Practical Issues in the Use of ABFT and a New Failure Model

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

{jgabriel,pprata,mzrela,henrique}@dei.uc.pt

[#] Universidade de Coimbra - Dep. Eng. Informática
Pinhal de Marrocos   P-3030 Coimbra - Portugal

[&] Universidade da Beira Interior – Dep. Matemática/Informática
Rua Marquês d'Ávila e Bolama   P- 6200 Covilhã, Portugal

Abstract

In this paper we study the behavior of Algorithm Based Fault Tolerance (ABFT) techniques under faults injected according to a quite general fault model. Besides the problem of roundoff error in floating point arithmetic, we identify two further weakpoints, namely lack of protection of data during input and output, and incorrect execution of the correctness checks. We propose the Robust ABFT technique to handle those weakpoints. We then generalize it to programs that use assertions, where similar problems arise, leading to the technique of Robust Assertions, whose effectiveness is shown by fault injection experiments on a realistic control application. With this technique a system follows a new failure model, that we call 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 value depends on the output assertions used. We claim that this failure model is very useful to describe the behavior of many low redundancy systems.

Keywords: Failure models, assertions, ABFTs, error detection methods, fault injection