VHDL Modelling and Analysis of Fault Secure Systems

Jason Coppens, Dhamin Al-Khalili, and Côme Rozon
Department of Electrical and Computer Engineering
Royal Military College of Canada
Kingston, Ontario K7K 7B4

Abstract

This paper presents an analysis process targeted for the verification of fault secure systems during their design phase. This process deals with a realistic set of micro-defects at the device level which are mapped into mutant and saboteur based VHDL fault models in the form of logical and/or performance degradation faults. Automatic defect injection and simulation are performed through a VHDL test bench. Extensive post processing analysis is performed to determine defect coverage, figure of merit for fault secureness, and MTTF.

1. Introduction

For systems where security and reliability are critical, the design must be tolerant to defects. These tolerant designs must identify conditions where the correct operation of the system is compromised, then react to maintain system integrity. Testing for functionality or performing conventional fault simulation are insufficient to ensure correct operation of these systems. Any verification of critical designs must be comprehensive and satisfy certain requirements. A measure of the level of confidence that one can place in a system's ability to remain fault secure becomes the deciding factor in the selection of the desired design. Therefore, the analysis methodology and the circuit modeling techniques, in conjunction with realistic operational scenarios are the main ingredients for reliable results.

There have been studies aimed at developing statistical metrics which can be applied to critical logic blocks for the determination of their fault security [1,2]. These metrics can be extracted early in the design cycle. However, the determination of the parameters used in the metric calculation is often unclear and too general, leaving in doubt the results of these calculations.

The use of fault injection has been advocated by studies to carry out verifications for fault tolerant systems [2,3,4]. Fault injection involves the deliberate introduction of faulty behavior into a circuit, which is then monitored for a response through simulation. However, most of the proposed techniques do not address the problem at the physical defect level and the implication on circuit behavior.

In contrast to the above previous approaches, the proposed process carries out automatic defect injection into the circuit allowing for technology specific analysis of system behavior in a multi-fault environment. This environment include both logical faults and performance degradation. The proposed methodology meets the goal of developing a realistic technique for the verification of the critical blocks of fault secure ASIC designs.

2. Faulty behavior and security analysis

The progression of circuit behavior from defect to failure can be illustrated by the flow of states shown in Figure 1. If the detection scheme detects the error on the output and flags it as unreliable, then the system is said to have failed secure. Otherwise, if the system's checking scheme does not flag the erroneous output as being unreliable, then the system has failed insecure. Unexcited defects (either due to defect size or input pattern excitation) are considered dormant, and unexcited faults remain latent. The detection abilities of the checking hardware determines if the transition will be to a secure or insecure failure state

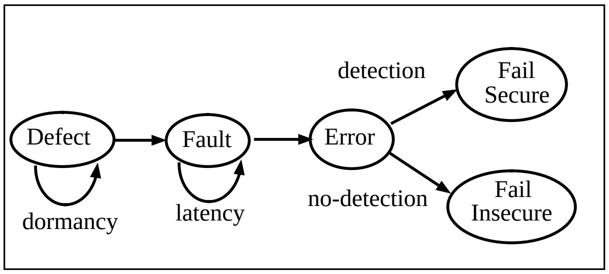

Figure 1. Defect path to failure

The analysis process proposed here has two thrusts: assurance of the fault security defects, and highlight of areas for design improvement. The requirement for an evaluation scheme is to obtain a level of confidence in the