CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Département Sciences et Technologies de l'Information et de la Communication

RTP n°21
Sûreté de fonctionnement
des systèmes informatiques complexes ouverts

[http://www.laas.fr/RTP21-SdF]

Journée de travail

Mercredi 5 novembre 2003

Amphithéâtre Stourdzé, Le Carré des Sciences, Paris

Comité de pilotage

Animateur du réseau :

Jean Arlat (LAAS-CNRS — Toulouse) [jean.arlat@laas.fr]

Membres :

- Michel Banâtre (IRISA — Rennes)
- Bernard Courtois (TIMA — Grenoble
- Frédéric Cuppens (ENSTB — Cesson-Sévigné)
- Marie-Claude Gaudel (LRI — Orsay)
- Christian Landrault (LIRMM — Montpellier)
- Jean-Claude Laprie (LAAS-CNRS — Toulouse)
- Bernard Pavard (IRIT — Toulouse)

Représentant de la direction scientifique du département STIC :

Luis Fariñas del Cerro (IRIT)

Objectifs scientifiques

- Croisement et capitalisation des intérêts et compétences afin de maîtriser la complexité des systèmes informatiques à fortes exigences en sûreté de fonctionnement
- Tendances et défis
  - Complexité et ouverture des systèmes : intégration, répartition, mobilité
  - Intégration de « composants sur étagère » (COTS ou LL)
  - Interactions matériel et logiciel (par ex. pilote de périphérique, SOCs)
  - Interdépendances entre les infrastructures (par ex.: énergie et information, etc.)
  - Adaptation autonome des systèmes informatiques à l'évolution (environnement ou interne), y compris en ce qui concerne les défaillances

Quelques RTPs…

RTP	Intitulé	Animateur(s)
19	Systèmes embarqués complexes ou contraints	Joseph Sifakis (Verimag)
20	Fiabilité, diagnostic et tolérance aux fautes des systèmes complexes	Sylviane Gentil (LAG)
13	Sécurité des accès, des échanges et des contenus	M. Riguidel (ENST) J.-P. Goedgebuer (UFC)
32	Acceptabilité, Ergonomie & Usages	Dominique Boullier (UTC) Bernard Pavard (IRIT)
48	Energie électrique : génération, stockage, transmission et usages	J.-P. Rognon (LEG-ENSIEG) J.-L. Sanchez (LAAS)

Quelques spécificités du RTP 21

- Mots-clés :

  Sûreté de fonctionnement, systèmes informatiques, ouverture, autonomie, mobilité, systèmes à logiciel prépondérant, tolérance aux fautes, élimination des fautes, prévision des fautes, fautes physiques, fautes de conception, erreurs humaines, malveillances

- Tolérance aux fautes accidentelles (matériel et logiciel) et malveillances (intrusions)

- Test et expériences contrôlées
  - Vérification de la tolérance aux fautes et évaluation de la couverture
  - Caractérisation des modes de défaillance -> *Benchmarking* (étalonnage) de la SdF

- Modélisation et évaluation des mesures de la SdF vis-à-vis des fautes accidentelles et des malveillances

