Application des méthodes formelles au contrôle du véhicule autonome

Yann Duplouy

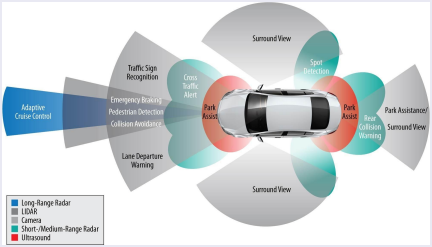
IRT SystemX et LSV

lundi 26 novembre 2018

Encadrants :
Serge Haddad et Béatrice Bérard

Développement des véhicules autonomes

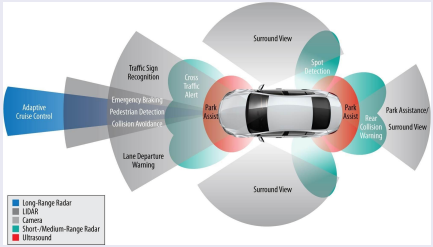
Des options d'aide à la conduite de plus en plus évoluées



- aide au freinage ;
- reconnaissance des panneaux ;
- conduite sur autoroute, etc.

Développement des véhicules autonomes

Des options d'aide à la conduite de plus en plus évoluées



- aide au freinage ;
- reconnaissance des panneaux ;
- conduite sur autoroute, etc.


Les Echos.fr

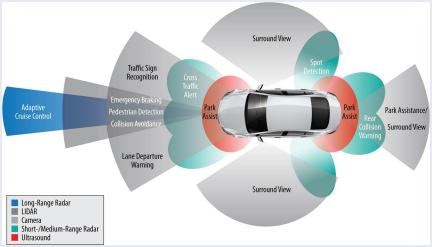
LES ECHOS: Tapez votre recherche OK

automobile

Accident mortel en Arizona : le véhicule autonome a détecté le piéton, sans l'éviter

Développement des véhicules autonomes

Des options d'aide à la conduite de plus en plus évoluées



- aide au freinage ;
- reconnaissance des panneaux ;
- conduite sur autoroute, etc.

Tests en situations réelles

- Risque d'accident ;
- Temps de roulage important ;
- Garantie limitée.

Illustration : Voie d'insertion

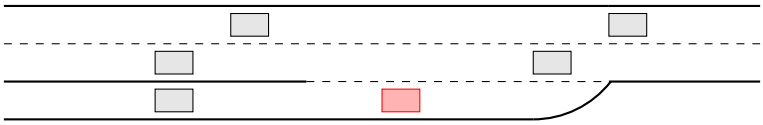


Illustration : Voie d'insertion

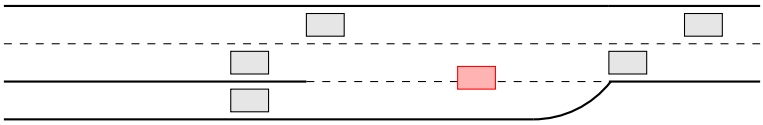


Illustration : Voie d'insertion

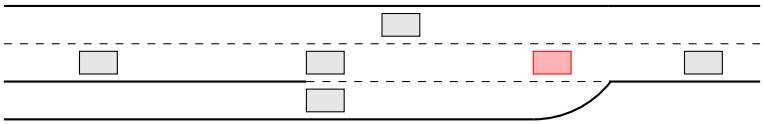
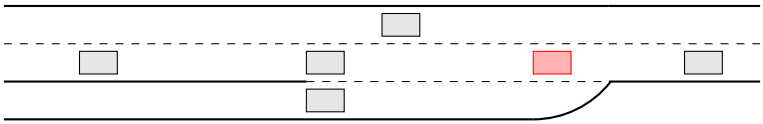


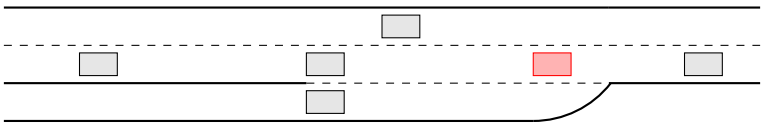
Illustration : Voie d'insertion



Paramètres de la simulation

- Caractéristiques de l'infrastructure ;
- Densité du trafic ;
- Comportements des autres véhicules.

Illustration : Voie d'insertion



Indices de performance

- Nature et taux de collision ;
- Force de la collision ;
- Position de la collision.

Défis scientifiques

Impossibilité d'une validation globale, d'où la nécessité :

- d'identifier les composants du véhicule à valider ;
- de caractériser les situations pertinentes.

Étapes préliminaires à la modélisation :

- choix du grain de modélisation ;
- description de l'environnement (possiblement aléatoire).

[Althoff *et al.* 2010, Bérard *et al.* 2008, Rizaldi *et al.* 2015, Rajhans 2013, Asplund *et al.* 2012]

Quel cadre pour l'évaluation de contrôleurs ?

Formalisation d'un système dynamique

- Des lois physiques pour la mécanique ;
- Des décisions du contrôleur ;
- Un environnement imprévisible.

$\Rightarrow$ Besoin d'un système hybride non-déterministe ou probabiliste.

Quel cadre pour l'évaluation de contrôleurs ?

Formalisation d'un système dynamique

- Des lois physiques pour la mécanique ;
- Des décisions du contrôleur ;
- Un environnement imprévisible.

$\Rightarrow$ Besoin d'un système hybride non-déterministe ou probabiliste.

Systèmes dynamiques

Uppaal
Simulink, etc

Systèmes probabilistes

Prism
Cosmos, etc

Objectifs

[*Integrating Simulink Models into the Model-Checker Cosmos*, Petri Nets 2018]

- Définir un **formalisme** pour les environnements véhiculaires ;
  - Fournir une **sémantique** de Simulink (modèles de contrôleurs), [Chapoutot 08, BBCP 11, BC 12]
  - Définir une **syntaxe** et **sémantique** des échanges entre les deux formalismes
- Développement de l'outil Cosmos ;
  - **Implémenter** cette sémantique dans l'outil Cosmos,
  - **Étendre** l'implémentation à la communication multi-modèles.

[*Statistical Model-Checking for Autonomous Vehicle Safety Validation*, SIA Simulation Numérique 2017]

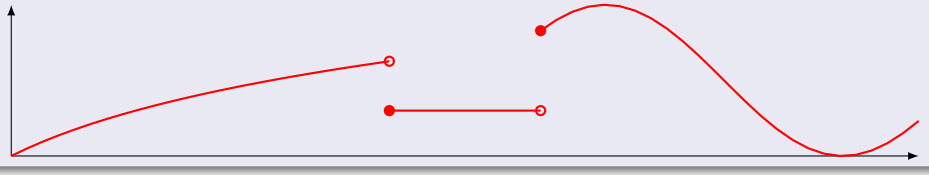
- **Valider** empiriquement la pertinence de l'approche

Plan

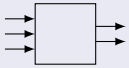
Composants de base de Simulink

Signal

Fonction à valeurs réelles, continue à droite avec limite à gauche.



