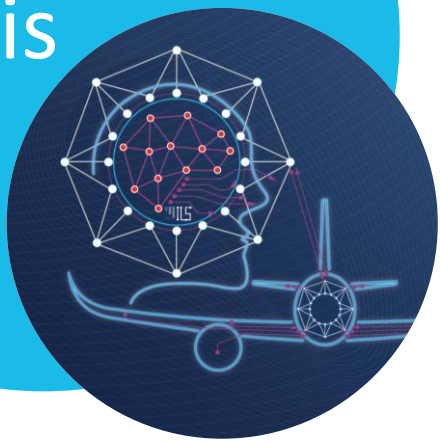
University of Stuttgart
Aerospace Engineering and Geodesy

ADVANCED METHODS FOR CERTIFICATION

Master's Thesis



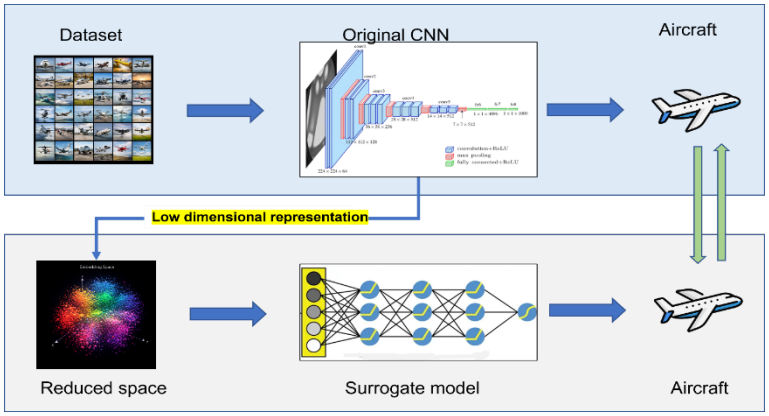
Deep learning testing and verification for avionics systems

Motivation and Background

Deep neural networks, particularly Convolutional Neural Networks (CNNs), have demonstrated remarkable performance across a wide range of computer vision applications. These capabilities have enabled their adoption in many safety-critical domains. Despite their success, the increasing architectural complexity of CNNs poses significant challenges for formal verification and systematic testing for unintended behavior detection.

A common observation is that transforming high-dimensional inputs into compact and reduced representations (embeddings) preserves most of the discriminative information. This raises a fundamental research question: ***can the behavior of a CNN be reproduced by a simpler neural network trained only on these embeddings?***

If such a behavior-preserving surrogate model exists, it could significantly reduce the computational cost of verification and testing by scaling up verification methods while retaining high fidelity to the original CNN.



Goal

The primary goal of this thesis is to investigate whether a surrogate model in terms of Feed-Forward Neural Network (FFNN) trained on a small space can exhibit behavior equivalent or near-equivalent to the original CNN. The thesis aims to assess under what conditions a surrogate model can reliably replace a CNN for tasks such as classification, robustness testing, and formal verification.

Tasks

This thesis can be structured into the following steps:

1. Literature Review and State of the Art of formal verification and testing methods for neural networks.
2. Train a baseline CNN on a well-known dataset and train a surrogate model on a reduced input space.
3. Behavioral Similarity Analysis: Compare CNN and FFNN predictions and agreements on well-defined test data.
4. Identify regions where surrogate behavior diverges from the CNN.
5. Investigate whether the formal guarantees established for a surrogate model FFNN can be transferred to the original CNN.
6. Investigate how the surrogate model can be used to scale up existing verification and testing methods.

Expected Outcomes

- A trained CNN and corresponding FFNN surrogate
- Evidence of behavior preservation for the surrogate FFNN
- A systematic evaluation framework for comparing neural network behaviors
- Insights into how surrogate models can simplify neural network verification and testing

Interested ?

Send your application to:

Dr. Yassine AKHIAT
Yassine.akhiat@ils.uni-stuttgart.de

Or

Prof. Zamira Daw
Zamira.daw@ils.uni-stuttgart.de