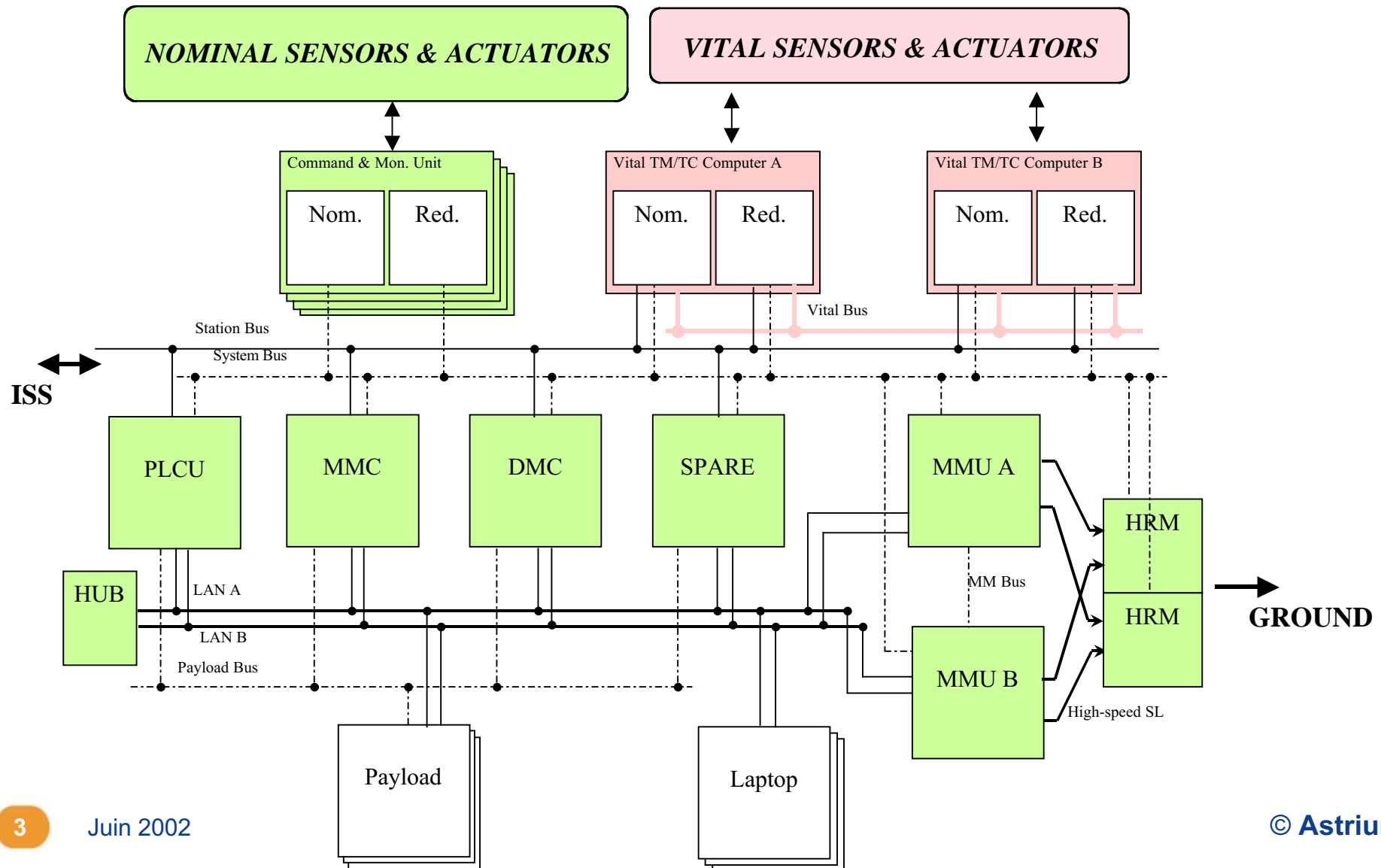


**Middleware embarqué pour la gestion  
des données de Columbus**

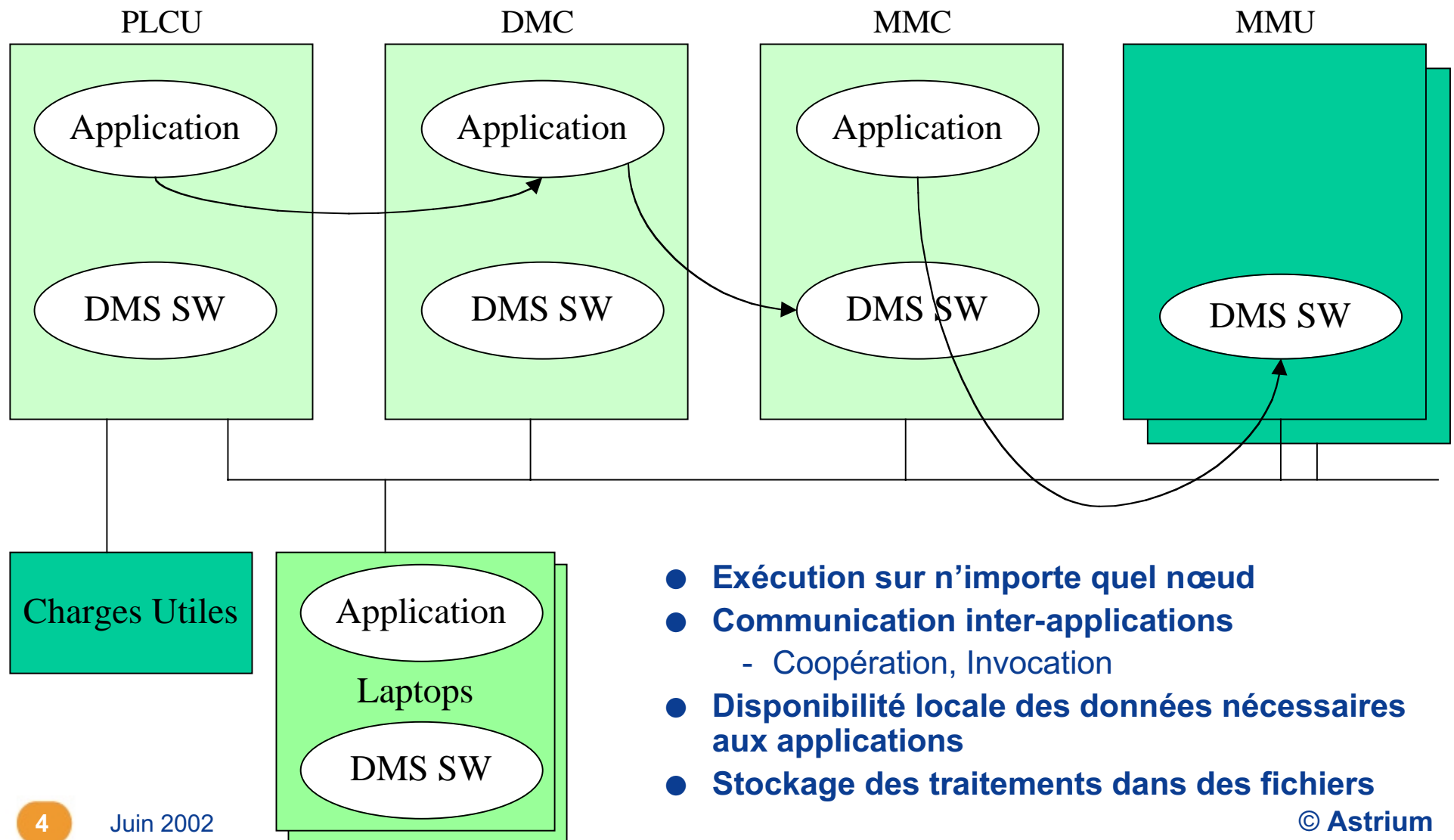
# Présentation du système COF

- **Système servant de support aux expériences embarquées dans ISS**
  - Exécution des applications spécifiques aux expériences
  - Gestion et stockage des résultats
- **Système distribué**
  - Trois Nœuds ayant des fonctions différentes
    - Gestion des charges utiles
    - Gestion des données
    - Gestion de la mission
  - Un nœud de «réserve» en cas de défaillance de l'un des trois autres
  - Un serveur de fichier NFS en redondance «chaude» (réplication semi-active)
  - Laptops permettant la surveillance et le contrôle du processus
- **Motivation du système distribué**
  - Offrir une puissance de calcul supérieure à celle d'un système centralisé

# Architecture Matérielle



# Besoins des logiciels d'application



- **Exécution sur n'importe quel nœud**
- **Communication inter-applications**
  - Coopération, Invocation
- **Disponibilité locale des données nécessaires aux applications**
- **Stockage des traitements dans des fichiers**

# Présentation du DMS SW

- **Offre le support d'exécution des applications**
  - Applications = processus systèmes (ADA) et procédures interprétées (FLAP)
  - Lancement, gestion, terminaison
  - Communications
  - Distribution des données utiles aux applications sur les nœuds adéquats
  - Distribution des traitements
- **Interface de contrôle**
  - Gestion des messages CCSDS et SW
  - RPC
- **Surveille le bon fonctionnement du système**
  - Détection d'erreurs matérielles
    - Charge utile, bus, nœud
  - Reconfiguration
- **Interface avec le matériel**
  - Drivers matériels

