Vérification de la sûreté des systèmes basés réseaux de neurones s'appuyant sur les méthodes formelles

Safety verification of neural network based systems using formal methods

Soutenance de thèse – Clavière Arthur
17 juillet 2023 à 10h00
Salle des thèses, ISAE-SUPAERO, 10 Avenue Edouard Belin, Toulouse

Devant le jury composé de :

M. Eric GOUBAULT – Rapporteur : Professeur Ecole Polytechnique
Mme Susanne GRAF – Rapportrice : Directrice de recherche CNRS
M. Benedikt BOLLIG – Examinateur : Directeur de recherche CNRS
Mme Elisa FROMONT – Examinatrice : Professeure Université de Rennes
M. Joao MARQUES-SILVA – Examinateur : Directeur de recherche CNRS
M. Eric Asselin – Co-encadrant de thèse : Ingénieur Collins Aerospace
Mme Claire PAGETTI – Directrice de thèse : Directrice de recherche ONERA

Résumé

La thèse a porté sur l'étude et la vérification de la sûreté de fonctionnement de systèmes contrôlés par réseaux de neurones. Un tel système combine un système physique et un contrôleur basé réseaux de neurones, dont l'intérêt peut être : (1) d'approximer un autre contrôleur, déjà existant, mais en demandant moins de ressources de calcul (sachant qu'un contrôleur dispose souvent de ressources limitées) ou (2) de reproduire le comportement d'un humain (ce qui peut s'avérer intéressant pour les systèmes autonomes). Dans le cas où le système contrôlé par réseaux de neurones est critique, il est important de vérifier sa sûreté de fonctionnement. A cette fin, nous avons d'abord considéré le cas (1) pour lequel nous avons développé une méthode et un outil (appelé SAM) afin de comparer les deux contrôleurs et montrer que le contrôleur basé réseaux de neurones est une approximation correcte du contrôleur original. Ensuite, nous avons considéré le cas général (1) + (2) pour lequel notre approche a été de vérifier le système contrôlé par réseaux de neurones en entier. Cette seconde contribution comporte deux aspects : (i) le développement d'un modèle basé automate hybride du système étudié et (ii) un outil, appelé SAMBA, qui permet l'analyse de cet automate hybride.

The thesis focused on the study of neural network controlled systems and the verification of their safety. Such systems combine a physical system with a neural network controller which may: (1) approximate the behavior of an existing controller while demanding less computational resources (which is of particular interest for a controller that generally has limited resources) or (2) reproduce a human-like behavior (which can be particularly interesting for autonomous systems). If the neural network controlled system is safety-critical, then it is of particular interest to demonstrate that it does not encounter any unsafe state over time. For this purpose, we first considered the case (1) for which we developed a method and a tool (named SAM) to compare the two controllers and show that the neural network controller correctly approximates the target controller. Then we considered the general case (1) + (2) for which our approach was to verify the whole neural network controlled system, not only the controller. More precisely, we developed: (i) a hybrid-automaton model of the neural network controlled system assumed in the thesis and (ii) a tool, called SAMBA, that allows the analysis of this hybrid automaton.

Mots clés

Réseaux de neurones, Sûreté, Méthodes formelles

Neural networks, Safety, Formal methods

Vous êtes invité à rejoindre la web-conférence ZOOM via le lien ci-dessous :

https://zoom.us/j/95283774436

ONERA

THE FRENCH AEROSPACE LAB