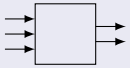
Briques de base : les blocs



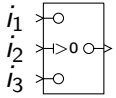
- Signaux d'*entrée* et de *sortie*
- *Opérateurs* avec paramètres

Composants de base de Simulink

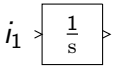
Briques de base : les blocs



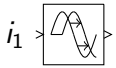
- Signaux d'*entrée* et de *sortie*
- *Opérateurs* avec paramètres



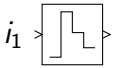
$$\mathrm{op}(i_1, i_2, i_3)(t) = \text{si } i_2(t) > 0 \text{ alors } i_1(t) \text{ sinon } i_3(t)$$



$$\mathrm{op}(i_1)(t) = v_0 + \int_{t_0}^{t} i_1(\tau)\mathrm{d}\tau$$

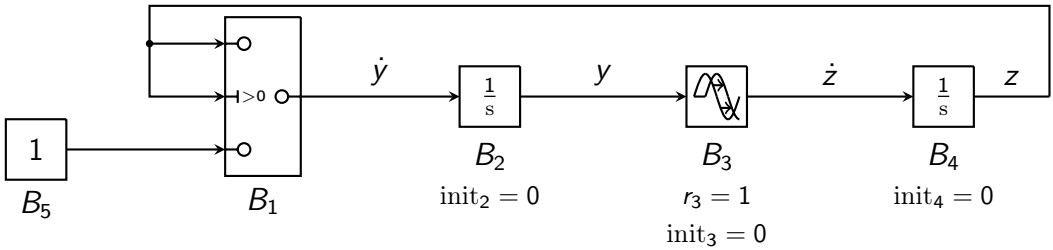


$$\mathrm{op}(i_1)(t) = \text{si } t \geq t_0 + r \text{ alors } i_1(t - r) \text{ sinon } v_0$$

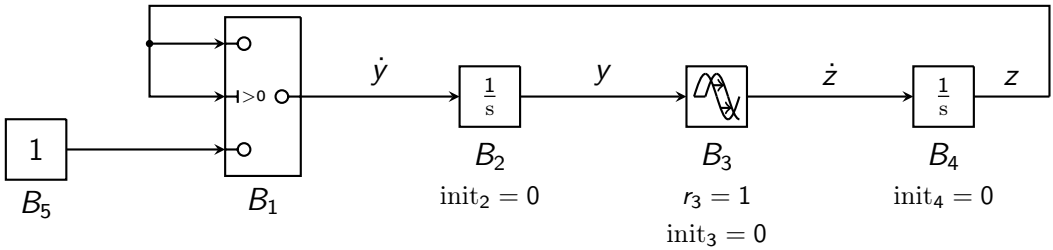


$$\mathrm{op}(i_1)(t) = i_1\left(t_0 + d\left\lfloor \frac{t - t_0}{d} \right\rfloor\right)$$

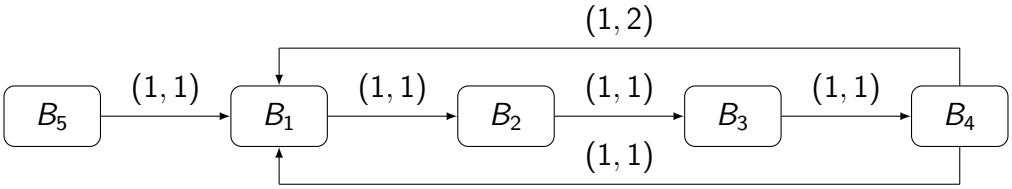
Architecture d'un modèle Simulink



Architecture d'un modèle Simulink



Correction : absence d'un circuit immédiat

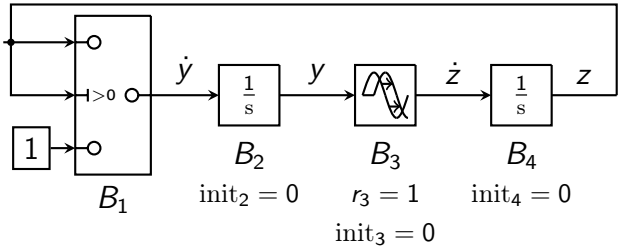


Démarche

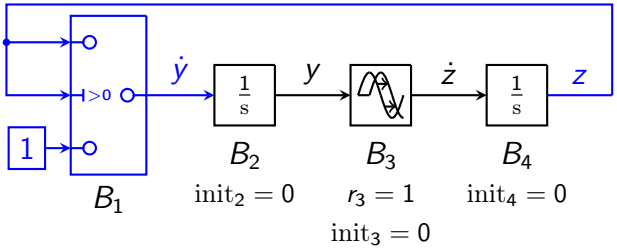
Définir une sémantique opérationnelle caractérisée par sa trajectoire :
le vecteur $\vec{w}$ des valeurs des signaux de sortie
sur un intervalle de simulation $\mathbb{T} = [t_0, t_{end}]$.

- Sémantique exacte
- Sémantique opérationnelle
  - implémentable efficacement,
  - avec une garantie de précision.

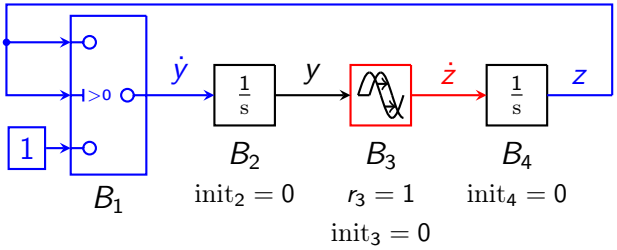
Des graphes arrières aux équations différentielles paramétrées



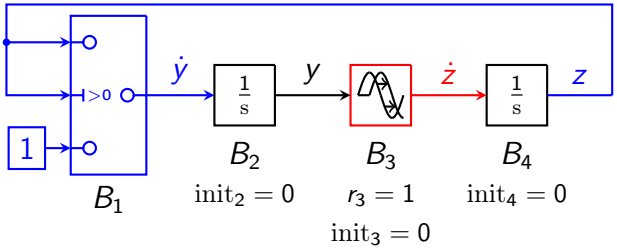
Des graphes arrières aux équations différentielles paramétrées



Des graphes arrières aux équations différentielles paramétrées



Des graphes arrières aux équations différentielles paramétrées



Des équations différentielles paramétrées

$\dot{z}(t) = s_3(t)$ nécessite la détermination de $s_3(t) = y(t - r_3)$

$\dot{y}(t) = \text{si } z(t) > 0 \text{ alors } z(t) \text{ sinon } 1$ requiert l'élimination de la conditionnelle

Instanciation en équations différentielles

Établir les systèmes d'équation différentielles dépendant :

- du *mode* pour les blocs à seuils ;
- de l'*historique* pour les blocs à retard.

Instanciation en équations différentielles

Établir les systèmes d'équation différentielles dépendant :

- du *mode* pour les blocs à seuils ;
- de l'*historique* pour les blocs à retard.

