

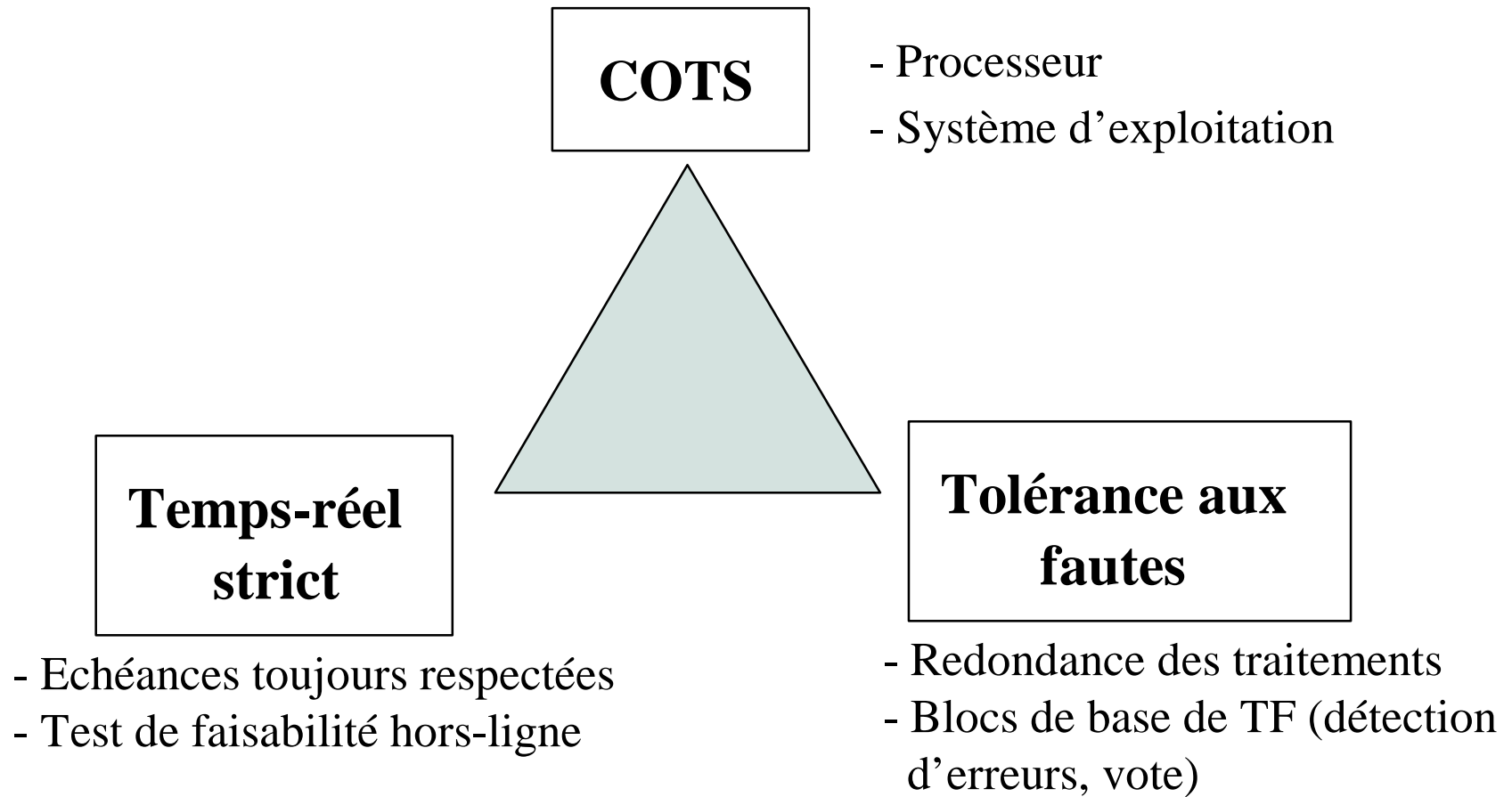
Utilisation de « COTS » pour la construction de systèmes distribués temps-réel strict à sûreté critique

