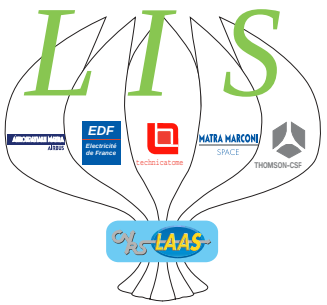
Atelier thématique n°5
Mardi 18 mars 2003 — LAAS-CNRS Toulouse

Composants COTS et sûreté de fonctionnement

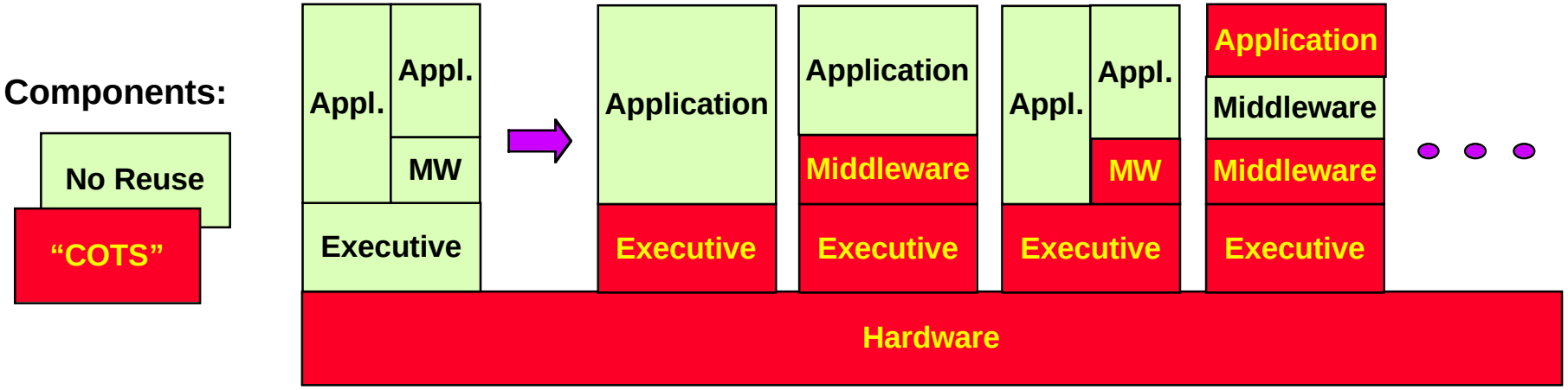
Jean Arlat
[arlat@laas.fr]



Components and Systems Concerned

- **Application:** Oracle, Flight Control,…
- **Middleware:** CORBA, DCOM, OLE,…
- **Operating System:** Unix, Windows, Linux,…
- **Microkernel:** Chorus, LinxOS, PalmOS,…
- **Processor:** Pentium, PowerPC,…

- Components of a computer system



- Embedded control systems
- Large-scale distributed systems: Web servers, ground stations, etc.
- SW development tools (simulators, compilers, etc.)

How to Build Dependable Systems from Undependable COTS Components?

