CHALMERS

Design and Evaluation Techniques for Detection and Coverage Estimation of Low-Level Errors

ÖRJAN ASKERDAL

Licentiatuppsats som presenteras vid seminarium i
Henry Wallmans rum, vån 6 S, Hörsalsvägen 11, Chalmers
Fredagen den 8 december 2000, kl. 10.00

Diskussionsledare är Dr. Rolf Johansson från
CR&T, Göteborg

Avhandlingen finns tillgänglig vid:
Institutionen för datorteknik
Chalmers Tekniska Högskola
412 96 Göteborg
Telefon 031-772 1000

ABSTRACT

The evolution of fast, small and low-cost microprocessors has led to their almost pervasive usage in automotive electronics, smart gadgets, communication devices, etc. These mass-market products, when deployed in safety-critical systems, require cost-efficient and dependable (fault tolerant) functionality. In order for the system to provide any degree of reliable services, a key and critical facet is the procedure for detection of the errors that the system is expected to tolerate.

This thesis addresses and makes novel contributions in two distinct areas: (a) The design of a cost-efficient solution for detection of low-level errors, and (b) Procedures to quantitatively evaluate the effectiveness of the developed error detection techniques. We also demonstrate the viability of functional level simulations for this objective. As error detection also affects the error handling process, this dependency is considered as well.

First different error detection techniques, based on spatial, temporal or information redundancy, are surveyed. Based on the cost and safety requirements, the fault tolerant aspects of double execution, i.e. executing tasks twice and then comparing the two results, was analyzed in greater detail. The analysis showed that double execution efficiently detects data errors caused by transient faults but, also, that data errors caused by persistent faults can be detected and the detection efficiency for these errors is dependent on the task schedule.

Based on this analysis, a cost-efficient solution for detection of various errors caused by both transient and persistent faults is presented. The solution is based on double execution, complemented with assertion checks, software-implemented self-test and watchdog timers. Since these techniques detect different errors, and all can be implemented using commercial-off-the-shelf (COTS) processors, high detection efficiency, low cost, and high applicability are achieved. Furthermore, it was observed that the use of various error detection techniques could enhance error diagnosis.

To evaluate an error detection technique's efficiency, fault injection is often used to test out the various fault scenarios at the design stage, thereby reducing the evaluation time over the process of establishing confidence in the device. When evaluating the detection efficiency for errors caused by persistent faults, simulation-based fault injection is viable. Simulation implies that system and fault models must be used. The choice of model complexity is a delicate balance between simulation time and accuracy. This thesis presents a novel approach to improve this balance for functional-level simulations of component internal faults.

This work emphasizes the importance of a comprehensive view of fault tolerance.

Key words: Error Detection Techniques, Fault Tolerance, Embedded Systems, Simulation-Based Fault Injection, Double Execution, Watchdog Timers, Assertion Checks, Self-Tests, COTS