Isabelle Puaut

INSA / IRISA - projet Solidor

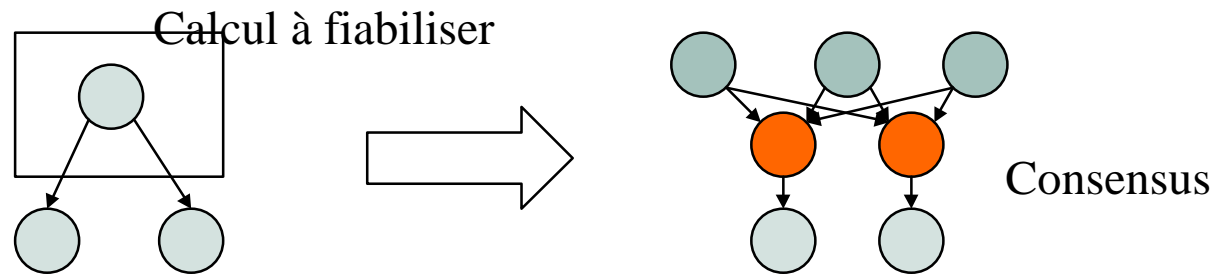
Coopération Inria/DGA/Dassault-Aviation

Problématique



Temps-réel - tolérance aux fautes

- Echéances strictes → doivent être connus avant exécution :
 - Structure des applications (DAG)
 - Redondance des applications pour tolérance aux fautes
- Réplication hors-ligne



→ Mécanisme **sélectif**

→ Intégration aisée dans tests de **faisabilité** [RTCSA99]

Temps-réel - tolérance aux fautes

- « COTS »

- Correction des tâches répliquées
 - Arrêt sur défaillance des processeurs, omissions réseau
- Validation des hypothèses sur « COTS » (travail en cours)
 - Couverture sans addition de détection d'erreurs
 - Mécanismes de détection d'erreurs additionnels
 - Assertions pour détection erreurs valuées et temporelles
 - Récupération des erreurs détectées par le matériel
 - Validation par injection de fautes

Temps-réel - « COTS »

Problématique (1/3)

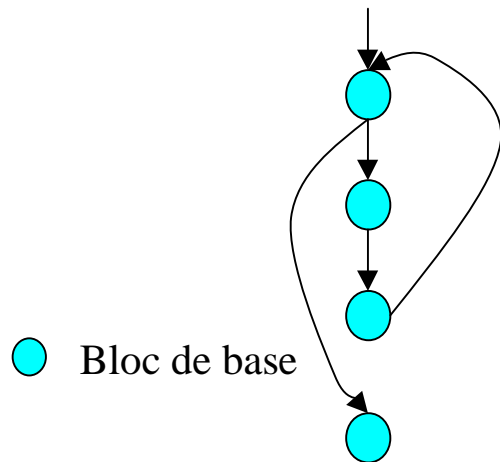
- Tests de faisabilité → temps d'exécution au pire cas (WCET) des programmes
- Méthodes courantes d'estimation des WCETs
 - Tests et mesures : problèmes :
 - | Exhiber le pire comportement de l'application
 - | Sûreté
- Obtention du temps d'exécution au pire cas par **analyse statique** du code source
 - sûre
 - automatique

Temps-réel - « COTS »

