

**A**

**TECHNICATOME**



# **Stratégie de choix d'un processeur pour applications embarquées safety-critical**

**20 novembre 2002 -- Atelier thématique du RIS**

# Les raisons d'une évolution

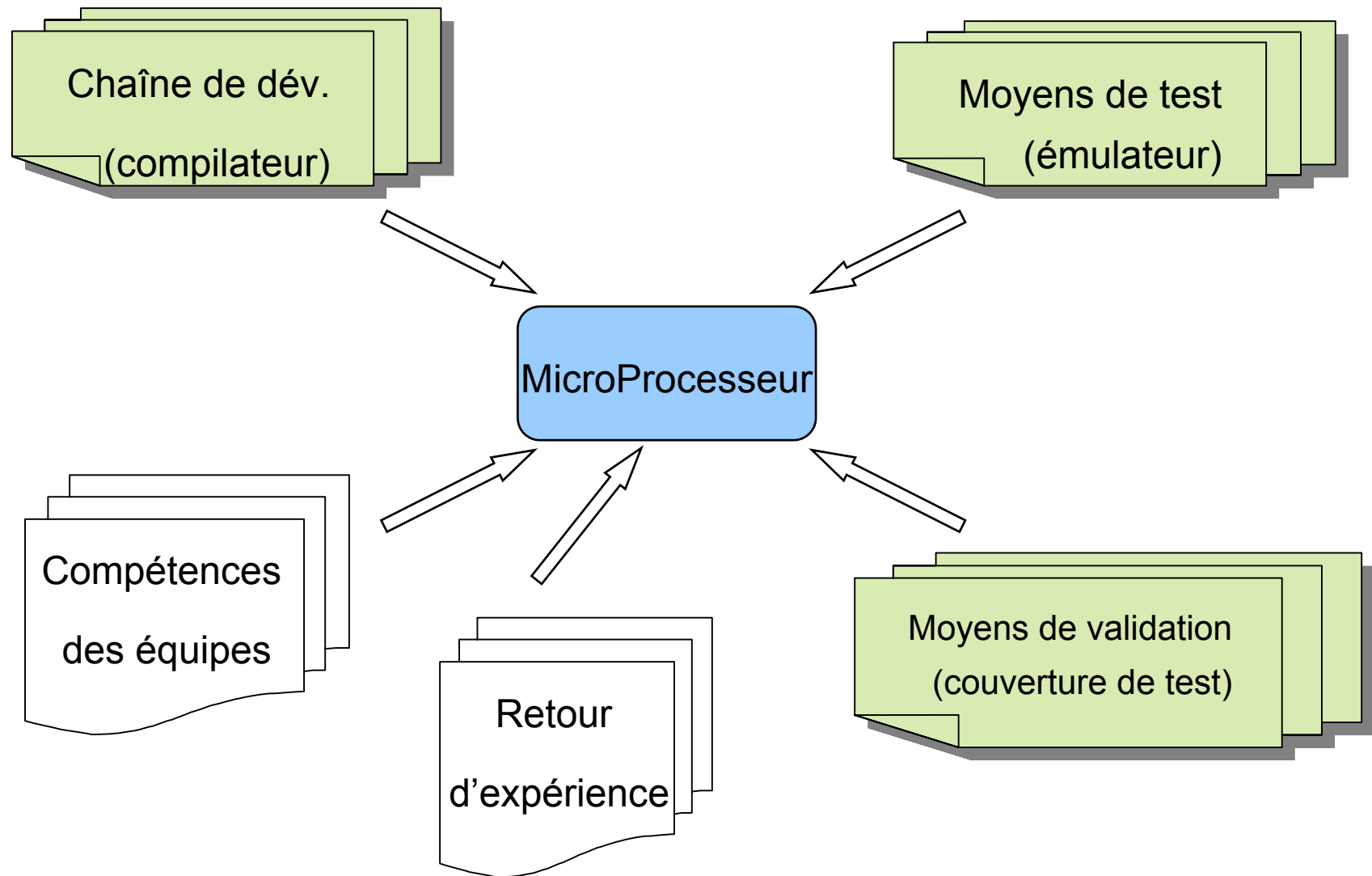
## ■ Installations à longue durée de vie