- Level of Confidence sufficient -> Integrate

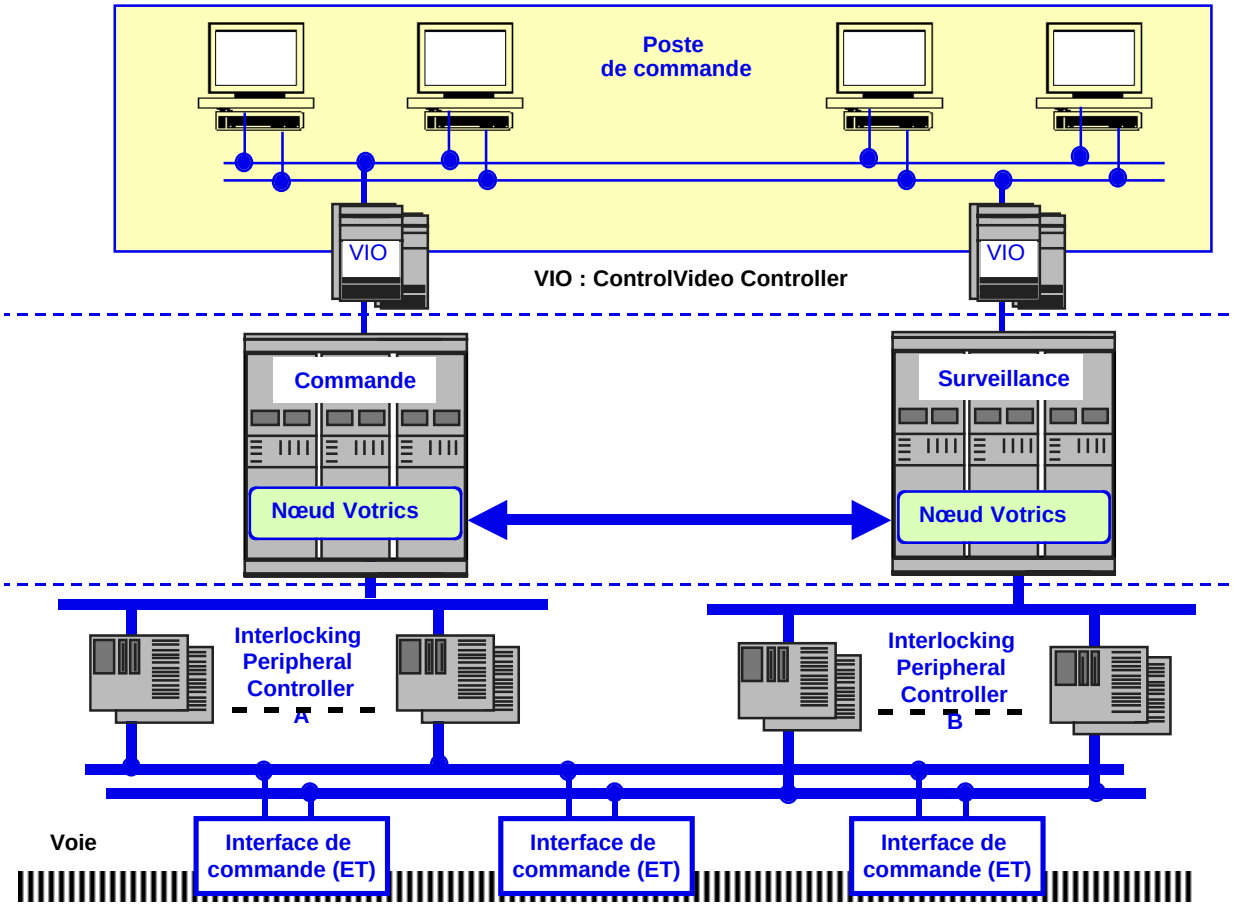
- Level of Confidence not sufficient:
  - -> Discard!
  - -> Fault containment mechanisms & service degradation
  - -> Fault containment mechanisms & service continuity
    [Depending on the degree of redundancy]

