Conception générale formelle des sous-systèmes électroniques d'un véhicule

Guilhem Pouzancre

09 juin 2005

C l e a r S y
Contact@Clearsy.com

EUROPARC de Pichaury
Bâtiment C1
1330, av. Guillibert de la Lauzière
13 856 Aix en Provence Cedex 3

Téléphone : 04.42.37.12.70
Télécopie : 04.42.37.12.71
www.clearsy.com

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Le SPRAT

« Le "SPRAT" est le système de franchissement le plus novateur actuellement conçu. Il n'a aucun équivalent au monde, et intéresse plusieurs armées étrangères. »

Extrait : www.cnim.fr

AFIS Association Française d'ingéniarie Système

CLEARSY SYSTEM ENGINEERING

Plan

- **Contenu du modèle du SPRAT**
- **Modélisation formelle**
  - ✓ B'Système et CompoSys
- **Méthode de modélisation du système**
- **Valeur ajoutée du modèle**
  - ✓ Création, Modification, Exploitation
- **Conclusion**

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Réalisation d'un document de conception système

Pour chaque sous-système on décrit :

- Ses fonctions
- Ses interfaces (fil, capteur, actionneur, paramètre réseaux, circuit hydraulique, circuit pneumatique, etc.)
- Ses règles de fonctionnement

Résultat : 50 sous-systèmes électroniques, 400 interfaces, 200 fonctions, ont été décrits.

Utilisation d'une méthode et d'un outil pour les descriptions : CompoSys

Modélisation couplée : méthode formelle B / langage naturel ;

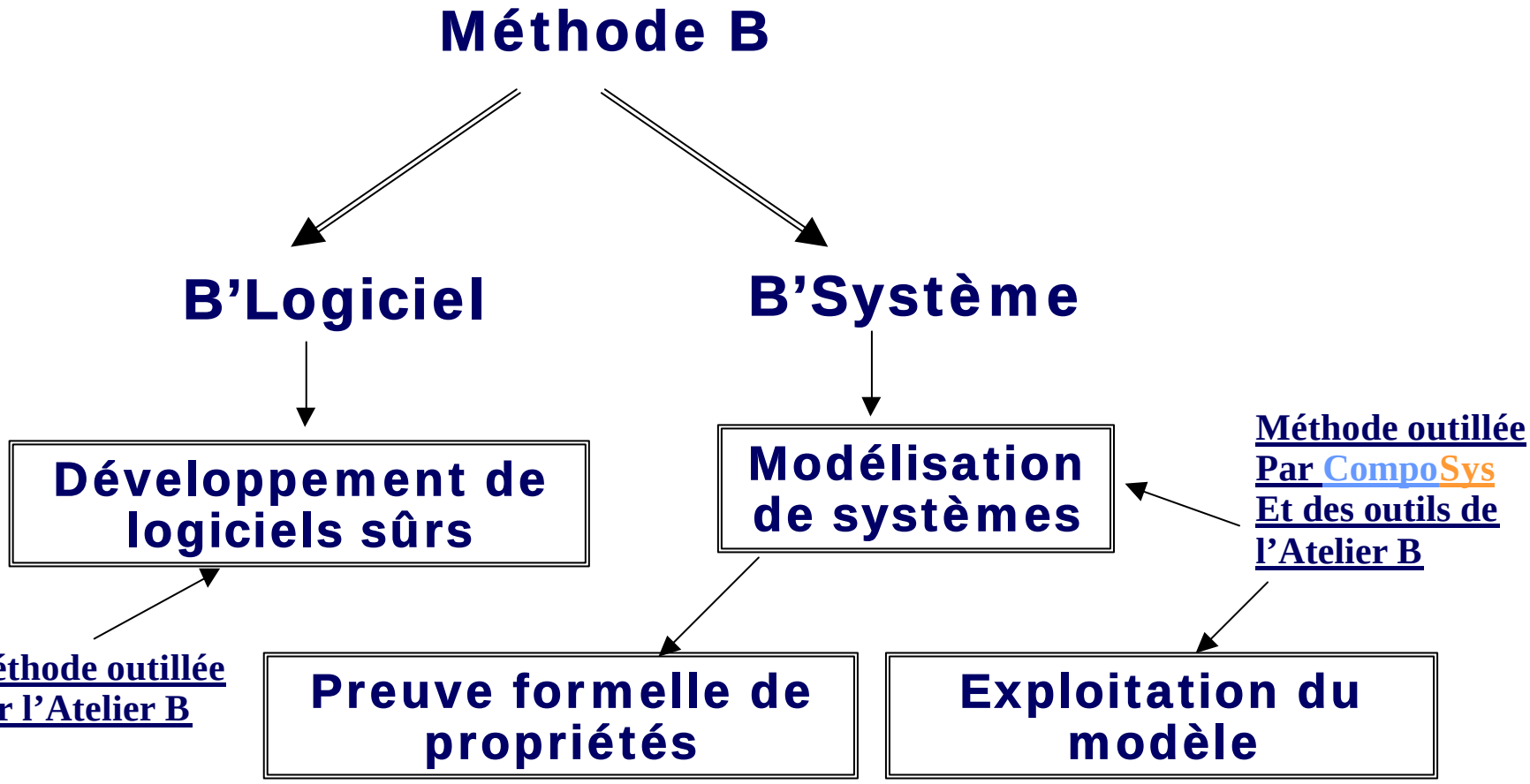
Vérifications automatiques et semi-automatiques de la cohérence ;

