RTNS: Scheduling Analysis under Fault Bursts

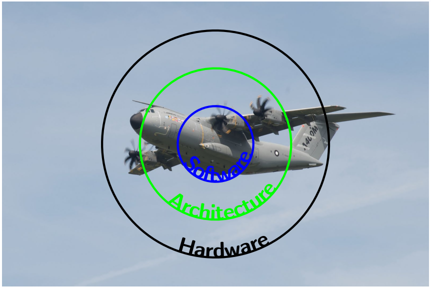
Florian Many, Frédéric Boniol, David Doose

DGA

ONERA
THE FRENCH AEROSPACE LAB

5 November 2010

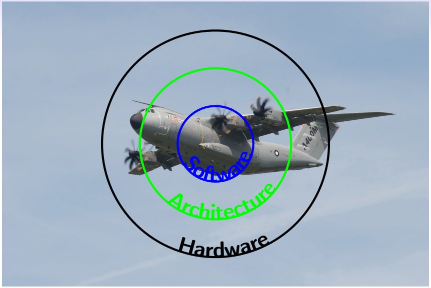
Context (1/3)



Different Layers of Protection

- Hardware Layer
- Architecture Layer
- Software Layer

Context (2/3)



Fault Tolerance Mechanisms

- Hardware Layer
  - Shield
  - Location
- Architecture Layer
  - Duplication et triplication of critical equipments
- Software Layer
  - Robust data model
  - Method based on code execution or re-execution

Context (3/3)

Real-Time System Overview

- A set of tasks with hard temporal constraints
- A scheduler to assign task to processors

Some Relevant Questions

- Assign priority to tasks
- Manage shared ressources
- Manage fault tolerance mechanisms

Schedulability Analysis

Prove *a priori* the respect of all temporal constraints

Plan of this Presentation

Problematic

Coupling Scheduling Analysis and Fault Tolerance

Guidelines

- Definition of a fault model
- Definition of the scheduler behaviour when an error occurs
- Schedulability Analysis

Fault Features

Origins of Faults

- Inner faults
  - Bad design or implementation
  - Electromagnetic Compatibility : Power supply and computer
- Environmental faults
  - Sensors masked by an outer object
  - Electromagnetic fields (radar waves), space rays

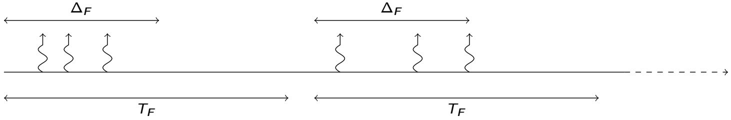
Consequences on Real-Time Systems

- Permanent $\Rightarrow$ Spatial Redundancy
- Transient $\Rightarrow$ Temporal Redundancy

Temporal Distributions

- Pseudo-periodic fault
- Fault bursts

Fault Burst Model



Burst Definition

- Δ_F = time interval during which there are potential faults
- Inner temporal distribution of faults unknown
- No fault outside a burst
- T_F = minimum time interval between two fault burst starts

Example of Phenomenon

- Aircraft through an electromagnetic field generated by radar waves

An Illustrated Example

Case of Rotative Air Radar [1, 2]

- For a fly-by or over ground aircraft :
  - Elapsed time between two swept : few seconds
  - Exposure time : tenth of seconds
- Worst case for a slow aircraft :
  - 15 swepts (2 seconds between swepts)
  - 100 ms of exposure time by swept

RTCA and EUROCAE
Guide to Certification Of Aircraft in a High Intensity Radiated Field (HIRF) Environment
ED 107 - ARP 5583, 2001.

RTCA and EUROCAE
Environmental Conditions and Testprocedures for Airborne Equipment
ED 14E - DO 160E, 2005.

Error-Detection and Error-Correction

Detection Mechanisms

- Use of acceptance tests, checksums, timer watchdogs etc...
- Instant of detection :
  - At the end of task
  - Checkpoints (splitted tasks)

Correction Method

- Re-execution of code
  - Full or partial re-execution of the erroneous task
  - Alternative tasks, recovery blocks
  - Exception Handlers
- Assumption : Re-execution of the task corrects all errors

Error Recovery Strategies

At Task Level

- **Tactic** = error-detection + error-correction

At System Level

- At error detection, different actions :
  - Manage preempted tasks
  - Anticipate potential undetected errors
- **Strategies**
  - Definition of scheduler behaviour towards preempted tasks

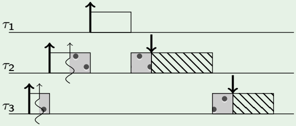
Remark

Error recovery strategies infer fault tolerance

Focused Error Recovery Strategies

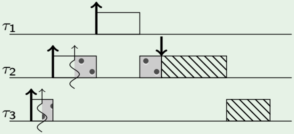
End Detection/Full Re-execution/Simple Strategy

- End Detection
- Full Re-execution of the faulty task
- Correction of the erroneous task
- Ex : Erronated data on a sensor

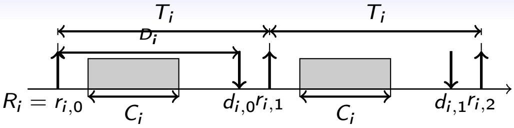


End Detection/Full Re-execution/Multiple Strategy

- End Detection
- Full Reexecution
- Correction ot the erroneous task
- Preventive correction of preempted tasks
- Ex : Corrupted shared data



Computational Model



Task Features

- WCET : C_i, Deadline : $D_{i,}$, Period : T_i
- Deadline less than or equal to period : $D_i \leq T_i$
- independent,periodic
- distinct priority