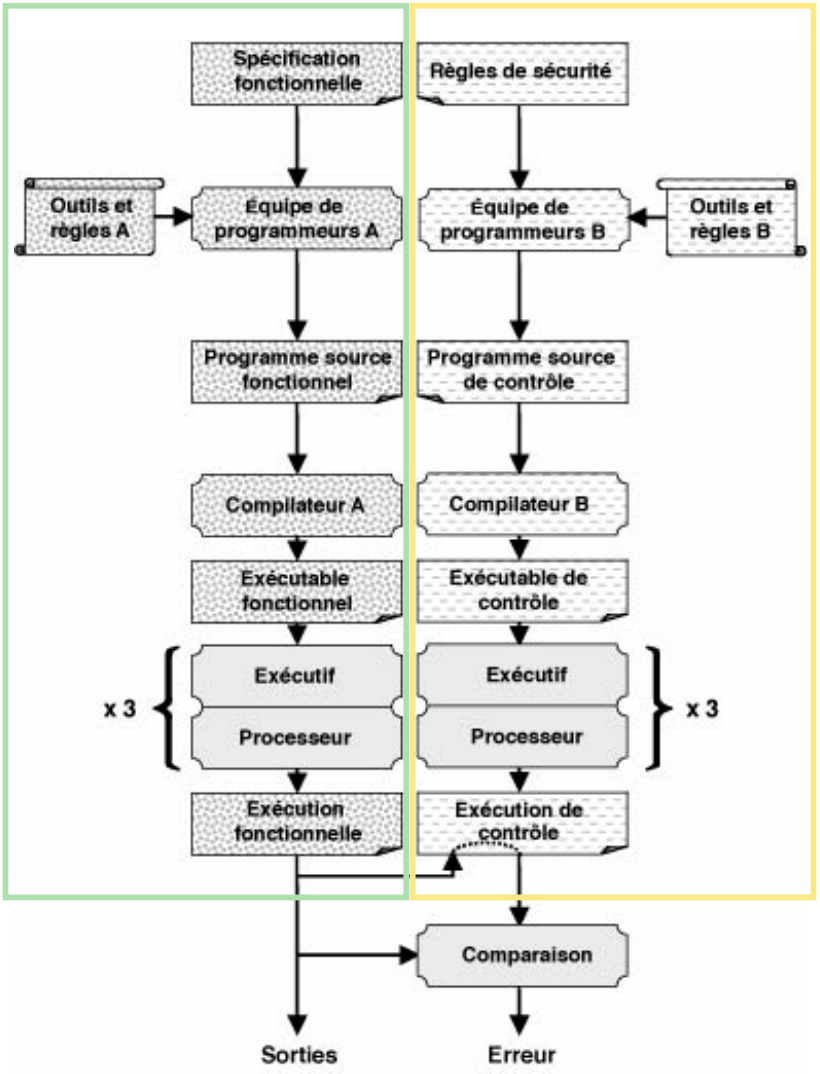
Related Architectural Solutions

⇩ Dependability Objectives / Type of COTS ⇨		Hardware	Kernel, OS, Middleware	Compiler	Application
Fault containment & service degradation	Control by independent functions	Series of protections, watchdog timer, coded processor, "safety bag", etc.			
	Partitioning	Insulation or communication by integrity checks			"IMA"
	Wrapping	Possible, but ?	Chorus & CORBA wrappers	Meta-compilation	Firewalling filtering,...
Fault containment & service continuity (d° redundancy)	Decorrelation of activity of identical components	Asynchr. redundant channels (*Elektra*)		1 compil. ≠ options	N/A
	Diversified components	B777	Applicable but ?	≠ Compilers	*NVP, RB, NSCP,...*

Contrôle
par fonctions
indépendantes

Safety Bag: Architecture Elektra
(Alcatel Austria)

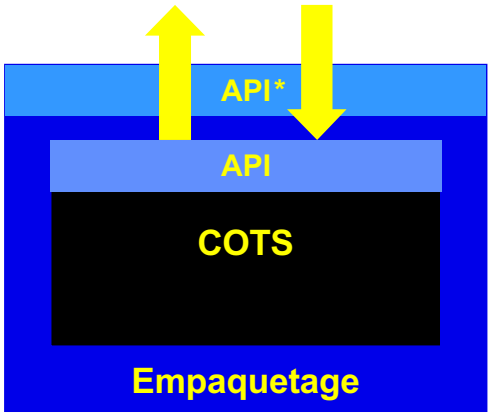




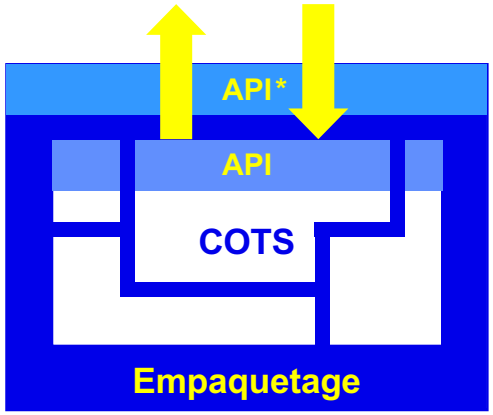
- Canaux indépendants pour traitement fonctionnel et traitement de contrôle (surveillance)
- Traitement de contrôle (test d'acceptation) : assertions exécutables

Empaquetage

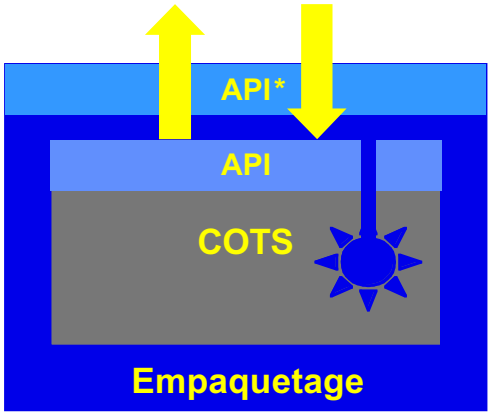
- **Objectifs :**
  - **Étendre la fonctionnalité**
    - e.g., interface POSIX sur RTOS COTS
  - **Restreindre la fonctionnalité**
    - limiter possibilités d'invocation à celles validées
  - **Filtrer paramètres d'entrée et de sortie**
    - limiter valeurs aux domaines acceptables
  - **Détecter et confiner les erreurs par assertions exécutables — efficacité dépend fortement :**
    - du degré de formalité de la spécification, et la connaissance que l'on en a
    - de l'observabilité des opérations internes



