Patrons de conception prouvés

Raffinement Incrémental de Modèles EvénementielS

ANR-006-SETIN-015

Thierry Lecomte - ClearSy
Dominique Méry – Loria
Dominique Cansell - Loria

22 Mai 2007

Journées Neptune

Plan

- Objectifs
- Pourquoi
- Comment
- Quand

Objectifs

- Transposer la notion de patron de conception logiciel à la conception de système
- En s'appuyant sur la méthode formelle B (raffinement et preuve) pour la modélisation de systèmes
- Pour construire des systèmes corrects par construction
- Pour accélérer le processus de développement, en limitant les retours en arrière

B pour la modélisation de systèmes

- Systèmes clos (système et environnement)

- Description par:
  - Variables d'états et propriétés (théorie des ensembles, logique des prédicats, substitutions)

```
inv3: (output = UP ⇒ status = NOMINAL)
```

  - Événements atomiques, instantanés, exprimés sous la forme de couples conditions-actions

```
commandUp
   WHEN
      grd1: status = NOMINAL
      grd2: output = DOWN
   THEN
      act1: output := UP
   END
```

B pour la modélisation de systèmes

- Description par:
  - Un état initial qui doit vérifier les propriétés attendues

```
INITIALISATION
   BEGIN
      act1: status := OFF
      act2: output := DOWN
   END
```

  - Un enchaînement non déterministe d'événements dont les conditions d'activations sont vraies. Propriétés vérifiées pour les actions appliquées.

Le raffinement

- Suite de modèles pour lesquels:
  - On ajoute de nouvelles variables
  - On remplace des variables (abstraites) par d'autres (concrètes)

  - On ajoute, supprime, regroupe, éclate des événements
  - On renforce les conditions des événements
  - On précise les actions

  - On identifie les propriétés nécessaires pour le modèle raffinant ne contredise pas le modèle raffiné (notamment invariant de collage)

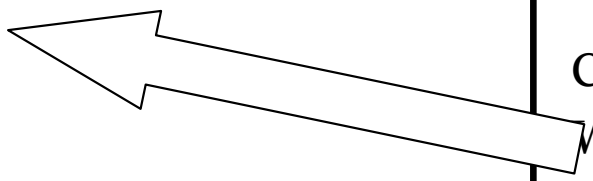
Exemple

Système de commande (abstrait)

État ∈ {OFF, INIT, NOMINAL, DEFAUT}
Sortie ∈ {0,1}

(Sortie=1 ⇒ Etat=NOMINAL)

CommandeHaut
WHEN
    Etat=NOMINAL
THEN
    Sortie := 1
END



Système de commande (2 calculateurs)

État1, Etat2 ∈ {OFF, INIT, NOMINAL, DEFAUT}
Sortie1, Sortie2 ∈ {0,1}

(Sortie=1 ⇒ Etat1=NOMINAL)
(Sortie=2 ⇒ Etat2=NOMINAL)

(Etat1=NOMINAL ∧ Etat2=NOMINAL ⇒
    Etat=NOMINAL)
(Sortie1=1 ∧ Sortie2=1 ⇒ Sortie=1)

CommandeHaut
WHEN
    Etat1=NOMINAL ∧ Etat2=NOMINAL
THEN
    Sortie1 := 1 || Sortie2 := 1
END

Le raffinement vs la preuve

- Processus itératif basé sur le verdict des outils de preuve
  - Un modèle entièrement prouvé est cohérent, un modèle partiellement prouvé est peut être faux
  - Une méthode: ajouter en invariant ce que le prouveur cherche à démontrer puis modifier les actions en conséquence.
  - En cas d'erreur de raffinement, l'effort de preuve est perdu (en partie)
  - Le raffinement nécessite une utilisation experte pour être efficace

Raffinement semi-automatique (1/2)

- Transformer graduellement un modèle abstrait en un modèle concret
- Par l'application des règles de transformations de modèles, générales ou particulières
- Les règles ont des conditions de déclenchement
- Un outil les applique de manière automatique (raffinement de donnée, raffinement de structure)
- L'utilisateur ajoute ou corrige des règles lorsque l'outil s'arrête

