Synchronous Artificial Neural Networks with Runtime Enforcement for Safety Critical Systems

Partha S. Roop, Hammond A. Pearce, Keyan Monadjem

September ??, 2018

Overview

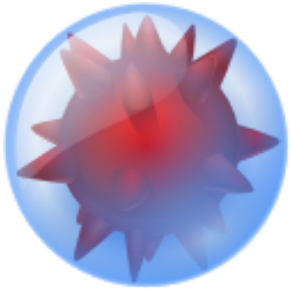
What is Artificial Intelligence? [1]

The aim for machines to intelligently decide the best course of action to meet their respective goals.

Machine-based...

- Acquisition and Manipulation of Knowledge
- Generation and Achievement of Goals

Are they useful?



Security

Finance

Analytics

Banking

Automotive

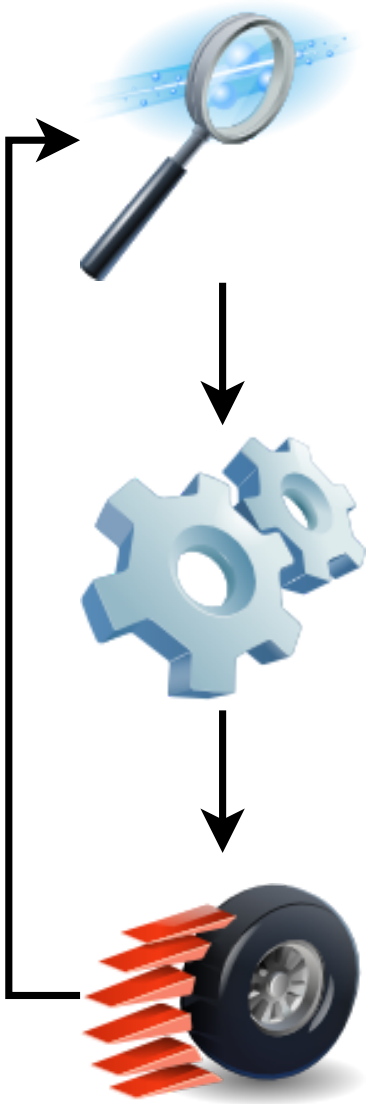
Image/Pattern Recognition

There are many kinds of AI

(Some) Types

- Symbolic AI
- Statistical Learning
- Sub-symbolic
  - Evolutionary Computation
  - Probabilistic Modelling
  - **Neural Networks**

AI is *reactive*...