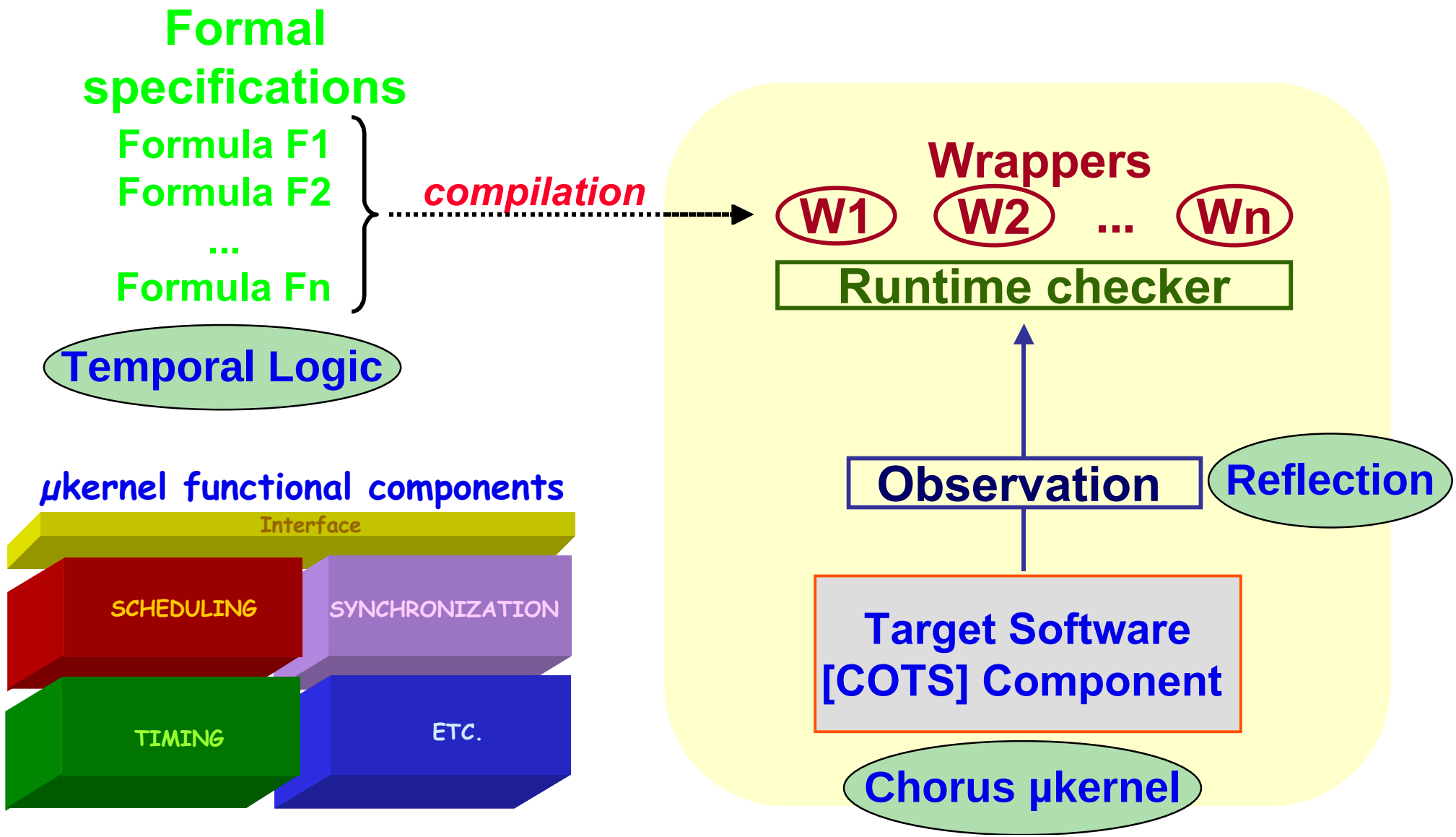
Boîte blanche
meilleure Observabilité (*open source*)



Boîte grise
interface réflective fournie par fabricant COTS permet l'*introspection*



Wrapping Framework for RT µkernels



MAFALDA-RT

Limitation de l'intrusion temporelle

Détection

Propagation

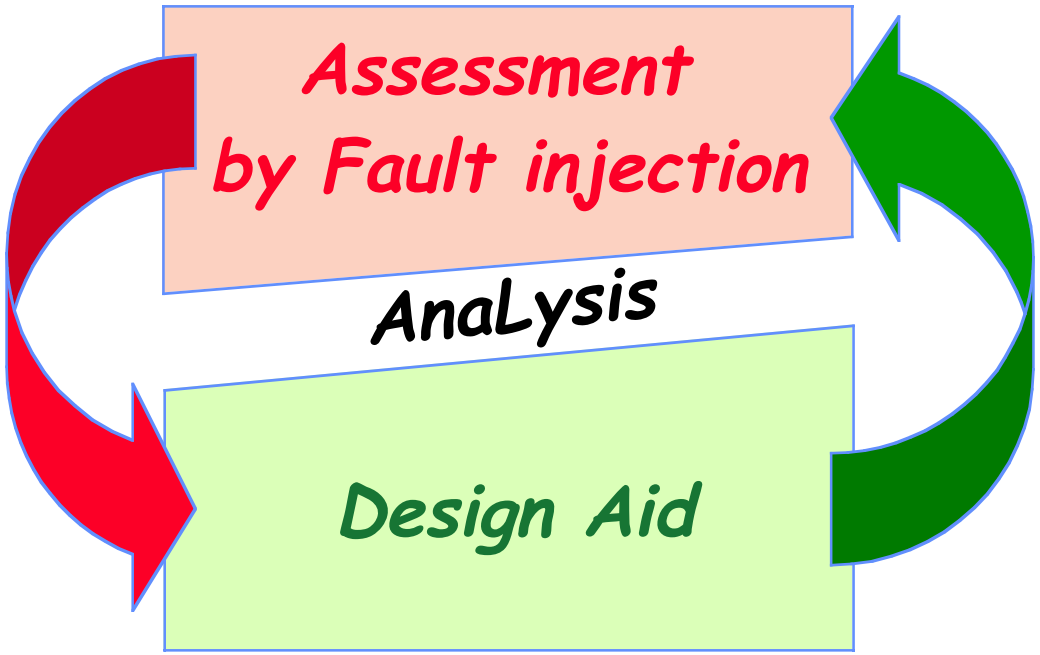
Défaillances (en valeur & en temps)

