



**CLEARSY**  
SYSTEM ENGINEERING

# Les principes de fonctionnement formalisés

Modélisation, en B événementiel, des fonctions mécaniques, électriques et informatiques d'un véhicule

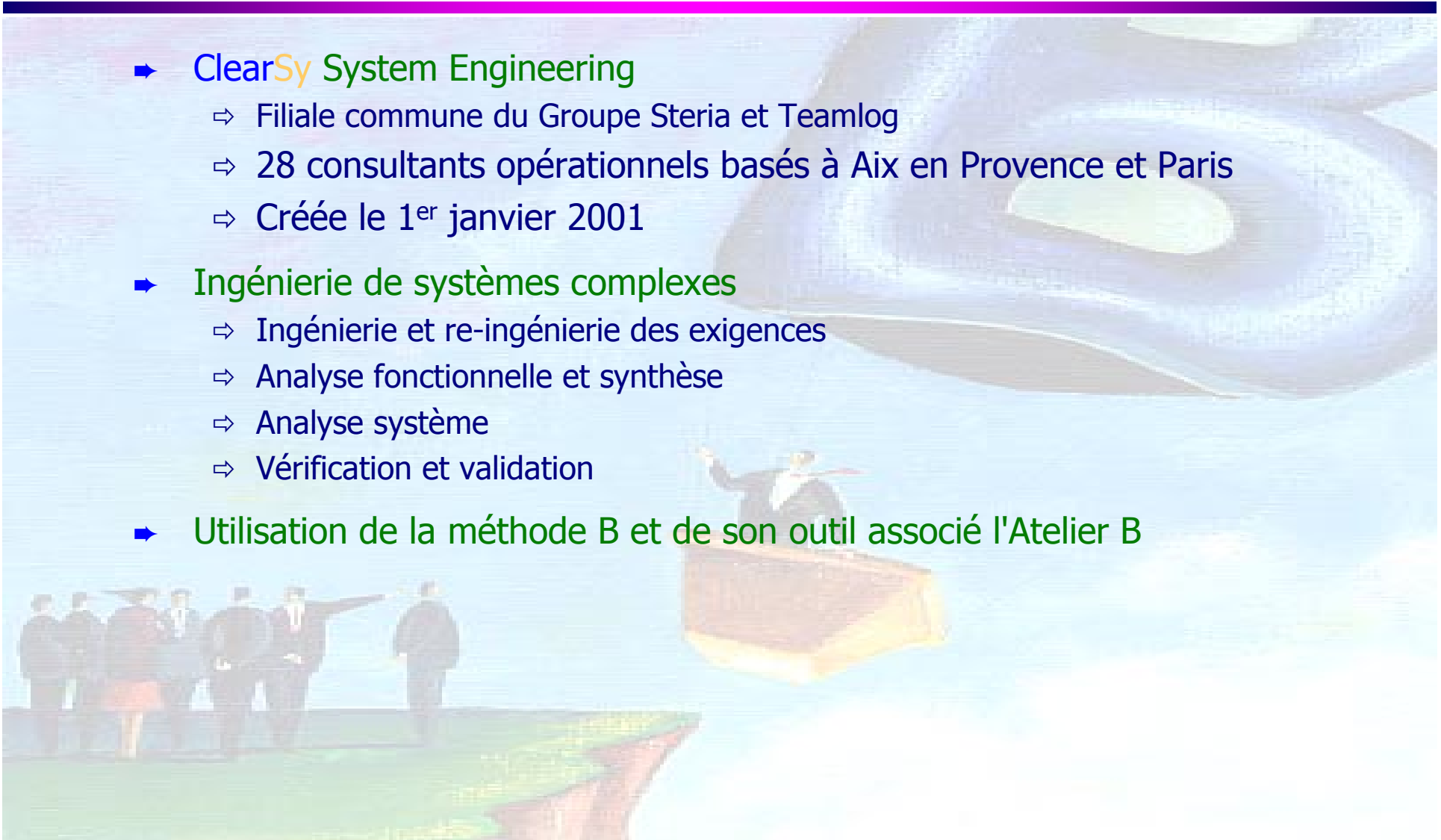




**CLEARSY**  
SYSTEM ENGINEERING

## Présentation de ClearSy

- **ClearSy System Engineering**
  - ⇒ Filiale commune du Groupe Steria et Teamlog
  - ⇒ 28 consultants opérationnels basés à Aix en Provence et Paris
  - ⇒ Créée le 1<sup>er</sup> janvier 2001
- **Ingénierie de systèmes complexes**
  - ⇒ Ingénierie et re-ingénierie des exigences
  - ⇒ Analyse fonctionnelle et synthèse
  - ⇒ Analyse système
  - ⇒ Vérification et validation
- **Utilisation de la méthode B et de son outil associé l'Atelier B**