# Définition de la couche middleware

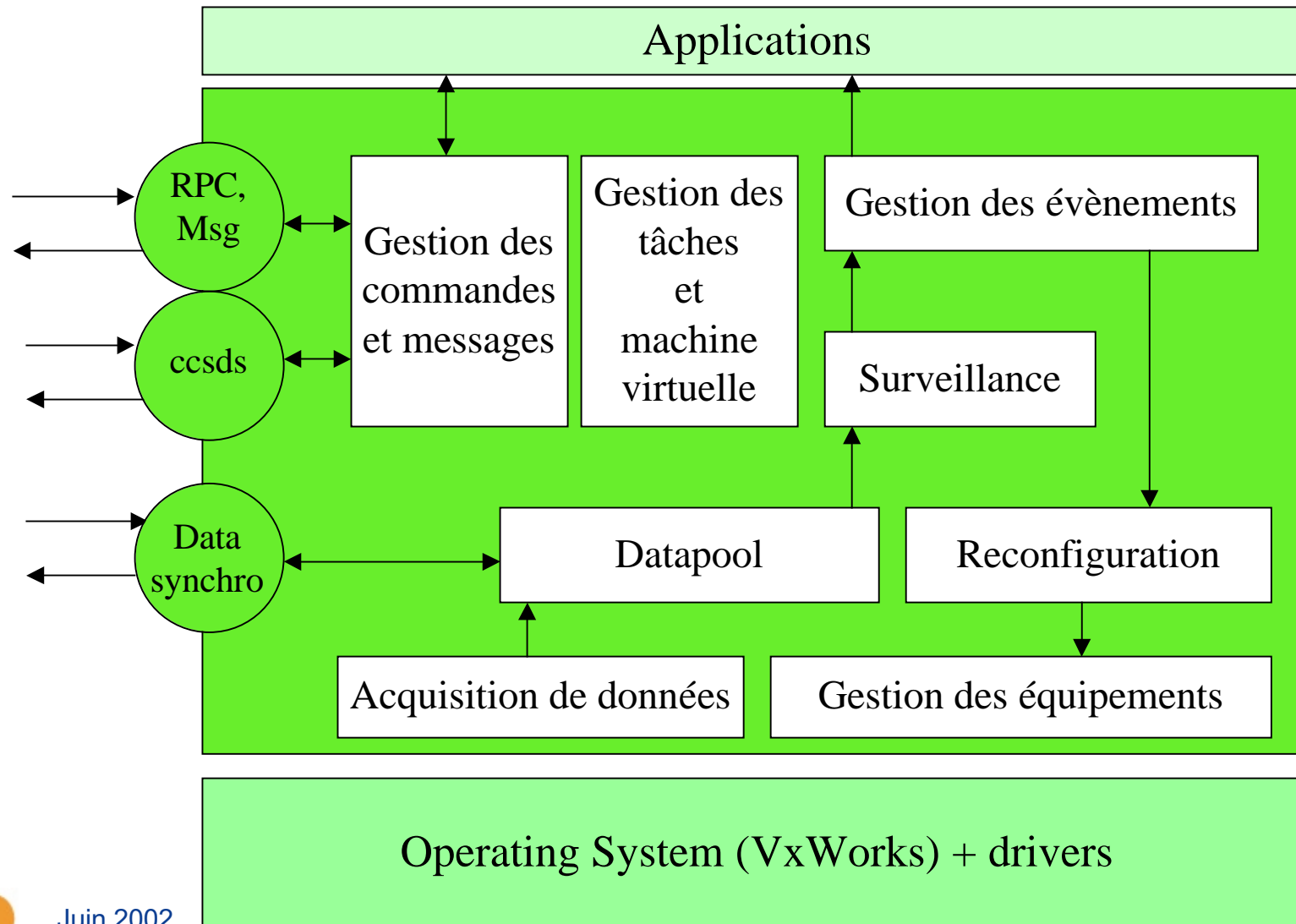
- **Partie « Active »**

- Acquisitions cycliques
- Distribution de données
- Surveillance du système
- Échanges de messages (sur couche IP)
- Gestion des applications
  - Gestion des tâches (démarrage, suspension, arrêt)
  - Interprétation de programmes (machine virtuelle)
- Gestion de la redondance dans le cas de la MMU

- **Partie « Passive »**

- Bibliothèques offrant diverses fonctions d'accès aux services systèmes
  - Gestion de fichiers
    - Enregistrement de traces
    - Sauvegarde de l'état du système (checkpointing)
  - Accès aux équipements
  - Configuration des services (surveillance, ...)