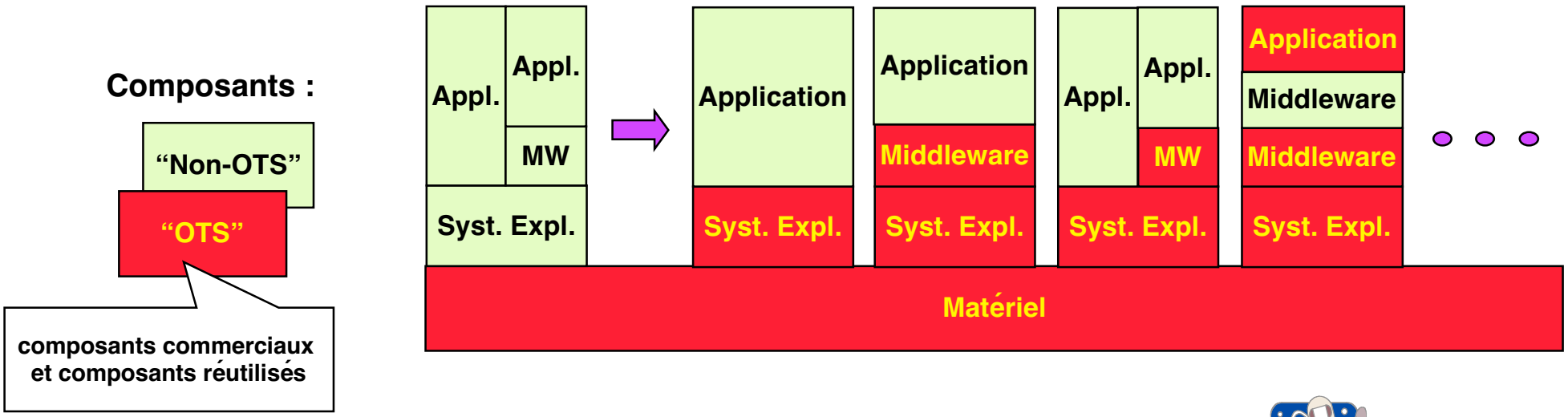
Quelques éléments sur la problématique

- Composants matériels
  - Fautes de conception résiduelles
  - Susceptibilité aux radiations
  - Non déterminisme
- Composants logiciels
  - Systèmes opératoires
  - Pilotes de périphérique
  - Intergiciels (*middleware*)
- Systèmes
  - Ouverture -> malveillances
  - Ségrégation -> Intégration
  - Réutilisation & intégration de composants
  - Infrastructures informationnelles
  - Evolution et adaptation
  - Mobilité et nomadicité
  - Allocation des fonctions H/S
  - Processus de développement

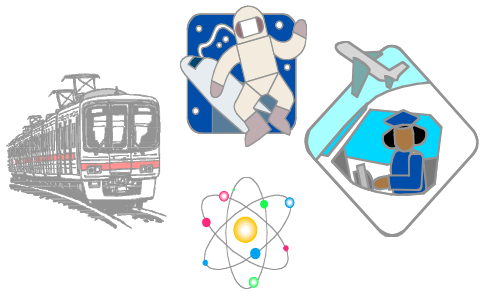
Réutilisation et intégration de composants

- **Application** : Oracle,...
- **Middleware** : CORBA, DCOM, OLE,...
- **Syst. Expl.** : Unix, Windows, Linux,...
- **Micronoyau** : Chorus, LynxOS, PalmOS,...
- **Processeur** : Pentium, PowerPC,...

- Composants d'un système informatique



- Systèmes « enfouis » (contrôle-commande)
- Serveurs Internet
- Logiciels de développement (simulateurs, compilateurs, etc.)



Caractérisation des modes de défaillances

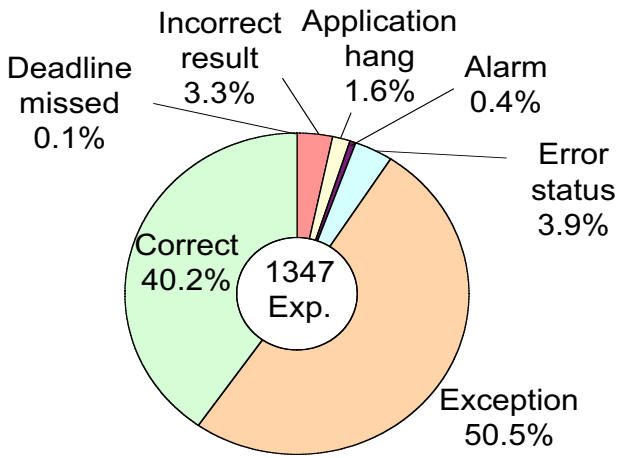
Expériences contrôlées par injection de fautes

- Développement de systèmes critiques intégrant des composants logiciels « sur étagère » (COTS ou LL)
  - ➤ Logiciels exécutifs

    micronoyaux temps réel, systèmes d'exploitation, intergiciels [*middleware*]