**CLEARSY**  
SYSTEM ENGINEERING

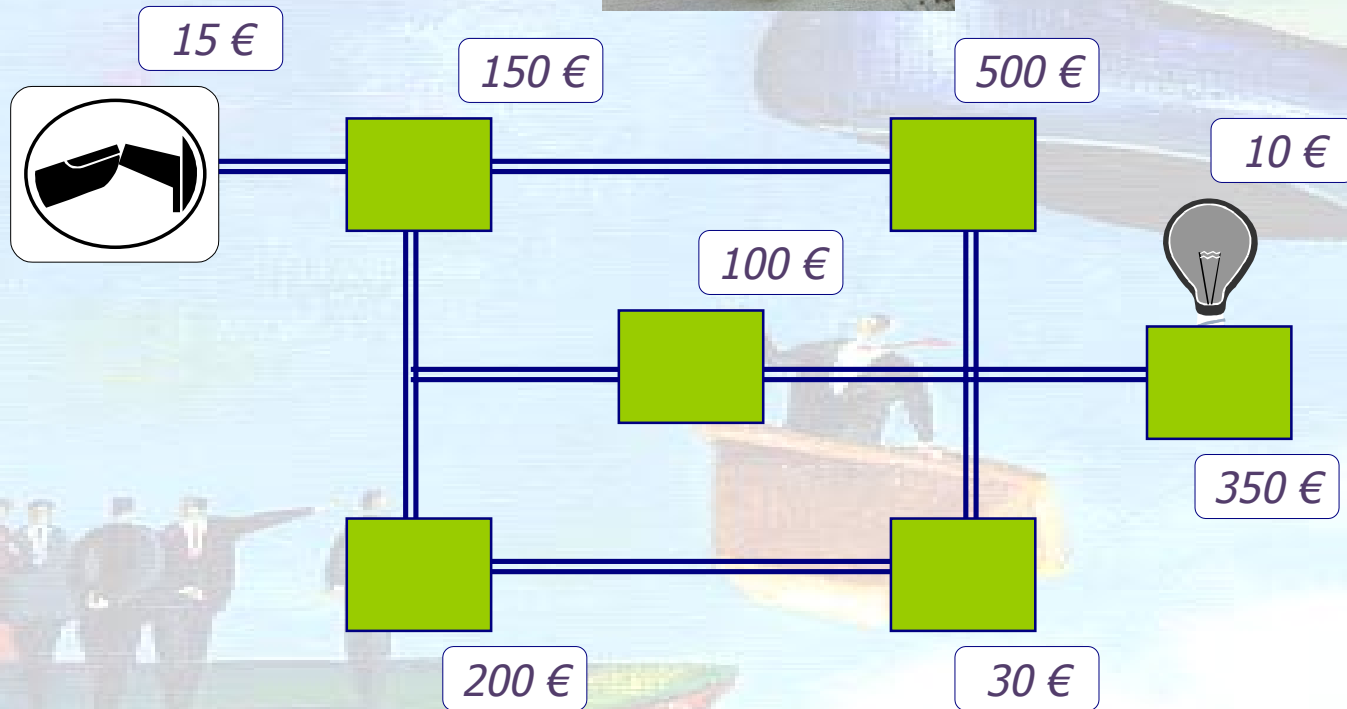
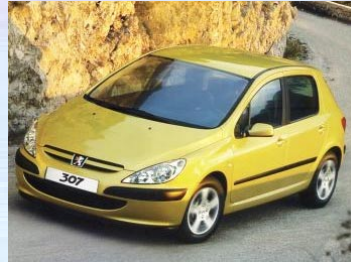
# Les principes de fonctionnements formalisés

- Les PFF sont réalisés pour le SAV « Automobiles Peugeot »
  
- Les PFF sont le résultat d'une expertise des spécifications techniques pour :
  - ⇒ Obtenir et formaliser les informations nécessaires à:
    - Diagnostiquer les pannes
    - Expliquer les nouvelles fonctionnalités au client



**CLEARSY**  
SYSTEM ENGINEERING

# Je change quoi ?





**CLEARSY**  
SYSTEM ENGINEERING

## Changer l'élément qui ne respecte pas ses propriétés de fonctionnement

- **Formaliser les propriétés essentielles de fonctionnement**
  - ⇒ Des éléments électriques, mécaniques
    - ⌚ Capteurs, actionneurs, Moteur, mécanismes de freinage, etc.
  - ⇒ Des éléments à base de calculateurs
  
- **Vérifier si le comportement de chaque élément remplaçable respecte ses propriétés**
  - ⇒ Il faut pouvoir faire le lien entre :
    - ⌚ Le fonctionnement du véhicule (grandeurs physiques)
    - ⌚ Les propriétés du modèle (variables abstraites)



**CLEARSY**  
SYSTEM ENGINEERING

## Trouver les propriétés essentielles

### ➤ La documentation technique

- ⇒ Première source d'information (50.000 pages)
- ⇒ Niveaux de détails très hétérogènes :
  - Détails de conceptions
  - Principes généraux
  - Quelques ambiguïtés, contradictions
  - Certains documents ne sont pas à jour

