Border Patrol Winter Quarterly Meeting

Jan de Muijnck-Hughes

10 July 2018

1 Project Overview

Border Patrol is an EPSRC funded collaboration between the universities of Glasgow, Imperial College, and Heriot-Watt to investigate the application of state-of-the-art advances in programming language design and theory to the construction, deployment, and testing of System-On-A-Chip architectures. Namely, we are using these advances to provide static compile-time guarantees about IP Cores and their connections, and runtime guarantees that third party IP Cores behave as described in their specification.

The three site's investigatory areas are

- **Glasgow**: Developing SoC Architecture Description Language.
- **Imperial**: Extending theory of Session Types for Hardware.
- **Heriot Watt**: Verifying Protocol Implementations.

Past activities were targeted towards initial readings, together with site visits to Xilinx Dublin & Penicuik, and development of experimental prototypes.

2 Activity Reporting

2.1 University of Glasgow

Jan at the University of Glasgow, has been developing a prototype modelling framework to allow for *Type-Driven Design of SoC*. Inspired by existing research and the IP-XACT standard, his modelling language presents a system of systems that tackle different aspects of SoC Design.

1. **Abstract Interface Description language (AIDL)**: Presents a way to specify parameterised abstract descriptions that describe the structure (signals) that interfaces on IP Cores communicate using. Work is being carried out to develop the language further, and model the structure of the AXI protocol, and other extant protocols such as LocalLink and APB.

2. **Component Specification language (CSL)**: Presents a language to specify interfaces on an IP Core. This language utilises (at the type-level) the descriptions from an AIDL instance to guarantee that the specified interface satisfies the specification. Further, this language allows one to mark IP Cores as trusted or not trusted.

3. **SoC Orchestration language (SoL)**: Presents an orchestration language to specify components in a SoC, and connect said components together. The orchestration languages uses information for the IP Core's interface specifications to ensure that valid connections are made between interfaces. For example, that only matching interfaces can be connected, or that a shared connection (with multiple initiator **and** targets) doesn't violate the supported number of connections.

Current work is on developing the framework to further enrich the model descriptions, and to facilitate generation of stubs in some HDL, IP-XACT descriptions, and other documentation formats.

2.2   Imperial College London

Nick, at Imperial College London, has been investigation how to extend his groups existing work into **Multiparty Session Types** to describe the behaviour of IP Cores with respect to an interface protocol.

Nick has examined the existing corpus of checks as performed by ARMs and Xilink protocol checkers to determine what Session Types can and cannot do. **Session Types** lacks an ability to model time, which **Timed Session Types** can help with. However, there is work to be done to see how **Timed Session Types** models interface protocols.

2.3   Heriot-Watt University

Rob, at Heriot-Watt University, has been investigating how to generate protocol monitor's from Imperial's behavioural descriptions.

Specifically, Rob has investigated extant work towards synthesisable checkers that use temporal assertions to ensure signals emanating from an IP Core are in the correct state. This has led him to research by McGill University that is characterised by the MBAC tool.

MBAC is a, licensed, hardware verification tool that when given a set of temporal assertions will generate **space efficient** assertion-checking hardware that is usable at simulation and run time. Rob posits that we can go from Session Type behavioural descriptions to temporal assertions (defined using a known standard) to monitoring code thatcan be used to assert the behaviour of third-party IP Cores.

3 EDF Energy

A representative from EDF Energy was in attendance. The project background and aims were explained, and it was noted there was potential impact of the research outcomes to the assurance lifecycle of safety critical systems. Open invitation for researchers to visit EDF in Cotswolds to investigate this impact more.

4 Action Points

- Jan to coordinate site visit to EDF in Cotswolds.
- Jan to coordinate next meeting.