Dependable Distributed Architecture for Safety Critical Applications

Kick-off meeting

PARIS – March 23rd 2011

Dependable Distributed Architecture for Safety Critical Applications

- **Dependable Distributed Architecture for Safety Critical Applications**
  - **Définition du terme « Dependable » : confiance justifiée que l'on peut placer dans un système, se caractérise par les 6 attributs suivants :**
    - **Availability ("readiness for correct service"),**
    - **Reliability ("continuity of correct service"),**
    - **Integrity ("maintaining the consistency of data"),**
    - **Maintainability ("ability for a process to undergo modifications and repairs"),**
    - **Safety ("absence of catastrophic consequences on the users and the environment")**
    - **Security ("prevention of unauthorized disclosure of information").**

Présentation du consortium : le contexte

- La multiplication des mécanismes de contrôle-commandes dans de nombreux secteurs d'activité a fortement développé les besoins en matière de sûreté de fonctionnement. Chaque domaine concerné développe depuis des années des approches hétérogènes et le domaine de la sûreté de fonctionnement repose aujourd'hui sur des gammes de produits propriétaires dont il est très difficile (voire impossible) de gérer l'interconnexion.
- Cette situation conduit à devoir entamer des procédures longues et coûteuses de certification lors de la conception de chaque nouvelle application. De plus, la segmentation sectorielle de l'existant interdit l'éclosion d'un marché dans lequel les effets de volume seraient en mesure de permettre l'apparition de solutions reconnues comme sûres de manière générique à des coûts largement inférieurs aux approches spécifiques actuelles. Une telle uniformisation présentera également l'avantage de réduire les coûts de maintenance et de faciliter la gestion de l'obsolescence des systèmes.

Présentation du consortium : les objectifs du consortium

- « travailler dans une démarche d'ouverture, à la réalisation et la standardisation de briques génériques, modulaires, démontrables, réutilisables et sûres servant à la réalisation de structures d'accueil matérielles et logicielles pour des applications critiques »
- « fournir un ensemble d'outils et de méthodologies permettant la démonstration du niveau de Sûreté de Fonctionnement pour les architectures génériques proposées »
- « assurer une complète ségrégation de l'application vis-à-vis de la structure d'accueil via des interfaces banalisées permettant une très forte réutilisation des applications »
- « permettre de travailler dans une démarche de certification incrémentale afin de limiter les coûts de développement et de réduire le time to market »
- « garantir une haute disponibilité et un niveau de sûreté maximal (DALA - SIL4) pour les systèmes sûrs fortement distribués »
- « garantir l'interopérabilité entre des produits et solutions venant de différents constructeurs »
- « assurer via une plateforme la génération d'application distribuée temps réel à partir d'ateliers métier existants »
- « fournir des produits COTS aptes à couvrir les besoins des systèmes critiques et s'interfacer avec des produits existants».

Les membres du Consortium

- Academiques
  - ENS Cachan
  - ENSTA
  - ENS ULM
- PME / ETI
  - Altis
  - Arion Entreprise
  - B&R Automation
  - C-S
  - ClearSy
  - DMAP
  - HPC Project
  - RTaW
  - Scilab Enterprise
  - Tronico
  - Wind River
- Grands Groupes
  - Alstom Power
  - CNES
  - EDF R&D
  - EADS
  - Nexter
  - Sagem
  - SNCF
- Organismes de standardisation
  - EPSG