Génération, vérification formelle et simulation de séquences de conduite pour un système complexe critique

Thomas Cochard, David Gouyon, Jean-François Pétin

Génération, vérification formelle et simulation de séquences de conduite pour un système complexe critique

Thomas Cochard, David Gouyon, Jean-François Pétin

thomas.cochard@univ-lorraine.fr

Contexte & problématique industrielle

- Contexte : **conduite de procédés industriels complexes à risques**
- Problématique industrielle : service d'aide à la décision pour la préparation de **séquences d'actions de conduite** (passage d'un état donné de l'installation à un état cible)
  - en réaction à des aléas (non disponibilité des matériels, modifications des objectifs de conduite, ...)
  - en tenant compte : de l'état actuel de l'installation, de la structure du système à conduire, des contraintes de sécurité, ...

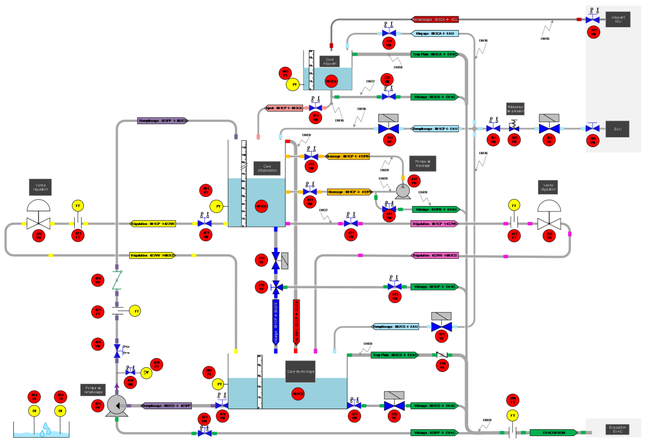


Figure 1: *Plateforme CISPI du CRAN*

Problématique scientifique adressée

→ Comment **générer/vérifier formellement** une séquence permettant d'atteindre un objectif défini ?

→ Comment **modéliser le système d'intérêt** pour assurer un **passage à l'échelle** des travaux ?

Approches existantes

Modélisation de systèmes complexes [Alur *et al.* 1994, ISA88 1998]

- Modélisation de systèmes réactifs hiérarchisés
- Prise en compte d'éléments hétérogènes (états, disponibilités, grandeurs physiques, ...)

Génération de séquences [Rivas *et al.* 1974, Li *et al.* 1997]

- Démonstration de l'existence d'une séquence d'action faisable (respectant les diverses contraintes de sécurité et de sûreté)
- Extension à la recherche d'un ensemble de solution faisables

Vérification de séquences [Baier *et al.* 2008, Li *et al.* 2014]

- Formalisation d'une séquence d'action en vue de sa vérification
- Simulation de la séquence pour vérifier à la fois l'atteinte de l'objectif et le respect des contraintes

Applicabilité d'approches existantes

ÉVALUATION de faisabilité de génération automatique d'une séquence d'actions basée sur une combinaison d'approches existantes : modèles en automates communicants avec une structuration basée sur la norme ISA88 et mécanisme de recherche d'atteignabilité [Cochard *et al.* 2015a, 2015b]

