

Formalisation de principes de fonctionnement

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

Guilhem Pouzancre — Jean-Philippe Pitzalis

ClearSy Europarc de Pichaury - Bat C2

1330, avenue G.G. de la Lauzière

F-13856 Aix-en-Provence Cedex 3

{guilhem.pouzancre,jean-philippe.pitzalis}@clearsy.com

RÉSUMÉ. Cet article présente la méthode employée pour formaliser, en B événementiel, les lois de fonctionnement d'un véhicule entier (parties électroniques, mécaniques, subjectives), afin d'améliorer son diagnostic.

ABSTRACT. In this paper, we introduce a method to formalize electronics, mechanics and subjective car behaviour. We use the formal models to diagnose the reason of any car failure (mechanic failures and bugs). This method is based on event B method and rigorous variable and event definitions.

MOTS-CLÉS : B, B événementiel, automobile, diagnostic, modèle, formalisation, ingénierie de systèmes complexes.

KEYWORDS: event-B, B model, automobile industry, diagnostic, formal method, system engineering.

1. Introduction

Avec l'arrivée massive de l'électronique embarquée, les fonctionnalités proposées par les constructeurs automobiles sont devenues de plus en plus complexes : les phares et les essuie-glaces s'allument automatiquement, le moteur règle finement la puissance disponible, le volume de l'autoradio varie en fonction de la vitesse, etc.

Les réparateurs automobiles sont confrontés à de nouveaux problèmes avec ces fonctions, qui dépendent de plusieurs calculateurs et actionneurs répartis sur des réseaux informatiques internes au véhicule (multiplexage). Un dysfonctionnement d'un capteur de vitesse peut entraîner un mauvais fonctionnement de votre autoradio ou du toit ouvrant. Une panne peut aussi être la conséquence d'un cas de fonctionnement non prévu par le concepteur ou d'un «bug» informatique. Par ailleurs, le réparateur doit maîtriser parfaitement la fonctionnalité pour isoler les véritables pannes, ou répondre à un client qui se plaint d'une mauvaise compréhension du comportement de son véhicule.

Afin d'appréhender ces nouveaux problèmes, les services après-vente doivent se munir de nouvelles méthodes et de nouveaux outils. Le diagnostic embarqué (ou autodiagnostic) permet déjà de couvrir une partie des pannes (le calculateur détecte certains courts-circuits ou circuits ouverts). Mais cet autodiagnostic a ses limites car il est lui-même une nouvelle fonctionnalité et peut, lui aussi, être mal compris ou sujet à des anomalies et des pannes.

Nous proposons une méthode formelle, consistant à vérifier si le comportement du véhicule réel respecte les lois de fonctionnement. Les lois sont formalisées en B événementiel avec un modèle par domaine de fonctionnalités : par exemple, gestion de l'éclairage, commande du moteur, boîte de vitesse automatique, etc.

Le dictionnaire des variables et le dictionnaire des événements (paragraphe 4) permettent de faire le lien entre la formalisation et le véhicule physique. Un modèle associé à ses deux dictionnaires constitue ce que nous appelons un «principe de fonctionnement formalisé», qui peut être utilisé directement par des spécialistes B, par un outil informatique, mais aussi par le personnel du service après-vente car nous le présentons dans un document en langage naturel.

Par ailleurs, cet article explique le contenu des modèles (paragraphe 2) et les règles de modélisation (paragraphe 3) utilisés pour obtenir les «principes de fonctionnement formalisés».

Le paragraphe 5 termine l'article en présentant le modèle et les dictionnaires d'une fonctionnalité d'un calculateur.

2. Le contenu des modèles

Le modèle B formalise les propriétés essentielles de fonctionnement que doit respecter le véhicule avec un niveau de détail constant. En effet, le niveau de détail est

essentiel, car c'est lui qui détermine d'une part le coût de la réalisation et d'autre part l'adéquation des principes de fonctionnement avec leur objectif, qui est de permettre d'identifier un éventuel élément défaillant. Il n'est pas nécessaire d'aller plus en détail car il n'appartient pas au garagiste de le réparer, mais seulement de l'identifier et de le remplacer.

Les propriétés du fonctionnement sont extraites des spécifications techniques du constructeur. Le niveau de détail est très hétérogène d'un document à l'autre. Les documents, qui traitent d'éléments spécifiques au constructeur ou de points nouveaux, donnent une description proche de la conception. Les propriétés sont formalisées en B événementiel, en faisant un effort d'abstraction pour éviter de modéliser les détails inutiles. Au contraire, il n'y aura pas suffisamment d'informations pour les produits livrés «clef en main» ou les parties sans difficulté de conception particulière. Il faut alors interroger le constructeur ou les fournisseurs pour avoir des compléments d'informations.

