Resumo

A evolução recente dos sistemas electrónicos tem permitido utilizá-los num número crescente de aplicações, com graus diversos de exigência na segurança de funcionamento, que não permitem algumas características dos sistemas confiáveis tradicionais, nomeadamente o custo elevado, bem como o volume e consumo de energia significativos. Na origem dessa evolução, temos a crescente densidade de integração permitida pela redução das geometrias, factores que no entanto degradam a fiabilidade dos circuitos e o seu tempo de vida, motivando um interesse crescente pela monitorização em serviço. Em paralelo, a infra-estrutura IEEE 1149.1 é cada vez mais utilizada nos testes de produção, mas raramente é activada durante o funcionamento dos componentes.

Nesta tese, e após uma introdução geral à área dos sistemas confiáveis, apresentamos em primeiro lugar a solução que denominamos CST (Concurrent Scan Test), que reutiliza a infra-estrutura 1149.1 e os vectores de teste definidos na produção, para efectuar uma monitorização concorrente do circuito de missão. Com uma sobrecarga de teste diminuta, o CST permite ainda uma tolerância a falhas restrita aos vectores de teste memorizados no controlador da infra-estrutura de teste.

Com o objectivo de expandir a aplicabilidade do CST ao projecto de sistemas tolerantes a falhas, apresentamos de seguida a arquitectura denominada XMR (Redundância Modular Incompleta), uma proposta destinada a circuitos integrados que devem tolerar as próprias falhas físicas em aplicações críticas, com um comportamento semelhante ao de uma arquitectura TMR (Redundância Modular Tripla) com intervalo de latência. A utilização de apenas duas réplicas do circuito de missão, associadas a uma infra-estrutura CST evoluída, permite confinar o erro nas células BST e votar, de forma discreta, com a informação dos vectores utilizados na monitorização.

Finalmente, e para responder às exigências que estas duas propostas colocam à fiabilidade da informação veiculada pela infra-estrutura BST, propomos o controlo de erros na transmissão, através de um bit de paridade, sem introduzir novos estados no controlador do TAP.

As propostas apresentadas foram validadas por simulação e implementação em dispositivos lógicos programáveis de média complexidade, sendo incluídas em anexo as respectivas especificações formais e os resultados da simulação.

Abstract

Recent advances in microelectronics technology enabled its usage in a growing number of applications, with varying requirements concerning the safety of operation. However, market reasons dictate that some characteristics of traditional dependable systems are not acceptable

in some applications, namely high cost and energy consumption. Sub-micron technologies and their inherent higher integration levels are the two main factors underlying the expansion of microelectronics to fault-tolerant systems, but these same factors are responsible for lower circuit reliability and a shorter life span, leading in turn to an increased interest for circuit monitoring during on-line operation. Independent of this fact, but of relevance in the context of this work, boundary scan became an important production test technology, steadily growing in acceptance since its approval as an IEEE standard in 1990. However, and in spite of the powerful operating modes provided by this test infrastructure, it is very seldomly used during normal circuit operation.

Following a general introduction to the characteristics of dependable systems, the Concurrent Scan Test (CST) proposal is presented, which reuses the 1149.1 infrastructure and the production test vectors, to enable concurrent monitoring of the mission circuits during system operation. The CST proposal has very low overhead in relation to the standard boundary scan infrastructure and enables a discrete fault tolerance mode, synchronous to the operation of the mission circuit and restricted to those vectors stored in the test controller memory.

The Incomplete Modular Redundancy (XMR) proposal is then presented, enabling the design of fault-tolerant systems based in the CST infrastructure. The XMR architecture addresses an application scope consisting of those integrated circuits required to withstand internal physical faults in safety-critical applications, and its operating characteristics are similar to those of a Triple Modular Redundancy (TMR) system with a latency interval. The use of only two replicas of each mission circuit, associated to an extended CST infrastructure, enables fault confinement in the boundary scan cells and the implementation of a discrete voting procedure, using the information contained in the set of test vectors used for concurrent monitoring. Besides enabling the detection of common mode faults in the replicas of the mission circuit, the XMR architecture can be integrated in a single component, with a better cost-benefit ratio, when compared to the alternatives traditionally available.

The information transmitted through the boundary scan infrastructure during concurrent monitoring has higher reliability requirements, due to the problems that may be caused by an error in the bit stream. To meet this requirement, the last chapter in this thesis proposes error detection through a parity control bit. This method does not require additional TAP controller states and retains the traditional state transition path for each test vector, if an error in the bit stream is allowed into the update stage during a short time interval, or enables detection before update, if two additional state transitions are acceptable.