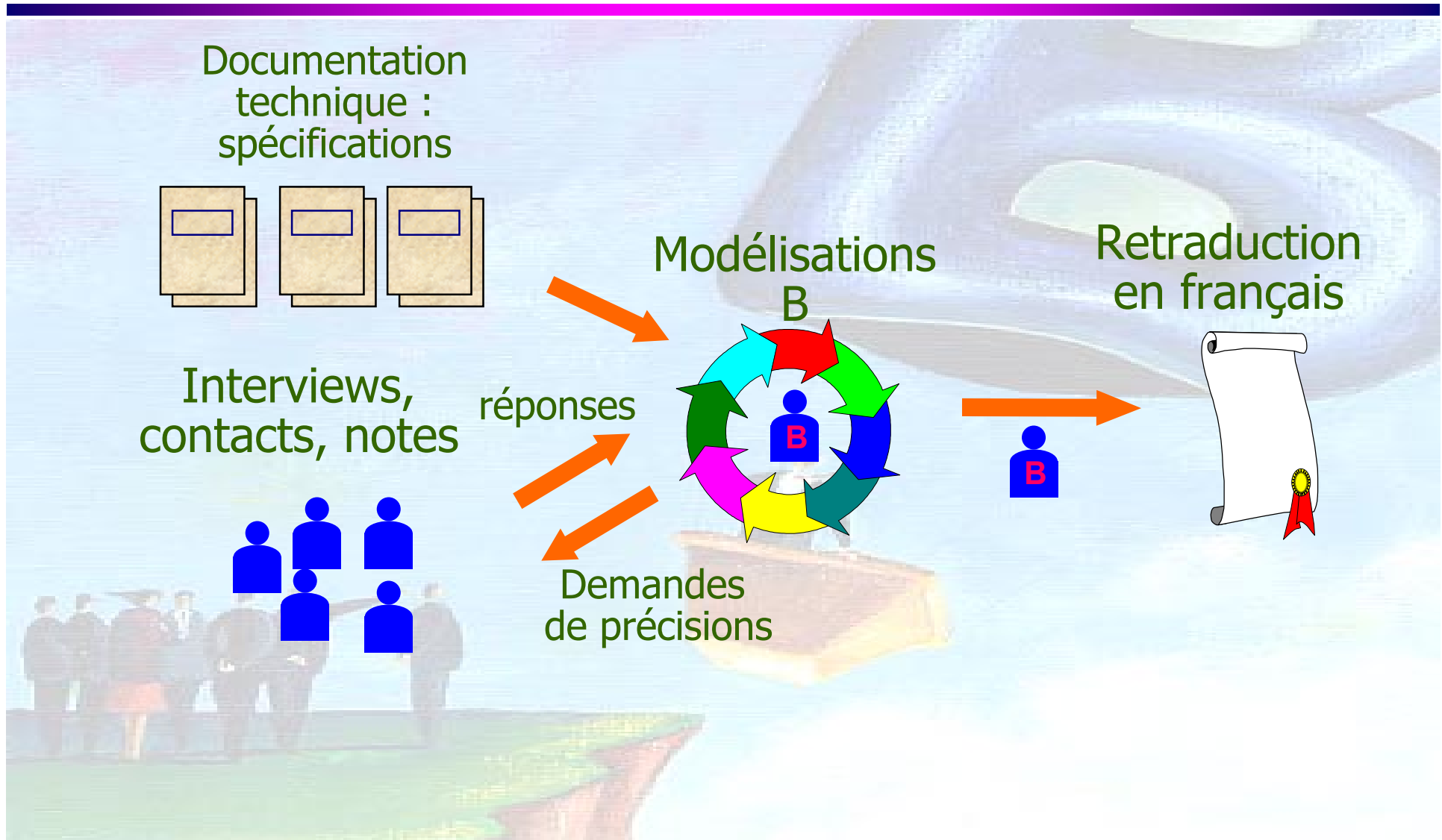
### ➤ La formalisation sert de réceptacle aux informations

- ⇒ La formalisation évite de se perdre dans la documentation technique
  - Il faut y extraire les propriétés fonctionnelles (PFF = 1500 pages)
- ⇒ La formalisation permet d'être cohérent
- ⇒ La formalisation permet de poser des questions précises

### ➤ Interview

- ⇒ Retrouver les propriétés essentielles
- ⇒ Obtenir les informations manquantes
- ⇒ Valider les hypothèses

# Processus de modélisation



# Quelques règles de formalisations

- ▶ **Les modèles sont en B événementiel**
  - ⇒ Un seul niveau de raffinement modélisé
  - ⇒ Utilisation de la preuve pour la cohérence interne des modèles
  - ⇒ Utilisation de quelques propriétés invariantes
  
- ▶ **Les propriétés sont exprimées par élément remplaçable:**
  - ⇒ Chaque événement B n'est associé qu'à un seul élément remplaçable
  - ⇒ Chaque variable B n'est associée qu'à un seul élément remplaçable
  - ⇒ Un événement ne peut modifier que les variables du même élément remplaçable
  
- ▶ **Le modèle décrit les propriétés d'un élément sain :**
  - ⇒ Dans un environnement sain
  - ⇒ Dans un environnement dégradé : si prévu par le constructeur
  - ⇒ On construit une abstraction et non pas une simplification du comportement réel



**CLEARSY**  
SYSTEM ENGINEERING

## Exemple : capteur du type thermistance

- Propriété modélisée : c'est le capteur qui mesure la température de l'huile
- Modèle du capteur  
EvtCapteur =  
BEGIN  
Vcapteur :∈ {Nominal, Chaud}  
END
- Définitions informelles
  - ⇒ Vcapteur = « Nominal », si la température du noyau est inférieure à 150°C
  - ⇒ Vcapteur = « Chaud », si la température du noyau est supérieure à 150°C



