

---

# Outils logiciels pour la combinaison de vérification fonctionnelle et d'évaluation de performances au sein de CADP

---

Christophe Joubert  
Séminaire VASY 2002  
30 Octobre 2002  
*Aix les Bains*

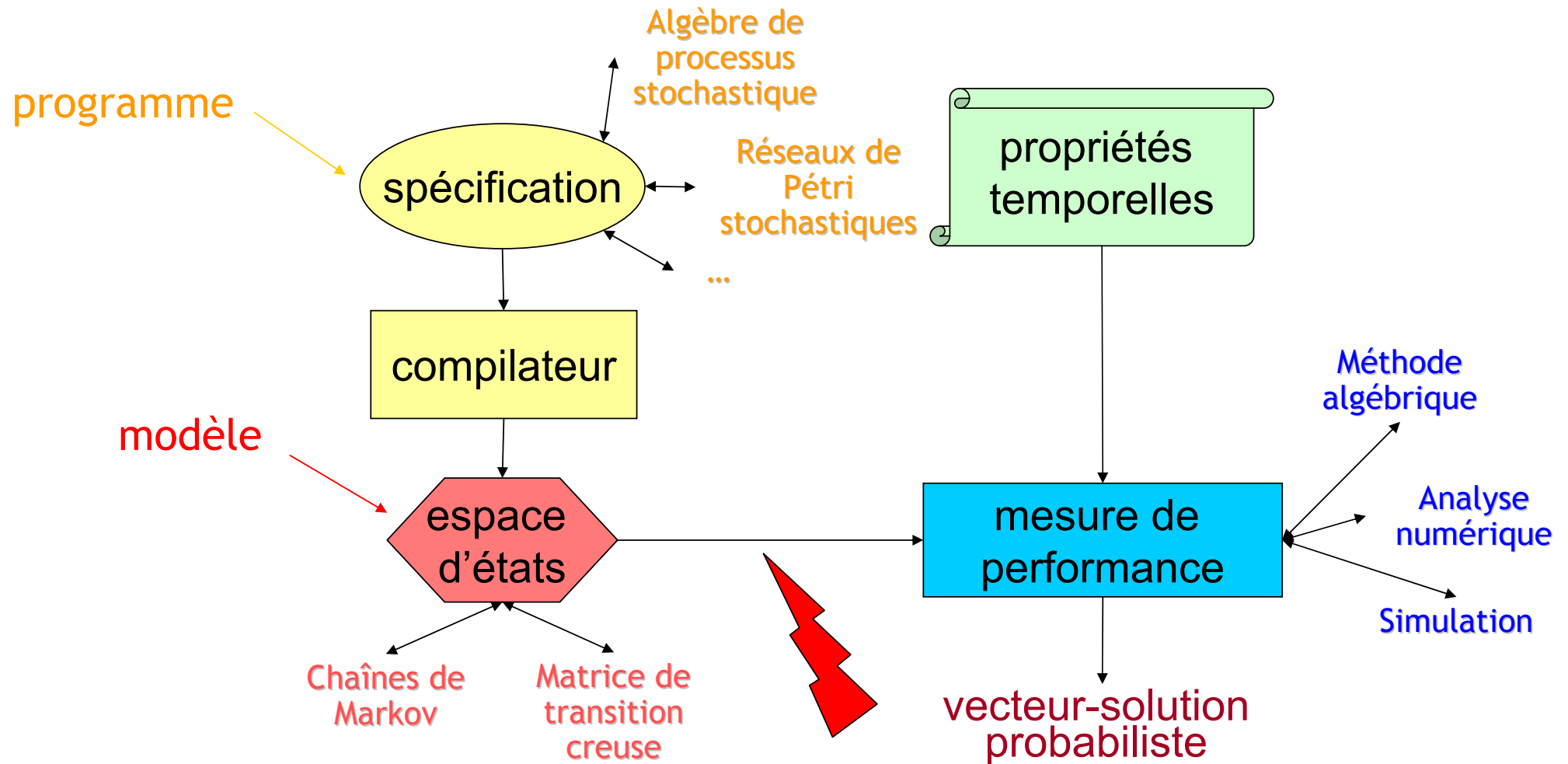
---

# Contexte du projet

---

- **Groupe FMT (Formal Methods and Tools)**
  - ✦ Spécification, conception et analyse formelle de systèmes distribués complexes
  - ✦ Collaborations avec le projet INRIA/VASY
  - ✦ Expertise dans le domaine des modèles stochastiques (chaînes de Markov)
- **Motivations**
  - ✦ Union des travaux pour confectionner une plateforme d'outils efficace en vérification fonctionnelle et en évaluation de performances