Les modèles couvrent des fonctionnalités «logicielles», mais aussi mécaniques (freinage, moteur, boîtes de vitesses) ou électriques.

3. Les règles de modélisation

En plus des règles de modélisation du B événementiel, il faut savoir précisément quel est le rôle de chaque élément remplaçable dans n'importe quel scénario. C'est pourquoi il est important de modéliser les propriétés par élément et non pas pour un ensemble d'éléments. Pour cela, chaque variable et chaque événement B est associé à un seul élément remplaçable. Ainsi, chaque événement représente la réaction d'un seul élément à une excitation donnée et n'applique une action que sur les variables du même élément. Si un même événement doit modifier les variables de deux éléments fonctionnels séparés, on crée deux événements couplés par une variable de phase. C'est le cas par exemple, lorsque la poignée d'une portière arrive en butée haute, la porte est simultanément libérée par le système de verrouillage qui est un élément séparé mais relié à la poignée par une biellette.

Par ailleurs, il est important que le modèle soit la traduction en B de la compréhension naturelle de la fonction. Autrement dit, il ne faut pas représenter le fonctionnement sous forme d'algorithme ou d'enchaînement complexes d'événements B. C'est le point qui nécessite le plus d'expérience de modélisation, car il faut s'abstraire de la forme des documents de référence, mais cet effort est essentiel pour ne pas diluer les propriétés essentielles dans des points de détail et pour éviter les «bugs» de description.

Nous allons illustrer notre démarche sur un exemple concret : la fonction de surveillance de la température d'huile.

Cette fonction est composée, entre autres, d'un capteur de température d'huile et d'un calculateur qui alerte le conducteur en cas de température excessive. Le capteur

est du type thermistance, sa résistance électrique (Re) varie en fonction (f) de la température de son noyau (Tn). La fonction f du capteur est définie de $-30..200^{\circ}\text{C}$ sur $51..2500$ Ohms. Le conducteur est alerté lorsque $Tn \geq 150^{\circ}\text{C}$.

Nous voulons modéliser comme propriété essentielle que le calculateur prend ses décisions sur les indications données par le capteur. L'événement «*EvtCapteur*» modifie la valeur du capteur en indiquant que «*Vcapteur*» peut prendre une des deux valeurs de l'ensemble après le symbole « $::$ » :

```

EvtCapteur =
BEGIN
  Vcapteur :: {Nominal, Chaud}
END

```

La définition complète de la variable *Vcapteur* et de l'événement *EvtCapteur* sont données dans le paragraphe 4. Ici, nous introduisons les cas de fonctionnement normal de la façon suivante :

- *Vcapteur* = Nominal si la température du noyau est inférieure à 150°C et $Re = f(Tn)$
- *Vcapteur* = Chaud si la température du noyau est supérieure ou égale à 150°C et $Re = f(Tn)$
- *EvtCapteur* modélise les changements lorsque la température du noyau passe au-dessus et en dessous de 150°C .

4. Les dictionnaires

Le modèle du capteur ci-dessus n'a aucun sens s'il n'est pas accompagné du paragraphe de définition. Ces définitions se trouvent dans le dictionnaire des variables et le dictionnaire des événements. Les dictionnaires font le lien entre la voiture concrète et le modèle. Par leur intermédiaire on peut dire si le comportement de chaque élément remplaçable est normal (respectant la spécification), anormal (panne ou bug) ou hors du périmètre de modélisation.

4.1. Dictionnaire des variables

Le dictionnaire des variables est construit en associant à chaque variable un ensemble d'observables. Les observables sont les paramètres à prendre en compte pour observer le véhicule et ils sont définis sur un domaine de valeurs.

La méthode employée pour choisir les observables reste informelle et intuitive ; nous l'illustrons par quelques exemples :

- Le choix naturel du paramètre d'observation d'un interrupteur est la position de la partie mobile ; de même, pour un voyant, l'intensité lumineuse et la couleur émise sont les paramètres les plus intuitifs. Mais d'autres paramètres sont possibles, nous

pourrions choisir comme observable le bruit de l'interrupteur ou la chaleur dissipée par le voyant. Pour faire ce choix de paramètres, il faut se rappeler l'objectif des modèles qui est la réparation des éléments. Il est extrêmement rare qu'un client se plaigne de la chaleur émise par un voyant.