Génération automatique du document final et de différentes vues du système

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

B'Système : une méthode outillée basée sur la méthode B



AFIS Association Française d'ingénierie Système

CLEARSY SYSTEM ENGINEERING

Conception générale formelle des sous-systèmes électroniques d'un véhicule

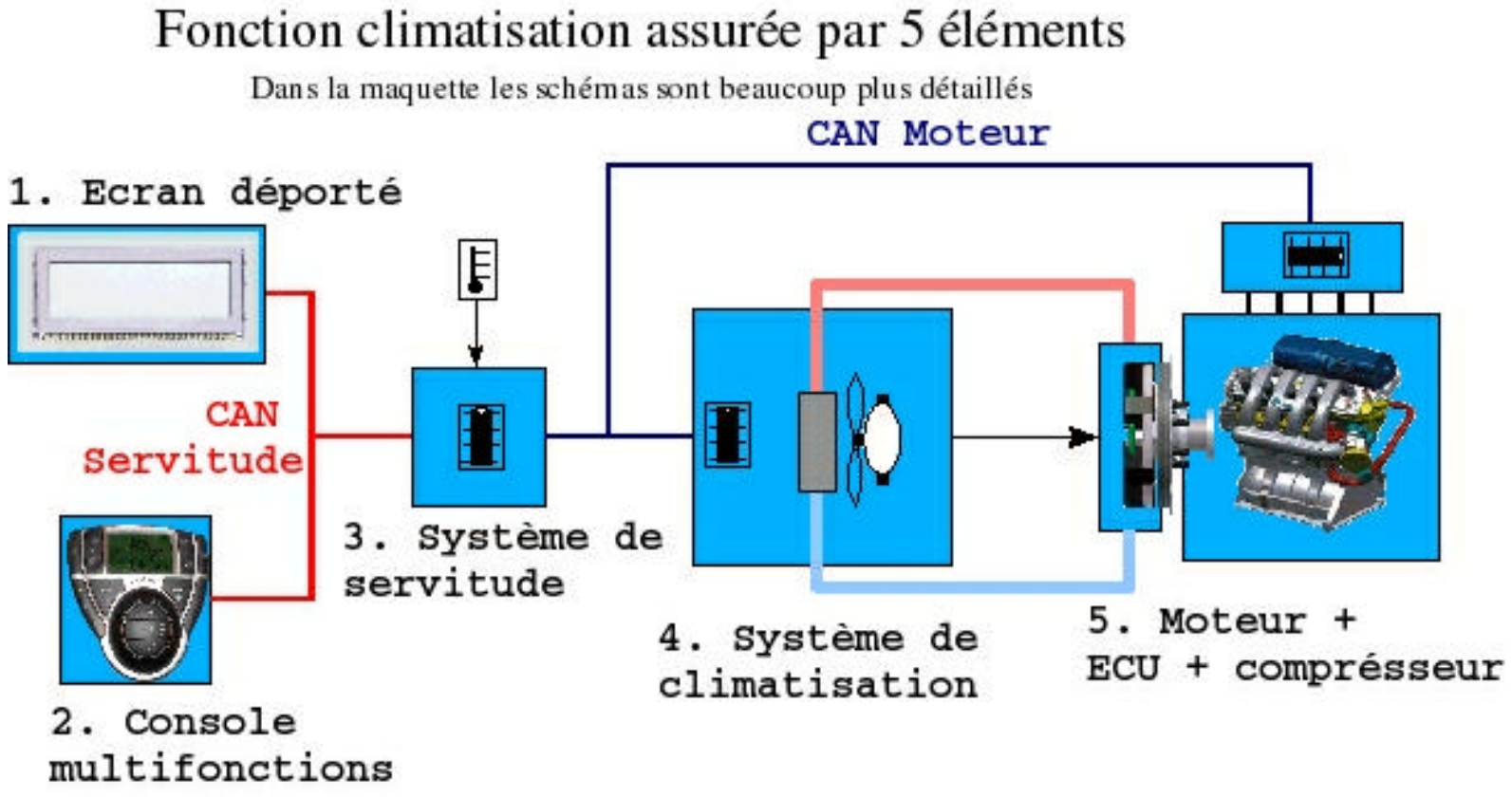
- Notre méthode est basée sur le langage B'Système, qui a été adapté et outillé pour réaliser des descriptions de systèmes électroniques