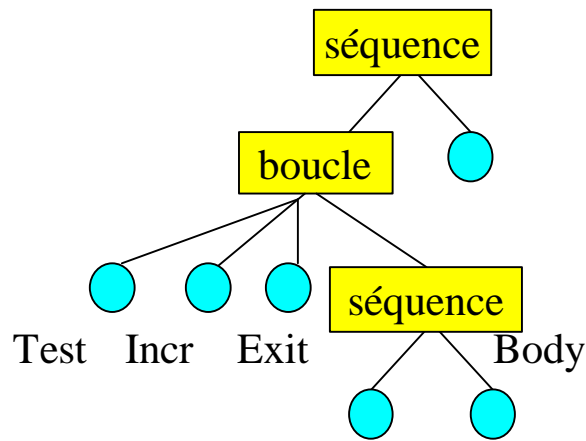
Problématique (2/3)

- Langage adapté à l'analyse
 - absence de récursivité et d'appels dynamiques
 - annotations de boucle
- Représentations du programme

Graphe de contrôle de flot



Arbre syntaxique



→ Calcul WCET pour chaque bloc de base

→ Calcul WCET global par réduction de l'arbre syntaxique

$$\begin{aligned} \text{WCET boucle} &= \text{WCET}(\text{Init}) \\ &+ (\text{WCET}(\text{Test}) + \text{WCET}(\text{Body})) * \\ &\text{maxiter} + \text{WCET}(\text{Test}) + \text{WCET}(\text{Exit}) \end{aligned}$$

Temps-réel - « COTS »

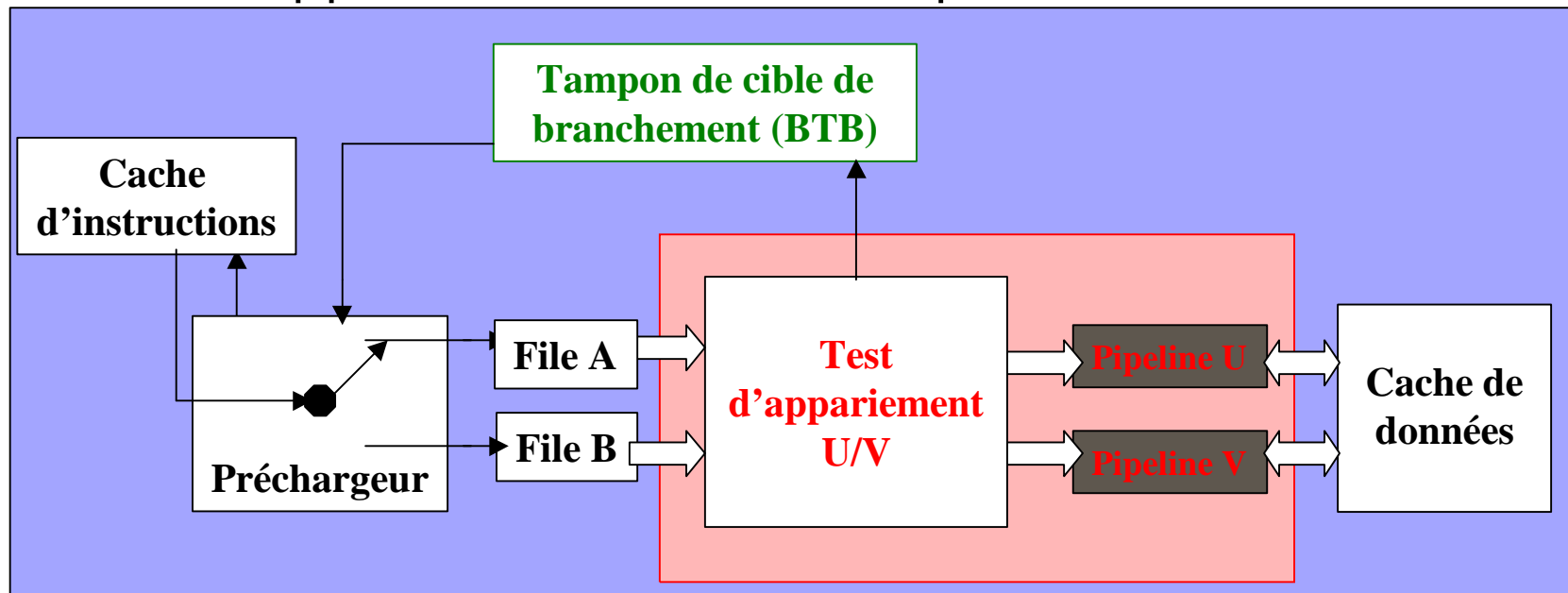
Problématique (3/3)

