$$

- $C_i$  : WCET
- $I_i$  : Interférences dûes aux tâches de plus hautes priorités
- $F_i$  : Coût temporel dûes aux tactiques de correction

# Détection et correction des erreurs

## Mécanismes de détection

- Utilisation de tests d'acceptance
- Instant de détection :
  - A la fin de la tâche
  - A différents endroits de la tâche

## Méthode de correction

- La correction d'erreurs s'effectue par la réexécution de code :
  - Réexécution complète ou partielle de la tâche
- Hypothèse : les erreurs de la tâche sont intégralement corrigées.

# Stratégies face aux fautes

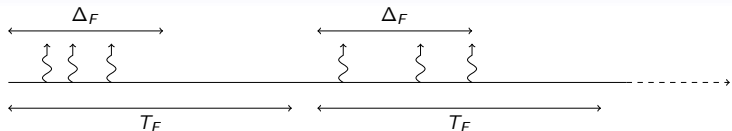
## Stratégies

- Comment : Correction des erreurs  $\Rightarrow$  Tolérance aux fautes
- Moyen : Utilisation de tactique = détection + correction
- **Stratégies** : Comportement vis à vis des tâches préemptées

## Exemples de stratégie

- End Detection/Full Reexecution/Simple (**ED/FR/S**)
  - correction de la tâche erronée
- End Detection/Full Reexecution/Multiple (**ED/FR/M**)
  - correction de la tâche erronée + tâches préemptées

# Distribution en rafale



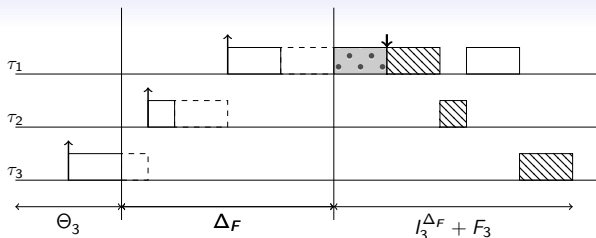
## Définition d'une rafale

- Intervalle de temps pendant lequel il y a potentiellement des fautes
- $\Delta_F$  = intervalle de temps de la perturbation
- $T_F$  = minimum entre deux débuts de rafale

## Propriété

- Pas de fautes hors rafales

# Analyse d'ordonnançabilité (1/2)



## Calcul du pire temps de réponse $\Theta^{\Delta_F}$

$$\Theta_i^{\Delta_F} = \Theta_i + \Delta_F + (I_i^{\Delta_F} + F_i) \quad (2)$$

- $\Theta_i$  : WCRT sans fautes
- $I_i^{\Delta_F}$  : Interférences après la fin de la rafale
- $\Delta_F$  : Durée de la rafale
- $F_i$  : Coût temporel dûes aux stratégies de correction

## Analyse d'ordonnançabilité (2/2)

### Calcul de $F_i$ pour ED/FR/S

$n$  détections,  $n$  corrections

$$F_i = 2 \times \sum_{hp(i)} C_j + 2 \times C_i \quad (3)$$

### Calcul de $F_i$ pour ED/FR/M

1 détection,  $n$  corrections

$$F_i = \sum_{j \in hp(i)} C_j + \max_{j \in hp(i)} C_j + C_i \quad (4)$$

$$F_i = \max_{j \in hp(i)} \left( C_j + \sum_{k=i-1}^{k=j} C_k \right) + C_i \quad (5)$$

# Conclusions et perspectives

## Bilan de la partie étude d'ordonnançabilité

- Distribution temporelle
  - Modèle de rafales de fautes
- Détection et correction des erreurs
  - Définition de stratégies
- Analyse d'ordonnancement

## Ajout de la partie sûreté de fonctionnement

- Intégrer les différents modes de défaillance
- Affiner les stratégies en couplant sdf et ordonnancement
- Valider simultanément sdf/ordonnancement

# Communication et formations

## Communications

- FAC 2009 (IRIT)
- Article en rédaction (conférence(s) à identifier)

## Formations

- Analysis, Observation and Control of Time Delay Systems
- EJCP 2009