Title:

Artificial Neural Networks for (Safe) Cyber-Physical Systems

Notes:

* CPS must be “safe”, so having “safe” in title may not be necessary.
* ANNs must be mentioned.
* Synchronous probably does not have to be mentioned.
* CPS should be mentioned; they are a core component of this field of research.

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 new approach to verifiable ANNs is proposed using the synchronous paradigm to introduce Synchronous Artificial Neural Networks (SANNs). Logical time is allocated to the operations of the SANNs, providing sound compositional primitives. This enables the composition of interacting ANNs to ensure causality and determinism.*

*In this thesis we introduce SANNs as a new approach to the safe use of ANNs in CPS. We mathematically verify these SANNs using formal methods, and when embedded on time predictable platforms, static analysis of these SANNs is enabled. Additionally, we propose the combination of SANNs and other synchronous functional components, notably Runtime Enforcement (RE), by formally defining Meta Neural Networks (MNNs). These synchronous MNNs allow for the creation of causal, deterministic, predictable controllers and/or plants for CPS.*

*ANNs for this thesis were implemented in Esterel for the design of synchronous, predictable systems. We demonstrate the efficacy of our approach by developing CPS with MNN controllers; ranging from MNNs with 5 neurons to MNNs with 10,000+ neurons. This thesis also introduces a compiler made that converts ANNs created and trained using Keras, Python to the predictable MNNs previously introduced.*

Notes:

* Wanted to mention CPS.
* Introduced the overall concept of SANNs first, and what they enable.
* Then mentioned the combination of synchronous components, i.e. MNNs.
* Mentioned Esterel and MNN2C.
* Mentioned what the benchmarks will be.