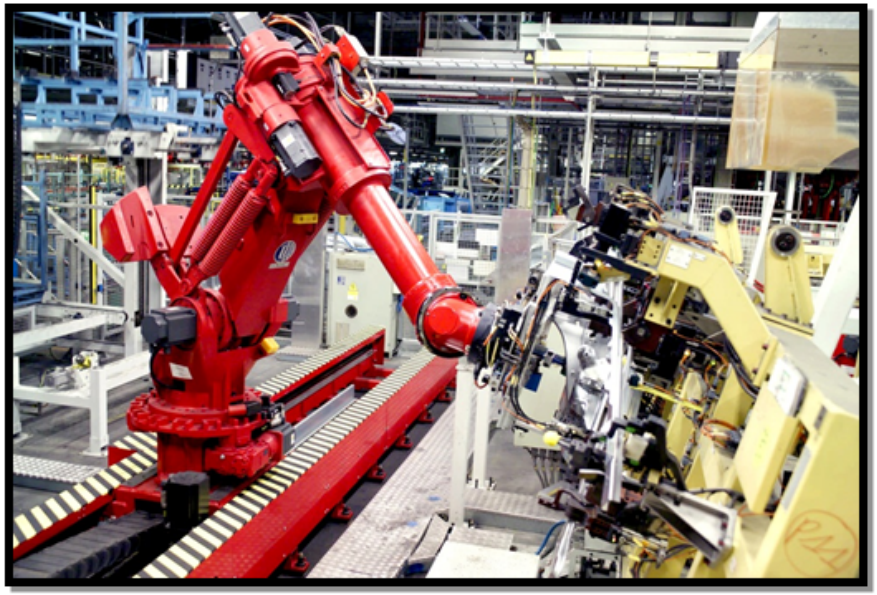


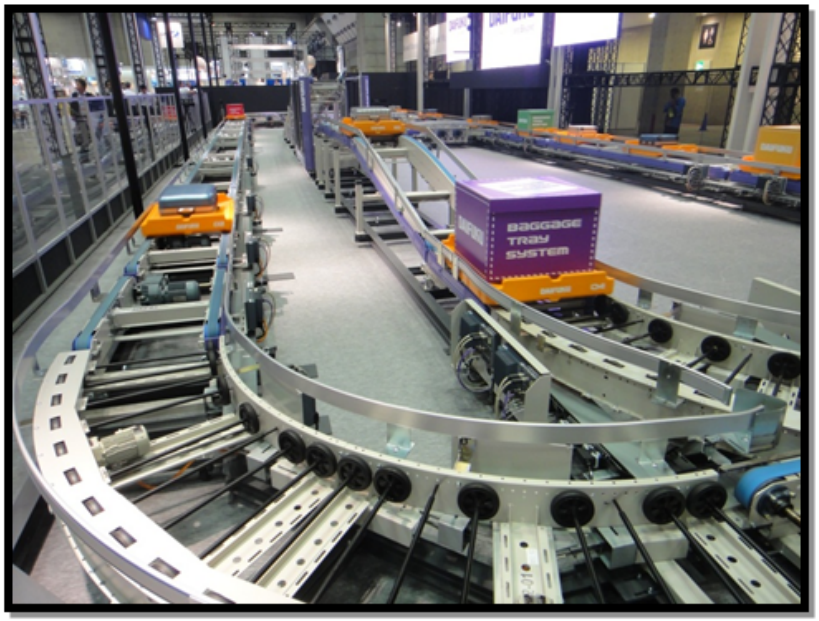
1. Perceive Environment

2. Analyse Findings

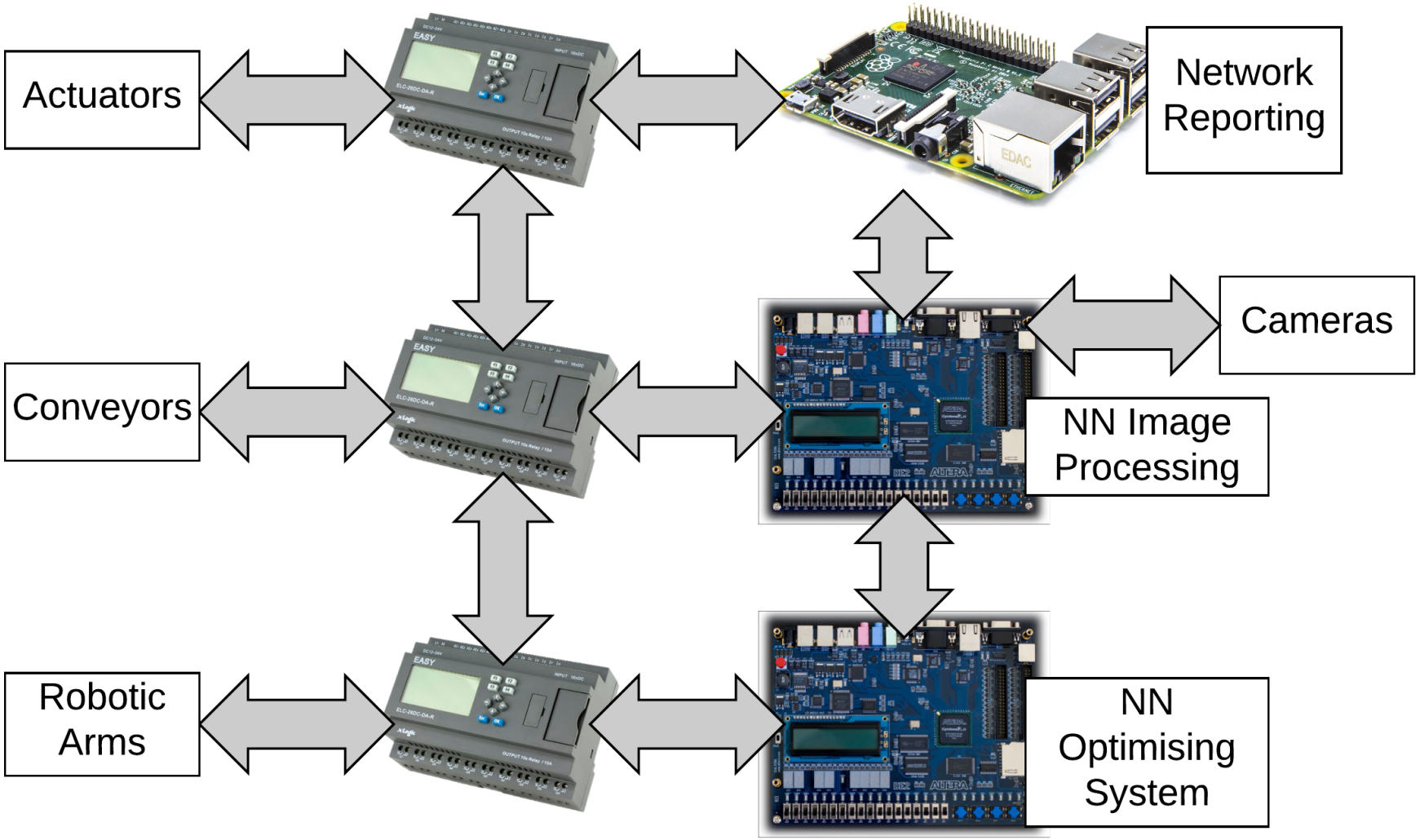
3. Act in interest of goal

Reactive Safety-Critical Systems





AI Controllers?



The Problem: Post-verified ANNs for safety critical systems

Safety critical ANNs

- Software / Systems based on ML can be very complex.
- Not suitable for safety critical systems without validation/verification.
- Existing techniques to verify/validate ANNs for safety critical environments (proactive): not always ideal.
- Few solutions for *reactive* safety critical ANNs.
- When is an ANN *safe* to use?
- Functional Analysis?
- **Runtime Enforcement** (reactive)?

Our proposal

A formal approach for **reactive** safety-critical AI systems

- Synchronous semantics
  - Similar Capture/Process/Emit lifecycle
- Compositionality
- **Synchronous Runtime Enforcement**

Overview

A brief overview of ML

- Make programs that learn from data without being explicitly programmed to do so
- - Decision trees
  - **Neural Networks - deep learning**
  - Reinforcement learning

A brief overview of NN

- Type of machine learning
- Originally designed to model the brain
- One neural network is a group of interconnected nodes, called artificial neurons, which pass signals among themselves
- Many different network structures
- Many different ways to allow neural networks to learn

Why are Current Implementations bad?

Complicating Static Analysis

- Not verified for safety-critical systems.
- Difficult to quantify an ANN.
- How to make ANNs safe?

Overview

Current AI in safety-critical applications

- Process to determine ANN safety during creation - validation/verification.
  - Unit testing
  - Rule extraction
  - Strict guidelines
- Safety Critical Artificial Neural Networks (SCANNs)
  - Fuzzy Self-Organising Maps (FSOMs)
  - Rule extraction + insertion
  - Safety cases

Overview

Introduction to Synchronous Semantics

- No chance of deadlocks occurring during runtime.
- Loops are bounded.
- Causality is maintained.
- Resource use is monitored.
- Consistent function output.
- **Runtime enforcement**
- Easier to analyse WCET.

Runtime Enforcement

- Input-to-output functions
- Input/output checking
- Training guiding
- Inter-layer enforcement

Running example: ?

Overview

References

[1] A. Sloman, "What is artificial intelligence?," *The University of Birmingham, Computer Science Department (junio, 9, 1998). http://www. cs. bham. ac. uk/~ axs/misc/oxford/whatsai. openday. pdf*, 1998.

Source code access