- L'outil : CompoSys

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Exemples de sous systèmes



Méthode : cinq tâches itératives

1. **Décomposition du système en sous-systèmes**

2. **Recensement des fonctions des sous-systèmes**

3. **Descriptions formelles des fonctions**
   - Quels paramètres et comment elles les utilisent

4. **Description informelle de l'implantation des interfaces dans le système**

5. **Enrichissement du modèle formel**
   - Langage naturel, schémas, autres formalismes.

Exemple de sous-système

1. **Composant : BVA (boîte de vitesse automatique)**

2. **Fonction : en position « drive » la BVA change de vitesse en fonction du régime moteur.**

3. **Description formelle de la fonction :**
   - ✓ Conditions
     - PosBVA = Drive
   - ✓ Description de la fonction
     - Rapport :(

       Rapport : {Neutre, Un, deux, Trois, Quatre} &

       Rapport = StrategieBVA (RegimeMoteur))

Enrichissement du modèle formel

4. Définition des paramètres en langage naturel

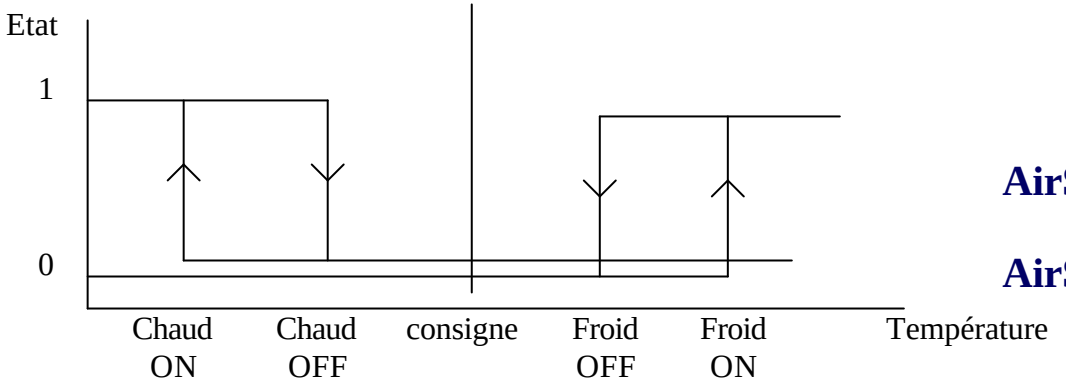
PARAMETER RegimeMoteur CAN

Régime moteur

5. Utilisation d'autres formalismes

PARAMETER « Regul » Algorithme

Fonction de régulation de la température



AirSoufflé : {Chaud, Ambiant, Froid}

AirSoufflé := *Regul*(Température, Consigne)

Définition informelle de la fonction « *Regul* »

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Modèle à double face

- **Face formelle**
  - ✓ Explications non ambiguës
  - ✓ Automatisation des vérifications et calculs des vues
- **Face informelle**
  - ✓ On réalise un lien entre les entités formelles et les entités du système
  - ✓ Toutes les interfaces et les fonctions sont décrites

Face formelle

- **Vérifications Syntaxiques Automatiques**
  - ✓ Vérifications syntaxiques : modèle, liens modèle – langage naturel ...
  - ✓ Vérifications de type, portée des paramètres, ...
  - ✓ Règles de cohérences : environ 50 dans CompoSys.

  Ex : Vérifier que chaque paramètre est utilisé et produit par un sous-système, avec des types de données compatibles

- **Preuves formelles : automatiques / semi-automatiques**
  - ✓ Invariants/Raffinements/Abstractions : techniques pour reformuler les descriptions (utile pour les descriptions compliquées)
  - ✓ Preuves mathématiques que les différentes formulations ne se contredisent pas.

