Cybersécurité pour les systèmes embarqués critiques à base d'Intelligence Artificielle

Céline Bellanger*[1]

[1]enac – Ecole Nationale de l'Aviation Civile - ENAC – France

Résumé

L'intelligence artificielle est de plus en plus utilisée dans les systèmes embarqués critiques, et particulièrement dans l'aéronautique. Elle peut remplacer des fonctions existantes comme la stabilisation ou le guidage ; ou ouvrir de nouvelles possibilités comme la réalisation de toutes les phases de vol de façon autonome notamment grâce à la reconnaissance d'images. Cependant, elle peut être la cible de nouveaux types de cyberattaques, spécifiques à l'intelligence artificielle. Dans ce document, nous présentons nos travaux en cours et à venir pour améliorer la sûreté des réseaux de neurones utilisés dans les systèmes embarqués. Nous nous appuierons sur des méthodes formelles pour étudier les propriétés temporelles des signaux issus des réseaux de neurones. L'approche visera à 1. définir les méthodes et outils pour évaluer les propriétés exprimées en Signal Temporal Logic (STL), 2. caractériser les propriétés d'intérêts dans cette logique STL et 3. étudier la validité de contrôleurs à base de réseaux de neurones vis-à-vis de ces propriétés.

*Intervenant