Équations différentielles paramétrées

$$\dot{z}(t) = s_3(t)$$

$$\dot{y}(t) = \text{si } z(t) > 0 \text{ alors } z(t) \text{ sinon } 1$$

Équations différentielles sur $[0, 1]$
mode $z(t) \in]-\infty, 0]$, historique $s_3(t) = 0$

$$\dot{z}(t) = 0$$

$$\dot{y}(t) = 1$$

Sémantique exacte : $\vec{w}$ est une trajectoire si

Il existe

- une partition $\mathbb{T} = \bigcup_{i=0}^{N-1} [t_i, t_{i+1}]$
- un mode m_i sur chaque intervalle $[t_i, t_{i+1}]$ cohérent avec $\vec{w}$

tels que pour tout i

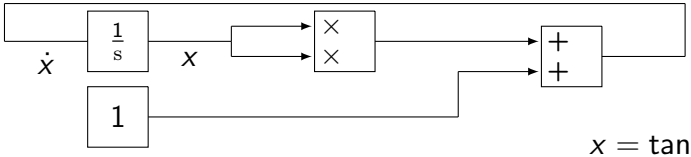
- il n'y a aucun échantillonnage dans $[t_i, t_{i+1}]$;
- tous les retards positifs sont plus grands que $t_{i+1} - t_i$;

et

$\vec{w}$ est solution de ED_i sur $[t_i, t_{i+1}]$ où $\mathrm{ED_i}$ est l'équation différentielle instanciée selon le mode m_i et la valeur de $\vec{w}$ sur $[t_0, t_i]$.

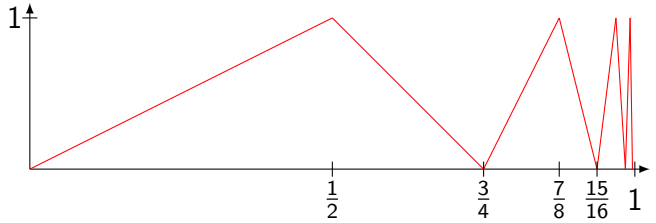
Cas sans trajectoire

- Équation différentielle sans solution sur l'intervalle de simulation :



$$\dot{x} = 1 + x^2$$
$$\mathbb{T} = [0, \tfrac{\pi}{2}]$$
$$x = \tan(t) \text{ sur } [0, \tfrac{\pi}{2}[$$

- Infinité de franchissements de seuil :



$$\mathbb{T} = [0, 1]$$

Résultats sur la sémantique exacte

Théorème (Unicité)

Un SK-modèle a au plus une trajectoire.

Théorème (Indécidabilité)

Le problème de l'existence d'une trajectoire d'un SK-modèle est indécidable.

De la sémantique exacte à une sémantique approchée

Problèmes de la sémantique exacte

- Le type réel ($\mathbb{R}$) n'est pas implémentable ;
- La sémantique dépend d'une infinité de valeurs sur les intervalles $[t_0, t_{\text{end}}]$;
- L'intégration requiert généralement une méthode numérique.

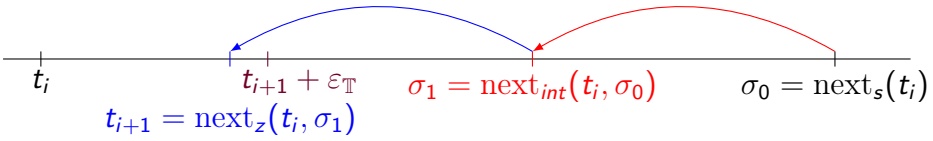
Défis de la sémantique approchée

- Calcul du prochain pas de temps selon les changements discrets ;
- Intégration à pas variable nécessaire ;
- Interpolation requise pour l'évaluation des blocs à retard.

Sémantique approchée $(\varepsilon_{\mathbb{T}}, \varepsilon_V)$

Principe général

1. construction *itérative* des instants d'échantillonnage $(t_i)_{i \in I}$:
   - contraintes statiques (next_s) ;
   - contraintes liées à l'intégration (next_{int}) ;
   - recherche des franchissements de seuil à ε_V près (next_z).
2. calcul des valeurs des signaux correspondants ;
3. calcul sur $]t_{i+1}, t_{i+1} + \varepsilon_{\mathbb{T}}]$ des valeurs de signaux pour déterminer le mode.



Résultats sur la sémantique approchée

Conjecture

Sous certaines conditions de franchissement de seuils,
pour tout modèle admettant $\vec{w}$ comme trajectoire exacte et pour tout $\varepsilon > 0$
il existe $\varepsilon_{\mathbb{T}}$ et ε_V tels que $\|\vec{w}_{\varepsilon_{\mathbb{T}},\varepsilon_V} - \vec{w}\| \leq \varepsilon$.

Résultats sur la sémantique approchée

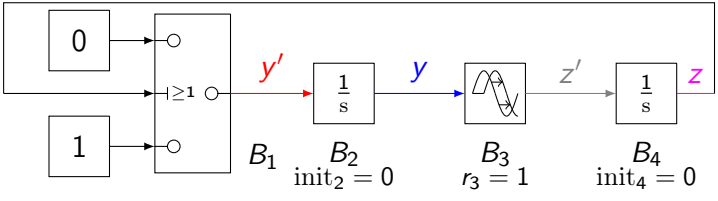
Conjecture

Sous certaines conditions de franchissement de seuils,
pour tout modèle admettant $\vec{w}$ comme trajectoire exacte et pour tout $\varepsilon > 0$
il existe $\varepsilon_{\mathbb{T}}$ et ε_V tels que $\|\vec{w}_{\varepsilon_{\mathbb{T}},\varepsilon_V} - \vec{w}\| \leq \varepsilon$.

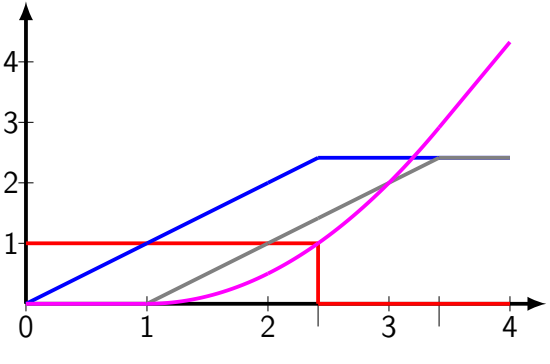
- Cette sémantique est opérationnelle et implémentée dans Cosmos.
- Elle répond aux objectifs attendus :
  - Efficacité,
  - Précision.

  Validation empirique dans Cosmos.

