Robust Assertions and Fail-Bounded Behavior[1]

Paula Prata[&], Mário Rela[#], Henrique Madeira[#] and João Gabriel Silva[#]

[&] Universidade da Beira Interior – Dep. Informática /IT/CISUC
Rua Marquês d'Ávila e Bolama P- 6200 Covilhã, Portugal
pprata@di.ubi.pt

[#] Universidade de Coimbra - Dep. Eng. Informática /CISUC
Pinhal de Marrocos P-3030 Coimbra, Portugal
{mzrela, henrique, jgabriel}@dei.uc.pt

Abstract

In this paper the behavior of assertion-based error detection mechanisms is characterized under faults injected according to a quite general fault model. Assertions based on the knowledge of the application can be very effective at detecting corruption of critical data caused by hardware faults. The main drawbacks of that approach are identified as being the lack of protection of data outside the section covered by assertions, namely during input and output, and the possible incorrect execution of the assertions.

To handle those weak-points the Robust Assertions technique is proposed, whose effectiveness is shown by extensive fault injection experiments. With this technique a system follows a new failure model, that is called Fail-Bounded, where with high probability all results produced are either correct or, if wrong, they are within a certain bound of the correct value, whose exact distance depends on the output assertions used.

Any kind of assertions can be considered, from simple likelihood tests to high coverage assertions such as those used in the Algorithm Based Fault Tolerance paradigm. We claim that this failure model is very useful to describe the behavior of many low-cost fault-tolerant systems, that have low hardware and software redundancy, like embedded systems, were cost is a severe restriction, yet full availability is expected.

Index Terms: Hardware faults, Error detection, ABFT, Robust assertions, Failure models, Fail-bounded.

---

[1] This work was partially supported by the Portuguese Ministério da Ciência e do Ensino Superior, the FEDER program of the European Union through the R&D Unit 326/94 (CISUC) and the Group of Networks and Multimedia of the Institute of Telecommunications - Covilhã Lab, Portugal, and the project POSI/1625/95/2001 (PARQUANTUM)

The present paper is an extended evolution of the conference paper:

- J.G. Silva, P. Prata, M. Rela and H. Madeira "Practical Issues in the Use of ABFT and a New Failure Model," in 28th Int'l Symposium on Fault-Tolerant Computing, Munich, Germany, June 23-25, 1998, pp. 26-35.