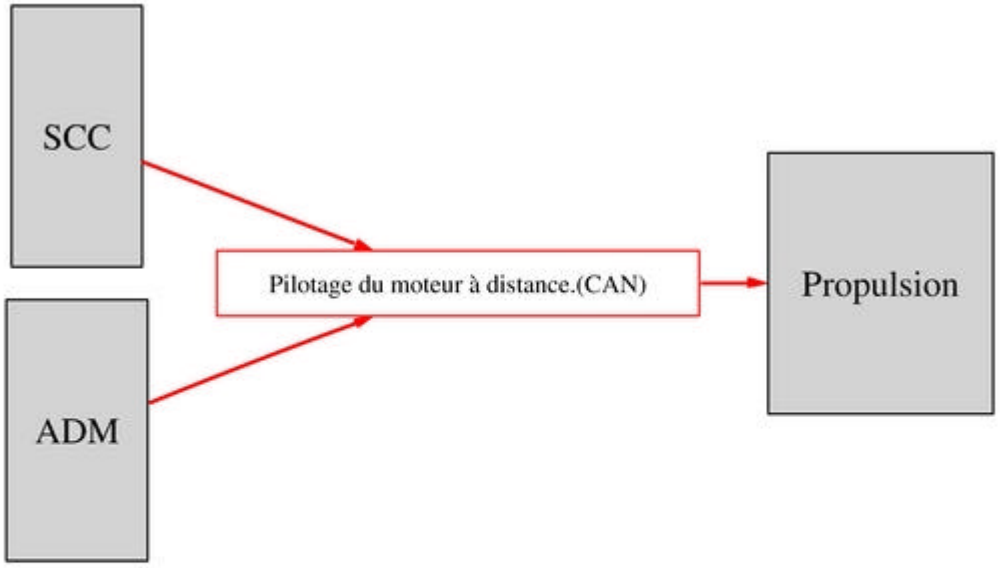
  Exemple d'Invariant : Le véhicule a besoin de courant électrique pour démarrer

  Moteur = Dem => AlimPrincipale = TRUE

- **Génération automatique des vues.**
  - ✓ L'outil génère plusieurs représentations de la même information.

Face informelle

Les vues générées sont en langage naturel



Les opérations qui dépendent de ce paramètre sont:

- Propulsion Pilotage du moteur à distance.

Les opérations qui modifient ce paramètre sont:

- ADM Pilotage des crabots
- SCC Passerelle CAN -> Ethernet

Autres exemples de vues :

- **Matrices réseaux**
- **Réseaux électriques**
- **Vue par composant**
- **Vue par chaîne fonctionnelle**

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Apports de la modélisation

Association Française d'Ingéniarie Système

CLEARSY SYSTEM ENGINEERING

Apports lors de la création du modèle : la précision d'un langage mathématique

- **Les spécifications fonctionnelles :**
  - ✓ Elles sont vérifiées
  - ✓ Elle sont complétées
  - ✓ Des difficultés sont anticipées

Une « pré-intégration » fonctionnelle des composants est réalisée

Apport lors de l'exploitation du modèle

- **Le modèle est une base d'information commune aux activités transverses de :**
  - ✓ Vérifications et intégration
  - ✓ Sûreté de fonctionnement
  - ✓ Dimensionnement des réseaux
    - CAN, électriques, ...
  - ✓ Études d'impact
  - ✓ Formation

Quelques références CompoSys

- **Intégration fonctionnelle du véhicule militaire : SPRAT**

- **Modélisation de 3 véhicules pour le diagnostic : 206, 307, 407**

- **Étude système : façades de quai RATP**

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Point de vue

❑ Principales difficultés techniques :

- ✓ Choix du niveau de formalisation (à confier à une personne expérimentée)
- ✓ Des descriptions formelles multi-métiers (mécanique, électronique, hydraulique, ...) qui requièrent des notions de mathématiques

❑ Principaux avantages

- ✓ Une approche guidée, outillée et éprouvée sur des cas industriels.
- ✓ Très bonne et rapide appréhension du système.
- ✓ Connaissance transmissible et réutilisable.
- ✓ Économique, chiffrable, travail itératif.

Conclusion

- **Le modèle est une « *base d'informations* »**
  - ✓ Sous-systèmes, Fonctions, Paramètres
  - ✓ Que l'on alimente en « expliquant » les fonctions
  - ✓ « Explications » mixtes : B et autre formalisme

- **Utilisation de cette base pour les travaux transverses**
  - ✓ Vérifications de compatibilité entre les composants
  - ✓ SDF, bilans électriques, diagnostic ...
  - ✓ Calculs

- **Une méthode outillée et économique de modélisation en B'Système : COMPOSYS**
  - ✓ Bientôt une version en bêta test.
  - ✓ Actuellement ce type de modélisation est réalisée par ClearSy

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING