

Apport d'une approche à objets fondée sur les réseaux de Petri à l'analyse des systèmes hybrides

Emilia Villani : Escola Politecnica da USP, São Paulo, Brésil

Jean-Claude Pascal : LAAS-CNRS, Toulouse, France

Paulo Eigi Miyagy : Escola Politecnica da USP, São Paulo, Brésil

Robert Valette : LAAS-CNRS, Toulouse, France

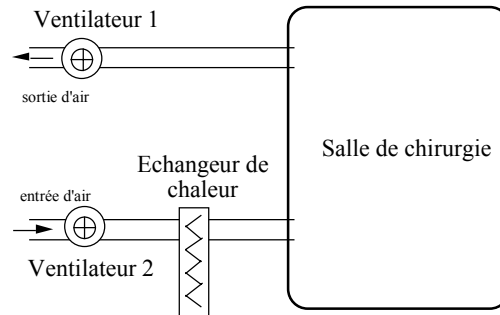
<http://www.laas.fr/~robert>

Objectif

Définir une méthode pour la preuve de propriétés :

- **Compatible avec les techniques de preuve existantes**
- **Compatible avec les outils de spécification utilisés**
- **Non nécessairement automatisée (non décidabilité)**
- **Applicable à des problèmes de complexité moyenne**
- **Concernant les systèmes hybrides**

Exemple de système



Système de conditionnement d'air

Moyens (1)

"Diviser pour régner"

- **Preuve par composition de preuves élémentaires**
- **Partir d'une décomposition en objets (UML)**
- **Décomposer également / dynamiques discrète et continue**
- **Utiliser les réseaux de Petri pour le discret**
 - Systèmes hybrides pour lesquels la dynamique discrète est importante
 - Parallélisme = indépendance
 - Objets à réseaux de Petri / Réseaux de Petri à objets

Moyens (2)

Objets (dynamiques) Hybrides

- **Comportement** : Un réseau de Petri (dynamique discrète)
- **Méthodes**: Syst. équations algébro-différentielles / places RdP (dynamique continue) : phases des méthodes
- **Interactions entre continu et discret** (seuils => transitions)
- **Communications** : Transitions méthodes offertes/requises
- **Variables internes** (continues et discrètes)

Exemple d'objet

$$P_{16} : Q_{ec} = 0$$

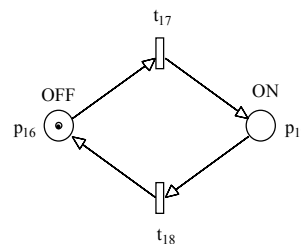
$$P_{17} : \begin{cases} \frac{d\theta_{aux}}{dt} = 1 \\ Q_{ec} = Q_r * \left(1 - \frac{1}{\theta_{aux} + 1}\right) * \left(\frac{2 * m_{air}}{m_{air} + m_T}\right) \end{cases}$$

m_{air} calculé par ventilateur 2
 Q_{ec} utilisé par salle de chirurgie

$$t_{17} : \theta_{aux} = 0$$

$$t_{18} : Q_{ec} = 0$$

t_{17} et t_{18} sont deux méthodes offertes (utilisées par commutateur)



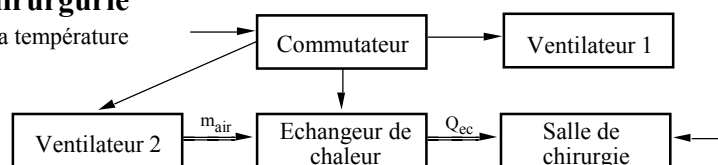
Echangeur de chaleur

Le beurre et l'argent du beurre

- **Une contradiction entre :**
 - Avoir un grand pouvoir descriptif
 - Analyser, prouver formellement et facilement
- **Pas de variable partagée entre les objets**
 - Partage de paramètres constants (au moins pour chaque configuration du système)
 - Utilisation de variables continues calculées dans d'autres objets (pas de cycle de causalité)
- **Des communications rares et définies de façon statique**
 - Pas de diffusion, pas de détermination dynamique du destinataire

Les objets du modèle du système

- **Commutateur/superviseur local**
 - gère les configurations (ventilateurs 1 et 2, échangeur de chaleur)
- **Echangeur de chaleur**
- **Ventilateurs (1 et 2)**
- **Salle de chirurgie**
 - calcul de la température



Preuve modulaire

Liste d'hypothèses nécessaires

$$H_{ei}, \dots, H_{cj}, \dots, H_{dk}, \dots, D_{ml}, \dots \vdash C$$

H_{ei} : environnement global, domaine de validité

H_{cj} : propriétés des variables continues utilisées (domaines par ex.)

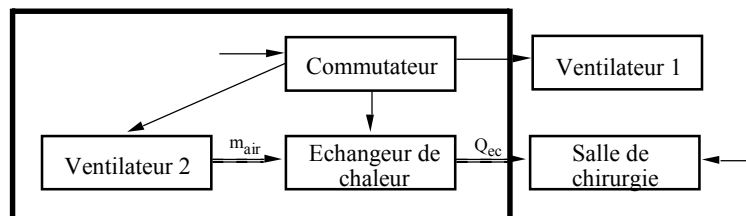
H_{dk} : propriétés de la dynamique discrète globale

D_{ml} : déductions et techniques de preuves applicables dans l'objet étudié

\Rightarrow Obligations de preuves pour les H (sauf H_{ei})

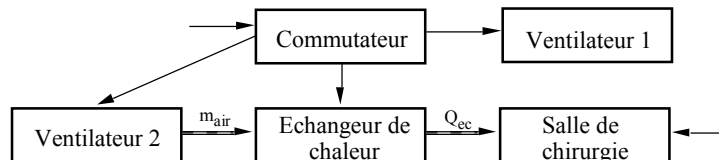
Exemple de preuve 1

- Le ventilateur 2 doit toujours être en fonctionnement quand l'échangeur est en service (correspond à une H_d)
- On construit le réseau de Petri du système des 3 objets
- On exhibe un invariant (poids positifs et négatifs)



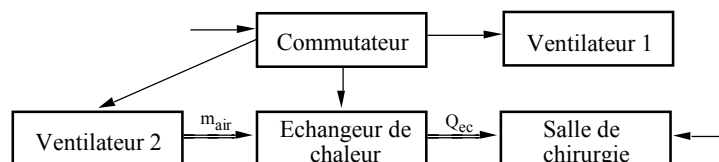
Exemple de preuve 2 (1)

- On passe de T_0 à T_f avant la date θ_i (objet "salle de chirurgie")
- H_{ei} : Etat initial; L'objet "commutateur" n'est pas arrêté
- H_{cl} : $\int Q_{ec} < K$ dans "échangeur" (\Rightarrow obligation de preuve)



Exemple de preuve 2 (2)

- C : $\int Q_{ec} < K$ dans "échangeur"
- H_{ei} : Etat initial; L'objet "commutateur" n'est pas arrêté
- m_{air} est une constante : preuve 1 (H_d et obligation de preuve)



Conclusion

- **Découper pour transformer une preuve complexe en un ensemble de preuves plus simples**
- **Permet d'aborder des domaines où la décidabilité n'existe pas**

MAIS

- **Preuves "manuelles"**
- **Il faut limiter le pouvoir d'expression**
 - Fusions statiques des transitions
 - Pas de cycle de dépendance des variables