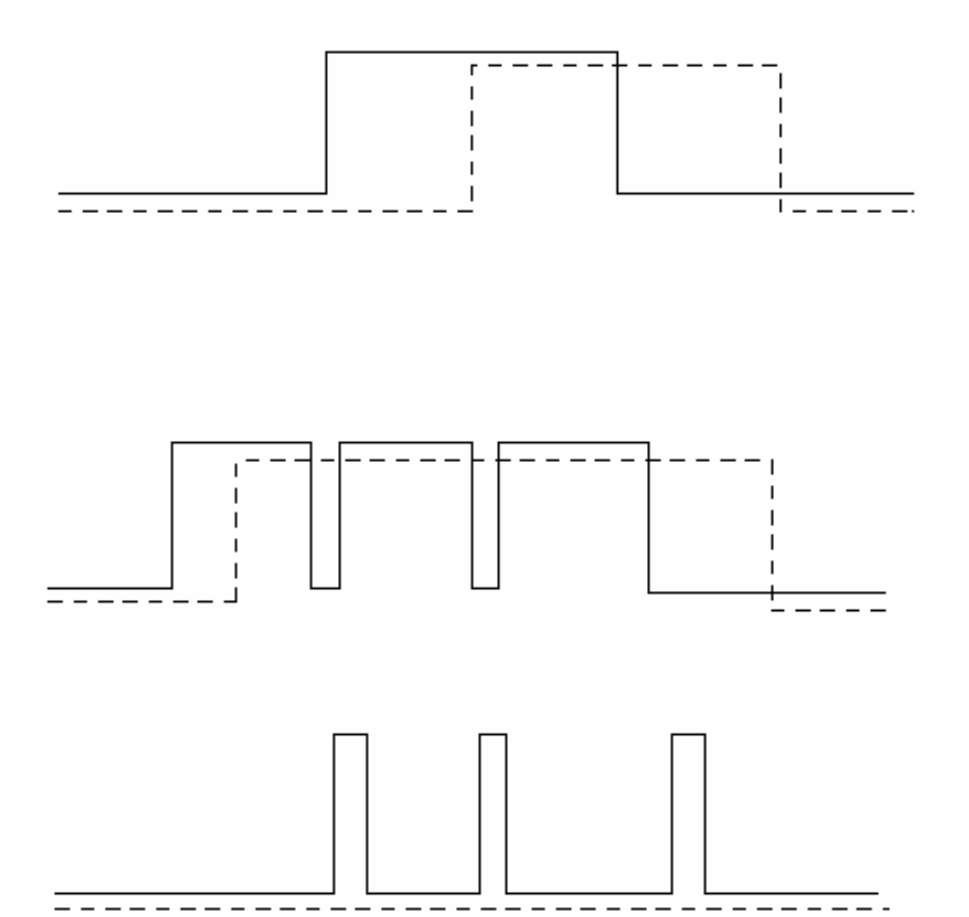
Raffinement semi-automatique (2/2)

- Applications:
  - METEOR: 80 000 lignes de code Ada
  - Roissy VAL: 150 000 lignes de code Ada
- Inconvénients:
  - **Les règles de raffinement ne sont pas validées par l'outil**
  - Progression lente et verbeuse: une multitude de petits pas
  - Le modèle de départ doit contenir tous les détails
- Avantages:
  - Les modèles ainsi décomposés sont plus facilement prouvables

Les patrons de conception prouvés

- Notion proposée par J.R. Abrial
- Réutiliser des résultats de modélisation qui ont été prouvés
- Un patron est un ensemble cohérent de variables, d'événements et de propriétés modélisant une notion
- Premiers patrons identifiés d'après le cas d'étude de la presse (INRS)