Traces d'exécution

Caractéristiques temporelles du noyau (temps de basculement)

Analyse du séquencement des événements observés

Microkernel



Spécification formelle en logique temporelle

Compilation

Vérificateur en ligne

Mécanismes "d'empaquetage"
- détection
- recouvrement

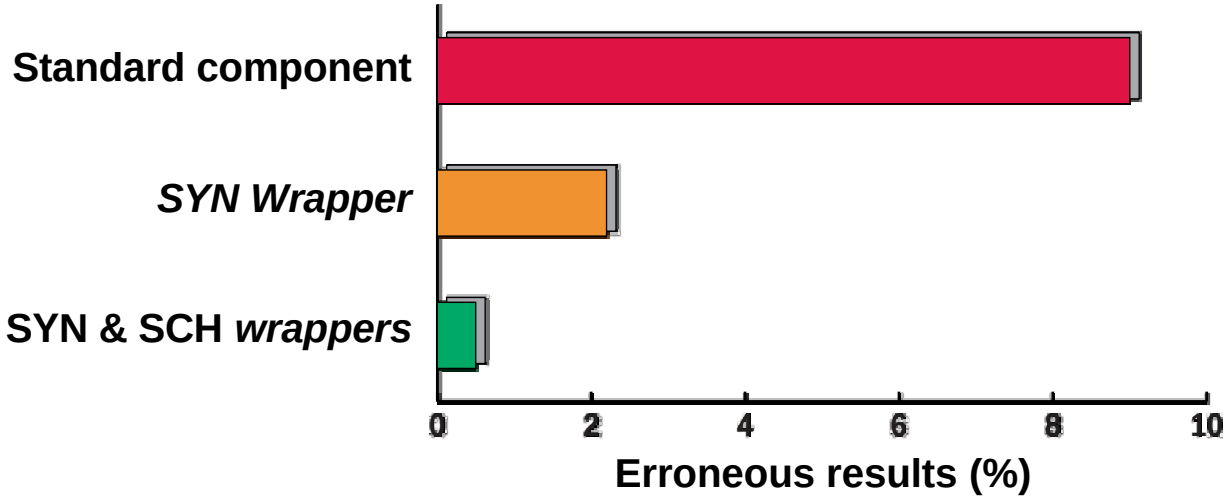
Mise en œuvre réflexive

Analyse explicite du surcoût temporel

for Real-Time systems

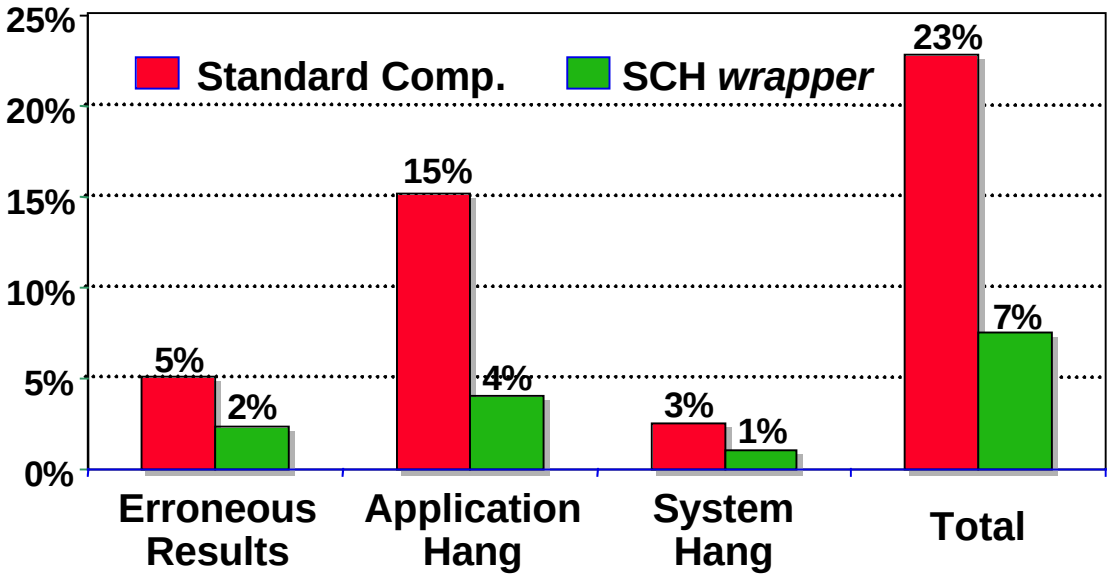
Impact of Wrapping

Chorus microkernel
[Salles et al. 99 (FTCS-29)]



