Synchronous Neural Networks for Cyber-Physical Systems

Abstract:

*Cyber-physical systems (CPS), such as autonomous vehicles or smart power grids, use interactive machine learning modules for decision making. Current design approaches use multiple machine learning modules, often using Artificial Neural Networks (ANNs), to achieve the desired functionality. Current approaches to verification and validation of these ANNs are generally either very difficult, time consuming and/or not fully reliable. A key feature missing is related to the use of NNs in real-time systems, which demand the capability of worst-case analysis.*

*In this thesis we introduce Synchronous Neural Networks (SNNs) as a new approach to the safe use of ANNs in CPS. SNNs provide synchronous semantics to ANNs. This enables real-time operation and facilitates static timing analysis of individual ANNs. We define these SNNs using formal methods, and when embedded on time predictable platforms, static analysis of these SNNs is enabled.*

*We propose Meta Neural Networks (MNNs) as a framework for the systematic composition of SNNs. This enables compositional system design using multiple SNNs and other synchronous functional components, while maintaining the synchronous semantics of the system. These synchronous MNNs allow for the creation of causal, deterministic, predictable controllers for CPS.*

*The combination of MNNs and Run-time Enforcers (RE), which enforce a set of desired policies by transforming inputs and outputs suitably, is proposed as solution to deal with misclassifications made by MNNs. These enforced MNNs are shown to be able to effectively deal with misclassifications and avoid safety violations due to unsafe MNN inputs and/or outputs.*

*Finally, we propose a tool that extends Keras to give it a MNN description capability. We then automatically generate C code, which are shown to perform even better than our earlier MNN implementations using Esterel. Initially, MNNs for this thesis were implemented in Esterel for the design of synchronous systems, while subsequent MNNs were implemented using this tool. We demonstrate the efficacy of our approach by developing CPS benchmarks with MNN controllers, while ensuring the safety of the system and environment.*