Patron: synchronisation faible



pat0_1: $a \in \{0,1\}$

pat0_2: $r \in \{0,1\}$

pat0_3: $ca \in \mathbb{N}$

pat0_4: $cr \in \mathbb{N}$

pat0_5: $cr \leq ca$

pat0_6: $r = 0 \wedge a = 1 \Rightarrow cr < ca$

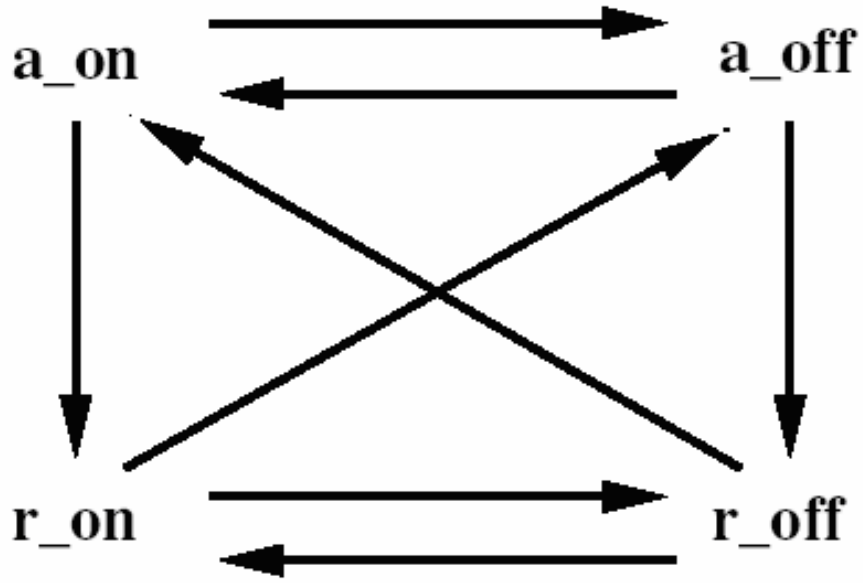
Patron: synchronisation faible

a_on
when
$a = 0$
then
$a := 1$
$ca := ca + 1$
end

a_off
when
$a = 1$
then
$a := 0$
end

r_on
when
$r = 0$
$a = 1$
then
$r := 1$
$cr := cr + 1$
end

r_off
when
$r = 1$
$a = 0$
then
$r := 0$
end



Patron: synchronisation faible

a_on	$\rightsquigarrow$	push_start_motor_button
a_off	$\rightsquigarrow$	release_stop_motor_button
r_on	$\rightsquigarrow$	treat_start_motor
r_off	$\rightsquigarrow$	treat_release_start_motor_button
a	$\rightsquigarrow$	$start\_motor\_button$
r	$\rightsquigarrow$	$start\_motor\_impulse$
0	$\rightsquigarrow$	ko
1	$\rightsquigarrow$	ok

