Combiner des diagrammes d'état étendus et la méthode B pour la validation de systèmes industriels

Thomas Fayolle

June 08, 2016

Validation de systèmes industriels :

- Systèmes critiques : sémantique formelle
- Systèmes spécifiques : connaissance du domaine à modéliser
- Systèmes complexes : pouvoir les spécifier par étapes

ASTD:

- diagrammes états/transitions
  - des états qui peuvent être hérarchiques
  - des transitions
  - des états historiques
- opérateurs des algèbres de processus
  - Fermeture de Kleene
  - Entrelacement/Synchronisation
  - Choix
  - Etc...

Langage B/Event-B:

- Langages basés sur la théorie des ensembles
- Méthodes qui utilisent le raffinement
- En résumé :
  - Une opération a une précondition et une postcondition
  - Une opération ne peut être effectuée que si sa précondition est vraie
  - Des propriétés peuvent être écrites sous la forme d'invariants

Un exemple ferroviaire pour illustrer la méthode

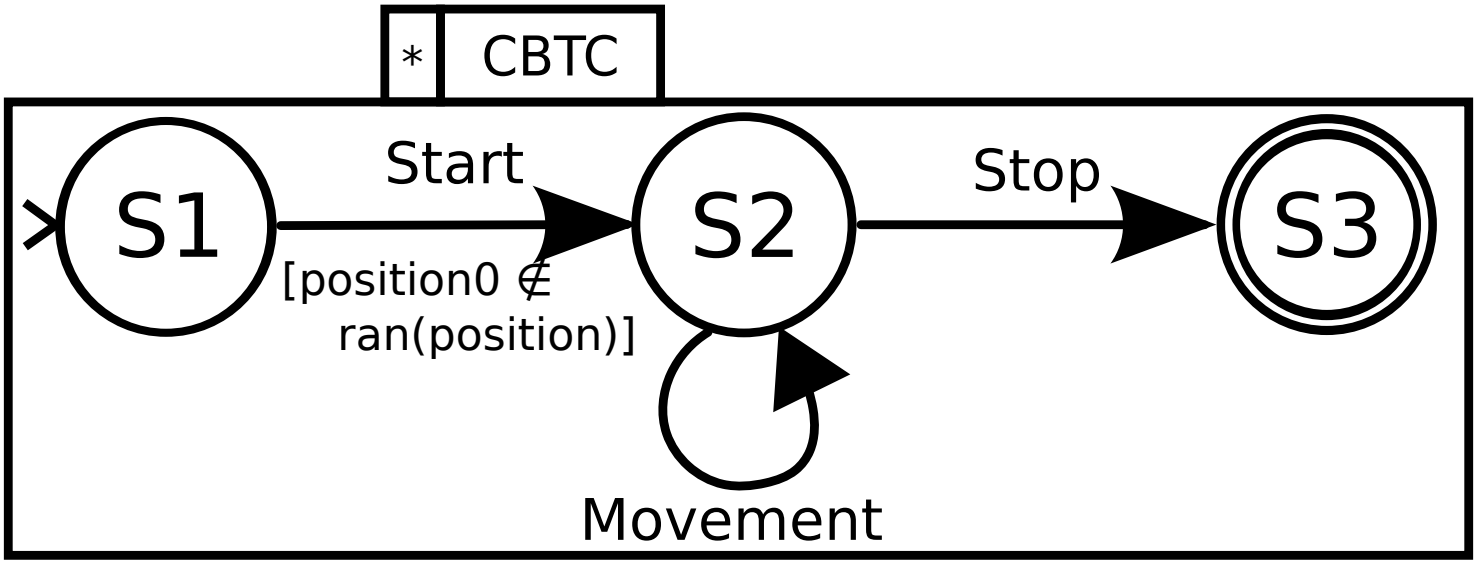


Figure: Comportement d'un train

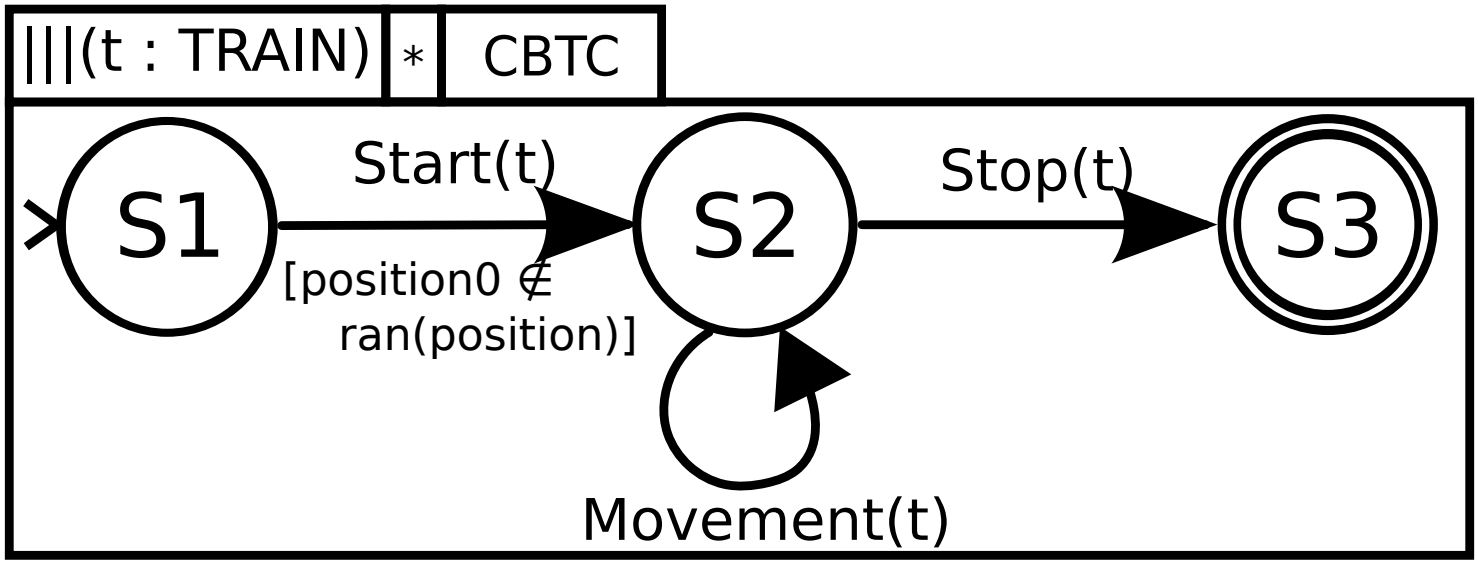


Figure: Comportement d'un ensemble de train

Le modèle de donnée (écrit en Event-B)

- Une variable *position*
- Fonction qui associe à chaque train un point de la voie
- Les trains avancent dans le même sens

Quelles actions sur les données du système :

- *Start_act* : donne une position au train
- *Stop_act* : retire la position d'un train
- *Movement_act* : change la position du train telle que :
  - Le train avance (ne recule pas)
  - Le train ne double pas les trains devant lui

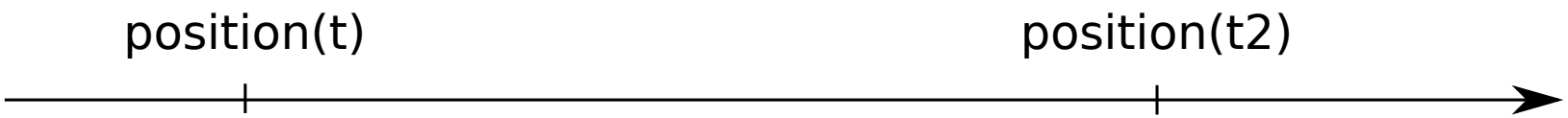


Figure: Mouvement d'un train

Donc :

- *Stop_act* et *Movement_act* ne peuvent être faits que si le train a une position
- *Start_act* ne peut être fait que si le train n'a pas de position

