Reliable SW/HW Co-Design for Wireless Communication System
Integrating the Spin model checker and Celoxica's DK Suite

Stefanos Skoulaxinos
Heriot-Watt University, Riccarton Campus, Edinburgh, UK

Introduction

A recent study has shown that embedded code increases annually by 28% while embedded engineers by only 8%. According to the same survey to counterbalance this, the only available option is the deployment of more abstract and productive development processes. We seem to be commencing a new era in the embedded logic design, a novel breed of tools, High Level Language Compilers (HLLCs) are entering the market and propose to perform a truly decisive innovation, bridging the gap between software and hardware. Effortless code turn-arounds, faster time to market, increased code readability, System Level Integration are some of the appealing benefits of such tools. What is even promising though is the potential contribution in the design lifecycle. Breathing life into SW/HW co-design can provide the gateway for the introduction of strategic reliability enhancement methods currently utilized in Computer Science such as formal specification, exhaustive verification and structured design principles. The aim of this paper and the associated research project launched in Heriot-Watt University, is to present how High Level Compilers for FPGAs can be combined with proven software methodologies and practices promoting more dependable embedded applications. The product of this work outlined the framework for the development of the Long Range Identification Tag targeting the FPGA Technology and also presented in the document.

Development of Wireless Communication System - LRID Tag

Reliability is particularly significant if the system is to be embedded at a remote location, as late modifications may not be feasible. The LRID Tag, a wireless application developed in Heriot-Watt University resides in this group. It is expected to operate effectively for a number of years upon its remote implantation without any form of maintenance.

Aiming to accommodate such level of robustness, we have attempted to integrate a number of Technologies, Methods and Tools including the widely adopted Spin Software Model Checker, and Celoxica's DK Synthesis Tool. A safety-orientated design lifecycle unfolding around the spin model checker, high quality specifications and formal verification promote early error detection and correction. Through automated code translation and hardware implementation in the DK Compiler, both software and hardware failure scenarios are addressed and resolved. Furthermore, to enhance autonomous capacity and survivability of the device, run-time monitoring architectures including watchdog timers and forward error correction codes (FEC) are deployed to detect a wide range of mal-operations. Multi layered exception handling routines developed in the compiler can effectively locate and recover from a wide range of SW and HW faults. The embedded device is finally tested under a lab emulated EMI scheme aiming to quantify system survivability.
The core of the application is developed in Promela. Simulation under Spin is performed in this phase. The Promela model is translated with the aid of Bison and Flex to a language compatible with the Synthesis tools for FPGAs (HandelC). The HDL source produced in the preceding phase is imported in Xilinx ISE. Generation of the configuration bit stream follows. In this phase, the design can be examined exhaustively through formal verification. It is checked for deadlock conditions, responsiveness, assertions and mutual exclusion violations. The abstract operation implemented by the system is briefly outlined. A number of languages can be deployed in this phase, UML, CORE, YSM and JSD.

The HDL source produced in the preceding phase is imported in Xilinx ISE. Generation of the configuration bit stream follows. Configuration file is downloaded to the FPGA device and system testing is carried out.

### Figure 1 Testing Procedure
- Base Station Xilinx Spartan IIE
  - Utilized to control data communication with user PC, ID reception from antenna and tag location computations, all processes executed in parallel
  - Capable of correlating multiple IDs in a truly concurrent manner
  - 100 MHz on-board oscillator
  - Can deploy 32 MB of on-board SDRAM
  - The Spartan III board supports 3.3V and 2.5V I/O standards

### Figure 2 Development Lifecycle
- Requirements Analysis
  - System Specifications
- System Design in Promela
  - Process Meta Language
- Formal Verification in the Spin Model Checker
- Code translation under Bison(Vaccc) and Flex
- Synthesis to Hardware and System Integration
- Testing on Hardware

### Figure 3 Reliability Estimation I (CASRE)
- MTBF = 18 seconds
- MTBF Fault Tolerance Disabled

### Figure 4 Reliability Estimation II (CASRE)
- MTBF = 59 seconds
- MTBF Fault Tolerance Enabled

### Figure 5 Base Station Execution Overhead

### Figure 6 Remote Station Execution