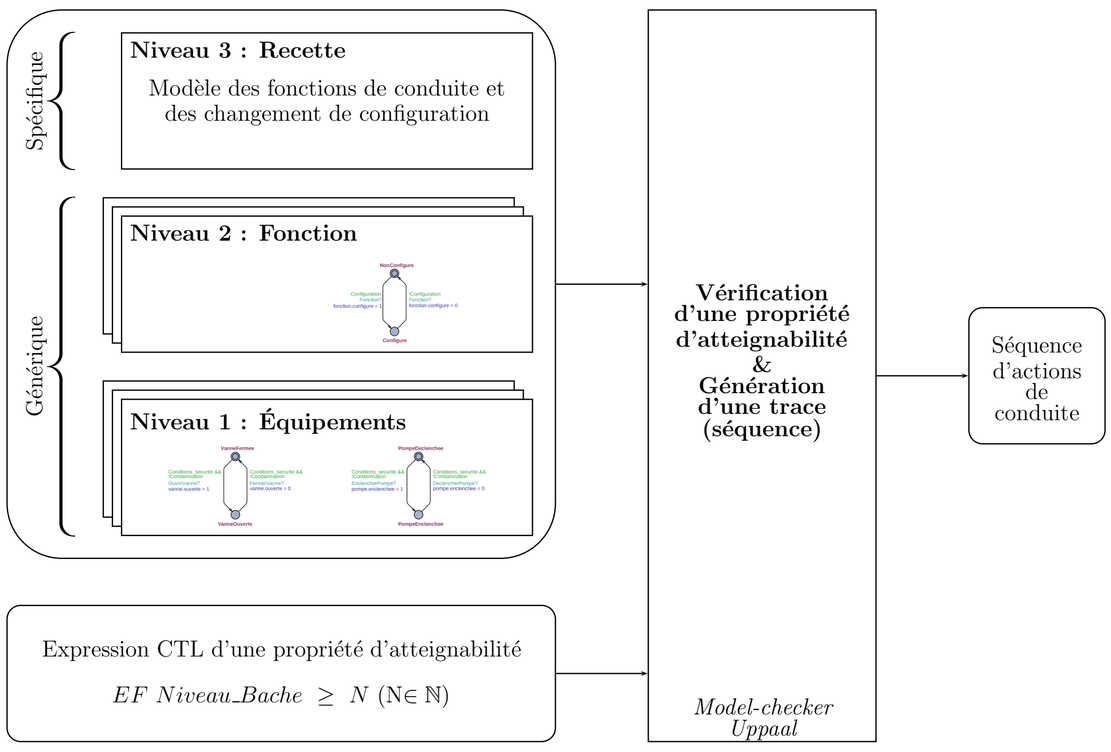


Figure 2: *Approche de génération de séquences*

Publications

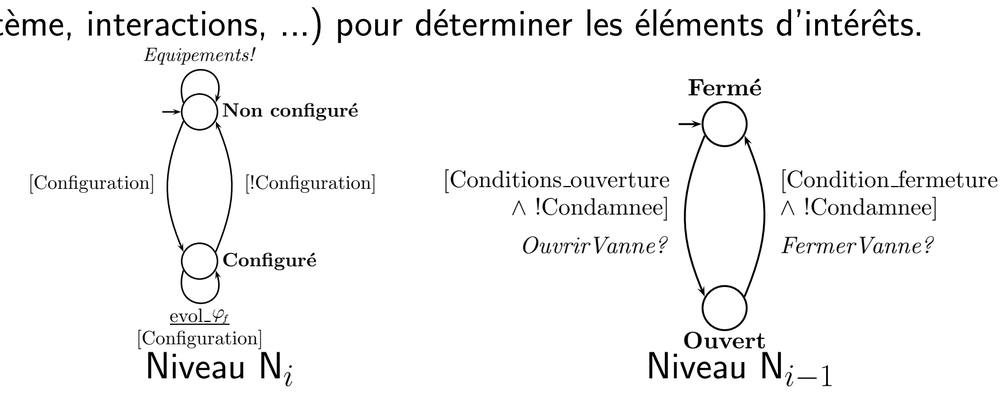
(Cochard *et al.*, 2015a) Thomas Cochard, David Gouyon, Jean-François Pétin. Génération de séquences d'actions sûres par recherche d'atteignabilité. Génie logiciel, 2015, Mars 2015 (112), pp.43-50.

(Cochard *et al.*, 2015b) Thomas Cochard, David Gouyon, Jean-François Pétin. Generation of safe plant operation sequences using reachability analysis. 20th IEEE Conference on Emerging Technologies & Factory Automation. ETFA 2015, September 2015, Luxembourg, Luxembourg.

Proposition d'une approche de modélisation pour réduire l'espace d'état

Apports de la conduite par objectif

PARCOURS de l'espace d'état limité aux éléments nécessaires et suffisants : utilisation de connaissances métiers (structure du système, interactions, ...) pour déterminer les éléments d'intérêts.



→ **Première réduction de l'espace d'état**

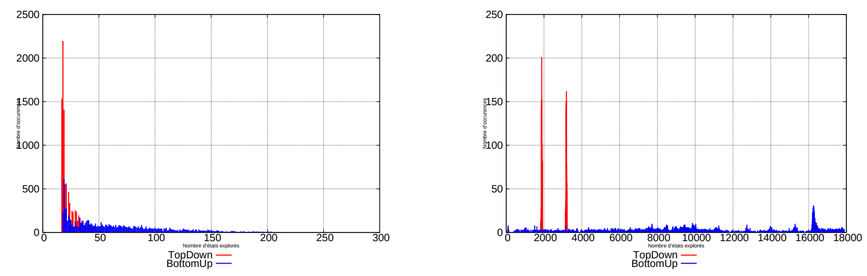


Figure 3: *Étude comparative des deux approches*

Apports des techniques de réduction/d'abstraction de modèles

ON propose de combiner l'approche précédente avec une **technique d'abstraction** et de décomposer l'organisation hiérarchisée du système en k niveaux $N_{k-1} \dots N_0$ par paires de niveaux (N_{i+1}, N_i) :

1. Modèle A, détaillé, au niveau N_{i+1}
2. Modèles B_j, abstraits, au niveau N_i

afin de construire un modèle de niveau $\mathcal{M}_{(N_{i+1},N_i)}$ tel que :

$$\mathcal{M}_{(N_{i+1},N_i)} = A||B_1||B_2|| \dots ||B_j$$

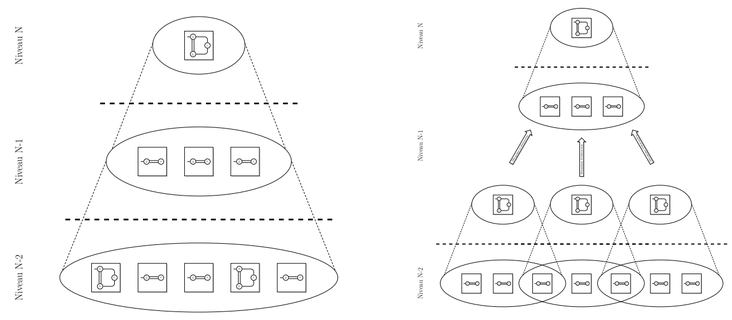


Figure 4: *Découpage du système par niveaux hiérarchiques*

Perspectives

- Proposition d'une **démarche systématique d'abstraction**
- **Preuve d'équivalence** entre les modèles abstraits et détaillés
- **Application** sur un cas d'étude industriel