Ces conditions sont marquées comme gardes des événements Event-B et doivent être vérifiées

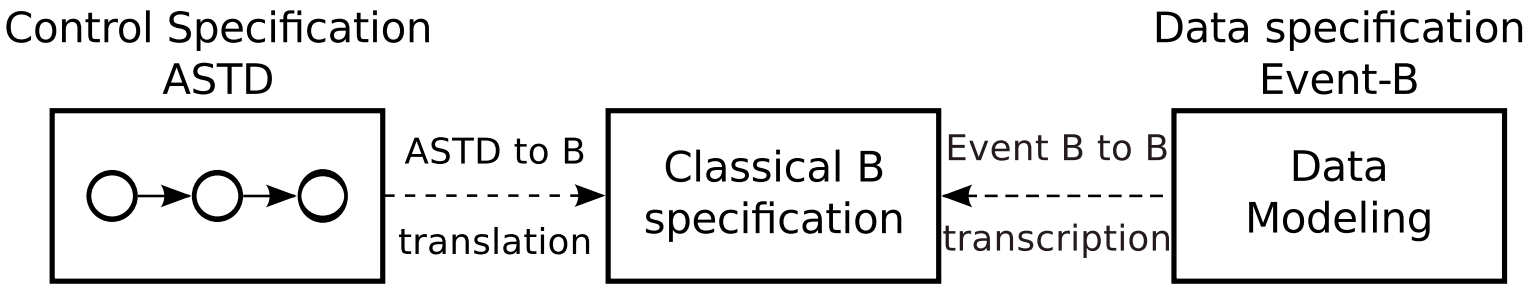


Figure: Methodologie de modélisation

Problème :

- Le train doit connaitre les positions des autres trains
- On souhaite ajouter un contrôleur pour contrôler le mouvement des trains
- Le contrôleur est représenté par une opération de calcul

Raffinement ASTD:

- On peut rajouter et/ou enlever des événements
- Les traces doivent être conservées si on regarde les événements communs
- Définition formelle dans M. Frappier et al. “Refinement patterns for ASTDs”. In: *FACS* 26.5 (2014), pp. 919–941. DOI: 10.1007/s00165-013-0286-3.

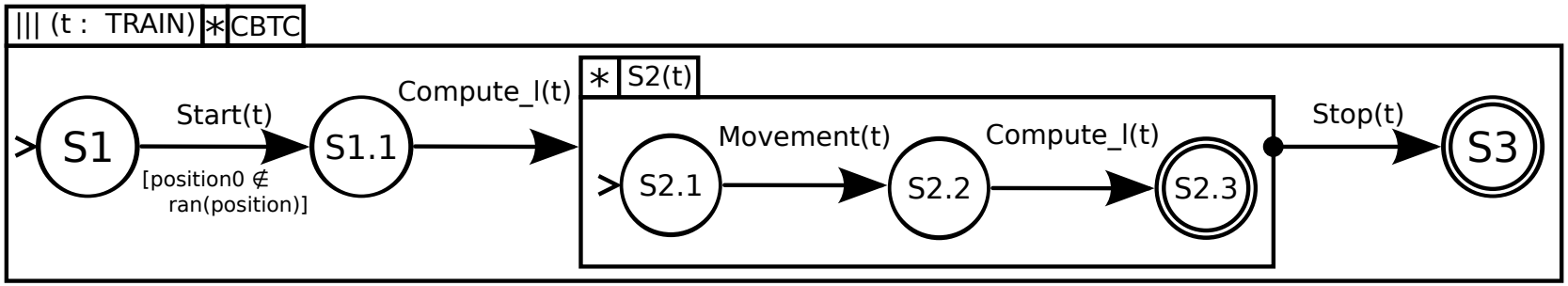
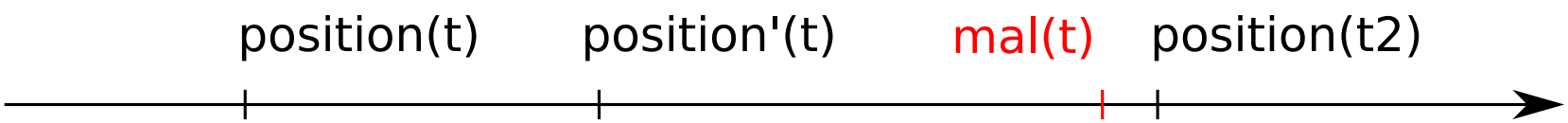