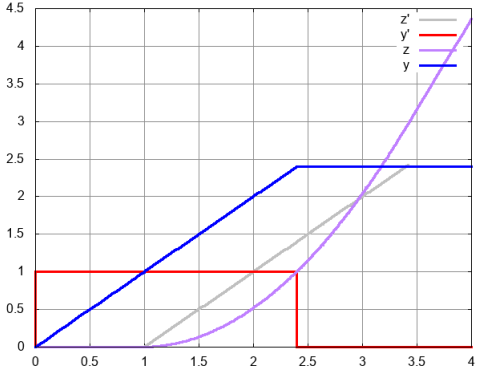
Illustration



Sémantique exacte



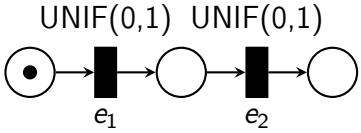
Sémantique approchée (Cosmos)



Plan

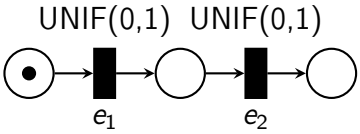
Réseaux de Petri stochastiques colorés

RdP stochastique

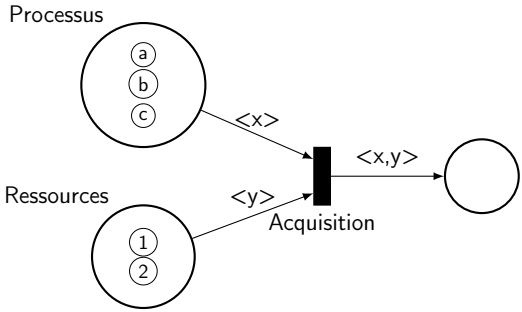


Réseaux de Petri stochastiques colorés

RdP stochastique

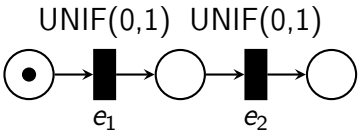


RdP coloré

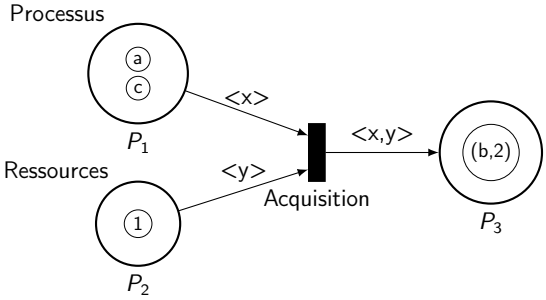


Réseaux de Petri stochastiques colorés

RdP stochastique



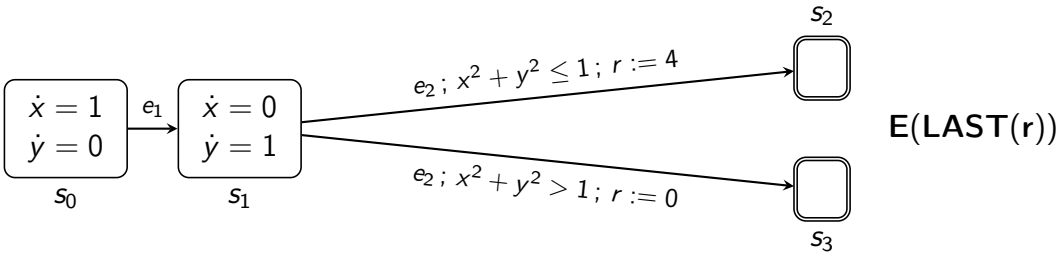
RdP coloré



La logique HASL : calcul de π

Formule HASL

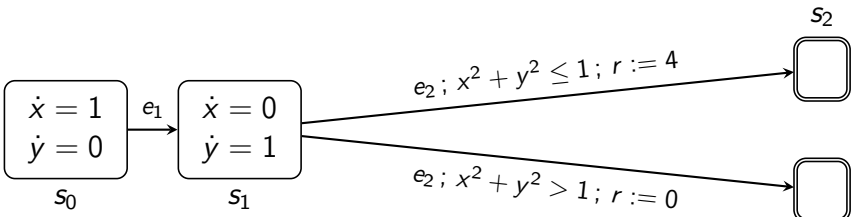
Un automate hybride déterministe et une expression.



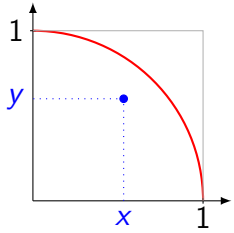
La logique HASL : calcul de π

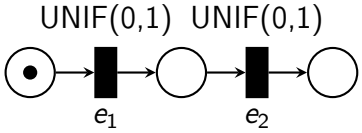
Formule HASL

Un automate hybride déterministe et une expression.



E(LAST(r))





Cosmos : un *model-checker* statistique complet et efficace

Comparaison à un seuil

- test statique ;
- test séquentiel (test de Wald).

Estimation par un intervalle de confiance

- bornes de Clopper-Pearson (statique, distribution binomiale) ;
- bornes de Chernoff-Hoeffding (statique, v.a. bornée) ;
- bornes de Chow-Robbins (séquentiel, valide si largeur IC $\to 0$) ;
- approximation gaussienne (statique, valide si $N_{sim} \to +\infty$).

Simulation à évènements discrets

Évènements

- Les évènements sont *concurrents* ;
- Un évènement consiste en un identifiant, un temps absolu, une priorité et un poids aléatoire.

Simulation à évènements discrets

Évènements

- Les évènements sont *concurrents* ;
- Un évènement consiste en un identifiant, un temps absolu, une priorité et un poids aléatoire.

File d'évènements

Les évènements sont ordonnés dans une file

Simulation à évènements discrets

Évènements

- Les évènements sont *concurrents* ;
- Un évènement consiste en un identifiant, un temps absolu, une priorité et un poids aléatoire.

File d'évènements

Les évènements sont ordonnés dans une file

Boucle de simulation

- Extraire l'évènement programmé «le plus tôt» ;
- Mettre à jour l'état selon le type de l'évènement ;
- Retirer les évènements désactivés ;
- Insérer les évènements nouvellement activés.

Extension à la simulation multi-modèles

Boucle de simulation

- Choix d'une file *unique* ;
- Affectation de l'évènement courant au modèle correspondant.

Extension à la simulation multi-modèles

Boucle de simulation

- Choix d'une file *unique* ;
- Affectation de l'évènement courant au modèle correspondant.

Solution générique.

Extension à la simulation multi-modèles

Boucle de simulation

- Choix d'une file *unique* ;
- Affectation de l'évènement courant au modèle correspondant.

Solution générique.

Communication entre modèles

- *Format* des données échangées ;
- *Caractéristiques* de leur synchronisation.

Extension à la simulation multi-modèles

Boucle de simulation

- Choix d'une file *unique* ;
- Affectation de l'évènement courant au modèle correspondant.

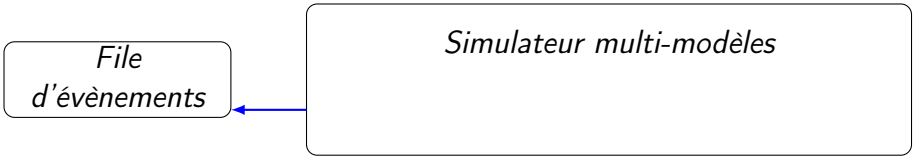
Solution générique.

Communication entre modèles

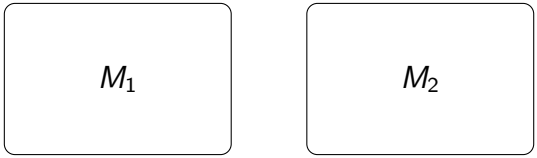
- *Format* des données échangées ;
- *Caractéristiques* de leur synchronisation.

Solution *ad hoc* : Réseau de Petri stochastique coloré et SK-modèle.

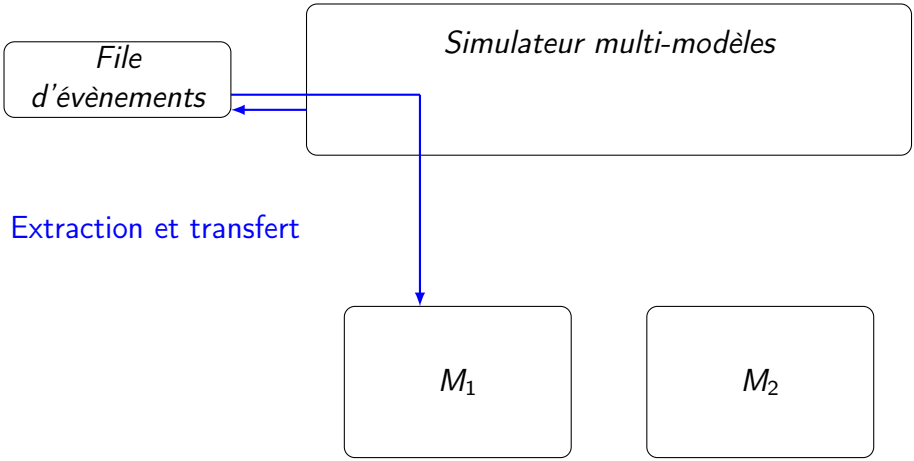
Simulation multi-modèles



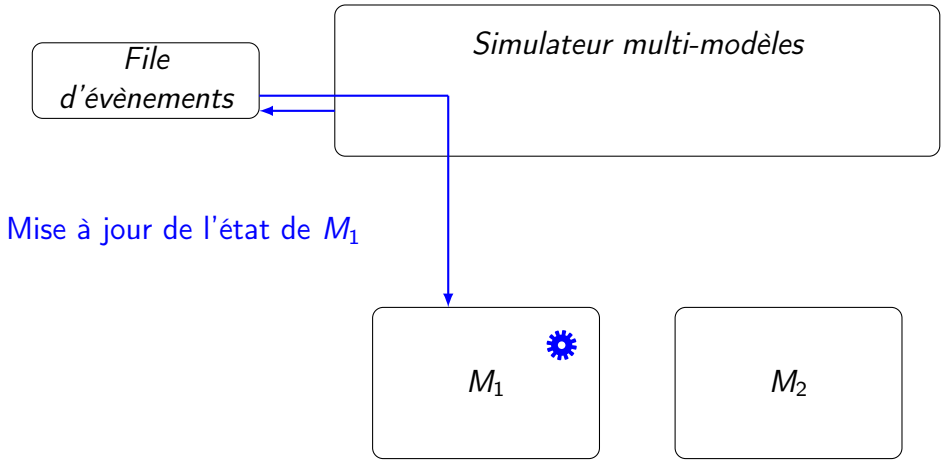
Requête d'évènement



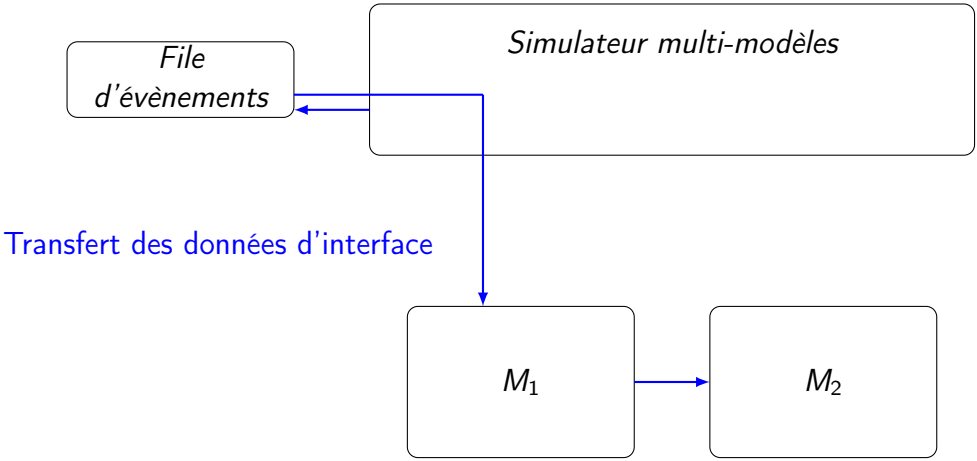
Simulation multi-modèles



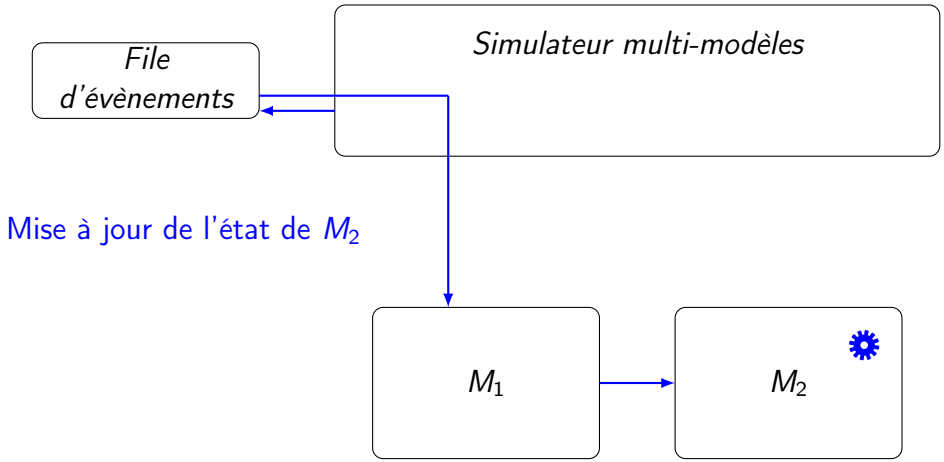
Simulation multi-modèles



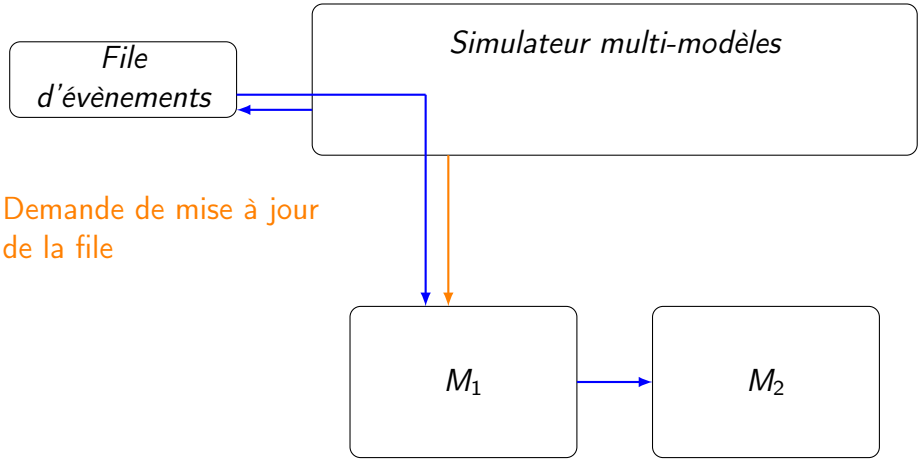
Simulation multi-modèles



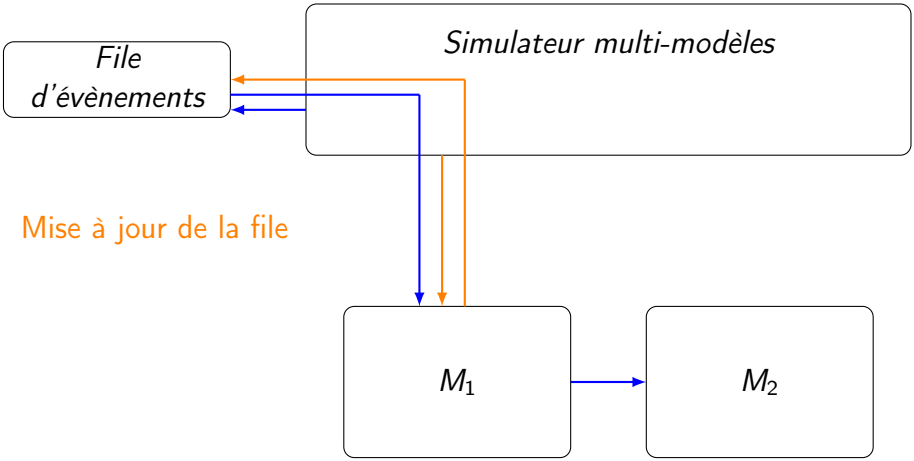
Simulation multi-modèles



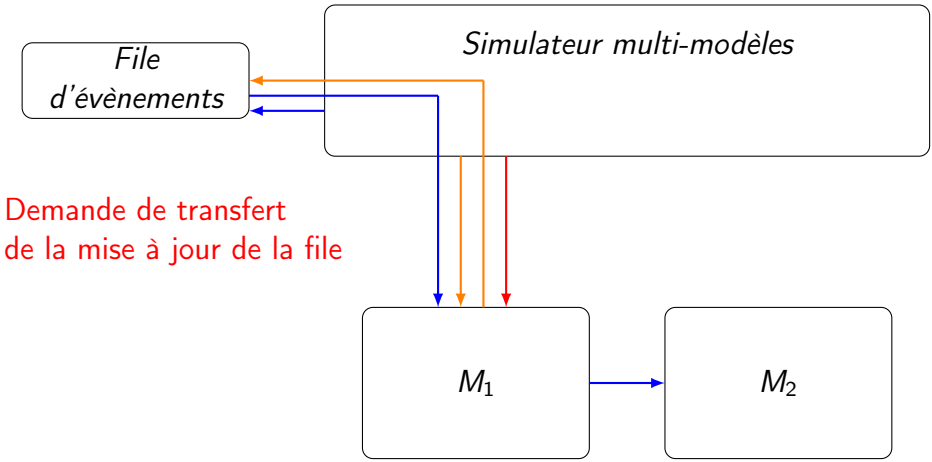
Simulation multi-modèles