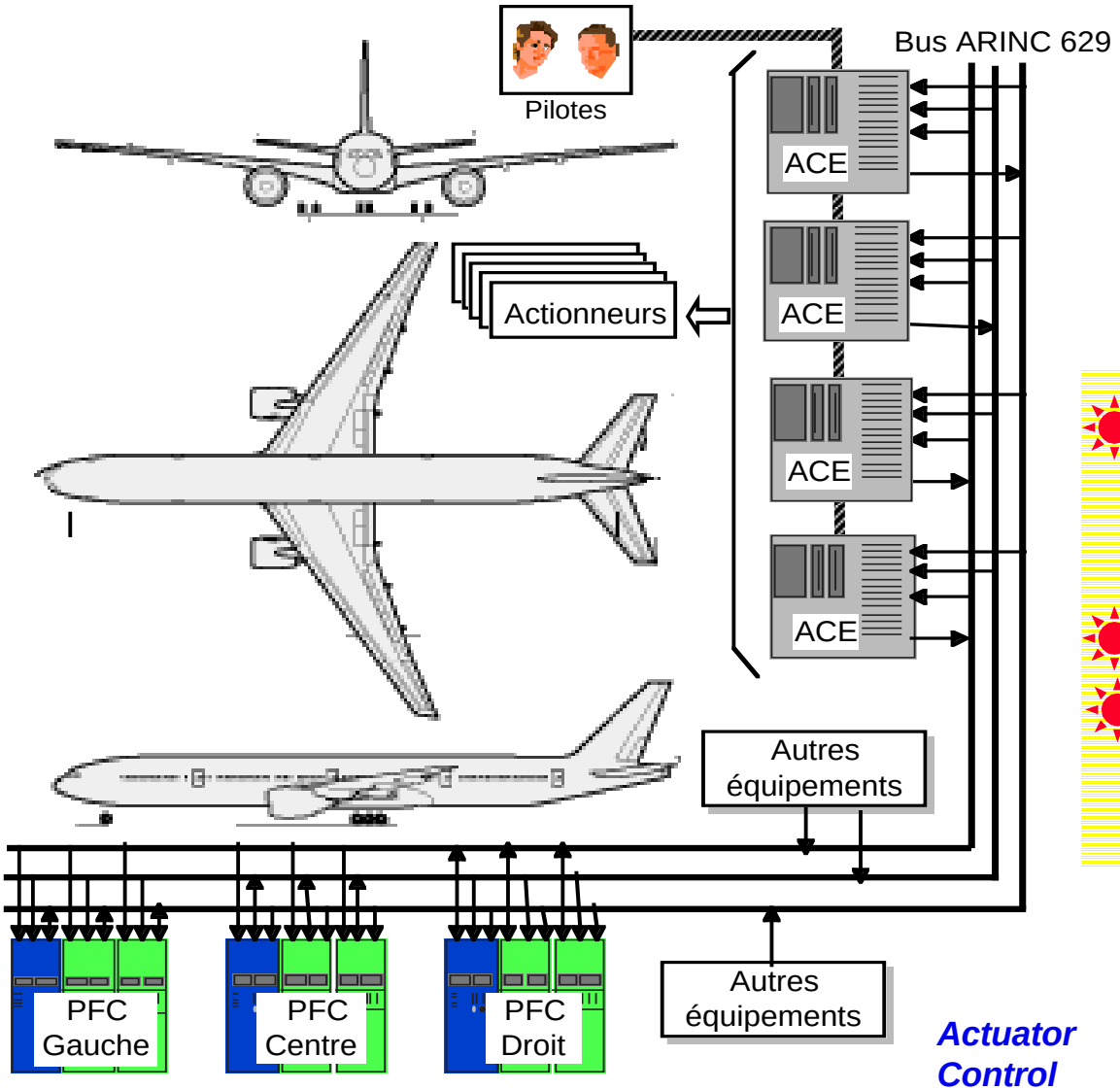
Synchronisation component: "SYN"

Task Scheduling Component: "SCH"