- 1ère génération (68000), marchés militaires : Mise en service en 1989 dernière mise en service de matériel neuf : 2003
- 2ième génération (68020), marchés militaires puis civils :
  - Mise en service en 1994
  - Reprise en 1998 pour adaptation d'E/S et optimisation
  - Encore dans notre offre en 2001
- 3ième génération (coldfire), marchés civils : mise en service 2002, dernière mise en service de matériel neuf : 2014

## ■ Obsolescences

- 1ière et 2ième générations : émulateurs en fin de vie
- Constat : Les moyens de test sont le point faible, (ensuite le composant lui-même et enfin la chaîne de développement logiciel).

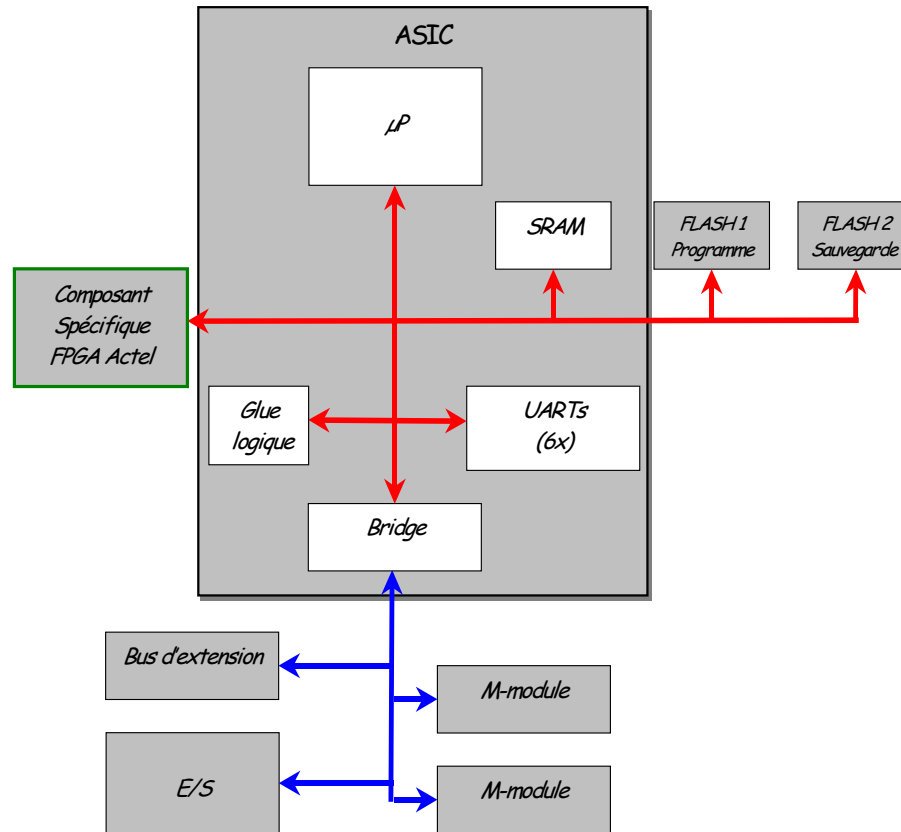
# Environnement d'une carte CPU



# Définition du besoin

- Objectif SIL4 / safety critical
  - Déterminisme (cache, optimisation interne)
  - Contraintes de ségrégation, de technologies
  - Complexité du processeur
- Durée de vie importante
  - Fabrication et modification HW de la carte : 13 ans
  - Modification SW : 25 ans
  - Durée de vie opérationnelle : 40 ans
- Développement < 12 mois, lancement fin 2001.
- Quantités prévisionnelles : 300 à 600 cartes par an pendant 10 ans
- Performances et E/S
  - Compatibilité avec génération précédente (obsolescence niveau fonction)
  - Monocarte embarquée, format double Europe 1 pas, 10 Watts
  - 2 réseaux de terrains, liaisons séries, 50 MIPS.