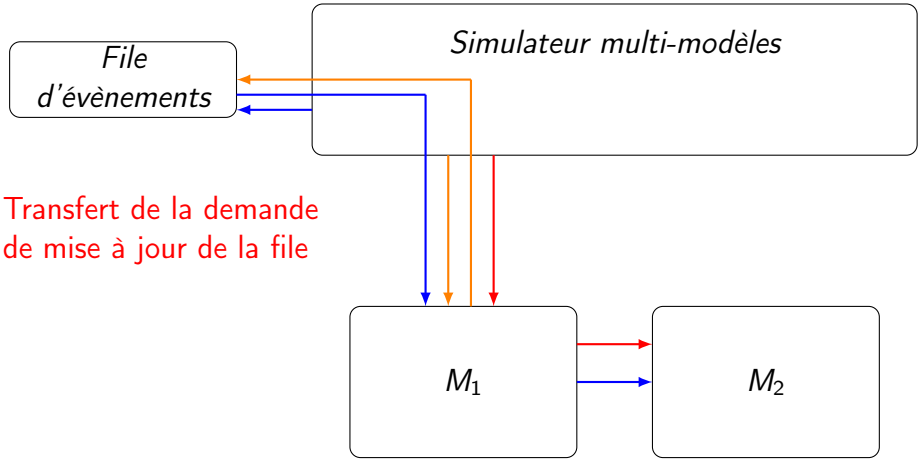
Simulation multi-modèles



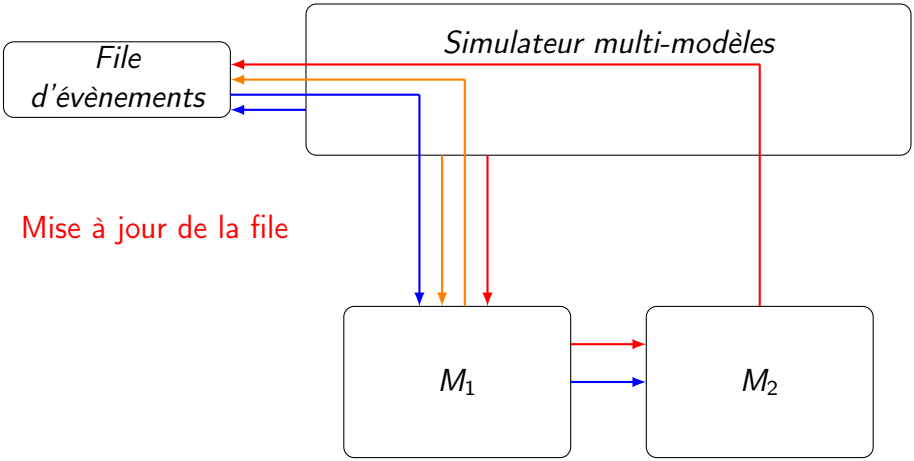
Simulation multi-modèles



Simulation multi-modèles



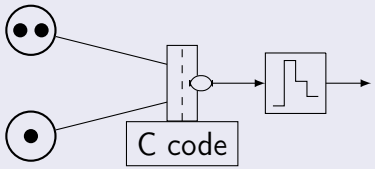
Simulation multi-modèles



Communication entre RdP et Simulink

Transition d'interface pour les entrées Simulink

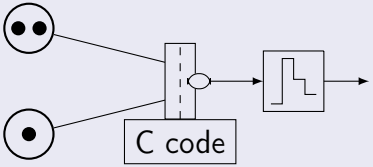
- Connexion des places par arcs de *lecture* ;
- Déclenchement par modification des places ;
- Lecture des nouveaux contenus ;
- Génération des signaux par code C.



