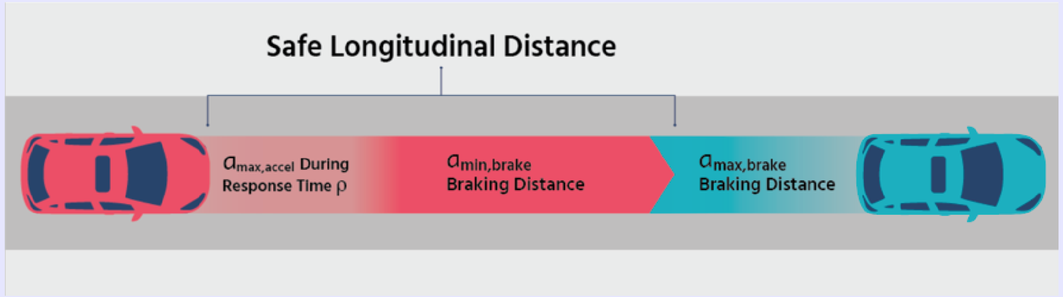
Cyber$_\Phi$



Cyber$_\Phi$ - Un cadre pour modéliser les systèmes cyber-physiques

- interaction simultanée des acteurs et des environnements
- communication entre acteurs possible
- temps continu ($\mathbb{R}_0$)
- observables multidimensionnel de la physique newtonienne
- vue discrétisée (échantillonnée) des observables continus des systèmes
- raffinement entre modèle abstrait et code exécutable possible
- ... permettant l'analyse formelle par test et preuve

Isabelle/HOL-CSP, un plongement conservatif de CSP en HOL

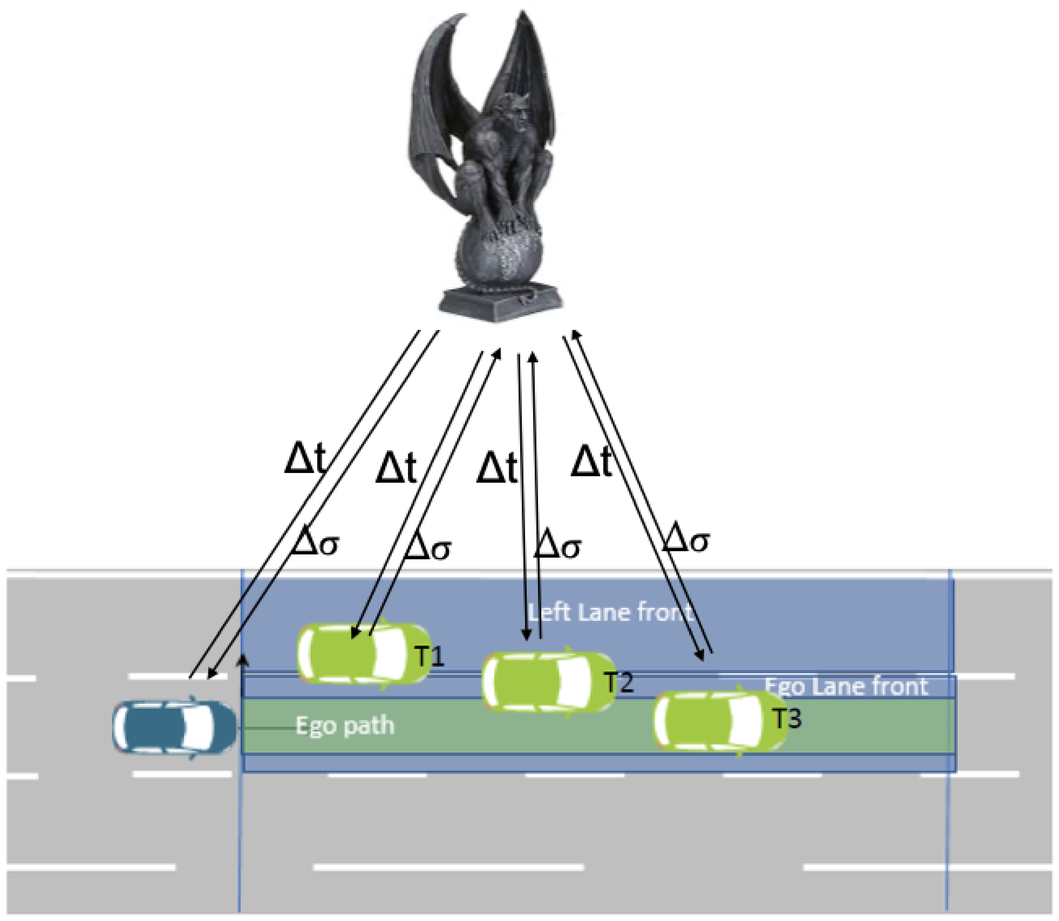
Communicatig Sequential Processes(CSP) est une algèbre de processus pour la communication et la concurrence, basé sur les travaux de Hoare et Roscoe dans les années 80 et 90 (et des extensions depuis).

$$a \longrightarrow P,\ P \sqcap P',\ P \Box P',\ Skip,\ Stop,\ P \,|||\, P',\ P \,[\![S]\!]\, P',\ \mu X.\ P\ X$$

$$\bigsqcap x{\in}A \longrightarrow P\ x,\ \Box\, x{\in}A \longrightarrow P\ x,\ \ |||x{\in}B.\ P\ x,\ [\![S]\!]x{\in}B.\ P\ x$$

HOL-CSP est un plongement conservatif de CSP en Isabelle/HOL permettant des types d'ordre supérieur et des alphabets infinis.