**Il est important de formaliser uniquement les propriétés essentielles**

**CLEARSY**  
SYSTEM ENGINEERING

- ➔ **Nous aurions pu formaliser:**
  - ⇒ Que la résistance électrique ( $R_e$ ) varie en fonction de la température du noyau ( $T_n$ ) :  $R_e = f(T_n)$
  - ⇒ Que l'inertie thermique de la sonde provoque un décalage entre la température de l'huile et  $T_n$ .
  - ⇒ Etc.
- ➔ **Mais nous ne les avons pas formalisées car :**
  - ⇒ La première est une propriété approximative
  - ⇒ La seconde est un effet secondaire
- ➔ **Il faut éviter la formalisation de propriétés superflues car :**
  - ⇒ Elles augmentent le prix de la modélisation
  - ⇒ On risque d'introduire des « bugs » de description
  - ⇒ Elles ne servent pas à identifier un élément défaillant

# Comment faire le lien entre la voiture et le modèle ?

## ■ Propriétés essentielles

### **MACHINE**

Huile

### **OPERATIONS**

EvtChangementMode =

### **SELECT**

VcAlim = ON

### **THEN**

VcEmission :(

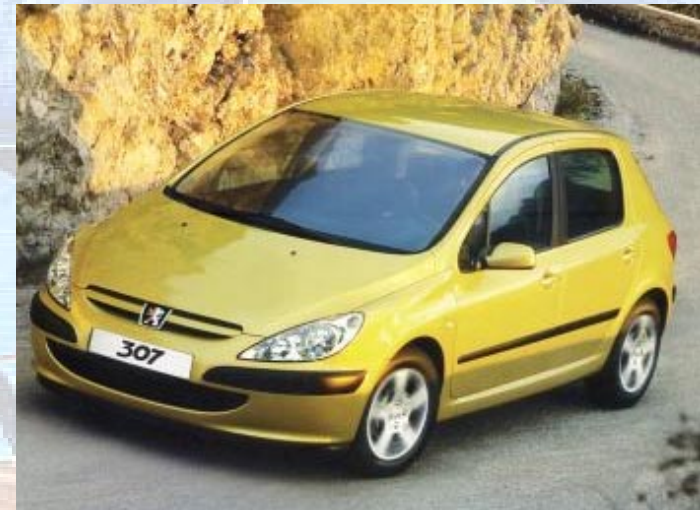
(Vcapter : {CC, CO} =>  
VcEmission = Secours) &

(Vcapter : {Chaud,  
Nominal} => VcEmission =  
Nominale))

**END ;**



## ■ Voiture réelle



# Faire le lien entre la voiture physique et le modèle

- L'opérateur observe des paramètres physiques et des événements réels (observables)
  - ⇒ Température, tension électrique, bruits, couleurs, enregistrements réseaux ...
  - ⇒ Ouverture d'une porte, freinage d'urgence, démarrage ...
- Le modèle est composé de variables et d'événements B
- Il faut définir les variables en fonction des observables, pour que:
  - ⇒ Quelque soit l'état du véhicule il faut pouvoir déterminer si:
    - ⊕ Il respecte les propriétés formalisées dans le modèle : normal
    - ⊕ Il ne respecte pas les propriétés : en panne
    - ⊕ Il est en dehors du périmètre de modélisation
- Il faut définir les observables sur un domaine de valeurs
  - ⇒ Les observables et leurs domaines déterminent les limites du modèle



**CLEARSY**  
SYSTEM ENGINEERING

## Exemples d'observables

### ➔ Observables et leurs domaines

#### ⇒ Observation d'un réseau

##### ⇒ Valeur d'un paramètre réseau

– Domaine : 0 .. 255 pour une grandeur codée sur 1 octet

##### ⇒ Fréquence d'émission : 0 .. 10 Hz

#### ⇒ Observation d'un paramètre physique

##### ⇒ Température : -30° .. 200°C

##### ⇒ Régime moteur : 0 .. 10 000 tr/min

#### ⇒ Observation qualitative

##### ⇒ Bruit du moteur: Aucun, démarreur, Simple injection, post-injection

##### ⇒ Luminosité d'une ampoule : nulle, réglementaire, bizarre



**CLEARSY**  
SYSTEM ENGINEERING

# Restrictions sur les observables

- Il faut rester dans les limites des spécifications des éléments remplaçables:
  - ⇒ Quel est le comportement normal d'un ordinateur :
    - Lorsqu'il est alimenté en 250V alternatif ?
    - Alors qu'il est prévu pour fonctionner en 12V continu !
  - ⇒ Le constructeur ne spécifie pas le fonctionnement en 250V
    - Le domaine de valeur est restreint aux données du constructeur : 0 .. 16V
- Il faut associer un moyen de mesure à un observable
- La définition d'une variable est de la forme:
  - Les observables : O1, O2, .. On
  - **Variable** = **definition**(O1, O2, .. On)
  - **Variable** : Dv & O1, O2, .. On : D1xD2x..Dn
  - **Definition** est une fonction définie de D1xD2x..Dn → Dv



**CLEARSY**  
SYSTEM ENGINEERING

# Définition complète de $V_{\text{capteur}}$

## ➤ Définition de $V_{\text{capteur}}$

⇒ La résistance électrique ( $R_e$ ) varie en fonction de la température du noyau ( $T_n$ ) :  
 $R_e = f(T_n)$