Communication entre RdP et Simulink

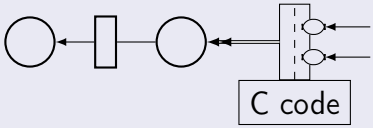
Transition d'interface pour les entrées Simulink

- Connexion des places par arcs de *lecture* ;
- Déclenchement par modification des places ;
- Lecture des nouveaux contenus ;
- Génération des signaux par code C.

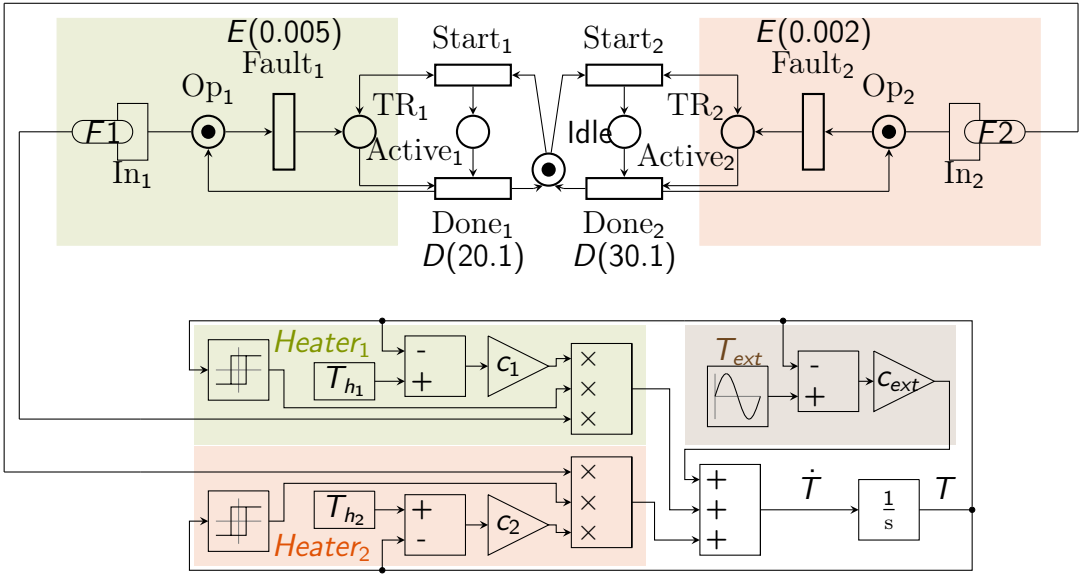


Transition d'interface pour les sorties Simulink

- Connexion des places par arcs de *lecture* ;
- Déclenchement par étape de Simulink ;
- Génération du contenu par code C.



Contrôle de la température d'une pièce (1/4)

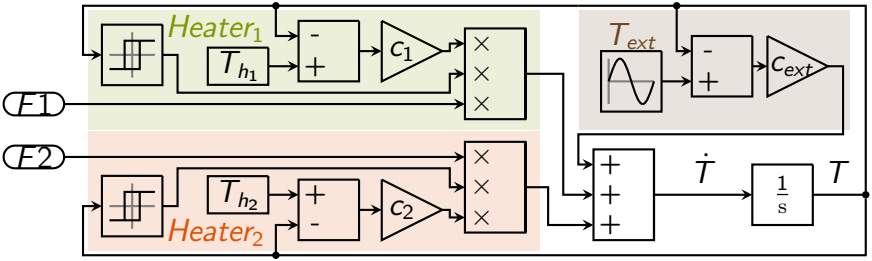


Contrôle de la température d'une pièce (2/4)

Deux radiateurs pour garder la température d'une pièce entre 20°C et 25°C.

Modèle Simulink de la température

- Température extérieure modélisée par une sinusoïde 5-25°C ;
- Blocs à hystéresis désactivant au-dessus de 25°C et réactivant sous 20°C ;
- Température dépendante de la température externe et des activations.

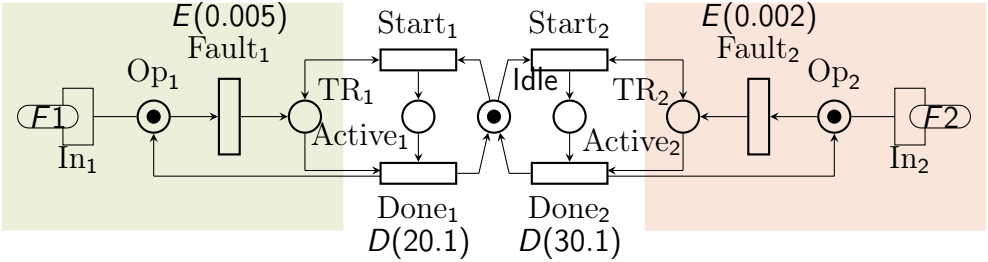


Contrôle de la température d'une pièce (3/4)

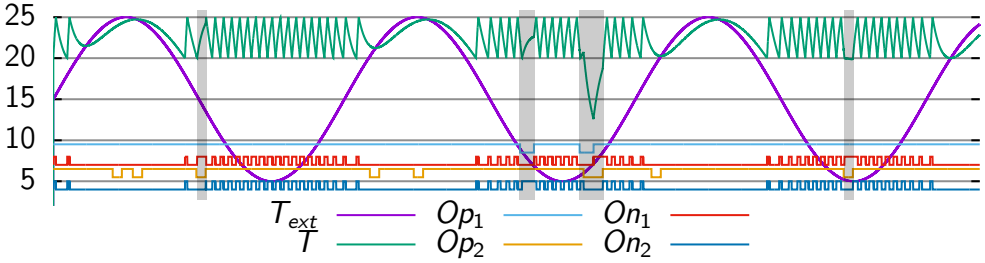
Deux radiateurs pour garder la température d'une pièce entre 20°C et 25°C.

Réseau de Petri stochastique pour la disponibilité des radiateurs

- Taux de panne des radiateurs suivant une loi exponentielle ;
- Un seul réparateur avec des transitions déterministes.



Contrôle de la température d'une pièce (4/4)



Une trajectoire (fournie par Cosmos)

Op_i : absence de panne d'un radiateur
On_i : activation d'un radiateur
T : température de la pièce
T_{ext} : température extérieure

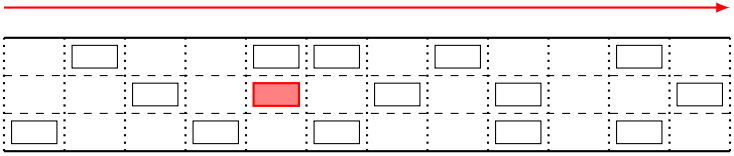
En grisé, panne d'un ou plusieurs radiateurs

Plan

Cas d'étude

Autoroute embouteillée

- Deux comportements de l'environnement ;
- Deux contrôleurs



Cas d'étude

Autoroute embouteillée

- Deux comportements de l'environnement ;
- Deux contrôleurs

	Accélération douce				Accélération agressive			
	Basique		Change-voie		Basique		Change-voie	
I_1	0.838 ± 0.005		0.023 ± 0.005		0.847 ± 0.005		0.022 ± 0.005	
	468.51s	36 120	153.41s	6 620	459.67s	34 520	147.94s	6 020
I_2	267.44 ± 6.68		102.61 ± 2.56		282.23 ± 7.06		106.22 ± 2.66	
	71.48s	5 400	4 147 s	169 640	74s	5 480	3 766 s	154 120

I_1 : taux de collision,
I_2 : moyenne de distance parcourue si collision.