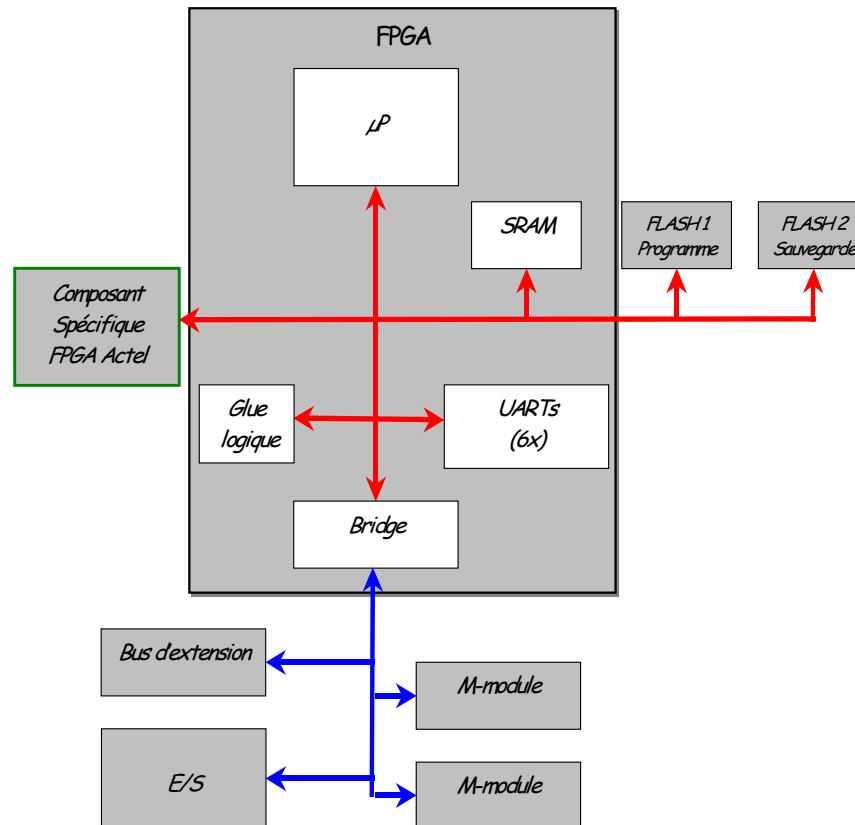
# Architecture à base d'un ASIC



- Faible quantité : Europractice
- Techno : imposée par ARM (IP HW)
- Licence ARM : qq centaines de keuro
- Validation du cœur : large diffusion
- Délais >>12 mois (délais run/techno)
- Cycle de vie : stabilisé
- Moyens de test limités
- Obsolescence : 6000 pièces minimum : stockage
- Peu adapté à de multiples projets dérivant une même carte (interfaces figées)