➤  $V_{\text{capteur}} \in \{\text{Nominal}, \text{Chaud}, \text{CC}, \text{CO}, \text{Bizarre}\} \&$

➤  $f \in -30..200 \rightarrow 51..2500 \&$

➤ Quelque soit  $T_n \in -30 .. 200 \Rightarrow$

-  $R_e = f(T_n) \Rightarrow$

•  $T_n < 150 \Rightarrow V_{\text{capteur}} = \text{Nominal}$

•  $T_n \geq 150 \Rightarrow V_{\text{capteur}} = \text{Chaud}$

-  $R_e \neq f(T_n) \Rightarrow$

•  $R_e \in 0 .. 50 \Rightarrow V_{\text{capteur}} = \text{CC}$

•  $R_e \in 51 .. 2500 \Rightarrow V_{\text{capteur}} = \text{Bizarre}$

•  $R_e > 2500 \Rightarrow V_{\text{capteur}} = \text{CO}$

## ➤ La définition des variables fait le lien entre:

⇒ Les variables B abstraites et les paramètres physiques

➤ La définition peut être informelle



**CLEARSY**  
SYSTEM ENGINEERING

## Rappel du modèle de la thermistance

### ➤ Modèle du capteur

EvtCapteur =

BEGIN

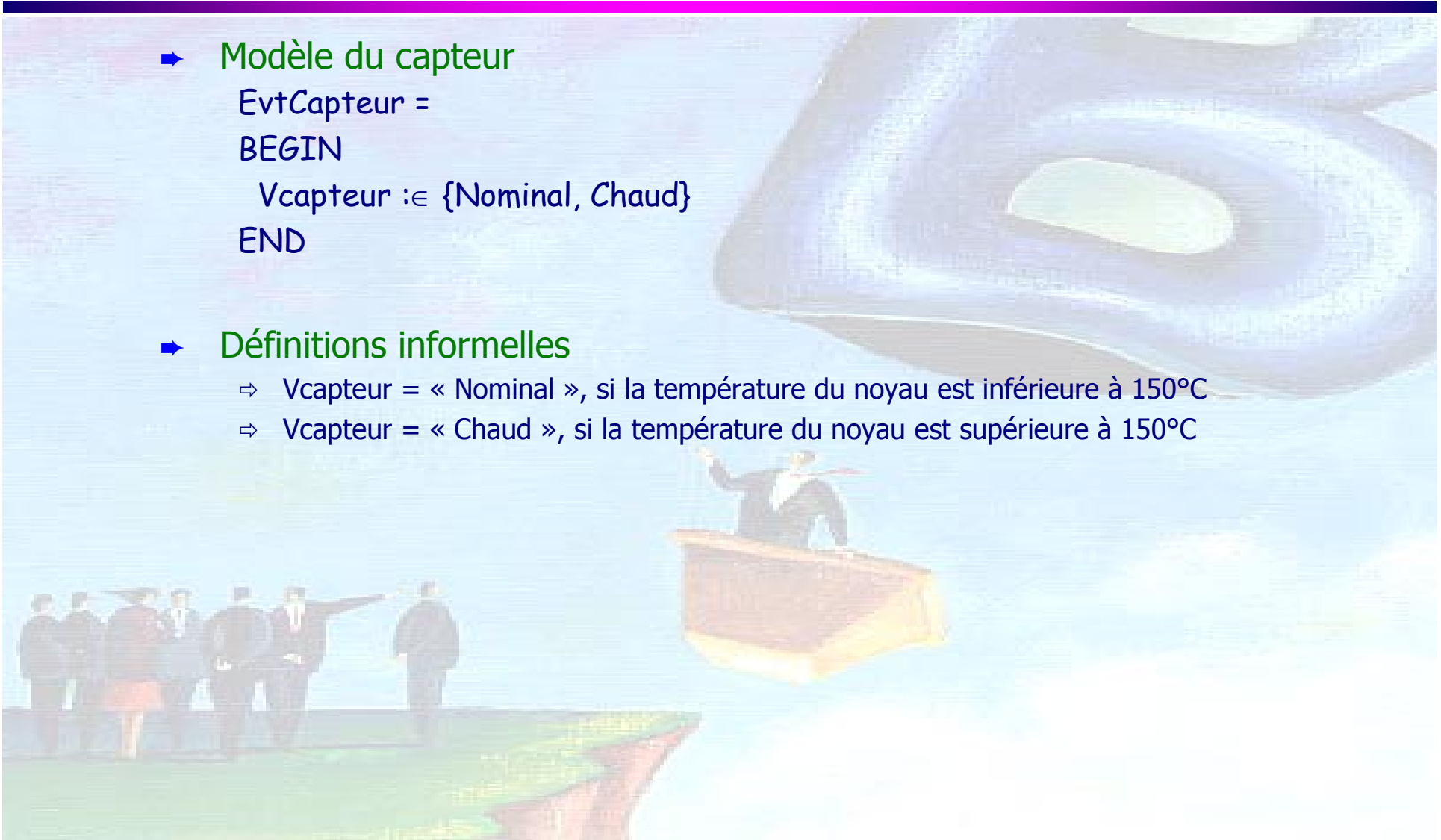
Vcapteur :∈ {Nominal, Chaud}

END

### ➤ Définitions informelles

⇒ Vcapteur = « Nominal », si la température du noyau est inférieure à 150°C