- Une fois les observables fixés, il faut choisir un domaine de valeurs pour ces observables. On peut considérer uniquement deux positions pour un interrupteur (ouvert et fermé) ou retenir toutes les positions, y compris les intermédiaires. Dans le premier cas, le modèle n'est pas applicable lorsque l'interrupteur est dans une position transitoire, il ne permet pas de savoir si le comportement est normal.

- Pour un capteur, qui transforme une grandeur physique en un signal électrique, les observables généralement choisis sont : la grandeur physique (par exemple la vitesse du véhicule) ou la tension, la fréquence, la résistance, l'intensité, selon la technologie employée.

- Il existe aussi des paramètres plus complexes mais néanmoins à prendre en compte car ils sont observables par le client. Par exemple, les bruits de combustion du moteur, les à-coups dus à l'élasticité de traction. Pour les valeurs de ces observables, on utilise des critères qualitatifs tels que : le «bruit normal» ou l'«éclairage réglementaire».

- Pour un calculateur, l'observation est effectuée par ses entrées-sorties analogiques ou numériques ; ainsi, on utilisera les valeurs des trames émises ou reçues sur une liaison multiplexée. En revanche, sauf exception, la température du calculateur n'est pas choisie comme «observable».

Dans le cas du modèle de la thermistance, présenté dans le paragraphe 3, les observables retenus sont : la résistance électrique (R_e), la température du noyau (T_n) et la fonction f .

Les valeurs choisies pour un observable dépendent aussi des limites des spécifications des éléments car pour toutes ces valeurs, il faut être capable de décrire le fonctionnement normal. Ainsi, par exemple, il est impossible de prévoir le comportement d'un calculateur lorsqu'il est alimenté en 250 V alternatif alors qu'il est conçu pour fonctionner avec du 12 V continu ; cet observable sera donc borné entre 0 et 16V qui sont les conditions normales d'alimentation dans un véhicule. Le modèle de la thermistance est applicable uniquement lorsque T_n est compris entre -30 et 200 °C.

De manière plus générale, il faut toujours pouvoir associer un moyen de mesure à un observable, même si ce moyen est difficile à mettre en œuvre sur un véhicule.

Après avoir associé aux variables leurs observables, il faut définir la valeur de chaque variable en fonction des valeurs des observables, dans la limite des domaines de définition. De cette manière, quelles que soient les valeurs observées, le dictionnaire précise la valeur de chaque variable. Cela permet de prédire si le scénario réel est normal ou pas.

Ainsi dans l'exemple de la thermistance, nous constatons que la définition de V_{capteur} n'est pas complète. En effet, elle ne précise pas quelle est sa valeur lorsque

$Re \neq f(Tn)$. Par ailleurs, les domaines de définition des observables ne sont pas précisés. Aussi la définition complète est la suivante :

- Les observables associés à la variable *Vcapteur* sont les suivants :
 - La résistance électrique du capteur, *Re*, définie de 0 Ohms à l'infini,
 - La température du noyau de la sonde, *Tn*, définie sur $-30..200^{\circ}\text{C}$,
 - La fonction caractéristique de la thermistance, *f*, définie de $-30..200^{\circ}\text{C}$ sur $51..2500$ Ohms.
- Quelle que soit la valeur de *Tn* sur son domaine de définition :
 - Si $Re = f(Tn)$ et $Tn < 150$ alors $V_{\text{capteur}} = \textit{Nominal}$
 - Si $Re = f(Tn)$ et $Tn \geq 150$ alors $V_{\text{capteur}} = \textit{Chaud}$
 - Si $Re \neq f(Tn)$ et $Re \in 0..50$ alors $V_{\text{capteur}} = \textit{CC}$
 - Si $Re \neq f(Tn)$ et $Re \in 51..2500$ alors $V_{\text{capteur}} = \textit{Defaillant}$
 - Si $Re \neq f(Tn)$ et $Re > 2500$ alors $V_{\text{capteur}} = \textit{CO}$

La valeur particulière *Defaillant* permet de dire explicitement que le capteur est défaillant lorsque $Re \neq f(Tn)$. Par ailleurs, *CC* et *CO* sont les états de la sonde lorsque ses fils de connexions sont respectivement en court-circuit et coupés. L'événement *EvtCapteur* (paragraphe 3) affecte uniquement les valeurs *Nominal* et *Chaud* à *Vcapteur* et non pas *CC*, *CO* ou *Defaillant*, car il s'agit alors de situations de panne ; or, les modèles formalisent les propriétés d'un comportement sain.