# Évaluation de performance



---

# Objectifs et plan

---

1. Modèles stochastiques
2. Réducteur de modèles mixtes
3. Expérimentations et résultats
4. Bilan et perspectives

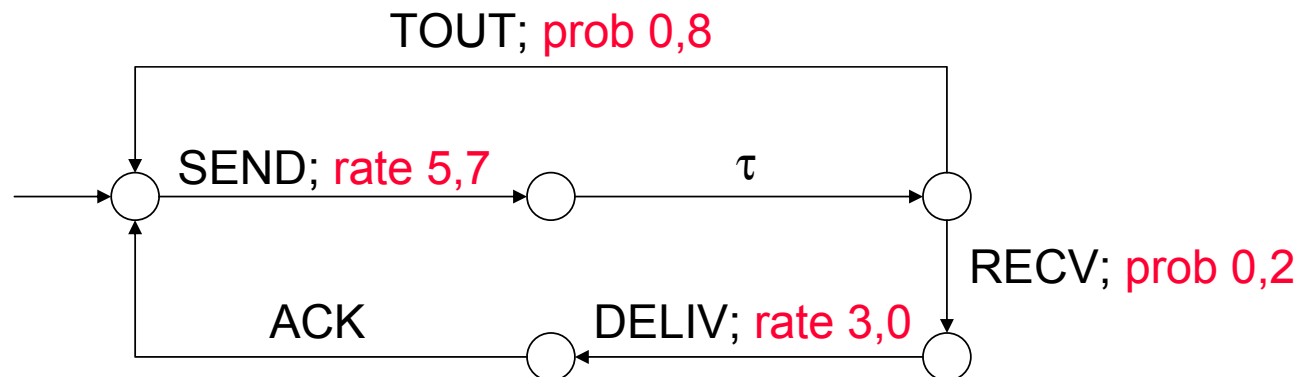
# Modèles stochastiques

- Processus stochastique
  - ✦ Famille de variables aléatoires  $\{X_t, t \in T\}$ 
    - $X_t$  est caractérisée par une fonction de distribution
- Processus Markovien
  - ✦ Processus stochastique + propriété Markovienne
    - (comportement futur entièrement défini par l'instant présent, donc totalement indépendant de son histoire)
- Chaîne de Markov
  - ✦ Processus Markovien + homogénéité + espace d'états discret
- CTMC (Continuous Time Markov Chain)
  - ✦ Chaîne de Markov + temps continu

# STE stochastiques

- Modèles

- ★ Généralisation des STE d'algèbre de processus:  $M = (S, A, T, R, s_0)$
- ★  $\Leftrightarrow$  Chaînes de Markov Interactives (IMC) [Hermanns98]:



- **STE probabilistes** : transitions "**prob  $p$** " et "**label ; prob  $p$** "
- **STE stochastiques** : transitions "**rate  $\lambda$** " et "**label ; rate  $\lambda$** "
- **STE mixtes** : (**STE probabiliste**  $\cup$  **STE stochastique**) + transitions étiquetées par des actions "**label**"

# Réducteur de modèles mixtes

- Motivations

- ✦ Générer un CTMC à partir d'un STE mixte sous forme d'IMC
- ✦ Réduire par factorisation le non-déterminisme présent dans les modèles mixtes
- ✦ Simplifier à la volée selon la condition de « bonne spécification »

# Définitions

- *Bien spécifié* :
  - ✦ se dit d'une IMC dont la CTMC résultante est unique, quelque soit les décisions non-déterministes choisies.
- Types d'états dans modèles mixtes
  - ✦ *Stable* : que des transitions **stochastiques** sortantes
  - ✦ *Case* : au moins une transition **probabiliste** sortante, et de possibles transitions stochastiques sortantes ignorées
  - ✦ *Décision* : au moins une transition **d'action** sortante, et de possibles transitions stochastiques sortantes ignorées