System Features

- uniprocessor
- fixed priority assignement
- fault free scheduler

Evaluation of Task Set Feasibility

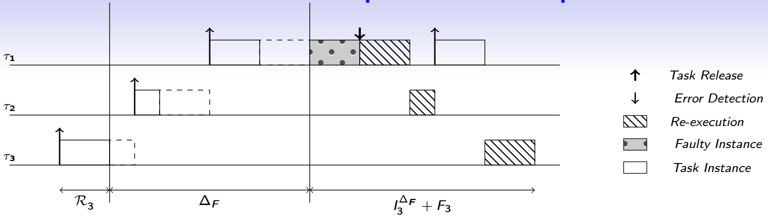
Validation Techniques

- Upper bound to the processor utilisation
- Worst Case Response Time
- Model Checking (multiprocessor)
- Workload

Worst Case Response Time

- (Completion time - release date) task in the worst case
- schedulable task $\tau_{\mathbf{i}}$: $WCRT \leq D_{\mathbf{i}}$
- task set feasible : $\forall i, \tau_{\mathbf{i}}$ *schedulable*

Worst Case Response Time Equation



Computation of the Worst Case Response Time $\mathcal{R}_i^{\Delta F}$

$$\mathcal{R}_i^{\Delta F} = \qquad \mathcal{R}_i^{\Delta F} = \mathcal{R}_i \qquad \mathcal{R}_i^{\Delta F} = \mathcal{R}_i + \Delta_F \qquad \mathcal{R}_i^{\Delta F} = \tag{1}$$

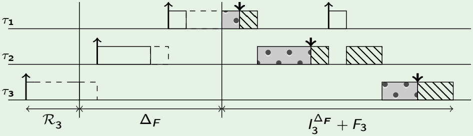
- $\mathcal{R}_i$: Free fault WCRT
- Δ_F : Duration of the fault burst
- Interference due to the highest priority tasks after the fb end

$$I_I^{\Delta F} = \sum_{hp(i)} \left\lceil \frac{\mathcal{R}_i^{\Delta F} - (\mathcal{R}_i + \Delta_F)}{T_j} \right\rceil C_j \tag{2}$$

- F_i : Additional temporal cost due to the error recovery strategies

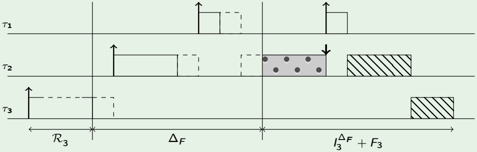
Evaluation of Recovery Term F_i

Computation of F_i for the ED/FR/S strategy



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

Computation of the F_i for the ED/FR/M Strategy



$$F_i = \max_{j \in hp(i)} \left(C_j + \sum_{k=i-1}^{k=j} C_k \right) + C_i \quad (4)$$

Example

$\Delta_F = 100$								
P	T	C	D	$\mathcal{R}$	S	$\mathcal{R}^{\Delta_F}$	M2	$\mathcal{R}^{\Delta_F}$
1	300	10	300	10	20	**130**	20	**130**
2	500	50	500	60	120	**290**	70	**240**
3	800	150	800	210	420	**800**	260	**630**

Descritpion

- 3-task set with $D_i = T_i$
- scheduler : Rate Monotonic

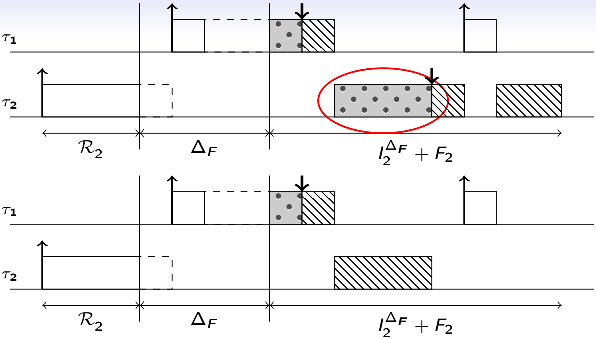
Benefits

- Efficiency of strategies : significative reduction of WCRT (25%)
- Unvailibility of the system : $T_F = 800$, $\Delta_F = 100 \Rightarrow 12,5\%$

First impression

- Multiple strategy better than simple

Simulation (1/2)



Qualitative explanation of the benefits

- "Temporal Economy" ⇒ reduction of necessary error-detections
- In practice, temporal additional cost (preventive re-executions)
- **But** effective approach for the validation of RTS

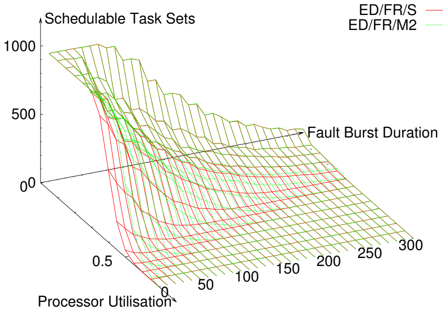
Simulation (2/2)

Description

- 10-task sets
- 1000 task sets for a given range of processor utilisation
- variation of the fault burst

Comparison of Strategies : U = 0.5 [1]

- Simple : $\Delta_F = 3\%$ of the longest period
- Multiple : $\Delta_F = 14\%$ of the l.p



M. Pandya and M. Malek
Minimum achievable utilization for fault-tolerant processing of periodic tasks
IEEE Transactions on Computers, 47(10) :1102–1112, 1998.

Conclusions

Conclusion

- A representative issue : UAVs in Radar waves (ONERA research)
- Results :
  - Fault Burst Model
  - Error recovery strategies
  - Schedulability Analysis
  - Realistic approach showed by simulation

Perspectives

- Implement strategies in a RTOS
- Works at system level $\Rightarrow$ entry points :
  - safety : equipment failure
  - platform features

Thanks for your attention