- Analyse de WCET sur éléments COTS : problématique
 - Matériel sur étagères :
 - | complexité des architectures actuelles des processeurs (caches, pipelines, prédiction de branchement)
 - Système d'exploitation sur étagères
 - | Disponibilité des sources du système
 - | identification du pire chemin d'exécution
- Problème général de l'analyse de WCET : identification du pire chemin d'exécution
 - Annotations de boucles adaptées aux boucles imbriquées [RTS99]

Temps-réel - « COTS »

Analyse matériel « COTS » (1/6)

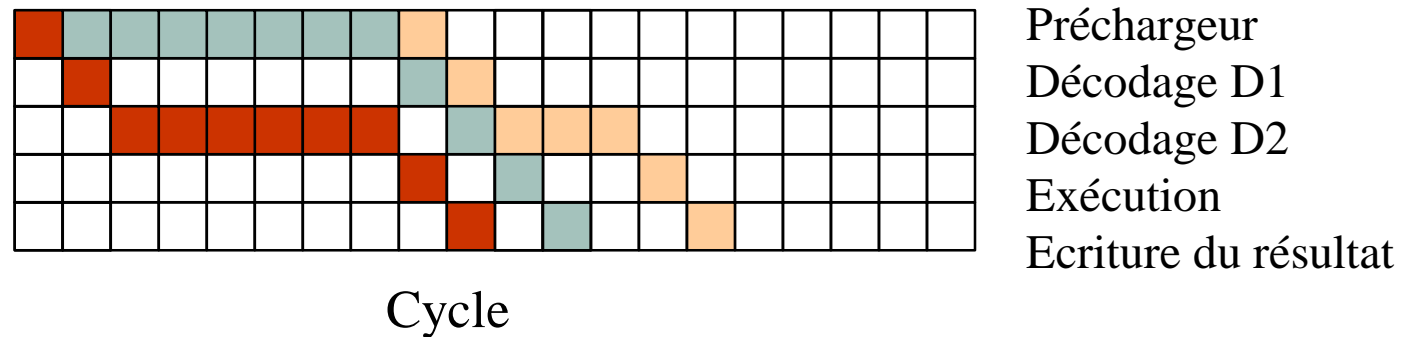
- **Cache d'instructions** : réduction temps de chargement
- **Pipeline double (U/V)** : exécution de 2 instructions/cycle
- **BTB** : suppression délais causés par les branchements



Temps-réel - « COTS »

Analyse matériel « COTS » (2/6)

- Pipeline double (U/V)
 - Simulation statique de l'état d'occupation des pipelines



- Simuler l'appariement des instructions

Temps-réel - « COTS »

Analyse matériel « COTS » (3/6)

- Cache d'instructions
 - Simulation statique du contenu du cache d'instructions à tout moment de l'exécution.
 - Classification des instructions
- Mécanisme de prédiction de branchement
 - BTB : Branch Target Buffer : enregistre l'historique des branchements (4 états)
 - Prédit si un branchement sera pris ou non lors de son exécution
 - Résultat : prédiction correcte ou erronée (délai en cas de mauvaise prédiction)

Temps-réel - « COTS »