# Algorithme Principal

- $\forall s, \text{stable}(s) :$ 
  - $\forall s' \in \text{succ}(s) :$ 
    - $E = \text{WSC}(s')$
    - $\forall (n,v) \in E$ 
      - $P(s,n) = P(s,s') \cdot v$

# Algorithme WSC récursif

- $WSC(s)$  :

- ✦  $Stable(s)$  :

- $\rightarrow \{(s,1)\}$

- ✦  $Case(s)$  :

- $E' = \emptyset$

- $\forall s' \in succ(s)$  :

- $\Delta E = WSC(s')$

- $\Delta \forall (n,v) \in E$

- ★ if  $\exists (n,v') \in E'$

- $E' = E' \setminus (n,v')$

- $E' = E' \cup (n, v' + P(s,s').v)$

- ★ else  $E' = E' \cup (n, P(s,s').v)$

- $\rightarrow E'$

- ✦  $Décision(s)$  :

- $E_1 = E_2 = \emptyset$

- $\forall s' \in succ(s)$  :

- $\Delta$  if  $E_1 = \emptyset$

- ★  $E_1 = WSC(s')$

- $\Delta$  else

- ★  $E_2 = WSC(s')$

- ★ if  $E_1 \neq E_2$

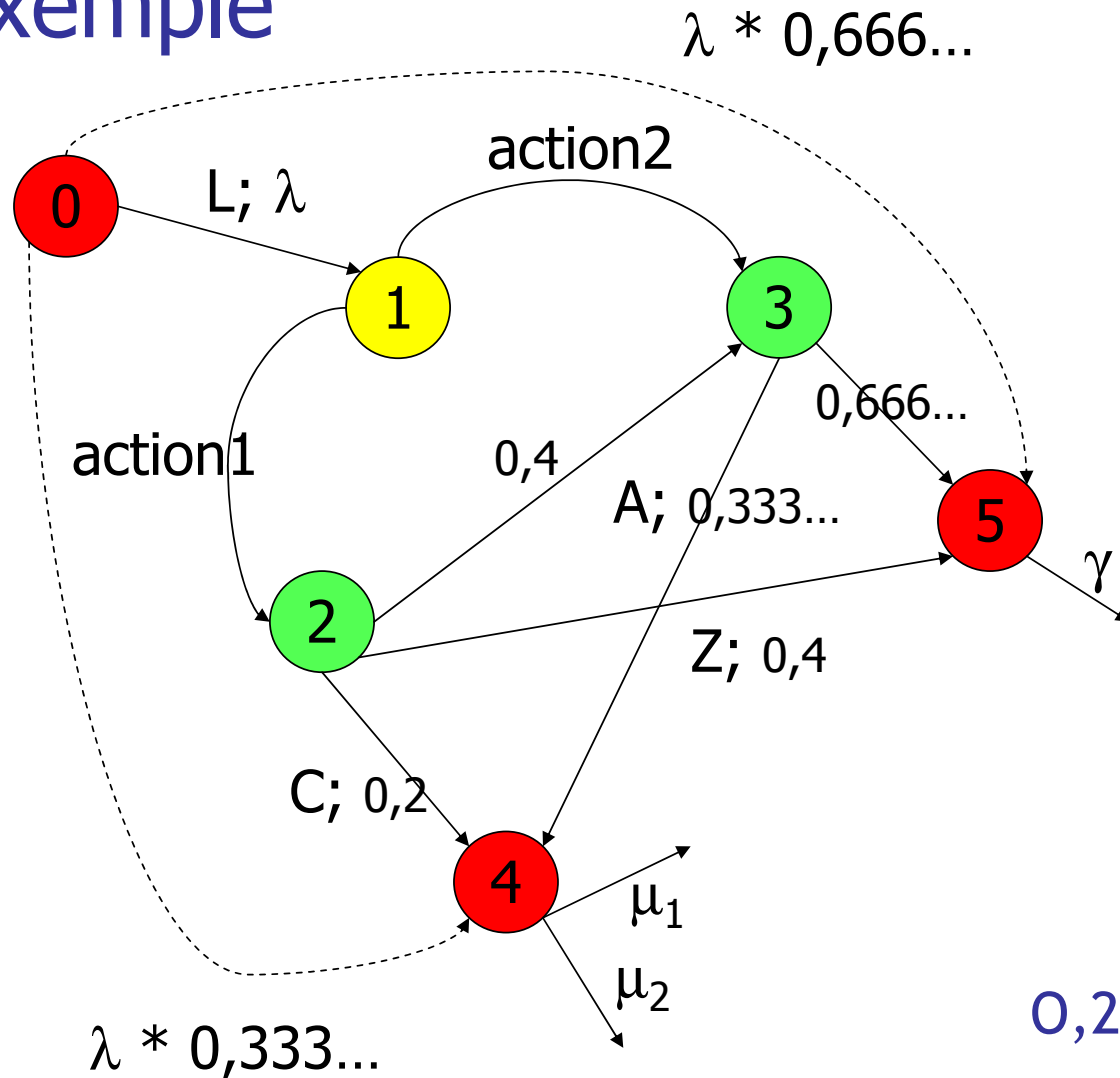
- $\rightarrow$  ERREUR

- pas « bien spécifié »

- $\rightarrow E_1$

# Modèle *bien spécifié*

- Exemple



- État *stable*
- État *décision*
- État *case*

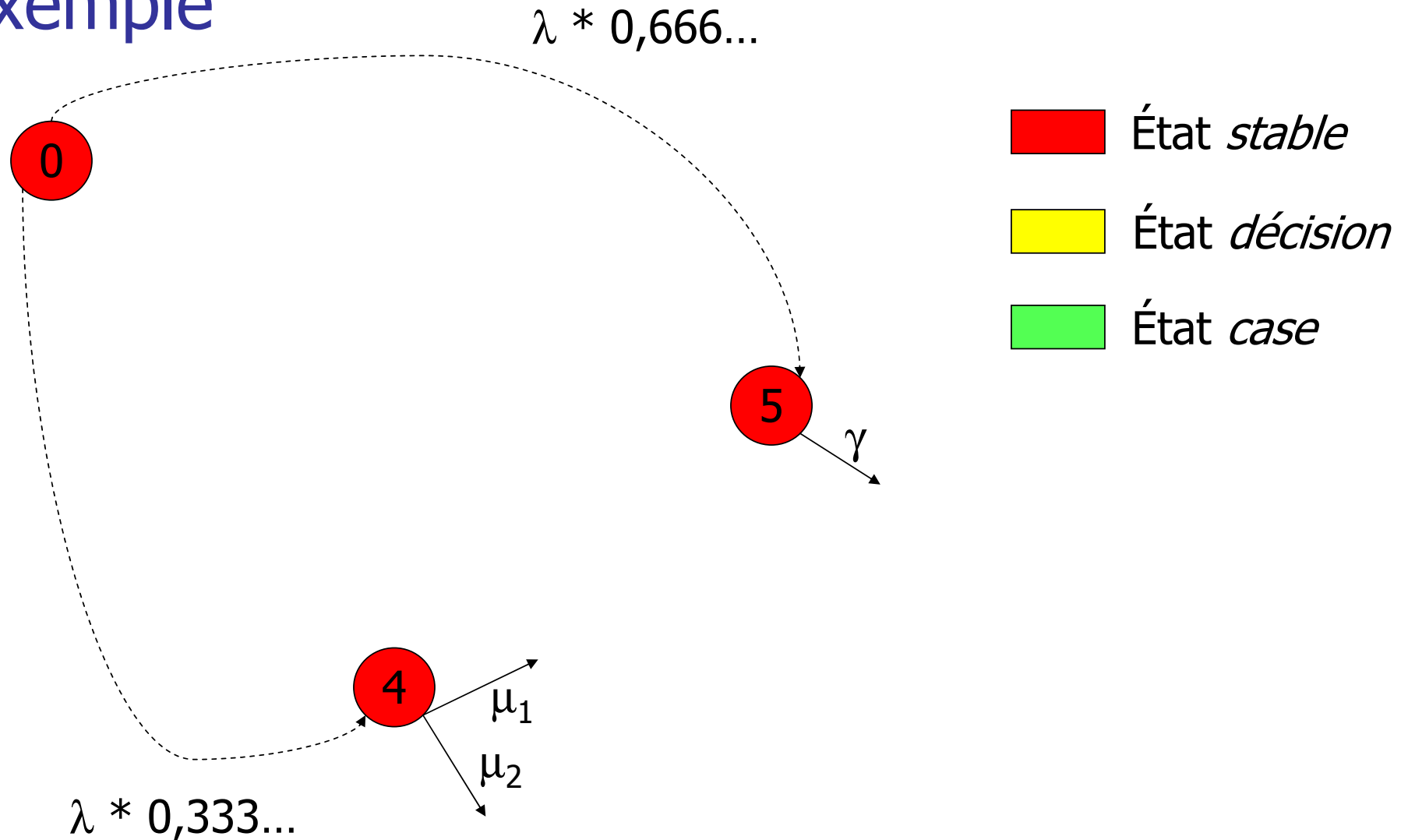
0,333...