# Définition de la couche middleware



# Communications

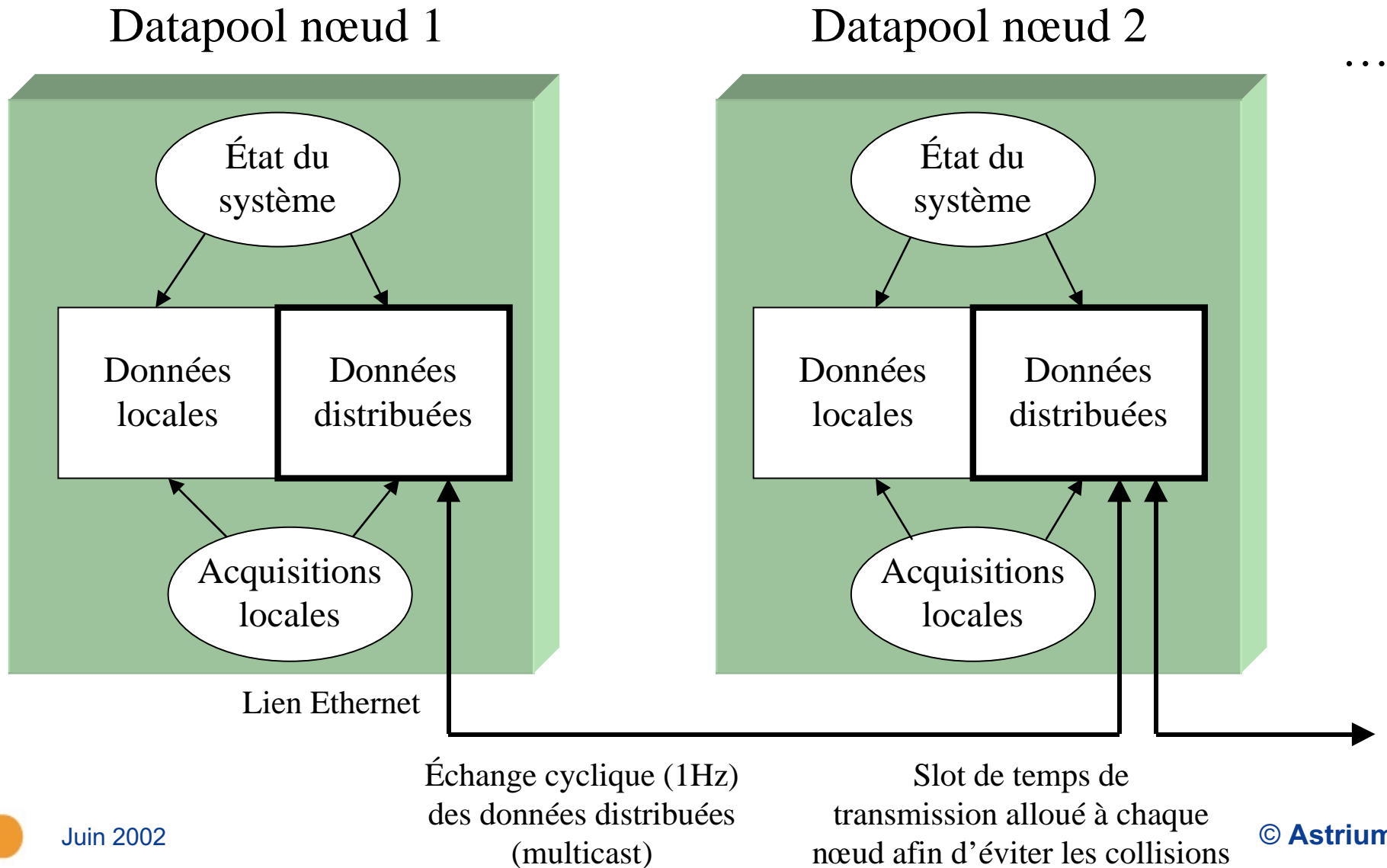
- **Multiples liens de communication**

- Lien Ethernet entre calculateurs
  - Échange de messages UDP
  - RPC
- Lien 1553 entre calculateurs et équipements
  - Acquisition de données liées aux équipements (stockées dans le datapool)

- **Multiples moyens de communiquer implémentés par le middleware**

- Messages CCSDS (TM, TC), empaquetés par des «SW Messages»
- SW messages, paquets UDP d'un format défini véhiculés sur lien Ethernet
- Multicast: distribution du datapool via le lien ethernet
  