Le Noyau de HOL-Cyber$_\Phi$ en un coup d'oeil



$$demon \equiv \bigsqcap \Delta t{\in}\mathbf{R}_+ \rightarrow \Box \sigma_g{\in}\Sigma \rightarrow demon$$

$$actor_{id}\ ds\ \sigma_g \equiv \Box\ \Delta t{\in}\mathbf{R}_+ \rightarrow \sqcap\ \sigma'_g \in \{\Sigma \mid \Sigma[id] \in moves\} \rightarrow actor_{id}\ ds\ \sigma'_g$$

$$moves \equiv (kinematics\ (\sigma_g[id])\ \Delta t)\ `\ (ds\ id\ \sigma_g)$$

$$S\ \sigma_0 \equiv demon\ [\![\mathbf{R} \uplus \Sigma]\!]\ (|||\ id \in IDS.\ actor_{id}\ ds\ \sigma_0)$$

$$S_P{}'\ \sigma_0 \equiv demon\ [\![\mathbf{R} \uplus \Sigma]\!]\ ((\![\ I\ ]\!]\ id \in IDS.\ actor_{id}\ ds\ \sigma_0) \setminus \{I\})$$

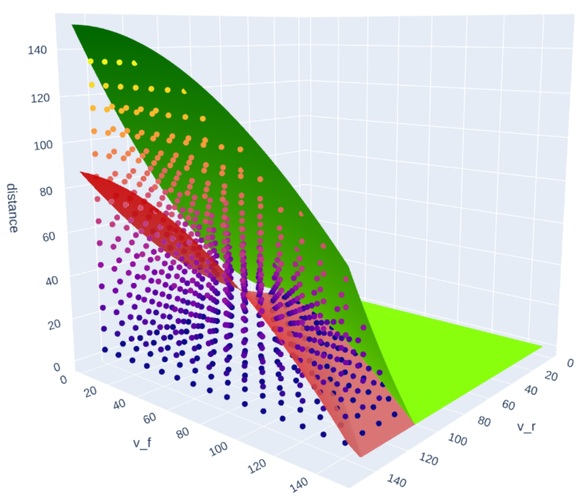
Isabelle/HOL pour les données, CSP pour l'Interaction

- riche bibliothèque avec arithmétique, listes, ensembles, nombre réels ...
- espaces vectoriels et analyse fonctionnelle (HOL-Analysis)
- bitvectors et environnements de vérification de langages bas-niveau (C)
- équations différentielles pour définir *kinematics*

$$SOME\ (x',v',a').\ \ v' = deriv\ x\ \wedge\ a' = deriv\ v \wedge (x',v',a') = M\ (x',\ v',\ a') \wedge x'(0) = x(0) \wedge v'(0) = v(0) \wedge a'(0) = a_0$$

$$\begin{aligned} x' &= x + \Delta t * v + (\Delta t^2/2) * a_0, \\ v' &= v + \Delta t * a_0, \\ a' &= a_0 \end{aligned}$$

La matrice M permet de modéliser des forces extérieures, la topologie des routes, la résistance de l'air ... HOL-Analysis offre aussi un cadre pour des approximations de trajectoires comme les zonotopes...

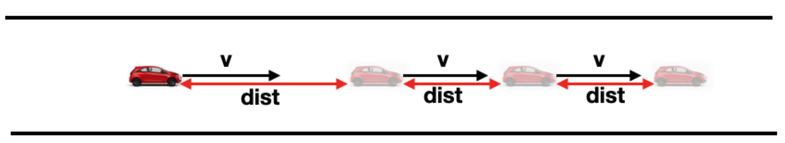


Génération des tests fonctionnels :

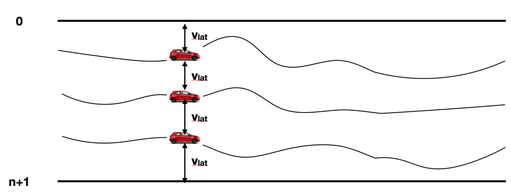
- à partir des "nappes"
- à partir des points de basculement

Étude de Cas : "driving strategies ds" des Véhicules Autonomes

Dans le cadre de modélisation Cyber$_\Phi$, les acteurs ont un état physique (position, vitesse, accélération, accélérations potentielles). La *stratégie de conduite* est une fonction de la scène globale, qui calcule un ensemble d'accélérations possibles. L'acteur en choisit une de manière non-déterministe et l'applique pendant l'intervalle de temps Δt.



Pour la stratégie RSS de Shalev-Shwartz, Shammah, et Shashua, nous avons fourni la preuve formelle qu'il n'y aura pas de collision dans un modèle postulant de fortes hypothèses : "Capteurs parfaits", "Pas de confusion entre types d'acteurs", "Conducteurs compétents", 'Topologie triviale".



Nous avons également prouvé la srûreté pour plusieurs généralisations de RSS, notamment la possibilité de déplacements latéraux pour N voitures.

Notre orientation de recherche consiste à affaiblir ces hypothèses.

Collaborations

- Université de York
- IRT SystemX

Bibliographie

- Paolo Crisafulli, Safouan Taha, and Burkhart Wolff, *Modeling and analysing cyber-physical systems in HOL-CSP*, Robotics Auton. Syst. **170** (2023), 104549.