4.2. Dictionnaire des événements

Après avoir défini le dictionnaire des variables, il reste à présenter le contenu du dictionnaire des événements. Son rôle est de faire correspondre les événements du modèle, qui sont en nombre limité, avec des événements concrets dont le nombre est infini.

Par exemple chaque fois que la température de la thermistance, *Tn*, augmente ou diminue d'une unité de mesure, nous pouvons considérer qu'un événement concret s'est produit. Du côté de la modélisation, l'événement *EvtCapteur* est beaucoup moins «vivace», puisqu'il modifie la valeur de *Vcapteur* uniquement lorsque la température du noyau passe en dessous ou au-dessus de 150°C .

Par ailleurs dans un modèle B, par définition, un événement est atomique, c'est-à-dire qu'un événement ne peut pas s'étaler dans le temps. Toutefois, certains événements concrets ont une durée «importante». Par exemple, l'accélération par un conducteur est un événement concret qui peut commencer au moment où la pédale bouge d'un degré et se terminer à l'instant où le moteur est revenu en régime stable. Dans cette situation, il est nécessaire de trouver et de préciser, dans le dictionnaire, des points de repères univoques : par exemple, l'instant où la pédale se stabilise ou alors l'instant où le contrôleur moteur arrête la sur-injection de la quantité d'essence.

Ainsi, la définition de l'événement *EvtCapteur* du modèle de la thermistance est la suivante :

- Lorsque $V_{\text{capteur}} = \text{Nominal}$, *EvtCapteur* représente l'instant où la température, T_n , atteint 150°C.
- Lorsque $V_{\text{capteur}} = \text{Chaud}$, *EvtCapteur* représente l'instant où T_n descend en dessous de 150°C.

Une erreur habituelle consiste à confondre la définition d'un événement B avec la re-formulation de son contenu en français, ce qui n'est pas nécessaire puisque son contenu est formalisé. La traduction des modèles B en langage naturel est un autre sujet qui n'est pas abordé dans cet article.

Pour conclure ce paragraphe, il est intéressant de remarquer que si chaque variable B était associée à un seul observable, avec le même ensemble de définitions, alors la modélisation serait un simulateur du véhicule qui deviendrait aussi complexe que celui-ci. On voit qu'il est nécessaire de faire la modélisation avec des variables abstraites qui sont différentes des observables, afin de gagner en abstraction.

5. Modélisation d'un calculateur

Après avoir modélisé la thermistance, nous présentons la modélisation du fonctionnement du calculateur. Celui-ci acquiert la température d'huile mesurée par la thermistance. Lorsque le calculateur est alimenté, il émet, sur le réseau informatique du véhicule, une valeur qui dépend de la température de l'huile. En cas de circuit ouvert ou de court-circuit, il émet la valeur 255.

Dans cette modélisation, nous reprenons la variable *Vcapteur* définie dans le modèle de la thermistance aux paragraphes 3 et 4. Nous introduisons les nouvelles variables *VcAlim* et *VcEmission*.

L'observable associé à la variable *VcAlim* est la tension U aux bornes du connecteur d'alimentation du calculateur. Elle est définie de 0 à 16 volts. On pose :

- Si $U = 0$ alors $V_{\text{cAlim}} = \text{OFF}$
- Si $U \in 10..16$ alors $V_{\text{cAlim}} = \text{ON}$
- Si $U \in 1..9$ alors $V_{\text{cAlim}} = \text{Defaillant}$

Les observables associés à la variable *VcEmission* sont :

- La résistance électrique du capteur, Re , définie de 0 Ohms à l'infini,
- La fréquence d'émission du message «température d'huile», ($Freq$), définie entre 0 et 10 Hz,
- La valeur du message, (Val), définie entre 0 et 255,
- La fonction caractéristique de la thermistance, f , définie de $-30..200^\circ\text{C}$ sur $51..2500$ Ohms.

La définition de *VcEmission* exprime que le message «température d'huile» doit être émis au minimum à 2Hz et qu'il doit être égal à la température du noyau de la sonde +30°C (f^{-1}), sauf en cas de court-circuit ou de circuit ouvert ($Re \notin 51..2500$). D'une manière plus formelle, cela donne :

- Si $Freq \geq 2$ et $Re \in 51..2500$ et $Val = f^{-1}(Re) + 30$ alors $VcEmission = Nominal$
- Si $Freq \geq 2$ et $Re \in 51..2500$ et $Val \neq f^{-1}(Re) + 30$ alors $VcEmission = Defaillant$
- Si $Freq \geq 2$ et $Re \notin 51..2500$ et $Val = 255$ alors $VcEmission = Secours$
- Si $Re \notin 51..2500$ et $Val \neq 255$ alors $VcEmission = Defaillant$
- Si $Freq = 0$ alors $VcEmission = NonEmis$
- Si $Freq < 2$ alors $VcEmission = Defaillant$

Certaines combinaisons de valeurs pour les observables sont impossibles sur une voiture saine. Ainsi, elles confirment la présence d'une panne. On repère les valeurs interdites en affectant la valeur *Defaillant* à la variable.