- Remote Procedure Calls: invocations de fonctions distantes entre calculateurs (de sorte que la procédure soit exécutée sur le nœud dont elle dépend)

# Datapool - Distribution des données



# Détection d'erreurs

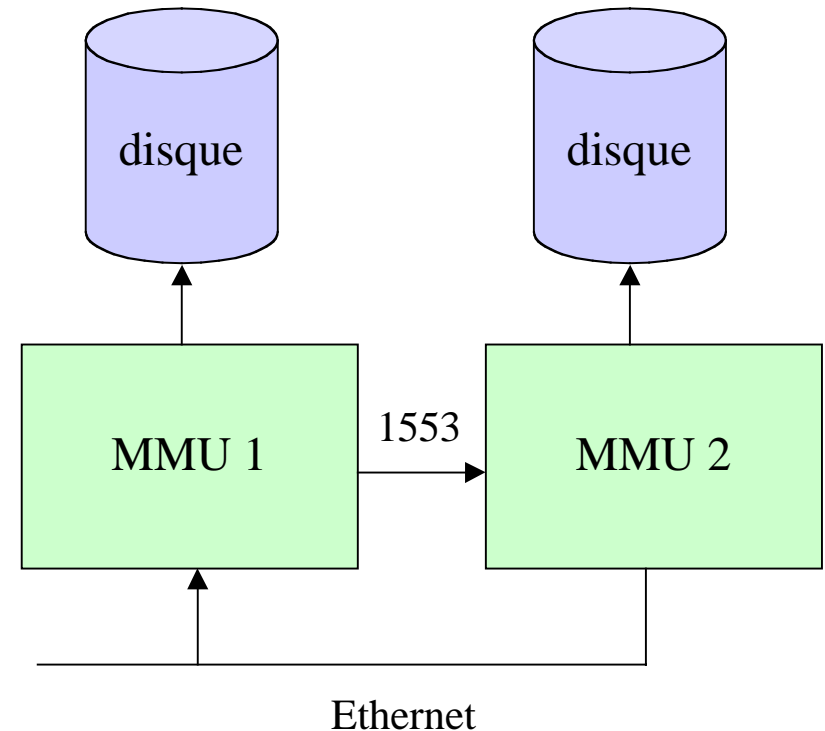
- **Par le biais de valeurs erronées dans le datapool**
  - Surveillance et filtrage des données
    - Recherche à tolérer les erreurs intermittentes
  - Réaction en cas d'anomalies détectées: événement soulevé pour déclencher une action éventuelle de reconfiguration
- **Par le biais de programmes dédiés**
  - Gestion de la redondance de la MMU
- **Par le biais de la couche de bas niveau accédant au hardware (drivers)**
  - Détection de matériels défectueux (1553, Ethernet, ...)
  - Réaction par action immédiate:
    - Ex.: utilisation du bus 1553 redondant

# Gestion du nœud redondant (Spare)

- **Détection de la défaillance d'un nœud**
  - Surveillance de PLCU et MMC par DMC
    - Via des acquisitions de statuts d'équipements (disponibles dans le datapool)
  - Surveillance de DMC par VTC
- **Extinction du nœud défaillant et allumage du nœud redondant**
- **Reprise de l'état du système sur état sauvegardé**
  - Checkpointing «simple» réalisé au niveau du système (hors applications)
  - Sauvegarde sur support stable (MMU)
  - Recouvrement d'erreur par poursuite

# Gestion de la redondance du serveur de fichiers

- **Réplication semi-active**
- **Le maître reçoit les données et les traite**
- **Il fournit les données à l'esclave qui les écrit directement sur le disque**
- **L'esclave espionne le maître et prend la main en cas de défaillance de celui-ci (hypothèse silence sur défaillance)**
- **L'esclave remplace alors le maître sur le bus Ethernet (vol d'adresse)**



# Conclusion

- **Système embarqué novateur pour le spatial**
  - Distribution
  - Généricité du système
    - Facilement instanciable d'un nœud sur l'autre
- **Présente toutes les caractéristiques des «middleware» spatiaux**
  - Couche de services passifs (ex.: interfaces d'accès aux équipements)
  - Couche de services actifs (ex.: surveillances, reconfigurations)
- **Non exempt de défauts**
  - Possibilité de perdre des paquets en distribuant le datapool
    - Perte (temporaire) de cohérence de l'état du datapool entre les différents nœuds
    - Pas de protocole de diffusion fiable, ni de cohérence interactive entre les nœuds