Patron: synchronisation forte

pat0_1: $a \in \{0, 1\}$

pat0_2: $r \in \{0, 1\}$

pat0_3: $ca \in \mathbb{N}$

pat0_4: $cr \in \mathbb{N}$

pat2_1: $a = 1 \wedge r = 0 \Rightarrow ca = cr + 1$

pat2_2: $a = 0 \vee r = 1 \Rightarrow ca = cr$

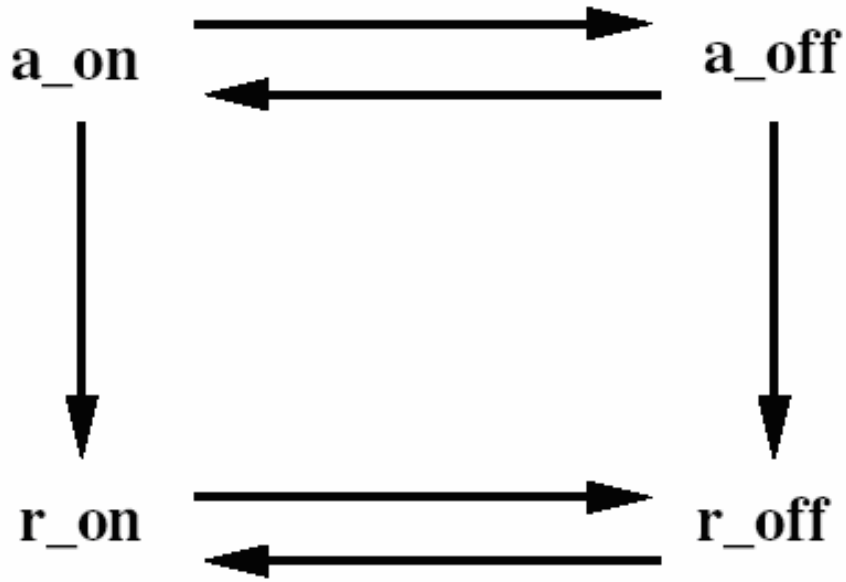
Patron: synchronisation forte

a_on
when
$r = 0$
$a = 0$
then
$a := 1$
$ca := ca + 1$
end

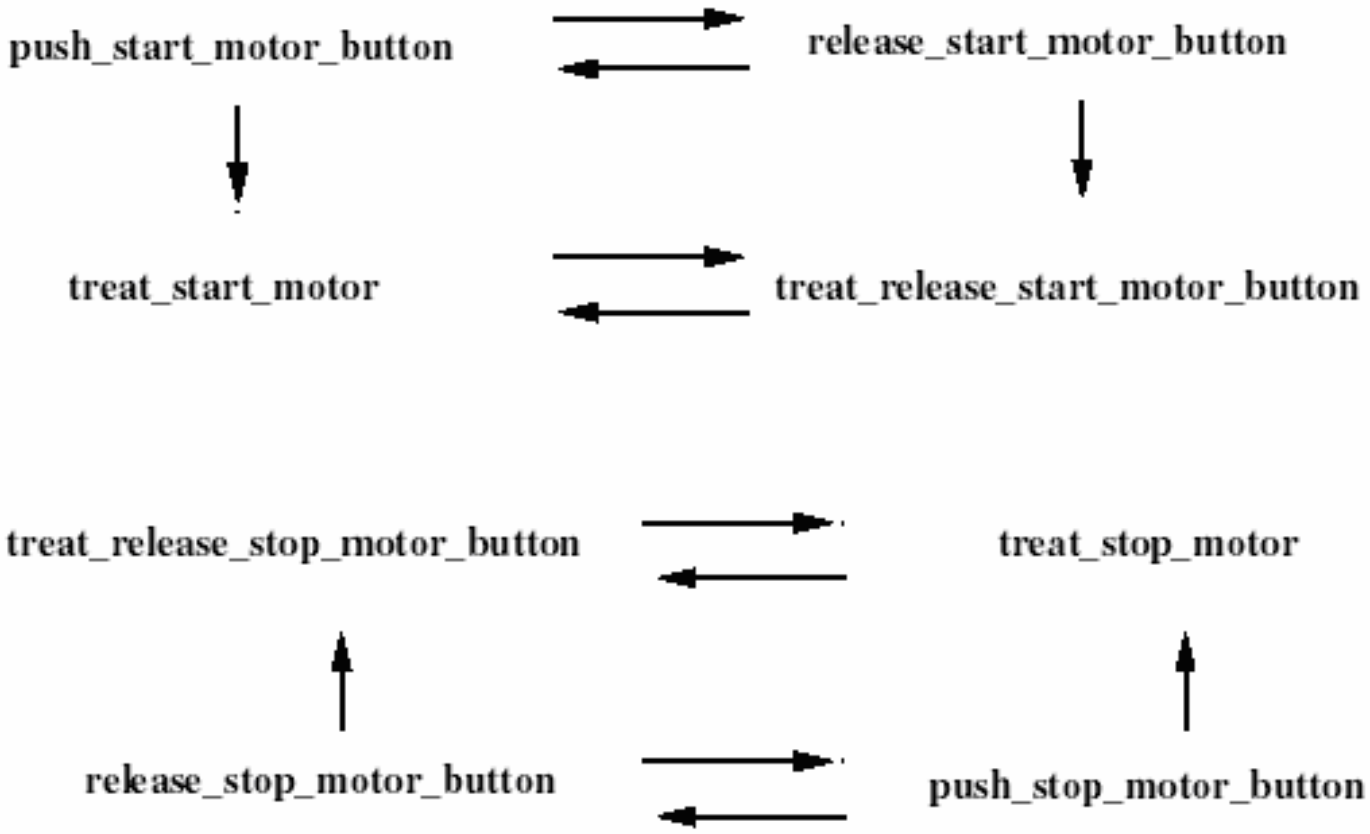
a_off
when
$r = 1$
$a = 1$
then
$a := 0$
end