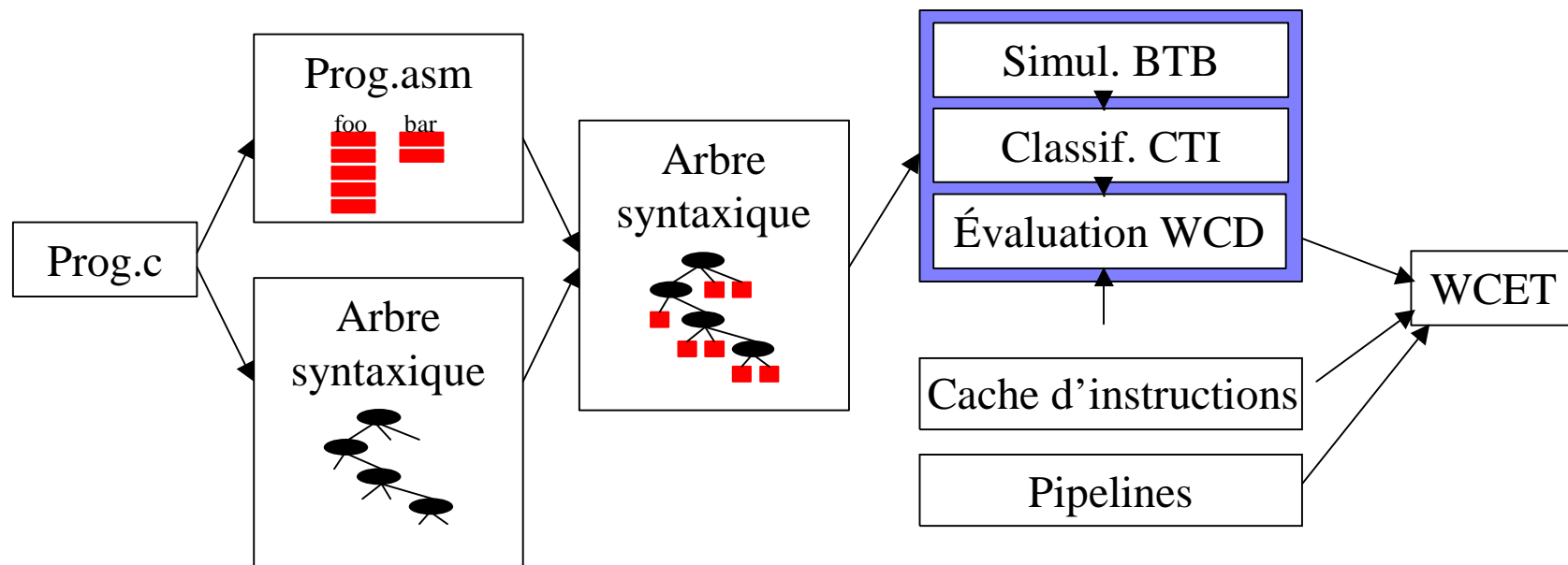
Analyse matériel « COTS » (4/6)

- Principe d'intégration de l'influence de la prédiction de branchement
 - Simulation statique du contenu du BTB
 - Classification des instructions de transfert de contrôle (dirigé par la syntaxe)
 - Calcul du surcoût à l'exécution d'après leur classification
 - Intégration au calcul de WCET

Temps-réel - « COTS »

Analyse matériel « COTS » (5/6)

- Heptane (Hades Embedded Processor Timing ANalyzEr)