et **bien spécifié !**

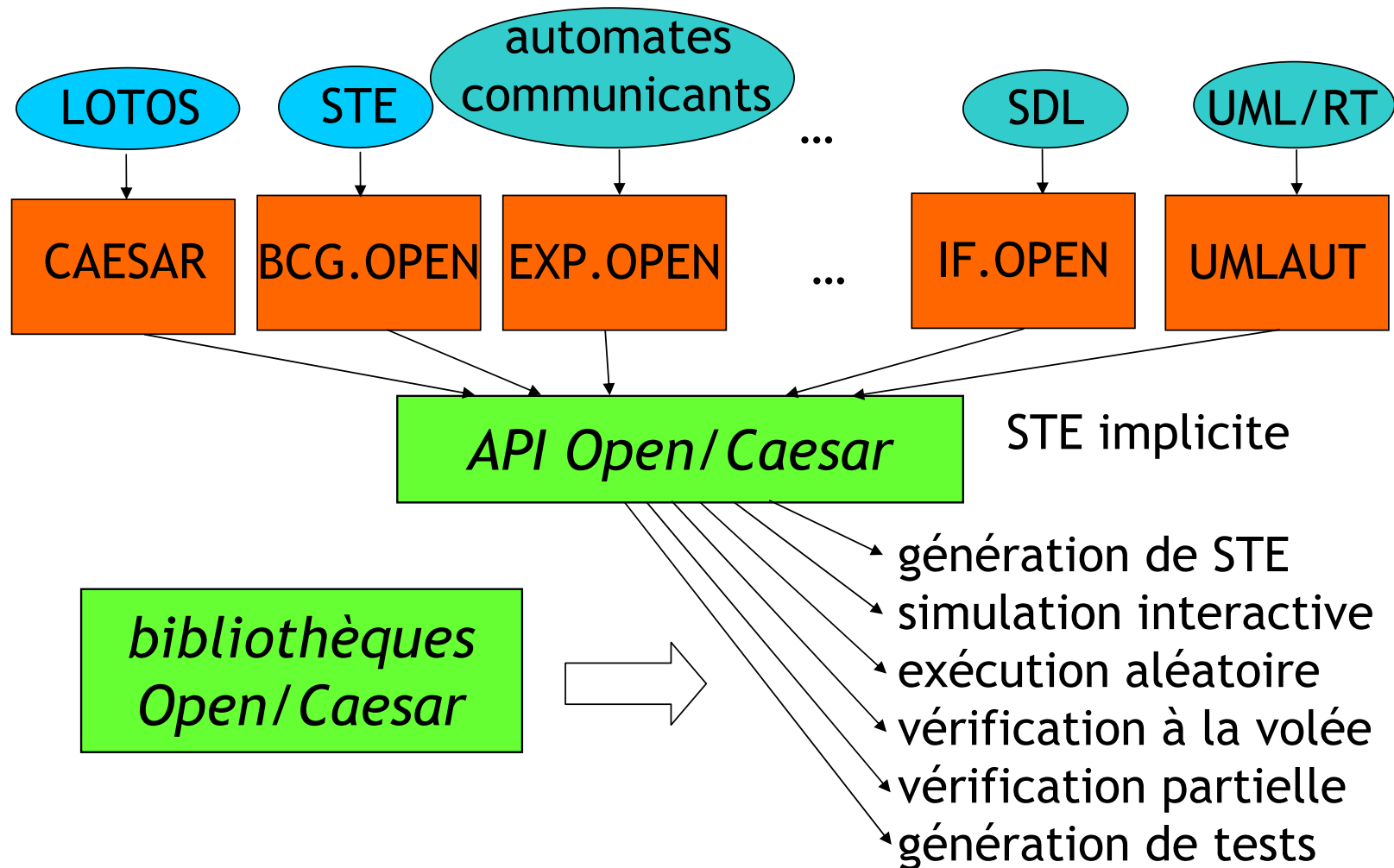
$$0,2 + 0,4 * 0,333\dots = 6/30 + 4/30 = 0,333\dots$$