Figure: Raffinement


position(t)
position'(t)
mal(t)
position(t2)

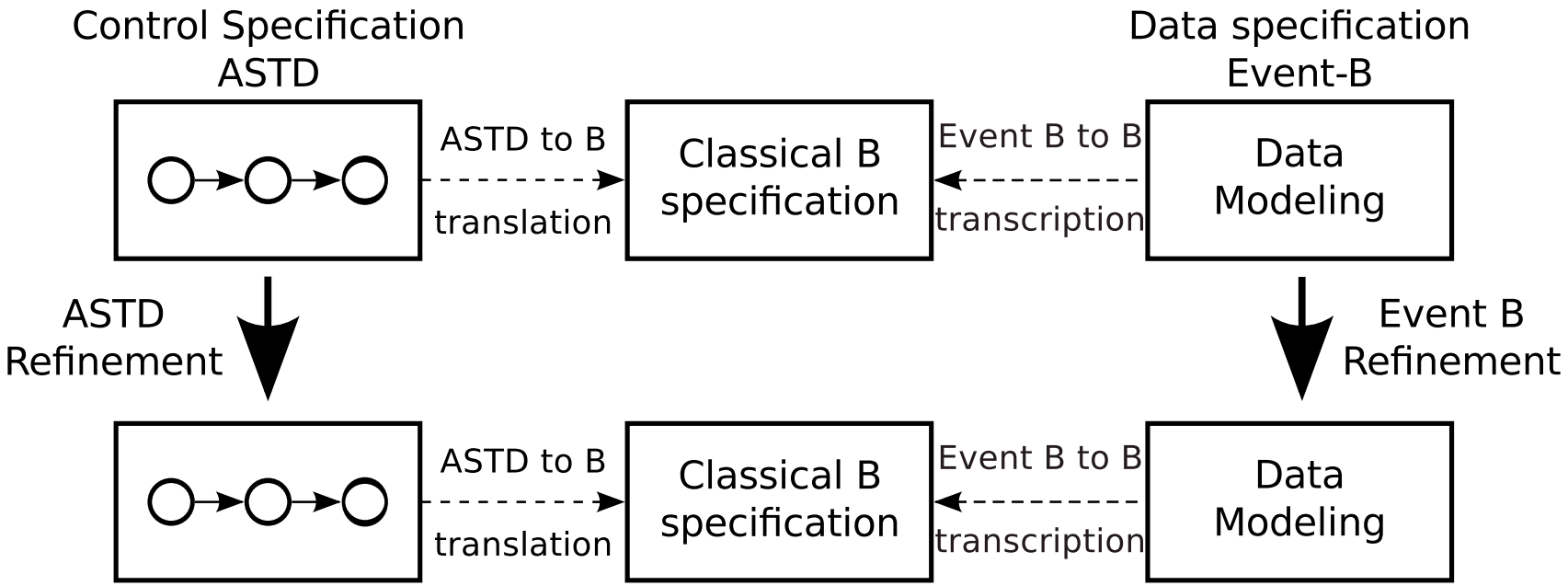


Figure: Methodologie de modélisation

Les avantages :

- Une représentation :
  - graphique : parle aux ingénieurs spécialisés
  - formelle : permet la vérification de propriété, empêche les ambiguïtés
  - concise : facilite la lisibilité

Les inconvénients :

- Les outils ne sont pas encore tous développés
- Le raffinement notamment n'a pas d'outils
- La preuve de la cohérence horizontale est coûteuse
  - Solution envisagée : utiliser le raffinement

Des questions ?