Diversification des composants

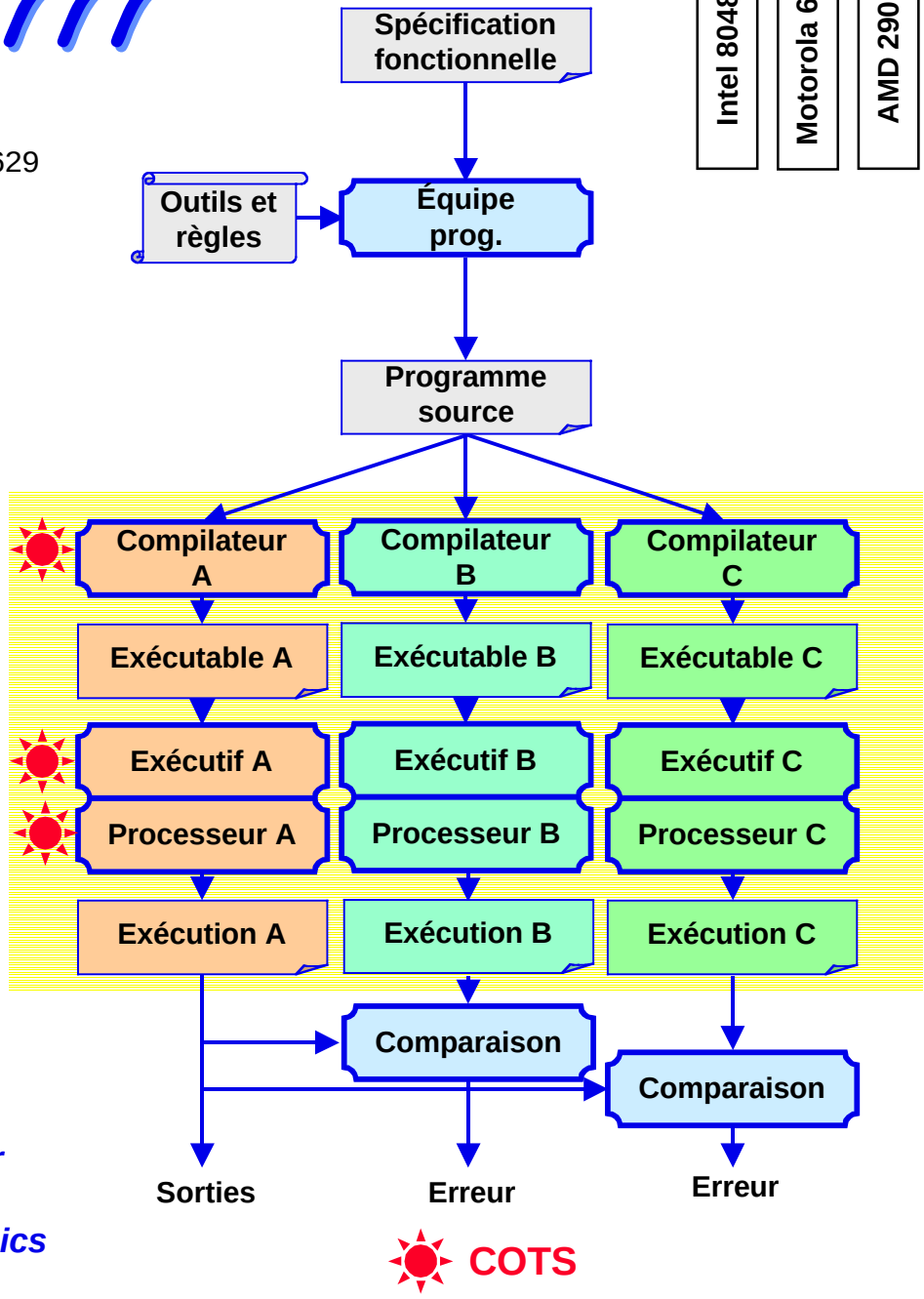
Boeing 777



Primary Flight Computers

Actuator Control Electronics

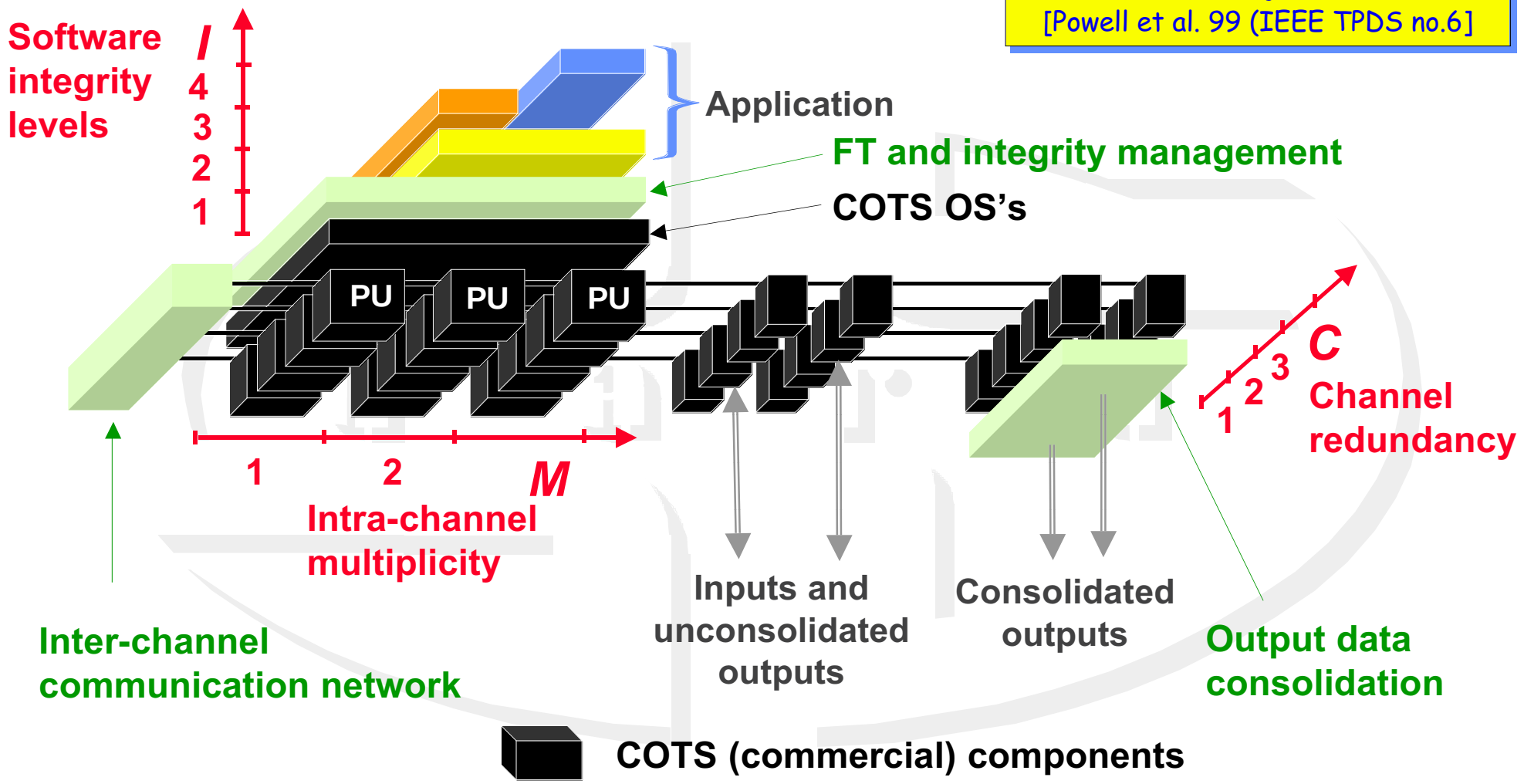
Intel 80486 | Motorola 6840 | AMD 29050



Combinaison d'approches

The GUARDS Generic Architecture

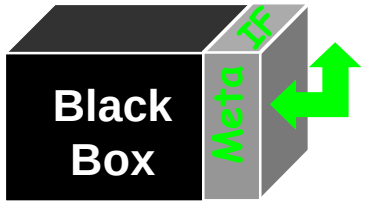
ESPRIT Project 20716
[Powell et al. 99 (IEEE TPDS no.6]



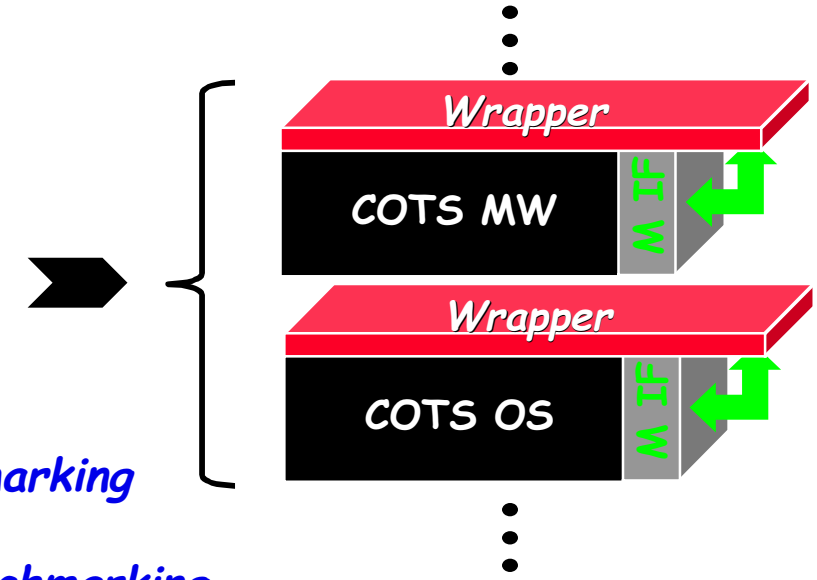
The GUARDS Partners: Technicatome (Coordinator) (F), Ansaldo Segnalamento Ferroviario (I), Matra Marconi Space France (F), INTECS Sistemi (I), Siemens Austria (A), LAAS-CNRS (F), Pisa Dependable Computer Center (I), Univ. of York (UK)

Conclusion

- Assimilation Level:



- Certification of COTS components (*OSE RTOS Kernel*)
- COTS components: HW, OS, Middleware,…
- Architectural Solutions:
  —> Layered Reflective Wrappers



- Benchmarking of COTS components
  —> IFIP WG 10.4 *SIG on Dependability Benchmarking*
  [www.dependability.org]
  —> IST-2000-25425 *Project Dependability Benchmarking*
  [www.laas.fr/DBench]
- Emergence of Open Source Solutions (GT LL)