Cas d'étude

Autoroute embouteillée

- Deux comportements de l'environnement ;
- Deux contrôleurs

	Accélération douce				Accélération agressive			
	Basique		Change-voie		Basique		Change-voie	
I_1	0.838 ± 0.005		0.023 ± 0.005		0.847 ± 0.005		0.022 ± 0.005	
	468.51s	36 120	153.41s	6 620	459.67s	34 520	147.94s	6 020
I_2	267.44 ± 6.68		102.61 ± 2.56		282.23 ± 7.06		106.22 ± 2.66	
	71.48s	5 400	4 147 s	169 640	74s	5 480	3 766 s	154 120

I_1 : taux de collision,
I_2 : moyenne de distance parcourue si collision.

Cas d'étude

Autoroute embouteillée

- Deux comportements de l'environnement ;
- Deux contrôleurs

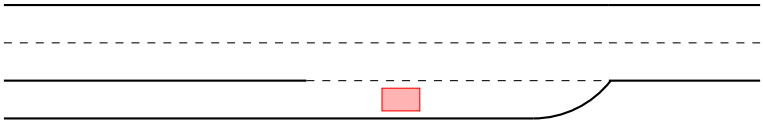
	Accélération douce				Accélération agressive			
	Basique		Change-voie		Basique		Change-voie	
I_1	0.838 ± 0.005		0.023 ± 0.005		0.847 ± 0.005		0.022 ± 0.005	
	468.51s	36 120	153.41s	6 620	459.67s	34 520	147.94s	6 020
I_2	267.44 ± 6.68		102.61 ± 2.56		282.23 ± 7.06		106.22 ± 2.66	
	71.48s	5 400	4 147 s	169 640	74s	5 480	3 766 s	154 120

I_1 : taux de collision,
I_2 : moyenne de distance parcourue si collision.

Cas d'étude

Insertion dans une autoroute

- Trois paramètres pour l'environnement ;
- Deux contrôleurs.



Cas d'étude

Insertion dans une autoroute

- Trois paramètres pour l'environnement ;
- Deux contrôleurs.

	Contrôleur 1			
	10	10 ↗	10 ◎ ↗	20 ◎ ↗
% collision véhicule	[0.016, 0.019]	[0.043, 0.047]	[0.041, 0.046]	[0.126, 0.133]
% collision garde-fou	[0.053, 0.057]	[0.067, 0.073]	[0.070, 0.076]	[0.035, 0.039]
% insertion réussie	[0.925, 0.929]	[0.881, 0.887]	[0.880, 0.887]	[0.829, 0.838]
Force collision	[0.016, 0.019]	[0.100, 0.112]	[0.100, 0.111]	[0.184, 0.197]
Simulations	151 000	81 000	83 000	71 000
Temps	1 672s	1 014s	1 519s	3 601s

Cas d'étude

Insertion dans une autoroute

- Trois paramètres pour l'environnement ;
- Deux contrôleurs.

	Contrôleur 1			
	10	10 ↗	10 ◎ ↗	20 ◎ ↗
% collision véhicule	[0.016, 0.019]	[0.043, 0.047]	[0.041, 0.046]	[0.126, 0.133]
% collision garde-fou	[0.053, 0.057]	[0.067, 0.073]	[0.070, 0.076]	[0.035, 0.039]
% insertion réussie	[0.925, 0.929]	[0.881, 0.887]	[0.880, 0.887]	[0.829, 0.838]
Force collision	[0.016, 0.019]	[0.100, 0.112]	[0.100, 0.111]	[0.184, 0.197]
Simulations	151 000	81 000	83 000	71 000
Temps	1 672s	1 014s	1 519s	3 601s

Cas d'étude

Insertion dans une autoroute

- Trois paramètres pour l'environnement ;
- Deux contrôleurs.

	Contrôleur 1			
	10	10 ↗	10 ◎ ↗	20 ◎ ↗
% collision véhicule	[0.016, 0.019]	[0.043, 0.047]	[0.041, 0.046]	[0.126, 0.133]
% collision garde-fou	[0.053, 0.057]	[0.067, 0.073]	[0.070, 0.076]	[0.035, 0.039]
% insertion réussie	[0.925, 0.929]	[0.881, 0.887]	[0.880, 0.887]	[0.829, 0.838]
Force collision	[0.016, 0.019]	[0.100, 0.112]	[0.100, 0.111]	[0.184, 0.197]
Simulations	151 000	81 000	83 000	71 000
Temps	1 672s	1 014s	1 519s	3 601s

Cas d'étude

Insertion dans une autoroute

- Trois paramètres pour l'environnement ;
- Deux contrôleurs.

	Contrôleur 2			
	10	10 ↗	10 ◎ ↗	20 ◎ ↗
% collision véhicule	$[0.080, 0.089]$	$[0.144, 0.155]$	$[0.182, 0.185]$	$[0.202, 0.220]$
% collision garde-fou				
% insertion réussie	$[0.793, 0.805]$	$[0.770, 0.783]$	$[0.815, 0.817]$	$[0.780, 0.798]$
Force collision	$[0.259, 0.286]$	$[0.466, 0.504]$	$[0.601, 0.607]$	$[0.486, 0.537]$
Insertion trop lente	$[0.112, 0.121]$	$[0.069, 0.078]$	$[8.1 \cdot 10^{-4}, 9.3 \cdot 10^{-4}]$	-
Simulations	37 000	34 000	2 000 000*	16 000
Temps	515s	486s	39 041s	828s

N^* Nombre maximum fixé de simulations atteint Nul par construction

Résultats obtenus

Sémantique pour Simulink

- Sémantiques exacte et opérationnelle d'un modèle Simulink
- Implémentation dans Cosmos

Modélisation multi-formalismes

- Spécification
- Intégration d'une instance RdPSC-Simulink dans Cosmos

Modélisation et évaluation de deux cas d'étude

Perspectives

Établissement d'une garantie de précision de la sémantique opérationnelle

Nouvelles extensions pour Cosmos :

- Définition d'une communication multi-modèles générique
- Implémentation de nouveaux blocs Simulink
- Ajout de formalismes bio-informatiques

Contribution à la suite du projet de l'IRT SystemX

Perspectives

Établissement d'une garantie de précision de la sémantique opérationnelle

Nouvelles extensions pour Cosmos :

- Définition d'une communication multi-modèles générique
- Implémentation de nouveaux blocs Simulink
- Ajout de formalismes bio-informatiques

Contribution à la suite du projet de l'IRT SystemX

Merci de votre attention !