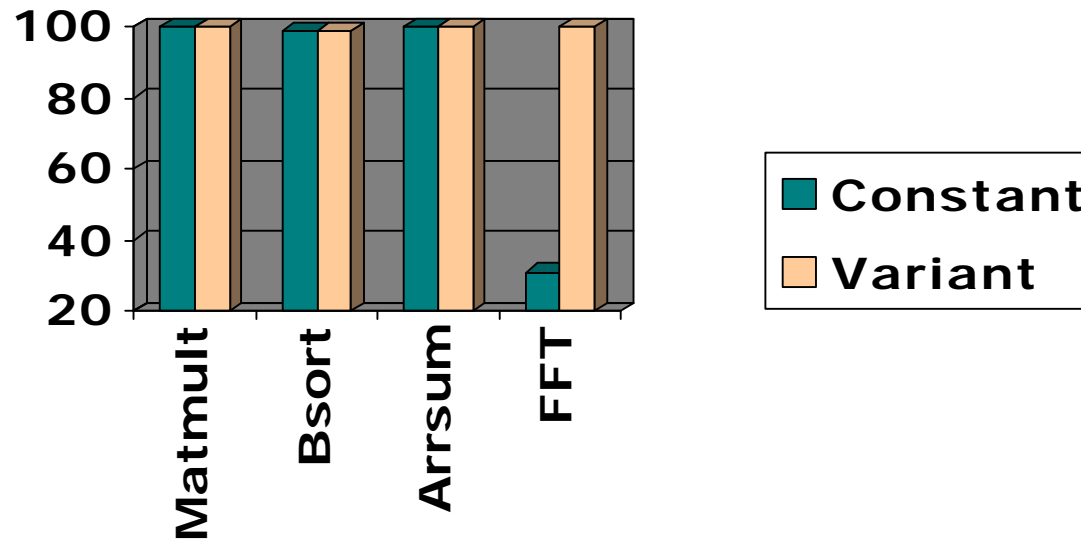


Temps-réel - « COTS »

Analyse matériel « COTS » (6/6)

- Résultats d 'analyse concernant la prédiction de branchement

Taux de prédictions correctes



Temps-réel - « COTS »

Analyse logiciel « COTS » (1/4)

- Analyse du noyau temps-réel RTEMS (Oar)
 - analyse de 12 directives (gestion de tâches, sémaphores)
 - 82 fichiers, 14000 lignes de code
 - Par directive RTEMS
 - en moyenne 38 fonctions dans son graphe d'appel
 - en moyenne 11 blocs de base par fonction

Temps-réel - « COTS »

Analyse logiciel « COTS » - (2/4)

■ Appels de fonctions

- Beaucoup d'appels externes, fort taux de réutilisation des fonctions → WCET partiel
- Appels dynamiques :
 - | peu nombreux
 - | fonction appelée toujours connue statiquement (sauf routines d'extension)
- Pas de récursivité

■ Code non structuré

- Fichiers assembleur : pas de problème (changement de contexte)
- Présence de *goto* : code restructurable

Temps-réel - « COTS »

Analyse logiciel « COTS » (3/4)

- Boucles (21 boucles seulement)
 - Pas d'imbrication de boucles
 - Boucles infinies : pas de problème (tâche *idle*)
 - Nombre maximal d'itérations
 - | Obtention directe : 25% des boucles
 - | Gestion des noms d'objets
 - | Allocation dynamique de mémoire (first-fit)
 - | Gestion de files d'attente
 - | Boucle de l'ordonnanceur

Temps-réel - « COTS »

Analyse logiciel « COTS » (4/4)

■ Conclusions

- RTEMS analysable par analyse statique du source
- Profil de code système :
 - | WCET partiel, multi-fichiers
- Nombre maximum d'itérations de boucles pas toujours trivial à déterminer
- Algorithmes non adaptés à l'analyse de WCET

■ Travaux futurs

- Evaluation du pessimisme de l'analyse
- Algorithmes adaptés à l'analyse de WCET

Pour plus d'informations

■ Publications

■ [RTCSA99]

P. Chevochot, I. Puaut, Scheduling Fault-Tolerant Distributed Hard Real-Time Tasks Independently of the Replication Strategies, Proc. of the 6th International Conference on Real-Time Computing Systems and Applications (RTCSA'99), Hong-Kong, China, december 1999.

■ [RTS99]

A. Colin, I. Puaut, Worst Case Execution Time Analysis for a Processor with Branch Prediction, Real-Time Systems, Special issue on worst-case execution time analysis, 1999.

■ Site Web

■ <http://www.irisa.fr/solidor/work/hades.html>

■ Mail : puaut@irisa.fr