r_on
when
$r = 0$
$a = 1$
then
$r := 1$
$cr := cr + 1$
end

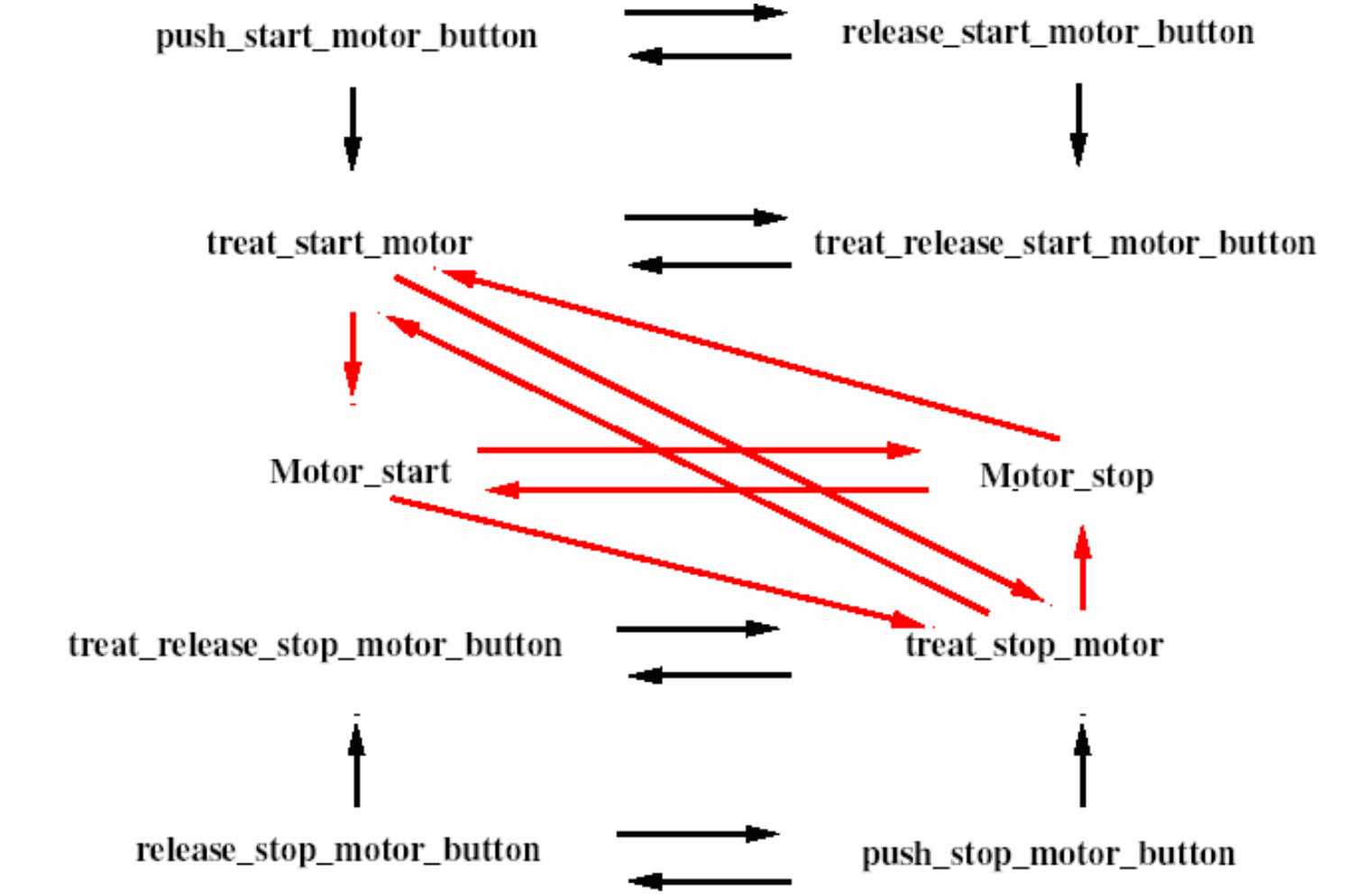
r_off
when
$r = 1$
$a = 0$
then
$r := 0$
end



Patrons: combinaisons



Patrons: combinaisons



Intérêt

- Réduction du temps de modélisation et preuve (bootstrap du cas d'étude INRS):
  - 8 niveaux de raffinement, entièrement prouvés automatiquement
  - 14 obligations de preuve pour valider 4 patrons.
- Construit d'après un objectif de validation des objets conçus
- Capturent l'information orientée preuve du système en cours de construction

Jalons

- RIMEL est un projet de 3 ans débuté en 2007
- Reprise de modèles existants pour analyse:
  - Presse pneumatique (étude INRS)
  - Composants microélectroniques et politique de sécurité EAL5+
  - Commande des portes palières ligne 13 (RATP)
  - Véhicule militaire (CNIM)
- Construction d'un catalogue de patrons de conception prouvés
- Développement de cas d'études et enrichissement du catalogue
  - Systèmes distribués
- Développement d'outils permettant une industrialisation de l'approche (plateforme Rodin)
  - Éditeur de patron
  - Outil d'instanciation de patron

Merci de votre attention

RIMEL: http:// rimel.loria.fr

RODIN: http:// sourceforge.net/projects/rodin-b-sharp