COMIT
Une bibliothèque de composants logiciels sécurisés pour applications relatives à la sûreté

Atelier du Ris Le 6/06/2002 TOULOUSE

TECHNICATOME

COMIT : Sommaire de la présentation

- Les applications visées,
- Les objectifs,
- L'architecture,
- Les modèles de COTS,
- Les composants réutilisables,
- La construction,
- Un exemple d'instance,
- Le développement.

COMIT : Les applications

> Caractéristiques des applications visées :

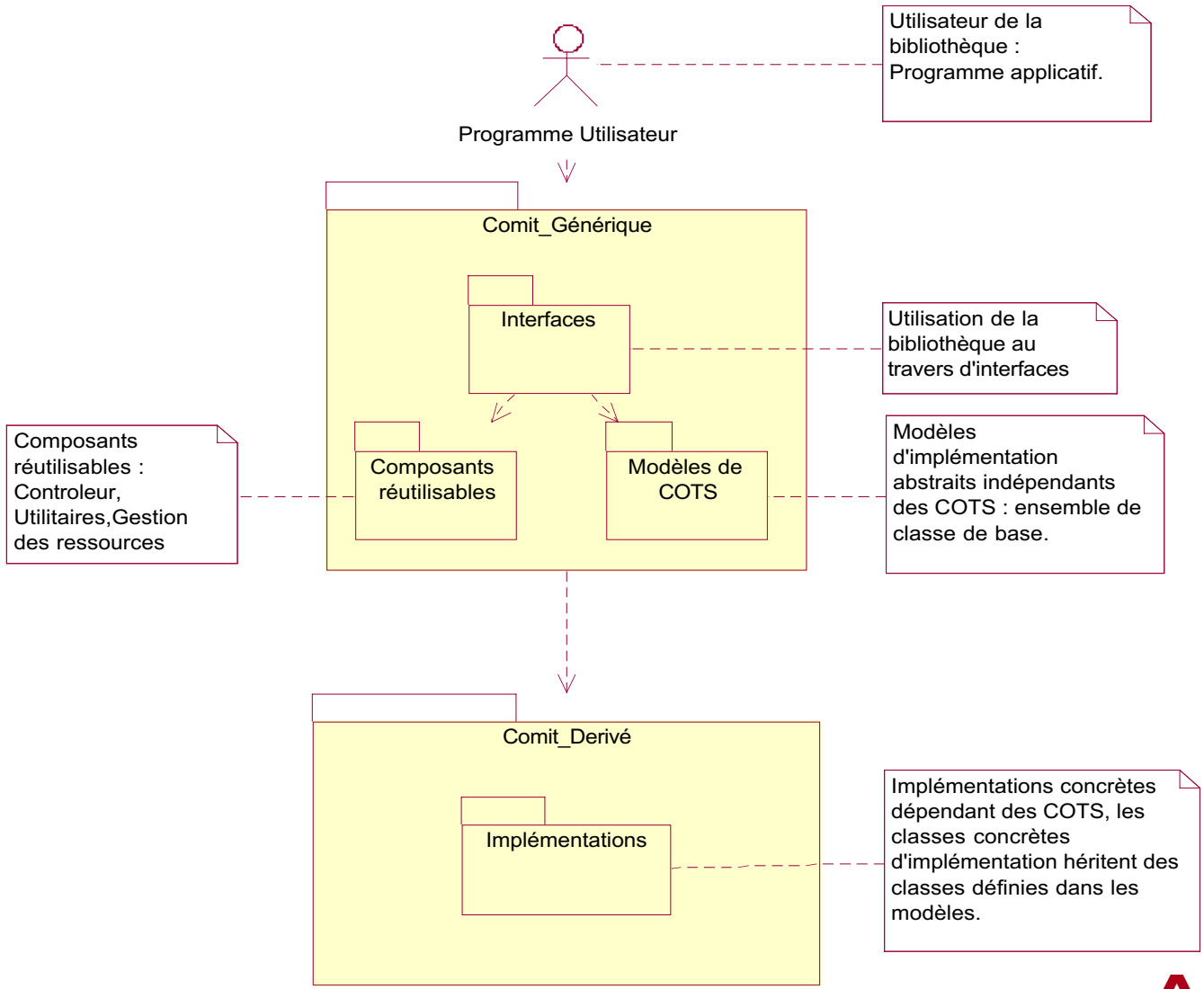
- Contrôle commande de chaufferie nucléaire (supervision, régulation et commande d'actionneurs),
- Embarquées et Enfouies,
- En rapport avec la sûreté (niveau B : safety related),
- Cycliques (Applicatif sous la forme d'une boucle primaire),
- Fonctionnement 24 sur 24 sans intervention,
- Basées sur des COTS (Matériel et logiciel),
- Pérennité importante (>10ans).

COMIT : Les objectifs

> Objectifs de la bibliothèque :

- Pérennisation des logiciels d'application (Indépendance totale vis à vis des cots),
- Encapsulation et sécurisation des cots (Contrôle des paramètres d'appels, Restriction d'utilisation),
- Uniformisation des développements (modèle d'application, interface uniforme),
- Réutilisation (capitalisation des composants métiers).

COMIT : L'architecture



TECHNICATOME

COMIT : Les modèles de COTS

- Modèles génériques de COTS :
  - Système d'exploitation,
  - Carte unité centrale,
  - Entrées / Sorties locales (Tout ou Rien et Analogiques),
  - Entrées / Sorties distantes (Lignes séries, Réseau Ethernet),
  - Réseau de terrain déterministe,
  - Système graphique.
- Chaque modèle s'utilise au travers d'une ou plusieurs classes d'interface.
- L'implémentation concrète sur un COTS donné se fait par héritage d'une ou plusieurs classes de base du modèle.

COMIT : Les composants réutilisables

> Composants réutilisables :

- Modèle d'application,
- Gestion de ressources matérielles,
- Contrôle d'échéance des processus,
- Inspection du code en fonctionnement,
- Gestion des défauts et mise à l'état sûr (Chien de garde),
- Communication synchrone par messages sécurisés (entre process mono CPU et entre process multi CPU sur le même fond de panier).

Les composants s'utilisent soit au travers d'une classe d'interface soit par héritage d'une classe de base.

COMIT : La construction

Basée sur la notion d'instance :

- Configurée exactement sur les besoins d'une application,
- Construite à partir d'un ensemble de COTS matériels et logiciels donné,
- Intégrée sur le matériel de l'équipement définitif,
- Attribution d'un numéro de version pour l'instance.

COMIT : Un exemple d’ instance

> Une instance de comit existe pour une application de supervision :

avec les COTS logiciels suivants:

- Système d’exploitation QNX6,
- Système graphique PHOTON,
- Bibliothèque Réseau de terrain Fip Device Manager,

et les COTS matériels suivants :

- Carte CPU VME 6U à base de Pentium,
- Fond de panier bus VME,
- Coupleurs Mmodule FIP sur carte porteuse.

COMIT : Le développement

- Développement niveau B (Plan qualité, Plan de gestion de Conf., Plan de vérification, Règles de codage, Revues formelles, Etc…),
  - Conception avec la Notation UML (outil rational rose) ,
  - Codage en C++ avec restrictions (usage limité des templates et maîtrise de l'allocation dynamique, pas d'utilisation de la STL),
  - Programmation défensive en utilisant les exceptions,
  - Tests unitaires avec 100% de couverture du code atteignable (outil rational test real time).