⇒ Vcapteur = « Chaud », si la température du noyau est supérieure à 150°C



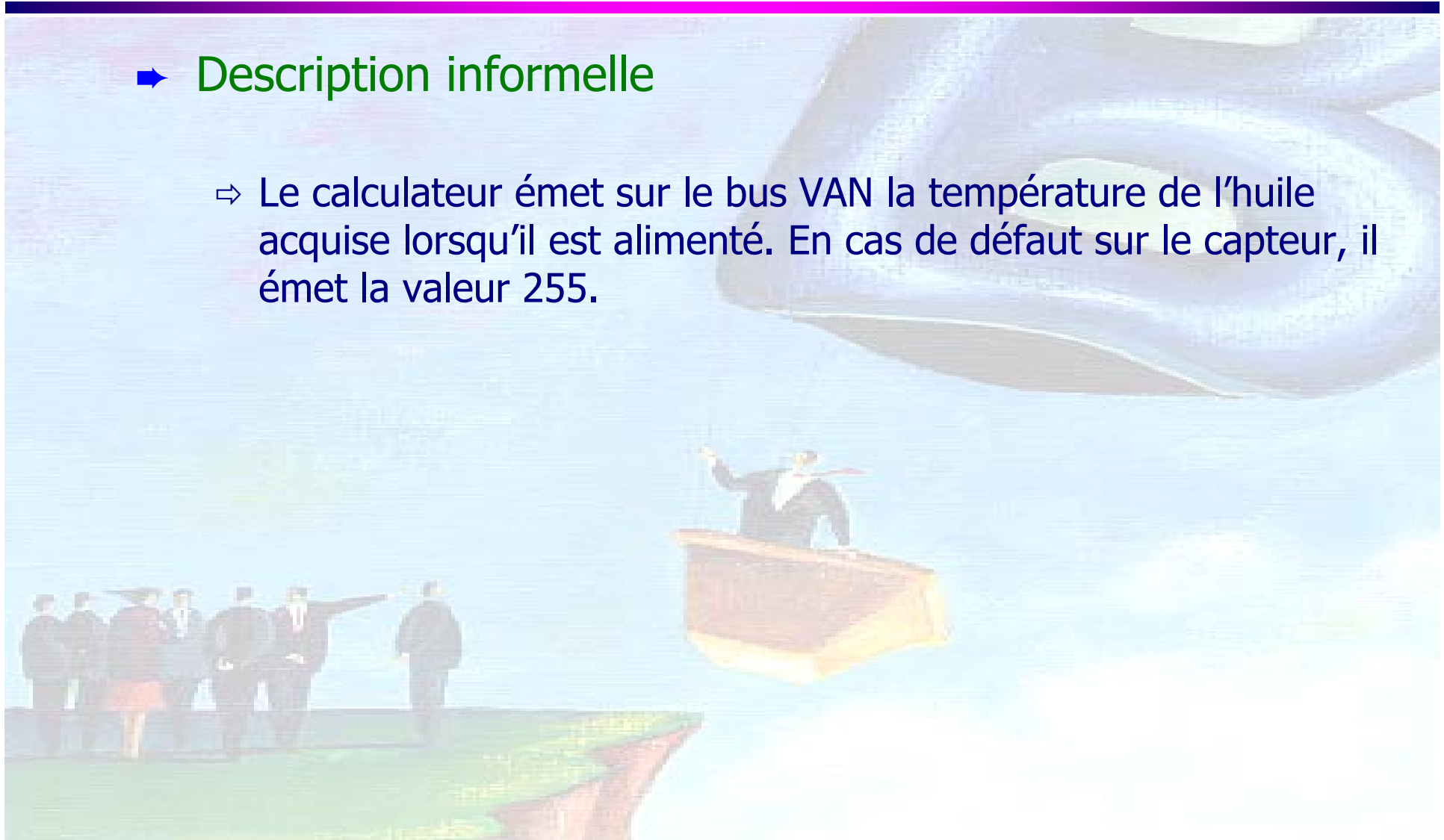


**CLEARSY**  
SYSTEM ENGINEERING

## Acquisition de la température d'huile par le calculateur

### ➔ Description informelle

- ⇒ Le calculateur émet sur le bus VAN la température de l'huile acquise lorsqu'il est alimenté. En cas de défaut sur le capteur, il émet la valeur 255.





**CLEARSY**  
SYSTEM ENGINEERING

## Exemple : Acquisition de la température d'huile par le calculateur

```
EvtAlimentation =  
SELECT  
  VcAlim = OFF  
THEN  
  VcEmission :(  
    (Vcapter : {CC, CO} => VcEmission = Secours) &  
    (Vcapter : {Chaud, Nominal} => VcEmission = Nominale)) ||  
  VcAlim := ON  
END ;
```

```
EvtChangementMode =  
SELECT  
  VcAlim = ON  
THEN  
  VcEmission :(  
    (Vcapter : {CC, CO} => VcEmission = Secours) &  
    (Vcapter : {Chaud, Nominal} => VcEmission = Nominale))  
END ;
```

```
EvtVeille =  
SELECT  
  VcAlim = ON  
THEN  
  VcAlim := OFF ||  
  VcEmission := NonEmis  
END
```