**Risques techniques et planning trop élevés**

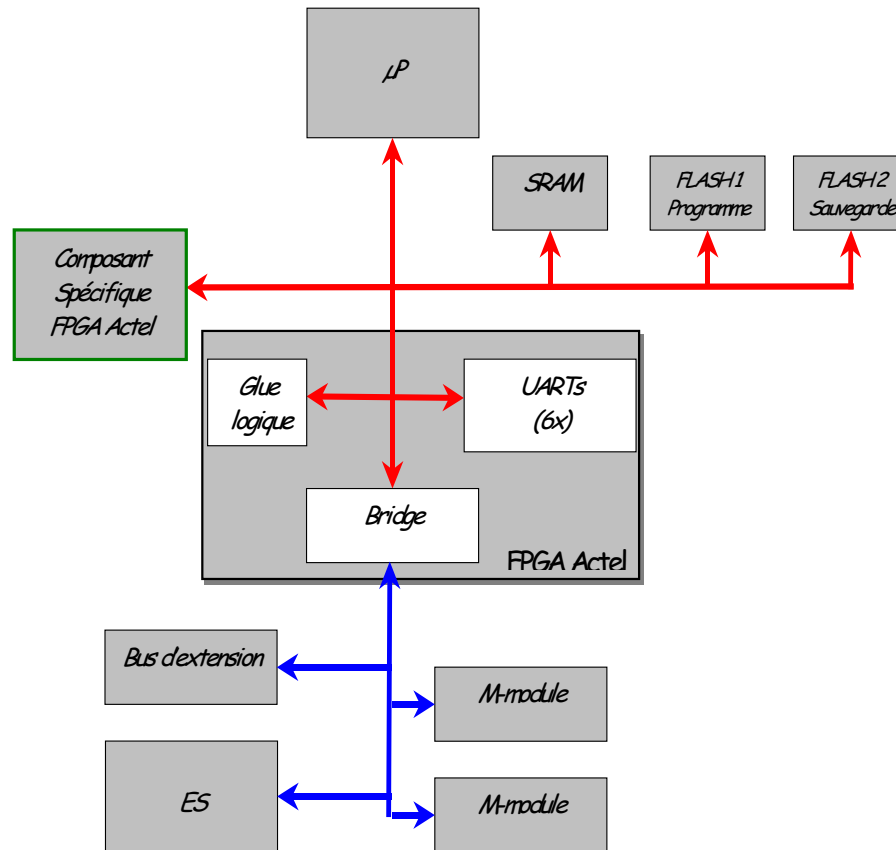
# Architecture à base de FPGA intégrant le $\mu P$



- Choix quasi imposé du  $\mu P$  (à la date du choix)
- Techno : Altera imposée par ARM (IP HW).
- Validation du cœur : peu diffusé sur cette techno
- IP SW non retenu (pb de validation)
- Délais <12 mois
- Cycle de vie : naissant
- Disponibilité des Moyens de test limitée dans le temps.
- Obsolescence : faible ou fort à long terme

**Technologie naissante, moyens de test limités**

# Architecture à base de composants discrets



- Large choix de µP possible
- Techno : large choix possible
- Validation du cœur : large diffusion
- Délais <12 mois
- Cycle de vie : stabilisé
- Moyens de test : tierce partie
- Obsolescence : risque moyen  
(risque = disparition famille)

**Interfaces ouvertes, choix sécurisant**

# Architecture à base de composants discrets

## ■ Processeurs envisagés

- MIPS32K, ARM disponible plutôt sous forme de cœur
- HITACHI SH4/SH7 : intégration des mémoires ram et flash. Pour Gros Volume (400 pièces = lot d'évaluation)
- Processeur de communication (powerQUICCII...)
- PowerPC 555 : intégration des mémoires ram et flash. Pour Gros Volume
- PowerPC 603e: la seule alternative viable au Coldfire.

## ■ PowerPC 603e

- Largement utilisé dans le militaire (carte COTS VME...)
- Mais :
  - Ratio Complexité/prestation important
  - Évolution constante (1 masque # 18 mois)
  - Processeur non connu par les équipes TECHNICATOME.

# Les raisons du choix Coldfire 5307

## ■ Contraintes projets

- Coldfire 5307 en début de cycle de vie
- 3 fournisseurs de moyens de test complets (point moins critique car ressource de débbug type BDM intégrée utilisable pour les modif SW à long terme)
- Traitement d'obsolescence : par un autre  $\mu$ P de la famille coldfire (pas de 2ième source, pas de  $\mu$ P équivalent actuellement)

## ■ Contraintes de Sûreté de fonctionnement

- Au final intégration encore moins poussée à cause des besoins de ségrégation pour la sécurité



# Conclusion

---

- La reprise de la carte a permis
  - Une optimisation des coûts
  - De prévenir les obsolescences
- Reste à faire
  - Validation complète de la carte
  - Analyse de SdF complète
  - Certification
- Perspectives
  - Bloc IP, disponibilité à moyen terme de processeurs dédiés sécurité ?
  - Difficulté de validation associée ?