UPMC/MASTER/INFO/STL/SVP
Spécification et Vérification de Programmes
Modélisation B: les feux

P. Manoury F. Peschanski

2014

Nous allons voir maintenant comment utiliser le formalisme B pour spécifier un problème de gestion des feux d'un carrefour. Cet exemple est largement inspiré d'une petite étude de cas que J.-Y. Chauvet a publiée dans *1st Conference on the B method, Proceedings, ed. Henri Habrias, Nantes 1996.*

Nous adopterons, pour développer cet exemple la démarche suivante :

1. rédaction du cahier des charges(spécification non-formelle)
2. analyse du cahier des charges et traduction de ces éléments pertinents en formules (pré-spécification formelle)
3. définition d'une machine abstraite organisant les éléments de la pré-spécification formelle (spécification formelle)

Spécification informelle

La circulation d'un carrefour est réglée par deux feux tricolores dont les couleurs sont vert, orange ou rouge. Sur chacun des feux une seule des couleurs est active à la fois. Le système de feux du carrefour peut être en service ou hors service. Lorsque le système est hors service, les deux feux sont oranges. Lorsque le système est en service, la couleur de chacun des feux change suivant le cycle : orange puis rouge puis vert puis orange, etc ...

Un véhicule ne peut s'engager sur une voie que si le feu n'est pas rouge. Les feux doivent être réglés de façon à ce que deux véhicules venant de voix différentes ne se trouvent pas en même temps sur le carrefour. On définit donc la *propriété de sécurité* suivante :

(S) *lorsque le système est en service, l'un des deux feux est au rouge*

Il ne faut cependant pas que par soucis excessif de sécurité, le carrefour soit bloqué. On pose donc la *propriété de disponibilité* :

(D) *lorsque le système est en service, l'un des feux au moins n'est pas au rouge*

Le système doit être équitable : il faut qu'il permette alternativement aux véhicules de chaque voix de pouvoir s'engager sur le carrefour. On énonce donc la *propriété d'équité* :

(E) *lors du changement de couleur, l'un au moins des deux feux doit effectivement changer*

On désire obtenir un système assurant :

la mise en service des feux d'un carrefour ;

la gestion du changement de couleurs des feux.

Pré-spécification formelle

Il s'agit à cette étape de la construction de la spécification formelle de définir un *modèle mathématique* du système. Pour mener à bien cette tâche, il faut faire dans la spécification informelle le tri entre l'essentiel et l'accessoire. Dans la pratique, ce tri doit être mené en relation constante avec les rédacteurs du cahier des charges.

Dans notre exemple, nous retiendrons les phrases (ou morceaux de phrase) suivants :

1. ≪deux feux tricolores dont les couleurs sont vert, orange ou rouge≫
2. ≪le système [...] peut être en service ou hors service≫
3. ≪lorsque le système est hors service, les deux feux sont oranges≫
4. ≪lorsque le système est en service, la couleur des feux changent suivant le cycle : orange puis rouge pui vert puis orange, etc ...≫
5. ≪lorsque le système est en service, l'un des deux feux est au rouge≫
6. ≪lorsque le système est en service, l'un des feux au moins n'est pas au rouge≫
7. ≪lors du changement de couleur, l'un au moins des deux feux doit effectivement changeguid

Votre travail

Il s'agit maintenant de traduire chacun des éléments retenus en formules : c'est la finalisation de la pré-spécification formelle. Puis d'intégrer les éléments formalisés de spécification dans le modèle B : invariants, opérations, preuve d'établissement et de conservation de l'invariant.