## ➤ Définition de « VcAlim »

⇒ VcAlim est définie par la tension (U) aux bornes du connecteur d'alimentation

➤  $U = 0 \Rightarrow VcAlim = OFF$

➤  $U \in 10 .. 16 \Rightarrow VcAlim = ON$

➤  $U \in 1 .. 9 \Rightarrow VcAlim = Défaillante$

## ➤ Définition de « VcEmission »

⇒ VcEmission est définie avec les observables suivants :

➤ La fréquence (Freq) d'émission du message « température d'huile »

➤ La valeur du message (Val)

➤ La résistance (Re) du capteur



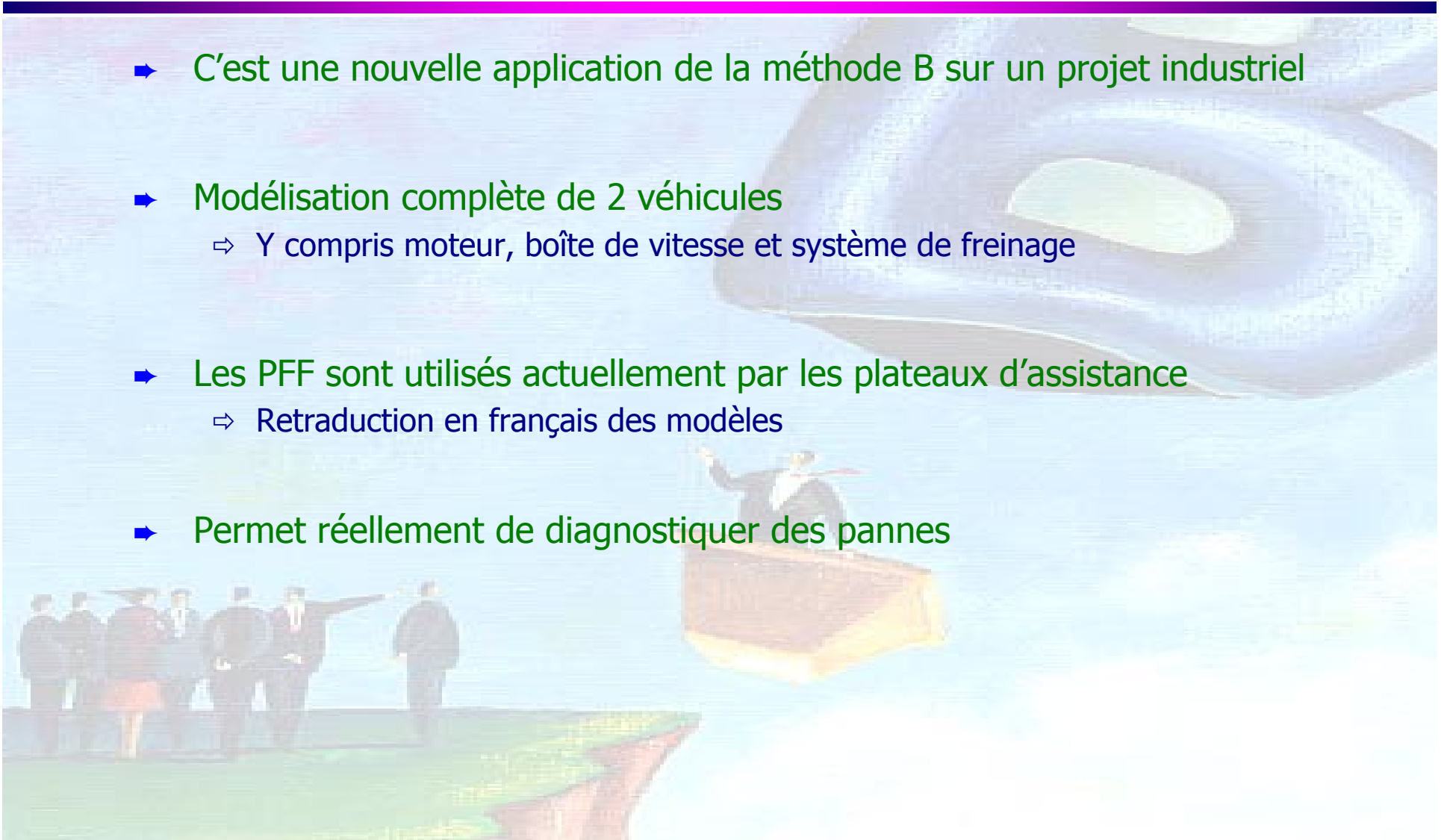
**CLEARSY**  
SYSTEM ENGINEERING

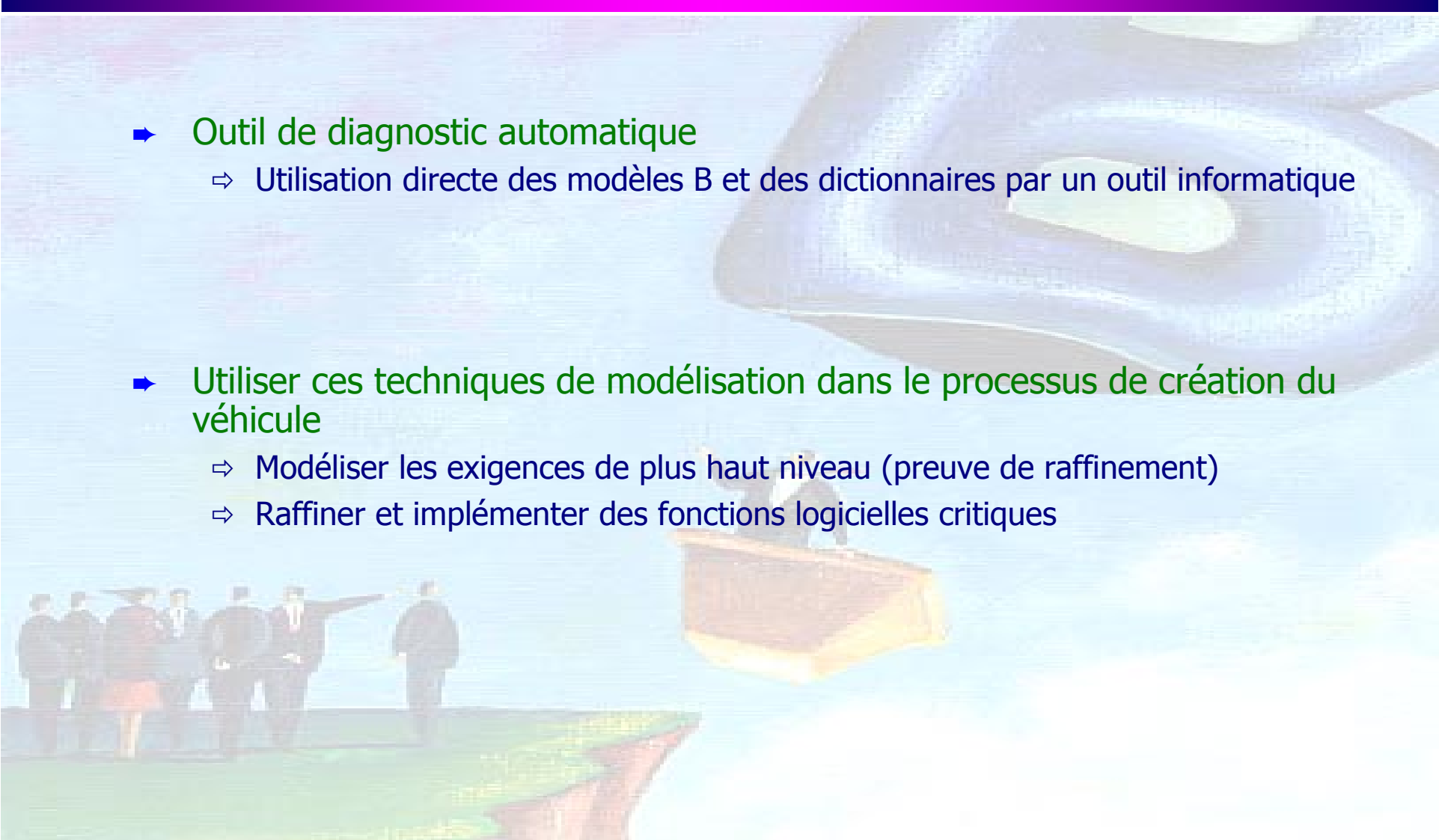
## Dictionnaire suite

- ⇒  $\text{Freq} \in 0 \dots 1000$  &
- ⇒  $\text{Val} \in 0 \dots 255$  &
- ⇒  $\text{Re}$  est un naturel &
- ⇒  $\text{VcEmission} \in \{\text{Nominale}, \text{Secours}, \text{NonEmis}, \text{Défaillante}\}$  &
  - ⊙  $\text{Freq} \geq 200 \Rightarrow$ 
    - $\text{Re} \in 51 \dots 2500 \Rightarrow$ 
      - $\text{Val} = f^{-1}(\text{Re}) + 30 \Rightarrow \text{VcEmission} = \text{Nominale}$
      - $\text{Val} \neq f^{-1}(\text{Re}) + 30 \Rightarrow \text{VcEmission} = \text{Défaillante}$
    - $\text{Re} \notin 51 \dots 2500 \Rightarrow$ 
      - $\text{Val} = 255 \Rightarrow \text{VcEmission} = \text{Secours}$
      - $\text{Val} \neq 255 \Rightarrow \text{VcEmission} = \text{Défaillante}$
  - ⊙  $\text{Freq} = 0 \Rightarrow \text{VcEmission} = \text{NonEmis}$
  - ⊙  $\text{Freq} = 1..199 \Rightarrow \text{VcEmission} = \text{Défaillante}$

## Conclusion

- C'est une nouvelle application de la méthode B sur un projet industriel
- Modélisation complète de 2 véhicules
  - ⇒ Y compris moteur, boîte de vitesse et système de freinage
- Les PFF sont utilisés actuellement par les plateaux d'assistance
  - ⇒ Retraduction en français des modèles
- Permet réellement de diagnostiquer des pannes



- 
- **Outil de diagnostic automatique**
    - ⇒ Utilisation directe des modèles B et des dictionnaires par un outil informatique
  - **Utiliser ces techniques de modélisation dans le processus de création du véhicule**
    - ⇒ Modéliser les exigences de plus haut niveau (preuve de raffinement)
    - ⇒ Raffiner et implémenter des fonctions logicielles critiques