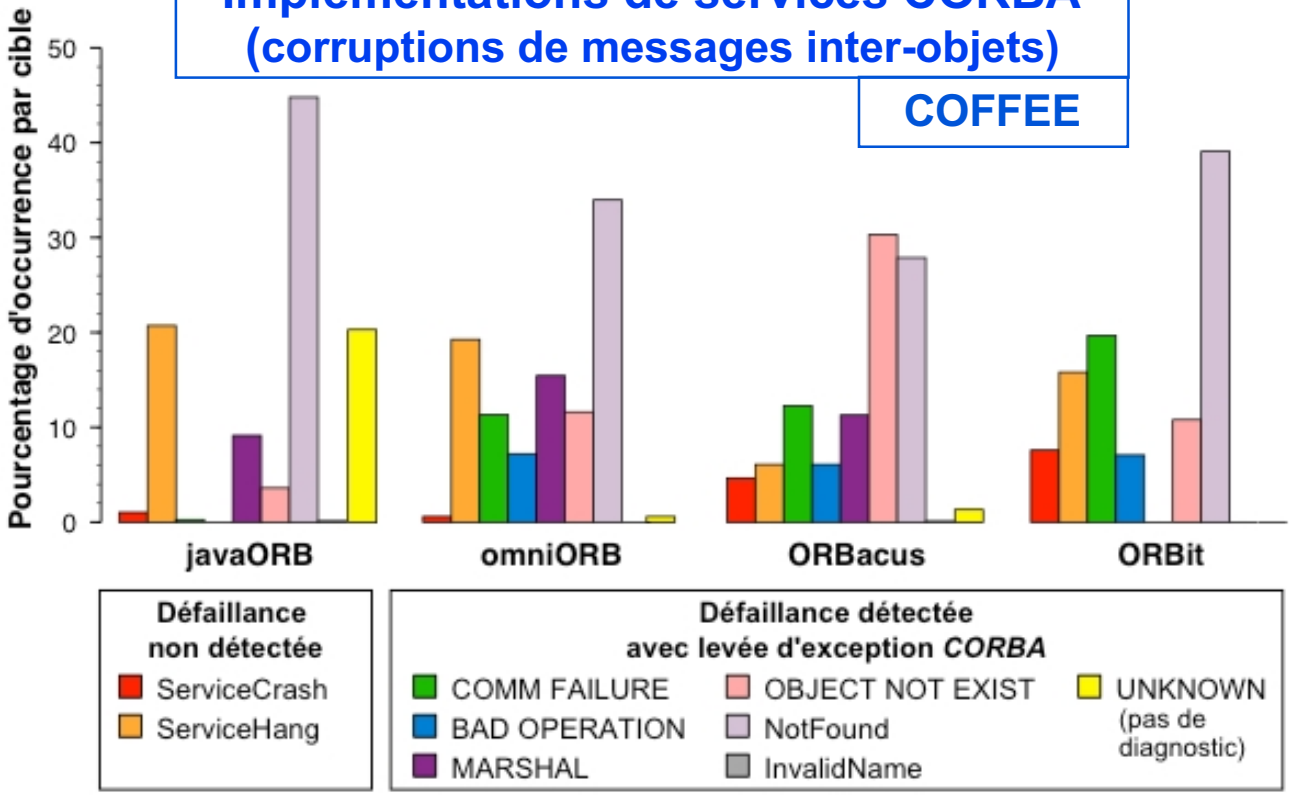
µnoyau TR (Chorus)
(*bit-flips* en mémoire)

MAFALDA-RT



Implémentations de services CORBA
(corruptions de messages inter-objets)

COFFEE



Étalonnage de la sûreté de fonctionnement

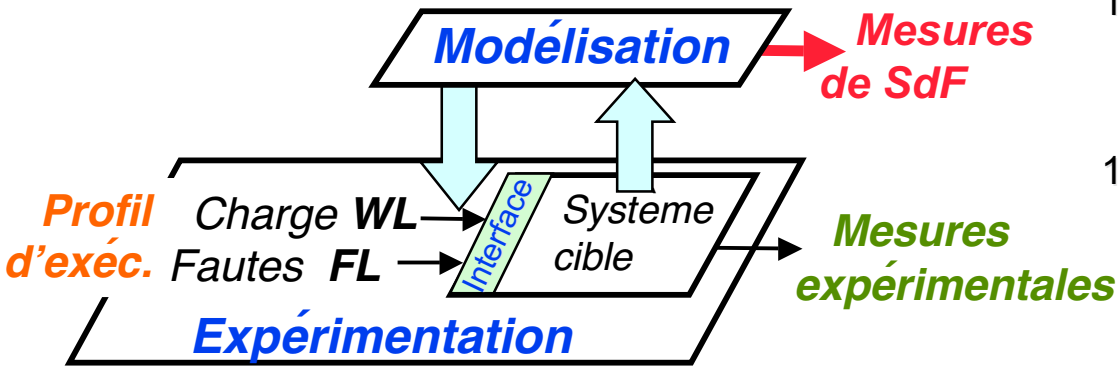
- Définition et développement de *benchmarks* (moyens et procédures) permettant une caractérisation objective et reconnue des comportements de systèmes et de composants logiciels en présence de fautes ≈ *benchmarks* de performance,…