# Modèle *bien spécifié*

- Exemple

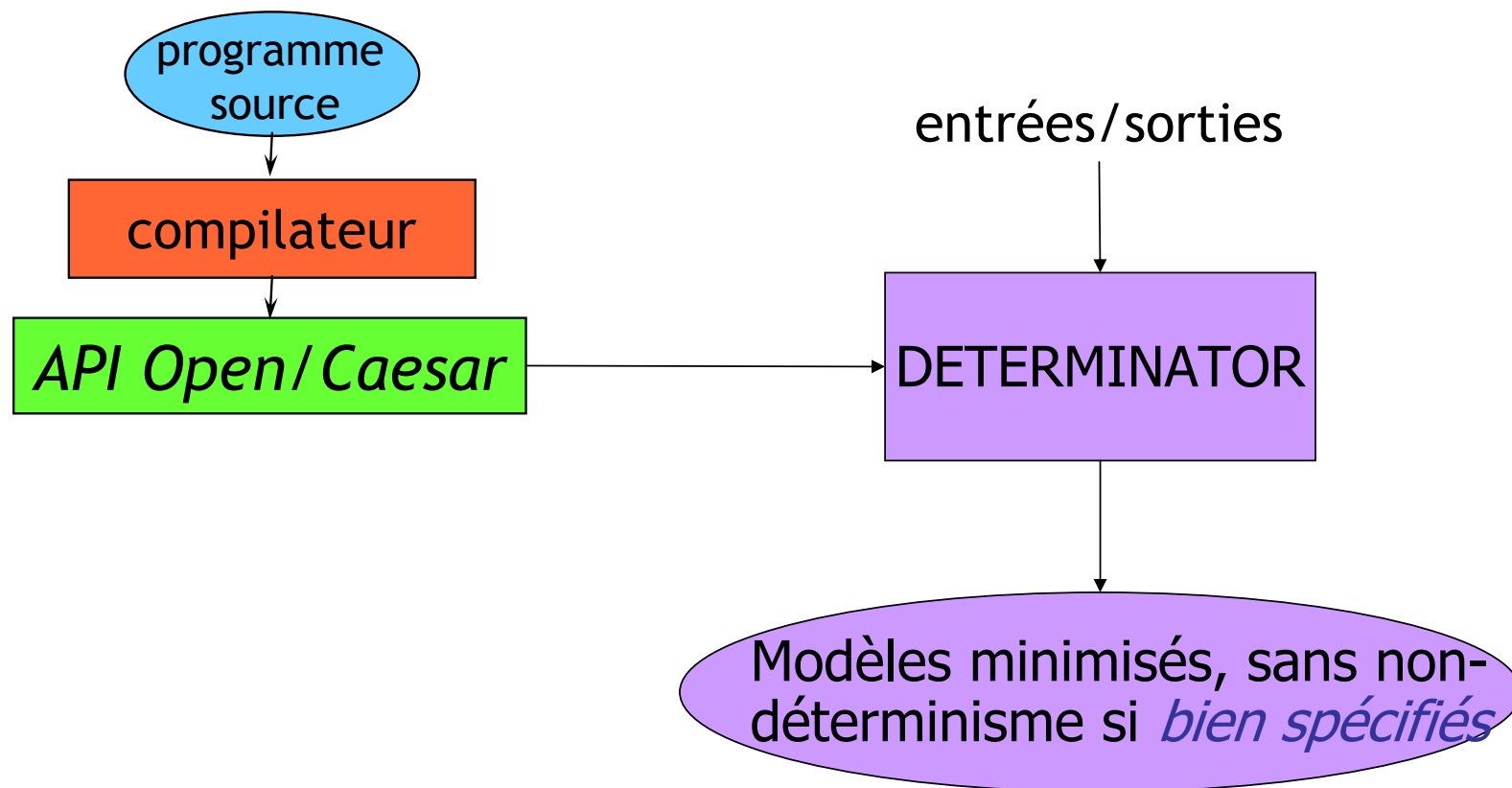


# OPEN/CAESAR

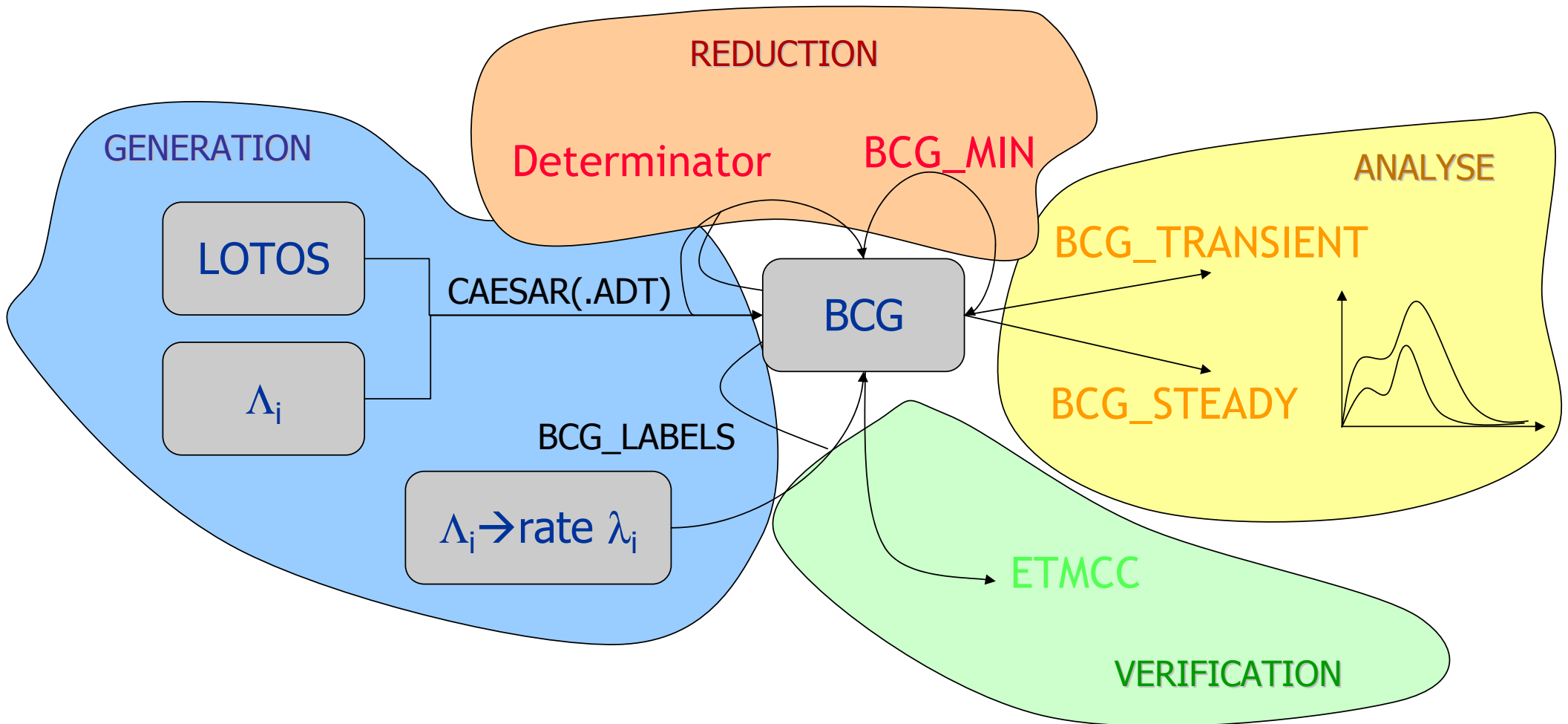


# Intégration du **nouveau** composant

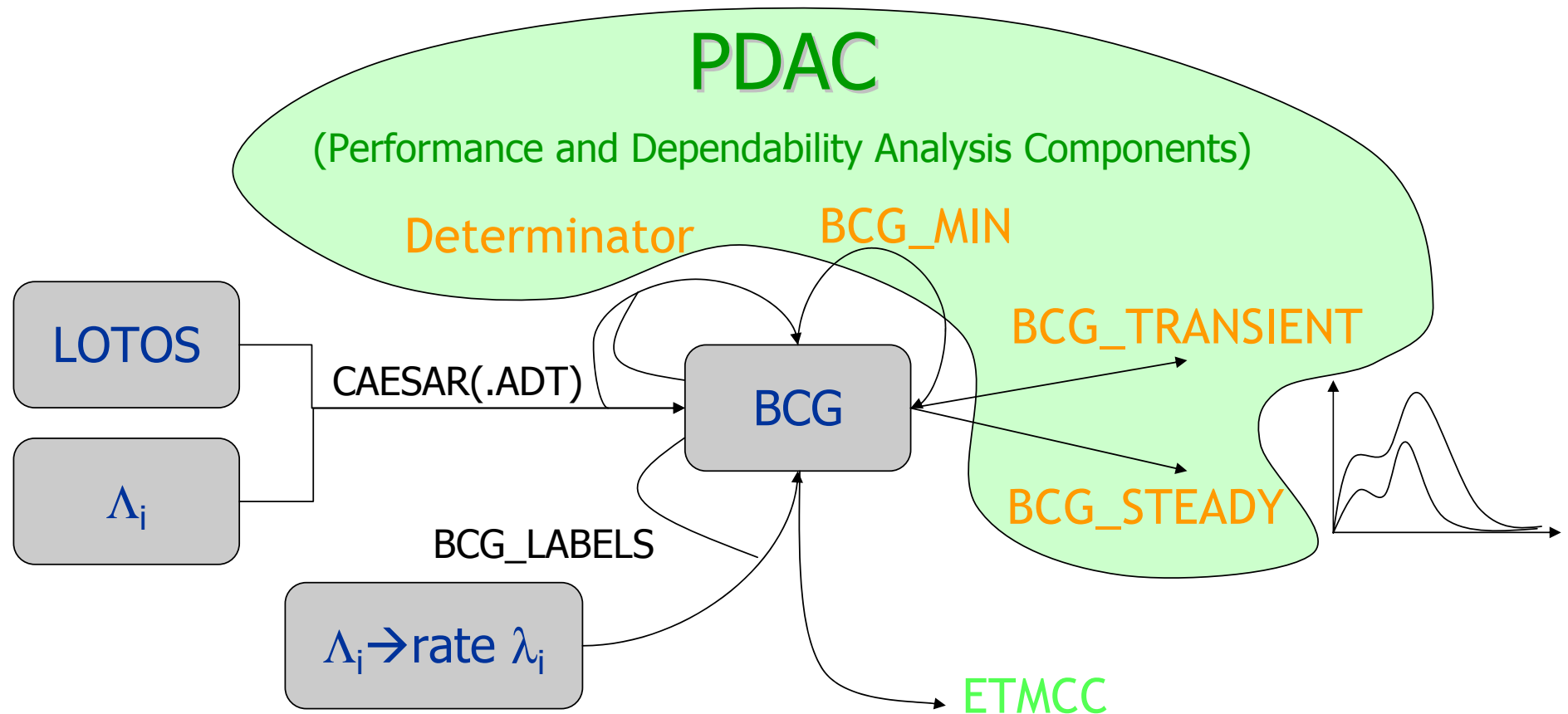
Minimisation à la volée de modèles stochastiques bien spécifiés, contenant du non-déterminisme.



# Évaluation de performance



# Évaluation de performance





# Bilan

- **Un** outil complètement implémenté, utilisant la technologie de CADP :
  - ✦ Determinator : **réducteur** de modèles mixtes
- **PDAC** : une extension de CADP aux aspects temporels des systèmes
  - ✦ Bcg\_Transient
  - ✦ Bcg\_Steady
  - ✦ Bcg\_Min
  - ✦ Determinator
- **Bibliothèque** de fonctions d'analyse de STE mixtes

# Perspectives

- **Intégration** de PDAC dans la prochaine version de CADP (2003)
- Bibliothèque **générique** utilisée par les composants de PDAC
- **Travaux futurs**
  - ✦ Au niveau de la spécification
    - Génération automatique de contraintes stochastiques dans un STE classique
  - ✦ Au niveau de la vérification
    - Connexions à des simulateurs existants
    - Conception de simulateurs Markoviens parallèles