Special Session on Early Life Failures

Deshmukh, Jyotirmoy; Kunz, Wolfgang; Wunderlich, Hans-Joachim; Hellebrand, Sybille

Proceedings of the 35th VLSI Test Symposium (VTS'17) Caesars Palace, Las Vegas, Nevada, USA, 9-12 April 2017

doi: http://dx.doi.org/10.1109/VTS.2017.7928933

Abstract: In recent years early life failures have caused several product recalls in semiconductor and automotive industries associated with a loss of billions of dollars. They can be traced back to various root-causes. In embedded or cyber-physical systems, the interaction with the environment and the behavior of the hardware/software interface are hard to predict, which may lead to unforeseen failures. In addition to that, defects that have escaped manufacturing test or "weak" devices that cannot stand operational stress may for example cause unexpected hardware problems in the early life of a system. The special session focuses on the first aspect. The first contribution discusses how the interaction with the environment in cyberphysical systems can be appropriately modeled and tested. The second presentation then deals with a cross-layer approach identifying problems at the hardware/software interface which cannot be compensated by the application and must therefore be targeted by specific tests.

Special Session on Early Life Failures

Jyotirmoy Deshmukh, Toyota Technical Center, USA
Wolfgang Kunz, TU Kaiserlautern, Germany
Hans-Joachim Wunderlich, University of Stuttgart, Germany (Moderator)
Sybille Hellebrand, University of Paderborn, Germany (Organizer)

I. Introduction

In recent years early life failures have caused several product recalls in semiconductor and automotive industries associated with a loss of billions of dollars. They can be traced back to various root-causes. In embedded or cyber-physical systems, the interaction with the environment and the behavior of the hardware/software interface are hard to predict, which may lead to unforeseen failures. In addition to that, defects that have escaped manufacturing test or "weak" devices that cannot stand operational stress may for example cause unexpected hardware problems in the early life of a system. The special session focuses on the first aspect. The first contribution discusses how the interaction with the environment in cyber-physical systems can be appropriately modeled and tested. The second presentation then deals with a cross-layer approach identifying problems at the hardware/software interface which cannot be compensated by the application and must therefore be targeted by specific tests.

II. Testing and Fault Localization for Embedded Controllers (J. Deshmukh)

The model-based development paradigm is increasingly being used for the design of embedded controllers in the cyber-physical systems (CPS) domain. The main motivation is to identify and eliminate possible issues in the system design at an early development stage. This is made possible by having reasonably high-fidelity plant models that capture the physical aspects of the CPS system, and controller models designed using a visual, block-diagram based programming language such as Simulink (from the Mathworks). A challenge is that control designers often do not have machine-checkable requirements on the overall behavior of the closed-loop model (consisting of the plant and the controller models).

We suggest the use of Signal Temporal Logic as a candidate formalism to model such requirements. A key advantage of using STL is that in addition to Boolean satisfaction semantics on real-valued traces, it also offers quantitative semantics that indicate a degree of satisfaction of the given STL formula by a trace. This allows us to consider techniques to automatically generate interesting test cases using optimization-based approaches [1], automatically identify worst-case behaviors and temporal requirements from closed-loop models [2], and localize faults in the closed-loop model using statistical methods. We will look at some success stories from the deployment of these techniques to engineers designing production-oriented models of control systems within Toyota.

III. A HW/SW Cross-Layer Approach for Determining Application-Critical Hardware Faults in Embedded Systems (W. Kunz)

Hardware devices of recent technology nodes are intrinsically more susceptible to faults than previous devices. Early life failures contribute increasingly to testing costs and jeopardize the safety of the overall system. This calls for new methods of error detection and for a sophisticated on-chip testing infrastructure. However, any attempt to cover all errors for all theoretically possible scenarios that a system might be used in can easily lead to excessive costs. Instead, an application-dependent approach should be taken, i.e., strategies for test and error resilience must target only those errors that can actually have an effect in the situations in which the hardware is being used.

In this talk, we describe a method to inject faults into hardware (HW) and to formally analyze their effects on the software (SW) behavior [3]. We describe how this analysis can be implemented based on a HW-dependent software model called program netlist (PN). We show how program netlists can be extended to formally model the behavior of a program in the event of one or more hardware faults. A PN-based analysis is presented capturing the effects of faults in the architectural states of the system and at the software level. Then, it is shown how these results can be related precisely with gate-level faults located anywhere in the hardware. We present a method that exploits standard gate-level ATPG in combination with constraints obtained from PN-level analysis to determine hardware faults at the gate level that are "application-redundant". Our experimental results show the feasibility of the proposed approach and point out its application in safety analysis for embedded systems.

References

[1] J. V. Deshmukh, X. Jin, J. Kapinski, and O. Maler, "Stochastic local search for falsification of hybrid systems," Proceedings International Symposium on Automated Technology for Verification and Analysis, pp. 500-517, 2015

[2] X. Jin, A. Donzé, J. V. Deshmukh, and S. A. Seshia, "Mining requirements from closed-loop control models," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 34, No. 11, pp. 1704-1717, 2015

[3] C. Bartsch, C. Villarraga, D. Stoffel, and W. Kunz, "A HW/SW Cross-Layer Approach for Determining Application-Redundant Hardware Faults in Embedded Systems," Journal of Electronic Testing, Vol. 33, No. 1, pp. 77-92, 2017