Le dictionnaire des événements est le suivant :

- *EvtAlimentation* modélise le comportement du calculateur à l'instant où *U* se stabilise entre 10 et 16V.
- *EvtVeille* modélise le comportement du calculateur à l'instant où *U* se stabilise à 0V.
- *EvtChangementMode* modélise le comportement du calculateur à l'instant où le calculateur émet le premier message après le changement de plage de valeurs de *Re*.

Après avoir donné le contenu des dictionnaires, voici le contenu du modèle :

```

EvtAlimentation =
SELECT
  VcAlim = OFF
THEN
  IF Vcaptereur = CC OR Vcaptereur = CO
  THEN
    VcEmission := Secours
  ELSIF Vcaptereur = Chaud OR Vcaptereur = Nominal
  THEN
    VcEmission := Nominal
  END ||
  VcAlim := ON
END ;
EvtChangementMode =
SELECT
  VcAlim = ON
THEN
  IF Vcaptereur = CC OR Vcaptereur = CO
  THEN

```

```

        VcEmission := Secours
    ELSIF Vcapteur = Chaud OR Vcapteur = Nominal
    THEN
        VcEmission := Nominal
    END
END ;

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

```

Dans le cas de cette fonction, il est inutile de formaliser le fonctionnement du calculateur lorsque $U \in 1..9$. En effet, c'est un cas de fonctionnement dégradé qui n'est pas géré par le véhicule. En revanche, la détection des courts-circuits et des circuits ouverts est une fonctionnalité du calculateur modélisé.

La rigueur des dictionnaires et la construction formelle des modèles, permettraient d'automatiser, en partie, la tâche qui consiste à vérifier si le comportement de chaque élément remplaçable est conforme aux propriétés exprimées dans le modèle et ainsi de diagnostiquer l'origine d'une panne. L'outil est en cours d'étude.

6. Conclusion

Les techniques de modélisation présentées dans cet article ont été mises en œuvre industriellement pour le service après-vente PEUGEOT. Les modélisations complètes ont été réalisées pour toutes les fonctions de deux véhicules ; un véhicule est décrit par environ 50 modèles B, 7000 événements, 70.000 lignes de B et 2000 variables abstraites.

Les «principes de fonctionnement formalisés» dans leur forme textuelle sont actuellement utilisés par les spécialistes des plateaux d'assistance. L'utilisation directe des modèles B au travers d'un outil informatique permettant de faire du diagnostic automatique est actuellement à l'étude.

Initialement, la méthode B était essentiellement utilisée pour des développements de logiciels sûrs, embarqués sur des systèmes critiques. Nous avons ici exploité les possibilités d'expression et surtout d'abstraction du langage B dans un contexte beaucoup plus large que le logiciel. La preuve mathématique a été utilisée ici uniquement pour montrer la cohérence des modèles. Nous n'avons pas cherché à retrouver et exprimer les exigences initiales ayant conduit à la création du système décrit fonctionnellement.

Les principes de fonctionnement formalisés constituent un moyen d'abstraction que nous souhaiterions associer à d'autres niveaux :

- les niveaux supérieurs si un processus formel B était utilisé en phase de conception du système,
- les niveaux inférieurs si des processus formels B étaient utilisés pour les phases de développement de certaines parties logicielles critiques.

L'utilisation de la modélisation formelle arbitrairement abstraite autorisée par B, nous a permis d'allier la précision mathématique à l'abstraction qui est nécessaire pour exprimer les lois comportementales sans faire une pseudo programmation du véhicule. Nous sommes convaincus que ces mêmes travaux, menés sans formalisation, n'auraient pas conduit à l'exactitude et à la levée d'ambiguïté qui ont pu être ainsi atteintes.

7. Bibliographie

- [ABR 96] ABRIAL J.-R., *The B Book - Assigning Programs to Meanings*, Cambridge University Press, August 1996.
- [ABR 98] ABRIAL J.-R., MUSSAT L., « Introducing Dynamic Constraints in B », *B'98 : Recent Advances in the Development and Use of the B Method, LNCS 1393*, Springer-Verlag, 1998, p. 83–128.