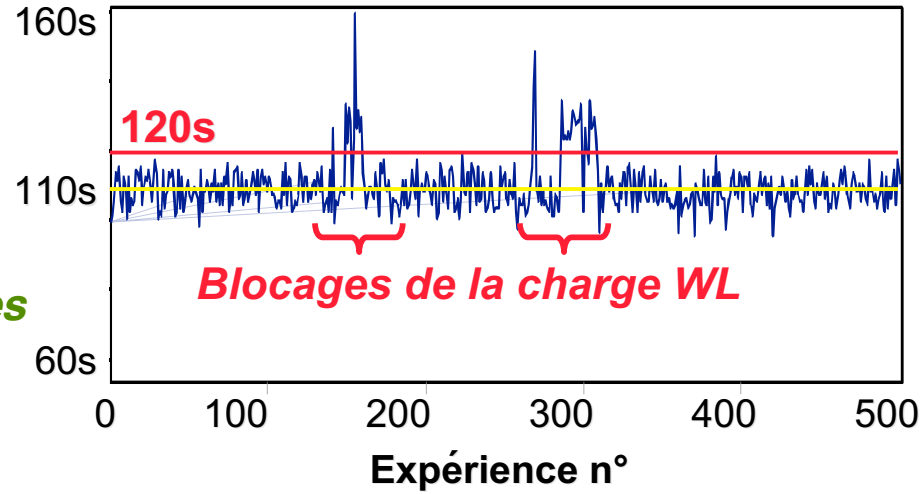
Cadre conceptuel

- Profil d,exécution représentatif et appliqué sur une interface de référence
- Mesures significatives pour un utilisateur (mes. de robustesse et mes. temporelles)

Ex. de résultats - *Windows*

- Mesure exp. : temps de relance
- WL : client TPC-C
- FL : corruption des paramètres des appels système





Les Actions Spécifiques du RTP 21

AS	Intitulé et Animateurs	RTP
23	Techniques avancées de tests des systèmes complexes Richard Castanet, LaBRI et Hélène Waeselynck, LAAS	19
75	Méthodes et outils logiciels pour le développement de systèmes d'exploitation Gilles Muller, EMN	05
111	Techniques de spécification et de test pour les composants logiciels de communication Ana R. Cavalli INT-Evry	01
161	Testabilité des systèmes informatiques Lydie du Bouquet, LSR-IMAG	

Le RIS : Réseau d'Ingénierie de la Sûreté de fonctionnement

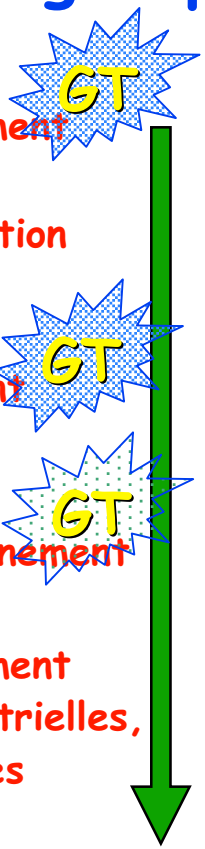
- Domaine : Ingénierie de la sûreté de fonctionnement des systèmes à logiciel prépondérant
- Prolongement de la coopération établie dans le cadre du LIS sous une forme renouvelée :
  - Participation industrielle et académique élargie
  - Favoriser la mise en place de partenariats (programmes de R & D)
  - Stimuler les réflexions communes

- Comité d'Orientation -> Pilotage du réseau
- Ateliers thématiques -> Analyse d'un thème
- Groupes de Travail -> Réflexion approfondie et document de synthèse

Mise en place en janvier 2001 pour 4 ans

Les activités du *RIS*
(http//:www.ris.prd.fr)

Ateliers thématiques et groupes de travail



1	Logiciel libre et sûreté de fonctionnement	*J. Arlat LAAS-CNRS*	LAAS — 14/12/2000
2	Usages et perspectives pour la production de logiciels sûrs	*M. Kaâniche LAAS-CNRS*	LAAS — 19/10/2001
3	Intergiciel et sûreté de fonctionnement	*J.-C. Fabre LAAS-CNRS*	LAAS — 6/6/2002
4	Nouvelles architecture et technologies des processeurs et sûreté de fonctionnement	*Y. Crouzet LAAS-CNRS* *F. Rodet Technicatome*	Technicatome — 20/12/2002
5	Justification de sûreté de fonctionnement (*dependability case*) : approches industrielles, méthodes de construction et structures	*P.-J. Courtois AVN Nuclear* *M. Kaâniche LAAS-CNRS*	LAAS — 18/3/2003

Ouvrage Collectif « LL et SdF » (Hermes-Lavoisier)
et Journée de présentation le 17 sept. 2003